Privilege Management for Unix and Linux 22.3
Installation Guide

Table of Contents

Privilege Management for Unix and Linux Installation Guide

This guide provides the information that is needed to perform a basic installation of the Privilege Management for Unix and Linux software.

> 📌 *Note: Privilege Management for Unix and Linux refers to the product formerly known as PowerBroker for Unix and Linux.*

> 📌 *Note: Specific font and line spacing conventions are used to ensure readability and to highlight important information, such as commands, syntax, and examples.*

> ⊘ **IMPORTANT!**
>
> *The BeyondInsight integration for Privilege Management for Unix and Linux is no longer supported. Instead, PMUL uses BeyondInsight for Unix & Linux and ElasticSearch.*

> ⊘ **IMPORTANT!**
>
> *Both **pbguid** and **pbsguid** are deprecated as of PMUL version 22.3.0.*

Sample Policy Files

When you install Privilege Management for Unix and Linux, you can choose to copy sample Privilege Management for Unix and Linux policy files to the installation host. These sample policy files include detailed explanations of what they do. You can use these files to learn how policy files are typically written for various scenarios. The directory that these sample files are copied to is determined by the GUI library directory option that you specify during installation. By default, this directory is **/usr/local/lib/pbbuilder**. A **readme_samples** text file in that directory includes a brief description of each sample file.

Installation Considerations

Privilege Management for Unix and Linux is a non-intrusive software program that does not require kernel reconfiguration, a system reboot, or the replacement of system executable files. The items in this section contain information you should consider when planning your implementation.

> **⊘ IMPORTANT!**
>
> *The BeyondInsight integration for Privilege Management for Unix and Linux is no longer supported. Instead, PMUL uses BeyondInsight for Unix & Linux and ElasticSearch.*

> ℹ *For information on the platforms and operating systems that are supported by Privilege Management for Unix and Linux, please see Supported Platforms at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

Flavor and Release Definitions

Flavor is a BeyondTrust term that defines a build of a BeyondTrust product, such as Privilege Management for Unix and Linux, that is compiled and tested for a certain range of operating system versions and underlying hardware. For instance, when this guide was written, Privilege Management for Unix and Linux was available for several flavors of Linux operating systems. The included README file describes which flavor is the right match for specific combinations of hardware and operating systems in the **Release Identifier** column. The release identifier is the flavor plus the version of the Privilege Management for Unix and Linux distribution.

BeyondTrust product releases are uniquely identified by a string that indicates their hardware and software characteristics. This string contains the following information:

- BeyondTrust product
- Hardware architecture
- Flavor
- Major version number
- Minor version number
- Release number
- Build number
- Service pack number

An example version number in the extracted tarball directory path is: **pmul_linux.x86-64_10.3.0-15**

- **pmul** is the BeyondTrust product Privilege Management for Unix and Linux.
- **linux** is the flavor.
- **x86-64** is the hardware architecture.
- **10** is the major version number 3 is the minor version number 0 is the release number.
- **15** is the build number.

Functionality is identical for all releases with the same version number. Releases within a version denote a maintenance release and include new ports and resolved issues. Release notes describe the issues that are addressed by the release.

TC: 12/7/2022

> **⚠ IMPORTANT!**
>
> *If you believe you are using the correct Privilege Management for Unix and Linux version for the system but the installer is returning a flavor mismatch error, please contact BeyondTrust Technical Support for assistance.*

Interactive Versus Packaged Installation

All Privilege Management for Unix and Linux flavors can be installed by using an interactive program that presents you with a series of options. Your choices determine the details of the Privilege Management for Unix and Linux installation for a particular host.

The client registration facility can be used to automate the installation of new clients by downloading the default configuration from the primary license server. Options are defaulted within the interactive installation, and shared encryption keys are copied over.

For certain flavors, Privilege Management for Unix and Linux can be installed by using package installers. Package installers enable you to choose the options once, and then install that configuration of Privilege Management for Unix and Linux non-interactively on multiple identical hosts. Using package installers also takes advantage of the operating system's installation management system, which tracks the source of installed files and enables their safe removal.

> ℹ️ *For more information, please see Supported Platforms at https://www.beyondtrust.com/docs/privilege-management/unix-linux/supported-platforms.htm.*

Interactive and Packaged Installations on the Same Computer

Although it is possible to combine interactive and packaged Privilege Management for Unix and Linux installations on the same computer, we do not recommend this practice. If both interactive and packaged installations are present, and you remove the packaged installation, the shared libraries are removed even though they are needed by the interactive installation. This behavior is inherent in all package installations and is not specific to Privilege Management for Unix and Linux.

In the case of SELinux, if you attempt to perform a package installation on a computer that already has an interactive installation present, the package installation is not allowed. The reason for this limitation is that the SELinux Privilege Management for Unix and Linux packages can fail to install because RPM does not have the permissions to change SELinux file types that are already installed.

If you must combine interactive and packaged Privilege Management for Unix and Linux installations on the same computer, follow these recommendations:

- For the interactive installation, use a prefix and suffix installation.
- Install the shared libraries for the interactive and packaged installations in separate directories, by doing one of the following:
  - In the interactive installation, specify an alternative shared library directory with the BeyondTrust built-in third-party library directory menu item.
  - Use the relocatable base directory feature of the package installer.

> 📌 *Note: Privilege Management for Unix and Linux SELinux policies are no longer provided. When installing Privilege Management for Unix and Linux on Red Hat Enterprise Linux (RHEL) 5 with SELinux enabled and using the targeted policy, Privilege Management binaries run unconfined.*

Prefix and Suffix Installations

Privilege Management for Unix and Linux can be installed with prefixes or suffixes to create unique installations for multiple installs or for ease of identification.

> 📌 *Note: Prefixes and suffixes cannot be used with any of the package installers.*

> **i** *For instructions about using prefixes and suffixes for a Privilege Management for Unix and Linux installation, please see "Prefix and Suffix Installation Instructions" on page 89.*

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

10

Resource Overhead

There are not any startup or shutdown programs associated with Privilege Management for Unix and Linux. From a system resource perspective, a basic Privilege Management for Unix and Linux session uses about the same overhead as a telnet session with additional front-end work for processing the policy security file. I/O logging can add the equivalent of another telnet session.

Instances of the Privilege Management for Unix and Linux daemons, **pbmasterd** and **pblocald**, are requested by **pbrun** and are actually started by the superdaemon when a monitored task request is submitted to pbrun. Instances of the Privilege Management for Unix and Linux log server daemon, **pblogd**, are actually started by the superdaemon. The superdaemon is **inetd**, **xinetd**, **launchd**, or **SMF** depending on the platform.

> 📌 **Note:** *Within this guide, references to **inetd**, **xinetd**, **launchd**, and **SMF** are used interchangeably unless otherwise denoted.*

For systems based on RedHat version 7+, **xinetd** is no longer installed by default, since it has been superceded by **systemd**, which is an init system. The installation program of Privilege Management for Unix and Linux performs a check to see if **systemd** exists and is functional. If it exists, it configures Privilege Management for Unix and Linux daemons to be managed by **systemd**. If **systemd** is not present, the installation program checks if **xinetd** is installed and running and displays a warning message if it is not.

Having the superdaemon start **pblogd**, **pbmasterd**, and **pblocald** when requested by **pbrun** is the normal way to initiate the Privilege Management for Unix and Linux daemons. It is also possible to explicitly start the daemon as a persistent daemon.

> 📌 **Note:** *The terms **monitored task** and **secured task** are interchangeable.*

SSL adds some startup overhead for certificate exchange and verification. The encryption overhead is slightly larger than self-contained encryption technologies (such as DES) because of the use of packet checksums by SSL.

> 📌 **Note:** *Privilege Management for Unix and Linux requires 10 to 50MB of disk space, depending on the installation options selected.*

> ℹ️ *For more information, please see the* Privilege Management for Unix and Linux *Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

Required Utilities for Privilege Management for Unix and Linux

The Privilege Management for Unix and Linux installer requires the following Unix and Linux utilities and built-in commands:

awk	cut	getopt	ps	sort	unset
basename	date	grep	pwd	stty	vi
cat	diff	id	read	tar	wc
cd	dirname	kill	rm	tee	xargs
chmod	df	ls	rmdir	touch	
chown	echo	mkdir	sed	tr	
cksum	eval	more	set	trap	
clear	exec	mv	shift	umask	
cp	export	od	sleep	uname	

Installation Directories

Privilege Management for Unix and Linux is not sensitive about the location of its binary files; you can place them in any convenient directory. However, there are a few points to consider when you are selecting installation directories:

- It is important to install the Privilege Management for Unix and Linux **pbrun** and **pbssh** programs in a directory that is in the user's path.
- Online manuals (such as user man pages and Privilege Management for Unix and Linux documentation) should be accessible from every computer to enable users to get online help for Privilege Management for Unix and Linux programs.

Default Directories

The following table lists various Privilege Management for Unix and Linux components and their locations. The installation script uses these locations by default, but you can change them during installation. Usually **/usr/local/bin** is used for user programs and **/usr/sbin** for administrator and daemon programs (depending on the platform).

Default Directories for Privilege Management for Unix and Linux Components

Directory	Files	Description
/etc (v9.4.1 and earlier) **/opt/pbul/policies** (v9.4.3+)	**pb.conf**	Default policy. Includes **/etc/pb/pbul_policy.conf** (v9.4.1 and earlier) **/opt/pbul/policies/pbul_policy.conf** (v9.4.3+)
/etc/pb (v9.4.1 and earlier) **/opt/pbul/policies** (v9.4.3+)	**pbul_policy.conf**	Main policy containing the following roles: • Helpdesk role • PBTest (connectivity test) • Controlled Shells • Admin Role • Demo Role • Splunk Role • Sudo Role
/etc/pb (v9.4.1 and earlier) **/opt/pbul/policies** (v9.4.3+)	**pbul_functions.conf**	Functions and procedures implementing the roles in **pbul_policy.conf**
/etc	**pb.key**	Encryption key
	pb.settings	Privilege Management for Unix and Linux configuration file (server-side component)
	pbsudo.settings	Privilege Management for Unix and Linux configuration file (client component)
/usr/adm, **/var/adm**, or **/var/log**	**pb.eventlog**	Default event log file
	pblocald.log	**pblocald** diagnostic log file
	pblogd.log	**pblogd** diagnostic log file
	pbmasterd.log	**pbmasterd** diagnostic log file

Directory	Files	Description
	pbrun.log	**pbrun** diagnostic log file
	pbssh.log	**pbssh** diagnostic log file
	pbsync.log	**pbsync** diagnostic log file
	pbsyncd.log	**pbsyncd** diagnostic log file
/usr/local/bin	**pbbench**	Utility
	pbcall	Utility
	pbksh	Utility
	pbless	Utility
	pbmg	Utility
	pbnvi	Utility
	pbrun	Utility
	pbssh	Utility
	pbumacs	Utility
	pbsh	Utility
	pbvi	Utility
/usr/local/lib/pbbuilder		Contains the various GUI and **pbguid** components. Do not make any changes in this directory.
/usr/sbin	**pbdbutil**	Utility providingPrivilege Management database maintenance.
	pbcheck	Utility
	pbencode	Utility
	pbkey	Utility
	pblocald	Daemon
	pblog	Utility
	pblogd	Daemon
	pbmasterd	Daemon
	pbpasswd	Utility
	pbreplay	Utility
	pbsum	Utility
	pbsync	Utility
	pbsyncd	Daemon
	pbversion	Utility
/opt/pbul/dbs	**pbsudo.db**	Database files generated and used by Privilege Management for Unix and Linux
	pbsvc.db	
	pbsvccache.db	
	pbdbsync.db	
	pbregclnt.db	

Directory	Files	Description
	pbrbpolicy.db	
	pbevent.db	
	pbfim.db	
	pbrstkeys.db	
	pblogarchive.db	
	pblogcache.db	

The default log directory varies by platform to match that platform's conventions. The directories **/usr/adm**, **/var/adm**, and **/var/log** are used interchangeably throughout as the default location of the Privilege Management for Unix and Linux log files.

Change /opt/pbul Base Directory

As seen in the previous table, files that Privilege Management for Unix and Linuxgenerates at runtime are created under **/opt/pbul**. If you want to change this default location, use pbinstall's **basedir** menu to specify a directory location.

If there is no previous settings file, or if you are running **pbinstall -i** to ignore previous settings, changing **basedir** will cause the following settings to be updated with the new location and enabled to ensure that runtime files do not end up in the old default location:

Keyword	Value
basedir	**<basedir>**
databasedir	**<basedir>/dbs**
lockfilepath	**<basedir>/locks**
scriptdir	**<basedir>/scripts**
licensestatsdb	**<basedir>/dbs/pblicense.db**
licensestatswq	**<basedir>/dbs/pblicense.wq**
pbrestkeyfile	**<basedir>/pbrstkeys.db**
schedulingservicedb	**<basedir>/dbs/pbsched.db**
messageroutersocketpath	**<basedir>/msgrouter**
writequeuepath	**<basedir>/msgrouter**
clntregdb	**<basedir>/dbs/pbregclnt.db**
eventdb	**<basedir>/dbs/pbevent.db**
odbcinidir	**<basedir>/etc**
servicedb	**<basedir>/dbs/pbsvc.db**
svccachedb	**<basedir>/dbs/pbsvccache.db**
dbsyncdb	**<basedir>/dbs/pbdbsync.db**
policypersistentvariabledb	**<basedir>/dbs/pbpolpersistvar.db**
policydir	**<basedir>/policies**
policyfile	**<basedir>/policies/pb.conf**
policydb	**<basedir>/dbs/pbrbpolicy.db**
sudoersdb	**<basedir>/dbs/pbsudo.db**

Keyword	Value
sudoersdir	<basedir>/sudoersdir
logarchivedb	<basedir>/dbs/pblogarchive.db
logcachedb	<basedir>/dbs/pbiologcache.db
iologcachedb	<basedir>/dbs/pbiologcache.db
integratedproductsqueuedb	<basedir>/dbs/pbintprodq.db
iologactiondb	<basedir>/dbs/pbiologaction.db
advkeystrokeactionpolicydb	<basedir>/dbs/pbadvkeystrokeactionpolicy.db
advkeystrokeactioncachedb	<basedir>/dbs/pbadvkeystrokeactioncache.db
elasticsearchidxtemplate	<basedir>/elk/etc/pbelasticsearchtemplate.json
siemcachedb	<basedir>/dbs/pbsiemcache.db
elkcreddb	<basedir>/dbs/pbelkcred.db
dequeuedatabasedir	<basedir>/dequeuedbs
fileintegritydb	<basedir>/dbs/pbfim.db
fileintegritysignaturesdb	<basedir>/dbs/pbfimsignatures.db
elkecsconfiguration	<basedir>/elk/etc/pbelkecsconfiguration.json

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

16

System File Modifications

Privilege Management for Unix and Linux does not replace any Unix and Linux files or binaries during installation, but it does modify the following system files:

- **/etc/inetd.conf** (or **xinetd.conf**, **launchd**, **systemd** or **SMF** configuration file)
- **/etc/services**

These files are automatically backed up as files with the same name and the extension **.sybak.####**.

The changes made to these files depend on whether a policy server host, run host, GUI host, log synchronization host, or log host is being installed. Depending on the selected installation options, each file has lines removed, added, or both.

For **/etc/inetd.conf** (or your **xinetd.conf**, **launchd**, or **SMF** configuration), the installer tries to determine the superdaemon configuration file that is used on the active system. Most systems use the superdaemon's default configuration file name while the rest of the systems use a switch or command line format. This makes it possible to determine the superdaemon's configuration files that need to be configured. **xinetd** uses **/etc/xinetd.conf** and any specified **includedir** file directories.

> *Tip: Removal of earlier releases of Privilege Management for Unix and Linux with version 6.0 checks for and removes its xinetd configuration.*

SMF is used on Solaris 10+ and uses a configuration database.

Starting with version 7.1.0, if the system Privilege Management for Unix and Linux is being installed on is IPv6-capable and the configuration of **inetd**, **xinetd**, **SMF** (Solaris), is being performed, the super daemon configuration is set for IPv6 rather than IPv4.

Privilege Management for Unix and Linux Policy Files

/opt/pbul/policies/pb.conf (from v9.4.3+ and **/etc/pb.conf** prior to v9.4.3) is usually the root or entry point to the Privilege Management for Unix and Linux policy tree. Although **pb.conf** can contain actual policy code, we recommend that you use it strictly as a list of **include** statements that reference other policy modules. Referencing other policy modules in the **pb.conf** file keeps a large policy tree manageable.

> ℹ️ *For more information about policy files, please see the* Privilege Management for Unix and Linux *Policy Language Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

Role Based Policy Database

With the introduction *Privilege Management for Unix and Linux* version 9, there is a Role Based Policy Database. Role Based Policy simplifies 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. It also simplifies bulk import and bulk export of data. Once the customers data is held within the Role Based Policy database, it is much easier to provide management information, such as user entitlement reports. This can be used instead of policy script configuration to quickly and succinctly define, retrieve, and report on role based policy.

> ℹ️ *For more information, please see the* Privilege Management for Unix and Linux Administration Guide *at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

Default Policies

Starting with version 8.0.0, a default policy is installed by default if an existing policy does not exist. The files **pbul_policy.conf** and **pbul_functions.conf** are created in the **/opt/pbul/policies** directory by default. **pbul_policy.conf** is included in the main policy by default **/opt/pbul/policies/pb.conf** from v9.4.3+ and **/etc/pb.conf** prior to v9.4.3.

This default policy contains the following roles.

Helpdesk Role

- Enabled by default. When invoking **pbrun helpdesk**, the role allows any user in HelpdeskUsers (default **root**) to initiate a Helpdesk Menu as **root** on any host in HelpdeskHosts (default submithost only). The actions include
  - Obtaining a list of processes (**ps -ef**)
  - Checking if a machine is available (**ping <host>**)
  - Obtaining a list or current users on this host (**who -H**)
  - Displaying the Host's IP settings (**ifconfig -a**)

PBTest

- Enabled by default for all users on all hosts. The role allows **pbrun pbtest** to be used to check connectivity and the policy.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

18

TC: 12/7/2022

Controlled Shells

- Enabled by default. The role allows users in **ControlledShellUsers** (by default the submituser) for runhosts in **ControlledShellHosts** (by default only submithost) to enable I/O logging for **pbksh/pbsh**. I/O logs are created by default in **/tmp/pb.<user>.<runhost>.<YYYY-MM-DD>.[pbksh|pbsh].XXXXXX**. This role has a list of commands (empty by default) to elevate privileges for as well as a list of commands (empty by default) to reject.

Admin Role

- Enabled by default. The role allows users in **AdminUsers** (by default **root**) to run any command on runhosts in **AdminHosts** (by default only submithost).

Demo Role

- Disabled by default. The role allows users in **DemoUsers** (default all users) to run commands in **DemoCommands** (default **id** and **whoami**) as **root** on any host in **DemoHosts** (default all hosts).

Splunk Role

Disabled by default. If enabled, only when pbrun is invoked, enables iologging (creating iologs in **/pbiologs**), sets default ACA rule, enables aca session history and sets **iologcloseaction** to a script sending records to Splunk.

Sudo Role

Disabled by default, allows users in **SudoUsers** (only **root**, by default) to run any command on runhosts defined in **SudoHosts** (default submithosts).

This serves as a demo policy for the sudo wrapper which requires policy modification before it is installed. It illustrates what changes to start with to make all the sudo wrapper options available.

The policy ends by allowing all users to run any command as themselves without any privilege escalation.

Network and File Encryption

Privilege Management for Unix and Linux can encrypt data to help guard against attacks. Several encryption modes are supported. The installation script uses the **pbkey program** to create an encryption key in the key file, **/etc/pb.key**. This file must then be placed on all Privilege Management for Unix and Linux systems in a Privilege Management for Unix and Linux installation.

Because the **pb.settings** file is required to be in the **/etc** directory, the key file used to encrypt **pb.settings** must also be in the **/etc** directory.

> *Note: A key file can be added to the installation when using **pbinstall**. For more information about the key file, please see "Installation Process" on page 30.*

> *For more information about encryption, or for about Kerberos and SSL, please see the Privilege Management for Unix and Linux Admin Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

Configure Third-Party Libraries

When Privilege Management for Unix and Linux is configured with Kerberos, SSL, LDAP, or CURL, it requires the appropriate third-party libraries. The Privilege Management for Unix and Linux installation provides Kerberos, SSL, LDAP, or CURL libraries that are designed to work with Privilege Management for Unix and Linux. It is recommended that you install the Privilege Management for Unix and Linux third-party libraries. However, you do have the option of using your own third-party libraries.

> **⚠ IMPORTANT!**
>
> *Shared libraries can be adversely affected when both interactive and packaged Privilege Management for Unix and Linux installations are present on the same computer. For more information, please see "Installation Preparation" on page 25.*

Use Privilege Management for Unix and Linux Third-Party Libraries

If you have your own Kerberos, SSL, LDAP, or CURL libraries but wish to use Privilege Management for Unix and Linux third-party libraries, you should do one of the following:

- Remove your libraries from **/usr/lib** or **/lib** and point to the Privilege Management for Unix and Linux third-party libraries in **/usr/lib/beyondtrust/pb** or **/usr/lib/symark/pb** in **pb.settings**.
- Replace your third-party libraries with the Privilege Management for Unix and Linux third-party libraries in **/usr/lib** or **/lib** and specify this directory in **pb.settings**.

Third-Party Library File Names and Locations

If you are installing Privilege Management for Unix and Linux shared libraries, the following files are installed:

- Kerberos:
    - **llibcom_err.so.3.0**
    - **libk5crypto.so.3.1**
    - **libkrb5support.so.0.1**
    - **libkrb5.so.3.3**
    - **libgssapi_krb5.so.2.2**
- SSL:
    - **libcrypto.so.1.1**
    - **libssl.so.1.1**
- LDAP:
    - **liblber-2.5.so.0.1.7**
    - **libldap-2.5.so.0.1.7**
- CURL:
    - **libcurl.so.4.8.0**

Shared Library Directory Location for AIX and HP (PA RISC)

For AIX and HP (PA-RISC), the directory for installing third-party libraries must be in one of the following locations:

- **/usr/lib/beyondtrust/pb**
- **/usr/lib**
- **/lib**
- **/usr/local/lib**

If any other directory is specified, it is rejected with an error message that instructs you to use one of these directory locations.

Shared Library File Name for AIX

The notation used on AIX to specify LDAP libraries is different from other platforms. On AIX, for archived third-party libraries, you need to specify the shared object that is a member of the archive and add it to the file name.

The notation for default LDAP libraries is:

- **/usr/lib/beyondtrust/pb/liblber-2.5.a(liblber-2.5.so.0)**
- **/usr/lib/beyondtrust/pb/libldap-2.5.a(libldap-2.5.so.0)**

For example, if **libcom_err.a.3.0** is an archive and **shr.0.3.0** is the actual shared object, the file specification for the member of the archive is **libcom_err.a.3.0(shr.0.3.0)**.

> *Note: For SSL and Kerberos, it is not necessary to alter the file name because the library is not an archive.*

Use Your Own Third-Party Libraries

If you have chosen to configure Privilege Management for Unix and Linux with Kerberos, SSL, or LDAP, and do not load Privilege Management for Unix and Linux built-in third-party libraries, you must specify your own shared library file names. If you have Kerberos, SSL, or LDAP libraries of your own in **/usr/lib** or **/lib** and you are using them for other applications, you need to use your libraries for Privilege Management for Unix and Linux as well and not use any of the libraries in **/usr/lib/beyondtrust/pb** or **/usr/lib/symark/pb**. During the Privilege Management for Unix and Linux installation, specify **no** for the install option **Install BeyondTrust built-in libraries**, and then enter the appropriate shared library directory and filename.

> *For more information about the installation instructions, please see "Advanced Installation Instructions Using pbinstall" on page 46.*

Install Third-Party Libraries in Future Installations

If you do not enable the third-party libraries during the Privilege Management for Unix and Linux installation and in the future you decide to enable Kerberos, SSL, or LDAP in your Privilege Management for Unix and Linux policy, then you must do the following:

- Install Privilege Management for Unix and Linux third-party libraries or your own third-party libraries.
- In the **pb.settings** file, do one of the following:
  - If you are using the Privilege Management for Unix and Linux third-party libraries, specify the directories to install the operating system third-party libraries in by setting the following keywords to specify the full path and library file names:
    - **sharedlibkrb5dependencies**
    - **sharedlibssldependencies**
    - **sharedlibLDAPdependencies**
    - **sharedlibcurldependencies**

If you are using your own third-party libraries, then perform the following actions.

- Specify the Kerberos library setting and provide the full path and library file names.
- Specify the SSL library setting and provide the full path and library file names.
- Specify the LDAP library setting and provide the full path and library file names.
- Specify the CURL library setting and provide the full path and library file names.
- Ensure that your libraries are listed in the correct order. For example, if lib1 is dependent on lib2, you must list lib2 first, followed by lib1.

Improve Security

Additional configuration can improve the security of Privilege Management for Unix and Linux.

Privilege Management for Unix and Linux does not contain a Certificate Authority; therefore, certificates generated during install are self-signed, and cannot be used to properly identify the host. Creating and deploying proper x509 certificates, with hostname information in the Subject Alternative Name field, allows Privilege Management for Unix and Linux hosts to properly identify hosts.

TLS clients can verify the server's certificate and hostname by adding the **ValidateServer** option to the **ssloptions** keyword in **/etc/pb.settings**. For TLS, **pbmasterd** and **pblocald** are clients to **pblogd**. Additionally, servers can validate the certificates and hostname of the client hosts by adding the **ValidateClients** option to the **ssloptions** keyword in **/etc/pb.settings**.

Configure Privilege Management for Unix and Linux to use the **SSLFirst** keyword in **/etc/pb.settings**. This keyword must have the same value on all hosts in the Privilege Management for Unix and Linux domain. The **SSLFirst** keyword results in SSL/TLS occurring prior to any Privilege Management for Unix and Linux proprietary protocol negotiations (that use symmetric keys), reducing any issue with compromised symmetric network encryption keys.

The TLS ciphers should be changed to disallow anonymous ciphers.

Edit the **sslpbruncipherlist** and **sslservercipherlist** entries in **/etc/pb.settings**:

```
sslpbruncipherlist        TLSv1.2:!SSLv2:!3DES:!MD5:!ADH:!AECDH:!DHE:!eNULL:@STRENGTH
sslservercipherlist       TLSv1.2:!SSLv2:!3DES:!MD5:!ADH:!AECDH:!DHE:!eNULL:@STRENGTH
```

Edit the **ssl.cipher-list** entry in **/usr/lib/beyondtrust/pb/rest/etc/pblighttpd.conf**:

```
ssl.cipher-list           = " TLSv1.2:!SSLv2:!3DES:!MD5:!ADH:!AECDH:!DHE:!eNULL:@STRENGTH"
```

Installation Preparation

This section lists the items that you need to plan for and be aware of before starting the Privilege Management for Unix and Linux installation.

Pre-installation Checks

pbulpreinstall.sh performs some basic preinstallation checks such as:

- Checks hostname resolution and DNS and name services resolution to verify that the default ports are not in use.
- Checks for sufficient disk space.
- Reports technical support-related information such as the operating system, NIC information, gateway, and super daemon status. If Privilege Management for Unix and Linux is already installed, the Privilege Management for Unix and Linux roles such as **submithost**, **runhost**, **policy perver**, **logserver**, and **pbx** are reported.

This script has an optional **-t <datetime in UTC>** argument, which initiates a time verification check. This check simply validates that the host's time is within 60 seconds of the time specified. The time specified must be UTC, in the format 20130827154130, such as:

date -u '+%Y%m%d%H%M%S'

This script has an optional **-f** argument, which causes **pbulpreinstall.sh** to produce machine readable output intended for the BeyondInsight for Unix & Linux installation console.

Prior to installation, the **pbulpreinstall.sh** script is located in the Privilege Management for Unix and Linux distribution in the following directory **powerbroker/<version>/<flavor>/install**. After installation, this script is installed in the **'$inst_admin'** directory. **/usr/sbin** is the default.

Obtain a License Validation Key

To install Privilege Management for Unix and Linux, you need a license string, which is provided by your BeyondTrust sales representative.

Privilege Management for Unix and Linux primary license server hosts perform the license resolution functions for Privilege Management for Unix and Linux and are the only Privilege Management for Unix and Linux host types that require a license key. For a policy server host to accept a task, the primary license server must have a current valid license key. The distribution includes a temporary license key with a two month expiration date from the date of the installation.

If installing using **pbinstall**, the license key may be configured during installation using the Privilege Management for Unix and Linux license installation menu item. After the installation is complete, the Privilege Management for Unix and Linux license can also be added using the **pbadmin --lic -u** command.

Obtain root Access

Installation of the Privilege Management for Unix and Linux product requires root access.

Plan Privilege Management for Unix and Linux Hosts

A Privilege Management for Unix and Linux installation includes several host types, each of which performs specific functions. Prior to installation, you need to determine which host type needs to be placed on the individual machines in your environment.

> 📌 **Note:** *Privilege Management for Unix and Linux must be installed separately on each machine running any type of Privilege Management for Unix and Linux host.*

Select License Servers

Determine which hosts to use as license servers. These are the machines that perform the license resolution functions for Privilege Management for Unix and Linux. These hosts are the only types that require a license key. They store and maintain the product license, parameters, and usage information.

The first installation of Privilege Management for Unix and Linux becomes the primary license server. Subsequent license server installations obtain their data when the primary license server performs synchronization.

Select Submit Hosts

Select Submit Hosts determines which machines to use as submit hosts. These are the machines where **pbrun** is installed and executed. **pbrun** is the Privilege Management for Unix and Linux utility used to submit secure tasks that might run on the same or different hosts. At minimum, one submit host must be available to process monitored task requests.

Select Run Hosts

Determine which machines to use as Privilege Management for Unix and Linux run hosts. These are the machines where **pblocald**, **pbsh**, and **pbksh** are installed and executed. **pblocald** is the daemon process that executes secure tasks. At minimum, one run host must be available to process accepted task requests.

Multiple Privilege Management for Unix and Linux components can be installed on a single machine. For example, it is possible for a single physical machine to serve as a submit host, policy server host, run host, log host, and log sync host.

Select Policy Server Hosts

Determine which machines to use as Privilege Management for Unix and Linux policy server hosts. These are the machines where **pbmasterd** is installed and executed. **pbmasterd** is the daemon process that accepts or rejects all tasks that are submitted by submit hosts, and if accepted, it authorizes a specific run host to execute each task. The policy server host is where policy files reside (by default **/opt/pbul/policies/pb.conf** from v9.4.3+ and **/etc/pb.conf** prior to v9.4.3). Any policy files referenced by include statements are also in the policy file.

There must be at least one policy server host in a Privilege Management for Unix and Linux installation. We recommend that a second, failover policy server host also be installed and have the same policy files as the primary policy server host to give redundancy to your Privilege Management for Unix and Linux installation.

Depending on the size of your Privilege Management for Unix and Linux environment and the volume of tasks executed through the Privilege Management for Unix and Linux system, it may be desirable to add additional Privilege Management for Unix and Linux policy server hosts to your Privilege Management for Unix and Linux installation. Additional Privilege Management for Unix and Linux policy server hosts can be added during the initial installation of Privilege Management for Unix and Linux or afterward.

Select Log Hosts

Using a log host to record event and I/O logs is optional. To use this feature, determine which machine (or machines) to use as Privilege Management for Unix and Linux log hosts. This machine is where **pblogd** is installed and executed. For Privilege Management for Unix and Linux, if a log host is not used, **pbmasterd** and **pblocald** are responsible for logging activities. As with policy server hosts, multiple log

hosts are recommended to provide redundancy. When there is a log host failover, the log synchronization utilities in Privilege Management for Unix and Linux can be used to resynchronize the log entries.

The load on the log hosts varies with the amount of logging performed. I/O logs require greater resources on the log hosts. Additional log hosts can be added to your environment during installation or afterward, as needed.

Enable Log Synchronization Host

Log synchronization enables a log host, or a policy server host that is acting as a log host, to participate in log synchronization. Install the log synchronization component on any log host or policy server host that may participate in log synchronization. Log synchronization should be installed on each log or policy server host if you are installing primary and failover log hosts, or are installing policy server hosts that are acting as log hosts.

If log synchronization is used, then one or more machines need to have the ability to initiate log synchronization.

Privilege Management for Unix and Linux Utilities

Using the Privilege Management for Unix and Linux utilities is optional. The Privilege Management for Unix and Linux utilities are secured versions of vi, nvi, mg, umacs, and less. Privilege Management for Unix and Linux utilities can only be installed on a machine where a Privilege Management for Unix and Linux run host is installed.

Privilege Management for Unix and Linux Shells

Using the Privilege Management for Unix and Linux shells is optional. ThePrivilege Management for Unix and Linux shells are secured versions of the Korn Shell and the Borne Shell. The Privilege Management for Unix and Linux & Linux shells can be installed only on a machine where a Privilege Management for Unix and Linux submit host is installed.

Select Port Numbers

You need to decide whether to use the Privilege Management for Unix and Linux default port numbers or to specify your own. Privilege Management for Unix and Linux uses the following default port numbers:

pbmasterd	24345
pblocald	24346
pblogd	24347
pbguid	24348
pbsguid	24349
pbsyncd	24350
pbrestport	24351

If you decide to change the port number defaults, be sure to choose port numbers that do not conflict with those already in use. See **/etc/services**. Also, if present and active, review the services NIS map. Privilege Management for Unix and Linux port numbers must use the non-reserved system ports. The allowed port numbers are 1024 to 65535.

Select Installation Directories

Decide whether to use the Privilege Management for Unix and Linux default installation directories or to specify your own. Specifying your own installation directories allows for Privilege Management for Unix and Linux optimization of the local installation.

Select syslog

Use of syslog is optional. Determine if the policy server host, run host, submit host, log sync host, and/or log host should generate syslog records when system error conditions are encountered.

Select Encryption

By default, Privilege Management for Unix and Linux installs with AES-256 encryption; however, it can support a large number of encryption technologies. In Privilege Management for Unix and Linux v3.0 and earlier, DES and 3DES are supported. Beginning with Privilege Management for Unix and Linux v3.2, many additional encryption modes are supported.

> *Prior to selecting which encryption technology you plan to use, please see the Privilege Management for Unix and Linux Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

Firewalls

Privilege Management for Unix and Linux can be used in a firewall environment with special configuration.

> *If you are installing Privilege Management for Unix and Linux into an environment where the Privilege Management for Unix and Linux components need to communicate across firewalls, please see the Privilege Management for Unix and Linux Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm before installing.*

Use NIS

Privilege Management for Unix and Linux can use NIS to provide configuration services for Privilege Management for Unix and Linux settings. Netgroups can be defined for the Accept policy servers (**pbacceptmaster**), Submit solicy servers (**pbsubmitmasters**) and log host (**pblogservers**) settings. NIS can also be used to provide port lookup information for the Privilege Management for Unix and Linux components. If NIS is running in your environment, consider using Privilege Management for Unix and Linux netgroups and port definitions.

Verify Proper TCP/IP Operation

Privilege Management for Unix and Linux uses TCP/IP as its communication protocol. Therefore, it is essential that TCP/IP be working correctly before Privilege Management for Unix and Linux installation. Use programs such as ping, netstat, route, or traceroute to verify correct TCP/IP operation among all hosts that will have Privilege Management for Unix and Linux components installed.

Verify Network Host Information

Ensure that each network host knows the names and addresses of all other network hosts. Network host information is generally stored in the **/etc/hosts** file on each network host machine or in the NIS maps or DNS files on a server. Each submit host should resolve all of the policy server host names correctly. Each policy server host should resolve all submit, run, GUI, and log host names correctly. The resolution must work correctly in both directions: name-to-IP address and IP address-to-name.

After installation, the **pbbench** utility generates warnings for any host name resolution issues on a host where Privilege Management components are installed.

Installation Process

Privilege Management for Unix and Linux supports interactive installation methods and package installation methods. Before you choose which installation method to use, we recommend that you review the indicated section.

- Use **pbinstall: pbinstall** is a command-line script that can be used to install (or upgrade) Privilege Management for Unix and Linux. It enables the user to review each setting during the installation process and customize the Privilege Management for Unix and Linux installation on that host.

A wrapper script, **run_pbinstall**, is available to simplify installation of all Privilege Management for Unix and Linux components.

- Use **pbmakeremotetar:pbmakeremotetar** enables you to clone a Privilege Management for Unix and Linux installation on a host across other hosts. **pbmakeremotetar** is effective when you have multiple systems that are running the same Privilege Management for Unix and Linux flavor and are to be configured identically.
- Use **pbpatchinstall: pbpatchinstall** enables you to install Privilege Management for Unix and Linux patches on installations of Privilege Management for Unix and Linux v4.0 and higher.
- Use package installers: For Solaris, Linux, HP-UX, and AIX, you can install Privilege Management for Unix and Linux using package installers.

---

i *For more information, please see the following:*
- *"run_pbinstall" on page 216*
- *"pbmakeremotetar" on page 217*
- *"Example of a pbpatchinstall Execution" on page 85*
- *"Solaris Package Installer" on page 91*
- *"Linux Package Installer" on page 117*
- *"HP-UX Package Installer" on page 174*
- *"AIX Package Installer" on page 139*
- *"Custom Installations" on page 87*

Basic pbinstall Information

The following list provides basic information about the **pbinstall** script:

- The **pbinstall** script is located in the Privilege Management for Unix and Linux distribution in the **powerbroker/<version>/<flavor>/install** directory.
- **pbinstall** can be run from a Privilege Management for Unix and Linux distribution CD or from an unpacked tar file. The **pbinstall** install script guides you through the installation and enables you to specify which Privilege Management for Unix and Linux components to install.
- Run **pbinstall** on each machine that needs Privilege Management for Unix and Linux components installed.
- Superuser authority is required to run **pbinstall**. Before running **pbinstall**, either log on as **root** or use the **su** command to acquire root privileges.
- **pbinstall** can be run with various options.

> ℹ️ *For more information, please see .*

Navigate the pbinstall Menu and Choose Option Values

The **pbinstall** script presents options in a numbered menu. Because of the large number of options, the menu is divided into pages. You use the navigation characters listed below to navigate the pages. To use a navigation character, type the character and press **Enter**.

The navigation characters are as follows:

- **C:** Continue installation
- **N:** Next menu page
- **P:** Previous menu page
- **R:** Redraw menu (not shown due to space limitations)
- **X:** Exit script without performing any configuration

To set the value of a menu option, type the number for that option and press **Enter**. Specify the value for the option and press **Enter**. For **Yes** and **No** options, you can specify **N**, **n**, **Y**, or **y**.

You might also see the following prompts, which are synonymous:

- **Press return to continue**
- **Hit return to continue**

Review the messages preceding these prompts on the screen. Press **Return**, **Enter**, **<carriage return>**, or **<line feed>** for the installation process to continue.

pbinstall Installation Menu Conventions

Conventions for the **pbinstall** installation menu include the following:

- Some options are displayed only if other options or the system configuration allow them.
- The item numbers vary with the configuration of the installation target system.
- The step numbers for the basic Privilege Management for Unix and Linux installation instructions do not necessarily match the option numbers in the **pbinstall** installation script.

- If the current value of an option forces the line to be longer than 80 characters, the value within the square brackets is truncated and appended with ellipsis (…).

- Menu pages are limited to a maximum of 18 items. To view additional options, use the navigation characters: **N** (for next page) or **P** (for previous page).

- The values that are shown in the installation menu are examples and not necessarily the defaults or recommended values for your system. Your defaults and existing values (on a re-installation) will appear in the appropriate places when **pbinstall** executes.

- **Yes** and **No** answers are not case-sensitive and may be abbreviated as **y** and **n**.

- **pbinstall** is designed for 24 line by 80 column displays. Using a larger display is also supported.

- **pbinstall** does not support smaller displays.

- Although white space, line terminators, and shell (sh) meta characters are usually allowed in file and directory names, Privilege Management for Unix and Linux does not support them. Do not use them in Privilege Management for Unix and Linux file or directory names.

ℹ️ *For more information, please see the following:*

- *On a basic installation, "Step-by-Step Instructions for a Basic Installation Using pbinstall" on page 42*

- *On advanced installation options, "Advanced Installation Instructions Using pbinstall" on page 46*

- *Privilege Management for Unix and Linux Admin Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm*

Installation Events Using pbinstall

When pbinstall runs, the following actions occur:

- If client registration is used:
  - The **/etc/pb.settings** file is downloaded from the primary license server.
  - The **/etc/pb.key** (or equivalent) is downloaded from the primary license server.

- If SSL is enabled the SSL server certificates are downloaded from the primary license server.
  - The REST services daemon (**pbconfigd**) is installed and configuration made to the operating system to enable service management through the native operating system service manager.

- The **/etc/pb.settings** file is created. It contains various parameters and settings that Privilege Management for Unix and Linux uses at run time. Privilege Management for Unix and Linux cannot run without this file.

- The installation process also creates a work file, **/etc/pb.cfg**. The **pb.cfg** file is used to locate the Privilege Management for Unix and Linux components during upgrades and uninstalls.

- The **/etc/pb**.key file is created. It stores the encryption key. This step is completed only if the Privilege Management for Unix and Linux encryption option is selected.

- If you choose to add entries to **/etc/services**, then the following two steps are performed:
  - The **/etc/services** file is backed up to **/etc/services.sybak.####**. The installation script backs up files using the name format **{original_name}.sybak.####**, where **####** is a number between 0000 and 9999. By default, up to 10 of these files are kept in the directory. This backup method is especially advantageous when performing multiple installations and uninstalls.
  - Entries are added to the **/etc/services** file for **pbmasterd**, **pblocald**, **pblogd**, **pbguid**, and **pbsguid**.

- If the system uses **inetd.conf** for superdaemon configuration, then the following three steps are performed. If the system uses **xinetd.conf**, then similar steps are performed.

- The **/etc/inetd.conf** file is backed up to a file called: **/etc/inetd.sybak.####**.
- Entries are added to the **inetd.conf** file. These entries enable **inetd** to start instances including:
  - **pbmasterd:** Validate a monitored task request.
  - **pblocald:** Execute a monitored task request that has been accepted by **pbmasterd**.
  - **pblogd:** Perform logging.
  - **pblighttpd:** Run Privilege Management REST services.
- The **inetd** superdaemon restarts.
- The appropriate Privilege Management for Unix and Linux programs and online man pages are copied to the specified installation directories.
- During the installation, you have the option to view the generated install script. This option is only for troubleshooting by BeyondTrust Technical Support; the generated install script contains thousands of lines of code.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

33

Privilege Management for Unix and Linux pbinstall Installation Menu

The **pbinstall** script is a comprehensive list of the installation menu options and default prompts. The items displayed vary depending on your system, options selected, and any settings that are found from a current or removed Privilege Management for Unix and Linux installation. The values used here are for demonstration purposes and are not necessarily the defaults or recommended values for a given installation.

The following list shows all the menu options. However, the menu option numbers that you see might differ from this list, depending on your Privilege Management for Unix and Linux flavor.

Opt	Description	[Value]
1	Install Everything Here (Demo Mode)?	[yes]
2	Install License Server?	[yes]
3	Install Registry Name Services Server?	[no]
4	Install Client Registration Server?	[yes]
5	Install Policy Server Host?	[yes]
6	Install Run Host?	[yes]
7	Install Submit Host?	[yes]
8	Install PBSSH?	[yes]
9	Install sudo Policy Server?	[yes]
10	Install Log Host?	[yes]
11	Enable Logfile Tracking and Archiving?	[yes]
12	Is this a Log Archiver Storage Server?	[yes]
13	Is this a Log Archiver Database Server?	[yes]
14	Install File Integrity Monitoring Policy Server?	[yes]
15	Install REST Services?	[yes]
16	List of License Servers?	[kandor]
17	Central License	[]
18	Enable License History?	[no]
19	Installation base directory?	[/opt/pbul]
20	Database directory?	[/opt/pbul/dbs]
21	Path to Password Safe 'pkrun binary'	[]
22	Password Safe certificate file	[]
23	Primary failover Password Safe appliances	[]

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

34

Opt	Description	[Value]
24	Support short names in Password Safe certificate?	[no]
25	Install Synchronization program?	[yes]
26	Install Utilities: pbvi, pbnvi, pbmg, pbumacs, pbless	[yes]
27	Install pbksh?	[yes]
28	Install pbsh?	[yes]
29	Install man pages?	[yes]
30	Will this host use a Log Host?	[yes]
31	AD Bridge Integration?	[yes]
32	Install AD Bridge?	[no]
33	Enable failover event logging to AD Bridge?	[yes]
34	Enable successful connection event logging to AD Bridge?	[yes]
35	Enable event logging to AD Bridge?	[no]
36	AD Bridge shared libraries	[/opt/pbis/lib64/libeventlo...]
37	Integration with BeyondInsight?	[yes]
38	Send event log records to BeyondInsight?	[yes]
39	BeyondInsight hostname	[none]
40	BeyondInsight Workgroup ID	[BeyondTrust Workgroup]
41	BeyondInsight SSL port number	[443]
42	BeyondInsight SSL Client Certificate	[none]
43	BeyondInsight SSL CA file	[none]
44	Index IO Logs using Solr?	[yes]
45	Solr hostname	[none]
46	Solr SSL port number	[8443]
47	Solr SSL CA file	[none]
48	Solr SSL Client key file	[none]
49	Solr SSL Client Certificate file	[none]
50	Registry Name Service database path?	[/opt/pbul/dbs/pbsvc.db]
51	Client Registry database path?	[/opt/pbul/dbs/pbregclnt.db]

Opt	Description	[Value]
52	sudo policy database file path and filename?	[/opt/pbul/dbs/pbsudo.db]
53	Directory location for sudo policy files?	[/opt/pbul/sudoersdir]
54	Synchronization program can be initiated from this host?	[yes]
55	Daemons location	[/usr/sbin]
56	Number of reserved spaces for submit process information of pbmasterd, pblogd, and pblocald	[80]
57	Administration programs location	[usr/bin]
58	User programs location	[usr/local/bin]
59	Policy include (sub) file directory	[/opt/pbul/policies]
60	Policy file name	[/opt/pbul/policies/pb.conf]
61	User man page location	[/usr/local/man/man1]
62	Admin man page location	[/usr/local/man/man8]
63	Log Archive Storage Server name	[]
64	Log Archive destination directory?	[/var/log/pblogarchive]
65	Log Archiver Database Server name	[]
66	Log Tracking Database file path and filename?	[/opt/pbul/dbs/pblogarchive.db]
67	Enable Caching of Log Locations?	[yes]
68	Event Logfile Name Cache Database file path?	[/opt/pbul/dbs/pblogcache.db]
69	I/O Logfile Name Cache Database file path?	[/opt/pbul/dbs/pbiologcache.db]
70	REST Service installation directory?	[/usr/lib/beyontrust/pb/rest]
71	Install REST API sample code?	[no]
72	REST API sample code directory?	[/usr/local/lib/pbrest]
73	Pblighttpd user	[pblight]
74	Create Pblighttpd user?	[yes]
75	Pblighttpd user UID	[]
76	Pblighttpd user GID	[]
77	Pblighttpd user group name	[pblight]
78	File Integrity Monitor db path?	[/opt/pbul/dbs/pbfim.db]
79	Configure systemd?	[yes]

Opt	Description	[Value]
80	Command line options for pbmasterd	[-ar]
81	Policy Server Delay	[500]
82	Policy Server Protocol Timeout	[-1]
83	pbmasterd diagnostic log	[/var/log/pbmasterd.log]
84	Eventlog filename	[/var/log/pb.eventlog]
85	Configure eventlog rotation via size?	[]
86	Configure eventlog rotation path?	[]
87	Configure eventlog rotation via cron?	[no]
88	Validate Submit Host Connections?	[no]
89	List of Policy Servers to submit to	[kandor]
90	pbrun diagnostic log?	[none]
91	pbssh diagnostic log?	[none]
92	Allow Local Mode?	[yes]
93	Additional secured task checks?	[no]
94	Suppress Policy Server host failover error messages?	[yes]
95	List of Policy Servers to accept from	[kandor]
96	pblocald diagnostic log	[/var/log/pblocald.log]
97	Command line options for pblocald	[]
98	Syslog pblocald sessions?	[no]
99	Record PTY sessions in utmp/utmpx?	[yes]
100	Validate Policy Server Host Connections?	[no]
101	List of Log Hosts	[kandor]
102	Command line options for pblogd	[]
103	Log Host Delay	[500]
104	Log Host Protocol Timeout	[-1]
105	pblogd diagnostic log	[/var/log/pblogd.log]
106	List of log reserved filesystems	[none]
107	Number of free blocks per log system filesystem	[0]

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

37

TC: 12/7/2022

Opt	Description	[Value]
108	Command line options for pbsyncd	[]
109	Sync Protocol Timeout	[-1]
110	pbsyncd diagnostic log	[/var/log/pbsyncd.log]
111	pbsync diagnostic log	[/var/log/pbsync.log]
112	pbsync sychronization time interval (in minutes)	[15]
113	Add installed shells to /etc/shells	[no]
114	pbksh diagnostic file	[/var/log/pbksh.log]
115	pbsh diagnostic file	[/var/log/pbsh.log]
116	Stand-alone pblocald command	[none]
117	Stand-alone root shell default iolog	[/pbshell.iolog]
118	Use syslog?	[yes]
119	Syslog facility to use?	[LOG_AUTHORITY]
120	Base Daemon port number	[24345]
121	pbmasterd port number	[24345]
122	pblocald port number	[24346]
123	pblogd port number	[24347]
124	pbguid port number	[24348]
125	REST Service port number	[24351]
126	Add entries to '/etc/services'	[yes]
127	Allow non-reserved port connections	[yes]
128	Inbound Port range	[1024-65535]
129	Outbound Port range	[1025-65535]
130	Man pages should be packed with []	[]
131	Man page extension	[]
132	Network encryption options	[aes-256:keyfile=/etc/pb.key]
133	Event log encryption options	[none]
134	I/O log encryption options	[none]
135	Report encryption options	[none]

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

38

TC: 12/7/2022

Opt	Description	[Value]
136	Policy file encryption options	[none]
137	Settings file encryption type	[none]
138	REST API encryption options	[aes-256:keyfile=/etc/pb.re...]
139	Configure with Kerberos v5?	[yes]
140	Policy Server Daemon Kerberos Principal	[pbmasterd]
141	Local Daemon Kerberos Principal	[pblocald]
142	Log Daemon Kerberos Principal	[pblogd]
143	Sync Daemon Kerberos Principal	[pbsyncd]
144	Kerberos Keytab File	[/etc/krb5.keytab]
145	Enforce High Security Encryption?	[yes]
146	Use SSL?	[yes]
147	SSL Configuration?	[requiressl sslfirst]
148	SSL pbrun Certificate Authority Directory?	[none]
149	SSL pbrun Certificate Authority File?	[none]
150	SSL pbrun Cipher List?	[cipherlist=TLSv1.2:!SSLv2:...]
151	SSL pbrun Certificate Directory?	[none]
152	SSL pbrun Certificate File?	[none]
153	SSL pbrun Private Key Directory?	[none]
154	SSL pbrun Private Key File?	[none]
155	SSL pbrun Certificate Subject Checks?	[none]
156	SSL Server Certificate Authority Directory	[none]
157	SSL Server Certificate Authority File?	[none]
158	SSL Server Cipher List?	[cipherlist=TLSv1.2:!SSLv2:...]
159	SSL Server Certificate Directory?	[none]
160	SSL Server Certificate File?	[/etc/pbssl.pem]
161	SSL Server Private Key Directory?	[none]
162	SSL Server Private Key File?	[/etc/pbssl.pem]
163	SSL Server Certificate Subject Checks?	[none]

Opt	Description	[Value]
164	SSL Certificate Country Code	[US]
165	SSL Certificate State/Province	[AZ]
166	SSL Certificate Location (Town/City)	[Phoenix]
167	SSL Certificate Organizational Unit/Department	[Security]
168	SSL Certificate Organization	[BeyondTrust]
169	Configure Privilege Management for Unix & Linux with LDAP?	[yes]
170	Install BeyondTrust built-in third-party libraries?	[no]
171	BeyondTrust built-in third-party library directory	[/usr/lib/beyondtrust/pb]
172	Kerberos shared library default directory	[none]
173	Kerberos libkrb5 shared library filename	[none]
174	Kerberos libgssapi_krb5 shared library filename	[none]
175	Kerberos libcom_err shared library filename	[none]
176	Kerberos libk5crypto shared library filename	[none]
177	SSL shared library default directory	[none]
178	SSL libssl shared library filename	[none]
179	SSL libcrypto shared library filename	[none]
180	LDAP shared library default directory	[none]
181	LDAP libldap shared library filename	[none]
182	LDAP liblber shared library filename	[none]
183	Use PAM?	[no]
184	PAM service for password verification	[none]
185	PAM session service	[none]
186	PAM suppress password prompting?	[yes]
187	PAM library file name	[none]
188	Call pam_setcred?	[no]
189	Enable non-PAM Solaris Projects?	[no]
190	Solaris Projects library file name	[none]
191	Allow Remote Jobs?	[yes]

Opt	Description	[Value]
192	UNIX Domain Socket directory	[none]
193	Reject Null Passwords?	[no]
194	Enable TCP keepalives?	[no]
195	Name Resolution Timeout	[0]

Step-by-Step Instructions for a Basic Installation Using pbinstall

The basic **pbinstall** procedure assumes that you have successfully downloaded and unarchived the Privilege Management for Unix and Linux distribution or have a Privilege Management for Unix and Linux CD.

ℹ️ *For additional information about Privilege Management for Unix and Linux components and more options for **pbinstall**, please see the following:*

- *"Installation Preparation" on page 25*
- *"Advanced Installation Instructions Using pbinstall" on page 46*

Run a Basic Installation Using pbinstall

To perform a basic Privilege Management for Unix and Linux installation using the **pbinstall** script, use the following procedure:

1. If you downloaded Privilege Management for Unix and Linux using the Web or FTP, then do the following. To install Privilege Management for Unix and Linux from a CD, skip to step 2.

   - Create the **/opt/beyondtrust** directory if it does not already exist.
   - Extract the Privilege Management for Unix and Linux installation files by executing the following command:

   ```
   gunzip -c pmul<flavor_version>.tar.Z | tar xvf -
   ```

2. To install from a CD, insert it into the CD-ROM drive on your machine. Mount the CD by entering:

   ```
   mount /cdrom <device_name>
   ```

📌 **Note:** *Your system may require additional command options or have a different mount point. For more information, please see the mount main page for your system.*

---

3. Navigate to the appropriate install directory on the file system or CD.

4. Start the **pbinstall** script with the following command:

   ```
   ./pbinstall
   ```

5. Press **Enter** after you read the initial messages.

6. A prompt will ask if this is the first installation in the enterprise:

   ```
   Privilege Management for Unix and Linux must have a designated Primary Server to provide
   control and consistency for all its components/entities.
   The Primary Server must be installed and configured first before all other hosts.
   Is this the first installation in the enterprise (designated Primary Server) [yes]?
   ```

7. If you install a new client you may wish to use the client registration facility. When first invoking **pbinstall**, the following is displayed:

```
Client registration provides a method of automatic configuration based upon a profile
provided by your Primary License Server. To use this functionality you will need to know
specific parameters from your  Primary License Server setup. Please see the installation
guide for details.
Do you wish to utilize client registration? [no]? yes
Enter the Application ID generated on the Primary License Server: appid
Enter the Application Key generated on the Primary License Server: 0b5e954e- be38-424d-b7e7-
3e0ec91d9301

Enter the Primary License Server address/domain name for registering clients:
master.organization.com
Enter the Primary License Server REST TCP/IP port [24351]:
Enter the Registration Client Profile name[default]:
```

If you wish to enable automatic configuration using client registration, you need the following:

- REST Application ID
- REST Application Key
- Network name or IP address of the primary license server that has been configured to enable client registration
- REST services port
- Name of the client registration profile configured by the administrator

Once you have the data and have entered them into the **pbinstall** prompts, the configuration of the client is downloaded and the installation continues. All defaults used during the rest of the installation process are from the information retrieved.

8. A prompt asks if you want to install the Registry Name Services.

```
The Registry Name Service of Privilege Management for Unix and Linux facilitates location of
other services within the pmul enterprise with the aid of a centralized data repository.
IMPORTANT: It is highly recommended to utilize client registration if you are using Registry
Name Services. Do you wish to utilize Registry Name Service? [yes]?
```

If you answer **no** to the previous question, **Is this the first installation?**, you are asked to register the host as a Registry Name Service client.

To enable the use of Registry Name Services each client needs to be registered with the primary server.

```
Please complete the questions below to enable this registration.
Enter the Application ID generated on the Primary Registry Name Server:  appid
Enter the Application Key generated on the Primary Registry Name Server:  appkey
Enter the address/domain name for the Primary Registry Name Server:  host
Enter the Primary Registry Name Server REST TCP/IP port [24351]:
```

If RNS is specified, the defaults for submitmasters, acceptmasters, logservers, etc, are changed to asterisk (*), and **registrynameserver yes** is added to the prospective **pb.settings**.

9. The pbinstall menu displays a set of options similar to the following:

Opt	Description	[Value]
1	Install Everything Here (Demo Mode)?	[no]

Opt	Description	[Value]
2	Install License Server?	[no]
3	Install Registry Name Services Server?	[no]
4	Install Client Registration Server?	[no]
5	Install Policy Server Host?	[yes]
6	Install Run Host?	[yes]
7	Install Submit Host?	[yes]
8	Install PBSSH?	[yes]
9	Install Log Host?	[yes]
10	Enable Logfile Tracking and Archiving?	[yes]
11	Is this a Log Archiver Storage Server?	[no]
12	Is this a Log Archiver Database Server?	[no]
13	Install File Integrity Monitoring Polic...	[no]
14	Install REST Services?	[yes]
15	List of License Servers	[*]

📌 **Note:** *The following instructions select the required options to do a basic installation only.*

10. Choose your options.
11. Use the **c** navigation command to continue the installation.
12. A prompt asks if you want to view the install script. Specify **n**.

> ⓘ **IMPORTANT!**
>
> *This option is intended for troubleshooting by BeyondTrust Technical Support. The generated install script contains thousands of lines of code.*

13. A prompt asks if you want to install the product now. Specify **y**.

The Privilege Management for Unix and Linux install script executes and installs Privilege Management for Unix and Linux components on this machine.

14. If a Privilege Management for Unix and Linux policy file exists, it is not modified. Starting with version 8.0, if you do not have a policy file, a default policy is installed by default. The files **{prefix}pbul_policy.conf{suffix}** and **{prefix}pbul_functions.conf {suffix}** are created in the default directory **/opt/pbul/policies** from v9.4.3+ and **/etc** prior to v9.4.3. **{prefix}pbul_policy.conf {suffix}** is then included in the main policy (by default **/opt/pbul/policies/{prefix}pb.conf {suffix}** from v9.4.3+ and **/etc/ {prefix}pb.conf {suffix}** prior to v9.4.3).

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

44

> **⚠ IMPORTANT!**
>
> *An empty policy file rejects all Privilege Management for Unix and Linux commands. For information about writing policy files, see the Privilege Management for Unix and Linux Policy Language Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

15. Change the permissions on the policy file so that it can be read by root only:

```
chmod 600 /opt/pbul/policies/pb.conf
```

The installation is now complete.

> ℹ *For more information, please see "Advanced Installation Instructions Using pbinstall" on page 46.*

Advanced Installation Instructions Using pbinstall

This section provides step-by-step instructions for using all the installation options that are available using the **pbinstall** script. These options are discussed in the order that they are used in the Privilege Management for Unix and Linux installation menu.

> 📌 **Note:** *These steps are optional and should be selected after reviewing "Installation Considerations" on page 7 and "Installation Preparation" on page 25.*

In addition, some options do not appear unless certain combinations of options are selected.

> ℹ️ *For more information, please see "Complete the Installation" on page 76.*

Start pbinstall

If you downloaded Privilege Management for Unix and Linux using the Web or FTP, do the following.

1. Extract the tarball files into /opt/beyondtrust by executing the following command:

```
gunzip -c pmul<flavor_version>.tar.Z | tar xvf -
```

2. Navigate to the installation directory:

```
cd /opt/beyondtrust/powerbroker/<version>/<flavor>/install
```

3. Execute the installation script by typing:

```
./pbinstall
```

4. After reading the initial messages, press **Enter**.

> ℹ️ *For more information, please see the following:*
>
> - *On how to install Privilege Management for Unix and Linux from a CD, "Step-by-Step Instructions for a Basic Installation Using pbinstall" on page 42*
> - *If you are using a prefix or suffix, or both, "Prefix and Suffix Installation Instructions" on page 89*

Use the Menu Options

> 📌 **Note:** *Depending on your operating system and other factors, the option numbers listed in the following table may not match the menu option numbers you see on the screen, and some items might not be available. In these steps, **choose this option** means to type the number that corresponds to the option on the screen and press **Enter**.*

Opt #	Menu Item	Description
1	Install Everything Here (Demo Mode)?	Choose this option and specify **y** to install the policy server host, run host, submit host, and log host on this computer. This option is useful for testing or demonstrating Privilege Management for Unix and Linux on a single computer in your environment.
2	Install license server?	Specify **y** to install a license server which provides product license management for Privilege Management for Unix and Linux.
3	Install Registry Name Services Server?	Specify **y** to install the Registry Name Service which provides the product with a method of addressing and locating other parts of Privilege Management for Unix and Linux. Installing the Registry Name Services Server makes installing the Sudo Policy Server mandatory. *For more information, please see* "Install Sudo Policy Server" on page 267.
4	Install Client registration Server?	Specify **y** to install the client registration Server which provides a repository for customized install profiles. If you already chose to install the Registry Name Service, installing client registration Server is mandatory.
5	Install Policy Server Host?	Choose this option and specify **y** to install the policy server host component on this host.
6	Install Run Host?	Choose this option and specify **y** to install the run host component on this host.
7	Install Submit Host?	Choose this option and specify **y** to install the submit host component on this host. *Note: This option installs **pbrun**.*
8	Install PBSSH	This item is available only when you specify **y** for the previous item. Using the Privilege Management for Unix and Linux**pbssh** program, you can 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 Privilege Management for Unix and Linux installed on them; such devices can include Windows computers and certain network devices. Choose this option and specify **y** to install the **ppssh** program.
9	Install sudo Policy Server?	Enter **y** to configure the server to be able to store and process sudo policies. Installing the Sudo Policy Server is mandatory if installing the Registry Name Services Server.
10	Install Log Host?	Choose this option and specify **y** to install the log host component on this host.
11	Enable Logfile Tracking and Archiving?	If the installation detects that the user is installing the policy server host or the log host on the current machine, it displays in the menu the install question *Enable Logfile Tracking and Archiving?* and set it to **yes** by default. When the answer to this question is set to yes, the installer prompts the user for the Log Archive Storage Server name and the Log Archiver Database Server name. Log Tracking and Archiving requires REST services to be installed.
12	Is this a Log Archiver Storage Server?	If the current machine is the intended Log Archive Database Server, it must have the REST service preinstalled on it. It is also required to have the **logarchivedb** setting in **pb.settings**, which specifies the SQLite database that stores the location of logfiles, as well as where the archiving information is located.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

47

TC: 12/7/2022

Opt #	Menu Item	Description
		If the answer to this question is set to **yes**, the install displays the following question: ```Configure this host to be a Log Archive Storage Server which receives logfiles to archive and stores them in the appropriate path: Yes This host will be configured as a Log Archiver Storage Server No This host will NOT be configured as a LogArchiver Storage Server Set as a Log Archiver Storage Server? [no]? yes The Log Archive Storage Server which will accept and place archived logfiles in a designated pathname. Ensure that it is located in filesystem with ample free space to accommodate incoming logfiles. Enter the default directory path for archived logfiles []: /pbul/logs``` It also sets the **Log Archive Storage Server name** to the hostname of the current machine.
13	Is this a Log Archiver Database Server?	If the current machine is the intended Log Archive Database Server, it must have the **REST** service preinstalled on it. It is also required to have the **logarchivedb** setting in **pb.settings**, which specifies the SQLite database that stores the location of logfiles, as well as where the archiving information is located. If the answer to this question is set to **yes**, the install displays the following question: ```Configure this host to be a Log Archive Database Server which creates and maintains the log tracking database: Yes This host will be configured as a Log Archiver Database Server No This host will NOT be configured as a LogArchiver Database Server Set as a Log Archiver Database Server? [no]? yes Privilege Management for Unix and Linux will create and maintain a SQLite database to track the location of logfiles. Specify the path and filename of the SQLite logfile tracking database file and ensure that the given database file system has ample space for growth. Enter the path and filename of Privilege Management for Unix and Linux's SQLite log tracking database file []: /var/log/pbul90_tracking.db``` It also sets the **Log Archive Database Server name** to the hostname of the current machine.
14	Install File Integrity Monitoring Policy Server?	Specify **y** to install and configure the centralized repository for FIM policies.
15	Install REST Services?	This option is automatically enabled to install the Privilege Management RESTful web-based API for

Opt #	Menu Item	Description
		product settings, policy configuration, and I/O log retrieval. When installing server-side components of Privilege Management for Unix and Linux, installing the REST Services is mandatory. This option is automatically enabled to install the Privilege Management RESTful web-based API for product settings, policy configuration, and I/O log retrieval. When installing server-side components of Privilege Management for Unix and Linux, installing the REST Services is mandatory.
16	List of license servers	Enter a space-separated list of hostnames of license servers within the Privilege Management for Unix and Linux installation. The primary license server is first in the list, followed by secondary license servers listed in order of failover. If Registry Name Service is configured, this value should be an asterisk (*), denoting that the value is held within the service database.
17	Central License	Enter the JSON-formatted data which represents the license you received from your BeyondTrust representative.
18	Enable License HI	Choose yes to enable the logging of license usage history
19	Installation base directory?	By default, Privilege Management for Unix and Linuxcreates subdirectories and files it needs under '/opt/pbul' by default. This menu option allows you to change the base directory path. The base directory provided must be: • an absolute path • owned by root • only root can read/write It is recommended that you provide a directory location that is dedicated for Privilege Management for Unix and Linux.
20	Database directory?	Choose this option and select a secure directory location. This path is assigned to the **databasedir** setting which defines the default location of databases used in Privilege Management for Unix and Linux, when only the relative path is provided.
21	Path to Password Safe 'pkrun' binary	This item is available only if you choose to install **PBSSH**. Choose this option to specify where the BeyondTrustPassword Safe**pkrun** binary resides. The **pbssh** command can use BeyondTrustPassword Safe for the userid's password acquisition. To do this, Privilege Management for Unix and Linux needs to know where the BeyondTrustPassword Safe**pkrun** binary resides. Choose this option and do one of the following: • Specify the absolute path where **pkrun** resides. • Specify **none** to clear the entry (default).
22	Password Safe certificate file	[]
23	Primary failover Password Safe appliances	[]
24	Support short names in Password Safe certificate?	[no]

Opt #	Menu Item	Description
25	Install Synchronization program?	Choose this option and specify **y** to enable this host to participate in log synchronization.
26	Install Utilities: pbvi, pbnvi, pbmg, pbumacs, pbless	Choose this option and specify **y** to install the Privilege Management for Unix and Linux utilities on this host.
27	Install pbksh?	Choose this option and specify **y** to install the **pbksh** component on this host.
28	Install pbsh?	Choose this option and specify **y** to install the **pbsh** component on this host.
29	Install man pages?	Choose this option and specify **y** to install the man pages.
30	Will this host use a Log Host?	Choose this option and specify **y** to log the components on this host to a log server.
31	AD Bridge Integration?	The **pbinstall** program does not detect whether AD Bridge is installed. Choose this option and specify one of the following: • **no** to disable Privilege Management for Unix and Linux integration with AD Bridge. This is the default. • **yes** to enable Privilege Management for Unix and Linux integration with AD Bridge.
32	Install AD Bridge?	[no]
33	Enable failover event logging to AD Bridge?	[yes]
34	Enable successful connection event logging to AD Bridge?	[yes]
35	Enable event logging to AD Bridge?	[no]
36	AD Bridge shared libraries	[/opt/pbis/lib64/libeventlo...]
37	Integration with BeyondInsight?	This option is available for log servers and policy server hosts. This option allows the sending of eventlog records to BeyondInsight and indexing of I/O logs.
38	Send event log records to BeyondInsight?	[yes]
39	BeyondInsight hostname	[none]
40	BeyondInsight	[BeyondTrust Workgroup]

Opt #	Menu Item	Description
	Workgroup ID	
41	BeyondInsight SSL port number	[443]
42	BeyondInsight SSL Client Certificate	[none]
43	BeyondInsight SSL CA file	[none]
44	Index IO Logs using Solr?	[yes]
45	Solr hostname	[none]
46	Solr SSL port number	[8443]
47	Solr SSL CA file	[none]
48	Solr SSL Client key file	[none]
49	Solr SSL Client Certificate file	[none]
50	Registry Name Service database path?	[/opt/pbul/dbs/pbsvc.db]
51	Client Registry database path?	[/opt/pbul/dbs/pbregclnt.db]
52	sudo policy database file path and filename?	[/opt/pbul/dbs/pbsudo.db]
53	Directory location for sudo policy files?	[/opt/pbul/sudoersdir]
54	Synchronization can be initiated from this host?	Choose this option and specify **y** to install **pbsync** to enable this host to start log synchronization.
55	Daemons location	Choose this option and specify a location for it. We recommend that you use the default location, but you can choose to specify a different location. However, do not use system directories for this purpose.
56	Number of reserved spaces for submit process information of	Available in v8.0 and later, and only on Linux and AIX platforms, this feature modifies the **pbmasterd**, **pblocald** and **pblogd** command line arguments (viewable via ps) to include information about the originating **pbrun** request. This allows administrators to determine which **pbrun/pbmasterd/pblocald/pblogd** processes are related to a given request.

Opt #	Menu Item	Description
	pbmasterd, pblogd, and pblocald [80]	Choose this option and specify the number of space to reserve in the process list of **pbmasterd**, **pblocald** and **pblogd** processes by adding a **-i** to the daemon startup files. This new command line option is used to reserve space in the process list so that the command line argument space can be updated with information about the originating request (**submituser**, **submithost**, **runcommand**, and the **pbrun pid**).
57	Administration programs location	Choose this option and specify a location for administration programs. We recommend that you use the default location, but you can choose to specify a different location. However, do not use system directories for this purpose.
58	User programs location	Choose this option and specify a location for user programs. We recommend that you use the default location, but you may choose to specify a different location. However, do not use system directories for this purpose.
59	Policy include (sub) file directory	Choose this option and specify a directory for the policy files. We recommend that you use the default location, but you can specify a different location. However, do not use system directories for this purpose.
60	Policy file name	Enter the Privilege Management for Unix and Linux policy file name.
61	User man page location	[/usr/local/man/man1]
62	Admin man page location	[/usr/local/man/man8]
63	Log Archive Storage Server name	The Log Archive Storage Server is the destination host where the logfiles are archived. The **PBUL REST** service must be pre-installed on that machine. There is no default value for this field, but the user is not allowed to proceed without specifying the appropriate server name. The value is saved in the **logarchivehost** setting.
64	Log Archive destination directory?	[/var/log/pblogarchive]
65	Log Archiver Database Server name	The Log Archive Database Server is the destination host where the logfile tracking database resides. The **REST** service must be preinstalled on that machine. There is no default value for this field, but the user is not allowed to proceed without specifying the appropriate server name. The value is saved in the **logarchivedbhost** setting.
66	Log Tracking Database file path and filename?	[/opt/pbul/dbs/pblogarchive.db]
67	Enable Caching of Log Locations?	[yes]
68	Event Logfile Name Cache Database file path?	[/opt/pbul/dbs/pblogcache.db]
69	I/O Logfile Name	Enter the path of the database file to cache the location of event and I/O logfiles. It is used when

Opt #	Menu Item	Description
	Cache Database file path?	integrating BeyondInsight for Unix and Linux with Privilege Management for Unix and Linux. Enter **none** to disable the feature.
70	REST Service installation directory?	This menu item is enabled only if **REST** services are to be installed.
71	Install REST API sample code?	This menu item is enabled only if **REST** services are to be installed.
72	REST API sample code directory?	[/usr/local/lib/pbrest]
73	Pblighttpd user	The user name used to run the REST services as. The default value is **pblight**. This user is created if you answer **yes** to the menu option **Create Pblighttpd User?**. This menu item is enabled only if installing **REST** Services.
74	Create Pblighttpd user?	[yes]
75	Pblighttpd user UID	[]
76	Pblighttpd user GID	[]
77	Pblighttpd user group name	Enter a user group name or use the default value. The pblighttpd user specified in step 73 is assigned to the group name provided. • If you enter a group name that does not exist, that group is created and the pblighttpd user specified in step 73 is assigned to it. • If you enter a group name that exists, then the pblighttpd user is assigned to that preexisting group.
78	File Integrity Monitor db path?	[/opt/pbul/dbs/pbfim.db]
79	Configure systemd?	Choose this option and specify **y** if you want to configure the file. Privilege Management for Unix and Linux can be configured into the **systemd**, **inetd**, **xinetd**, **launchd**, or **SMF** superdaemons, which are OS-dependent. These superdaemons are used by Privilege Management for Unix and Linux to listen on a TCP/IP port for inbound connections requesting Privilege Management for Unix and Linux daemon services. When the superdaemon detects a connection request, it forks a copy of the Privilege Management for Unix and Linux daemon to serve the request. 📌 *Note: If you specify **no**, any existing Privilege Management for Unix and Linux installation that is configured with the specified prefix and/or suffix is removed from the superdaemon configuration.* 📌 *Note: This menu option is platform dependent. On older RHEL or other operating systems using **inetd** or **xinetd**, it may display **Configure inetd** or **xinetd**, while on Solaris, it displays*

Opt #	Menu Item	Description
		📌 **Configure Solaris Services**.

80	Command line options for pbmasterd	Choose this option and specify the command line options that you want. Available syntax and command line options for **pbmasterd** are:
		
		```Syntax: [-arsV] [-e logfile]```
		```[--disable_optimized_runmode]```
		
		-a: Send the job acceptance messages to syslog.
		
		-e: Use the log file as the **pbmasterd** diagnostic log file. The **-e** command line option overrides the syslog setting in the **pb.settings** file. You must specify the file name if you use the **-e** option.
		
		-r: Send the job rejection messages to syslog.
		
		-s: Send the error messages to syslog. The **-s** command line option overrides the syslog setting in the **pb.settings** file, if you want to change it in the future.
		
		-V: Print the version number mismatch messages.
		
		none: Erase all options.
		
		--disable_optimized_runmode: Suppresses optimized run mode for any tasks that are authorized by this policy server host.
		
		📌 *Note: The installation is currently set to use the syslog in the Privilege Management for Unix and Linux***pb.settings** *file. This setting is the default.*

81	Policy Server Delay	Choose this option and specify the length of time (in milliseconds) that a **pbrun** command should wait for an initial connection to a policy server host. If a connection does not occur within a specified number of milliseconds, then the command uses another host that is specified in the **pb.settings** file for submitmasters.
82	Policy Server Protocol Timeout	Choose this option and specify the length of time the daemon should wait for a response from a policy server host or the time a policy server host should wait for a response from another Privilege Management for Unix and Linux program.
83	pbmasterd diagnostic log	Choose this option and specify a location. This option enables you to specify where the **pbmasterd** diagnostic log is located.
84	Eventlog filename	Choose this option and specify a location. This option enables you to specify where the event log file is located.
85	Configure eventlog rotation via size	Choose this option and specify a size for event log rotation.
86	Configure eventlog rotation path	Choose this option and specify a path where the event log is moved to.
87	Configure eventlog	Choose this option add a cron job to rotate the eventlog, and specify the cron minute, hour, days-of-the-

Opt #	Menu Item	Description
	rotation via cron	month, month, and days-of-the-week fields.
88	Validate Submit Host Connections?	Choose this option and specify one of the following settings. The Privilege Management for Unix and Linux policy server daemon (**pbmasterd**) can use name resolution to validate the host name and IP address of the submit host connection to a policy server host. • Specify **y** to validate submit host connections. If you decide to use this facility, then you must do the following: ○ Ensure that name resolution works correctly on all machines. ○ Ensure all policy server hosts and submit hosts are upgraded to Privilege Management for Unix and Linux v3.5.7 or higher before enabling this feature. ○ Ensure that each submit host connection's host name and IP address match those that are listed in the policy server host's name resolution services. • Specify **n** to disable this checking. This setting is the default value.
89	List of Policy Servers to submit to	Choose this option and do the following: • If submitmasters already has a value, specify **y** at the **Do you wish to make changes to this list?** prompt. • At the **Enter Policy Server list (submitmasters)** prompt, specify a host name, or a list of space-delimited host names, to serve as policy servers to submit secured tasks to (a fully-qualified domain name may be required): The host names should now appear in the List of Privilege Management policy server hosts to submit to line of the **pbinstall** menu.
90	pbrun diagnostic log?	Choose this option and specify a location for the diagnostic log. This option is typically used only when requested by BeyondTrust Technical Support.
91	pbssh diagnostic log?	The BeyondTrustPrivilege Management for Unix and Linux**pbssh** program can maintain a separate, individual host diagnostic log file. This log file is typically only used when requested by BeyondTrust Technical Support. Specify a full path specification for the **pbssh** diagnostic log file or **none** for none.
92	Allow Local Mode?	Choose this option and specify **y** to allow Local Mode. This option allows the requested secured task to replace the executing copy of **pbrun**. Local Mode executes secured tasks on the submit host only.
93	Additional secured task checks?	Choose this option and specify whether to enable additional secured task checks. This option determines whether the run host or submit host performs an additional check on the security of the requested command. This check helps to ensure that the command cannot be compromised by a user other than root or the user running the Privilege Management for Unix and Linux command (for example, sys, oracle). This setting is used on run hosts or submit hosts using Local Mode. The policy language variable **runsecurecommand** can be set by the configuration policy on the policy server host for the same effect. • Specify **y** to check the runcommand and all directories above it to see if anyone other than root or the runuser has write permission. If the command file or any of the directories above it are writable by anyone other than root or the runuser, then the run host refuses to run the command.

Opt #	Menu Item	Description
		• Specify **n** to disable this feature.
94	Suppress Policy Server host failover error messages?	When a connection to policy server host fails, Privilege Management for Unix and Linux fails over to another available policy server host (if configured), and generate an error message regarding the event. Choose this option and do one of the following: • Specify **n** to enable the policy server host failover error messages (default). • Specify **y** to suppress the policy server host failover error messages.
95	List of Policy Servers to accept from	Choose this option and then do the following: • If acceptmasters already has a value, specify **y** at the **Do you wish to make changes to this list?** prompt. • At the **Enter Incoming Policy Server list (acceptmasters)** prompt, specify a host name, or a list of space-delimited host names, to serve as policy servers to accept secured tasks from (a fully-qualified domain name may be required). The accept policy server host name should now display in the **List of Privilege Management Policy Server hosts to accept from ...** line of the **pbinstall** menu.
96	pblocald diagnostic log	Choose this option and specify a directory and file name for it.
97	Command line options for pblocald	Choose this option and specify the command line options that you want. Available syntax and command line options for **pblocald** are: ```[-sV] [-e logfile] [-m master_host]``` • **-s:** Send error messages to syslog. The **-s** command line option overrides the syslog setting in the **pb.settings** file if you decide to change it in the future. • **-e:** Use logfile as the pblocald diagnostic log file. The **-e** command line option overrides the settings file. • **-m:** Accept pbmasterd connections from master_host only. Multiple **-m** options can be used to specify more than one host. • **-V:** Print version number mismatch messages. • **none:** Erase all options. The installation is currently set to use the syslog in the Privilege Management for Unix and Linux**pb.settings** file. This setting is the default.
98	Syslog pblocald sessions?	Choose this option and specify **y** to log **pblocald** accepted and rejected requests to syslog.
99	Record PTY sessions in utmp/utmpx?	Choose this option and specify **y** to record Privilege Management for Unix and Linux terminal sessions in the **utmp** (or **utmpx**) file.
100	Validate Policy Server Host	Choose this option and specify one of the following settings. The Privilege Management for Unix and Linux local daemon (**pblocald**) can use name resolution to validate the host name and IP address of the

Opt #	Menu Item	Description
	Connections?	policy server host connection to a run host. • Specify **y** to validate policy server host connections. This validation requires that each policy server connection's host name and internet address match those that are retrieved from name resolution services. 📌 **Note:** *If you decide to use this facility, then you must ensure that name resolution works correctly on all machines before enabling this feature. You must also ensure that all policy server hosts and run hosts are upgraded to Privilege Management for Unix and Linux v3.5.7 or later before enabling this feature.* • Specify **n** to disable this checking. This setting is the default value.
101	List of Log Hosts	Choose this option and specify which machines are to be log hosts. Privilege Management for Unix and Linux needs to know which machines you have selected as log hosts. Log hosts are the hosts that policy server hosts select to perform event and I/O logging. To accomplish this task, policy server looks at the setting for logservers in the **pb.settings** file. This logservers setting contains the names of the log host machines or a netgroup. You can add, modify, or remove machine names by doing the following: • If logservers already has a value, specify **y** at the **Do you wish to make changes to this list?** prompt. • At the **Enter Log Server list (logservers)** prompt, specify a host name, or a list of space-delimited host names, to serve as Log Hosts: The log host names should now appear in the **List of Privilege ManagementLog Hosts** line of the **pbinstall** menu. A logserver must be installed before enabling the **changemanagementevents** keyword.
102	Command line options for pblogd	Choose this option and specify the command line options that you want. The available syntax and command line options for **pblogd** are: ``` [-ars] [-e logfile] ``` **-a:** Record accept events on syslog. **-e:** Use **logfile** as the **pblogd** diagnostic log file. If you previously specified the **pblogd** log file as **/var/log/pblogd.log**, the **-e** command line option overrides the **pblogd** setting in the **pb.settings** file. **-r:** Record reject events on syslog. **-s:** Send error messages to syslog. If you have previously specified to use the **syslog** setting in the **pb.settings** file, the **-s** command line option overrides the settings file if you decide to change it in the future. **none:** Erase all options.
103	Log Host Delay	Choose this option and specify the length of time (in milliseconds) that a daemon should wait for an initial connection to a log host. If a connection does not occur within a specified number of milliseconds, then it tries another server that is specified in the logservers setting in the **pb.settings** file.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

57

TC: 12/7/2022

Opt #	Menu Item	Description
104	Log Host Protocol Timeout	Choose this option and specify the length of time a daemon should wait for a response from a log host or the time a log host should wait for a response from another Privilege Management for Unix and Linux program. Enter the value of the log host protocol timeout (-1 to 1200000). 0 or -1 disables this timeout. -1 is the default.
105	pblogd diagnostic log	Choose this option and specify a location for it. This option enables you to specify the directory and file name for the **pblogd** diagnostic log. Enter **none** for no error reporting.
106	List of log reserved file systems	Choose this option to specify reserved file systems. Privilege Management for Unix and Linux allows the log host to control the file system space and enables the immediate failover to the next log host. • Enter **none** to specify no reserved file systems. • To specify reserved file systems, type the names of the reserved file systems that you want to failover. Use spaces to separate multiple file system names. When a file system is specified in this option, you also should use the next option to specify the minimum number of free blocks that the log system file must have available. If that number of free blocks is not available, then the logging is done on the next log host.
107	Number of free blocks per log system file	Choose this option and specify the minimum number of free blocks or enter **0** to have no minimum number of free blocks allowed for the file systems specified in the previous option. The valid values for the minimum number of free blocks are 0 to 2048000.
108	Command line options for pbsyncd	Choose this option and specify the command line options that you want. The available command line options for **pbsyncd** are: ```[-s] [-e logfile]``` • **-e:** Use **logfile** as the **pbsyncd** diagnostic log file. • **-s:** Use the syslog facilities.
109	Sync Protocol Timeout	Choose this option and specify the length of time a synchronization client or server should wait for protocol checks to be completed. Enter the value of the synchronization protocol timeout (-1 to 1200000). 0 or -1 disables this timeout. -1 is the default.
110	pbsyncd diagnostic log	Choose this option and specify the directory and file name for the **pbsyncd** diagnostic log.
111	pbsync diagnostic log	This option enables you to specify the directory and file name for the **pbsync** diagnostic log.
112	pbsync synchronization time interval (in minutes)	Choose this option to specify the time interval in minutes between synchronizations.
113	Add installed shells to /etc/shells	Choose this option and specify whether to add installed shells. The operating system can validate your Privilege Management for Unix and Linux shells and then add them to **/etc/shells**. • **yes:** Add installed shells to **/etc/shells**.

Opt #	Menu Item	Description
		• **no:** Do not add installed shells to **/etc/shells**.
114	pbksh diagnostic file	Choose this option to specify the directory and file name for the **pbksh** diagnostic log.
115	pbsh diagnostic file	Choose this option to specify the directory and file name for the **pbsh** diagnostic log.
116	Stand-alone pblocald command	shell executes with the system in Single-User Mode, it is necessary to know which command to execute for some secured task requests that are handled by **pblocald**. This setting provides the Privilege Management for Unix and Linux shell, running in Single-User Mode, with the **pblocald** command to execute. Specify the full command for the local daemon. Choose this option and indicate whether to specify a stand-alone **pblocald** command. When a Privilege Management for Unix and Linux `/usr/sbin/[prefix]pblocald[suffix] -s` 📌 *Note: When you specify the command, any installation prefix or suffix must be included. Specify **none** to specify no command for the local daemon in Single-User Mode.*
117	Stand-alone root shell default iolog	[/pbshell.iolog]
118	Use syslog?	Choose this option to specify whether to use the system syslog facility. The Privilege Management for Unix and Linux programs can send errors reported by the policy server and local daemons to the syslog. If you decide to use the system's syslog facility, then you must ensure that the facility selected for use by Privilege Management for Unix and Linux is enabled according to your system's documentation. • Specify **y** to use the system syslog facility. • Specify **n** to not use the system syslog facility.
119	Syslog facility to use?	Choose this option to specify the syslog facility to use. For Privilege Management for Unix and Linux to use the syslog facility, it must be specified. The facilities that can be specified are: • LOG_AUTH security/authorization messages • LOG_AUTHPRIV security/authorization messages (Linux). Only supported in Privilege Management for Unix and Linux 7.1.0 and later. • LOG_DAEMON daemon messages • LOG_LOCAL0 local messages • LOG_LOCAL1 local messages • LOG_LOCAL2 local messages • LOG_LOCAL3 local messages • LOG_LOCAL4 local messages • LOG_LOCAL5 local messages

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

59

Opt #	Menu Item	Description
		• LOG_LOCAL6 local messages • LOG_LOCAL7 local messages • LOG_USER user messages 📌 **Note:** *The default **[LOG_AUTH]** is usually sufficient. The message severity level that is used by Privilege Management for Unix and Linux is **LOG_INFO**.*
120	Base daemon port number	⊘ **IMPORTANT!** *Unlike individual daemon ports, the base port may not be a Unix or Linux domain socket or a program name. Any daemon port that is already set to either a Unix or Linux domain socket or program name will not be changed. However, the used port number will be skipped. For more information about assigning ports, see "Installation Preparation" on page 25.* Choose this option and do one of the following: • If ports 24345 to 24350 are available for all of the Privilege Management for Unix and Linux daemon ports, then accept these ports and continue the installation. • If those ports are not available, then do one of the following: ○ Specify an available port number that also has the next six sequential port numbers available to set all of the Privilege Management for Unix and Linux daemon ports. The specified value must be numeric and must fall within the range from 1024 to 65530 (inclusive). The **pbmasterd** port is set to the specified value. The **pblocald** port is set to the specified value +1. The **pblogd** port is set to the specified value +2. The **pbguid** port is set to the specified value +3. The **pbsguid** port is set to the specified value +4. The **pbsyncd** port is set to the specified value +5. The **pbrest** port is set to the specified value +6. ○ Use the following port-related menu options to set the port numbers individually for **pbmasterd**, **pblocald**, **pblogd**, **pbguid**, **pbsyncd** and **pbrestport**.
121	pbmasterd port number	Choose this option to specify the port number for **pbmasterd**. The Privilege Management for Unix and Linux policy server host daemon (**pbmasterd**) requires a dedicated port number or a Unix or Linux domain socket name to receive inbound secured task requests from submit hosts. See **Important!** in step 126.
122	pblocald port number	Choose this option to specify the port number for **pblocald**. The Privilege Management for Unix and

Opt #	Menu Item	Description
		Linux run host daemon (**pblocald**) requires a dedicated port number or a Unix or Linux domain socket name to receive inbound secured task requests from policy server hosts. See **Important!** in menu item **Base daemon port number**.
123	pblogd port number	Choose this option to specify the port number for **pblogd**. The Privilege Management for Unix and Linux log host daemon (**pblogd**) requires a dedicated port number or a Unix or Linux domain socket name to receive inbound secured task requests from policy server and local daemons. See **Important!** in menu item **Base daemon port number**.
124	pbsyncd port number	Choose this option to specify the port number for **pbsyncd**. The Privilege Management for Unix and Linux log synchronization daemon (**pbsyncd**) requires a dedicated port number or a Unix or Linux domain socket name to receive inbound requests. See **Important!** in menu item **Base daemon port number**.
125	REST Service port number	Choose the TCP/IP port number on which the **REST** service is listening, on the primary policy manager.
126	Add entries to '/etc/services'	Choose this option and specify **y** to have the services entries added to **/etc/services**. Privilege Management for Unix and Linux must be able to look up the port numbers to be used by the various Privilege Management for Unix and Linux services. The port number lookup can be done from NIS after you manually create the appropriate NIS entries. Otherwise, these services should be listed in **/etc/services**. Only ports that are specified by number for the Privilege Management for Unix and Linux daemons can have services added to **/etc/services**. Unix and Linux domain sockets and ports that are specified by name are not added to **/etc/services** by this installation procedure. 📌 *Note: On some systems you must put entries into your NIS services map (or reboot) because **inetd** ignores /etc/services after boot time.*
127	Allow non-reserved port connections	Choose this option and choose one of the following: • Specify **y** to allow non-reserved port connections. • Specify **n** to disallow connections from non-reserved port connections.
128	Inbound port range	The **MinListeningPort** setting in the **pb.settings** file determines the lower bound on the originating port range that may be used to make Privilege Management for Unix and Linux connections on the listening side. The **MaxListeningPort** setting determines the upper bound on the originating port range that may be used to make Privilege Management for Unix and Linux connections on the listening side. Choose this option and do the following: • Specify the value of the minimum port number to listen on. The value of this setting must be between 1 and the current value of the **MaxListeningPort** setting (65535). • Specify the value of the maximum port number to listen on. The value of this setting must be between the current value of the **MinListeningPort** setting (1025) and 65535.
129	Outbound port range	The **MinOutgoingPort** setting in the **pb.settings** file determines the lower bound on the originating port range that may be used to make Privilege Management for Unix and Linux connections on the originating side. The **MaxOutgoingPort** setting determines the upper bound on the originating port

Opt #	Menu Item	Description
		range that may be used to make Privilege Management for Unix and Linux connections on the originating side. Choose this option and do the following: • Specify the value of the minimum outbound port number to originate from. The value of this setting must be between 1 and 65535. • Specify the value of the maximum outbound port number to originate from. The value of this setting must be between the current value of the MinOutgoingPort setting (600) and 65535. Starting with version 8.0, the new default in **pbinstall** for the minimum value of the outbound port range was changed from 600 to 1025. However, if you don't set this value during the install and the keyword **minoutgoingport** is commented out in the **pb.settings**, the default used by the binaries is still 600. This is in order to keep backward compatibility with older releases of Privilege Management for Unix and Linux.
130	Man pages should be packed with []	[]
131	Man page extension	[]
132	Network encryption options	💡 *Tip: Before specifying any file types are to be encrypted, see Network Traffic and File Encryption in the Privilege Management for Unix and Linux System Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.* Choose this option and do one of the following: • Specify **none** to not use any network encryption. Optionally, you can type the start date and/or end date for not using any network encryption in the format: **yyyy/mm/dd**. Dates are evaluated in Universal Coordinated Time (UTC). • To add a new network encryption option, do the following: 　○ Specify **a** to add a new network encryption option.

Opt #	Menu Item	Description
		○ Specify the encryption type from the list in the following table. The default for version 8.0 and later is AES-256, and for versions prior to 8.0 is DES. The default (AES-256 or DES) is used if end dates are specified for the listed network encryption algorithm and they have all expired. If you do not want the default to be used, then specify a network encryption or **none** with no end date.

Algorithm	Encryption Type
none	none
DES	des 3des
	tripledes
AES	aes-16-16 (or aes-128) aes-16-24 (or aes-192) aes-16-32 (or aes-256) aes-24-16
	aes-24-24 aes-24-32 aes-32-16 aes-32-24 aes-32-32
Blowfish	blowfish
Cast128	cast128
Gost	gost
Loki97	loki97
Saferplus	saferplus-16 saferplus-24 saferplus-32
Serpent	serpent-16 serpent-24 serpent-32
Threeway	threeway
Tiny	tiny
Twofish	twofish-16 twofish-24 twofish-32

○ Type the full path and file name where Privilege Management for Unix and Linux is to place the encryption key file. The default is **/etc/pb.key**. Privilege Management for Unix and Linux requires a key file to use encryption. We recommend that you specify the **/etc** directory for the encryption key file.

○ Optional. Type the start date and/or end date for the encryption pair in the format: **yyyy/mm/dd**. Dates are evaluated in Universal Coordinated Time (UTC).

> (!) **IMPORTANT!**
>
> *Administrators must ensure that all hosts are using the same encryption pair; otherwise, the hosts cannot communicate with each other.*

- Specify **e** to edit an existing network encryption option and specify the number of the network encryption option. You can edit any of the following items for the selected option:

  ○ Network encryption type

  ○ Location and file name for the encryption file

Opt #	Menu Item	Description
		○ Start date for the encryption pair to take effect ○ End date for the encryption pair • Specify **d** to delete an existing network encryption option and specify the number of the network encryption option to delete it. • Specify **x** to exit this option.

133	Event log encryption options	Choose this option and do one of the following:
		
		• Specify **none** to not use any event log encryption. Optionally, you may type the start date and/or end date for not using any event log encryption in the format: **yyyy/mm/dd**. Dates are evaluated in Universal Coordinated Time (UTC).
		• To add a new event log encryption option, do the following:
		
		  ○ Specify a to add a new event log encryption option.
		  ○ Set the encryption type. The default for version 8.0 and later is AES-256, and for versions prior to 8.0 is DES.
		  ○ Specify the full path and file name where Privilege Management for Unix and Linux is to place the encryption key file. The default is **/etc/pb.key**. Privilege Management for Unix and Linux requires a key file to use encryption. We recommend that you specify the **/etc** directory for the encryption key file.
		  ○ Optional. Type the start date and/or end date for the encryption pair in the format: **yyyy/mm/dd**. Dates are evaluated in Universal Coordinated Time (UTC).
		• Specify **e** to edit an existing event log encryption option and specify the number of the event log encryption option. You can edit any of the following items for the selected option:
		
		  ○ Event log encryption type
		  ○ Location and file name for the encryption file
		  ○ Start date for the encryption pair to take effect
		  ○ End date for the encryption pair
		• Specify **d** to delete an existing event log encryption option and specify the number of the event log encryption option to delete it.
		• Choose **x** to exit this option.

134	I/O log encryption options	Choose this option and do one of the following:
		
		• Specify **none** to not use any I/O log encryption. Optionally, you may type the start date and/or end date for not using any I/O log encryption in the format: **yyyy/mm/dd**. Dates are evaluated in Universal Coordinated Time (UTC).
		• To add a new I/O log encryption option, do the following:
		
		  ○ Specify **a** to add a new I/O log encryption option.
		  ○ Set the encryption type. The default for version 8.0 and later is AES-256, and for versions prior to 8.0 is DES.
		  ○ Specify the full path and file name where Privilege Management for Unix and Linux is to place the encryption key file. The default is **/etc/pb.key**. Privilege Management for Unix

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

64

TC: 12/7/2022

Opt #	Menu Item	Description
		and Linux requires a key file to use encryption. We recommend that you specify the **/etc** directory for the encryption key file. ○ Optional. Type the start date and/or end date for the encryption pair in the format: **yyyy/mm/dd**. Dates are evaluated in Universal Coordinated Time (UTC). **⊘ IMPORTANT!** *Administrators must ensure that all hosts are using the same encryption pair; otherwise, the hosts cannot communicate with each other.* • Specify **e** to edit an existing I/O log encryption option and specify the number of the I/O log encryption option. You can edit any of the following items for the selected option: 　○ I/O log encryption type 　○ Location and file name for the encryption file 　○ Start date for the encryption pair to take effect 　○ End date for the encryption pair • Specify **d** to delete an existing I/O log encryption option and specify the number of the I/O log encryption option to delete it. • Choose **x** to exit this option.
135	Report encryption options	Choose this option and do one of the following: • Specify **none** to not use any report encryption. Optionally, you may type the start date and/or end date for not using any report encryption in the format: **yyyy/mm/dd**. Dates are evaluated in Universal Coordinated Time (UTC). • To add a new report encryption option, do the following: 　○ Specify a to add a new report encryption option. 　○ Set the encryption type. The default for version 8.0 and later is AES-256, and for versions prior to 8.0 is DES. 　○ Specify the full path and file name where Privilege Management for Unix and Linux is to place the encryption key file. The default is **/etc/pb.key**.Privilege Management for Unix and Linux requires a key file to use encryption. We recommend that you specify the **/etc** directory for the encryption key file. 　○ Optional. Type the start date and/or end date for the encryption pair in the format: **yyyy/mm/dd**. Dates are evaluated in Universal Coordinated Time (UTC). **⊘ IMPORTANT!** *Administrators must ensure that all hosts are using the same encryption pair; otherwise, the hosts cannot communicate with each other.*

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

65

Opt #	Menu Item	Description

		• Choose **e** to edit an existing report encryption option and specify the number of the report encryption option. You can edit any of the following items for the selected option:
		
		    ○ Report encryption type
		    ○ Location and file name for the encryption file
		    ○ Start date for the encryption pair to take effect
		    ○ End date for the encryption pair
		
		• Choose **d** to delete an existing report encryption option and specify the number of the report encryption option to delete it.
		
		• Choose **x** to exit this option.

136	Policy file encryption options	Choose this option and do the following:
		
		• Enter **none** to not use any policy file encryption.
		
		• To use the policy file encryption options, do the following:
		
		    ○ Set the encryption type. The default for version 8.0 and later is AES-256, and for versions prior to 8.0 is DES.
		    ○ Specify the full path and file name where Privilege Management for Unix and Linux is to place the encryption key file. The default is **/etc/pb.key**.Privilege Management for Unix and Linux requires a key file to use encryption. We recommend that you specify the **/etc** directory for the encryption key file.

137	Settings file encryption type	Choose this option and do one of the following: • Specify **none** to not use any settings file encryption. • Specify one of the encryption types.

138	REST API encryption options	Configure encryption for the REST service Application Key database. Choose this option and do one of the following:
		
		• Specify **none** to not use encryption for the REST keystore. Optionally you may type the start date and/or end date for not using any REST keystore encryption in the format: **yyyy/mm/dd**. Dates are evaluated in Universal Coordinated Time (UTC).
		
		• To add a new REST keystore encryption option, do the following:
		
		    ○ Choose **a** to add a new REST keystore encryption option.
		    ○ Set the encryption type. The default for version 8.0 and later is AES-256, and for versions prior to 8.0 is DES.
		    ○ Specify the full path and file name where Privilege Management for Unix and Linux is to place the encryption key file. The default is **/etc/pb.rest.key**. Privilege Management for Unix and Linux requires a key file to use encryption. We recommend that you specify the **/etc** directory for the encryption key file.
		    ○ Optional. Type the start date and/or end date for the encryption pair in the format: **yyyy/mm/dd**. Dates are evaluated in Universal Coordinated Time (UTC).
		
		• Choose **e** to edit an existing REST keystore encryption option and specify the entry number of the encryption option to change. You can edit any of the following items for the selected option:

Opt #	Menu Item	Description
		○ REST keystore encryption type.
		○ Location and file name for the encryption file
		○ Start date for the encryption pair to take effect
		○ End date for the encryption pair
		• Choose **d** to delete an existing REST keystore encryption option and specify the entry number of the encryption option to delete.
		• Specify **x** to exit this option.
139	Configure with Kerberos v5?	Choose this option and do one of the following:
		• Specify **n** if Kerberos v5 is not used.
		• Specify **y** to configure using Kerberos v5. You need also to perform steps 148 through 152.
140	Policy Server Daemon Kerberos Principal	[pbmasterd]
141	Local Daemon Kerberos Principal	[pblocald]
142	Log Daemon Kerberos Principal	[pblogd]
143	Sync Daemon Kerberos Principal	[pbsyncd]
144	Kerberos Keytab File	[/etc/krb5.keytab]
145	Enforce High Security Encryption	Enabling High Security enforces configuration to adhere to FIPS 140-2 security. Non-FIPS compatible encryption and hashing algorithms will be disabled. SSL running in strict FIPS mode will be enabled, enhancing the security of the installation.
146	Use SSL?	Choose this option and do one of the following:
		• Enter **y** to use SSL. When using SSL, you need to perform steps 155 to 176.
		• Enter **n** to not use SSL and skip steps 155 to 176.
		Starting in version 10.3.2, on new installs the option **SSLFirst** is turned on by default.
147	SSL Configuration?	Choose this option and do one of the following:
		• Specify **allownonssl** to allow connections to and from non-SSL hosts.
		• Specify **clientcertificates** to require client certificates.
		• Specify **requiressl** to allow communication among Privilege Management for Unix and Linux components without requiring Privilege Management for Unix and Linux client certificates. This option is not compatible with the **AllowNonSSL** option.
		• Specify **none** to clear all existing parameters.

Opt #	Menu Item	Description
148	SSL pbrun Certificate Authority Directory?	Choose this option and do one of the following: • Specify the directory location for the SSL **pbrun** certificate authority files. • Specify **none** to not specify a directory for the SSL **pbrun** certificate authority file. If you do not specify a directory, then you must specify the full path and file name for the SSL **pbrun** certificate authority file in the next step.
149	SSL pbrun Certificate Authority File?	Choose this option and do one of the following: • Specify the file name for the SSL **pbrun** certificate authority file. If you did not specify a directory in the previous step, then you need to provide the full path and file name. • Specify **none** to not specify a filename for the SSL pbrun certificate authority file. **⊙ IMPORTANT!** *Failure to specify this file name results in failed communication negotiation.*
150	SSL pbrun Cipher List?	SSL provides a variety of algorithms that can be used for encryption. This option enables you to restrict the set of encryption algorithms that are used by **pbrun** for server communication to a subset of those ciphers that are available to SSL. Choose this option and do one of the following: • Specify **ALL** to allow all ciphers to be used from the list in the following table: <table><tr><td>NULL-MD5</td><td>NULL-SHA</td></tr><tr><td>EXP-RC4-MD5</td><td>RC4-MD5</td></tr><tr><td>RC4-SHA</td><td>EXP-RC2-CBC-MD5</td></tr><tr><td>EXP-DES-CBC-SHA</td><td>DES-CBC-SHA</td></tr><tr><td>DES-CBC3-SHA</td><td>EXP-EDH-DSS-DES-CBC-SHA</td></tr><tr><td>EDH-DSS-CBC-SHA</td><td>EDH-DSS-DFS-CBC3-SHA</td></tr><tr><td>EXP-EDH-RSA-DES-CBC-SHA</td><td>EDH-RSA-DES-CBC-SHA</td></tr><tr><td>EDH-RSA-DES-CBC3-SHA</td><td></td></tr></table> • Specify one or more of the ciphers. If more than one cipher is specified, then type a space between the ciphers.
151	SSL pbrun Certificate Directory?	Choose this option and do one of the following: • Specify the directory location for the SSL **pbrun** certificate file. • Specify **none** to not specify a directory for the SSL **pbrun** certificate file. If you do not specify a directory, then you must specify the full path and file name for the SSL **pbrun** certificate file in the next step.
152	SSL pbrun	Choose this option and do one of the following:

Opt #	Menu Item	Description
	Certificate File?	• Specify the file name for the SSL **pbrun** certificate file. If you did not specify a directory in the previous step, you need to provide the full path and file name. • Specify **none** to not specify a file name for the SSL **pbrun** certificate file. **(!) IMPORTANT!** *Failure to specify this file name results in failed communication negotiation.*
153	SSL pbrun Private Key Directory?	Choose this option and do one of the following: • Specify the directory for the SSL **pbrun** private key file. • Specify **none** to not specify a directory for the SSL **pbrun** private key file. If you do not specify a directory, you need to provide the full path and file name in the next step.
154	SSL pbrun Private Key File?	Choose this option and do one of the following: • Specify the file name for the SSL **pbrun** private key file. This is the PEM-formatted private key for the client certificate file. If you did not specify a directory in the previous step, then you need to provide the full path and file name. • Specify **none** to not specify a filename for the SSL **pbrun** private key file. **(!) IMPORTANT!** *Failure to specify this file name results in failed communication negotiation.*
155	SSL pbrun Certificate Subject Checks?	The **sslpbrunverifysubject** setting enables strings or substrings of the subjects of SSL certificates to be checked and accepted by **pbrun** from **pbmasterd**. Choose this option and do one of the following: • Specify the string or substring to check in the SSL **pbrun** certificate subject. If the specified string or substring finds a match in the certificate subject, then the connection proceeds; otherwise, the connection fails. • Specify **none** to remove all checks.
156	SSL Server Certificate Authority Directory?	Choose this option and do one of the following: • Specify the directory for the SSL server certificate authority file. • Specify **none** to not specify a directory for the SSL server certificate file. If you do not specify a directory, then you need to provide the full path and file name for the SSL server certificate authority directory in the next step.
157	SSL Server Certificate Authority File?	Choose this option and do one of the following: • Specify the file name for the SSL server certificate authority file. If you did not specify a directory

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

69

TC: 12/7/2022

Opt #	Menu Item	Description
		in the previous step, then you need to provide the full path and file name. • Specify **none** to not specify a SSL server certificate authority file. **(!) IMPORTANT!** *Failure to specify this file name results in failed communication negotiation.*
158	SSL Server Cipher List?	OpenSSL provides a variety of algorithms which can be used for encryption. This option enables you to restrict the set of encryption algorithms that are used by the SSL server for communication to a subset of those ciphers that are available to OpenSSL. Choose this option and do one of the following: • Specify **ALL** to allow all ciphers in the following table to be used <table><tr><td>NULL-MD5</td><td>NULL-SHA</td></tr><tr><td>EXP-RC4-MD5</td><td>RC4-MD5</td></tr><tr><td>RC4-SHA</td><td>EXP-RC2-CBC-MD5</td></tr><tr><td>EXP-DES-CBC-SHA</td><td>DES-CBC-SHA</td></tr><tr><td>DES-CBC3-SHA</td><td>EXP-EDH-DSS-DES-CBC-SHA</td></tr><tr><td>EDH-DSS-CBC-SHA</td><td>EDH-DSS-DFS-CBC3-SHA</td></tr><tr><td>EXP-EDH-RSA-DES-CBC-SHA</td><td>EDH-RSA-DES-CBC-SHA</td></tr><tr><td>EDH-RSA-DES-CBC3-SHA</td><td></td></tr></table> • Specify one or more of the ciphers. If more than one cipher is specified, type a space between the ciphers.
159	SSL Server Certificate Directory?	Choose this option and do one of the following: • Specify the directory for the SSL server certificate file. • Specify **none** to not specify a directory for the SSL server certificate file. If you do not specify a directory, then you need to provide the full path and file name for the SSL server certificate file in the next step.
160	SSL Server Certificate File?	Choose this option and do one of the following: • Specify the file name for the SSL server certificate file. If you did not specify a directory in the previous step, you need to provide the full path and file name. • Specify **none** to not specify a SSL server certificate file name. As a convenience, pbinstall can generate the SSL server certificate file if it doesn't yet exist, provided that the absolute path is specified and the parent directories already exist.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

70

Opt #	Menu Item	Description
		⚠ **IMPORTANT!** *Failure to specify this file name results in failed communication negotiation.*
161	SSL Server Private Key Directory?	Choose this option and do one of the following: • Specify the directory for the SSL server private key file. • Specify **none** to not specify a directory for the SSL server private key file. If you do not specify a directory, then you need to provide the full path and file name for the SSL server private key file in the next step.
162	SSL Server Private Key File?	Choose this option and do one of the following: • Specify the file name for the SSL server private key file. If you did not specify a directory in the previous step, then you need to provide the full path and file name. • Specify **none** to not specify the SSL server private key file name. As a convenience, pbinstall can generate the SSL Server private key file if it doesn't yet exist, provided that the absolute path is specified and the parent directories already exist. ⚠ **IMPORTANT!** *Failure to specify this file name results in failed communication negotiation.*
163	SSL Server Certificate Subject Checks?	Choose this option and do one of the following: • Specify the string or substring to check in the SSL server certificate subject. If the specified string or substring finds a match in the certificate subject, then the connection proceeds; otherwise, the connection fails. • Specify **none** to remove all checks.
164	SSL Certificate Country Code	The Country Code used when creating client x509 certificates.
165	SSL Certificate State/Province	The State/Province used when creating client x509 certificates.
166	SSL Certificate Location/Town	The general location or town used when creating client x509 certificates.
167	SSL Certificate Organizational Unit	The organizational unit used when creating client x509 certificates.
168	SSL Certificate Organization	The organization used when creating client x509 certificates.

Opt #	Menu Item	Description
169	Configure Privilege Management for Unix & Linux with LDAP?	Choose this option and do one of the following: • Specify **n** to not enable Privilege Management for Unix and Linux to use LDAP • Specify **y** to enable Privilege Management for Unix and Linux to use LDAP.
170	Install BeyondTrust built-in third-party libraries?	Choose this option and do one of the following: • Specify **y** to install the BeyondTrust built-in third-party libraries. • Specify **n** to not install BeyondTrust built-in third party libraries. 📌 *Note: If you are using LDAP, Kerberos, or SSL, then you need to install third-party libraries. You can install the BeyondTrust third-party libraries or your own. We recommend that you use the BeyondTrust third-party libraries.*
171	BeyondTrust built-in third-party library directory	Choose this option and specify the directory for the BeyondTrust built-in third-party libraries. You also need to specify a directory for your own built-in libraries in step 188 .
172	Kerberos shared library default directory	[none]
173	Kerberos libkrb5 shared library filename	[none]
174	Kerberos libgssapi_krb5 shared library filename	[none]
175	Kerberos libcom_err shared library filename	[none]
176	Kerberos libk5crypto shared library filename	[none]
177	SSL shared library default directory	[none]
178	SSL libssl shared library filename	[none]
179	SSL libcrypto shared library filename	[none]
180	LDAP shared	[none]

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

72

TC: 12/7/2022

Opt #	Menu Item	Description
	library default directory	
181	LDAP libldap shared library filename	[none]
182	LDAP liblber shared library filename	[none]
183	Use PAM?	Privilege Management for Unix and Linux enables the use of Pluggable Authentication Modules (PAM) when Privilege Management for Unix and Linux asks for password confirmation. The authentication and account management portions of this service are invoked whenever Privilege Management for Unix and Linux verifies a password. • PAM is used on a policy server host when the **getuserpasswd()** and **getgrouppasswd()** policy functions are invoked and this setting is set to **y**. • PAM is used on a submit host when the policy calls the **submitconfirmuser()** policy language function and this setting is set to **y**. • PAM is used on a run host when the policy sets the **runconfirmuser** policy language variable to **TRUE** and this setting is set to **y**. Choose this option and do one of the following: • Specify **y** to use PAM Privilege Management for Unix and Linux processing on this machine. You also need to perform the next PAM-related steps. • Specify **n** to not use PAM Privilege Management for Unix and Linux processing on this machine.
184	PAM service for password verification	[none]
185	PAM session service	[none]
186	PAM suppress password prompting?	[yes]
187	PAM library file name	[none]
188	Call pam_setcred?	[no]
189	Enable non-PAM Solaris Projects?	[no]
190	Solaris Projects library file name	[none]

Opt #	Menu Item	Description

191	Allow Remote Jobs?	When this option is set to **n**, Privilege Management for Unix and Linux prohibits the control of remotely executed jobs as follows:
		
		• On a policy server host, requests that have different submit host and run host names are automatically rejected. The **runhost** policy variable is set to read only.
		• On a submit host, the **-h** option for the **pbrun** command is disabled, and the runhost variable of the request is set to the IP address of the submit host.
		• On a run host, all requests that do not originate from the Run Host are rejected. Choose this option and do one of the following:
		    ○ Specify **y** to allow remote jobs. This setting is the default.
		    ○ Specify **n** to not allow remote jobs.

192	UNIX Domain Socket directory	When Privilege Management for Unix and Linux determines that communication may occur using Unix or Linux domain sockets, there must be a protected directory that contains the sockets used for reconnects and backconnects. Using Unix and Linux domain sockets for communication between daemons on the same machine should be more efficient than TCP socket communications. The directory that is specified for Privilege Management for Unix and Linux Unix and Linux domain sockets must be protected from non-root read and write access, and each of the parent directories must be protected from non-root write access. Choose this option and specify the directory for the Privilege Management for Unix and Linux Unix or Linux domain socket.
193	Reject Null Passwords?	Choose this option and do one of the following: • Specify **n** to match an entered null password to any existing password. • Specify **y** to require the user to exactly match the password.
194	Enable TCP keepalives?	Privilege Management for Unix and Linux enables the communication TCP connections to use the TCP stack's keepalive feature. TCP keepalives can be useful in cases where a firewall keeps track of idle TCP connections and terminates the sessions prematurely. Choose this option and do one of the following: • Specify **n** to disable TCP keepalive signals. • Specify **y** to enable TCP keepalive signals.
195	Name Resolution Timeout	Privilege Management for Unix and Linux attempts to obtain fully qualified domain names when a **pblogd**, **pblocald**, **pbmasterd**, or **pbrun** session is started. This setting defines the timeout period (in seconds) to be used for the request to expire. Choose this option and do one of the following: • Set the value to **0** to disable this feature (default). • Set the value from 1 to 7200 to define the number of seconds to use for the timeout period.

For more information, please see the following:

ⓘ
- *"Privilege Management for Unix & Linux and AD Bridge" in the Privilege Management for Unix & Linux System Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*
- *On SSL, "Secure Socket Layers and Public Key Infrastructure" in the Privilege Management for Unix and Linux System Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm*
- *"Configure Third-Party Libraries" on page 21*

Complete the Installation

After you finish making menu choices, do the following to complete the installation:

1. Use the **c** command to continue the installation.
2. A prompt asks if all of the installation settings are correct. If they are correct, then specify **y**. If they are not correct, then specify **n**, make the necessary changes, and continue the previous step.
3. A prompt asks if you want to view the installation script. Choose **n**.

> **(!) IMPORTANT!**
>
> *This option is intended for troubleshooting by BeyondTrust Technical Support; the generated installation script contains thousands of lines of code.*

4. A prompt asks if you want to install the product now. Press **Enter** to accept the default of **y**.
5. The installation script now executes and installs Privilege Management for Unix and Linux components on this machine.
6. If a Privilege Management for Unix and Linux policy file exists, it is not modified. If you do not have a policy file, then create a policy file using the following command:

```
touch /opt/pbul/policies/pb.conf
```

> **(!) IMPORTANT!**
>
> *An empty policy file rejects all Privilege Management for Unix and Linux commands. For information about writing policy files, see the* *Privilege Management for Unix and Linux Policy Language Guide* *at* *https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm*.

7. Change the permissions on the policy file so that it can be read by root only:

```
chmod 600 /opt/pbul/policies/pb.conf
```

The installation is now complete.

Example of a pbinstall Execution

The following is an example of a **pbinstall** execution:

> **Example:**
>
> ```
> /usr/local/lib/pbbuilder will be created as part of the installation
> /etc/pb.key exists.. taking a copy...
> ```

```
Checking disk space...

... mountpoints are
/ /dev /net/build/build /net/nethome/nethome/tmp
/net/nethome/nethome/user /pbis

... local mount points are
/ /dev

Mount Point Needed Available Flag
/ 27117 359448716 works

Disk Free space on selected mountpoints appears to be okay.

Are all the installation settings correct [yes]? Creating the installation script:
'/opt/symark/powerbroker/v8.0/pbx86_64_linuxA-8.0.0-06/install/PowerBroker_ Install'
An install script has been made that will install BeyondTrust Privilege Management


according to your settings. View the install script [no]?
Install BeyondTrust Privilege Management for Unix and Linux now [yes]?

Executing '/opt/symark/powerbroker/v8.0/pbx86_64_linuxA-8.0.0- 06/install/PowerBroker_
Install'
Creating settings file /etc/pb.settings
Removing PowerBroker service definitions (if any) from /etc/services. Adding PowerBroker
service definitions to /etc/services.
Removing any PowerBroker definitions from SuperDaemon xinetd file
/etc/xinetd.conf
Adding PowerBroker definitions to SuperDaemon configurations /etc/xinetd.conf. Installed
/usr/lib/beyondtrust/pb/libcom_err.so.3.0
Installed /usr/lib/beyondtrust/pb/libgssapi_krb5.so.2.2 Installed
/usr/lib/beyondtrust/pb/libk5crypto.so.3.0 Installed
/usr/lib/beyondtrust/pb/libkrb5.so.3.2 Installed
/usr/lib/beyondtrust/pb/libcrypto.so.0.9.8 Installed
/usr/lib/beyondtrust/pb/libssl.so.0.9.8 Installed /usr/lib/beyondtrust/pb/liblber-
2.3.so.0.2.12 Installed /usr/lib/beyondtrust/pb/libLDAP-2.3.so.0.2.12 Installed
/usr/lib/beyondtrust/pb/libcurl.so.4.3.0
Created symbolic link /usr/lib/beyondtrust/pb/libcom_err.so.3 Created symbolic link
/usr/lib/beyondtrust/pb/libcom_err.so Created symbolic link
/usr/lib/beyondtrust/pb/libgssapi_krb5.so.2 Created symbolic link
/usr/lib/beyondtrust/pb/libgssapi_krb5.so Created symbolic link
/usr/lib/beyondtrust/pb/libk5crypto.so.3 Created symbolic link
/usr/lib/beyondtrust/pb/libk5crypto.so Created symbolic link
/usr/lib/beyondtrust/pb/libkrb5.so.3
Created symbolic link /usr/lib/beyondtrust/pb/libkrb5.so Created symbolic link
/usr/lib/beyondtrust/pb/libcrypto.so.0 Created symbolic link
/usr/lib/beyondtrust/pb/libcrypto.so Created symbolic link
/usr/lib/beyondtrust/pb/libssl.so.0 Created symbolic link
/usr/lib/beyondtrust/pb/libssl.so
Created symbolic link /usr/lib/beyondtrust/pb/liblber-2.3.so.0 Created symbolic link
/usr/lib/beyondtrust/pb/liblber-2.3.so Created symbolic link
```

```
/usr/lib/beyondtrust/pb/libLDAP-2.3.so.0 Created symbolic link
/usr/lib/beyondtrust/pb/libLDAP-2.3.so Created symbolic link
/usr/lib/beyondtrust/pb/libcurl.so.4 Created symbolic link
/usr/lib/beyondtrust/pb/libcurl.so Installed pbrun as /usr/local/bin/pbrun
Installed /usr/local/man/man1/pbrun.1 Installed pbssh as /usr/local/bin/pbssh Installed
/usr/local/man/man1/pbssh.1 Installed pbrunssh as /usr/local/bin/pbrunssh Installed
pbmasterd as /usr/sbin/pbmasterd Installed /usr/local/man/man8/pbmasterd.8
Installed pbfwdevents as /usr/sbin/pbfwdevents Installed
/usr/local/man/man8/pbfwdevents.8 Installed pblocald as /usr/sbin/pblocald Installed
/usr/local/man/man8/pblocald.8 Installed pblogd as /usr/sbin/pblogd


Installed /usr/local/man/man8/pblogd.8 Installed pbguid as /usr/sbin/pbguid Installed
/usr/local/man/man8/pbguid.8 Installed pbsyncd as /usr/sbin/pbsyncd Installed
/usr/local/man/man8/pbsyncd.8 Installed pbencode as /usr/sbin/pbencode Installed
/usr/local/man/man8/pbencode.8 Installed pbhostid as /usr/sbin/pbhostid Installed
/usr/local/man/man8/pbhostid.8 Installed pblicense as /usr/sbin/pblicense Installed
/usr/local/man/man8/pblicense.8 Installed pbpasswd as /usr/sbin/pbpasswd Installed
/usr/local/man/man8/pbpasswd.8 Installed pbsum as /usr/sbin/pbsum Installed
/usr/local/man/man8/pbsum.8
Installed pbbench as /usr/local/bin/pbbench Installed /usr/local/man/man1/pbbench.1
Installed pbcheck as /usr/sbin/pbcheck Installed /usr/local/man/man8/pbcheck.8 Installed
pbcall as /usr/local/bin/pbcall Installed pbless as /usr/local/bin/pbless Installed
/usr/local/man/man1/pbless.1 Installed pbmg as /usr/local/bin/pbmg Installed
/usr/local/man/man1/pbmg.1 Installed pbnvi as /usr/local/bin/pbnvi Installed
/usr/local/man/man1/pbnvi.1 Installed pbumacs as /usr/local/bin/pbumacs Installed
/usr/local/man/man1/pbumacs.1 Installed pbvi as /usr/local/bin/pbvi Installed
/usr/local/man/man1/pbvi.1 Installed pbkey as /usr/sbin/pbkey
Installed /usr/local/man/man8/pbkey.8 Installed pblog as /usr/sbin/pblog Installed
/usr/local/man/man8/pblog.8 Installed pbreplay as /usr/sbin/pbreplay Installed
/usr/local/man/man8/pbreplay.8 Installed pbmerge as /usr/sbin/pbmerge Installed
/usr/local/man/man8/pbmerge.8 Installed pbsync as /usr/sbin/pbsync Installed
/usr/local/man/man8/pbsync.8 Installed pbping as /usr/sbin/pbping Installed
/usr/local/man/man8/pbping.8 Installed pbprint as /usr/sbin/pbprint Installed
/usr/local/man/man8/pbprint.8 Installed pbksh as /usr/local/bin/pbksh Installed pbsh as
/usr/local/bin/pbsh Installed pbreport as /usr/sbin/pbreport Installed
/usr/local/man/man8/pbreport.8 Installed pbuvqrpg as /usr/sbin/pbuvqrpg Installed
/usr/local/man/man8/pbuvqrpg.8 Installed pbversion as /usr/sbin/pbversion Installed
/usr/local/man/man8/pbversion.8 Installed /usr/local/man/man8/pbinstall.8 Installed
/usr/local/man/man8/pbuninstall.8


Installed /usr/local/man/man8/pbmakeremotetar.8 Installed
/usr/local/man/man8/pbpatchinstall.8
Placing policy examples in '/usr/local/lib/pbbuilder'
Placing pbguid html help files in '/usr/local/lib/pbbuilder' Installing /etc/pb.key
Reloading SuperDaemon Configurations...
Done Reloading SuperDaemon Configurations...


-------------------------------------------------------------------------------
Installing default role-based policy pbul_policy.conf and pbul_functions.conf in
```

```
/opt/pbul/policies
The main policy pbul_policy.conf will be included in /opt/pbul/policies/pb.conf

Installed pbul_policy.conf as /opt/pbul/policies/pbul_policy.conf
-------------------------------------------------------------------------------
You will have to edit the /opt/pbul/policies/pb.conf file now.
Installed pblighttpd as /usr/lib/beyondtrust/pb/rest/sbin/pblighttpd Installed
pblighttpd-svc as /usr/lib/beyondtrust/pb/rest/sbin/pblighttpd-svc Installed
/usr/lib/beyondtrust/pb/rest/lib/mod_access.so
Installed /usr/lib/beyondtrust/pb/rest/lib/mod_dirlisting.so Installed
/usr/lib/beyondtrust/pb/rest/lib/mod_fastcgi.so Installed
/usr/lib/beyondtrust/pb/rest/lib/mod_indexfile.so Installed
/usr/lib/beyondtrust/pb/rest/lib/mod_staticfile.so Installed
/usr/lib/beyondtrust/pb/rest/..//pbsudoers_server.so
Installed pbconfigd as /usr/lib/beyondtrust/pb/rest/sbin/pb900pbconfigd Installed
pbrestcall as /usr/sbin/pbrestcall
Starting pblighttpd-svc service.BeyondTrust Privilege Management for Unix and Linux
Installation terminated successfully.
```

pbmakeremotetar Installation Script

Deployment of Privilege Management for Unix and Linux across multiple machines of the same platform type can be simplified by cloning the installations. Installation cloning is done by making a remote tarball using **pbmakeremotetar**, a menu-driven, interactive installation script.

pbmakeremotetar Installation Information

The section contains information about running an example **pbmakeremotetar** installation.

- **pbmakeremotetar** is used to clone an installed copy of Privilege Management for Unix and Linux so it can be quickly installed on other hosts that use the same Privilege Management for Unix and Linux flavor. The directory structure on the target systems must also be the same as on the host that is running **pbmakeremotetar**.
- **pbmakeremotetar** properly configures (as appropriate) **/etc/services** and the superdaemon configuration files (**/etc/inetd.conf**, **/etc/xinetd.conf**, or **SMF**).
- For Policy Server target installations, an initial installation (not a remote installation) must be done before any target remote installation. Doing so ensures that all licensing issues are handled properly.
- Different target system installation working directories should be used for different prefix and/or suffix versions of cloned installations.
- **pbmakeremotetar** scans the main policy file (by default **/opt/pbul/policies/pb.conf** from v9.4.3+ and **/etc/pb.conf** prior to v9.4.3) for included policy files and includes them in the tarball. If the main policy file is encrypted, **pbmakeremotetar** is not able to scan it for included policy files. Therefore, if the main policy file is encrypted, you must do one of the following:
  - Restore the unencrypted policy file before running the **pbmakeremotetar** installation script.
  - Specify each encrypted policy file in the editor session after answering **y** to the **Do you wish to make changes to this list?** prompt:
  - Manually move the encrypted files to the target systems.

- For **pbmakeremotetar/pbremoteinstall** installations where integration with AD Bridge is desired, if AD Bridge is configured on the system where the Privilege Management for Unix and Linux instance is cloned, when the cloned instance is installed, if the AD Bridge libraries are missing, then a warning message is displayed.

Remote Installations Using pbmakeremotetar

Remote installations using **pbmakeremotetar** perform the following three basic steps:

1. Execute **pbmakeremotetar**.
2. Make the created tar file available to the target system.
3. Unarchive the tar file and execute **remote_unpack** from that tar file.

Example of a pbmakeremotetar Execution

The following is an example of a **pbmakeremotetar** execution:

> ***Example:***
>
> ```
> # ./pbmakeremotetar -a /opt/beyondtrust/pb.tar
> Starting pbmakeremotetar main() from /opt/beyondtrust/powerbroker/v6.0/pbx86_ linuxB-
> 6.0.0-01/install/.
>
> pbmakeremotetar
>
> This command is used to duplicate the current system's installation of BeyondTrust
> Privilege Management for Unix and Linux to allow this duplication to be installed on one
> or more identically configured systems.
> x86_linuxB
> Hit return or enter to continue...
>
> Checking tar command for needed switches...
> Done checking tar command for needed switches...
> Making file /opt/beyondtrust/pb.tar for architecture x86_linuxB Reading /etc/pb.cfg
>
> Current additional files for deployment: [displays list of files]
> Do you wish to make changes to this list [no]?
>
> Building encapsulated tarball
> /etc/pb.cfg
> /etc/pb.conf
> /etc/pb.key
> /etc/pb.settings
> /etc/pb.key
> /opt/beyondtrust/powerbroker/v6.0/pbx86_linuxB-6.0.0-01/install/./pb.keyfiles
> /opt/beyondtrust/powerbroker/v6.0/pbx86_linuxB-6.0.0- 01/install/./pbremoteinstall
> /opt/beyondtrust/powerbroker/v6.0/pbx86_linuxB-6.0.0-01/install/./pb_install_
> support
> /opt/beyondtrust/powerbroker/v6.0/pbx86_linuxB-6.0.0- 01/install/./pbmakeremotetar
> /opt/beyondtrust/powerbroker/v6.0/pbx86_linuxB-6.0.0-01/install/./pbuninstall
> /opt/beyondtrust/powerbroker/v6.0/pbx86_linuxB-6.0.0-01/install/./sy_install_ support
> ```

```
/usr/lib/symark/pb/.BeyondTrustCreated
/usr/lib/symark/pb/.pbinstalls
/usr/lib/symark/pb/libcom_err.so
/usr/lib/symark/pb/libcom_err.so.3
/usr/lib/symark/pb/libcom_err.so.3.0
/usr/lib/symark/pb/libcrypto.so
/usr/lib/symark/pb/libcrypto.so.0
/usr/lib/symark/pb/libcrypto.so.0.9.7
/usr/lib/symark/pb/libgssapi_krb5.so
/usr/lib/symark/pb/libgssapi_krb5.so.2
/usr/lib/symark/pb/libgssapi_krb5.so.2.2
/usr/lib/symark/pb/libk5crypto.so
/usr/lib/symark/pb/libk5crypto.so.3
/usr/lib/symark/pb/libk5crypto.so.3.0
/usr/lib/symark/pb/libkrb5.so
/usr/lib/symark/pb/libkrb5.so.3
/usr/lib/symark/pb/libkrb5.so.3.2
/usr/lib/symark/pb/liblber-2.3.so
/usr/lib/symark/pb/liblber-2.3.so.0
/usr/lib/symark/pb/liblber-2.3.so.0.2.12
/usr/lib/symark/pb/libLDAP-2.3.so
/usr/lib/symark/pb/libLDAP-2.3.so.0
/usr/lib/symark/pb/libLDAP-2.3.so.0.2.12
/usr/lib/symark/pb/libssl.so
/usr/lib/symark/pb/libssl.so.0
/usr/lib/symark/pb/libssl.so.0.9.7
/usr/local/bin/pbbench
/usr/local/bin/pbcall
/usr/local/bin/pbksh
/usr/local/bin/pbless
/usr/local/bin/pbmg
/usr/local/bin/pbnvi
/usr/local/bin/pbrun
/usr/local/bin/pbsh
/usr/local/bin/pbumacs
/usr/local/bin/pbvi
/usr/local/man/man1/pbbench.1
/usr/local/man/man1/pbless.1
/usr/local/man/man1/pbmg.1
/usr/local/man/man1/pbnvi.1
/usr/local/man/man1/pbrun.1
/usr/local/man/man1/pbumacs.1
/usr/local/man/man1/pbvi.1
/usr/local/man/man8/pbcheck.8
/usr/local/man/man8/pbencode.8
/usr/local/man/man8/pbguid.8
/usr/local/man/man8/pbhostid.8
/usr/local/man/man8/pbkey.8
/usr/local/man/man8/pblicense.8
/usr/local/man/man8/pblocald.8
/usr/local/man/man8/pblog.8
/usr/local/man/man8/pblogd.8
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

81

```
        /usr/local/man/man8/pbmasterd.8
        /usr/local/man/man8/pbmerge.8
        /usr/local/man/man8/pbpasswd.8
        /usr/local/man/man8/pbprint.8
        /usr/local/man/man8/pbreplay.8
        /usr/local/man/man8/pbreport.8
        /usr/local/man/man8/pbsum.8
        /usr/local/man/man8/pbsync.8
        /usr/local/man/man8/pbsyncd.8
        /usr/local/man/man8/pbuvqrpg.8
        /usr/sbin/pbcheck
        /usr/sbin/pbencode

        /usr/sbin/pbhostid
        /usr/sbin/pbkey
        /usr/sbin/pblocald
        /usr/sbin/pblog
        /usr/sbin/pblogd
        /usr/sbin/pbmasterd/usr/sbin/pbmerge
        /usr/sbin/pbpasswd
        /usr/sbin/pbprint
        /usr/sbin/pbreplay
        /usr/sbin/pbreport
        /usr/sbin/pbsum
        /usr/sbin/pbsync
        /usr/sbin/pbsyncd
        /usr/sbin/pbuvqrpg
        Building encapsulating tarball remote_unpack
        pb.tar.tar

        /opt/beyondtrust/pb.tar has been built
```

Make the Tar File Available to the Remote System

To make the tar file available to the remote system, you can use FTP (image mode), NFS, or any other mechanism as long as the security and integrity of the binary tar file are maintained.

If **tar –x** warns about a directory checksum error, then the tar file archive may be corrupt because it was copied in ASCII, not binary (or image) mode.

Untar the Remote Archive and Execute remote_unpack

When the tar file is made available to the remote system, a temporary working directory must be selected to unarchive the remote archive. An installation work directory other than **/tmp** should be selected (for the same reasons as with **pbinstall**). Unpacking the archive makes the encapsulated tar archive and a script called **remote_unpack** visible.

The **remote_unpack** script then executes. This script unpacks the encapsulated tar file (putting the files in their required places) and reconfigures the system files (**/etc/services** and the superdaemon configuration) for Privilege Management for Unix and Linux.

The following listing shows an example execution of the **remote_unpack** script:

SALES: www.beyondtrust.com/contact   SUPPORT: www.beyondtrust.com/support   DOCUMENTATION: www.beyondtrust.com/docs

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

82

TC: 12/7/2022

> **Example:**
>
> ```
> # cd {workingdirectory}
> # tar -xvf {tarfilename}.tar
> x remote_unpack, 1250 bytes, 3 tape blocks
> x tarfilename.tar.tar, 48152576 bytes, 94048 tape blocks
> # ./remote_unpack
>
> Deploying executable files...
>
> x /usr/local/bin/pbrun, 4282296 bytes, 8364 tape blocks x /usr/local/man/man1/pbrun.1,
> 2852 bytes, 6 tape blocks
> x /usr/local/bin/pbbench, 3414416 bytes, 6669 tape blocks x
> /usr/local/man/man1/pbbench.1, 1152 bytes, 3 tape blocks x /usr/local/bin/pbless, 178964
> bytes, 350 tape blocks
> x /usr/local/man/man1/pbless.1, 743 bytes, 2 tape blocks x /usr/local/bin/pbmg, 52 bytes,
> 1 tape blocks
> x /usr/local/man/man1/pbmg.1, 809 bytes, 2 tape blocks x /usr/local/bin/pbumacs, 52
> bytes, 1 tape blocks
> x /usr/local/man/man1/pbumacs.1, 832 bytes, 2 tape blocks x /usr/local/bin/pbvi, 212000
> bytes, 415 tape blocks
> x /usr/local/man/man1/pbvi.1, 1107 bytes, 3 tape blocks x /usr/local/bin/pbcall, 3585880
> bytes, 7004 tape blocks x /usr/sbin/pblocald, 4714020 bytes, 9208 tape blocks
> x /usr/local/man/man8/pblocald.8, 1525 bytes, 3 tape blocks x /usr/sbin/pbcheck, 4202964
> bytes, 8209 tape blocks
> x /usr/local/man/man8/pbcheck.8, 2824 bytes, 6 tape blocks x /usr/sbin/pbhostid, 191596
> bytes, 375 tape blocks
> x /usr/local/man/man8/pbhostid.8, 815 bytes, 2 tape blocks x /usr/sbin/pbkey, 187548
> bytes, 367 tape blocks
> x /usr/local/man/man8/pbkey.8, 1113 bytes, 3 tape blocks x /usr/sbin/pblog, 3836692
> bytes, 7494 tape blocks
> x /usr/local/man/man8/pblog.8, 5346 bytes, 11 tape blocks x /usr/sbin/pbpasswd, 186536
> bytes, 365 tape blocks
> x /usr/local/man/man8/pbpasswd.8, 1413 bytes, 3 tape blocks x /usr/sbin/pbreplay, 3550320
> bytes, 6935 tape blocks
> x /usr/local/man/man8/pbreplay.8, 3522 bytes, 7 tape blocks x /usr/sbin/pbsum, 77872
> bytes, 153 tape blocks
> x /usr/local/man/man8/pbsum.8, 853 bytes, 2 tape blocks x /usr/sbin/pbencode, 3163940
> bytes, 6180 tape blocks
> x /usr/local/man/man8/pbencode.8, 927 bytes, 2 tape blocks x /usr/sbin/pbmasterd, 5505740
> bytes, 10754 tape blocks
> x /usr/local/man/man8/pbmasterd.8, 1578 bytes, 4 tape blocks x /usr/sbin/pblogd, 3956552
> bytes, 7728 tape blocks
> x /usr/local/man/man8/pblogd.8, 1015 bytes, 2 tape blocks x /usr/sbin/pbguid, 6537648
> bytes, 12769 tape blocks
> x /usr/local/lib/pbbuilder/.BeyondTrustCreated, 29 bytes, 1 tape blocks x
> /usr/local/lib/pbbuilder/fileselect.html, 1075 bytes, 3 tape blocks
> x /usr/local/lib/pbbuilder/iolog.html, 2346 bytes, 5 tape blocks x
> /usr/local/lib/pbbuilder/log.html, 1139 bytes, 3 tape blocks
> x /usr/local/lib/pbbuilder/settings.html, 23014 bytes, 45 tape blocks x
> /usr/local/lib/pbbuilder/variables.html, 34964 bytes, 69 tape blocks
> x /usr/local/lib/pbbuilder/.BeyondTrustCreated, 29 bytes, 1 tape blocks x
> /usr/local/lib/pbbuilder/fileselect.html, 1075 bytes, 3 tape blocks
> ```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

83

```
x /usr/local/lib/pbbuilder/iolog.html, 2346 bytes, 5 tape blocks x
/usr/local/lib/pbbuilder/log.html, 1139 bytes, 3 tape blocks
x /usr/local/lib/pbbuilder/settings.html, 23014 bytes, 45 tape blocks x
/usr/local/lib/pbbuilder/variables.html, 34964 bytes, 69 tape blocks
x /opt/beyondtrust/pb/install/pbremoteinstall, 3362 bytes, 7 tape blocks
x /opt/beyondtrust/pb/install/pbmakeremotetar, 14650 bytes, 29 tape blocks x
/opt/beyondtrust/pb/install/pbuninstall, 11565 bytes, 23 tape blocks
x /opt/beyondtrust/pb/install/pb_install_support, 13212 bytes, 26 tape blocks
x /opt/beyondtrust/pb/install/sy_install_support, 93560 bytes, 183 tape blocks
x /opt/beyondtrust/pb/install/platform, 5971 bytes, 12 tape blocks x /etc/pb.key, 1026
bytes, 3 tape blocks
x /opt/beyondtrust/pb/install/pb.cfg, 1161 bytes, 3 tape blocks
x /opt/beyondtrust/pb/install/pb.cfg.sparc_solaris7, 2 bytes, 1 tape blocks x
/opt/beyondtrust/pb/install/pb.cfg.default, 2 bytes, 1 tape blocks
x /etc/pb.settings, 1915 bytes, 4 tape blocks
x /usr/local/man/man8/pbinstall.8, 6047 bytes, 12 tape blocks x
/usr/local/man/man8/pbuninstall.8, 2569 bytes, 6 tape blocks
x /usr/local/man/man8/pbmakeremotetar.8, 4239 bytes, 9 tape blocks x /etc/pb.conf, 202
bytes, 1 tape blocks
Configure System now? [yes]
Starting pbremoteinstall main() from /opt/beyondtrust//pb_xyzzy/pb/install Reading
/opt/beyondtrust/pb/install/pb.cfg
Reading /opt/beyondtrust/pb/install/pb.cfg.sparc_solaris7 Reading
/opt/beyondtrust/pb/install/pb.cfg.default
Removing PowerBroker service definitions (if any) from /etc/services. Removing
PowerBroker service definitions (if any) from /etc/services. Adding PowerBroker service
definitions to /etc/services.
Looking for SuperDaemons to configure...
Finished looking for SuperDaemons to configure...
Removing any PowerBroker definitions from SuperDaemon inetd file
/etc/inetd.conf
Adding PowerBroker definitions to SuperDaemon configurations
/etc/inetd.conf.
Reloading SuperDaemon Configurations...
Done Reloading SuperDaemon Configurations...
/opt/beyondtrust/pb/install/pbremoteinstall ... Done
```

pbpatchinstall Installation Script

BeyondTrust occasionally releases patches to the Privilege Management for Unix and Linux product that improve performance and fix problems. You install these patches with the **pbpatchinstall** installation script.

pbpatchinstall Installation Information

This section contains information about installing a Privilege Management for Unix and Linux patch with the **pbpatchinstall** script.

pbpatchinstall determines the current release of Privilege Management for Unix and Linux that is installed on the machine and whether the release is compatible with the current patch. Multiple patches can be installed.

Based on the type of Privilege Management for Unix and Linux host that is installed on the machine (policy server host, submit host, log host, and so forth), **pbpatchinstall** copies only the appropriate files to the appropriate directories to replace the existing files. **pbpatchinstall** makes a backup copy of all replaced files. These backup files are then available to restore the original files if the patch needs to be removed.

> 📌 **Note:** *All Privilege Management for Unix and Linux daemons running a process during the patch installation should be stopped before using **pbpatchinstall** and restarted after using **pbpatchinstall**.*

After you extract a Privilege Management for Unix and Linux patch tarball file, the patch version becomes part of the directory path. For example, in the patch directory: **/opt/beyondtrust/powerbroker/v5.1/ pbx86_linuxA-5.1.2-03-sp1/install**, the patch version is **pbx86_linuxA-5.1.2-03-sp1**.

The **pbpatchinstall** installation process performs the following:

- Inventories the Privilege Management for Unix and Linux installation, using prefixes and/or suffixes (if any). Use the **-p** and/or **-s** arguments if you want **pbpatchinstall** to use prefixes and/or suffixes.
- Validates the existence and version of the Privilege Management for Unix and Linux binary files that should be present for each component.
- Lists the Privilege Management for Unix and Linux components that are currently installed.

The Privilege Management for Unix and Linux patch release number must match the installed Privilege Management for Unix and Linux release number. If the release numbers do not match, a prompt is displayed, stating that the patch release does not match the existing Privilege Management for Unix and Linux release and asks if you want to install the patch release over the existing Privilege Management for Unix and Linux release. To complete the installation, type **y**.

> 📌 **Note:** *To run the patch installation without this prompt, use the **-f** argument.*

Example of a pbpatchinstall Execution

The following is an example of a **pbpatchinstall** execution:

> 🔍 **Example:**
>
> ```
> #pwd
> /opt/beyondtrust/powerbroker/v5.1/pbx86_linuxB-5.1.1-03-sp1/install
> # ./pbpatchinstall
>
> Starting pbpatchinstall from /opt/beyondtrust/powerbroker/v5.1/pbx86_linuxB
> -5.1.1-03-sp1/install/.x86_linuxB BeyondTrust PowerBroker Patch Installation
> Checking MANIFEST against release directory Trying /etc/pb.settings
> Settings are from file='/etc/pb.settings'
> Reading /etc/pb.cfg
> PowerBroker version 5.1.0-08 established from /etc/pb.cfg PowerBroker components
> currently installed:
> run_host submit_host log_synchronization secure_gui_host utilities
> pbksh log_sync_initiator
>
> All installed binaries match Privilege Management for Unix and Linux version 5.1.0-08
> ```

```
Version is not evaluated for binaries pbuvqrpg and pbnvi.

Patch release 5.1.1 does not match Privilege Management for Unix and Linux release 5.1.0
Install PowerBroker patch release 5.1.1 over Privilege Management for Unix and Linux
release 5.1.0? [no] y Checking disk space...
... mountpoints are
/ /boot /data /dev /net/nethome/nethome/user

... local mount points are
/ /boot /data /dev

Mount Point Needed Available Flag
/ 1024 2921852 works
/data 2590 126953328 works
Disk Free space on selected mountpoints appears to be okay. Patched /usr/sbin/pbencode
installed.
Patched /usr/local/bin/pbbench installed. Patched /usr/local/bin/pbrun installed. Patched
/usr/sbin/pbreport installed. Patched /usr/local/bin/pbksh installed.
6 files patched, replaced files moved to /opt/beyondtrust/powerbroker/v5.1/pbx86_linuxB-
5.1.1-03- sp1/bin_patchbkp
NOTE: In order to remove patch, directory /opt/beyondtrust/powerbroker/v5.1/pbx86_linuxB-
5.1.1-
03-sp1/bin_patchbkp must be left in place.
/etc/pb.cfg updated with patch information. 5.1.1-03-sp1 patches installed.
```

Custom Installations

The preferred methods for installing Privilege Management for Unix and Linux are to use the command line **pbinstall** or **pbmakeremotetar**. In some instances, however, customer requirements may dictate some custom installation methods. This section covers several topics you should be aware of when planning a custom installation.

Before performing a custom installation of Privilege Management for Unix and Linux, several issues need to be taken into consideration:

- Third-party libraries
- Executable files
- **pb.settings** file
- **pb.key** file
- Superdaemon configuration update
- Policy files for policy server hosts

There are some concerns about file system accessibility when using remotely mounted file systems. If an installation initially references files on a system with a different name (due to network and/or NIC configurations), the target system may have problems referencing the files correctly on the original host.

Third-Party Libraries

The appropriate third-party libraries are required when Privilege Management for Unix and Linux is configured with SSL, Kerberos, or LDAP.

> *For more information about third-party libraries, please see "Configure Third-Party Libraries" on page 21.*

Executable Files

Regardless of how Privilege Management for Unix and Linux is placed on multiple systems, the proper executable and supporting files for the flavor and functions of the system must be visible and executable on that system.

It is possible to place the target of the administration, user, daemon, and/or utility programs on a remotely mounted file system. If this is done, the following issues must be addressed:

- The correct flavor for a system must be visible in the path for the given system.
- The superuser owner and **suid** setting of **pbrun** must be handled properly.
- The remotely mounted file system must be very reliable.
- Privilege Management for Unix and Linux event, I/O, and daemon error logs are not supported when written to remotely mounted file systems.

Settings File

The **/etc/pb.settings** file must be properly configured for the functions that the new host is to perform, and the install scripts do this. When performing a custom install, each machine needs a correctly configured **/etc/pb.settings** file.

Key File

If encryption is used, then the **pb.key** file must be the same across all cooperating Privilege Management for Unix and Linux installations. This is typically a manual distribution (because the **pb.key** file can be compromised if it is not handled properly) except when performing a remote installation using the archive from **pbmakeremotetar**.

superdaemon Configuration

The superdaemons on the system must be configured for the Privilege Management for Unix and Linux daemon configuration. The Privilege Management for Unix and Linux installation performs this configuration automatically.

> ℹ️ *For more information about superdaemons, please see the documentation for your operating system.*

Policy Files for Policy Server Hosts

Policy files and their subfiles must be copied between policy server hosts so that all of the policy servers use the same policies.

Privilege Management for Unix and Linux, being an authentication tool and not a software distribution tool, does not automatically propagate policy files between policy server hosts. It is possible, and left as an exercise, to write procedures and policies that allow a central policy server host to propagate policy files to other policy server hosts.

Policy subfiles are copied if their name is specified as a constant. If the name is specified as a variable or string concatenation in the parent policy, then that policy is not copied by **pbmakeremotetar** and must be manually propagated to the target machines.

The policy subfile directory tree and directories referenced by the policies should be created to insure the multiple policy server hosts have the same directory tree.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

88

TC: 12/7/2022

Prefix and Suffix Installation Instructions

A prefixed or suffixed installation is performed by specifying the **-p** or **-s** arguments to **pbinstall** and **pbuninstall**, respectively. Both options take one argument: the prefix or suffix to be used.

With a prefix or suffix specified, or both, the names of all of the executable programs, services and ports, and default log file names are qualified with that prefix or suffix, or both.

Prefixes are always added to the beginning of the name. Suffixes, with the exception of the daemon error logs and man page file names, are added to the end of the name. Daemon error logs are named (for example) **{prefix}pbmasterd{suffix}.log**.

> **Note:** *You cannot use a prefixed or suffixed installation with Privilege Management package installations.*

If Privilege Management for Unix and Linux is installed with a prefix or suffix, execute **pbuninstall** using the same prefix or suffix. Failure to correctly specify the prefix or suffix to **pbuninstall** results in either **pbuninstall** failing or the uninstall of the incorrect copy of Privilege Management for Unix and Linux.

> **Note:** *The **pb.cfg** file is also prefixed or suffixed when it is created.*

> **i** *For more information, please see the following:*
> - *"Installation Programs" on page 212*
> - *"pbuninstall" on page 230*

Run Prefixed and Suffixed Installations

To run a prefix installation, type:

```
./pbinstall -p prefix
```

prefix is the prefix you are using.

To run a suffix installation, type:

```
./pbinstall -s suffix
```

suffix is the suffix you are using.

To run a prefix and suffix installation, type:

```
./pbinstall -p prefix -s suffix
```

prefix is the prefix and **suffix** is the suffix you are using.

Package Installer

The following sections detail how to install the server-side components of Privilege Management for Unix and Linux on Solaris, Linux, HPUX and AIX using the system native package installer.

Privilege Management for Unix and Linux has several separate component packages for each log server, run host, policy server, etc.

Starting with v9.0, the shared library component package and the **REST API** component package need to be installed prior to installation of policy server, GUI, run host, submit host and log server.

Solaris Package Installer

This section describes how to install Privilege Management for Unix and Linux using a package installer for Solaris 9 or 10 on an x86 or SPARC computer. Use the Solaris package installer if you want to do any of the following:

- Install Privilege Management for Unix and Linux using the Solaris Package Manager.
- Make the Privilege Management for Unix and Linux installation packages available on a JumpStart server to automate the installation of Solaris computers.

The Privilege Management for Unix and Linux Solaris package installer that is described here is not compatible with the BeyondTrust Privilege Management v5.x packages. If the Symark Privilege Management v5.x packages are installed, you must remove them before installing the Privilege Management for Unix and Linux Solaris packages.

Prerequisites

To use the Solaris package installer, you must have the following:

- Package tarball file for the appropriate Privilege Management for Unix and Linux flavor

Note: For the Solaris package installer, the tarball files are cumulative. That is, an update tarball file contains a complete Privilege Management for Unix and Linux installation. It is not necessary to install a baseline version of Privilege Management for Unix and Linux before installing an update.

- Root access or superuser privileges

Note: The Solaris package installer does not support prefix or suffix installations.

Plan Your Installation

When preparing to use the Solaris package installer, you should be familiar with the following concepts and restrictions:

- **Component packages:** A Privilege Management for Unix and Linux component package is a Solaris datastream (.ds) file that installs a portion of the Privilege Management for Unix and Linux application.

  The Privilege Management for Unix and Linux component packages are:

  - **BTPBlogh.ds:** Contains the log host, **pbsync**, and **pbsyncd**.
  - **BTPBlibs.ds:** Contains the shared libraries.
  - **BTPBrest.ds:** Contains the REST API files.
  - **BTPBrnsh.ds:** Contains Registry Name Service files.
  - **BTPBlich.ds:** Contains the license server files.
  - **BTPBmsth.ds:** Contains the policy server host, **pbsync**, and **pbsyncd**.
  - **BTPBsbmh.ds:** Contains the submit host andPrivilege Management for Unix and Linux shells.
  - **BTPBrunh.ds:** Contains the run host andPrivilege Management for Unix and Linux utilities.

Which component packages are required depends on the type of Privilege Management for Unix and Linux host you create, such as policy server host, log host, and so forth. You can select the types of Privilege Management for Unix and Linux hosts in the **pbinstall** installation menu, as shown in the following table.

Menu Selection	Required Components
Install everything here (demo mode)? = Yes	**BTPBmstr**
	BTPBrunh
	BTPBsbmh
	BTPBlogh
	BTPBguih
	BTPBlibs
Install Policy Server Host? = Yes	**BTPBmstr**
Install Run Host? = Yes	**BTPBrunh**
Install Submit Host? = Yes	**BTPBsbmh**
Install Log Host? = Yes	**BTPBlogh**
Install BeyondTrust built-in third-party libraries? = Yes	**BTPBlibs**
Install Registry Name Services Server? [yes]	**BTPBrnsh.ds**
Install License Server? [yes]	**BTPBlich.ds**

- **Configuration package:** Solaris installation package that is used to install the following files:

  - **pb.settings:** Hardcoded target location **/etc/pb.settings**

  - **pb.cfg:** Hardcoded target location **/etc/pb.cfg**

  - All the encryption keyfiles defined for **networkencryption**, **eventlogencryption**, **iologencryption**, **reportencryption**, **policyencryption**, and **restkeyencryption**

  - By default, two key files are created: **pb.key** and **pb.rest.key**

  - The sysadmin can define multiple encryption with different keyfiles in locations other than **/etc**. To upgrade and retain settings on the target machine, view all encryption settings in **/etc/pb.settings** and copy the files to the **settings_files** directory before running **"pbinstall -z" and pbcreate*cfgpkg**

  - **pb.conf** (for Policy Server hosts)

  - Man pages for the **pbinstall** and **pbcreatesolcfgpkg** programs

The Privilege Management for Unix and Linux configuration package is created by the **pbcreatesolcfgpkg** program. The component packages must be installed before you install the configuration package.

- **Response file: pbcreatesolcfgpkg** may also create a corresponding response file. The response file contains select information provided to **pbinstall** to customize objects contained within the prebuilt component package. For example, it ensures correct ownership of **pblighttpd** files. This file is created in the component package directory, **/unzip-dir/powerbroker/<version>/<flavor>/package** if it is accessible. If it is not, it is created in the current directory in the same location where the component package is created. Its name contains the same prefix supplied to **pbcreatesolcfgpkg**.

- **Package name:** Name of the installation package stored in the Solaris package manager database. For Privilege Management for Unix and Linux package installations, this name is the same as the package file name without the .ds extension.
- **Package administration file:** Contains alternative settings that control how Solaris packages are installed.
- **Relocated base directory:** The directory where the Privilege Management for Unix and Linux binary files and log files are installed. You can choose an alternative directory in which to install these files.
- **pbinstall program:** To create the Privilege Management for Unix and Linux settings files, you use the **pbinstall** program with the **-z** (settings only) option. **pbinstall -z** only creates the settings files and is incompatible with the following command line options:

Options Incompatible with pbinstall -z	Description
-b	Runs **pbinstall** in batch mode.
-c	Skip the steps that process or update the Privilege Management for Unix and Linux settings file.
-e	Runs install script automatically by bypassing the menu step of **pbinstall**.
-i	Ignores previous **pb.settings** and **pb.cfg** files.
-p	Sets the pb installation prefix.
-s	Sets the pb installation suffix.
-u	Install the utility programs.
-x	Creates a log synchronization host (that is, installs **pbsyncd**).

When you execute **pbinstall** with the **-z** option, you can see two menu items that are not otherwise available:

- **Enter existing pb.settings path:** Enables you to specify your own **pb.settings** file. **pbinstall** reads this settings file and populates the remaining menu choices. You can override some menu choices. If set to **none**, then **pbinstall** does not read a settings file. The remaining menu choices are populated with default values.
- **Enter directory path for settings file creation:** Enables you to specify an alternative output directory for the settings files. The default directory is **/unzip-dir/powerbroker/<version>/<flavor>/install/settings_files**, where **unzip-dir** is the directory where the package tarball file was unzipped.

The behavior of **pbinstall -z** depends on whether certain additional command line options are specified:

- If no other command line options are specified, **pbinstall** initially presents a short version of the installation menu (items 1–8 only). Depending on the choices you make in these items, further menu items become available.
- If command line options **-g**, **-l**, **-m**, **-o**, **-r**, or **-w** are specified, **pbinstall** presents an expanded version of the installation menu that reflects the host types that you are configuring.

When running **pbinstall** with the **-z** option, the following menu items are preprogrammed and cannot be changed:

- **Install man pages?**
- **Daemon location**
- **Administration programs location**
- **User programs location**
- **GUI library directory**
- **Policy include (sub) file directory**

- **User man page location**
- **Admin man page location**
- **Policy filename**
- **BeyondTrust built-in third-party library directory**

In addition, the values of the following menu items determine the values of other menu items:

Options Preset When Running pbinstall -z	
Setting this menu option to Yes	**Sets these values to Yes**
Install Policy Server Host?	Install Synchronization? Synchronization can be initiated from this host?
Install Run Host?	Install Utilities?
Install Submit Host?	Install PBSSH? Install pbksh? Install pbsh? Will this host use a Log Host?
Install Log Host?	Install Synchronization? Synchronization can be initiated from this host?

If you plan to use Registry Name Service and are running **pbinstall -z** on a client host (non-primary server), you must perform client registration. This is necessary to properly set up the registry name service database. Client registration also requires that you collect the following information from the Privilege Management for Unix and Linux primary server:

- REST Application ID
- REST Application Key
- Primary server network name or IP address
- Primary License Server REST TCP/IP port
- Registration Client Profile name

- **Registering client with Primary RNS:** If Registry Name Services is enabled for Privilege Management for Unix and Linux, each client host (after the first server installation) needs to be registered with the Primary Registry Name Server. When using package installers on a target host, a post-install configuration script (**/opt/pbul/scripts/pbrnscfg.sh**) is provided to be manually executed on that host to properly register it. This post-install configuration script will ask for information about the Primary Registry Name Server, including the Application ID (appid), Application Key (appkey), address/domain name, and the REST TCP/IP port number. This is the same information provided during the client registration part of a **pbinstall -z** install which generates the settings file.

If you prefer a more convenient method of registering RNS clients where the post-install configuration script is non-interactive, Privilege Management for Unix and Linux can save the relevant information in a hidden file during the settings-only run of pbinstall, bundle it with the configuration package, and automatically apply it to the target host when that package is installed. However, understand that this is not secure, but is available if the security-convenience trade-off is acceptable. To enable this, refer to the question regarding post-install configuration script displayed when running **pbinstall -z**.

ℹ️ *For more information, please see the following:*

- *"Relocate the Base Directory" on page 101*
- *If you use the package installer to install Privilege Management for Unix and Linux on a computer that already has an interactive Privilege Management for Unix and Linux installation on it, "Interactive Versus Packaged Installation" on page 9 for additional considerations*
- *For complete **pbinstall** command-line options, please see "Installation Programs" on page 212*

Choose a Package Administration File

We recommend that you use the package administration files that are provided by BeyondTrust (**BTPBadmin** and **BTPBadmin<suffix>**). These package administration files are configured to eliminate interactive prompts during package installation. If you want to use the Solaris default package administration file or other package administration file for your environment, you may be required to respond to prompts to install the packages.

> 📌 ***Note:*** *When installing a package using custom JumpStart, the installation process is required to be noninteractive.*

Use Privilege Management for Unix and Linux Packages on Solaris Zones

The Privilege Management for Unix and Linux Solaris package installer supports Solaris Zones in Solaris release 10. The primary operating system instance is referred to as the *global zone*. All zones that are not the global zone are referred to as *non-global zones*.

> 📌 ***Note:*** *Solaris release 10 is required. The use of Solaris Zones is not supported on earlier releases. There are three types of zones:*
> - ***Sparse root:*** *A sparse zone is the default zone configuration and is configurable. It shares the read-only global zone's /usr /lib /platform and /sbin partitions.*
> - ***Whole root:*** *A whole root zone does not share global zone partitions, which increases configuration flexibility.*
> - ***Branded:*** *A branded zone allows virtualization of Solaris 8, 9, or Linux and shares no partitions from the global zone. Branded zones are available as of Solaris 10 release 08/07 update 4.*

> 📌 ***Note:*** *Privilege Management for Unix and Linux Solaris Packages do not JumpStart to non-global zones. Using Custom JumpStart to install packages on Solaris 10 Zoned systems results in errors as the zones are not running during JumpStart execution.*

Installing Privilege Management for Unix and Linux Solaris Packages on Zones is very similar to installing these packages on Solaris systems without zones. However, keep the following considerations in mind:

- Privilege Management for Unix and Linux Solaris packages are designed to be installed from the global zone. Packages are propagated to the sparse and whole root zones upon global zone **pkgadd** and upon zone creation.
- Privilege Management for Unix and Linux Solaris packages are designed to be uninstalled from the global zone. Packages are removed from sparse and whole root zones upon the global zone **pkgrm**.
- Privilege Management for Unix and Linux Solaris packages can be installed in the global zone only, by using the **pkgadd -G** command. Privilege Management for Unix and Linux Solaris packages cannot be installed in sparse zones (with read-only partitions) and should instead be installed in the global zone. Although Privilege Management for Unix and Linux Solaris packages could be installed into a whole-root zone, Privilege Management for Unix and Linux Solaris packages are designed to be installed from the global zone. Packages installed on a whole-root zone are subject to overwriting by packages installed in the global zone.
- As Solaris branded zones are fully contained instances of Solaris 8 or 9, Privilege Management for Unix and Linux packages should be installed as with non-zoned Solaris instances. Loading packages to the global zone does not update a branded zone. Privilege Management for Unix and Linux Solaris packages for Solaris branded zones running Linux are not supported.
- The Privilege Management for Unix and Linux Solaris configuration package must be removed before removing any Privilege Management for Unix and Linux component packages and must be removed individually. Privilege Management for Unix and Linux Solaris component packages may be removed simultaneously.

Overview of Steps

Using the Privilege Management for Unix and Linux Solaris package installer involves the following steps:

1. Unpack the Privilege Management for Unix and Linux package tarball file.
2. Use the **pbinstall** program to create Privilege Management for Unix and Linux settings files.
3. Use the **pbcreatesolcfgpkg** program to create the Privilege Management for Unix and Linux configuration package along with a corresponding response file used for additional customization.
4. Perform a package installation using the Solaris **pkgadd** command for any required components.
5. Perform a package installation using the Solaris **pkgadd** command for the Privilege Management for Unix and Linux configuration package.
6. If Registry Name Service is enabled and installed on a non-primary server, run **/opt/pbul/scripts/pbrnscfg.sh** to register the host.

ℹ️ *For more detail on the steps above, please see* .

TC: 12/7/2022

Installation Procedure

> 📌 **Note:** *Before installing Solaris packages, if the directories where files are installed, **/usr/local**, **/usr/bin** etc., are symbolic links to other directories, then set the environment variable **PKG_NONABI_SYMLINKS** to true:*
>
> ```
> # PKG_NONABI_SYMLINKS=true
> # export PKG_NONABI_SYMLINKS
> ```
>
> *This prevents the symbolic links from being removed by the **pkgadd** command on Solaris.*

To install Privilege Management for Unix and Linux using the Solaris Package Manager, do the following:

1. Extract the package tarball files into the **/opt/beyondtrust/** directory by executing the following command:

   ```
   gunzip -c pmul<flavor_version>_pkg.tar.Z | tar xvf -
   ```

2. Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/install/** directory.
3. Execute the following command:

   ```
   ./pbinstall -z
   ```

   You can include other options with the **-z** option. Use the **-R** option if you want to specify an alternate base directory for installing the component packages.

   You are asked if you want to use client registration. If you plan to enable Registry Name Service, and are installing on a host that is not designated as a primary server, you must run client registration.

   pbinstall then asks if you want to enable Registry Name Service.

   pbinstall displays the Privilege Management for Unix and Linux installation menu.

4. Make your menu selections.

   When the menu selection process is complete, **pbinstall** creates the following files in the specified location:

   - **pb.settings**
   - **pb.cfg**
   - **pb.key** (if encryption is enabled)
   - **pb.conf** (for Policy Server host)

> 📌 **Note:** *The **Enter existing pb.settings path** menu option enables you to specify your own **pb.settings** file to use. Also, the **Enter directory path for settings file creation** menu option enables you to specify where to save the generated settings files. These menu options are available only when running **pbinstall** with the **-z** option.*

5. Optional. For a Privilege Management for Unix and Linux client, if client-server communications are to be encrypted, replace the generated **pb.key** file with the **pb.key** file from the policy server host. Also, copy any other required key files into the same directory.

SALES: www.beyondtrust.com/contact   SUPPORT: www.beyondtrust.com/support   DOCUMENTATION: www.beyondtrust.com/docs

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

97

TC: 12/7/2022

6. Optional. For a policy server host, write a policy file (**pb.conf**) and place it in the directory with the other generated files. If you do not provide a **pb.conf** file, a **pb.conf** file with the single command **reject;** is generated and packaged.

   Starting with v8.0, **pbinstall -z** can optionally install the default role-based policies and asks:

   ```
   Installing default role-based policy pbul_policy.conf and pbul_functions.conf in <install_
   dir>/settings_files
   Would you like to use the default role-based policy in the configuration package?
   ```

   - Answer **Yes** for new installs only.
   - If you are upgrading an existing configuration package, to avoid overwriting your existing policy, answer **No**.

   ```
   Use the default role-based policy [Y]?
   ```

   - If you answer **Yes**, the default **pb.conf**, **pbul_policy.conf** and **pbul_functions.conf** are created and installed on the policy server.
   - If you are installing over an existing installation, and have an existing policy in place, answer **No**.

7. Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/install/** directory.

8. Run the **pbcreatesolcfgpkg** utility by typing:

   ```
   pbcreatesolcfgpkg -p suffix -s directory
   ```

   - **suffix** is appended to the filenames of the configuration package datastream file and the package administration file; length can be up to 26 characters (3 characters for unpatched Solaris 8).
   - **directory** contains the Privilege Management for Unix and Linux settings and configuration files to include in the package.

   The **pbcreatesolcfgpkg** utility creates the following files:

   - Configuration package file **BTPBcf<suffix>.ds**
   - Package administration file **BTPBadmin<suffix>**
   - Response file **BTPB<suffix>.resp**

9. Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/package/** directory.

10. Optional. To install Privilege Management for Unix and Linux in an alternative base directory, edit the provided **BTPBadmin** file and change the **basedir=default** entry as follows:

    ```
    basedir=target_base_directory
    ```

    target_base_directory is the absolute path of the target base directory.

11. For each required component package, run the Solaris **pkgadd** utility to install the component package by typing:

    ```
    pkgadd -a BTPBadmin -r response-file  -d pkg-datastream-file pkg-name
    ```

    pkg-datastream-file is the name of the component package datastream **(.ds) file**. **response-file** is the location and name of the response file, if generated, and **pkg-name** is the name of the package. For Privilege Management for Unix and Linux packages, the package name is the same as the datastream file name without the .ds extension.

> **Example:**
>
> ```
> pkgadd -a BTPBadmin -r ./BTPB<suffix>.resp -d BTPBrunh.ds BTPBrunh
> ```
>
> *If no response file is generated (not applicable):*
>
> ```
> pkgadd -a BTPBadmin -d BTPBrunh.ds BTPBrunh
> ```

12. Run the Solaris **pkgadd** utility to install the Privilege Management for Unix and Linux configuration package by typing:

```
pkgadd -a BTPBadmin<suffix> -d BTPBcf<suffix>.ds BTPBcf<suffix>
```

<suffix> is the suffix specified when the Privilege Management for Unix and Linux configuration package is created in step 8.

13. Verify the installation of the packages with the Solaris **pkginfo** utility by typing:

```
pkginfo | grep BTPB
```

14. If Registry Name Service is enabled and installed on a non-primary server, register the host with the Primary Registry Name Server using a post-install configuration script. Gather the Application ID, Application Key, network name or IP address, and REST TCP/IP port of the primary server, then run the script to register the host and follow the prompts:

```
/opt/pbul/scripts/pbrnscfg.sh
```

> **Note:** *If you install Privilege Management for Unix and Linux using a custom JumpStart session, the Privilege Management for Unix and Linux configuration package should be added or removed only once per session to avoid installing conflicting rc scripts.*

> *For more information, please see the following:*
>
> - *For other options you can use with the pbinstall **-z** option, "Plan Your Installation" on page 91*
> - *"pblighttpd" on page 228*
> - *"pbcreatesolcfgpkg" on page 227*

Remove Privilege Management for Unix and Linux Packages

Removing the Privilege Management for Unix and Linux packages completely uninstalls Privilege Management for Unix and Linux from a computer. To remove the Privilege Management for Unix and Linux packages, do the following:

1. Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/install/** directory.

2. Remove the Privilege Management for Unix and Linux packages by typing:

```
pkgrm -na ./BTPBadmin config-package-name component-package-1 ... component-package-n
```

- **BTPBadmin** is the package administration file that is supplied by BeyondTrust. You can specify a different package administration file, or leave out the **-a** option to use the default package administration file. The **BTPBadmin** package administration file is designed to make the package installation and removal processes run noninteractively.

- **config-package-name** is the name of the package specified when the configuration package is installed. Because of the dependency relationship between the configuration package and the component packages, this package name must come first in the list.

- **component-package-1** through **component-package-n** are the names of the packages specified when the component packages are installed.

Relocate the Base Directory

The Solaris package management system enables you specify an alternative base directory for package installation. With this feature, you can specify a directory to install the Privilege Management for Unix and Linux binary files and log files in. Certain files, such as **pb.settings**, **pb.cfg**, and Privilege Management for Unix and Linux key files, must be located in the **/etc** directory for Privilege Management for Unix and Linux to run. These files are not relocatable. To relocate the base directory from the default / (root) directory, do the following:

1. On the target machine, create the target base directory if it does not already exist.

2. When you run **pbinstall**, use the **-R** option and specify the new base directory.

3. Before installing the Privilege Management for Unix and Linux component packages, edit the provided **BTPBadmin** package administration file and change the **basedir** entry to refer to the new base directory.

    Change the **basedir=default** entry as follows:

    ```
    basedir=target_base_directory
    ```

    target_base_directory is the absolute path of the target base directory.

4. When you install the component packages, execute **pkgadd** with the **-a** option and use the **BTPBadmin** package administration file.

    For each required component package, run the Solaris **pkgadd** utility to install the component package by typing:

    ```
    pkgadd -a BTPBadmin -r response-file  -d pkg-datastream-file pkg-name
    ```

    pkg-datastream-file is the name of the component package datastream **(.ds) file**. **response-file** is the location and name of the response file, if generated, and **pkg-name** is the name of the package. For Privilege Management for Unix and Linux packages, the package name is the same as the datastream file name without the .ds extension.

Example:

```
pkgadd -a BTPBadmin -r ./BTPB<suffix>.resp -d BTPBrunh.ds BTPBrunh
```

If no response file is generated (not applicable):

```
pkgadd -a BTPBadmin -d BTPBrunh.ds BTPBrunh
```

Update Privilege Management for Unix and Linux with the Solaris Package Installer

The Privilege Management for Unix and Linux Solaris package installer can be used to update an existing Privilege Management for Unix and Linux installation to a new version. The existing Privilege Management for Unix and Linux version should have been installed with the Privilege Management for Unix and Linux package installer.

> 📌 **Note:** *It is possible to use the Solaris package installer to install Privilege Management for Unix and Linux over an existing version that was installed with **pbinstall**. However, doing so is not recommended because it can result in unused files from the existing version remaining in the file system.*

Package Update Considerations

Installing a Privilege Management for Unix and Linux update with the Solaris package installer is similar to using the Solaris package installer to install Privilege Management for Unix and Linux for the first time. Keep these considerations in mind when you prepare to update Privilege Management for Unix and Linux:

- Technically, the Privilege Management for Unix and Linux Solaris packages are update packages, as opposed to upgrade packages. An update package overwrites the existing files before registering the new version number in the Solaris Package Manager database.
- A Privilege Management for Unix and Linux Solaris update package contains a complete Privilege Management for Unix and Linux installation, not just the files that have changed since the previous release.
- The Privilege Management for Unix and Linux Solaris update packages are compatible with JumpStart.
- If you have more than one Privilege Management for Unix and Linux package on a computer, you should update all packages on that computer.
- A newer release can introduce features that use new settings or configurations. In which case, an upgrade of the configuration package of Privilege Management for Unix and Linux is also needed.
- Unlike Privilege Management for Unix and Linux patches that are installed with **pbpatchinstall**, update packages cannot be rolled back to a previous release. However, you can install an older package over a newer one, effectively rolling back to the older release.

Package Update Procedure

Follow this procedure to update your installation of Privilege Management for Unix and Linux using the Solaris package installer:

1. Obtain the tarball file for the Solaris update packages that are appropriate for your hardware. The tarball file name has the format **pmul<flavor>-v.v.r-b-pn_pkg.tar.Z**, where:
   - **<flavor>** indicates the operating system and hardware architecture.
   - **v.v.r** is the major and minor version number and the release number.
   - **b** is the build number.
   - **n** is the update number.
2. Extract the package tarball files into the **/unzip-dir/** directory of the computer that you are updating by executing the following command:

```
gunzip -c pmul<flavor_version>_pkg.tar.Z | tar xvf -
```

3. Navigate to the **/unzip-dir/powerbroker/<version>/<flavor>/install/** directory.
4. Create the **settings_files** directory and change directory to that location.
5. To retain or correctly update the settings of the current installation, copy the following files from the target installation host into the settings_files directory you created in step 4:

- /etc/pb.settings
- /etc/pb.cfg
- encryption keys defined in pb.settings for networkencryption, eventlogencryption, iologencryption, reportencryption, policyencryption, and restkeyencryption settings (if enabled)

> 📌 **Note:** In a default installation, there are typically 2 key files created: **pb.key** and **pb.rest.key**.

- policy file defined in **policyfile** setting in **pb.settings** (if the target installation is a Policy Server)

> 📌 **Note:** In a default installation, the policy file is located in **/opt/pbul/policies/pb.conf**.

6. Execute the following command and verify the installation settings:

```
./pbinstall -z
```

7. Create the upgrade configuration package by running the **pbcreatesolcfgpkg** utility:

```
pbcreatesolcfgpkg -p suffix
```

Use the current suffix of the installation to be upgraded. Use the suffix you provided in the initial package installation in step 8 of the **Installation Procedure**.

Another way to find the suffix is to run the following command on the target installation host to get the list of packages installed:

```
pkginfo -x | grep BTPB
```

Identify the suffix of the Privilege Management for Unix and Linux configuration package using this format:

```
BTPBcf<suffix>
```

8. Navigate to the **/unzip-dir/powerbroker/<version>/<flavor>/package/** directory.
9. Optional. To install Privilege Management for Unix and Linux in an alternative base directory, edit the provided **BTPBadmin** file and change the **basedir=default** entry as follows:

```
basedir=target_base_directory
```

target_base_directory is the absolute path of the target base directory.

10. For each required component package, run the Solaris **pkgadd** utility to install the component package by typing:

```
pkgadd -a BTPBadmin -r response-file -d pkg-datastream-file pkg-name
```

pkg-datastream-file is the name of the component package datastream (.ds) file. response-file is the location and name of the response file, if generated, and pkg-name is the name of the package. For Privilege Management for Unix and Linux packages, the package name is the same as the datastream file name without the .ds extension.

> *Example:*
>
> ```
> pkgadd -a BTPBadmin -r ./BTPB<suffix>.resp -d BTPBrunh.ds BTPBrunh
> ```
>
> *If no response file is generated (not applicable):*
>
> ```
> pkgadd -a BTPBadmin -d BTPBrunh.ds BTPBrunh
> ```

11. Navigate to the **/unzip-dir/powerbroker/<version>/<flavor>/install/** directory.

12. Run the Solaris **pkgadd** utility to install the Privilege Management for Unix and Linux configuration package by typing:

```
pkgadd -a BTPBadmin<suffix> -d BTPBcf<suffix>.ds BTPBcf<suffix>
```

<suffix> is the suffix specified when the Privilege Management for Unix and Linux configuration package is created in step 7.

13. Verify the installation of the packages with the Solaris **pkginfo** utility by typing:

```
pkginfo -x | grep BTPB
```

Upgrade the Configuration Package

When upgrading the configuration package (cfg pkg), some settings that are part of the package might need settings and configuration files copied from the existing installation to the staging host.

Files included in the cfg package:

- **pb.settings:** Hardcoded target location **/etc/pb.settings**.
- **pb.cfg:** Hardcoded target location **/etc/pb.cfg**.
- All the encryption key files defined for networkencryption, eventlogencryption, iologencryption, reportencryption, policyencryption, and restkeyencryption. By default, two key files are typically created:
  - **pb.key**
  - **pb.rest.key**

  The sysadmin can define encryption with different key files in locations other than **/etc**. Therefore, when upgrading, and to retain what is installed on the target machine, look at all the encryption settings in **/etc/pb.settings**. Copy the settings to the **settings_files** directory before running **pbinstall -z** and **pbcreate*cfgpkg**.

- Policy file if the target is a policy server.

Sample Execution for the Solaris Package Installer

The sample execution shows the installation of a Privilege Management for Unix and Linux submit host, run host, and shared libraries using the Privilege Management for Unix and Linux Solaris package installer.

This sample execution is divided into the following parts:

- Generate the Privilege Management for Unix and Linux settings files.
- Create the Privilege Management for Unix and Linux configuration package using the **pbcreatesolcfgpkg** program.
- Install the component packages using the **pkgadd** command.
- Install the configuration package using the **pkgadd** command.

Generate the Privilege Management for Unix and Linux Settings Files

This section of the execution shows the generation of the Privilege Management for Unix and Linux settings files (**pb.key**, **pb.cfg**, and **pb.settings**) and also displays the Privilege Management for Unix and Linux installation menu. This output was generated using the **pbinstall** program with the options: **-z**, **-l**, and **-r**.

> 🔍 ***Example:***
>
> ```
> # ./pbinstall -z -l -r
> Starting pbinstall main() from /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
> 18/install/.
> solaris9-10.x86
> WARNING:When creating configuration packages to be installed on Solaris Zones, care must
> be taken to set log file directories to Zone-writable partitions.
> The default Solaris sparse zone has the following read-only and/or shared partitions,
> although configuration can vary:
> /usr /lib /platform /sbin
> The Privilege Management for Unix and Linux log file default directory for Solaris Zones
> is '/var/adm'.
>
> Privilege Management for Unix and Linux Settings File Generation
>
> Please read thePrivilege Management for Unix and Linux Installation Instructions before
> proceeding.
>
> Checking MANIFEST against release directory
>
> Press return to continue
>
> The Registry Name Service of Privilege Management for Unix and Linux facilitates location
> of other services within the PMUL enterprise with the aid of a centralized data
> repository.
> IMPORTANT: client registration is required if this is not the Primary Server and you
> intend to use Registry Name Services.
> Do you wish to utilize Registry Name Service? [yes]? no
> BeyondTrust Privilege Management for Unix and Linux Installation Menu
>         Opt  Description                              [Value]
>         1  Install Everything Here (Demo Mode)?        [no]
> ```

```
 2  Install License Server?                   [no]
 3  Install Registry Name Services Server?    [no]
 4  Install Client Registration Server?       [no]
 7  Install Submit Host?                       [yes]
 8  Install PBSSH                              [yes]
10  Install Log Host?                          [yes]
11  Enable Logfile Tracking and Archiving?    [yes]
12  Is this a Log Archiver Storage Server?    [no]
13  Is this a Log Archiver Database Server?   [no]
14  Install File Integrity Monitoring Polic... [no]
15  Install REST Services?                    [yes]
16  List of License Servers                   [*]
19  Path to Password Safe 'pkrun' binary      []
23  Install Synchronization program?          [yes]
25  Install Secure GUI Host?                  [yes]
26  Install Utilities: pbvi, pbnvi, pbmg, p... [yes]
27  Install pbksh?                            [yes]
28  Install pbsh?                             [yes]
29  Install man pages?                        [no]
30  Will this host use a Log Host?            [yes]
31  AD Bridge Integration?                    [no]
37  Integration with BeyondInsight?           [no]
55  Synchronization program can be initiate... [yes]
56  Daemons location                          [/usr/sbin]
57  Number of reserved spaces for submit pr... [80]
58  Administration programs location          [/usr/sbin]
59  User programs location                    [/usr/local/bin]
60  GUI library directory                     [/usr/local/lib/pbbuilder]
61  Policy include (sub) file directory       [/opt/pbul/policies]
62  Policy file name                          [/opt/pbul/policies/pb.conf]
65  Log Archive Storage Server name           []
67  Log Archiver Database Server name         []
69  Logfile Name Cache Database file path?    [/opt/pbul/dbs/pblogcache.db]
70  REST Service installation directory?      [/usr/lib/beyondtrust/pb/rest]
71  Install REST API sample code?             [no]
73  Pblighttpd user                          [pblight]
75  Pblighttpd user UID                       []
76  Pblighttpd user GID                       []
78  Configure systemd?                        [yes]
79  Command line options for pbmasterd        [-ar]
80  Policy Server Delay                       [500]
81  Policy Server Protocol Timeout            [-1]
82  pbmasterd diagnostic log                  [/var/log/pbmasterd.log]
83  Eventlog filename                         [/var/log/pb.eventlog]
84  Configure eventlog rotation via size?     []
85  Configure eventlog rotation path?         []
86  Configure eventlog rotation via cron?     [no]
87  Validate Submit Host Connections?         [no]
88  List of Policy Servers to submit to       [kandor]
89  pbrun diagnostic log?                     [none]
90  pbssh diagnostic log?                     [none]
91  Allow Local Mode?                         [yes]
```

```
92   Additional secured task checks?         [no]
93   Suppress Policy Server host failover er... [yes]
94   List of Policy Servers to accept from    [kandor]
95   pblocald diagnostic log                  [/var/log/pblocald.log]
96   Command line options for pblocald        []
97   Syslog pblocald sessions?                [no]
98   Record PTY sessions in utmp/utmpx?       [yes]
99   Validate Policy Server Host Connections? [no]
100  List of Log Hosts                        [kandor]
101  Command line options for pblogd          []
102  Log Host Delay                           [500]
103  Log Host Protocol Timeout                [-1]
104  pblogd diagnostic log                    [/var/log/pblogd.log]
105  List of log reserved filesystems         [none]
106  Number of free blocks per log system fi... [0]
107  Command line options for pbsyncd         []
108  Sync Protocol Timeout                    [-1]
109  pbsyncd diagnostic log                   [/var/log/pbsyncd.log]
110  pbsync diagnostic log                    [/var/log/pbsync.log]
111  pbsync sychronization time interval (in... [15]
112  Add installed shells to /etc/shells      [no]
113  pbksh diagnostic file                    [/var/log/pbksh.log]
114  pbsh diagnostic file                     [/var/log/pbsh.log]
115  Stand-alone pblocald command             [none]
116  Stand-alone root shell default iolog     [/pbshell.iolog]




121  Use syslog?                              [yes]
122  Syslog facility to use?                  [LOG_AUTHPRIV]
123  Base Daemon port number                  [24345]
124  pbmasterd port number                    [24345]
125  pblocald port number                     [24346]
126  pblogd port number                       [24347]


129  pbsyncd port number                      [24350]
130  REST Service port number                 [24351]
131  Add entries to '/etc/services'           [yes]
132  Allow non-reserved port connections      [yes]
133  Inbound Port range                       [1025-65535]
134  Outbound Port range                      [1025-65535]
137  Network encryption options               [aes-256:keyfile=/etc/pb.key]
138  Event log encryption options             [none]
139  I/O log encryption options               [none]
140  Report encryption options                [none]
141  Policy file encryption options           [none]
142  Settings file encryption type            [none]
143  REST API encryption options              [aes-256:keyfile=/etc/pb.re...]
144  Configure with Kerberos v5?              [no]
150  Enforce High Security Encryption?        [yes]
```

```
        151  Use SSL?                                    [yes]
        152  SSL Configuration?                          [requiressl]
        153  SSL pbrun Certificate Authority Directory?  [none]
        154  SSL pbrun Certificate Authority File?       [none]
        155  SSL pbrun Cipher List?                      [HIGH:!SSLv2:!3DES:!MD5:@ST…]
        156  SSL pbrun Certificate Directory?            [none]
        157  SSL pbrun Certificate File?                 [none]
        158  SSL pbrun Private Key Directory?            [none]
        159  SSL pbrun Private Key File?                 [none]
        160  SSL pbrun Certificate Subject Checks?       [none]
        161  SSL Server Certificate Authority Direct...  [none]
        162  SSL Server Certificate Authority File?      [none]
        163  SSL Server Cipher List?                     [HIGH:!SSLv2:!3DES:!MD5:@ST...]
        164  SSL Server Certificate Directory?           [none]
        165  SSL Server Certificate File?                [/etc/pbssl.pem]
        166  SSL Server Private Key Directory?           [none]
        167  SSL Server Private Key File?                [/etc/pbssl.pem]
        168  SSL Server Certificate Subject Checks?      [none]
        169  SSL Certificate Country Code                [US]
        170  SSL Certificate State/Province              [AZ]
        171  SSL Certificate Location (Town/City)        [Phoenix]
        172  SSL Certificate Organizational Unit/Dep...  [Security]
        173  SSL Certificate Organization                [BeyondTrust]
        174  Configure Privilege Management for Unix...  [no]
        175  Install BeyondTrust built-in third-part...  [yes]
        176  BeyondTrust built-in third-party librar...  [/usr/lib/beyondtrust/pb]
        188  Use PAM?                                    [no]
        196  Allow Remote Jobs?                          [yes]
        197  UNIX Domain Socket directory                [none]
        198  Reject Null Passwords?                      [no]
        199  Enable TCP keepalives?                      [no]
        200  Name Resolution Timeout                     [0]
        N for the next menu page, P for the previous menu page, C to continue, X to exit
        Please enter a menu option [For technical support call 1-800-234-9072]> c


Generating key file /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/settings_files/pb.key...

Are all the installation settings correct [yes]?
Generating config file /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/settings_files/pb.cfg
Creating the settings file creation script
Backed up existing settings file creation script to:
'/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/pbcreatesettingsfile.ctime.May_26_11:01'
Running settings file creation script
Creating settings file /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/settings_files/pb.settings
Generated settings files are in directory: /opt/acpkg/powerbroker/v9.4/pmul_solaris9-
10.x86_9.4.3-18/install/settings_files
Privilege Management for Unix and Linux Settings File Generation completed successfully.
```

Create the Privilege Management for Unix and Linux Configuration Package Using pbcreatesolcfgpkg

This section shows the creation of the Privilege Management for Unix and Linux configuration package using the **pbcreatesolcfgpkg** program with the **-p** and **-s** options.

> *Note: At the end of its output, the **pbcreatesolcfgpkg** script shows which Privilege Management for Unix and Linux component packages need to be installed.*

Example:

```
# cd /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-18/install
# ./pbcreatesolcfgpkg -p CLIENT1 -s /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_
9.4.3-18/install/settings_files
pbcreatesolcfgpkg: starting from /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install

Warning: Unpatched Solaris 8 has a 9 character package name limitation!
The package name created 'BTPBcfCLIENT1' is 13 characters...

pbcreatesolcfgpkg: keyfile pb.key will be included in package
Reading /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-18/install/settings_
files/pb.cfg
## Building pkgmap from package prototype file.
## Processing pkginfo file.
## Attempting to volumize 15 entries in pkgmap.
part  1 -- 637 blocks, 24 entries
## Packaging one part.
/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/pkgmap
/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/pkginfo
/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/root/etc/init.d/sypbcfg_svcsinetdsmf
/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/root/etc/pb.cfg
/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/root/etc/pb.key
/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/root/etc/pb.settings
/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/root/etc/rc2.d/S99sypbcfg_pbpatton
/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/root/var/adm/pbksh.log
/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/root/var/adm/pblocald.log
/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/root/var/adm/pbsh.log
/opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
```

```
         18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/install/checkinstall
         /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
         18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/install/copyright
         /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
         18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/install/depend
         /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
         18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/install/postinstall
         /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
         18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/install/postremove
         /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
         18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/install/preinstall
         /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-
         18/install/BTPBcfCLIENT1/BTPBcfCLIENT1/install/preremove
         ## Validating control scripts.
         ## Packaging complete.
         pbcreatesolcfgpkg: created package BTPBcfCLIENT1 in /opt/acpkg/powerbroker/v9.4/pmul_
         solaris9-10.x86_9.4.3-18/install/BTPBcfCLIENT1
         Checking uninstalled directory format package <BTPBcfCLIENT1> from
         </opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-18/install/BTPBcfCLIENT1>
         ## Checking control scripts.
         ## Checking package objects.
         ## Checking is complete.
         pbcreatesolcfgpkg: pkgchk for spooled package BTPBcfCLIENT1 succeeded.
         Transferring <BTPBcfCLIENT1> package instance
         pbcreatesolcfgpkg: pkgtrans for package BTPBcfCLIENT1 succeeded.
         Checking uninstalled stream format package <BTPBcfCLIENT1> from
         </opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-18/install/BTPBcfCLIENT1.ds>
         ## Checking control scripts.
         ## Checking package objects.
         ## Checking is complete.
         rm: Cannot remove any directory in the path of the current working directory
         /var/tmp/aaaJEaG90/BTPBcfCLIENT1
         pbcreatesolcfgpkg: pkgchk for datastream package BTPBcfCLIENT1 succeeded.
         pbcreatesolcfgpkg: spooled package BTPBcfCLIENT1 removed.

         pbcreatesolcfgpkg: package datastream file is: /opt/acpkg/powerbroker/v9.4/pmul_solaris9-
         10.x86_9.4.3-18/install/BTPBcfCLIENT1.ds
         pbcreatesolcfgpkg: package admin file is: /opt/acpkg/powerbroker/v9.4/pmul_solaris9-
         10.x86_9.4.3-18/install/BTPBadminCLIENT1

         pbcreatesolcfgpkg: the following packages will need to be loaded to the target system:
         BTPBrunh BTPBsbmh BTPBlibs

         pbcreatesolcfgpkg: completed.
```

Install Component Packages Using the pkgadd Command

This section shows the execution of the **pkgadd** command to install component packages for the submit host, run host, and shared libraries. The execution text also includes copyright, trademark, trade secrets, and other legal text; however, those notices and text were removed from the following excerpt to save space:

Example:

```
# cd /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-18/package
# ls
BTPBadmin    BTPBguih.ds  BTPBlibs.ds  BTPBlogh.ds  BTPBmsth.ds  BTPBrest.ds  BTPBrnsh.ds
 BTPBrunh.ds  BTPBsbmh.ds
# pkgadd -a BTPBadmin -d BTPBlibs.ds BTPBlibs
Processing package instance <BTPBlibs> from </opt/acpkg/powerbroker/v9.4/ppmul_solaris9-
10.x86_9.4.3-18/package/BTPBlibs.ds>
BeyondTrust PowerBroker Shared Libraries - Root Delegation and Privilege Management
(x86) 9.4.3-18
## Executing checkinstall script.
Using /> as the package base directory.
## Processing package information.
## Processing system information.
## Verifying package dependencies.
## Verifying disk space requirements.
Installing BeyondTrust PowerBroker Shared Libraries - Root Delegation and Privilege
Management as <BTPBlibs>
        ## Executing preinstall script.
        ## Installing part 1 of 1.
        /usr/lib/beyondtrust/pb/libcom_err.so <symbolic link>
        /usr/lib/beyondtrust/pb/libcom_err.so.3 <symbolic link>
        /usr/lib/beyondtrust/pb/libcom_err.so.3.0
        /usr/lib/beyondtrust/pb/libcrypto.so <symbolic link>
        /usr/lib/beyondtrust/pb/libcrypto.so.1 <symbolic link>
        /usr/lib/beyondtrust/pb/libcrypto.so.1.0.0
        /usr/lib/beyondtrust/pb/libcurl.so <symbolic link>
        /usr/lib/beyondtrust/pb/libcurl.so.4 <symbolic link>
        /usr/lib/beyondtrust/pb/libcurl.so.4.3.0
        /usr/lib/beyondtrust/pb/libgssapi_krb5.so <symbolic link>
        /usr/lib/beyondtrust/pb/libgssapi_krb5.so.2 <symbolic link>
        /usr/lib/beyondtrust/pb/libgssapi_krb5.so.2.2
        /usr/lib/beyondtrust/pb/libk5crypto.so <symbolic link>
        /usr/lib/beyondtrust/pb/libk5crypto.so.3 <symbolic link>
        /usr/lib/beyondtrust/pb/libk5crypto.so.3.1
        /usr/lib/beyondtrust/pb/libkrb5.so <symbolic link>
        /usr/lib/beyondtrust/pb/libkrb5.so.3 <symbolic link>
        /usr/lib/beyondtrust/pb/libkrb5.so.3.3
        /usr/lib/beyondtrust/pb/libkrb5support.so <symbolic link>
        /usr/lib/beyondtrust/pb/libkrb5support.so.0 <symbolic link>
        /usr/lib/beyondtrust/pb/libkrb5support.so.0.1
        /usr/lib/beyondtrust/pb/liblber-2.4.so <symbolic link>
        /usr/lib/beyondtrust/pb/liblber-2.4.so.2 <symbolic link>
        /usr/lib/beyondtrust/pb/liblber-2.4.so.2.10.3
        /usr/lib/beyondtrust/pb/libLDAP-2.4.so <symbolic link>
        /usr/lib/beyondtrust/pb/libLDAP-2.4.so.2 <symbolic link>
        /usr/lib/beyondtrust/pb/libLDAP-2.4.so.2.10.3
        /usr/lib/beyondtrust/pb/libssl.so <symbolic link>
        /usr/lib/beyondtrust/pb/libssl.so.1 <symbolic link>
        /usr/lib/beyondtrust/pb/libssl.so.1.0.0
        /usr/lib/beyondtrust/pb/pam_radius_auth.so <symbolic link>
        /usr/lib/beyondtrust/pb/pam_radius_auth.so.1 <symbolic link>
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

111

```
            /usr/lib/beyondtrust/pb/pam_radius_auth.so.1.3.17
            [ verifying class <none> ]
## Executing postinstall script.
            Checking installation of package: BTPBlibs
Installation of <BTPBlibs> was successful.# pkgadd -a BTPBadmin -d  BTPBsbmh.ds BTPBsbmh
Processing package instance <BTPBsbmh> from </opt/acpkg/powerbroker/v9.4/pmul_solaris9-
10.x86_9.4.3-18/package/BTPBsbmh.ds>
BeyondTrust PowerBroker Submit Host - Root Delegation and Privilege Management
            (x86) 9.4.3-18
            ## Executing checkinstall script.
            Using /> as the package base directory.
            ## Processing package information.
            ## Processing system information.
            1 package pathname is already properly installed.
            ## Verifying package dependencies.
            ## Verifying disk space requirements.
            Installing BeyondTrust PowerBroker Submit Host - Root Delegation and Privilege
Management as <BTPBsbmh>
            ## Executing preinstall script.
            ## Installing part 1 of 1.
            /opt/pbul/scripts/pbrnscfg.sh
            /usr/lib/secure/64/libpbul_aca-elf64.so
            /usr/lib/secure/libpbul_aca-elf32.so
            /usr/local/bin/pbbench
            /usr/local/bin/pbcall
            /usr/local/bin/pbksh
            /usr/local/bin/pbrun
            /usr/local/bin/pbrunssh
            /usr/local/bin/pbsh
            /usr/local/bin/pbssh
            /usr/local/man/man1/pbbench.1
            /usr/local/man/man1/pbrun.1
            /usr/local/man/man1/pbssh.1
            /usr/local/man/man8/pbclienthost_uuid.8
            /usr/local/man/man8/pbcreatesolcfgpkg.8
            /usr/local/man/man8/pbdbutil.8
            /usr/local/man/man8/pbencode.8
            /usr/local/man/man8/pbinstall.8
            /usr/local/man/man8/pbregister.8
            /usr/local/man/man8/pbsum.8
            /usr/local/man/man8/pbulpreinstall.sh.8
            /usr/local/man/man8/pbversion.8
            /usr/sbin/pbclienthost_uuid
            /usr/sbin/pbdbutil
            /usr/sbin/pbencode
            /usr/sbin/pbregister
            /usr/sbin/pbsnapshot.sh
            /usr/sbin/pbsum
            /usr/sbin/pbulpreinstall.sh
            /usr/sbin/pbversion
            [ verifying class <none> ]
            ## Executing postinstall script.
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

112

TC: 12/7/2022

```
            Checking installation of package: BTPBsbmh
Installation of <BTPBsbmh> was successful.
# pkgadd -a BTPBadmin -d BTPBrunh.ds BTPBrunh
Processing package instance <BTPBrunh> from </opt/acpkg/powerbroker/v9.4/pmul_solaris9-
10.x86_9.4.3-18/package/BTPBrunh.ds>
BeyondTrust PowerBroker Run Host - Root Delegation and Privilege Management
(x86) 9.4.3-18
## Executing checkinstall script.
Using /> as the package base directory.
        ## Processing package information.
        ## Processing system information.
        25 package pathnames are already properly installed.
        ## Verifying package dependencies.
        ## Verifying disk space requirements.
        Installing BeyondTrust PowerBroker Run Host - Root Delegation and Privilege
Management as <BTPBrunh>
        ## Executing preinstall script.
        ## Installing part 1 of 1.
        /usr/local/bin/pbless
        /usr/local/bin/pbmg
        /usr/local/bin/pbnvi
        /usr/local/bin/pbumacs
        /usr/local/bin/pbvi
        /usr/local/man/man1/pbless.1
        /usr/local/man/man1/pbmg.1
        /usr/local/man/man1/pbnvi.1
        /usr/local/man/man1/pbumacs.1
        /usr/local/man/man1/pbvi.1
        /usr/local/man/man8/pblocald.8
        /usr/sbin/pblocald
        [ verifying class <none> ]
        ## Executing postinstall script.

Checking installation of package: BTPBrunh
Installation of <BTPBrunh> was successful.
```

Installing the Configuration Package Using the pkgadd Command

This section shows the execution of the Solaris **pkgadd** command to install the configuration package. Following installation of the configuration package, the installation is verified by submitting the **id** command to Privilege Management for Unix and Linux, and the Solaris **pkginfo** utility is used to list the Privilege Management for Unix and Linux packages that are installed.

The execution text also includes copyright, trademark, trade secrets, and other legal text; however, those notices and text were removed from the following excerpt to save space:

Example:

```
# cd /opt/acpkg/powerbroker/v9.4/pbul_solaris9-10.x86_9.4.3-18/install
        # pkgadd -a ./BTPBadminCLIENT1 -d BTPBcfCLIENT1.ds BTPBcfCLIENT1
        Processing package instance <BTPBcfCLIENT1> from
</opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.x86_9.4.3-18/install/BTPBcfCLIENT1.ds>
        BeyondTrust PowerBroker Unix/Linux Configuration - Root Delegation and Privilege
Management
        (noarch) 9.4.3-18
        BeyondTrust PowerBroker Unix/Linux
        ## Executing checkinstall script.
        Checking installation of dependent component packages...
        ## Processing package information.
        ## Processing system information.
        6 package pathnames are already properly installed.
        ## Verifying package dependencies.
        ## Verifying disk space requirements.
        Installing BeyondTrust PowerBroker Unix/Linux Configuration - Root Delegation and
Privilege Management as <BTPBcfCLIENT1>
        ## Executing preinstall script.
        ## Installing part 1 of 1.
        /etc/init.d/sypbcfg_svcsinetdsmf
        /etc/pb.cfg
        /etc/pb.key
        /etc/pb.settings
        /etc/rc2.d/S99sypbcfg_pbpatton
        /etc/rc2.d/S99sypbcfg_svcsinetdsmf <symbolic link>
        /var/adm/pbksh.log
        /var/adm/pblocald.log
        /var/adm/pbsh.log
        [ verifying class <none> ]
        ## Executing postinstall script.
        Checking installation of package: BTPBcfCLIENT1
        'pkgchk' of package BTPBcfCLIENT1 succeeded
        Reading pb.cfg...
        Checking installation of dependent component packages...
        'pkgchk' of package BTPBlibs succeeded
        'pkgchk' of package BTPBsbmh succeeded
        'pkgchk' of package BTPBrunh succeeded
        Looking for SuperDaemons to configure...
        Finished looking for SuperDaemons to configure...
        Removing PowerBroker service definitions (if any) from /etc/inet/services.
        Adding PowerBroker service definitions to /etc/inet/services.
        Removing any PowerBroker definitions from SuperDaemon inetd file
/etc/inet/inetd.conf
        Adding PowerBroker definitions to SuperDaemon configurations
/etc/inet/inetd.conf.
        Reloading SuperDaemon Configurations...
        Done Reloading SuperDaemon Configurations...
        Updating Settings in database (if any)...
        Installation of <BTPBcfCLIENT1> was successful.

#  pkginfo | grep BTPB application BTPBcfCLIENT1
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

114

```
  BeyondTrust PowerBroker Unix/Linux Configuration - Root Delegation and Privilege
Management
application BTPBlibs
 BeyondTrust PowerBroker Shared Libraries - Root Delegation and Privilege Management
application BTPBrunh
   BeyondTrust PowerBroker Run Host - Root Delegation and Privilege Management
application BTPBsbmh
   BeyondTrust PowerBroker Submit Host - Root Delegation and Privilege Management
```

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

115

Sample of the Uninstall Process from a Package Installation

This section shows the execution of the Solaris pkgrm utility to remove the Privilege Management for Unix and Linux packages.

Example:

```
# cd /opt/acpkg/powerbroker/v9.4/pmul_solaris9-10.sparc_9.4.3-06/install
# pkgrm -na ./BTPBadminCLIENT1 BTPBcfCLIENT1 BTPBsbmh BTPBrunh BTPBlibs
        Reading pb.cfg...
        Looking for SuperDaemons to configure...
        Finished looking for SuperDaemons to configure...
        Removing PowerBroker service definitions (if any) from /etc/inet/services.
        Removing any PowerBroker definitions from SuperDaemon inetd file
/etc/inet/inetd.conf
        Reloading SuperDaemon Configurations...
        Done Reloading SuperDaemon Configurations...
        Removal of <BTPBcfCLIENT1> was successful.
        Removal of <BTPBsbmh> was successful.
        Removal of <BTPBrunh> was successful.
        Removal of <BTPBlibs> was successful.
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

116

Linux Package Installer

This section describes how to install Privilege Management for Unix and Linux using a package installer for Red Hat Enterprise Linux (RHEL) 4 or 5 on an x86, x86_64, ia64, or S/390 computer. Use the Linux package installation if you want to install Privilege Management for Unix and Linux using the Linux RPM package manager.

The Privilege Management for Unix and Linux Linux package installer that is described here is not compatible with the Privilege Management Privilege Management v5.x packages. You must remove BeyondTrust Privilege Management packages v5.x before installing Privilege Management for Unix and Linux Linux packages.

Prerequisites

To use the Linux package installer, you must have the following:

- Package tarball file for the appropriate Privilege Management for Unix and Linux flavor

> 📌 **Note:** *For the Privilege Management for Unix and Linux Linux package installer, the tarball files are cumulative. That is, an update tarball file contains a complete Privilege Management for Unix and Linux installation. It is not necessary to install a baseline version of Privilege Management for Unix and Linux before installing an upgrade.*

- Root access or superuser privileges
- RPM Package Manager (rpm) v4.4 or later

> 📌 **Note:** *The Privilege Management for Unix and Linux Linux package installer does not support prefix or suffix installations.*

Plan Your Installation

When preparing to use the Privilege Management for Unix and Linux package installer, you should be familiar with the following concepts and restrictions:

Component packages: A Privilege Management for Unix and Linux component package is an RPM package manager (.rpm) file that installs a part of the Privilege Management for Unix and Linux application. The Privilege Management for Unix and Linux component packages are listed below with the format **powerbroker-component-v.v.r.bb-pv.arch.rpm**, where:

- **component** = Privilege Management component package name
- **v** = major version v = minor version r = release
- **bb** = build
- **pv** = version number of the package
- **arch** = architecture (for example, i386)

Component Package	Description
powerbroker-loghost-v.v.r.bb-pv.arch.rpm	Contains log host, **pbsync**, and **pbsyncd**.
powerbroker-shlibs-v.v.r.bb-pv.arch.rpm	Contains shared libraries.

Component Package	Description
powerbroker-pbrest-v.v.r.bb-pv.arch.rpm	Contains REST API files.
powerbroker-rnssvr-v.v.r.bb-pv.arch.rpm	Contains Registry Name Service files.
powerbroker-licsvr-v.v.r.bb-pv.arch.rpm	Contains license server files.
powerbroker-master-v.v.r.bb-pv.arch.rpm	Contains policy server host, **pbsync**, and **pbsyncd**.
powerbroker-submithost-v.v.r.bb-pv.arch.rpm	Contains submit host and Privilege Management for Unix and Linux shells.
powerbroker-runhost-v.v.r.bb-pv.arch.rpm	Contains run host and Privilege Management for Unix and Linux utilities.

Which component packages are required depends on the type of Privilege Management for Unix and Linux host you create, such as policy server host, submit host, and so on. You can select the types of Privilege Management for Unix and Linux hosts in the **pbinstall** installation menu, as shown in the following table. For readability the ending of each component in the table (**-v.v.r.bb-pv.arch.rpm**) is removed.

Menu Selection	Required Components (-v.v.r.bb-pv.arch.rpm)
Install everything here (demo mode)? = Yes	**powerbroker-master** **powerbroker-runhost** **powerbroker-submithost** **powerbroker-loghost** **powerbroker-guihost** **powerbroker-shlibs**
Install Master Host? = Yes	**powerbroker-master**
Install Run Host? = Yes	**powerbroker-runhost**
Install Submit Host? = Yes	**powerbroker-submithost**
Install Log Host? = Yes	**powerbroker-loghost**
Install BeyondTrust built-in third-party libraries? = Yes	**powerbroker-shlibs**
Install Registry Name Services Server? [yes]	**powerbroker-rnssvr**
Install License Server? [yes]	**powerbroker-licsvr**

Configuration package: RPM package that is used to install the following files:

- **pb.settings:** Hardcoded target location **/etc/pb.settings**
- **pb.cfg:** Hardcoded target location **/etc/pb.cfg**
- All the encryption keyfiles defined for **networkencryption**, **eventlogencryption**, **iologencryption**, **reportencryption**, **policyencryption**, and **restkeyencryption**
- By default, two key files are created: **pb.key** and **pb.rest.key**

- The sysadmin can define multiple encryption with different keyfiles in locations other than **/etc**. To upgrade and retain settings on the target machine, view all encryption settings in **/etc/pb.settings** and copy the files to the **settings_files** directory before running **"pbinstall -z" and pbcreate*cfgpkg**
- **pb.conf** (for policy server hosts)
- Man pages for the **pbinstall** and **pbcreatelincfgpkg** programs

The Privilege Management for Unix and Linux configuration package is created by the **pbcreatelincfgpkg** program. The component packages must be installed before you install the configuration package.

Package name: Name of the package as stored in the RPM package manager database. For Privilege Management for Unix and Linux package installations, this name is the same as the package file name without the .arch.rpm extension.

Relocated base directory: The directory where the Privilege Management for Unix and Linux binary files and log files are installed. You can choose an alternative directory in which to install these files.

pbinstall program: To create the Privilege Management for Unix and Linux settings files, you use the **pbinstall** program with the **-z** (settings only) option. **pbinstall -z** only creates the settings files, and is *incompatible* with the following command line options:

Options Incompatible with pbinstall -z	Description
-b	Runs **pbinstall** in batch mode.
-c	Skip the steps that process or update the Privilege Management for Unix and Linux settings file.
-e	Runs install script automatically by bypassing the menu step of **pbinstall**.
-i	Ignores previous **pb.settings** and **pb.cfg** files.
-p	Sets the pb installation prefix.
-s	Sets the pb installation suffix.
-u	Installs the utility programs.
-x	Creates a log synchronization host (installs **pbsyncd**).

When you execute **pbinstall** with the **-z** option, you can see two menu items that are not otherwise available:

- **Enter existing pb.settings path:** This enables you to specify your own **pb.settings** file. **pbinstall** reads this settings file and populates the remaining menu choices. You can override some menu choices. If set to **none**, then **pbinstall** does not read a settings file. The remaining menu choices are populated with default values.
- **Enter directory path for settings file creation:** This enables you to specify an alternative output directory for the settings files. The default directory is **/unzip-dir/powerbroker/v<flavor>/<flavor>install/settings_files**, where **unzip-dir** is the directory where the package tarball file was unzipped.

The behavior of **pbinstall -z** depends on whether certain additional command line options are specified:

- If no other command line options are specified, **pbinstall** initially presents a short version of the installation menu. Depending on the choices you make in these items, further menu items become available.
- If command line options **-g**, **-l**, **-m**, **-o**, **-r**, or **-w** are specified, **pbinstall** presents an expanded version of the installation menu that reflects the host types that you are configuring.

When running **pbinstall** with the **-z** option, the following menu items are preprogrammed and cannot be changed:

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

119

- Install man pages?
- Privilege Management daemon location
- Administration programs location
- User programs location
- GUI library directory
- Policy include (sub) file directory
- User man page location
- Admin man page location
- Policy filename
- BeyondTrust built-in third-party library directory

In addition, the values of the following menu items determine the values of other menu items:

Options Preset When Running pbinstall -z	
Setting this menu option to Yes	**Sets these values to Yes**
Install Master Host?	Install Synchronization? Synchronization can be initiated from this host?
Install Run Host?	Install Utilities?
Install Submit Host?	Install PBSSH? Install pbksh? Install pbsh? Will this host use a Log Host?
Install Log Host?	Install Synchronization? Synchronization can be initiated from this host?

> **Note:** *If you plan to use the package installer to install Privilege Management for Unix and Linux on a computer that already has an interactive Privilege Management for Unix and Linux installation on it, see "Interactive Versus Packaged Installation" on page 9 for additional considerations.*

If you plan to use Registry Name Service and are running **pbinstall -z** on a client host (non-primary server), you must perform client registration. This is necessary to properly set up the registry name service database. Client registration also requires that you collect from the Privilege Management for Unix and Linux primary server the following information:

- REST Application ID
- REST Application Key
- Primary server network name or IP address
- Primary License Server REST TCP/IP port
- Registration Client Profile name

Registering client with Primary RNS: If Registry Name Services is enabled for Privilege Management for Unix and Linux, each client host (after the first server installation) needs to be registered with the Primary Registry Name Server. When using package installers on a target host, a post-install configuration script (**/opt/pbul/scripts/pbrnscfg.sh**) is provided to be manually executed on that host to properly register it. This post-install configuration script asks for information about the Primary Registry Name Server, including the Application ID (appid), Application Key (appkey), address/domain name, and the REST TCP/IP port number. This is the same information provided during the client registration part of a **pbinstall -z** install which generates the settings file.

If you prefer a more convenient method of registering RNS clients where the post-install configuration script is non-interactive, Privilege Management for Unix and Linux can save the relevant information in a hidden file during the settings-only run of **pbinstall**, bundle it with the configuration package, and automatically apply it to the target host when that package is installed. However, understand that this is not secure, but is available if the security-convenience trade-off is acceptable. To enable this, refer to the question regarding post-install configuration script displayed when running **pbinstall -z**.

> ℹ️ *For more information, please see the following:*
>
> - *"Relocate the Base Directory" on page 126*
> - *On **pbinstall** command-line options, "Installation Programs" on page 212*

Overview of Steps

Use of the Linux package installer involves the following steps:

1. Unpack the Privilege Management for Unix and Linux package tarball file.
2. Use the **pbinstall** program to create Privilege Management for Unix and Linux settings files.
3. Use the **pbcreatelincfgpkg** program to create the Privilege Management for Unix and Linux configuration package.
4. Perform a package installation using the Linux **rpm** command for any required components.
5. Perform a package installation using the Linux **rpm** command for the Privilege Management for Unix and Linux configuration package.
6. If Registry Name Service is enabled and installing on a non-primary servery, run **/opt/pbul/scripts/pbrnscfg.sh** to register the host.

> ℹ️ *For additional details on the above steps, please see "Installation Procedure" on page 122.*

Installation Procedure

To install Privilege Management for Unix and Linux using the RPM package manager, do the following:

1. Extract the package tarball files into the **/opt/beyondtrust/** directory by executing the following command:

```
tar xvfz pmul_<flavor_version>_pkg.tar.Z
```

2. Optional. The Privilege Management for Unix and Linux Linux package files are digitally signed. You can verify that the packages are genuine by doing the following:

   - Go to the www.beyondtrust.com, and click **Support** to display the Privilege Management for Unix and Linux Downloads page.
   - In the Customers section, click **Login**. Use your customer user name and password to log in to the Privilege Management for Unix and Linux Downloads page.
   - Click **Digital Signature file for Linux RPM packages** and download the tar file to the Linux computer.
   - Extract the key from the tar file.
   - Import the key to the RPM database with the following command:

   ```
   rpm --import keyfile
   ```

   keyfile is the file name of the key file.

   - Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/package/** directory.
   - Execute the following command:

   ```
   rpm -K *.rpm
   ```

   For each package, you should see output similar to the following:

   ```
   powerbroker-master-6.2.0.11-1.i386.rpm: (sha1) dsa sha1 md5 gpg OK
   ```

   The **OK** at the end of the line indicates that the package is genuine.

3. Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/install/** directory.
4. Execute the following command:

```
./pbinstall -z
```

You can include other options with the **-z** option. Use the **-R** option to specify an alternate base directory for installing the component packages.

pbinstall displays the Privilege Management for Unix and Linux installation menu.

You are asked if you want to use client registration. If you plan to enable Registry Name Service, and install on a host that is not designated as a primary server, you must run client registration.

pbinstall then asks if you want to enable Registry Name Service.

5. Make your menu selections. Note that the **Enter existing pb.settings path** menu option enables you to specify your own **pb.settings** file to use. Also, the **Enter directory path for settings file creation** menu option enables you to specify where to save the generated settings files. These menu options are available only when running **pbinstall** with the **-z** option.

    When the menu selection process is complete, **pbinstall** creates the following files in the specified location:

    - **pb.settings**
    - **pb.cfg**
    - **pb.key** (if encryption is enabled)
    - **pb.conf** (for policy server host)

6. Optional. For a Privilege Management for Unix and Linux client, if client-server communications are to be encrypted, replace the generated **pb.key** file with the **pb.key** file from the policy server host. Also, copy any other required key files into the same directory.

> 📌 **Note:** *This step is automatically done if you choose to use client registration.*

7. Optional. For a policy server host, write a policy file (**pb.conf**) and place it in the directory with the other generated files. If you do not provide a **pb.conf** file, a **pb.conf** file with the single command **reject;** is generated and packaged.

    Starting with v8.0, **pbinstall -z** can optionally install the default role-based policies and asks:

    ```
    Installing default role-based policy pbul_policy.conf and pbul_functions.conf in <install_
    dir>/settings_files
    Would you like to use the default role-based policy in the configuration package?
    ```

    - Answer **Yes** for new installs only.
    - If you are upgrading an existing configuration package, to avoid overwriting your existing policy, answer **No**.

    ```
    Use the default role-based policy [Y]?
    ```

    - If you answer **Yes**, the default **pb.conf**, **pbul_policy.conf** and **pbul_functions.conf** files are created and installed on the policy server.
    - If you plan to install over an existing installation, and have an existing policy in place, answer **No**.

8. Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/install/** directory.

9. Run the **pbcreatelincfgpkg** utility by typing:

    ```
    pbcreatelincfgpkg -p suffix -s directory
    ```

    - **suffix** is appended to the configuration package name; length can be up to 18 characters.
    - **directory** contains the Privilege Management for Unix and Linux settings and configuration files to include in the package.

    The **pbcreatelincfgpkg** utility creates the Privilege Management for Unix and Linux configuration package file, **powerbroker-config<suffix>-sv-pv.arch.rpm**.

10. Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/package/** directory.

11. For each required component package, run the Linux **rpm** utility to install the component package by typing:

```
rpm -iv package-file
```

package-file is the name of the component package (.rpm) file. For example:

```
rpm -iv powerbroker-submithost-9.4.1.03-1.x86_64.rpm
```

> **Note:** *To install all component packages, type the following command:*
>
> ```
> rpm -iv *.rpm
> ```

12. Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/install/** directory.

13. Run the Linux **rpm** utility to install the Privilege Management for Unix and Linux configuration package by typing:

```
rpm -iv package-file
```

package-file is the name of the configuration package (.rpm) file created in step 9.

14. Verify the installation of the packages by typing:

```
rpm -qa| grep powerbroker
```

15. If Registry Name Service is enabled and installed on a non-primary server, register the host with the Primary Registry Name Server using a post-install configuration script. Gather the Application ID, Application Key, network name or IP address, and REST TCP/IP port of the primary server, then run the script to register the host and follow the prompts:

```
/opt/pbul/scripts/pbrnscfg.sh
```

> *For more information, please see the following:*
>
> - *For other options you can use with the pbinstall **-z** option, "Plan Your Installation" on page 117*
> - *"pblighttpd" on page 228*
> - *"pbcreatelincfgpkg" on page 226*

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

124

TC: 12/7/2022

Remove Privilege Management for Unix and Linux Packages

Removing the Privilege Management for Unix and Linux packages completely uninstalls Privilege Management for Unix and Linux from a computer.

To remove the Privilege Management for Unix and Linux packages, type the following:

```
rpm -e config-package-name
    component-package-1 ... component-package-n
```

- **config-package-name** is the name of the package specified when the configuration package is installed. This package name is not required to come first in the list; **rpm** removes it first. However, if you remove packages with separate **rpm** processes, you must remove the configuration package first.
- **component-package-1** through **component-package-n** are the names of the packages specified when the component packages are installed.

> *Example:*
>
> ```
> rpm  -e  powerbroker-configPBUL941-9.4.1.03-1.x86_64  powerbroker-submithost-9.4.1.03-
> 1.x86_64
> ```

Relocate the Base Directory

Using the RPM package management system you can set an alternative base directory for installing packages. With this feature, you can specify a directory to install the Privilege Management for Unix and Linux binary files and log files in. Certain files, such as **pb.settings**, **pb.cfg**, and Privilege Management for Unix and Linux key files, must be located in the **/etc** directory for Privilege Management for Unix and Linux to run. These files are not relocatable.

To relocate the base directory from the default / (root) directory, do the following:

1. On the target machine, create the target base directory if it does not already exist.
2. When you run **pbinstall**, use the **-R** option and specify the new base directory.
3. When installing the component packages, execute **rpm** with the **--prefix** option and specify the relocated directory.

> *Example:*
>
> ```
> rpm  -ivh  --prefix /local/powerbroker  powerbroker-runhost-9.4.1.03-1.x86_64.rpm
> ```

> *Note: The files that are installed by the configuration package cannot be relocated. Do not use the **--prefix** option when installing the configuration package.*

Update Privilege Management for Unix and Linux with the Linux Package Installer

The Privilege Management for Unix and Linux Linux package installer can be used to upgrade an existing Privilege Management for Unix and Linux installation to a new version. The existing Privilege Management for Unix and Linux version should have been installed with the Privilege Management for Unix and Linux package installer.

> 📌 **Note:** *It is possible to use the Linux package installer to install Privilege Management for Unix and Linux over an existing version that was installed with **pbinstall**. However, we do not recommended doing so because it can result in unused files from the existing version remaining in the file system.*

Package Upgrade Considerations

Installing an upgrade with the Linux package installer is similar to using the Linux package installer to install Privilege Management for Unix and Linux for the first time. Keep these considerations in mind when you prepare to upgrade:

- Technically, the Privilege Management for Unix and Linux Linux packages are upgrade packages, as opposed to update packages. An upgrade package installs the new files before removing the existing files and registering the new version number in the RPM database.
- A Privilege Management for Unix and Linux Linux upgrade package contains a complete Privilege Management for Unix and Linux installation, rather than simply the files that have changed since the previous release.
- If you have more than one Privilege Management for Unix and Linux package on a computer, upgrade all packages on that computer.
- A newer release can introduce features that use new settings or configurations. In which case, an upgrade of the configuration package of Privilege Management for Unix & Linux is also needed.
- Unlike Privilege Management for Unix and Linux patches that are installed with **pbpatchinstall**, upgrade packages cannot be rolled back to a previous release. However, you can install an older package over a newer one, effectively rolling back to the older release.

> ℹ️ *For more information, please see "Revert to a Previous Version" on page 129.*

Package Upgrade Procedure

Follow this procedure to upgrade your installation of Privilege Management for Unix and Linux using the Linux package installer:

1. Obtain the tarball file for the Linux upgrade packages that are appropriate for your hardware. The tarball file name has the format **pmul_<flavor>-v.v.r-bb-pn_pkg.tar.Z**.

   - **<flavor>** indicates the operating system and hardware architecture.
   - **v.v.r** is the major and minor version number and the release number.
   - **bb** is the build number.
   - **n** is the update number.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

127

TC: 12/7/2022

2. Extract the package tarball files into the **/unzip-dir/** directory by executing the following command:

```
tar xvfz pmul_<flavor_version>_pkg.tar.Z
```

3. Navigate to the **/unzip-dir/powerbroker/v<version>/<flavor>/install/** directory

4. Create the **settings_files** directory and change directory to that location.

5. To retain or correctly update the settings of the current installation, copy the following files from the target installation host into the **settings_files** directory you created in step 4:

   - /etc/pb.settings
   - /etc/pb.cfg
   - encryption keys defined in pb.settings for networkencryption, eventlogencryption, iologencryption, reportencryption, policyencryption, and restkeyencryption settings (if enabled)

> **Note:** *In a default installation, there are typically 2 key files created:* **pb.key** *and* **pb.rest.key**.

   - policy file defined in **policyfile** setting in **pb.settings** (if the target installation is a Policy Server)

> **Note:** *In a default installation, the policy file is located in* **/opt/pbul/policies/pb.conf**.

6. Execute the following command and verify the installation settings:

```
./pbinstall -z
```

7. Create the upgrade configuration package by running the **pbcreatelincfgpkg** utility:

```
pbcreatelincfgpkg -p suffix
```

Use the current suffix of the installation to be upgraded. Use the suffix you provided during the initial package installation in step 9 of the **Installation Procedure**.

Another way to find the suffix is to run the following command on the target installation host to get the list of packages installed:

```
rpm -qa |grep powerbroker
```

Identify the suffix of the Privilege Management for Unix and Linux configuration package using this format:

```
powerbroker-config<suffix>-<version>.noarch
```

8. Navigate to the **/unzip-dir/powerbroker/v<version>/<flavor>/package/** directory.

9. Use the Linux **rpm** utility to upgrade the component packages by typing:

```
rpm -Uv package-file-1 package-file-2...
```

package-file-n is the name of a component package (.rpm) file.

> **Example:**
>
> ```
> rpm  -Uv  powerbroker-submithost-9.4.1.03-1.p2-1.x86_64.rpm  powerbroker-runhost-
> 9.4.1.03-1.p2-1.x86_64.rpm
> ```

10. Navigate to the **/unzip-dir/powerbroker/<version>/<flavor>/install/** directory.

11. Run the Linux **rpm** utility to install the Privilege Management for Unix and Linux configuration package by typing:

```
rpm -Uv package-file
```

package-file is the name of the configuration package (.rpm) file created in step 7.

12. Verify the installation of the packages by typing:

```
rpm -qa| grep powerbroker
```

Revert to a Previous Version

Unlike Privilege Management for Unix and Linux patches that are installed with **pbpatchinstall**, upgrade packages cannot be rolled back to a previous release. However, you can install an older package over a newer one, effectively rolling back to the older release. To install older packages over newer ones, use the following command:

```
rpm -Uv --oldpackage package-file-1 package file-2...
```

This command restores the previous release. Repeat the command to restore earlier releases. To restore a single package per **rpm** command, add the **--replacepkgs** option.

Upgrade the Configuration Package

When upgrading the configuration package (cfg pkg), some settings that are part of the package might need settings and configuration files copied from the existing installation to the staging host.

Files included in the cfg package:

- **pb.settings:** Hardcoded target location **/etc/pb.settings**.
- **pb.cfg:** Hardcoded target location **/etc/pb.cfg**.
- All the encryption key files defined for networkencryption, eventlogencryption, iologencryption, reportencryption, policyencryption, and restkeyencryption. By default, two key files are typically created:
  - **pb.key**
  - **pb.rest.key**

  The sysadmin can define encryption with different key files in locations other than **/etc**. Therefore, when upgrading, and to retain what is installed on the target machine, look at all the encryption settings in **/etc/pb.settings**. Copy the settings to the **settings_files** directory before running **pbinstall -z** and **pbcreate*cfgpkg**.

- Policy file if the target is a policy server.

Sample Execution for the Linux Package Installer

The sample execution shows the installation of a Privilege Management for Unix and Linux submit host, run host, and shared libraries using the Privilege Management for Unix and Linux Linux package installer.

This sample execution is divided into the following parts:

- Generate the Privilege Management for Unix and Linux settings files.
- Create the Privilege Management for Unix and Linux configuration package using the **pbcreatelincfgpkg** program.
- Install the component packages using the **rpm** command.
- Install the configuration package using the **rpm** command.

Generate the Privilege Management for Unix and Linux Settings Files

This section of the execution shows the generation of the Privilege Management for Unix and Linux settings files (**pb.key**, **pb.cfg**, and **pb.settings**) and also displays the Privilege Management for Unix and Linux installation menu. This output was generated using the **pbinstall** program with the options: **–z**, **-l**, and **-r:**

> *Example:*
>
> ```
> # ./pbinstall -zlr
> Starting pbinstall main() from /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
> 03/install/.
> linux.x86-64
>
> Privilege Management for Unix and Linux Settings File Generation
>
> Please read the Privilege Management for Unix and Linux Installation Instructions before
> proceeding.
>
> Checking MANIFEST against release directory
> Press return to continue
> The Registry Name Service of Privilege Management for Unix and Linux facilitates location
> of other services within the PMUL enterprise with the aid of a centralized
> data repository.
> IMPORTANT: client registration is required if this is not the Primary Server and you
> intend to use Registry Name Services.
> Do you wish to utilize Registry Name Service? [yes]? no
> BeyondTrust Privilege Management for Unix and Linux Installation Menu
>           Opt  Description                                  [Value]
>           1  Install Everything Here (Demo Mode)?        [no]
>           2  Install License Server?                     [no]
>           3  Install Registry Name Services Server?      [no]
>           4  Install Client Registration Server?         [no]
>           5  Install Policy Server Host?                 [yes]
>           6  Install Run Host?                           [yes]
>           7  Install Submit Host?                        [yes]
>           8  Install PBSSH?                              [yes]
>           10  Install Log Host?                          [yes]
>           11  Enable Logfile Tracking and Archiving?     [yes]
> ```

```
                12   Is this a Log Archiver Storage Server?      [no]
                13   Is this a Log Archiver Database Server?      [no]
                14   Install File Integrity Monitoring Polic...   [no]
                15   Install REST Services?                       [yes]
                16   List of License Servers                      [*]
                19   Path to Password Safe 'pkrun' binary         []
                23   Install Synchronization program?             [yes]
                25   Install Secure GUI Host?                     [yes]
                26   Install Utilities: pbvi, pbnvi, pbmg, p...   [yes]
                27   Install pbksh?                               [yes]
                28   Install pbsh?                                [yes]
                29   Install man pages?                           [no]
                30   Will this host use a Log Host?               [yes]
                31   AD Bridge Integration?                       [no]
                37   Integration with BeyondInsight?              [no]
                55   Synchronization program can be initiate...   [yes]
                56   Daemons location                             [/usr/sbin]
                57   Number of reserved spaces for submit pr...   [80]
                58   Administration programs location            [/usr/sbin]
                59   User programs location                       [/usr/local/bin]
                60   GUI library directory                        [/usr/local/lib/pbbuilder]
                61   Policy include (sub) file directory          [/opt/pbul/policies]
                62   Policy file name                             [/opt/pbul/policies/pb.conf]
                65   Log Archive Storage Server name              []
                67   Log Archiver Database Server name            []
                69   Logfile Name Cache Database file path?       [/opt/pbul/dbs/pblogcache.db]
                70   REST Service installation directory?
    [/usr/lib/beyondtrust/pb/rest]
                71   Install REST API sample code?                [no]
                73   Pblighttpd user                              [pblight]
                75   Pblighttpd user UID                          []
                76   Pblighttpd user GID                          []
                78   Configure systemd?                           [yes]
                79   Command line options for pbmasterd          [-ar]
                80   Policy Server Delay                          [500]
                81   Policy Server Protocol Timeout               [-1]
                82   pbmasterd diagnostic log                     [/var/log/pbmasterd.log]
                83   Eventlog filename                            [/var/log/pb.eventlog]
                84   Configure eventlog rotation via size?        []
                85   Configure eventlog rotation path?            []
                86   Configure eventlog rotation via cron?        [no]
                87   Validate Submit Host Connections?            [no]
                88   List of Policy Servers to submit to          [kandor]
                89   pbrun diagnostic log?                        [none]
                90   pbssh diagnostic log?                        [none]
                91   Allow Local Mode?                            [yes]
                92   Additional secured task checks?              [no]
                93   Suppress Policy Server host failover er...   [yes]
                94   List of Policy Servers to accept from        [kandor]
                95   pblocald diagnostic log                      [/var/log/pblocald.log]
                96   Command line options for pblocald           []
                97   Syslog pblocald sessions?                    [no]
```

```
              98   Record PTY sessions in utmp/utmpx?         [yes]
              99   Validate Policy Server Host Connections?    [no]
              100  List of Log Hosts                           [kandor]
              101  Command line options for pblogd             []
              102  Log Host Delay                              [500]
              103  Log Host Protocol Timeout                   [-1]
              104  pblogd diagnostic log                       [/var/log/pblogd.log]
              105  List of log reserved filesystems            [none]
              106  Number of free blocks per log system fi...  [0]
              107  Command line options for pbsyncd            []
              108  Sync Protocol Timeout                       [-1]
              109  pbsyncd diagnostic log                      [/var/log/pbsyncd.log]
              110  pbsync diagnostic log                       [/var/log/pbsync.log]
              111  pbsync sychronization time interval (in...  [15]
              112  Add installed shells to /etc/shells         [no]
              113  pbksh diagnostic file                       [/var/log/pbksh.log]
              114  pbsh diagnostic file                        [/var/log/pbsh.log]
              115  Stand-alone pblocald command                [none]
              116  Stand-alone root shell default iolog        [/pbshell.iolog]




              121  Use syslog?                                 [yes]
              122  Syslog facility to use?                     [LOG_AUTHPRIV]
              123  Base Daemon port number                     [24345]
              124  pbmasterd port number                       [24345]
              125  pblocald port number                        [24346]
              126  pblogd port number                          [24347]


              129  pbsyncd port number                         [24350]
              130  REST Service port number                    [24351]
              131  Add entries to '/etc/services'              [yes]
              132  Allow non-reserved port connections         [yes]
              133  Inbound Port range                          [1025-65535]
              134  Outbound Port range                         [1025-65535]
              137  Network encryption options                  [aes-256:keyfile=/etc/pb.key]
              138  Event log encryption options                [none]
              139  I/O log encryption options                  [none]
              140  Report encryption options                   [none]
              141  Policy file encryption options              [none]
              142  Settings file encryption type               [none]
              143  REST API encryption options                 [aes-
256:keyfile=/etc/pb.re...]
              144  Configure with Kerberos v5?                 [no]
              150  Enforce High Security Encryption?           [yes]
              151  Use SSL?                                    [yes]
              152  SSL Configuration?                          [requiressl]
              153  SSL pbrun Certificate Authority Directory?  [none]
              154  SSL pbrun Certificate Authority File?       [none]
              155  SSL pbrun Cipher List?                      [HIGH:!SSLv2:!3DES:!MD5:@ST…]
```

```
            156  SSL pbrun Certificate Directory?          [none]
            157  SSL pbrun Certificate File?               [none]
            158  SSL pbrun Private Key Directory?          [none]
            159  SSL pbrun Private Key File?               [none]
            160  SSL pbrun Certificate Subject Checks?     [none]
            161  SSL Server Certificate Authority Direct... [none]
            162  SSL Server Certificate Authority File?    [none]
            163  SSL Server Cipher List?
[HIGH:!SSLv2:!3DES:!MD5:@ST...]
            164  SSL Server Certificate Directory?         [none]
            165  SSL Server Certificate File?              [/etc/pbssl.pem]
            166  SSL Server Private Key Directory?         [none]
            167  SSL Server Private Key File?              [/etc/pbssl.pem]
            168  SSL Server Certificate Subject Checks?    [none]
            169  SSL Certificate Country Code              [US]
            170  SSL Certificate State/Province            [AZ]
            171  SSL Certificate Location (Town/City)      [Phoenix]
            172  SSL Certificate Organizational Unit/Dep... [Security]
            173  SSL Certificate Organization              [BeyondTrust]
            174  Configure Privilege Management for Unix... [no]
            175  Install BeyondTrust built-in third-part... [yes]
            176  BeyondTrust built-in third-party librar... [/usr/lib/beyondtrust/pb]
            188  Use PAM?                                  [no]
            196  Allow Remote Jobs?                        [yes]
            197  UNIX Domain Socket directory              [none]
            198  Reject Null Passwords?                    [no]
            199  Enable TCP keepalives?                    [no]
            200  Name Resolution Timeout                   [0]
            N for the next menu page, P for the previous menu page, C to continue, X to
exit
Please enter a menu option [For technical support call 1-800-234-9072]> c
Generating key file /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/settings_files/pb.key...

Are all the installation settings correct [yes]?
Generating config file /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/settings_files/pb.cfg
Creating the settings file creation script
Backed up existing settings file creation script to:
'/opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/pbcreatesettingsfile.ctime.Feb_13_16:28'
Running settings file creation script
Creating settings file /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/settings_files/pb.settings
Generated settings files are in directory: /opt/final/powerbroker/v9.4/pmul_linux.x86-64_
9.4.1-03/install/settings_filesPrivilege Management for Unix and Linux Settings File
Generation completed successfully.
```

Create the Privilege Management for Unix and Linux Configuration Package Using pbcreatelincfgpkg

This section shows the creation of the Privilege Management for Unix and Linux configuration package using the **pbcreatelincfgpkg** program with the **-p** and **-s** options.

> *Note: At the end of its output, the **pbcreatelincfgpkg** script shows which Privilege Management for Unix and Linux component packages need to be installed.*

Example:

```
# ./pbcreatelincfgpkg  -p CLIENTPAKU  -s /opt/final/powerbroker/v9.4/CLIENTPAKU_settings_
files
pbcreatelincfgpkg: starting from /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install
pbcreatelincfgpkg: keyfile pb.key will be included in package
Reading /opt/final/powerbroker/v9.4/CLIENTPAKU_settings_files/pb.cfg

pbcreatelincfgpkg: making PowerBroker Linux configuration package . . .
Executing(%prep): /bin/sh -e /var/tmp/rpm-tmp.kq2x6j
+ umask 022
+ cd /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-03/install/rpmbuild/BUILD
+ LANG=C
+ export LANG
+ unset DISPLAY
+ rm -rf '/opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILD/*'
+ exit 0
Executing(%build): /bin/sh -e /var/tmp/rpm-tmp.Z2J5QI
+ umask 022
+ cd /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-03/install/rpmbuild/BUILD
+ LANG=C
+ export LANG
+ unset DISPLAY
+ exit 0
Executing(%install): /bin/sh -e /var/tmp/rpm-tmp.wlumC7
+ umask 022
+ cd /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-03/install/rpmbuild/BUILD
+ '[' /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64 '!=' / ']'
+ rm -rf /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64
++ dirname /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64
+ mkdir -p /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT
+ mkdir /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64
+ LANG=C
```

```
+ export LANG
+ unset DISPLAY
+ mkdir -p /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/etc
+ mkdir -p /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/etc/pb
+ cp /opt/final/powerbroker/v9.4/CLIENTPAKU_settings_files/pb.settings
/opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/etc/pb.settings
+ cp /opt/final/powerbroker/v9.4/CLIENTPAKU_settings_files/pb.cfg
/opt/final/powerbroker/v9.4/pbul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/etc/pb.cfg
+ cp /opt/final/powerbroker/v9.4/CLIENTPAKU_settings_files/pb.key
/opt/final/powerbroker/v9.4/pbul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/etc/pb.key
++ dirname /var/log/pblocald.log
+ logfiledir=/var/log
+ '[' '!' -d /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/var/log ']'
+ mkdir -p /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/var/log
++ dirname /var/log/pbksh.log
+ logfiledir=/var/log
+ '[' '!' -d /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/var/log ']'
++ dirname /var/log/pbsh.log
+ logfiledir=/var/log
+ '[' '!' -d /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/var/log ']'
++ dirname /pbshell.iolog
+ logfiledir=/
+ '[' '!' -d /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/ ']'
+ /usr/lib/rpm/check-buildroot
+ /usr/lib/rpm/redhat/brp-compress
+ /usr/lib/rpm/redhat/brp-strip /usr/bin/strip
+ /usr/lib/rpm/redhat/brp-strip-static-archive /usr/bin/strip
+ /usr/lib/rpm/redhat/brp-strip-comment-note /usr/bin/strip /usr/bin/objdump
+ /usr/lib/rpm/brp-python-bytecompile /usr/bin/python
+ /usr/lib/rpm/redhat/brp-python-hardlink
+ /usr/lib/rpm/redhat/brp-java-repack-jars
Processing files: powerbroker-configCLIENTPAKU-9.4.1.03-1.noarch
Requires(interp): /bin/sh /bin/sh /bin/sh /bin/sh
Requires(rpmlib): rpmlib(CompressedFileNames) <= 3.0.4-1 rpmlib(FileDigests) <= 4.6.0-1
rpmlib(PayloadFilesHavePrefix) <= 4.0-1
Requires(pre): /bin/sh
Requires(post): /bin/sh
Requires(preun): /bin/sh
Requires(postun): /bin/sh
Checking for unpackaged file(s): /usr/lib/rpm/check-files
/opt/final/powerbroker/v9.4/pbul_linux.x86-64_9.4.1-
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

135

```
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64
Wrote: /opt/final/powerbroker/v9.4/pbul_linux.x86-64_9.4.1-
03/install/rpmbuild/RPMS/noarch/powerbroker-configCLIENTPAKU-9.4.1.03-1.noarch.rpm
Executing(%clean): /bin/sh -e /var/tmp/rpm-tmp.A8w0eY
+ umask 022
+ cd /opt/final/powerbroker/v9.4/pbul_linux.x86-64_9.4.1-03/install/rpmbuild/BUILD
+ rm -rf /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/etc
/opt/final/powerbroker/v9.4/pbul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/pbshell.iolog
/opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-
03/install/rpmbuild/BUILDROOT/powerbroker-9.4.1.03-1.x86_64/var
+ exit 0
pbcreatelincfgpkg: rpm package built
pbcreatelincfgpkg: rpm package verified
pbcreatelincfgpkg: rpm package 'powerbroker-configCLIENTPAKU-9.4.1.03-1.noarch.rpm'
placed in
/opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-03/install

pbcreatelincfgpkg: the following packages will need to be loaded to the target system:
powerbroker-runhost powerbroker-submithost powerbroker-shlibs

pbcreatelincfgpkg: completed.
```

Install Component Packages Using the rpm Command

This section shows the execution of the **rpm** command to install component packages for the submit host, run host, and shared libraries:

Example:

```
# cd /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-03/package
# rpm -iv powerbroker-shlibs-9.4.1.03-1.x86_64.rpm powerbroker-submithost-9.4.1.03-1.x86_
64.rpm  powerbroker-runhost-9.4.1.03-1.x86_64.rpm
warning: powerbroker-shlibs-9.4.1.03-1.x86_64.rpm: Header V3 DSA/SHA1 Signature, key ID
19227ca5: NOKEY
        Preparing packages for installation...
        powerbroker-shlibs-9.4.1.03-1
        powerbroker-runhost-9.4.1.03-1
        powerbroker-submithost-9.4.1.03-1
```

Install the Configuration Package Using the rpm Command

This section shows the execution of the Linux **rpm** command to install the configuration package. Following installation of the configuration package, the installation is verified by submitting the **id** command to Privilege Management for Unix and Linux, and the Linux **rpm -qa** utility is used to list the Privilege Management for Unix and Linux packages that are installed:

Example:

```
# cd /opt/final/powerbroker/v9.4/pmul_linux.x86-64_9.4.1-03/install
# rpm  -iv powerbroker-configCLIENTPAKU-9.4.1.03-1.noarch.rpm
Preparing packages for installation...
powerbroker-configCLIENTPAKU-9.4.1.03-1
Reading pb.cfg...
Updating Settings in database (if any)...
Checking installation of dependent component packages...
'rpm -V' of package powerbroker-shlibs succeeded
'rpm -V' of package powerbroker-submithost succeeded
'rpm -V' of package powerbroker-runhost succeeded
Looking for SuperDaemons to configure...
Finished looking for SuperDaemons to configure...
Removing PowerBroker service definitions (if any) from /etc/services.
Adding PowerBroker service definitions to /etc/services.
Removing any PowerBroker definitions from SuperDaemon xinetd file /etc/xinetd.conf
Adding PowerBroker definitions to SuperDaemon configurations   /etc/xinetd.conf.
Reloading SuperDaemon Configurations...
Done Reloading SuperDaemon Configurations...
# rpm -qa | grep powerbroker
powerbroker-runhost-9.4.1.03-1.x86_64
powerbroker-configCLIENTPAKU-9.4.1.03-1.noarch
powerbroker-shlibs-9.4.1.03-1.x86_64
powerbroker-submithost-9.4.1.03-1.x86_64

# pbrun id # test PowerBroker
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk), 10
(wheel),501(amanda)

# rpm -qa | grep powerbroker # list PowerBroker packages
powerbroker-runhost-9.4.1.03-1.x86_64
powerbroker-configCLIENTPAKU-9.4.1.03-1.noarch
powerbroker-shlibs-9.4.1.03-1.x86_64
powerbroker-submithost-9.4.1.03-1.x86_64
```

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

137

TC: 12/7/2022

Sample of the Uninstall Process from a Package Installation

This section shows the execution of the Linux rpm utility to remove the Privilege Management for Unix and Linux packages:

Example:

```
# rpm -e powerbroker-configCLIENTPAKU powerbroker-shlibs powerbroker- submithost
powerbroker-runhost
Reading pb.cfg...
Looking for SuperDaemons to configure...
Finished looking for SuperDaemons to configure...
Removing PowerBroker service definitions (if any) from /etc/services. Removing any
PowerBroker definitions from SuperDaemon xinetd file
/etc/xinetd.conf
Reloading SuperDaemon Configurations...
Done Reloading SuperDaemon Configurations...
```

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

138

TC: 12/7/2022

AIX Package Installer

This section describes how to install Privilege Management for Unix and Linux using a package installer for AIX v5.3, 6.1 and 7.0 on a POWER 64-bit computer. AIX package installers are compatible with or without workload partitions (WPARs). Use the AIX package installer if you want to install Privilege Management for Unix and Linux using the AIX **installp** command.

The Privilege Management for Unix and Linux AIX package installer that is described here is not compatible with the BeyondTrustPrivilege Management v5.x packages. If the BeyondTrust Privilege Management v5.x packages are installed, you must remove them before installing the Privilege Management for Unix and Linux AIX packages.

WPARs

If you have AIX v6.1 or higher, then you can use WPARs.

> ℹ️ *For more information about WPARs and propagating BeyondTrust AIX package installations to them, please see the following:*
> - *"Installation Procedure" on page 145*
> - *"View a List of Installed Privilege Management for Unix and Linux Packages" on page 163*

Prerequisites

To use the AIX package installer, you must have the following:

- Package tarball file for the appropriate Privilege Management for Unix and Linux flavor
- Root access or superuser privileges

> 📌 *Note: The Privilege Management for Unix and Linux AIX package installer does not support prefix or suffix installations.*

Plan Your Installation

When preparing to use the Privilege Management for Unix and Linux package installer, you should be familiar with the following concepts and restrictions:

Component packages: A Privilege Management for Unix and Linux component package is an AIX backup file format (.bff) file that installs a portion of the Privilege Management for Unix and Linux application. Privilege Management for Unix and Linux component packages use a format of **powerbroker.component-v.v.r.bb.bff**, where:

- **v** = major version
- **v** = minor version
- **r** = release
- **bb** = build

> 🔍 *Example: powerbroker.masterhost-6.2.0.05.bff*

Component package or file names	Description
powerbroker.loghost-v.v.r.bb.bff	Contains the log host, **pblogd**, and man pages. **powerbroker.common-v.v.r.bb.bff** is a prerequisite for this package.
powerbroker-pbrest-v.v.r.bb-pv.arch.rpm	Contains REST API files.
powerbroker.rnssvr-v.v.r.bb.bff	Contains Registry Name Service files.
powerbroker.licsvr-v.v.r.bb.bff	Contains license server files.
powerbroker.sharedlibs-v.v.r.bb.bff	Contains the shared libraries: **libcom_err.so.3.0, libcrypto.a, libgssapi_krb5.so.2.2, libk5crypto.so.3.1, libkrb5.so.3.3, liblber-2.5.a, libldap-2.5.a, libssl.a**. **powerbroker.common-v.v.r.bb.bff** is a prerequisite for this package.
powerbroker.common-v.v.r.bb.bff	Contains the shared files and **pbbench**, **pbcall**, **bencode**, **pbsum**, man pages and **pbinstall.8**, and **pbcreateaixcfgpkg.8**. This package is a prerequisite for all the previously listed packages: **powerbroker.masterhost**, **powerbroker.submithost**, **powerbroker.guihost**, **powerbroker.loghost** and **powerbroker.sharedlibs**.
powerbroker.mlcommon-v.v.r.bb.bff	Contains the policy server log shared files, **pblog**, **pbreplay**, **pbsyncd**, **pbsync**, and man pages. This package is a prerequisite for **powerbroker.masterhost-v.v.r.bb.bff** and **powerbroker.loghost-v.v.r.bb.bff**.
powerbroker.masterhost-v.v.r.bb.bff	Contains the policy server host, **pbcheck**, **pbkey**, **pbmasterd**, **pbpasswd**, **pbpatton**, **pbprint**, and man pages. **powerbroker.common-v.v.r.bb.bff** is a prerequisite for this package.
powerbroker.runhost-v.v.r.bb.bff	Contains the run host and Privilege Management for Unix and Linux utilities: **pblocald**, **pbless**, **pbmg**, **pbnvi**, **pbumacs**, **pbvi**, and man pages. **powerbroker.common- v.v.r.bb.bff** is a prerequisite for this package.
powerbroker.submithost-v.v.r.bb.bff	Contains the submit host and Privilege Management for Unix and Linux shells, **pbksh**, **pbsh**, **pbssh**, **pbrun**, and man pages. **powerbroker.common-v.v.r.bb.bff** is a prerequisite for this package.

Which component packages are required depends on the type of Privilege Management for Unix and Linux host you are creating, such as policy server host, log host, and so on. You can select the types of hosts in the **pbinstall** installation menu, as shown in the following table.

Menu Selection	Required Components
Install everything here (demo mode)? = Yes	powerbroker.masterhost-v.v.r.bb.bffpowerbroker.runhost-v.v.r.bb.bff
	powerbroker.submithost-v.v.r.bb.bff
	powerbroker.loghost-v.v.r.bb.bffpowerbroker.guihost-v.v.r.bb.bff
	powerbroker.sharedlibs-v.v.r.bb.bff
	powerbroker.common-v.v.r.bb.bff
	powerbroker.mlcommon-v.v.r.bb.bff

Install Policy Server Host? = Yes	powerbroker.masterhost-v.v.r.bb.bff
	powerbroker.common-v.v.r.bb.bff
	powerbroker.mlcommon-v.v.r.bb.bff
Install Run Host? = Yes	powerbroker.runhost-v.v.r.bb.bff
	powerbroker.common-v.v.r.bb.bff
Install Submit Host? = Yes	powerbroker.submithost-v.v.r.bb.bff
	powerbroker.common-v.v.r.bb.bff
Install Log Host? = Yes	powerbroker.loghost-v.v.r.bb.bff
	powerbroker.common-v.v.r.bb.bff
	powerbroker.mlcommon-v.v.r.bb.bff
Install BeyondTrust built-in third-party libraries? = Yes	powerbroker.sharedlibs-v.v.r.bb.bff
	powerbroker.common-v.v.r.bb.bff
Install Registry Name Services Server? [yes]	powerbroker.rnssvr-v.v.r.bb.bff
Install License Server? [yes]	powerbroker.licsvr-v.v.r.bb.bff

Configuration package: AIX installation package created by the user named **powerbroker.config[suffix]**, where **suffix** is user-defined. It contains the configuration files that are used to install the following files:

- **pb.settings:** Hardcoded target location **/etc/pb.settings**
- **pb.cfg:** Hardcoded target location **/etc/pb.cfg**
- All the encryption keyfiles defined for **networkencryption**, **eventlogencryption**, **iologencryption**, **reportencryption**, **policyencryption**, and **restkeyencryption**
- By default, two key files are created: **pb.key** and **pb.rest.key**
- The sysadmin can define multiple encryption with different keyfiles in locations other than **/etc**. To upgrade and retain settings on the target machine, view all encryption settings in **/etc/pb.settings** and copy the files to the **settings_files** directory before running **"pbinstall -z" and pbcreate*cfgpkg**
- **pb.conf** (for policy server hosts)
- Man pages for the **pbinstall** and **pbcreateaixcfgpkg** programs

The Privilege Management for Unix and Linux configuration package is created by the **pbcreateaixcfgpkg** program. The component packages must be installed before you install the configuration package.

Package name: Name of the installation package stored in the AIX database. For Privilege Management for Unix and Linux package installations, this name is the same as the package file name without the .bff extension.

pbinstall program: To create the Privilege Management for Unix and Linux settings files, you use the **pbinstall** program with the **-z** (settings only) option. **pbinstall -z** only creates the settings files and is *incompatible* with the following command line options:

Options Incompatible with pbinstall -z	Description
-b	Runs **pbinstall** in batch mode.

SALES: www.beyondtrust.com/contact   SUPPORT: www.beyondtrust.com/support   DOCUMENTATION: www.beyondtrust.com/docs

141

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

TC: 12/7/2022

-c	Skip the steps that process or update the Privilege Management for Unix and Linux settings file.
-e	Runs install script automatically by bypassing the menu step of **pbinstall**.
-i	Ignores previous **pb.settings** and **pb.cfg** files.
-p	Sets the pb installation prefix.
-s	Sets the pb installation suffix.
-u	Installs the utility programs.
-x	Creates a log synchronization host (that is, installs **pbsyncd**).

When you execute **pbinstall** with the **-z** option, you can see two menu items that are not otherwise available:

- **Enter existing pb.settings path:** Enables you to specify your own **pb.settings** file. **pbinstall** reads this settings file and populates the remaining menu choices. You can override some menu choices. If set to **none**, then **pbinstall** does not read a settings file. The remaining menu choices are populated with default values.
- **Enter directory path for settings file creation:** Enables you to specify an alternative output directory for the settings files. The default directory is **/unzip-dir/powerbroker/<version>/<flavor>/ install/settings_files**, where **unzip-dir** is the directory where the package tarball file was unzipped.

The behavior of **pbinstall -z** depends on whether certain additional command line options are specified:

- If no other command line options are specified, **pbinstall** initially presents a short version of the installation menu (items 1–8 only). Depending on the choices you make in these items, further menu items become available.
- If command line options **-g**, **-l**, **-m**, or **-r** are specified, **pbinstall** presents an expanded version of the installation menu that reflects the host types that you are configuring.

When running **pbinstall** with the **-z** option, the following menu items are preprogrammed and cannot be changed:

- **Install man pages?**
- **Daemon location**
- **Administration programs location**
- **User programs location**
- **GUI library directory**
- **Policy include (sub) file directory**
- **User man page location**
- **Admin man page location**
- **Policy filename**
- **BeyondTrust built-in third-party library directory**

In addition, the values of the following menu items determine the values of other menu items:

Options Preset When Running pbinstall -z	
Setting this menu option to Yes	**Sets these values to Yes**
Install Policy Server Host?	Install Synchronization? Synchronization can be initiated from this host?
Install Run Host?	Install Utilities?

Options Preset When Running pbinstall -z	
Install Submit Host?	Install PBSSH?
	Install pbksh? Install pbsh?
	Will this host use a Log Host?
Install Log Host?	Install Synchronization? Synchronization can be initiated from this host?

If you plan to use Registry Name Service and are running **pbinstall -z** on a client host (non-primary server), you must perform client registration. This is necessary to properly set up the registry name service database. Client registration will also require that you collect from the Privilege Management for Unix and Linux primary server the following information:

- REST Application ID
- REST Application Key
- Primary server network name or IP address
- Primary License Server REST TCP/IP port
- Registration Client Profile name

> **Tip:** *If you are using the package installer to install Privilege Management for Unix and Linux on a computer that already has an interactive Privilege Management for Unix and Linux installation on it, see "Installation Considerations" on page 7 for additional considerations.*

RNS client registration: If Registry Name Services is enabled for Privilege Management for Unix and Linux, each client host (after the first server installation) needs to be registered with the Primary Registry Name Server. When using package installers on a target host, a post-install configuration script (**/opt/pbul/scripts/pbrnscfg.sh**) is provided to be manually executed on that host to properly register it. This post-install configuration script asks for information about the Primary Registry Name Server, including the Application ID (appid), Application Key (appkey), address/domain name, and the REST TCP/IP port number. This is the same information provided during the client registration part of a **pbinstall -z** install which generates the settings file.

If you prefer a more convenient method of registering RNS clients where the post-install configuration script is non-interactive, Privilege Management for Unix and Linux can save the relevant information in a hidden file during the settings-only run of **pbinstall**, bundle it with the configuration package, and automatically apply it to the target host when that package is installed. However, understand that this is not secure, but is available if the security-convenience trade-off is acceptable. To enable this, refer to the question regarding post-install configuration script displayed when running **pbinstall -z**.

> **i** *For more complete **pbinstall** command-line options, please see "Installation Programs" on page 212*

Use Privilege Management for Unix and Linux Packages on AIX WPARs

The Privilege Management for Unix and Linux AIX package installer supports AIX WPARs in AIX v6.1 and higher. The primary operating system instance is referred to as the global WPARs. All WPARs that are not global are referred to as non-global WPARs.

> **Note:** *AIX release v6.1 or higher is required. The use of WPARs is not supported on earlier releases. There are two types of WPARs:*
> - *Shared WPARs share some of the global environment's file systems and are administered by the global environment.*
> - *Non-shared WPARs share none of the global environment's file systems and are treated as stand-alone systems.*

Installing Privilege Management for Unix and Linux AIX packages on WPARs is very similar to installing these packages on AIX systems without WPARs.

ℹ️ *For instructions, please see* *"Installation Procedure" on page 145*.

Overview of Steps

Using the Privilege Management for Unix and Linux AIX package installer involves the following steps:

1. Unpack thePrivilege Management for Unix and Linux package tarball file.
2. Use the **pbinstall** program to create Privilege Management for Unix and Linux settings files.
3. Use the **pbcreateaixcfgpkg** program to create the Privilege Management for Unix and Linux configuration package.
4. Perform a package installation using the AIX **installp** command for any required components.
5. Perform a package installation using the AIX **installp** command for the Privilege Management for Unix and Linux configuration package.
6. If Registry Name Service is enabled and installing on a non-primary servery, run **/opt/pbul/scripts/pbrnscfg.sh** to register the host.

ℹ️ *For more information, please see* *"Installation Procedure" on page 145*.

Installation Procedure

To install Privilege Management for Unix and Linux in the AIX global environment, do the following:

1. Extract the package tarball files into the **/opt/beyondtrust/ directory** by executing the following command:

```
gunzip -c pmul_<flavor_version>_pkg.tar.Z | tar xvf -
```

2. Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/install/** directory.
3. Execute the following command:

```
./pbinstall -z
```

You are asked if you want to use client registration. If you plan to enable Registry Name Service, and are installing on a host that is not designated as a primary server, you must run client registration.

pbinstall next asks if you want to enable Registry Name Service.

pbinstall displays the Privilege Management for Unix and Linux installation menu.

4. Make your menu selections. When the menu selection process is complete, **pbinstall** creates the following files in the specified location:

   - **pb.settings**
   - **pb.cfg**
   - **pb.key** (if encryption is enabled)
   - **pb.conf** (for policy server host)

> 📌 *Note: The **Enter existing pb.settings path** menu option enables you to specify your own **pb.settings** file to use. Also, the **Enter directory path for settings file creation** menu option enables you to specify where to save the generated settings files. These menu options are available only when running **pbinstall** with the **-z** option.*

5. Optional. For a Privilege Management for Unix and Linux client, if client-server communications are to be encrypted, replace the generated **pb.key** file with **pb.key** file from the policy server host. Also, copy any other required key files into the same directory.
6. Optional. For a policy server host, write a policy file (**pb.conf**) and place it in the directory with the other generated files. If you do not provide a **pb.conf** file, a **pb.conf** file with the single command **reject ;** is generated and packaged.

   Starting with v8.0, **pbinstall -z** can optionally install the default role-based policies and asks:

```
Installing default role-based policy pbul_policy.conf and pbul_functions.conf in <install_
dir>/settings_files

Would you like to use the default role-based policy in the configuration package?
```

   - Answer **Yes** for new installs only.
   - If you are upgrading an existing configuration package, to avoid overwriting your existing policy, answer **No**.

```
Use the default role-based policy [Y]?
```

- If you answer **Yes**, the default **pb.conf**, **pbul_policy.conf** and **pbul_functions.conf** files are created and installed on the policy server.
- If you are installing over an existing installation, and have an existing policy in place, answer **No**.

7. Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/install/** directory.

8. Run the **pbcreateaixcfgpkg** utility by typing:

```
pbcreateaixcfgpkg -p suffix -s directory
```

- **suffix** is appended to the filenames of the configuration package backup file format file and the package administration file; the length can be up to 26 characters.
- **directory** contains the Privilege Management for Unix and Linux settings and configuration files to include in the package.

The **pbcreateaixcfgpkg** utility creates the configuration package file, **powerbroker.config<suffix>-v.v.r.b.bff**.

9. Navigate to the **/opt/beyondtrust/powerbroker/<version>/<flavor>/package/** directory.

10. For each required component package, run the AIX **installp** command to install one component package by typing:

```
installp -agd ./ powerbroker.pkg-name
```

pkg-name is the name of the component package file.

> 🔍 **Example:**
>
> ```
> installp -agd ./ powerbroker.submithost
> ```

Using the **-g** option installs all the prerequisite packages along with the **powerbroker.submithost** package. In this case, **powerbroker.common** is a prerequisite package for the **powerbroker.submit** package.

Alternately you can install all the component packages by typing:

```
installp -agd ./ powerbroker
```

11. Run the AIX **installp** command to install the Privilege Management for Unix and Linux configuration package by typing:

```
installp -ad ./ powerbroker.config<suffix>
```

<suffix> is the suffix that is set when you create the Privilege Management for Unix and Linux configuration package in step 8.

12. Verify the installation of the packages with the AIX **lslpp** command by typing:

```
lslpp -l | grep powerbroker
```

13. If Registry Name Service is enabled and installed on a non-primary server, register the host with the Primary Registry Name Server using a post-install configuration script. Gather the Application ID, Application Key, network name or IP address, and REST TCP/IP port of the primary server, then run the script to register the host and follow the prompts:

SALES: www.beyondtrust.com/contact   SUPPORT: www.beyondtrust.com/support   DOCUMENTATION: www.beyondtrust.com/docs

146

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

TC: 12/7/2022

```
/opt/pbul/scripts/pbrnscfg.sh
```

> **i** *For additional information, please see the following:*
> - *For other options you can use with the pbinstall **-z** option, "Plan Your Installation" on page 139*
> - *"pblighttpd" on page 228*
> - *"pbcreateaixcfgpkg" on page 222*

Install Privilege Management for Unix and Linux onto WPARs

The process for installing Privilege Management AIX packages onto non-shared workload partitions (WPARs) is similar to the process for installing in the global AIX environment because the installed software is private to the non-shared WPAR. Therefore, there is no need for synchronization.

To install Privilege Management for Unix and Linux packages onto shared WPARs, follow the following:

1. Follow the procedures in the installation procedure to create the AIX packages.
2. Install Privilege Management component (usr) packages in the global AIX environment. The usr packages are visible to the WPARs.
3. Install Privilege Management configuration (root) package in the global AIX environment. The root packages are not visible to the WPARs until propagated.
4. To make the Privilege Management configuration (root) package visible to the WPARs, use the **syncwpar** command and propagate the packages to WPARs.
5. Optional. List the WPARs.

> **i** *For more information, please see the following:*
> - *"Use syncwpar to Propagate Additional Packages to Shared WPARs" on page 166*
> - *"View a List of WPARs" on page 165*

Remove Privilege Management for Unix and Linux Packages

Removing the Privilege Management for Unix and Linux packages completely uninstalls Privilege Management for Unix and Linux from a computer. To remove the packages, do the following:

1. Navigate to the **/opt/beyondtrust/powerbroker/<version>/aix/install/** directory.
2. Remove multiple Privilege Management for Unix and Linux packages by typing:

```
installp -u powerbroker.configClient component-package-1 ... component-package-n
```

- **configClient** is the name of the package specified during installation of the configuration package. Because of the dependency relationship between the configuration package and the component packages, this package name must come first in the list.
- **component-package-1** through **component-package-n** are the names of the packages specified during installation of the component packages, such as **powerbroker.submithost**.

> *Example:*
>
> ```
> installp -u powerbroker.configClient powerbroker.submithost powerbroker.loghost
> ```

Or you may remove a package and its prerequisites by using the **installp -gu** command.

> *Example: The following command removes the **powerbroker.runhost** package and its prerequisite package **powerbroker.common**:*
>
> ```
> installp -gu powerbroker.runhost
> ```

Remove AIX Package from Shared WPARs

To remove Privilege Management for Unix and Linux packages from shared workload partitions (WPARs), do the following:

1. Remove the Privilege Management for Unix and Linux packages from the global AIX environment using the following command:

```
installp -u powerbroker
```

All Privilege Management for Unix and Linux **usr** packages and the global **root** package are removed.

2. Remove the Privilege Management for Unix and Linux **root** packages from WPARs by doing either of the following:
    - Remove the Privilege Management for Unix and Linux **root** package from one or more specified WPARs by typing the following command from the global AIX environment:

```
syncwpar [nodeA] [nodeB] ... [nodeX]
```

nodeA, **nodeB**, ... **nodeX** are the names of the WPARs.

- Remove the Privilege Management for Unix and Linux **root** package from all WPARs by typing the following command from the global AIX environment:

```
syncwpar -A
```

When you use the **-A** option, all Privilege Management root packages are removed from WPAR.

> 📌 **Note:** *The **syncwpar** command synchronizes all packages between the AIX global environment and shared WPARs.*

3. Optional. Verify that the packages are removed from the WPARs.

> ℹ️ *For more information, please see the following:*
>
> - *An example of the **syncwpar** command in use at "Sample Removal of an AIX Package Installation" on page 170*
> - *For instructions to verify the packages are removed, "Sample Removal of an AIX Package Installation" on page 170*

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

149

Update Privilege Management for Unix and Linux with Update Packages

The Privilege Management for Unix and Linux AIX package installer can be used to update an existing Privilege Management for Unix and Linux installation to a new version. The existing Privilege Management for Unix and Linux version should have been installed using the Privilege Management for Unix and Linux package installer.

Update Package Considerations

Installing a Privilege Management for Unix and Linux update package is similar to using the AIX package installer to install Privilege Management for Unix and Linux for the first time. Keep these considerations in mind when you prepare to upgrade Privilege Management for Unix and Linux:

- Each release of Privilege Management for Unix and Linux AIX update packages contains only the updated files. Therefore, a full Privilege Management for Unix and Linux package installation (of the same major and minor version) must be performed before you can install an upgrade package. For example, before you can install update package version 9.2.1, you must have the full Privilege Management for Unix and Linux package version 9.2.0 installed.
- Each successive Privilege Management AIX update package is cumulative; for example, update package version 9.4.1 contains all of the updates in update package version 9.4.0.
- A newer release can introduce features that use new settings or configurations. In which case, an upgrade of the configuration package of Privilege Management for Unix and Linux is also needed.
- Update packages that have not been committed can be rejected. You cannot reject update packages that have been committed.
- Committing a given update package requires prior or concurrent commit of earlier update packages.
- The Privilege Management for Unix and Linux configuration package does not contain any executable files and therefore does not need to be upgraded. However, if you are creating a new configuration package, you should create it with the same version of Privilege Management for Unix and Linux as the component packages you are installing.

Update Package Procedure

Follow this procedure to update your installation of Privilege Management for Unix and Linux using the update packages:

1. Obtain the tarball file for the AIX update packages that are appropriate for your hardware. The tarball file name has the format **pmul_<flavor>-v.v.r-bb-update_pkg.tar.Z**, where:
   - **<flavor>** indicates the operating system and hardware architecture.
   - **v.v.r** is the major and minor version number and the release number.
   - **bb** is the build number.

2. Extract the package files into the **/unzip-dir/** directory by executing the following command:

   ```
   gunzip -c pmul_<flavor_version>-update_pkg.tar.Z | tar xvf -
   ```

3. Navigate to the **/unzip-dir/powerbroker/v<version>/<flavor>/install/** directory.
4. Create the **settings_files** directory and change directory to that location.
5. To retain or correctly update the settings of the current installation, copy the following files from the target installation host into the **settings_files** directory you created in step 4:

- /etc/pb.settings
- /etc/pb.cfg
- encryption keys defined in pb.settings for networkencryption, eventlogencryption, iologencryption, reportencryption, policyencryption, and restkeyencryption settings (if enabled)

📌 *Note: In a default installation, there are typically 2 key files created: **pb.key** and **pb.rest.key**.*

- policy file defined in **policyfile** setting in **pb.settings** (if the target installation is a Policy Server)

📌 *Note: In a default installation, the policy file is located in **/opt/pbul/policies/pb.conf**.*

6. Execute the following command to verify and update the installation settings in the **settings_files** directory:

```
./pbinstall -z
```

7. Create the upgrade configuration package by running the **pbcreateaixcfgpkg** utility:

```
pbcreateaixcfgpkg -p suffix
```

Use the current suffix of the installation to be upgraded. Use the suffix you provided during the initial package installation in step 8 of the **Installation Procedure**.

Another way to find the suffix is to run the following command on the target installation host to get the list of packages installed:

```
lslpp -l | grep powerbroker
```

Identify the suffix of the Privilege Management for Unix and Linux configuration package using this format:

```
powerbroker.config<suffix>
```

8. Navigate to the **/unzip-dir/powerbroker/version/flavor/package/** directory.
9. Run the AIX **installp** utility to install the Privilege Management for Unix and Linux component package or packages by typing:

```
installp -ad ./ powerbroker.package_name [v.v.r.bb] [powerbrokder.package_name [v.v.r.bb]
... ]
```

where:

- **package_name** is the name of the Privilege Management for Unix and Linux package to be installed.
- **v.v.r.bb** (optional) is the version, release, and build number, for example, 9.4.1.03.

10. Navigate to the **/unzip-dir/powerbroker/<version>/<flavor>/install/** directory.
11. Run the AIX **installp** command to install the Privilege Management for Unix and Linux configuration package by typing:

```
installp -ad ./ powerbroker.config<suffix>
```

<suffix> is the suffix that is set when you create the Privilege Management for Unix and Linux configuration package in step 7.

12. Commit the update package by typing:

```
installp -c powerbroker [v.v.r.bb]
```

v.v.r.bb (optional) is the version, release, and build number, for example, 9.4.1.03.

13. Verify the installation of the filesets with the AIX **lslpp** utility by typing:

```
lslpp -al powerbroker.package_name
```

package_name is the name of the Privilege Management for Unix and Linux package that you installed.

Reject an Update Package

You can reject an update package that has been applied but not committed by typing:

```
installp -r powerbroker.package_name [v.v.r.bb]
```

where:

- **package_name** is the name of the Privilege Management for Unix and Linux package that you want to reject.
- **v.v.r.bb** (optional) is the version, release, and build number, for example, 6.2.1.11 After an update package has been committed, you can not reject it.

Update Packages and WPARs

Installing update packages on workload partitions (WPARs) involves the same considerations as installing a baseline Privilege Management for Unix and Linux package on WPARs.

> For more information, please see *"Installation Procedure" on page 145*.

Upgrade the Configuration Package

When upgrading the configuration package (cfg pkg), some settings that are part of the package might need settings and configuration files copied from the existing installation to the staging host.

Files included in the cfg package:

- **pb.settings:** Hardcoded target location **/etc/pb.settings**.
- **pb.cfg:** Hardcoded target location **/etc/pb.cfg**.
- All the encryption key files defined for networkencryption, eventlogencryption, iologencryption, reportencryption, policyencryption, and restkeyencryption. By default, two key files are typically created:
  - **pb.key**
  - **pb.rest.key**

The sysadmin can define encryption with different key files in locations other than **/etc**. Therefore, when upgrading, and to retain what is installed on the target machine, look at all the encryption settings in **/etc/pb.settings**. Copy the settings to the **settings_ files** directory before running **pbinstall -z** and **pbcreate*cfgpkg**.

- Policy file if the target is a policy server.

Sample Execution for the AIX Package Installer

The sample execution shows the installation of a Privilege Management for Unix and Linux submit host, run host, and shared libraries using the Privilege Management for Unix and Linux AIX package installer.

This sample execution is divided into the following parts:

- Generate the Privilege Management for Unix and Linux settings files.
- Create the Privilege Management for Unix and Linux configuration package using the **pbcreateaixcfgpkg** program.
- Install the component packages using the **installp -ad** command.
- Install the configuration package using the **installp -ad** command.
- Use **syncwpar** to propagate additional AIX global environment packages to shared workload partitions (WPARs). WPARS are available with AIX v6.1 and higher.

Generate the Privilege Management for Unix and Linux Settings Files

This section of the execution shows the generation of the Privilege Management for Unix and Linux settings files (**pb.key**, **pb.cfg**, and **pb.settings**) and also displays the Privilege Management for Unix and Linux installation menu. This output was generated using the **pbinstall** program with the **-z** option.

Example:

```
# ./pbinstall -zlr
Starting pbinstall main() from /opt/bt_pkg/powerbroker/v9.4/pmul_aix52+_9.4.3-
18/install/.
aix52+
WARNING:
When creating configuration packages to be installed on AIX WPARs, care
must be taken to set log file directories to WPAR-writable partitions.
The default AIX shared WPAR has the following read-only and/or shared
partitions, although configuration can vary:
/usr /opt /proc
ThePrivilege Management for Unix and Linux log file default directory for AIX WPARs is
'/var/adm'.
         Privilege Management for Unix and Linux Settings File Generation

Please read thePrivilege Management for Unix and Linux Installation Instructions before
proceeding.

Checking MANIFEST against release directory

Press return to continue
The Registry Name Service ofPrivilege Management for Unix and Linux facilitates location
of other services within the PBUL enterprise with the aid of a centralized data
repository.
IMPORTANT: client registration is required if this is not the Primary Server and you
intend to use Registry Name Services.
Do you wish to utilize Registry Name Service? [yes]? no BeyondTrust Privilege Management
for Unix and Linux Installation Menu
```

```
             Opt   Description                              [Value]
             1   Install Everything Here (Demo Mode)?        [no]
             2   Install License Server?                     [no]
             3   Install Registry Name Services Server?      [no]
             4   Install Client Registration Server?         [no]
             5   Install Policy Server Host?                 [yes]
             6   Install Run Host?                           [yes]
             7   Install Submit Host?                        [yes]
             8   Install PBSSH                               [yes]
             10  Install Log Host?                           [yes]
             11  Enable Logfile Tracking and Archiving?      [yes]
             12  Is this a Log Archiver Storage Server?      [no]
             13  Is this a Log Archiver Database Server?     [no]
             14  Install File Integrity Monitoring Polic...  [no]
             15  Install REST Services?                      [yes]
             16  List of License Servers                     [*]
             19  Path to Password Safe 'pkrun' binary        []
             23  Install Synchronization program?            [yes]
             25  Install Secure GUI Host?                    [yes]
             26  Install Utilities: pbvi, pbnvi, pbmg, p...  [yes]
             27  Install pbksh?                              [yes]
             28  Install pbsh?                               [yes]
             29  Install man pages?                          [no]
             30  Will this host use a Log Host?              [yes]
             31  AD Bridge Integration?                      [no]
             37  Integration with BeyondInsight?             [no]
             55  Synchronization program can be initiate...  [yes]
             56  Daemons location                           [/usr/sbin]
             57  Number of reserved spaces for submit pr...  [80]
             58  Administration programs location           [/usr/sbin]
             59  User programs location                     [/usr/local/bin]
             60  GUI library directory                      [/usr/local/lib/pbbuilder]
             61  Policy include (sub) file directory        [/opt/pbul/policies]
             62  Policy file name                           [/opt/pbul/policies/pb.conf]
             65  Log Archive Storage Server name             []
             67  Log Archiver Database Server name           []
             69  Logfile Name Cache Database file path?     [/opt/pbul/dbs/pblogcache.db]
             70  REST Service installation directory?
[/usr/lib/beyondtrust/pb/rest]
             71  Install REST API sample code?               [no]
             73  Pblighttpd user                            [pblight]
             75  Pblighttpd user UID                         []
             76  Pblighttpd user GID                         []
             78  Configure systemd?                          [yes]
             79  Command line options for pbmasterd         [-ar]
             80  Policy Server Delay                        [500]
             81  Policy Server Protocol Timeout             [-1]
             82  pbmasterd diagnostic log                   [/var/log/pbmasterd.log]
             83  Eventlog filename                          [/var/log/pb.eventlog]
             84  Configure eventlog rotation via size?       []
             85  Configure eventlog rotation path?           []
             86  Configure eventlog rotation via cron?       [no]
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

155

TC: 12/7/2022

```
87   Validate Submit Host Connections?         [no]
88   List of Policy Servers to submit to       [kandor]
89   pbrun diagnostic log?                     [none]
90   pbssh diagnostic log?                     [none]
91   Allow Local Mode?                         [yes]
92   Additional secured task checks?           [no]
93   Suppress Policy Server host failover er...  [yes]
94   List of Policy Servers to accept from     [kandor]
95   pblocald diagnostic log                   [/var/log/pblocald.log]
96   Command line options for pblocald         []
97   Syslog pblocald sessions?                 [no]
98   Record PTY sessions in utmp/utmpx?        [yes]
99   Validate Policy Server Host Connections?  [no]
100  List of Log Hosts                         [kandor]
101  Command line options for pblogd           []
102  Log Host Delay                            [500]
103  Log Host Protocol Timeout                 [-1]
104  pblogd diagnostic log                     [/var/log/pblogd.log]
105  List of log reserved filesystems          [none]
106  Number of free blocks per log system fi...  [0]
107  Command line options for pbsyncd          []
108  Sync Protocol Timeout                     [-1]
109  pbsyncd diagnostic log                    [/var/log/pbsyncd.log]
110  pbsync diagnostic log                     [/var/log/pbsync.log]
111  pbsync sychronization time interval (in...  [15]
112  Add installed shells to /etc/shells       [no]
113  pbksh diagnostic file                     [/var/log/pbksh.log]
114  pbsh diagnostic file                      [/var/log/pbsh.log]
115  Stand-alone pblocald command              [none]
116  Stand-alone root shell default iolog      [/pbshell.iolog]




121  Use syslog?                               [yes]
122  Syslog facility to use?                   [LOG_AUTHPRIV]
123  Base Daemon port number                   [24345]
124  pbmasterd port number                     [24345]
125  pblocald port number                      [24346]
126  pblogd port number                        [24347]



129  pbsyncd port number                       [24350]
130  REST Service port number                  [24351]
131  Add entries to '/etc/services'            [yes]
132  Allow non-reserved port connections       [yes]
133  Inbound Port range                        [1025-65535]
134  Outbound Port range                       [1025-65535]
137  Network encryption options                [aes-256:keyfile=/etc/pb.key]
138  Event log encryption options              [none]
139  I/O log encryption options                [none]
140  Report encryption options                 [none]
```

```
              141   Policy file encryption options           [none]
              142   Settings file encryption type            [none]
              143   REST API encryption options              [aes-
256:keyfile=/etc/pb.re...]
              144   Configure with Kerberos v5?              [no]
              150   Enforce High Security Encryption?        [yes]
              151   Use SSL?                                 [yes]
              152   SSL Configuration?                       [requiressl]
              153   SSL pbrun Certificate Authority Directory? [none]
              154   SSL pbrun Certificate Authority File?    [none]
              155   SSL pbrun Cipher List?                   [HIGH:!SSLv2:!3DES:!MD5:@ST…]
              156   SSL pbrun Certificate Directory?         [none]
              157   SSL pbrun Certificate File?              [none]
              158   SSL pbrun Private Key Directory?         [none]
              159   SSL pbrun Private Key File?              [none]
              160   SSL pbrun Certificate Subject Checks?    [none]
              161   SSL Server Certificate Authority Direct... [none]
              162   SSL Server Certificate Authority File?   [none]
              163   SSL Server Cipher List?
[HIGH:!SSLv2:!3DES:!MD5:@ST...]
              164   SSL Server Certificate Directory?        [none]
              165   SSL Server Certificate File?             [/etc/pbssl.pem]
              166   SSL Server Private Key Directory?        [none]
              167   SSL Server Private Key File?             [/etc/pbssl.pem]
              168   SSL Server Certificate Subject Checks?   [none]
              169   SSL Certificate Country Code             [US]
              170   SSL Certificate State/Province           [AZ]
              171   SSL Certificate Location (Town/City)     [Phoenix]
              172   SSL Certificate Organizational Unit/Dep... [Security]
              173   SSL Certificate Organization             [BeyondTrust]
              174   Configure Privilege Management for Unix... [no]
              175   Install BeyondTrust built-in third-part... [yes]
              176   BeyondTrust built-in third-party librar... [/usr/lib/beyondtrust/pb]
              188   Use PAM?                                 [no]
              196   Allow Remote Jobs?                       [yes]
              197   UNIX Domain Socket directory             [none]
              198   Reject Null Passwords?                   [no]
              199   Enable TCP keepalives?                   [no]
              200   Name Resolution Timeout                  [0]
              N for the next menu page, P for the previous menu page, C to continue, X to
exit
Please enter a menu option [For technical support call 1-800-234-9072]> c

no such map in server's domain
No submitmasters was specified and no NIS netgroup called pbsubmitmasters found
Privilege Management for Unix and Linux needs to know the submitmasters(s) to work.
ThePrivilege Management for Unix and Linux programs need to know which Policy Server Host
(s) you have
decided to allow to act as submitmaster(s) for this machine.
Submitmasters take requests for secured tasks from Submit Hosts,
accept or reject them, and pass the accepted requests to a Run Host.
To locate submitmasters, programs look for a setting in the settings file
```

```
       containing the names of the submitmaster machines or a netgroup
       called pbsubmitmasters.

       Enter Policy Server list (submitmasters):  aix52-ca012-05.unix.symark.com
       no such map in server's domain
       No acceptmasters was specified and no NIS netgroup called pbacceptmasters found
       Privilege Management for Unix and Linux needs to know the acceptmasters(s) to work.

       ThePrivilege Management for Unix and Linux programs need to know which Policy Server Host
       (s) you have
       decided to allow to request execution of secured tasks to this machine.
       Hosts on the acceptmasters list are the Policy Server Hosts which are allowed
       to make secured task requests to this machine.

       To do this, programs look for a setting in the settings file containing the
       names of the acceptmasters machines or a netgroup called pbacceptmasters.

       Enter Incoming Policy Server list (acceptmasters):  aix52-ca012-05.unix.symark.com
       no such map in server's domain
       No log hosts was specified and no NIS netgroup called pblogservers foundPrivilege
       Management for Unix and Linux needs to know the log hosts(s) to work.

       ThePrivilege Management for Unix and Linux programs need to know which machine(s) you
       have selected as Log Host(s).  Log Hosts are hosts which Policy Servers
       select for Run Hosts to do event and I/O logging.

       To do this, pbmasterd looks for the setting logservers in the settings
       file. This setting contains the names of the Log Host machines or a netgroup.

       Current installation settings for Log Server(s):

       Enter Log Server list (logservers):  aix52-ca012-05.unix.symark.com

       Generating key file /opt/bt_pkg/powerbroker/v9.4/pmul_aix52+_9.4.3-18/install/settings_
       files/pb.key...

       Are all the installation settings correct [yes]?
       Generating config file /opt/bt_pkg/powerbroker/v9.4/pmul_aix52+_9.4.3-
       18/install/settings_files/pb.cfg
       Creating the settings file creation script
       Running settings file creation script
       Creating settings file /opt/bt_pkg/powerbroker/v9.4/pmul_aix52+_9.4.3-
       18/install/settings_files/pb.settings
       Generated settings files are in directory: /opt/bt_pkg/powerbroker/v9.4/pmul_aix52+_
       9.4.3-18/install/settings_files
       Privilege Management for Unix and Linux Settings File Generation completed successfully.
```

SALES: www.beyondtrust.com/contact   SUPPORT: www.beyondtrust.com/support   DOCUMENTATION: www.beyondtrust.com/docs   158

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or   TC: 12/7/2022
depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

Install Component Packages Using the installp Command

This section shows the execution of the **installp** command to install component packages for the submit host, run host, and shared libraries.

The execution text also includes copyright, trademark, trade secrets, and other legal text; however, those notices and text were removed from the following excerpt to save space:

Example:

```
# cd /opt/bt_pkg/powerbroker/v9.4/pbul_aix52+_9.4.3-18/package
# installp -ad ./ powerbroker.sharedlibs powerbroker.common powerbroker.runhost
powerbroker.submithost
+-----------------------------------------------------------------------------+
Pre-installation Verification...
+-----------------------------------------------------------------------------+
Verifying selections...done
Verifying requisites...done
Results...
SUCCESSES
---------
Filesets listed in this section passed pre-installation verification
and will be installed.
Selected Filesets
-----------------
powerbroker.common 9.4.3.18                  # BeyondTrust PowerBroker Comm...
powerbroker.runhost 9.4.3.18                 # BeyondTrust PowerBroker Run ...
powerbroker.sharedlibs 9.4.3.18              # BeyondTrust PowerBroker Shar...
powerbroker.submithost 9.4.3.18             # BeyondTrust PowerBroker Subm...
<< End of Success Section >>
+-----------------------------------------------------------------------------+
BUILDDATE Verification ...
+-----------------------------------------------------------------------------+
Verifying build dates...done
FILESET STATISTICS
------------------
4  Selected to be installed, of which:
4  Passed pre-installation verification
----
4  Total to be installed
+-----------------------------------------------------------------------------+
Installing Software...
+-----------------------------------------------------------------------------+
installp:  APPLYING software for:
powerbroker.common 9.4.3.18
Filesets processed:  1 of 4  (Total time:  1 secs).
installp:  APPLYING software for:
powerbroker.runhost 9.4.3.18
Filesets processed:  2 of 4  (Total time:  3 secs).
installp:  APPLYING software for:
powerbroker.submithost 9.4.3.18
sysck: 3001-036 WARNING:  File
```

```
     /usr/lib//libpbul_aca-xcoff64.so
     is also owned by fileset powerbroker.runhost.

sysck: 3001-036 WARNING:  File

     /usr/share/man/man8/pbclienthost_uuid.8
     is also owned by fileset powerbroker.runhost.

sysck: 3001-036 WARNING:  File

     /usr/lib//libpbul_aca-xcoff32.so
     is also owned by fileset powerbroker.runhost.

sysck: 3001-036 WARNING:  File

     /usr/sbin/pbclienthost_uuid
     is also owned by fileset powerbroker.runhost.

Filesets processed:  3 of 4  (Total time:  4 secs).
installp:  APPLYING software for:
powerbroker.sharedlibs 9.4.3.18
Finished processing all filesets.  (Total time:  5 secs).
+-----------------------------------------------------------------------------+
Summaries:
+-----------------------------------------------------------------------------+
Installation Summary
--------------------
Name                         Level           Part         Event         Result
-------------------------------------------------------------------------------
powerbroker.common           9.4.3.18        USR          APPLY         SUCCESS
powerbroker.runhost          9.4.3.18        USR          APPLY         SUCCESS
powerbroker.submithost       9.4.3.18        USR          APPLY         SUCCESS
powerbroker.sharedlibs       9.4.3.18        USR          APPLY         SUCCESS
```

Install the Configuration Package Using the installp Command

This section shows the execution of the AIX **installp -ad** command to install the configuration package. Following installation of the configuration package, the installation is verified by submitting the **pbrun id** command to Privilege Management for Unix and Linux, and the AIX **lslpp -l |grep powerbroker** command is used to list the Privilege Management for Unix and Linux packages that are installed.

The execution text also includes copyright, trademark, trade secrets, and other legal text; however, those notices and text were removed from the following excerpt to save space:

Example:

```
# cd /opt/bt_pkg/powerbroker/v9.4/pbul_aix52+_9.4.3-18/install
# installp -ad ./ powerbroker.configCLIENT1-9.4.3.18.bff
+-----------------------------------------------------------------------+
Pre-installation Verification...
+-----------------------------------------------------------------------+
Verifying selections...done
Verifying requisites...done
Results...
SUCCESSES
---------
Filesets listed in this section passed pre-installation verification
and will be installed.
Selected Filesets
-----------------
powerbroker.configCLIENT1 9.4.3.18        # BeyondTrust PowerBroker Unix...
<< End of Success Section >>
+-----------------------------------------------------------------------+
BUILDDATE Verification ...
+-----------------------------------------------------------------------+
Verifying build dates...done
FILESET STATISTICS
------------------
1  Selected to be installed, of which:
1  Passed pre-installation verification
----
1  Total to be installed
+-----------------------------------------------------------------------+
Installing Software...
+-----------------------------------------------------------------------+
installp:  APPLYING software for:
powerbroker.configCLIENT1 9.4.3.18
Reading pb.cfg...
Checking installation of dependent component packages...
'lppchk -f/-c' of package powerbroker.common succeeded
'lppchk -f/-c' of package powerbroker.runhost succeeded
'lppchk -f/-c' of package powerbroker.submithost succeeded
'lppchk -f/-c' of package powerbroker.sharedlibs succeeded
Looking for SuperDaemons to configure...
Finished looking for SuperDaemons to configure...
Removing PowerBroker service definitions (if any) from /etc/services.
Adding PowerBroker service definitions to /etc/services.
```

TC: 12/7/2022

```
Removing any PowerBroker definitions from SuperDaemon inetd file /etc/inetd.conf
Adding PowerBroker definitions to SuperDaemon configurations  /etc/inetd.conf.
Reloading SuperDaemon Configurations...
0513-095 The request for subsystem refresh was completed successfully.
Done Reloading SuperDaemon Configurations...
Updating Settings in database (if any)...

Checking installation of package: powerbroker.configCLIENT1
'lppchk -f/-c' of package powerbroker.configCLIENT1 succeeded
Finished processing all filesets.  (Total time:  5 secs).
+-----------------------------------------------------------------------------+
Summaries:
+-----------------------------------------------------------------------------+
Installation Summary
--------------------
Name                          Level         Part         Event        Result
-----------------------------------------------------------------------------
powerbroker.configCLIENT1     9.4.3.18      USR          APPLY        SUCCESS
powerbroker.configCLIENT1     9.4.3.18      ROOT         APPLY        SUCCESS
```

View a List of Installed Privilege Management for Unix and Linux Packages

To view a list of the installed Privilege Management for Unix and Linux packages, do the following:

```
# lslpp -l | grep powerbroker
```

A list similar to the one in the example below appears. The Privilege Management for Unix and Linux configuration package appears twice because there are **usr** and **root** package portions.

> **Example:**
>
> ```
> powerbroker.common        9.4.3.18  COMMITTED  BeyondTrust PowerBroker Common
> powerbroker.configCLIENT1
> powerbroker.runhost       9.4.3.18  COMMITTED  BeyondTrust PowerBroker Run
> powerbroker.sharedlibs    9.4.3.18  COMMITTED  BeyondTrust PowerBroker Shared
> powerbroker.submithost    9.4.3.18  COMMITTED  BeyondTrust PowerBroker Submit
> powerbroker.configCLIENT1
> ```

Perform a Cursory Test of Privilege Management for Unix and Linux on the AIX Global Environment

To perform a cursory test of Privilege Management for Unix and Linux on the AIX global environment, type the following:

```
# pbrun id
```

Results such as those shown in the example below are displayed:

> **Example:**
>
> ```
> uid=0(root) gid=0(system) groups=2(bin),3(sys),7(security),8(cron),10 (audit),11(lp),4
> (adm),1(staff),6(mail), 501(amanda)
> ```

View a List of WPARs

WPARs are a new feature of AIX and exist only in AIX v6.1 and higher. To view a list of WPARs, type the following:

```
# lswpar
```

A list similar to the one in the example below appears:

Example:

```
Name State Type Hostname Directory
---------------------------------------------
wpar01 A S wpar01 /wpars/wpar01
```

Use syncwpar to Propagate Additional Packages to Shared WPARs

The **syncwpar** command synchronizes all packages between the AIX global environment and shared workload partitions (WPARs). This section shows how to use **syncwpar** to propagate additional AIX global environment packages to shared WPARs. WPARs are a feature that exists only in AIX v6.1 and later.

Example:

```
# syncwpar wpar01
***************************************************************************
**
Synchronizing workload partition wpar01 (1 of 1).
***************************************************************************
**
Executing /usr/sbin/syncroot in workload partition wpar01. syncroot: Processing root part
installation status. syncroot: Synchronizing installp software.
+-----------------------------------------------------------------------------
+
Pre-installation Verification...
+-----------------------------------------------------------------------------
+
Verifying selections...done Verifying requisites...done Results...

SUCCESSES
---------
Filesets listed in this section passed pre-installation verification and will be
installed.

Selected Filesets
-----------------
powerbroker.configClient 6.2.0.1 # BeyondTrust PowerBroker Conf...

<< End of Success Section >>

+-----------------------------------------------------------------------------
+
BUILDDATE Verification ...
+-----------------------------------------------------------------------------
+
Verifying build dates...done FILESET STATISTICS
------------------
1 Selected to be installed, of which:
1 Passed pre-installation verification
----
1 Total to be installed



+-----------------------------------------------------------------------------
+
Installing Software...
+-----------------------------------------------------------------------------
+
```

```
installp: APPLYING software for: powerbroker.configClient 6.2.0.1

Reading pb.cfg...
Checking installation of dependent component packages... 'lppchk -f/-c' of package
powerbroker.common succeeded 'lppchk -f/-c' of package powerbroker.runhost succeeded
'lppchk -f/-c' of package powerbroker.submithost succeeded 'lppchk -f/-c' of package
powerbroker.sharedlibs succeeded Looking for SuperDaemons to configure...
Finished looking for SuperDaemons to configure...
Removing PowerBroker service definitions (if any) from /etc/services. Adding PowerBroker
service definitions to /etc/services.
Removing any PowerBroker definitions from SuperDaemon inetd file
/etc/inetd.conf
Adding PowerBroker definitions to SuperDaemon configurations /etc/inetd.conf. Reloading
SuperDaemon Configurations...
0513-095 The request for subsystem refresh was completed successfully. Done Reloading
SuperDaemon Configurations...
Checking installation of package: powerbroker.configClient 'lppchk -f/-c' of package
powerbroker.configClient succeeded Finished processing all filesets. (Total time: 2
secs).

+---------------------------------------------------------------------------
+
Summaries:
+---------------------------------------------------------------------------
+

Installation Summary
--------------------
Name Level Part Event Result
---------------------------------------------------------------------------
-
powerbroker.configClient 6.2.0.1 ROOT APPLY SUCCESS syncroot: Processing root part
installation status.
syncroot: Installp root packages are currently synchronized. syncroot: RPM root packages
are currently synchronized. syncroot: Root part is currently synchronized.
syncroot: Returns Status = SUCCESS
Workload partition wpar01 synchronized successfully. Return Status = SUCCESS.
```

Log in to Shared WPARs

Workload partitions (WPARs) are a feature that exists only in AIX v6.1 and higher.

To login to shared WPARs, type the following:

```
# clogin wpar01
```

Example: *A welcome message such as the one shown in the example below is displayed:*

```
* *
* Welcome to AIX Version 6.1! *
* *
```

Run a Cursory Test of Privilege Management on a Shared WPAR System

Workload partitions (WPARs) are a feature that exists only in AIX v6.1 and higher.

To run a cursory test of Privilege Management for Unix and Linux on a shared WPAR system, type the following:

```
# pbrun id
```

Results such as those shown in the example below are displayed:

> *Example:*
>
> ```
> uid=0(root) gid=0(system) groups=2(bin),3(sys),7(security),8(cron),10 (audit),11(lp)
> ```

Sample Removal of an AIX Package Installation

This section shows the execution of the AIX **installp -u** command to remove the Privilege Management for Unix and Linux packages.

Example:

```
# installp -u powerbroker
+-----------------------------------------------------------------------------+
Pre-deinstall Verification...
+-----------------------------------------------------------------------------+
Verifying selections...done
Verifying requisites...done
Results...
SUCCESSES
---------
Filesets listed in this section passed pre-deinstall verification
and will be removed.
Selected Filesets
-----------------
powerbroker.common 9.4.3.18                 # BeyondTrust PowerBroker Comm...
powerbroker.configCLIENT1 9.4.3.18          # BeyondTrust PowerBroker Unix...
powerbroker.runhost 9.4.3.18                # BeyondTrust PowerBroker Run ...
powerbroker.sharedlibs 9.4.3.18             # BeyondTrust PowerBroker Shar...
powerbroker.submithost 9.4.3.18             # BeyondTrust PowerBroker Subm...
<< End of Success Section >>
FILESET STATISTICS
------------------
5  Selected to be deinstalled, of which:
5  Passed pre-deinstall verification
----
5  Total to be deinstalled
+-----------------------------------------------------------------------------+
Deinstalling Software...
+-----------------------------------------------------------------------------+
installp:  DEINSTALLING software for:
powerbroker.configCLIENT1 9.4.3.18
Reading pb.cfg...
Looking for SuperDaemons to configure...
Finished looking for SuperDaemons to configure...
Removing PowerBroker service definitions (if any) from /etc/services.
Removing any PowerBroker definitions from SuperDaemon inetd file /etc/inetd.conf
Reloading SuperDaemon Configurations...
0513-095 The request for subsystem refresh was completed successfully.
Done Reloading SuperDaemon Configurations...
Filesets processed:  1 of 5  (Total time:  6 secs).
installp:  DEINSTALLING software for:
powerbroker.runhost 9.4.3.18
Filesets processed:  2 of 5  (Total time:  6 secs).
installp:  DEINSTALLING software for:
powerbroker.sharedlibs 9.4.3.18
Filesets processed:  3 of 5  (Total time:  7 secs).
installp:  DEINSTALLING software for:
```

```
powerbroker.submithost 9.4.3.18
Filesets processed:  4 of 5  (Total time:  7 secs).
installp:  DEINSTALLING software for:
powerbroker.common 9.4.3.18
Removing /opt/pbul
Finished processing all filesets.  (Total time:  8 secs).
+-----------------------------------------------------------------------------+
Summaries:
+-----------------------------------------------------------------------------+

Installation Summary
--------------------
Name                         Level            Part        Event       Result
-------------------------------------------------------------------------------
powerbroker.configCLIENT1    9.4.3.18         ROOT        DEINSTALL   SUCCESS
powerbroker.configCLIENT1    9.4.3.18         USR         DEINSTALL   SUCCESS
powerbroker.runhost          9.4.3.18         USR         DEINSTALL   SUCCESS
powerbroker.sharedlibs       9.4.3.18         USR         DEINSTALL   SUCCESS
powerbroker.submithost       9.4.3.18         USR         DEINSTALL   SUCCESS
powerbroker.common           9.4.3.18         USR         DEINSTALL   SUCCESS
```

Example of Using syncwpar to Propagate Package Removal From Shared WPARs

The **syncwpar** command synchronizes all packages between the AIX global environment and shared workload partitions (WPARs). This section shows an example of how to use the **syncwpar** command to propagate removal of AIX global environment packages from shared WPARs. WPARs are a feature that exists only in AIX v6.1 and higher.

*Note: When **syncwpar** is run and a Privilege Management configuration package is removed, the following message may display:*

"inulag: The file system has read permission only."

This message can be ignored.

Example:

```
# syncwpar wpar01
*************************************************************************
**
Synchronizing workload partition wpar01 (1 of 1).
*************************************************************************
**
Executing /usr/sbin/syncroot in workload partition wpar01. syncroot: Processing root part
installation status. syncroot: Synchronizing installp software.
+----------------------------------------------------------------------
+
```

SALES: www.beyondtrust.com/contact   SUPPORT: www.beyondtrust.com/support   DOCUMENTATION: www.beyondtrust.com/docs

171

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or   TC: 12/7/2022
depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

```
Pre-deinstall Verification...
+-----------------------------------------------------------------------------
+
Verifying selections...done Verifying requisites...done Results...

SUCCESSES
---------
Filesets listed in this section passed pre-deinstall verification and will be removed.

Selected Filesets
-----------------
powerbroker.configClient 6.2.0.1 # BeyondTrust PowerBroker Conf...

<< End of Success Section >> FILESET STATISTICS


------------------
1 Selected to be deinstalled, of which:
1 Passed pre-deinstall verification
----
1 Total to be deinstalled

+-----------------------------------------------------------------------------
+
Deinstalling Software...
+-----------------------------------------------------------------------------
+

installp: DEINSTALLING software for: powerbroker.configClient 6.2.0.1

Reading pb.cfg...
Looking for SuperDaemons to configure...
Finished looking for SuperDaemons to configure...
Removing PowerBroker service definitions (if any) from /etc/services. Removing any
PowerBroker definitions from SuperDaemon inetd file
/etc/inetd.conf
Reloading SuperDaemon Configurations...
0513-095 The request for subsystem refresh was completed successfully. Done Reloading
SuperDaemon Configurations...
inulag: The file system has read permission only. Finished processing all filesets.
(Total time: 1 secs).


+-----------------------------------------------------------------------------
+
Summaries:
+-----------------------------------------------------------------------------
+

Installation Summary
--------------------
Name Level Part Event Result
```

```
-------------------------------------------------------------------------------
-
powerbroker.configClient 6.2.0.1 ROOT DEINSTALL SUCCESS syncroot: Processing root part
installation status.
syncroot: Installp root packages are currently synchronized. syncroot: RPM root packages
are currently synchronized. syncroot: Root part is currently synchronized.
syncroot: Returns Status = SUCCESS
Workload partition wpar01 synchronized successfully. Return Status = SUCCESS.
```

Verify Removal of Privilege Management for Unix and Linux Packages

To verify that all Privilege Management for Unix and Linux packages were removed, type the following:

```
# lslpp -l | grep powerbroker
```

If all packages are removed, results such as those shown in the example below are displayed:

Example:

```
# <no output.>
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

173

TC: 12/7/2022

HP-UX Package Installer

This section describes how to install Privilege Management for Unix and Linux using a package installer for HP-UX 11i v1, 11i v2, or 11i v3. Use the HP-UX package installation if you want to install Privilege Management for Unix and Linux using the HP-UX Software Distributor (SD) on a local or remote computer.

> 📌 **Note:** *The Privilege Management for Unix and Linux HP-UX package installer that is described here is not compatible with the Privilege Management version 5 HP-UX depots. If the Privilege Management version 5 HP-UX depots are installed, you must remove them before installing the Privilege Management for Unix and Linux version 6 HP-UX depots.*

Prerequisites

To use the Privilege Management for Unix and Linux HP-UX package installer, you must have the following:

- Package tarball file for the appropriate Privilege Management for Unix and Linux flavor

> 📌 **Note:** *For the Privilege Management for Unix and Linux HP-UX package installer, the tarball files are cumulative. That is, an update tarball file contains a complete Privilege Management for Unix and Linux installation. It is not necessary to install a baseline version of Privilege Management for Unix and Linux before installing an update.*

- Root access or superuser privileges

> 📌 **Note:** *The Privilege Management for Unix and Linux HP-UX package installer does not support prefix/suffix installations.*

Plan Your Installation

When preparing to use the Privilege Management for Unix and Linux HP-UX package installer, you should be familiar with the following concepts and restrictions:

- **Depots** and **Filesets:** HP-UX packaged software is delivered as a single file called a depot (**.depot**) file. A depot can be thought of as a compressed file that contains one or more filesets. A fileset is a component of the software and may contain many files. Installing an HP-UX depot extracts the files from the filesets and writes them to the appropriate directory locations.
- **Component depot and component filesets:** A Privilege Management for Unix and Linux component fileset is a part of the Privilege Management for Unix and Linux component depot that installs a portion of the Privilege Management for Unix and Linux application. There are seven Privilege Management for Unix and Linux component filesets. In the following list, **arch** is the architecture of the target platform; for example, ia64A.
  - **PowerBroker-arch.LOGHOST:** Contains log host, **pbsync**, and **pbsyncd**.
  - **PowerBroker-arch.SHAREDLIBS:** Contains shared libraries.
  - **PowerBroker-arch.RESTHOST:** Contains REST API files.
  - **PowerBroker-arch.RNSSVR:** Contains Registry Name Service files.
  - **PowerBroker-arch.LICSVR:** Contains license server files.

- **PowerBroker-arch.MASTERHOST:** Contains policy server host, **pbsync**, and **pbsyncd**.
- **PowerBroker-arch.SUBMITHOST:** Contains submit host andPrivilege Management for Unix and Linux shells.
- **PowerBroker-arch.RUNHOST:** Contains run host andPrivilege Management for Unix and Linux utilities.

Which component filesets are required depends on the type of Privilege Management for Unix and Linux host you create, such as policy server host, submit host, and so on. You can select the types of Privilege Management for Unix and Linux hosts in the **pbinstall** installation menu, as shown in the following table:

Menu Selection	Required Components
Install everything here (demo mode)? = Yes	MASTERHOST
	RUNHOST
	SUBMITHOST
	LOGHOST
	GUIHOST
	SHAREDLIBS
Install Policy Server Host? = Yes	MASTERHOST
Install Run Host? = Yes	RUNHOST
Install Submit Host? = Yes	SUBMITHOST
Install Log Host? = Yes	LOGHOST
Install BeyondTrust built-in third-party libraries? = Yes	SHAREDLIBS
Install Registry Name Services Server? [yes]	RNSSVR
Install License Server? [yes]	LICSVR

- **Configuration depot:** HP-UX depot (separate from the component depot) that is used to install the following files:

  - **pb.settings:** Hardcoded target location **/etc/pb.settings**
  - **pb.cfg: Hardcoded target location /etc/pb.cfg**
  - All the encryption keyfiles defined for **networkencryption**, **eventlogencryption**, **iologencryption**, **reportencryption**, **policyencryption**, and **restkeyencryption**
  - By default, two key files are created: **pb.key** and **pb.rest.key**
  - The sysadmin can define multiple encryption with different keyfiles in locations other than **/etc**. To upgrade and retain settings on the target machine, view all encryption settings in **/etc/pb.settings** and copy the files to the **settings_files** directory before running **"pbinstall -z" and pbcreate*cfgpkg**
  - **pb.conf** (for policy server hosts)
- Diagnostic logs files

The Privilege Management for Unix and Linux configuration depot is created by the **pbcreatehpuxcfgpkg** program. The component filesets must be copied to the SD depot using the **swcopy** command before you copy the configuration fileset to the distribution depot.

- **SD Depot:** The SD depot is the software distribution depot, to which software depots are copied by using the HP-UX **swcopy** command prior to the installation of their filesets. By default, **/var/spool/sw** is the location of the SD depot.

- **pbinstall program:** To create the Privilege Management for Unix and Linux settings files, you use the **pbinstall** program with the **-z** (settings only) option. **pbinstall -z** only creates the settings files and is incompatible with the following command line options:

Option	Description
-b	Runs **pbinstall** in batch mode.
-c	Skip the steps that process or update the Privilege Management for Unix and Linux settings file.
-e	Runs install script automatically by bypassing the menu step of **pbinstall**.
-i	Ignores previous **pb.settings** and **pb.cfg** files.
-p	Sets the pb installation prefix.
-s	Sets the pb installation suffix.
-u	Install the utility programs.
-x	Creates a log synchronization host (that is, installs **pbsyncd**).

When you execute **pbinstall** with the **-z** option, you can see two menu items that are not otherwise available:

- **Enter existing pb.settings path:** Enables you to specify your own **pb.settings** file. **pbinstall** reads this settings file and populates the remaining menu choices. You can override some menu choices. If set to none, then **pbinstall** does not read a settings file. The remaining menu choices are populated with default values.
- **Enter directory path for settings file creation:** Enables you to specify an alternative output directory for the settings files. The default directory is **/unzip-dir/powerbroker/version/<flavor>/install/settings_files**, where **unzip-dir** is the directory where the package tarball file was unzipped and version is the Privilege Management for Unix and Linux version number.

  The behavior of **pbinstall -z** depends on whether certain additional command line options are specified:

- If no other command line options are specified, **pbinstall** initially presents a short version of the installation menu (items 1–8 only). Depending on the choices you make in these items, further menu items become available.
- If command line options **-g**, **-l**, **-m**, **-o**, **-r**, or **-w** are specified, **pbinstall** presents an expanded version of the installation menu that reflects the host types that you are configuring.

When running **pbinstall** with the **-z** option, the following menu items are preprogrammed and cannot be changed:

- Install man pages?
- Daemon location
- Administration programs location
- User programs location
- GUI library directory
- Policy include (sub) file directory
- User man page location
- Admin man page location
- Policy filename
- BeyondTrust built-in third-party library directory

In addition, the values of the following menu items determine the values of other menu items:

Options Preset When Running pbinstall -z	
Setting this menu option to Yes	**Sets these values to Yes**
Install Policy Server Host?	Install Synchronization? Synchronization can be initiated from this host?
Install Run Host?	Install Utilities?
Install Submit Host?	Install PBSSH? Install pbksh? Install pbsh? Will this host use a Log Host?
Install Log Host?	Install Synchronization? Synchronization can be initiated from this host?

If you plan to use Registry Name Service and are running **pbinstall -z** on a client host (non-primary server), you must perform client registration. This is necessary to properly set up the registry name service database. Client registration also requires that you collect from the Privilege Management for Unix & Linux primary server the following information:

- REST Application ID
- REST Application Key
- Primary server network name or IP address
- Primary License Server REST TCP/IP port
- Registration Client Profile name

> *Note: If you are using the package installer to install Privilege Management for Unix and Linux on a computer that already has an interactive Privilege Management for Unix and Linux installation on it, please see "Installation Considerations" on page 7 for additional considerations.*

RNS client registration: If Registry Name Services is enabled for Privilege Management for Unix and Linux, each client host (after the first server installation) needs to be registered with the Primary Registry Name Server. When using package installers on a target host, a post-install configuration script (**/opt/pbul/scripts/pbrnscfg.sh**) is provided to be manually executed on that host to properly register it. This post-install configuration script asks for information about the Primary Registry Name Server, including the Application ID (appid), Application Key (appkey), address/domain name, and the REST TCP/IP port number. This is the same information provided during the client registration part of a **pbinstall -z** install which generates the settings file.

If you prefer a more convenient method of registering RNS clients where the post-install configuration script is non-interactive, Privilege Management for Unix and Linux can save the relevant information in a hidden file during the settings-only run of **pbinstall**, bundle it with the configuration package, and automatically apply it to the target host when that package is installed. However, understand that this is not secure, but is available if the security-convenience trade-off is acceptable. To enable this, refer to the question regarding post-install configuration script displayed when running **pbinstall -z**.

> *For more complete **pbinstall** command-line options, please see the "Installation Programs" on page 212.*

Overview of Steps

Using the Privilege Management for Unix and Linux HP-UX package installer involves the following steps.

1. Unpack the Privilege Management for Unix and Linux HP-UX package tarball file.

2. Use the **pbinstall** program to create Privilege Management for Unix and Linux settings files.

3. Use the **pbcreatehpuxcfgpkg** program to create the Privilege Management for Unix and Linux configuration depot.

4. Use the HP-UX **swcopy** command to copy the Privilege Management for Unix and Linux component depot to the desired SD depot.

5. Use the HP-UX **swcopy** command to copy the Privilege Management for Unix and Linux configuration depot to the desired SD depot.

6. Use the HP-UX **swinstall** command to install the Privilege Management for Unix and Linux configuration depot. The dependencies that are identified in the configuration fileset will cause the appropriate component filesets to be installed as well.

7. If Registry Name Service is enabled and installed on a non-primary servery, run **/opt/pbul/scripts/pbrnscfg.sh** to register the host.

ℹ️ *For more detailed information on the above steps, please see "Installation Procedure" on page 178.*

Installation Procedure

To install Privilege Management for Unix and Linux using the HP-UX SD feature, do the following:

1. Extract the package tarball files into the **/unzip-dir/** directory by executing the following command:

   ```
   gunzip -c pmul_<flavor_version>_pkg.tar.Z | tar xvf -
   ```

2. Navigate to the **/unzip-dir/powerbroker/version/flavor/install/** directory.

3. Execute the following command:

   ```
   ./pbinstall -z
   ```

   You are asked if you want to use client registration. If you plan to enable Registry Name Service, and install on a host that is not designated as a primary server, you must run client registration.

   pbinstall then asks if you want to enable Registry Name Service.

   pbinstall displays the Privilege Management for Unix and Linux installation menu.

4. Make your menu selections. Note that the **Enter existing pb.settings path** menu option enables you to specify your own **pb.settings** file to use. Also, the **Enter directory path for settings file creation** menu option enables you to specify where to save the generated settings files. These menu options are available only when running **pbinstall** with the **-z** option. When the menu selection process is complete, **pbinstall** creates the following files in the specified location:

   - **pb.settings**
   - **pb.cfg**
   - **pb.key** (if encryption is enabled)
   - **pb.conf** (for policy server host)

5. Optional. For a Privilege Management for Unix and Linux client, if client-server communications are to be encrypted, replace the generated **pb.key** file with **pb.key** file from the policy server host. Also, copy any other required key files into the same directory.

6. Optional. For a policy server host, write a policy file (**pb.conf**) and place it in the directory with the other generated files. If you do not provide a **pb.conf** file, a **pb.conf** file with the single command **reject;** is generated and packaged.

Starting with v8.0, **pbinstall -z** can optionally install the default role-based policies and asks:

```
Installing default role-based policy pbul_policy.conf and pbul_functions.conf in <install_
dir>/settings_files
Would you like to use the default role-based policy in the configuration package?
```

Answer **Yes** for new installs only.

If you are upgrading an existing configuration package, to avoid overwriting your existing policy, answer **No**.

```
Use the default role-based policy [Y]?
```

If you answer **Yes**, the default **pb.conf**, **pbul_policy.conf** and **pbul_functions.conf** are created and installed on the policy server.

If you are installing over an existing installation, and have an existing policy in place, answer **No**.

7. Navigate to the **/unzip-dir/powerbroker/version/flavor/install/** directory.

8. Run the **pbcreatehpuxcfgpkg** utility by typing:

```
pbcreatehpuxcfgpkg [-d] -p depot-fileset-name -s directory
```

where:

- **-d** is an option that sets the component fileset dependency to **hppaD** rather than the default **hppaB**.
- **depot-fileset-name** is a user-specified name for the configuration fileset. The resulting fileset is **PowerBroker-Cfg.depot-fileset-name**.
- **directory** is the directory that contains the Privilege Management for Unix and Linux settings and configuration files to include in the configuration fileset.

The **pbcreatehpuxcfgpkg** utility creates the configuration depot with the file name **PowerBroker-Cfg-version.depot-fileset-name.depot**.

9. Navigate to the **/unzip-dir/powerbroker/version/flavor/package/** directory.

10. Run the HP-UX **swcopy** utility to copy the Privilege Management for Unix and Linux component depot to the desired SD depot by typing:

```
swcopy -s /path/PowerBroker-arch.depot PowerBroker-arch.FILESET [@ sd-directory]
```

where

- **path** is the absolute path to the directory that contains the Privilege Management for Unix and Linux component depot.
- **arch** is the target platform architecture.
- **FILESET** is the specific fileset to be copied; alternatively, use ***** instead of **PowerBroker-arch.FILESET** to copy all filesets.
- **sd-directory** is the desired SD directory; if you omit **@ sd-directory**, the default **/var/spool/sw** is used.

> 🔍 **Example:** *To copy only the log host component fileset:*
>
> ```
> # swcopy -s /unzip-dir/powerbroker/v9.4/pmul_hpux.hppa64_9.4.3/package/PowerBroker-
> hppa64-9.4.3.06.depot PowerBroker-hppa64.LOGHOST @ /var/spool/sw
> ```

> 🔍 **Example:** *To copy the log host and policy server host component filesets to the default SD depot:*
>
> ```
> # swcopy -s /unzip-dir/powerbroker/v9.4/pmul_hpux.hppa64_9.4.3-06/package/PowerBroker-
> hppa64-9.4.3.06.depot PowerBroker-hppa64.LOGHOST PowerBroker-hppa64.MASTERHOST
> ```

> 🔍 **Example:** *To copy all component filesets to the default SD depot:*
>
> ```
> swcopy -s /unzip-dir/powerbroker/v9.4/pmul_hpux.hppa64_9.4.3-06/package/PowerBroker-
> hppa64-9.4.3.06.depot\*
> ```

11. Run the HP-UX **swcopy** utility to copy the Privilege Management for Unix and Linux configuration fileset to the desired SD depot.

> 🔍 **Example:**
>
> ```
> # swcopy -s /unzip-dir/powerbroker/v9.4/pmul_hpux.hppa64_9.4.3-06/install/PowerBroker-
> Cfg-9.4.3.06.CLIENT.depot  PowerBroker-Cfg.CLIENT @ /var/spool/sw
> ```

12. Run the HP-UX **swinstall** utility to install the Privilege Management for Unix and Linux configuration fileset by typing:

```
swinstall PowerBroker-Cfg.depot-fileset-name
```

> 📌 **Note: depot-fileset-name** *is the configuration fileset name specified when the Privilege Management for Unix and Linux configuration package is created in step 8. Any component dependencies that are identified by the configuration fileset are automatically installed as well.*

> 📌 **Note:** *If you attempt to install filesets from more than one flavor onto a single system, the installation fails with an error message.*

13. Verify the installation of the filesets with the HP-UX **swverify** utility by typing one of the following commands:

```
swverify PowerBroker-arch
```

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

180

TC: 12/7/2022

```
swverify PowerBroker-Cfg
```

14. If Registry Name Service is enabled and installed on a non-primary server, register the host with the Primary Registry Name Server using a post-install configuration script. Gather the Application ID, Application Key, network name or IP address, and REST TCP/IP port of the primary server, then run the script to register the host and follow the prompts:

```
/opt/pbul/scripts/pbrnscfg.sh
```

> **Note:** Many of the HP-UX depot management commands display a message regarding where to find a log file that contains additional information. We recommend that you look at these log files, because some important diagnostic information appears in the log file but not in the utility's standard output.

> For more information, please see the following:
> - *"Plan Your Installation" on page 174"Plan Your Installation" on page 174*
> - *"Installation Process" on page 30*
> - *"pbcreatehpuxcfgpkg" on page 224*

Remove Privilege Management for Unix and Linux Filesets

Removing the Privilege Management for Unix and Linux depots completely uninstalls Privilege Management for Unix and Linux from a computer. Because the component filesets are dependencies of the configuration fileset, the configuration fileset must be removed first. To remove the Privilege Management for Unix and Linux filesets, do the following:

1. Remove the Privilege Management for Unix and Linux configuration fileset by typing:

```
swremove PowerBroker-Cfg.depot-fileset-name
```

> **Note: depot-fileset-name** is the name of the fileset that you specified when you created the configuration depot.

2. Remove the Privilege Management for Unix and Linux component filesets by typing:

```
swremove PowerBroker-arch
```

> **Note:** You can remove the configuration and component filesets in the same command, for example:
>
> ```
> swremove PowerBroker-Cfg.FILESET PowerBroker-arch
> ```

Remote Installation

Because the HP-UX SD system uses a daemon for software administration, you can install from a local depot to a remote machine, or install from a remote depot to a local machine. Additionally, you can install a depot to an *alternate root* and then remount the alternate root as an actual root on another node.

To install a depot on a remote system, you must have ACL access to that remote system; you can use the **swacl** command to manage these access controls. Use the **@** argument with the **swinstall** command.

> *Example:*
>
> ```
> swinstall PowerBroker-hppaB @ remotehost:/
> ```

To install a depot on an alternate root, you also use the **@** argument.

> *Example:*
>
> ```
> swinstall PowerBroker-hppaB @ /export/shared_root/node1
> ```

> *Note: For alternate root installation, you must run the **swconfig** utility on the actual node, after the alternate root is remounted as the node's actual root.*

> *For more information, please see the man pages for the HP-UX SD commands.*

Updating Privilege Management for Unix and Linux with Update Depots

The Privilege Management for Unix and Linux HP-UX package installer can be used to update an existing Privilege Management for Unix and Linux installation to a new version. The existing Privilege Management for Unix and Linux version should have been installed using the Privilege Management for Unix and Linux package installer.

Update Depot Considerations

Installing a Privilege Management for Unix and Linux update depot is similar to using the HP-UX package installer to install Privilege Management for Unix and Linux for the first time. Keep these considerations in mind when you prepare to upgrade Privilege Management for Unix and Linux:

- A Privilege Management for Unix and Linux HP-UX update depot contains a complete Privilege Management for Unix and Linux installation, not just the files that have changed since the previous release.
- Each Privilege Management for Unix and Linux update depot is cumulative; that is, it includes all previous update filesets that BeyondTrust released since the baseline version. Therefore, there is no need to install the previous update depots.
- A newer release can introduce features that use new settings or configurations. In which case, an upgrade of the configuration package of Privilege Management for Unix & Linux is also needed.

Unlike Privilege Management for Unix and Linux patches that are installed with **pbpatchinstall**, update filesets cannot be rolled back to a previous release. However, you can install an older fileset over a newer one, effectively rolling back to the older release.

Update Depot Procedure

Follow this procedure to update your installation of Privilege Management for Unix and Linux using the update depots:

1. Obtain the tarball file for the HP-UX update depots that are appropriate for your hardware. The tarball file name has the format **pmul_<flavor>-v.v.r-bb-update_pkg.tar.Z**, where:
   - **<flavor>** indicates the operating system and hardware architecture.
   - **v.v.r** is the major and minor version number and the release number.
   - **bb** is the build number.
2. Extract the depot files into the **/unzip-dir/** directory by executing the following command:

   ```
   tar xvfz pmul_<flavor_version>-update_pkg.tar.Z
   ```

3. Navigate to the **/unzip-dir/powerbroker/v<version>/<flavor>/install/** directory
4. Create the **settings_files** directory and change directory to that location.
5. To retain or correctly update the settings of the current installation, copy the following files from the target installation host into the **settings_files** directory you created in step 4:
   - /etc/pb.settings
   - /etc/pb.cfg
   - encryption keys defined in **pb.settings** for networkencryption, eventlogencryption, iologencryption, reportencryption, policyencryption, and restkeyencryption settings (if enabled)

> 📌 *Note: In a default installation, there are typically 2 key files created: **pb.key** and **pb.rest.key**.*

- policy file defined in **policyfile** setting in **pb.settings** (if the target installation is a Policy Server)

> 📌 *Note: In a default installation, the policy file is located in **/opt/pbul/policies/pb.conf**.*

6. Obtain the tarball file for the HP-UX update depots that are appropriate for your hardware. The tarball file name has the format **pmul_<flavor>-v.v.r-bb-update_pkg.tar.Z**, where:
   - **<flavor>** indicates the operating system and hardware architecture.
   - **v.v.r** is the major and minor version number and the release number.
   - **bb** is the build number.

7. Execute the following command to verify and update the installation settings in the **settings_files** directory:

```
./pbinstall -z
```

8. Obtain the tarball file for the HP-UX update depots that are appropriate for your hardware. The tarball file name has the format **pmul_<flavor>-v.v.r-bb-update_pkg.tar.Z**, where:
   - **<flavor>** indicates the operating system and hardware architecture.
   - **v.v.r** is the major and minor version number and the release number.
   - **bb** is the build number.

9. Create the upgrade configuration package by running the **pbcreatehpuxcfgpkg** utility:

```
pbcreatehpuxcfgpkg -p fileset-name
```

Use the current fileset-name of the installation to be upgraded. Use the fileset-name you provided during the initial package installation in step 8 of the .

Another way to find the fileset-name is to run the following command on the target installation host to get the list of packages installed:

```
swlist PowerBroker\*
```

Identify the fileset-name of the Privilege Management for Unix and Linux configuration package using this format:

```
PowerBroker-Cfg.<fileset-name>
```

10. Navigate to the directory: **/unzip-dir/powerbroker/version/flavor/package/**

11. Run the HP-UX **swcopy** utility to copy the Privilege Management for Unix and Linux component depot to the desired SD depot by typing:

```
swcopy -s /path/PowerBroker-arch.depot PowerBroker-arch.FILESET [@ sd-directory]
```

This is the absolute path to the directory that contains the Privilege Management for Unix and Linux component depot.

arch is the target platform architecture.

FILESET is the specific fileset to be copied. Alternatively, use ***** instead of **PowerBroker-arch.FILESET** to copy all filesets.

sd-directory is the desired SD directory. If you omit **@ sd-directory**, the default **/var/spool/sw** is used.

12. Navigate to the **/unzip-dir/powerbroker/version/flavor/install/** directory.

13. Run the HP-UX **swcopy** utility to copy the Privilege Management for Unix and Linux configuration fileset to the desired SD depot:

```
# swcopy -s /<cfgdepotdir>/PowerBroker-Cfg-<ver>.<filesetname>.depot  PowerBroker-
Cfg.<filesetname>
```

14. Run the HP-UX **swinstall** utility to install the Privilege Management for Unix and Linux component filesets by typing: **swinstall PowerBroker-arch**.

15. Verify the installation of the filesets with the HP-UX **swverify** utility by typing: **swverify PowerBroker-arch**.

Revert to a Previous Version

Unlike Privilege Management for Unix and Linux patches that are installed with **pbpatchinstall**, update depots cannot be rolled back to a previous release. However, you can install an older fileset over a newer one, effectively rolling back to the older release. To install older filesets over newer ones, use the following command:

```
swinstall -x allow_downdate=true PowerBroker-arch
```

This command restores the previous release. Repeat the command to restore earlier releases.

Upgrade Configuration Package

When upgrading the configuration package (cfg pkg), some settings that are part of the package might need settings and configuration files copied from the existing installation to the staging host.

Files included in the cfg package:

- **pb.settings:** Hardcoded target location **/etc/pb.settings**.
- **pb.cfg:** Hardcoded target location **/etc/pb.cfg**.
- All the encryption key files defined for networkencryption, eventlogencryption, iologencryption, reportencryption, policyencryption, and restkeyencryption. By default, two key files are typically created:
  - **pb.key**
  - **pb.rest.key**

  The sysadmin can define encryption with different key files in locations other than **/etc**. Therefore, when upgrading, and to retain what is installed on the target machine, look at all the encryption settings in **/etc/pb.settings**. Copy the settings to the **settings_files** directory before running **pbinstall -z** and **pbcreate*cfgpkg**.

- Policy file if the target is a policy server.

Generate the Privilege Management for Unix and Linux Settings Files

This section of the execution shows the generation of the Privilege Management for Unix and Linux settings files (**pb.key**, **pb.cfg**, and **pb.settings**) and also displays the Privilege Management for Unix and Linux installation menu. This output was generated using the **pbinstall** program with the **-z** option and selecting menu options to install a run host and a submit host:

Example:

```
# ./pbinstall -z
Starting pbinstall main() from /opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-
18/install/.
hpux.ia64
Privilege Management for Unix and Linux Settings File Generation

Please read thePrivilege Management for Unix and Linux Installation Instructions before
proceeding.

Checking MANIFEST against release directory

Press return to continue
The Registry Name Service of Privilege Management for Unix and Linux facilitates location
of other services within the pmul enterprise with the aid of a centralized
data repository.
IMPORTANT: client registration is required if this is not the Primary Server and you
intend to use Registry Name Services.
Do you wish to utilize Registry Name Service? [yes]? no
BeyondTrustPrivilege Management for Unix and Linux Installation Menu
Opt   Description                                [Value]
1     Install Everything Here (Demo Mode)?       [no]
2     Install License Server?                    [no]
3     Install Registry Name Services Server?     [no]
5     Install Policy Server Host?                [yes]
6     Install Run Host?                          [yes]
7     Install Submit Host?                       [yes]
9     Install sudo Policy Server?                [no]
10    Install Log Host?                          [yes]
14    Install File Integrity Monitoring Polic... [no]
N for the next menu page, C to continue, X to exit
Please enter a menu option [For technical support call 1-800-234-9072]> 7

Privilege Management for Unix and Linux executes secured tasks on hosts which are
designated as Run Hosts.  These hosts execute the commands using the pblocald daemon.

To allowPrivilege Management for Unix and Linux to execute a command, a host must be
configured as a Run Host.

Do you want this host to be a Run Host [no]? yes
BeyondTrustPrivilege Management for Unix and Linux Installation Menu
Opt   Description                                Value]
1     Install Everything Here (Demo Mode)?       [no]
2     Install License Server?                    [no]
3     Install Registry Name Services Server?     [no]
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

186

TC: 12/7/2022

```
5    Install Policy Server Host?              [yes]
6    Install Run Host?                        [yes]
7    Install Submit Host?                     [yes]
9    Install sudo Policy Server?              [no]
10   Install Log Host?                        [yes]
14   Install File Integrity Monitoring Polic... [no]
25   Install Secure GUI Host?                 [yes]
26   Install Utilities: pbvi, pbnvi, pbmg, p... [yes]
29   Install man pages?                       [no]
30   Will this host use a Log Host?           [yes]
31   AD Bridge Integration?                   [no]
55   Synchronization program can be initiate... [yes]
56   Daemons location                        [/usr/sbin]
59   User programs location                  [/usr/local/bin]
N for the next menu page, C to continue, X to exit
Please enter a menu option [For technical support call 1-800-234-9072]> 8
Privilege Management for Unix and Linux allows requests for secured tasks to be made on
hosts configured as Submit Hosts.

To have pbrun initiate requests for secured tasks, this host must be a Submit Host.

Do you want this host to be a Submit Host [no]? yes
BeyondTrustPrivilege Management for Unix and Linux Installation Menu
Opt   Description                             [Value]
1     Install Everything Here (Demo Mode)?    [no]
2     Install License Server?                 [no]
3     Install Registry Name Services Server?  [no]
4     Install Client Registration Server?     [no]
5     Install Policy Server Host?             [yes]
6     Install Run Host?                       [yes]
7     Install Submit Host?                    [yes]
8     Install PBSSH                           [yes]
9     Install sudo Policy Server?             [no]
10    Install Log Host?                       [yes]
11    Enable Logfile Tracking and Archiving?  [yes]
12    Is this a Log Archiver Storage Server?  [no]
13    Is this a Log Archiver Database Server? [no]
14    Install File Integrity Monitoring Polic... [no]
15    Install REST Services?                  [yes]
16    List of License Servers                 [*]
19    Path to Password Safe 'pkrun' binary    []
23    Install Synchronization program?        [yes]
25    Install Secure GUI Host?                [yes]
26    Install Utilities: pbvi, pbnvi, pbmg, p... [yes]
27    Install pbksh?                          [yes]
28    Install pbsh?                           [yes]
29    Install man pages?                      [no]
30    Will this host use a Log Host?          [yes]
31    AD Bridge Integration?                  [no]
37    Integration with BeyondInsight?         [no]
55    Synchronization program can be initiate... [yes]
56    Daemons location                        [/usr/sbin]
```

```
57   Number of reserved spaces for submit pr...    [80]
58   Administration programs location              [/usr/sbin]
59   User programs location                        [/usr/local/bin]
60   GUI library directory                         [/usr/local/lib/pbbuilder]
61   Policy include (sub) file directory           [/opt/pbul/policies]
62   Policy file name                              [/opt/pbul/policies/pb.conf]
65   Log Archive Storage Server name               []
67   Log Archiver Database Server name             []
69   Logfile Name Cache Database file path?        [/opt/pbul/dbs/pblogcache.db]
70   REST Service installation directory?          [/usr/lib/beyondtrust/pb/rest]
71   Install REST API sample code?                 [no]
73   Pblighttpd user                               [pblight]
75   Pblighttpd user UID                           []
76   Pblighttpd user GID                           []
78   Configure systemd?                            [yes]
79   Command line options for pbmasterd            [-ar]
80   Policy Server Delay                           [500]
81   Policy Server Protocol Timeout                [-1]
82   pbmasterd diagnostic log                      [/var/log/pbmasterd.log]
83   Eventlog filename                             [/var/log/pb.eventlog]
84   Configure eventlog rotation via size?         []
85   Configure eventlog rotation path?             []
86   Configure eventlog rotation via cron?         [no]
87   Validate Submit Host Connections?             [no]
88   List of Policy Servers to submit to           [kandor]
89   pbrun diagnostic log?                         [none]
90   pbssh diagnostic log?                         [none]
91   Allow Local Mode?                             [yes]
92   Additional secured task checks?               [no]
93   Suppress Policy Server host failover er...    [yes]
94   List of Policy Servers to accept from         [kandor]
95   pblocald diagnostic log                       [/var/log/pblocald.log]
96   Command line options for pblocald             []
97   Syslog pblocald sessions?                     [no]
98   Record PTY sessions in utmp/utmpx?            [yes]
99   Validate Policy Server Host Connections?      [no]
100  List of Log Hosts                             [kandor]
101  Command line options for pblogd               []
102  Log Host Delay                                [500]
103  Log Host Protocol Timeout                     [-1]
104  pblogd diagnostic log                         [/var/log/pblogd.log]
105  List of log reserved filesystems             [none]
106  Number of free blocks per log system fi...    [0]
107  Command line options for pbsyncd              []
108  Sync Protocol Timeout                         [-1]
109  pbsyncd diagnostic log                        [/var/log/pbsyncd.log]
110  pbsync diagnostic log                         [/var/log/pbsync.log]
111  pbsync sychronization time interval (in...    [15]
112  Add installed shells to /etc/shells           [no]
113  pbksh diagnostic file                         [/var/log/pbksh.log]
114  pbsh diagnostic file                          [/var/log/pbsh.log]
115  Stand-alone pblocald command                  [none]
```

```
116  Stand-alone root shell default iolog      [/pbshell.iolog]
121  Use syslog?                               [yes]
122  Syslog facility to use?                   [LOG_AUTHPRIV]
123  Base Daemon port number                   [24345]
124  pbmasterd port number                     [24345]
125  pblocald port number                      [24346]
126  pblogd port number                        [24347]
127  pbguid port number                        [24348]
128  Secure pbsguid port number                [24349]
129  pbsyncd port number                       [24350]
130  REST Service port number                  [24351]
131  Add entries to '/etc/services'            [yes]
132  Allow non-reserved port connections       [yes]
133  Inbound Port range                        [1025-65535]
134  Outbound Port range                       [1025-65535]
137  Network encryption options                [aes-256:keyfile=/etc/pb.key]
138  Event log encryption options              [none]
139  I/O log encryption options                [none]
140  Report encryption options                 [none]
141  Policy file encryption options            [none]
142  Settings file encryption type             [none]
143  REST API encryption options               [aes-256:keyfile=/etc/pb.re...]
144  Configure with Kerberos v5?               [no]
150  Enforce High Security Encryption?         [yes]
151  Use SSL?                                  [yes]
152  SSL Configuration?                        [requiressl]
153  SSL pbrun Certificate Authority Directory? [none]
154  SSL pbrun Certificate Authority File?     [none]
155  SSL pbrun Cipher List?                    [HIGH:!SSLv2:!3DES:!MD5:@ST…]
156  SSL pbrun Certificate Directory?          [none]
157  SSL pbrun Certificate File?               [none]
158  SSL pbrun Private Key Directory?          [none]
159  SSL pbrun Private Key File?               [none]
160  SSL pbrun Certificate Subject Checks?     [none]
161  SSL Server Certificate Authority Direct...  [none]
162  SSL Server Certificate Authority File?    [none]
163  SSL Server Cipher List?                   [HIGH:!SSLv2:!3DES:!MD5:@ST...]
164  SSL Server Certificate Directory?         [none]
165  SSL Server Certificate File?              [/etc/pbssl.pem]
166  SSL Server Private Key Directory?         [none]
167  SSL Server Private Key File?              [/etc/pbssl.pem]
168  SSL Server Certificate Subject Checks?    [none]
169  SSL Certificate Country Code              [US]
170  SSL Certificate State/Province            [AZ]
171  SSL Certificate Location (Town/City)      [Phoenix]
172  SSL Certificate Organizational Unit/Dep... [Security]
173  SSL Certificate Organization              [BeyondTrust]
174  Configure Privilege Management for Unix... [no]
175  Install BeyondTrust built-in third-part... [yes]
176  BeyondTrust built-in third-party librar... [/usr/lib/beyondtrust/pb]
188  Use PAM?                                  [no]
196  Allow Remote Jobs?                        [yes]
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

189

TC: 12/7/2022

```
197  UNIX Domain Socket directory                [none]
198  Reject Null Passwords?                       [no]
199  Enable TCP keepalives?                       [no]
200  Name Resolution Timeout                      [0]
N for the next menu page, P for the previous menu page, C to continue, X to exit
Please enter a menu option [For technical support call 1-800-234-9072]> c

ypcat:  no such map in server's NIS domain
No submitmasters was specified and no NIS netgroup called pbsubmitmasters found
Privilege Management for Unix and Linux needs to know the submitmasters(s) to work.
ThePrivilege Management for Unix and Linux programs need to know which Policy Server Host
(s) you have decided to allow to act as submitmaster(s) for this machine.
Submitmasters take requests for secured tasks from Submit Hosts,
accept or reject them, and pass the accepted requests to a Run Host.
To locate submitmasters, programs look for a setting in the settings file
containing the names of the submitmaster machines or a netgroup
called pbsubmitmasters.

Enter Policy Server list (submitmasters):  hp113-ca025-012.unix.symark.com
ypcat:  no such map in server's NIS domain
No acceptmasters was specified and no NIS netgroup called pbacceptmasters foundPrivilege
Management for Unix and Linux needs to know the acceptmasters(s) to work.

ThePrivilege Management for Unix and Linux programs need to know which Policy Server Host
(s) you have decided to allow to request execution of secured tasks to this machine.
Hosts on the acceptmasters list are the Policy Server Hosts which are allowed
to make secured task requests to this machine.

To do this, programs look for a setting in the settings file containing the
names of the acceptmasters machines or a netgroup called pbacceptmasters.

Enter Incoming Policy Server list (acceptmasters):  hp113-ca025-012.unix.symark.com
ypcat:  no such map in server's NIS domain
No log hosts was specified and no NIS netgroup called pblogservers found
Privilege Management for Unix and Linux needs to know the log hosts(s) to work.

ThePrivilege Management for Unix and Linux programs need to know which machine(s) you
have selected as Log Host(s).  Log Hosts are hosts which Policy Servers
select for Run Hosts to do event and I/O logging.

To do this, pbmasterd looks for the setting logservers in the settings
file. This setting contains the names of the Log Host machines or a netgroup.

Current installation settings for Log Server(s):

Enter Log Server list (logservers):  hp113-ca025-012.unix.symark.com

Generating key file /opt/pbpkg/powerbroker/v9.4/pbul_hpux.ia64_9.4.3-18/install/settings_
files/pb.key...

Are all the installation settings correct [yes]?
Generating config file /opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-
```

```
18/install/settings_files/pb.cfg
Creating the settings file creation script
Backed up existing settings file creation script to:
'/opt/pbpkg/powerbroker/v9.4/pbul_hpux.ia64_9.4.3-
18/install/pbcreatesettingsfile.ctime.May_26_15:05'
Running settings file creation script
Creating settings file /opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-
18/install/settings_files/pb.settings
Generated settings files are in directory: /opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_
9.4.3-18/install/settings_files
<MadCap:variable name="PM.PMUL" /> Settings File Generation completed successfully.
```

Create the Privilege Management for Unix and Linux Configuration Package Using pbcreatehpuxcfgpkg

This section shows the creation of the Privilege Management for Unix and Linux configuration depot using the **pbcreatehpuxcfgpkg** program with the **-p** and **-s** options.

> *Note: At the end of its output, the **pbcreatehpuxcfgpkg** script shows which Privilege Management for Unix and Linux component filesets need to be copied to the SD depot.*

Example:

```
# cd /opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-18/install
# ./pbcreatehpuxcfgpkg -p CLIENT1 -s /opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-
18/install/settings_files
pbcreatehpuxcfgpkg: starting from /opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-
18/install
pbcreatehpuxcfgpkg: keyfile pb.key will be included in package
pbcreatehpuxcfgpkg: reading /opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-
18/install/settings_files/pb.cfg
pbcreatehpuxcfgpkg: processing, please wait . . .

pbcreatehpuxcfgpkg: packaging PowerBroker Unix/Linux Configuration HP-UX Depot . . .
=======  05/26/17 15:19:42 PDT  BEGIN swpackage SESSION
* Session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com".

* Source:
pbul-qa-hpux11v3-01.unix.symark.com:/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-
18/install/PowerBroker-Cfg/psf/PowerBroker-Cfg.psf

* Target:
pbul-qa-hpux11v3-01.unix.symark.com:/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-
18/install/PowerBroker-Cfg/depot/PowerBroker-Cfg-9.4.3.18.CLIENT1.depot

* Software selections:
*
* Beginning Selection Phase.
* Reading the Product Specification File (PSF)
"/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-18/install/PowerBroker-
Cfg/psf/PowerBroker-Cfg.psf".

* Reading the product "PowerBroker-Cfg" at line 11.
* Reading the fileset "CLIENT1" at line 48.
NOTE:    The temporary target depot "/var/tmp/pkgAAA005165" has been
created.
* Selection Phase succeeded.
* Beginning Analysis Phase.
NOTE:    The fileset "PowerBroker-Cfg.CLIENT1" has a prerequisite
dependency on a software object which exists in another
```

🔍

```
   product, "PowerBroker-hppa64.RUNHOST", which was not selected
   for packaging and does not exist in the target depot.
   NOTE:    The fileset "PowerBroker-Cfg.CLIENT1" has a prerequisite
   dependency on a software object which exists in another
   product, "PowerBroker-hpia64.RUNHOST", which was not selected
   for packaging and does not exist in the target depot.
   NOTE:    The fileset "PowerBroker-Cfg.CLIENT1" has a prerequisite
   dependency on a software object which exists in another
   product, "PowerBroker-hppa64.SUBMITHOST", which was not
   selected for packaging and does not exist in the target depot.
   NOTE:    The fileset "PowerBroker-Cfg.CLIENT1" has a prerequisite
   dependency on a software object which exists in another
   product, "PowerBroker-hpia64.SUBMITHOST", which was not
   selected for packaging and does not exist in the target depot.
   NOTE:    The fileset "PowerBroker-Cfg.CLIENT1" has a prerequisite
   dependency on a software object which exists in another
   product, "PowerBroker-hppa64.SHAREDLIBS", which was not
   selected for packaging and does not exist in the target depot.
   NOTE:    The fileset "PowerBroker-Cfg.CLIENT1" has a prerequisite
   dependency on a software object which exists in another
   product, "PowerBroker-hpia64.SHAREDLIBS", which was not
   selected for packaging and does not exist in the target depot.
   NOTE:    One or more of the filesets you selected specify a dependency
   on software which exists in another product.  (See above).
   The other software was not selected for packaging and does not
   exist in the target depot.  (An unresolved dependency on
   another product may prevent the dependent product from being
   installed.)
   * Analysis Phase succeeded.
   * Beginning Package Phase.
   * Packaging the product "PowerBroker-Cfg".
   * Packaging the fileset "PowerBroker-Cfg.CLIENT1".
   * Package Phase succeeded.
   * Beginning Tapemaker Phase.
   * Copying the temporary depot to the tape
   "/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-18/install/PowerBroker-
   Cfg/depot/PowerBroker-Cfg-9.4.3.18.CLIENT1.depot".

   * Calculating the tape blocks required to copy the temporary
   depot to the tape
   "/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-18/install/PowerBroker-
   Cfg/depot/PowerBroker-Cfg-9.4.3.18.CLIENT1.depot".

   NOTE:    The temporary depot requires 220 Kbytes on the tape
   "/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-18/install/PowerBroker-
   Cfg/depot/PowerBroker-Cfg-9.4.3.18.CLIENT1.depot".

   * Writing the tape
   "/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-18/install/PowerBroker-
   Cfg/depot/PowerBroker-Cfg-9.4.3.18.CLIENT1.depot"
   (tape 1 of 1).
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

193

```
* Writing the fileset "PowerBroker-Cfg.CLIENT1" (1 of 1)
* Tape #1: CRC-32 checksum & size: 2376197741 225280
* Removing the temporary depot.
* Tapemaker Phase succeeded.
======  05/26/17 15:19:42 PDT  END swpackage SESSION
pbcreatehpuxcfgpkg: depot 'PowerBroker-Cfg-9.4.3.18.CLIENT1.depot' placed in
/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-18/install

pbcreatehpuxcfgpkg: the following depot filesets will need to be loaded to the target
system:
PowerBroker-{arch}.RUNHOST PowerBroker-{arch}.SUBMITHOST PowerBroker-{arch}.SHAREDLIBS
where {arch} is the appropriate architecture for the target system, 'hppa64' or 'ia64'.

pbcreatehpuxcfgpkg: completed.
```

Copy the Privilege Management for Unix and Linux Depots Using the swcopy Command

This section shows the execution of the **swcopy** command to copy the Privilege Management component and configuration depots to the default SD depot. This section also includes execution of the **swjob** and **swlist** commands to verify that the depots have been copied:

Example:

```
# swcopy -s /opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-18/package/PowerBroker-
hpia64-9.4.3.18.depot PowerBroker-hpia64.SHAREDLIBS PowerBroker-hpia64.SUBMITHOST
PowerBroker-hpia64.RUNHOST
=======  05/26/17 16:47:14 PDT  BEGIN swcopy SESSION (non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0263)
* Session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com".

* Beginning Selection
* "pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw":  This
target does not exist and will be created.
* Source:
/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-18/package/PowerBroker-hpia64-
9.4.3.18.depot

* Targets:
pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw
* Software selections:
PowerBroker-hpia64.RUNHOST,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
PowerBroker-hpia64.SHAREDLIBS,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
PowerBroker-hpia64.SUBMITHOST,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
* Selection succeeded.


* Beginning Analysis and Execution
* Session selections have been saved in the file
"/.sw/sessions/swcopy.last".
* The analysis phase succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
* The execution phase succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
* Analysis and Execution succeeded.


NOTE:   More information may be found in the agent logfile using the
command "swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0263
@ pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
=======  05/26/17 16:47:21 PDT  END swcopy SESSION (non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0263)
# swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0263 @ pbul-qa-hpux11v3-
01.unix.symark.com:/var/spool/sw
=======  05/26/17 16:47:15 PDT  BEGIN copy AGENT SESSION (pid=7319)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0263)
```

```
* Agent session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com". (pid=7319)
* Beginning Analysis Phase.
* Source:
pbul-qa-hpux11v3-01.unix.symark.com:/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-
18/package/PowerBroker-hpia64-9.4.3.18.depot

* Target:
pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw
* Target logfile:
pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw/swagent.log
* Reading source for product information.
* Reading source for file information.
NOTE:    The used disk space on filesystem "/var" is estimated to
increase by 91664 Kbytes.
This will leave 5407144 Kbytes of available user disk space
after the installation.
* Summary of Analysis Phase:
* 3 of 3 filesets had no Errors or Warnings.
* The Analysis Phase succeeded.
* Beginning the Copy Execution Phase.
* Filesets:         3
* Files:            105
* Kbytes:           90877
* Copying fileset "PowerBroker-hpia64.RUNHOST,r=9.4.3.18" (1 of
3).
* Copying fileset "PowerBroker-hpia64.SHAREDLIBS,r=9.4.3.18" (2
of 3).
* Copying fileset "PowerBroker-hpia64.SUBMITHOST,r=9.4.3.18" (3
of 3).
* Summary of Execution Phase:
* 3 of 3 filesets had no Errors or Warnings.
* The Execution Phase succeeded.
=======  05/26/17 16:47:21 PDT  END copy AGENT SESSION (pid=7319)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0263)
# swcopy -s /opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-18/install/PowerBroker-Cfg-
9.4.3.18.CLIENT1.depot PowerBroker-Cfg.CLIENT1
=======  05/26/17 16:49:48 PDT  BEGIN swcopy SESSION (non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0264)
* Session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com".

* Beginning Selection
* Target connection succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
* Source:
/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-18/install/PowerBroker-Cfg-
9.4.3.18.CLIENT1.depot

* Targets:
pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw
* Software selections:
```

```
PowerBroker-Cfg.CLIENT1,r=9.4.3.18,a=HP-UX_B.11.11/23/31_32/64_IA/PA,v=BeyondTrust
* Selection succeeded.


* Beginning Analysis and Execution
* Session selections have been saved in the file
"/.sw/sessions/swcopy.last".
* The analysis phase succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
* The execution phase succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
* Analysis and Execution succeeded.


NOTE:    More information may be found in the agent logfile using the
command "swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0264
@ pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
======= 05/26/17 16:49:48 PDT  END swcopy SESSION (non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0264)
# swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0264 @ pbul-qa-hpux11v3-
01.unix.symark.com:/var/spool/sw
======= 05/26/17 16:49:48 PDT  BEGIN copy AGENT SESSION (pid=7373)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0264)
* Agent session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com". (pid=7373)
* Beginning Analysis Phase.
* Source:
pbul-qa-hpux11v3-01.unix.symark.com:/opt/pbpkg/powerbroker/v9.4/pmul_hpux.ia64_9.4.3-
18/install/PowerBroker-Cfg-9.4.3.18.CLIENT1.depot

* Target:
pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw
* Target logfile:
pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw/swagent.log
* Reading source for product information.
* Reading source for file information.
NOTE:    The used disk space on filesystem "/var" is estimated to
increase by 232 Kbytes.
This will leave 5446360 Kbytes of available user disk space
after the installation.
* Summary of Analysis Phase:
* 1 of 1 filesets had no Errors or Warnings.
* The Analysis Phase succeeded.
* Beginning the Copy Execution Phase.
* Filesets:          1
* Files:             6
* Kbytes:          186
* Copying fileset "PowerBroker-Cfg.CLIENT1,r=9.4.3.18" (1 of 1).
* Summary of Execution Phase:
* 1 of 1 filesets had no Errors or Warnings.
* The Execution Phase succeeded.
======= 05/26/17 16:49:48 PDT  END copy AGENT SESSION (pid=7373)
```

```
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0264)
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

198

Install the Privilege Management for Unix and Linux Filesets Using the swinstall Command

This section shows the execution of the HP-UX **swinstall** command to install the Privilege Management for Unix and Linux filesets. Because the **swinstall** command automatically installs the dependent filesets, you need only run the **swinstall** command for the configuration fileset. Following installation of the configuration package, the installation is verified by submitting the **swlist**, **swjob**, and **swverify** commands. Finally, the **id** command is submitted to Privilege Management for Unix and Linux to test the installation.

> *Note: During the Privilege Management for Unix and Linux fileset installation process, you might see a warning message regarding "core transition links." You can ignore this warning.*

Example:

```
# swinstall PowerBroker-Cfg.CLIENT1
======= 05/26/17 16:50:39 PDT BEGIN swinstall SESSION
(non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0265)
* Session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com".

* Beginning Selection
* Target connection succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/".
* Source connection succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
* Source: /var/spool/sw
* Targets:  pbul-qa-hpux11v3-01.unix.symark.com:/
* Software selections:
PowerBroker-Cfg.CLIENT1,r=9.4.3.18,a=HP-UX_B.11.11/23/31_32/64_IA/PA,v=BeyondTrust
+ PowerBroker-hpia64.RUNHOST,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
+ PowerBroker-hpia64.SHAREDLIBS,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
+ PowerBroker-hpia64.SUBMITHOST,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
* A "+" indicates an automatic selection due to dependency or
the automatic selection of a patch or reference bundle.
* Selection succeeded.


* Beginning Analysis and Execution
* Session selections have been saved in the file
"/.sw/sessions/swinstall.last".
* The analysis phase succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/".
* The execution phase succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/".
* Analysis and Execution succeeded.


NOTE:   More information may be found in the agent logfile using the
command "swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0265
```

```
@ pbul-qa-hpux11v3-01.unix.symark.com:/".
======= 05/26/17 16:50:54 PDT  END swinstall SESSION (non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0265)
# swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0265 @ pbul-qa-hpux11v3-
01.unix.symark.com:/
======= 05/26/17 16:50:39 PDT  BEGIN install AGENT SESSION (pid=7464)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0265)
* Agent session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com". (pid=7464)
* Beginning Analysis Phase.
* Source:
pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw
* Target:            pbul-qa-hpux11v3-01.unix.symark.com:/
* Target logfile:
pbul-qa-hpux11v3-01.unix.symark.com:/var/adm/sw/swagent.log
* Reading source for product information.
* Reading source for file information.
* Executing preDSA command.
NOTE: The used disk space on filesystem "/" is estimated to increase by 24 Kbytes.
This will leave 205712 Kbytes of available user disk space after the installation.
NOTE: The used disk space on filesystem "/opt" is estimated to increase by 32 Kbytes.
This will leave 2466280 Kbytes of available user disk space after the installation.
NOTE: The used disk space on filesystem "/usr" is estimated to increase by 91552 Kbytes.
This will leave 3519968 Kbytes of available user disk space after the installation.
NOTE: The used disk space on filesystem "/var" is estimated to increase by 288 Kbytes.
This will leave 5410848 Kbytes of available user disk space after the installation.
* Summary of Analysis Phase:
* 4 of 4 filesets had no Errors or Warnings.
* The Analysis Phase succeeded.
* Beginning the Install Execution Phase.
* Filesets: 4
* Files:  111
* Kbytes:  91063
* Installing fileset "PowerBroker-hpia64.SUBMITHOST,r=9.4.3.18" because one or more other
selected filesets depend on it (1 of 4).
* Installing fileset "PowerBroker-hpia64.SHAREDLIBS,r=9.4.3.18" because one or more other
selected filesets depend on it (2 of 4).
* Installing fileset "PowerBroker-hpia64.RUNHOST,r=9.4.3.18" because one or more other
selected filesets depend on it (3 of 4).
* Installing fileset "PowerBroker-Cfg.CLIENT1,r=9.4.3.18" (4 of 4).
* Beginning the Configure Execution Phase.
NOTE: Reading pb.cfg...
NOTE: Looking for SuperDaemons to configure...
NOTE: Finished looking for SuperDaemons to configure...
NOTE: Removing PowerBroker service definitions (if any) from /etc/services.
NOTE: Adding PowerBroker service definitions to /etc/services
NOTE: Removing any PowerBroker definitions from SuperDaemon inetd file /etc/inetd.conf
NOTE: Adding PowerBroker definitions to SuperDaemon configurations /etc/inetd.conf
NOTE: Reloading SuperDaemon Configurations...
NOTE: Done Reloading SuperDaemon Configurations...
Updating Settings in database (if any)...
```

TC: 12/7/2022

```
* Summary of Execution Phase:
* 4 of 4 filesets had no Errors or Warnings.
* The Execution Phase succeeded.
=======  05/26/17 16:50:54 PDT  END install AGENT SESSION (pid=7464)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0265)

# swlist PowerBroker\*
# Initializing...
# Contacting target "pbul-qa-hpux11v3-01.unix.symark.com"...
#
# Target:  pbul-qa-hpux11v3-01.unix.symark.com:/
#
# PowerBroker-Cfg 9.4.3.18 BeyondTrust PowerBroker Unix/Linux - Root Delegation and
Privilege Management
PowerBroker-Cfg.CLIENT1 9.4.3.18 BeyondTrust PowerBroker Unix/Linux Configuration - Root
Delegation and Privilege Management
# PowerBroker-hpia64 9.4.3.18 BeyondTrust PowerBroker - Root Delegation and Privilege
Management
PowerBroker-hpia64.RUNHOST 9.4.3.18 BeyondTrust PowerBroker Run Host - Root Delegation
and Privilege Management
PowerBroker-hpia64.SHAREDLIBS 9.4.3.18 BeyondTrust PowerBroker Shared Libraries - Root
Delegation and Privilege Management
PowerBroker-hpia64.SUBMITHOST 9.4.3.18 BeyondTrust PowerBroker Submit Host - Root
Delegation and Privilege Management
# swverify PowerBroker-Cfg PowerBroker-hpia64
=======  05/26/17 16:52:13 PDT  BEGIN swverify SESSION
(non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0266)
* Session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com".

* Beginning Selection
* Target connection succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/".
* Software selections:
PowerBroker-Cfg.CLIENT1,l=/,r=9.4.3.18,a=HP-UX_B.11.11/23/31_32/64_IA/PA,v=BeyondTrust
PowerBroker-hpia64.RUNHOST,l=/,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
PowerBroker-hpia64.SHAREDLIBS,l=/,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
PowerBroker-hpia64.SUBMITHOST,l=/,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
* Selection succeeded.


* Beginning Analysis
* Session selections have been saved in the file
"/.sw/sessions/swverify.last".
* The analysis phase succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/".
* Verification succeeded.


NOTE: More information may be found in the agent logfile using the
```

```
command "swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0266
@ pbul-qa-hpux11v3-01.unix.symark.com:/".
======= 05/26/17 16:52:17 PDT  END swverify SESSION (non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0266)
# swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0266 @ pbul-qa-hpux11v3-
01.unix.symark.com:/
======= 05/26/17 16:52:14 PDT  BEGIN verify AGENT SESSION (pid=7787)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0266)
* Agent session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com". (pid=7787)
* Beginning Analysis Phase.
* Target:            pbul-qa-hpux11v3-01.unix.symark.com:/
* Target logfile:
pbul-qa-hpux11v3-01.unix.symark.com:/var/adm/sw/swagent.log
* Reading source for file information.
*    Configured    PowerBroker-hpia64.SUBMITHOST,l=/,r=9.4.3.18
*    Configured    PowerBroker-hpia64.SHAREDLIBS,l=/,r=9.4.3.18
*    Configured    PowerBroker-hpia64.RUNHOST,l=/,r=9.4.3.18
*    Configured    PowerBroker-Cfg.CLIENT1,l=/,r=9.4.3.18
* Summary of Analysis Phase:
Verified      PowerBroker-hpia64.SUBMITHOST,l=/,r=9.4.3.18
Verified      PowerBroker-hpia64.SHAREDLIBS,l=/,r=9.4.3.18
Verified      PowerBroker-hpia64.RUNHOST,l=/,r=9.4.3.18
Verified      PowerBroker-Cfg.CLIENT1,l=/,r=9.4.3.18
* 4 of 4 filesets had no Errors or Warnings.
* The Analysis Phase succeeded.
======= 05/26/17 16:52:17 PDT  END verify AGENT SESSION (pid=7787)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0266)
```

Sample of the Uninstall Process from a Package Installation

This section shows the execution of the HP-UX **swremove** utility to remove the Privilege Management for Unix and Linux depots. First, **swremove** is used to uninstall Privilege Management for Unix and Linux software from the host. Then, **swremove** is used to remove the Privilege Management for Unix and Linux depots from the SD depot:

Example:

```
# swremove PowerBroker-Cfg PowerBroker-hpia64
=======  05/27/17 09:54:20 PDT  BEGIN swremove SESSION
(non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0267)
* Session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com".

* Beginning Selection
* Target connection succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/".
* Software selections:
PowerBroker-Cfg.CLIENT1,l=/,r=9.4.3.18,a=HP-UX_B.11.11/23/31_32/64_IA/PA,v=BeyondTrust
PowerBroker-hpia64.RUNHOST,l=/,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
PowerBroker-hpia64.SHAREDLIBS,l=/,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
PowerBroker-hpia64.SUBMITHOST,l=/,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
* Selection succeeded.

* Beginning Analysis
* Session selections have been saved in the file
"/.sw/sessions/swremove.last".
* The analysis phase succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/".
* Analysis succeeded.

* Beginning Execution
* The execution phase succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/".
* Execution succeeded.

NOTE: More information may be found in the agent logfile using the
command "swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0267
@ pbul-qa-hpux11v3-01.unix.symark.com:/".
=======  05/27/17 09:54:26 PDT  END swremove SESSION (non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0267)
# swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0267 @ pbul-qa-hpux11v3-
01.unix.symark.com:/
=======  05/27/17 09:54:20 PDT  BEGIN remove AGENT SESSION (pid=16901)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0267)
* Agent session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com". (pid=16901)
* Beginning Analysis Phase.
* Target:  pbul-qa-hpux11v3-01.unix.symark.com:/
* Target logfile:
pbul-qa-hpux11v3-01.unix.symark.com:/var/adm/sw/swagent.log
```

```
* Reading source for file information.
* Summary of Analysis Phase:
* 4 of 4 filesets had no Errors or Warnings.
* The Analysis Phase succeeded.
* Beginning the Unconfigure Execution Phase.
* Filesets:           4
* Files:              111
* Kbytes:             91063
NOTE: Reading pb.cfg...
NOTE: Looking for SuperDaemons to configure...
NOTE: Finished looking for SuperDaemons to configure...
NOTE: Removing PowerBroker service definitions (if any) from /etc/services.
NOTE: Removing any PowerBroker definitions from SuperDaemon inetd file /etc/inetd.conf
NOTE: Reloading SuperDaemon Configurations...
NOTE: Done Reloading SuperDaemon Configurations...
* Beginning the Remove Execution Phase.
* Removing fileset "PowerBroker-Cfg.CLIENT1,l=/,r=9.4.3.18" (1 of 4).
* Removing fileset "PowerBroker-hpia64.RUNHOST,l=/,r=9.4.3.18" (2 of 4).
Removing /opt/pbul/scripts
* Removing fileset
"PowerBroker-hpia64.SHAREDLIBS,l=/,r=9.4.3.18" (3 of 4).
* Removing fileset
"PowerBroker-hpia64.SUBMITHOST,l=/,r=9.4.3.18" (4 of 4).
* Summary of Execution Phase:
* 4 of 4 filesets had no Errors or Warnings.
* The Execution Phase succeeded.
=======  05/27/17 09:54:26 PDT  END remove AGENT SESSION (pid=16901)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0267)
# swremove -d PowerBroker-Cfg PowerBroker-hpia64
=======  05/27/17 09:56:54 PDT  BEGIN swremove SESSION
(non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0268)
* Session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com".

* Beginning Selection
* Target connection succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
* Software selections:
PowerBroker-Cfg.CLIENT1,r=9.4.3.18,a=HP-UX_B.11.11/23/31_32/64_IA/PA,v=BeyondTrust
PowerBroker-hpia64.RUNHOST,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
PowerBroker-hpia64.SHAREDLIBS,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
PowerBroker-hpia64.SUBMITHOST,r=9.4.3.18,a=HP-UX_B.11.23/31_64_IA,v=BeyondTrust
* Selection succeeded.

* Beginning Analysis
* Session selections have been saved in the file
"/.sw/sessions/swremove.last".
* The analysis phase succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
* Analysis succeeded.
```

```
* Beginning Execution
* The execution phase succeeded for
"pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
* Execution succeeded.

NOTE:    More information may be found in the agent logfile using the
command "swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0268
@ pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw".
=======  05/27/17 09:56:54 PDT  END swremove SESSION (non-interactive)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0268)
# swjob -a log pbul-qa-hpux11v3-01.unix.symark.com-0268 @ pbul-qa-hpux11v3-
01.unix.symark.com:/var/spool/sw
=======  05/27/17 09:56:54 PDT  BEGIN remove AGENT SESSION (pid=17066)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0268)
* Agent session started for user
"root@pbul-qa-hpux11v3-01.unix.symark.com". (pid=17066)
* Beginning Analysis Phase.
* Target:
pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw
* Target logfile:
pbul-qa-hpux11v3-01.unix.symark.com:/var/spool/sw/swagent.log
* Reading source for file information.
* Summary of Analysis Phase:
* 4 of 4 filesets had no Errors or Warnings.
* The Analysis Phase succeeded.
* Beginning the Remove Execution Phase.
* Filesets:  4
* Files:  111
* Kbytes: 91063
* Removing fileset "PowerBroker-Cfg.CLIENT1,r=9.4.3.18" (1 of 4).
* Removing fileset "PowerBroker-hpia64.RUNHOST,r=9.4.3.18" (2 of 4).
* Removing fileset "PowerBroker-hpia64.SHAREDLIBS,r=9.4.3.18" (3  of 4).
* Removing fileset "PowerBroker-hpia64.SUBMITHOST,r=9.4.3.18" (4 of 4).
* Summary of Execution Phase:
* 4 of 4 filesets had no Errors or Warnings.
* The Execution Phase succeeded.
=======  05/27/17 09:56:54 PDT  END remove AGENT SESSION (pid=17066)
(jobid=pbul-qa-hpux11v3-01.unix.symark.com-0268)
```

Install Multiple Copies

It is possible to install multiple concurrent Privilege Management for Unix and Linux copies on the same machine. To install multiple copies, each copy must be a logically distinct installation. This type of installation is performed by using an installation prefix and/or suffix. Installing multiple, concurrent copies of Privilege Management for Unix and Linux affects the following:

- **pbinstall** and **pbuninstall**
- Remote installation using **pbmakeremotetar**
- Program names and execution
- Service names and port numbers
- NIS(+) netgroups
- Privilege Management for Unix and Linux settings file
- **root** policy file name
- Policy file contents
- Key file name
- Log file names

ℹ️ *For information about prefixed and suffixed installations, see "Prefix and Suffix Installation Instructions" on page 89.*

Remote Installation Using pbmakeremotetar with Prefixes and Suffixes

To make a remote tar archive using **pbmakeremotetar** for a prefixed installation, specify the prefix and/or suffix on the **pbmakeremotetar** command line with the **-p** and **–s** switches (as appropriate). The tar file name that is specified on the command line should be unique to avoid overwriting an existing tar archive.

Program Names and Execution

All program names are prefixed in a prefixed installation. **pblogd** is **{prefix}pblogd**, **pbdbutil** is **{prefix}pbdbutil**, and so forth. For example, if the prefix is **test**, **pbrun** is executed as follows:

```
testpbrun date
```

Suffixes are implemented in the same way.

Service Names and Port Numbers

All Privilege Management for Unix and Linux service names are prefixed or suffixed, or both. For example, using a prefix of **test**, the service name for **pblogd** is **testpblogd**. The entries are added to **/etc/services** by **pbinstall**.

Privilege Management for Unix and Linux service names and port numbers (whether prefixed, suffixed, or both) must be added manually to the NIS database on the NIS policy server.

When installing prefixed (and/or suffixed) installations of Privilege Management for Unix and Linux on a host with other Privilege Management for Unix and Linux installations, unique port numbers must be assigned for each installation. The installers do not check for unique port numbers and specifying overlapping ports may cause Privilege Management for Unix and Linux to function incorrectly.

NIS(+) Netgroup Names

All Privilege Management for Unix and Linux netgroup names (for example, **pblogservers**) are prefixed (for example, **{prefix}pblogservers**). Suffixes are added to the end of Privilege Management for Unix and Linux netgroup names.

Settings File

The **pb.settings** file name is prefixed with the prefix (for example, **/etc/{prefix}pb.settings**). Suffixes are added to the end of the filename. The installer work file name, **pb.cfg**, is also prefixed or suffixed.

root Policy Filename

The default root policy file name's basename is prefixed like any other Privilege Management for Unix and Linux component: **{prefix}pb.conf**. This enables the prefixed installation to have a policy file set that is separate from any other Privilege Management for Unix and Linux installation on the system. Suffixes are appended to the policy file name.

Policy File Contents

Client names (**pbrun**, **pbguid**, and **pbsguid**) are prefixed and/or suffixed like any other Privilege Management for Unix and Linux program. This means that any policy that checks for any of these clients must also take prefixes and/or suffixes into account.

If any Privilege Management for Unix and Linux programs are requested from the policy (that is, **pbrun** or **pbcall**), then the references to these programs must also be prefixed and/or suffixed. If the prefix or suffix is not specified, the default (unprefixed) installation of Privilege Management for Unix and Linux is used for the called **pbrun**, most likely with unintended results.

Policy subfiles may or may not be prefixed, depending on the needs of the installation.

Key File Name

The default key file name's basename is prefixed or suffixed like any other Privilege Management for Unix and Linux component: **{prefix}pb.key{suffix}**. This enables the prefixed or suffixed installation to have its own encryption key and be logically separate from any other Privilege Management for Unix and Linux installation on the system. If a different key file is specified in the **{prefix}pb.settings {suffix}** file and the **{prefix}pb.settings{suffix}** file is encrypted, then the default named **{prefix}pb.key{suffix}** must exist and is used to decrypt the **{prefix}pb.settings{suffix}** file.

Log File Names

For event logs, the default event log file name for a prefixed installation is **{prefix}pb.eventlog**. Event log files are prefixed and suffixed by default in the same way that the executable files are, unless the file names are overridden in the policy or the **pb.settings** file.

For error logs, the default error log for the Privilege Management for Unix and Linux daemons is **{prefix}{daemonname}.log**. Suffixes are placed before the **.log** part of the file name for daemon error log files.

I/O logs are not prefixed or suffixed unless specified in the policy. I/O logs have no default name. The name of these files must be explicitly set in the policy.

Man Pages

If man pages are installed in a prefixed and/or suffixed installation, then the man page file names have the prefix or suffix added to the file name, using the format: **{prefix}pbrun{suffix}.1**, where **1** is the section number of the man page. The text in the man page is not changed to reflect the prefix and/or suffix. In this example format, the displayed man page shows the command as **pbrun**, regardless of the prefix or suffix in use.

Sample Policy Files

The sample policy files are not renamed with a prefix or suffix, but the directory that they are stored in is changed to reflect the prefix or suffix. For instance, with a prefix of test, the default location for the sample policy files on Linux is **/usr/local/lib/testpbbuilder**.

Installation Verification

After you install Privilege Management for Unix and Linux, you should use the **pbbench** utility to identify any Privilege Management for Unix and Linux configuration, file permission, and network problems. **pbbench** reads and verifies the settings in the Privilege Management for Unix and Linux configuration file on the machine on which it is run. The **pbbench** utility uses system information, such as that found in **/etc/services** and **/etc/hosts** and/or NIS, to verify the information in the settings file.

The **pbbench** output can consist of informational, warning, and error messages. By default, this output appears on the monitor. It can be redirected to a file other than standard error using the command:

```
pbbench > filename
```

Example:

```
pbbench > pbbench.output
```

Only root users can run **pbbench** because it is treated as an administration program. By default, **pbbench** is installed in the **/usr/local/bin** directory.

To verify an installation using **pbbench**, do the following:

1. Start **pbbench** by executing the following command:

```
pbbench -V
```

2. If the utility does not report any warnings or errors, then the installation is complete. If **pbbench** returns warnings or errors, then identify and correct the problems, and rerun **pbbench**. Repeat this process until there are no problems.

Note: An error inhibits Privilege Management for Unix and Linux functionality, but a warning may or may not. All errors must be corrected, but it is only necessary to correct those warnings that affect Privilege Management for Unix and Linux operation.

3. If you are unable to correct the problems, contact BeyondTrust Technical Support.

*For more detailed information regarding **pbbench**, see Privilege Management for Unix and Linux Administration Programs in the Privilege Management for Unix and Linux System Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

Install Environment Variables

Privilege Management for Unix and Linux uses several environment variables to direct and modify the execution of programs and scripts. The following table describes these variables.

Variable	Description
COLUMNS	Specifies the width, in characters, of the current screen. This is used internally by the installation suite to request **ps**(1) (on most systems) to give more output on a line for the **ps –ef** command when determining current system state.
EDITOR	If the **VISUAL** environment variable is not set and this environment variable is set, then the specified editor becomes the default for editing files during the installation.
LINES	Specifies the number of lines on a page (screen). This variable is used on some systems by some programs to determine how many lines can be output.
PAGER	Specifies the page-viewing program. Use more, less, **pg**, or administrator-specified programs.
PATH	Specifies the locations of utilities such as **awk**, **fgrep**, **grep**, **gunzip**, **sed**, **tar**, **uncompress**, **wc**, and other Unix/Linux commands that are used by the installer.
ROWS	Used on some systems in place of the **LINES** environment variable. This usage is system dependant.
SHELL	Specifies the shell that is used by sub-shells of the installer. If specified, this should be **/bin/sh** or **/usr/bin/sh** as appropriate for your system.
SY_InstallBackupLimit	This variable limits the number of backup copies (the ***.sybak.####** files) of a given file that are allowed on a system for a given original file. The value of this environment variable must be an integer greater than or equal to 4. The default value (if this variable is not defined) is 10. The minimum value of 4 is necessary for internal installation suite processing. Some files (notably **/etc/services**) undergo two phases of processing. The first phase ensures that no entries that are relevant to the new installation exist in the file. The second adds any entries that are required by the new installation.
SY_InstallPageSize	Specifies the page size for the **pbinstall** menu page.
SY_InstallPageWidth	Specifies the page width for the **pbinstall** menu page.
TMPDIR	In addition to its traditional Unix and Linux usage, this variable specifies the directory of the **.cfg*** files that are produced and read by the installation suite. Files that are saved by **pbuninstall** can be saved in this directory. Temporary files that are created by the installation suite can also be created in this directory. The default value is **/tmp**. For some systems, and some sites which periodically clean out **/tmp**, this is an undesirable location for the installer files if an uninstallation or re-installation is being performed after these files have been removed. *Note: When a temporary directory is specified in* **pbinstall** *or* **Solrinstall***, TMPDIR is overwritten.* By design, Debian appears to clean **/tmp** when it boots. It is a good idea to point **TMPDIR** somewhere else, such as **/opt/beyondtrust/pb/TMPDIR**, after it is created for these systems during installation,

	pbmakeremotetar, and uninstallation processes.
VISUAL	Specifies the visual editor to use when editing parameter files during the installation process.

Installation Programs

This section describes the Privilege Management for Unix and Linux installation programs and their options.

pbinstall

pbinstall installs, updates, and configures all Privilege Management for Unix and Linux products. **pbinstall** is a menu-driven, interactive installation script. It enables the superuser installer to install, update, or reconfigure Privilege Management for Unix and Linux as required by configuration changes or updates. **pbinstall** properly configures (as appropriate) **/etc/services**, the superdaemon configuration files (**/etc/inetd.conf** and/or **/etc/xinetd.conf**), and Privilege Management for Unix and Linux for most execution environments.

An initial screen of legal information and credits is displayed, followed by a check to determine if the **VISUAL** or **EDITOR** environment variables select the editor to use during the installation. If you have not set either of these environment variables, then you are prompted to supply the path to an editor, with **vi** as the default.

Privilege Management for Unix and Linux is configured by a menu system with a menu of numbered selections and lettered options.

- To select an item to configure, type the number of that item and press **ENTER** to display the configuration prompts.
- To navigate the menu pages, use the following commands:
    - **C** Continue installation
    - **N** Next menu page
    - **P** Previous menu page
    - **R** Redraw menu (not shown due to space limitations)
    - **X** Exit script without performing any configuration
- After **C** is selected, you are asked if the settings are acceptable. If you indicate that they are not, then **pbinstall** returns to the configuration menu.
- If the settings are acceptable, then **pbinstall** asks if you want to view the generated installation script.

> **⚠ IMPORTANT!**
>
> *The generated installation script contains thousands of lines of code; therefore, viewing this script is recommended for advanced users only. To view the script, type **y**.*

- You are then asked if the generated installation script is to be executed. If it is not to be executed, then the name of that script is displayed and **pbinstall** exits. Otherwise, the script is immediately executed.

Multiple command line options can be used together. During an update installation, the **–m**, **–l**, **–r**, **–g**, and **–i** arguments have no effect and must be explicitly changed using the Privilege Management for Unix and Linux installation menu for **pbinstall**.

An update installation is an installation in which the previous Privilege Management for Unix and Linux version has not been uninstalled. It uses the same installation directories as the previous installation (including the **untar** and **unpack** occurring in the same directories as the previous installation if the distribution was using FTP), and uses the existing **pb.settings**, **pb.key**, and **pb.conf files**. If done properly, all (or almost all) of the previous installation parameters carry forward to the new installation.

Syntax

```
pbinstall [options]
```

Example:

```
pbinstall -h
```

Example:

```
pbinstall -L   hostname
```

Argument	Description
-a architecture	This option and its required argument explicitly specify which Unix or Linux architecture file to install. If the **–a** option is used, then the installer compares the expected flavor and the flavor that is specified with the **-a** option and displays a warning if they do not match. In Privilege Management for Unix and Linux v3.2 and earlier, the installation does not cross-check flavors. Beginning with Privilege Management for Unix and Linux v3.5, the installation script cross-checks flavors.
-A	Sets the Application ID for client registration.
-b	Runs **pbinstall** in batch mode. In batch mode, the specified existing and then default settings are automatically used. User intervention is not allowed and **hit enter** prompts are suppressed. This option also invokes **-e**.
-B	Specify base daemon port number.
-c	Causes **pbinstall** to skip the steps that process or update the Privilege Management for Unix and Linux settings file (**/etc/pb.settings**). This option is often used during the upgrade of an existing Privilege Management for Unix and Linux installation. The **/etc/pb.settings** file is not changed. It is backed up (to **/etc/pb.settings.sybak.####**) and replaced. Therefore, the creation and/or modification dates on the file may be changed.
-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 a production environment.
-D	Sets the address for the primary license server for client registration.
-e	Runs **pbinstall** automatically by bypassing the menu step of **pbinstall**. Bypassing the **pbinstall** menu step makes it impossible to change installation options or configurations.
-g	Creates a log host (that is, installs **pblogd**).

Argument	Description
-h	Prints the usage information for **pbinstall** and causes it to exit.
-i	Ignores previous **pb.settings** files.
-I [1]	Installs primary license server (infers -X and -Y).
-j <basedir>	This option defines the base directory for generated files/directories of Privilege Management for Unix and Linux which overrides the default **/opt/pbu**l directory.
-K	Sets the Application Key for client registration.
-l	Creates a run host (that is, installs **pblocald**).
-L host	This option with a following word argument specifies the hostname to be used in the **logservers** in **pb.settings**. A list of hosts can be specified by repeating the **-L** argument followed by the host: `-L host1 -L host2`
-m	Creates a policy server host (that is, installs **pbmasterd**).
-M host	This option with a following word argument specifies the hostame to be used in the **acceptmasters** and **submitmasters** in **pb.settings**. A list of hosts can be specified by repeating the **-M** argument followed by the host: `-M host1 -M host2`
-N	Set the Registration Profile name for client registration.
-O	Install the Privilege Management for Unix and Linux sudo wrapper. This option cannot be combined with other pbinstall options because sudo wrapper should be installed only after the other components are installed and configured. Before installing the sudo wrapper, you must ensure the PMUL policy is correctly configured for use with the sudo wrapper. ℹ️ *For more information, please see the Privilege Management for Unix and Linux Administration Guide.*
-p prefix	This option with a following word argument specifies an installation prefix for this installation.
-P	Sets the port for the primary license server for client registration.
-Q	Installs Primary Registry Name Server (infers **-S**, **-W** and **-X**).
-r	Creates a submit host; installs client software (**pbrun**, **pbsh**, **pbksh**).
-R directory	Specifies a base directory for applicable settings in the generated **pb.settings** file. Used with **-z** option only.
-s suffix	This option with a following word argument specifies an installation suffix for this installation.

Argument	Description
-S	Specifies **y** or **n** to enable or disable Registry Name Service.
-t	Set the temporary directory to be used during installation. When a temporary directory is defined, **TMPDIR** is overwritten, and the **tempfilepath** is included in **pb.settings**. ```-t /tmp/tempdir```
-u	Installs Privilege Management for Unix and Linux(**pbvi**, **pbless**, and so forth).
-v	Prints **pbinstall** version information and exits.
-W	Installs Registry Name Server.
-y <hostname>	Specifies license server(s) with one or more **-y <hostname>** arguments. **Note:** *The first host specified must be the primary license server.*
-Y	Installs license server.
-x	Creates a log synchronization host (that is, installs **pbsyncd**).
-X	Installs Client Registration Services
-z	Creates **pb.settings**, **pb.conf**, and (if applicable) **pb.key** files only. For use when installing Privilege Management for Unix and Linux with package installers. Cannot be combined with the **-b**, **-c**, **-e**, **-i**, **-o**, **-p**, **-s**. **-u**, **-w**, or **-x** options.
-Z	Installs File Integrity Policy Services

Files

Not applicable

> ℹ️ *For more information, please also see the following:*
> - *"pbmakeremotetar" on page 217*
> - *"pbuninstall" on page 230*

[1]This argument uses a capital "i".

run_pbinstall

run_pbinstall is a wrapper script for **pbinstall** that simplifies installation of Privilege Management for Unix and Linux components, providing a smaller set of options. It is meant to be used for fresh installation where it is acceptable to use default settings.

Syntax

```
run_pbinstall [options]
-a|b|c [--L host [-L host]...] [-M host [[-M host]...] [-p prefix] [-s suffix]
```

Example:

```
run_pbinstall -a
```

Example:

```
run_pbinstall -a -p adm1 -L lhost1 -L lhost2 -M mhost1
```

Arguments

`-a`	Install all components of Privilege Management for Unix and Linux. Equivalent to running **pbinstall -i -e -mgrlowux** .
`-b`	Install server (back-end) components of Privilege Management for Unix and Linux. It creates a policy server host (installs **pbmasterd**, log host (**pblogd**), and log synchronization host (**pbsyncd**). Equivalent to running **pbinstall -i -e -mgowx** .
`-c`	Install client components of Privilege Management for Unix and Linux. It creates a submit host (installs **pbrun**, **pbsh**, **pbksh**), run host (**pblocald**), and Privilege Management servers utility programs (**pbvi**, **pbless**, etc). Equivalent to running **pbinstall -i -e -rul**.
`-p prefix`	Specify Privilege Management installation prefix.
`-s suffix`	Specify Privilege Management installation suffix.
`-L hostname`	Specify log servers with one or more **-L <hostname>** arguments. The hostname is used for **logservers** in **pb.settings**.
`-M hostname`	Specify policy servers with one or more **-M <hostname>** arguments. The hostname is used for **acceptmasters** and **submitmasters** in **pb.settings**.
`-h`	Prints the usage information for **run_pbinstall** and exits.

pbmakeremotetar

pbmakeremotetar makes a clone of a configuration for a binary and configuration-compatible target environment for Privilege Management for Unix and Linux.

pbmakeremotetar is a menu-driven, interactive installation script. It enables the superuser installer to install, update, or reconfigure Privilege Management for Unix and Linux as required by configuration changes or updates. **pbmakeremotetar** properly configures (as appropriate) **/etc/services**, the superdaemon configuration files (**/etc/inetd.conf** and/or **/etc/xinetd.conf**), and Privilege Management for Unix and Linux for most execution environments.

pbmakeremotetar must be executed where the default directory is the directory in which **pbmakeremotetar** resides or the parent directory to the directory containing **pbmakeremotetar**.

An initial screen appears, reminding the user about the function of **pbmakeremotetar**. A prompt also appears, allowing a SIGINT (**CTRL+C**) to abort the script.

When the script continues, it determines the switches that are necessary for tar to function as desired. A list of files to transfer to the target system is generated and presented to the user for approval or editing.

When the file list is accepted, a tarball file that contains the selected files is created, with the specified **tarfilename** and with the additional file type of tar appended. The **remote_unpack** script is generated. Finally, a tarball file that contains both the first tarball file and the **remote_unpack** script is generated at the location that is specified by **tarfilename**.

After the final tarball file is created, it must be made available to the target systems. This can be done in any manner that preserves the security and binary integrity of the tarball file.

An installation work directory should be selected other than **/tmp** (for the same reasons as with **pbinstall**). The tarball file should be unpacked with the following commands:

```
$ cd {installation_directory}
$ tar -xvf {tarfilename_on_local_system}
$ ./remote_unpack
```

The **remote_unpack** script unpacks the encapsulated tarball file into the proper locations. The script then prompts you to allow the configuration of the system (**/etc/services**, superdaemon configuration files). If you allow this configuration, then these configuration files are automatically modified with the appropriate superdaemons instructed to reload their databases. If you decide not to do the configuration at this time, then the name of the script to continue with the configuration is displayed and the script exits.

For policy server target installations, an initial installation (using **pbinstall**) must be done before a target remote install. Doing so ensures the proper handling of all licensing issues.

Different target system installation (working) directories should be used for different prefix and/or suffix versions of cloned installations.

Encrypted policy files are not scanned for included policy files. You must process the encrypted policy files by restoring the unencrypted ones before running **pbmakeremotetar**, or by manually moving the encrypted files.

> 📌 **Note:** *If the settings file is encrypted, then **pbmakeremotetar** does not work. An unencrypted version of the settings file must be restored before **pbmakeremotetar** can work. An encrypted policy file is not handled properly.*

> ℹ️ *For details about including encrypted policy files or policy subfiles, please see "pbmakeremotetar Installation Information" on page 79.*

Syntax

```
pbmakeremotetar [options] tarfilename
```

> *Example:*
>
> ```
> pbmakeremotetar -h
> ```

Arguments

-a	Includes all Privilege Management for Unix and Linux installation types.
-b	Runs in batch mode (no confirmation prompts).
-c	Includes submit host software for target system.
-h	Displays this usage text and exits.
-l	Includes log host software for target system.
-m	Includes policy server software for target system.
-p prefix	Sets the Privilege Management for Unix and Linux installation prefix.
-r	Includes run host software for target system.
-s suffix	Sets the Privilege Management for Unix and Linux installation suffix.
-t	Rebuilds off of a previously generated file name list.
-v	Displays the script version and exits.
-w dirspec	Specifies the work directory to use when the directory containing pbmakeremotetar is read-only (for example, on a CD).
-x	Includes log synchronization host software for target system.
-A	Set the Application ID for RNS Client Registration.
-K	Set the Application Key for RNS Client Registration.
-D	Set the address of the primary server for RNS Client Registration.
-P	Set the port for the primary policy server for RNS Client Registration.
-N	Set the Registration Profile name for RNS Client Registration.
tarfilename	Specifies the name of the tarball file to create (may include the full path).

> *Note: Any combination of **-c**, **-g**, **-l**, **-r**, and **-m** may be specified if the current installation has those components.*

Registry Name Service (RNS) Support

Any new RNS-enabled Privilege Management for Unix and Linux installation must register with the RNS primary server to use the RNS features. **pbmakeremotetar** creates an RNS registration script to be included in the generated tar ball, and is extracted as **/opt/pbul/scripts/<prefix>pbrnscfg.sh<suffix>** by **remote_unpack** on the target host. **remote_unpack** also calls **pbremoteinstall**, which in turn, automatically invokes the RNS registration script. The script displays prompts asking for the necessary registration information (RNS Primary Server's **appid/appkey/address/port#**).

pbmakeremotetar also offers the user a choice to save their appid/appkey info to make it available for **pbrnscfg.sh**. However, this feature is provided only as a convenience. If you want to safeguard the appid/appkey info, decline **pbmakeremotetar**'s offer and just use the interactive prompt of **pbrnscfg.sh** when running on the target host.

If you are agreeable to saving the appid/appkey info, **pbmakeremotetar**creates the input file which is written to **/etc/.<prefix>pbrnscfg.in<suffix>** on the target host. The RNS registration script automatically looks for this hidden input file, thus skipping the interactive prompts.

Files

Not applicable

> ℹ️ *For more information, please also see the following:*

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

219

pbpatchinstall

- **[ver 5.1.2 and earlier]: pbpatchinstall** not available.
- **[ver 5.2 and later]: pbpatchinstall** available.

pbpatchinstall enables you to install and uninstall patches for installations that are running Privilege Management for Unix and Linux v4 and later.

> 📌 **Note:** *All Privilege Management for Unix and Linux daemons running a process during the patch installation should be stopped before using **pbpatchinstall** and restarted after using **pbpatchinstall**.*

Only root can run **pbpatchinstall**. It must be run from the install directory where the Privilege Management for Unix and Linux patch was untarred. For example, if you untarred the Privilege Management for Unix and Linux patch from the **/opt/beyondtrust** directory, the patch install directory is then **/opt/beyondtrust/powerbroker/v6.0/ pbx86_linuxA-6.0.0-16-sp1/install**.

pbpatchinstall should not be moved from this install directory because it is dependent on the included Privilege Management for Unix and Linux installer scripts (**sy_install_support** and **pb_install_support**) that are located there.

pbpatchinstall allows a Privilege Management for Unix and Linux patch to load if the patch release number differs from the Privilege Management for Unix and Linux installation release number. However, it does not allow a patch to load if the patch version does not match the Privilege Management for Unix and Linux installation major and minor version numbers.

pbpatchinstall does not run on Privilege Management for Unix and Linux versions earlier than v4.0 due to binary - version argument limitations. Also, **pbpatchinstall** does not report the binary version for executable files **pbnvi** or **pbuvqrpg**.

To uninstall a patch, go to the install directory where the patch was originally installed and execute **pbpatchinstall -u**. **pbpatchinstall** attempts to uninstall the patch version that is defined by the install directory where **pbpatchinstall** resides.

For example, if you run **pbpatchinstall** from the **/opt/beyondtrust/powerbroker/v5.1/ pbx86_linuxA-5.1.2-03-sp1/install** directory, **pbpatchinstall** attempts to uninstall the Privilege Management for Unix and Linux **pbx86_linuxA-5.1.2- 03-sp1** patch from that install directory.

If multiple patches are installed and you need to remove one or more of them, they must be removed in the reverse order from the order in which they were added.

Syntax

```
pbpatchinstall [options]
```

> 🔍 **Example:**
>
> ```
> pbpatchinstall -p test
> ```

This creates a Privilege Management for Unix and Linux installation using the prefix test.

Arguments

-a	This option and its required argument explicitly specify which Unix or Linux architecture file to install.

	If the **–a** option is used, then the installer compares the expected flavor and the flavor that is specified with the **-a** option and displays a warning if they do not match.
	In Privilege Management for Unix and Linux v3.2 and earlier, the installation does not cross- check flavors. Beginning with Privilege Management for Unix and Linux v3.5, the installation script cross-checks flavors.
-f	Forces the installation of the patch without a prompt, regardless of the release number.
-h	Displays the usage message and exits.
-p prefix	Sets the Privilege Management for Unix and Linux installation prefix.
-s suffix	Sets the Privilege Management for Unix and Linux installation suffix.
-u	Uninstalls the Privilege Management for Unix and Linux patch installation.
-v	Displays the version of **pbpatchinstall** and exits.

ℹ️ *For more information, please see the following:*
- *On Privilege Management for Unix and Linux version numbering, "Installation Considerations" on page 7."run_ pbinstall" on page 216*
- *"pbuninstall" on page 230*

pbcreateaixcfgpkg

- **[ver 6.1 and earlier]: pbcreateaixcfgpkg** not available.
- **[ver 6.2 and later]: pbcreateaixcfgpkg** available.

pbcreateaixcfgpkg creates an AIX lpp configuration package for BeyondTrust Privilege Management. **pbcreateaixcfgpkg** is a script that can be run interactively or non-interactively. The script enables a user to build a BeyondTrust Privilege Management AIX lpp configuration package, which is loaded along with one or more BeyondTrust Privilege Management AIX lpp component packages.

Unlike the Privilege Management AIX lpp component packages, which are created and distributed by BeyondTrust, AIX lpp configuration packages are created by the user. First, settings files must be created. This is accomplished by running **pbinstall** with the **-z** argument. Settings files are created by default in directory install/**settings_files**, although the user can specify the directory. The user may optionally put a policy file **pb.conf** in the **settings_files** directory to be included in the configuration package. After the settings files have been created, a user runs **pbcreateaixcfgpkg** from the Privilege Management install directory. **pbcreateaixcfgpkg** accepts the following arguments:

```
-h Help (this message) and exit.
-l Save (do not delete) package build directory.
-p User-specified lpp package name to be appended to powerbroker.config.
-s Settings files directory location.
-v Print version of pbcreateaixcfgpkg and exit.
```

If the **-p** or **-s** arguments are not supplied on the command line, the **pbcreateaixcfgpkg** script becomes interactive and prompts the user for input. The **-p** argument, user-specified package suffix, allows the user to suffix the package name with any name they wish, up to a total of 24 ASCII characters a-z, A-Z, 0-9 (including package base name config), For example, if the user enters **Client_Asia**, the configuration package is named **powerbroker.configClient_Asia**. If the length of the package name exceeds 24 characters, an error message is displayed, and the user is again prompted for the configuration package suffix.

The **-s** argument, settings files directory location, allows the user to specify the directory where the settings files to be included in the configuration package reside. The default value is **{pbinstall_directory}/settings_files**.

If the user wishes to include other Privilege Management installations keyfiles in the configuration package, the user needs to copy the keyfiles to the settings files directory prior to building the configuration package.

If a Privilege Management policy server configuration package is to be built, the user can include an existing policy file **pb.conf** in the settings files directory prior to building the config, the configuration package. If a Privilege Management policy server configuration package is to be built, the user can include an existing policy file **pb.conf** in the settings files directory prior to building the configuration package. If **pb.conf** is not included, a new **pb.conf** is created and packaged containing the entry:

```
reject;
```

The optional **-l** argument, save (do not delete) package build directory, allows the user to build the configuration package and not remove the package build directory, which is normally done after the package is built. The created package can be found in the current (install) directory, and will be the package name, for example, **powerbroker.configClient_Asia**, where the **-p** argument had been set to **Client_Asia**.

> 📌 *Note: Upon running **pbcreateaixcfgpkg**, the script informs the user as to which Privilege Management component packages need to be loaded on the target system. The Privilege Management configuration package does not load until the required component packages are loaded on the target system. AIX lpp packages are loaded using the **installp** command.*

Syntax

```
pbcreateaixcfgpkg [options]
```

Example:

```
pbcreateaixcfgpkg -v
```

Arguments

-h	Prints usage message and exits.
-l	Saves (does not delete) package build directory.
-p suffix	User-specified lpp package name to be appended to **powerbroker.config**.
-s directory	Settings files directory location.
-v	Prints version of **pbcreateaixcfgpkg** and exits.

ℹ️ For more information, please see *"run_pbinstall" on page 216*.

pbcreatehpuxcfgpkg

- **[ver 6.2 and earlier]: pbcreatehpuxcfgpkg** not available.
- **[ver 6.2.1 and later]: pbcreatehpuxcfgpkg** available.

pbcreatehpuxcfgpkg creates an HP-UX configuration depot for BeyondTrust Privilege Management. **pbcreatehpuxcfgpkg** is a script that can be run interactively or non-interactively. The script enables a user to build a BeyondTrust Privilege Management HP-UX configuration depot, which is loaded along with one or more BeyondTrust Privilege Management HP-UX component filesets.

Unlike the BeyondTrust HP-UX component depot, which is created and distributed by BeyondTrust, HP-UX configuration depots are created by the user. First, settings files must be created by running **pbinstall** with the **-z** argument. Settings files are created by default in directory install/**settings_files**, although the user can specify the directory. The user may optionally put a policy file **pb.conf** in the **settings_files** directory to be included in the configuration package. After the settings files have been created, user runs **pbcreatehpuxcfgpkg** from the Privilege Management for Unix and Linux install directory. **pbcreatehpuxcfgpkg** accepts the following arguments:

```
-d Set the component fileset dependency to hppaD rather than hppaB (default)
-h Help (this message) and exit.
-l Save (do not delete) depot build directory.
-p User-specified name for the configuration fileset.
-s Settings files directory location.
-v Print version of pbcreatehpuxcfgpkg and exit.
```

If one or both of the **-p** and **-s** arguments are not supplied on the command line, the **pbcreatehpuxcfgpkg** script becomes interactive and prompts you for input. The **-p** argument, user-specified fileset name, enables you to specify the configuration fileset name. The name can be between 4 and 15 ASCII characters (inclusive), and can be A-Z, 0-9, and the hyphen (-). The first character cannot be a hyphen. For example, if you specify **CLIENT-ASIA**, the configuration fileset is named **PowerBroker-Cfg[X].CLIENT-ASIA**. If the length of the fileset name is more than 15 or less than 4 characters, or if a hyphen is the first character, then an error message is displayed, and you are again prompted for the fileset name.

The **-s** argument, settings files directory location, enables you to specify the directory that contains the settings files to be included in the configuration package. The default value is **<pbinstall_directory>/settings_files**.

If you want to include other Privilege Management for Unix and Linux installations keyfiles in the configuration depot, you must copy the keyfiles to the settings files directory prior to building the configuration depot.

If a Privilege Management for Unix and Linux policy server configuration depot is to be built, you can include an existing policy file **pb.conf** in the settings files directory prior to building the configuration depot. If **pb.conf** is not included, a new **pb.conf** is created and packaged containing the entry:

```
reject;
```

The optional **-d** argument, set component fileset dependency to **hppaD** rather than **hppaB** (default), enables you to generate a Privilege Management for Unix and Linux configuration depot that can be used for either hppaD or ia64A systems. If you do not use this option, then **pbcreatehpuxcfgpkg** creates a configuration depot that can be used for either hppaB or ia64A systems.

> 📌 **Note:** *If you create configuration depots for different flavors, use the **-p** argument to specify different fileset names for each flavor.*

The optional **-l** argument, save (do not delete) depot build directory, enables you to build the configuration depot and not remove the depot build directory, which is normally removed after the depot is built. The created depot can be found in the current (install) directory, and is the depot name. For example, **PowerBroker-Cfg[X]-version.CLIENT-ASIA.depot**, where the **-p** argument had been set to **CLIENT-ASIA**.

Upon running **pbcreatehpuxcfgpkg**, note that the script informs you as to which Privilege Management for Unix and Linux component filesets need to be installed on the target system. The Privilege Management for Unix and Linux configuration package installs the required component filesets if they are not already installed, provided they have been copied into the appropriate SD depot. HP-UX depots are copied into the desired SD depot using the **swcopy** command and are installed using the **swinstall** command.

Syntax

```
pbcreatehpuxcfgpkg [options]
```

Example:

```
pbcreatehpuxcfgpkg -h
```

Arguments

-d	Generates a configuration depot that has, as its dependencies, component filesets for hppaD (these component filesets can also be used on ia64A systems).
	Without this argument, **pbcreatehpuxcfgpkg** generates a configuration depot that has, as its dependencies, component filesets for hppaB (which also can be used on ia64A systems).
-h	Prints usage message and exits.
-l	Saves (does not delete) package build directory.
-p depot _fileset_name	User-specified name for the configuration fileset. The resulting fileset is **PowerBroker-Cfg [X].depot-fileset-name**.
	The value of depot-fileset-name can be between 4 and 15 characters (inclusive), and allowed characters are A-Z, 0-9, and the hyphen (-); the first character cannot be a hyphen.
-s settings_files_directory _location	Settings files directory location.
-v	Prints version of **pbcreatehpuxcfgpkg** and exits.

For more information, please see *"run_pbinstall" on page 216*.

pbcreatelincfgpkg

- **[ver 5.2 and earlier]: pbcreatelincfgpkg** not available.
- **[ver 6.0 and later]: pbcreatelincfgpkg** available.

pbcreatelincfgpkg creates a Linux RPM installation package for Privilege Management for Unix and Linux configuration and settings files. Installing this package after the required Privilege Management for Unix and Linux component packages completes the Privilege Management for Unix and Linux package installation.

If the **-p** option or **-s** option is not specified, then you are prompted to supply these values.

The output from **pbcreatelincfgpkg** indicates which Privilege Management for Unix and Linux component packages must be installed before the Privilege Management for Unix and Linux configuration package.

After you create the configuration package with **pbcreatelincfgpkg**, you install the required component packages, then install the configuration package.

Syntax

```
pbcreatelincfgpkg [options]
```

> *Example:*
>
> ```
> pbcreatelincfgpkg -p SBM -s /opt/beyondtrust/powerbroker/v6.0/ pbx86_linuxB-6.0.0-
> 09/install/settings_files
> ```
>
> *This uses the Privilege Management for Unix and Linux settings and configuration files that are located in **/opt/beyondtrust/powerbroker/v6.0/pbx86_linuxB-6.0.0-09/ install/settings_files** and creates an RPM file (**powerbroker-configSBM-6.0.0-09-1- noarch.rpm**) in the current directory.*

Arguments

-h	Displays the usage message and exits.
-p package_suffix	Specifies a suffix of up to 18 characters to append to the configuration package name.
-s directory	Specifies the directory that contains the Privilege Management for Unix and Linux settings and configuration files to include in the package. The default value is **./settings_files**.
-v	Displays the version of **pbcreatelincfgpkg** and exits.

pbcreatesolcfgpkg

- **[ver 5.2 and earlier]: pbcreatesolcfgpkg** not available.
- **[ver 6.0 and later]: pbcreatesolcfgpkg** available.

pbcreatesolcfgpkg creates a Solaris installation package and corresponding package administration file for Privilege Management for Unix and Linux configuration and settings files. Installing this package after the required Privilege Management for Unix and Linux component packages completes the Privilege Management for Unix and Linux package installation.

If the **-p** option or **-s** option is not specified, then you are prompted to supply these values.

The output from **pbcreatesolcfgpkg** indicates which Privilege Management for Unix and Linux component packages must be installed before the Privilege Management for Unix and Linux configuration package.

After you create the configuration package with **pbcreatesolcfgpkg**, you install the required component packages, then install the configuration package.

Syntax

```
pbcreatesolcfgpkg [options]
```

Example:

```
pbcreatesolcfgpkg -p SBM -s /opt/beyondtrust/powerbroker/v6.0/ pbsparc_solarisC-6.0.0-
09/install/settings_files
```

*This example uses the Privilege Management for Unix and Linux settings and configuration files that are located in
/opt/beyondtrust/powerbroker/v6.0/pbsparc_solarisC-6.0.0-09/install/settings_ files and creates a datastream file
(**SYPBcfSBM.ds**) and package admin file (**SYPBcfSBM**) in the current directory.*

Arguments

-h	Displays the usage message and exits.
-l	Saves (does not delete) the spooled package directory, from which the package datastream (.ds) file is created. The spooled package directory is normally deleted after the datastream file is created. Saving the spooled package directory can help BeyondTrust Technical Support to diagnose installation problems.
-p package_suffix	Specifies a suffix to append to the file names of the Privilege Management for Unix and Linux configuration package file and package admin file. This suffix can be up to 26 characters in length (3 characters for unpatched Solaris 8).
-s directory	Specifies the directory that contains the Privilege Management for Unix and Linux settings and configuration files to include in the package. The default value is **./settings_files**.
-v	Displays the version of **pbcreatesolcfgpkg** and exits.

pblighttpd

The **pblighttpd_svc.sh** script is packaged in the distribution tar under **<installdir>/powerbroker/<version>/pbul_*/bin**.

When the REST service is installed and configured to continuously run in the background, the script is installed. It is required when at least one PMUL server component is present. If the installation is a PMUL client-only installation, it is configured to be managed by the superserver daemon, and there is no need for this script to be present.

By default, **pbinstall** places the script in **$inst_admindir** and is set to **/usr/sbin**. However, the location can be changed in the installation menu with the option **Where do you want the administrator programs installed?**.

The script is removed by **pbuninstall** from **$inst_admindir**.

This script should be installed with each server/client component package. Below are commands for each package type.

AIX

```
/usr/bin/startsrc -s ${prefix}pblighttpd${suffix}
/usr/bin/stopsrc -s ${prefix}pblighttpd${suffix}
```

Darwin

```
/bin/launchctl load "/Library/LaunchDaemons/com.beyondtrust.${prefix}pblighttpd${suffix}.plist"
/bin/launchctl unload "/Library/LaunchDaemons/com.beyondtrust.${prefix}pblighttpd${suffix}.plist"
```

Solaris

```
/usr/sbin/svcadm enable ${prefix}pblighttpd${suffix}
/usr/sbin/svcadm disable ${prefix}pblighttpd${suffix}


/etc/init.d/${prefix}pblighttpd${suffix} start
/etc/init.d/${prefix}pblighttpd${suffix} stopt
```

HP

```
/sbin/init.d/${prefix}pblighttpd${suffix} start
/sbin/init.d/${prefix}pblighttpd${suffix} stop
```

Linux

```
/bin/systemctl start ${prefix}pblighttpd${suffix}.service
/bin/systemctl stop ${prefix}pblighttpd${suffix}.service
```

```
/usr/sbin/service ${prefix}pblighttpd${suffix} start
/usr/sbin/service ${prefix}pblighttpd${suffix} stop

*: /etc/init.d/${prefix}pblighttpd${suffix} start
   /etc/init.d/${prefix}pblighttpd${suffix} stop
```

pbuninstall

pbuninstall is a menu-driven, interactive script that is used to uninstall Privilege Management for Unix and Linux. **pbuninstall** properly configures (as appropriate) **/etc/services** and the superdaemon configuration files (**/etc/inetd.conf** and/or **/etc/xinetd.conf**) for the removal of Privilege Management for Unix and Linux from most execution environments.

pbuninstall must be executed where the default directory is the directory in which **pbuninstall** resides, or the parent directory to the directory containing **pbuninstall**.

When **pbuninstall** is executed, you are presented with a reminder of the script's function and prompted: Hit return to continue. Using **CTRL+C** at this time stops the execution of the script.

> 📌 *Note: **pbuninstall** removes only those installations that are explicitly named on the command line. It must be run separately for each prefixed and suffixed installation.*

During execution, the script identifies files to move to **$TMPDIR** (log, policy, and configuration files), copies them to **$TMPDIR** (typically **/tmp**) and removes them from their original location. Files to be removed are removed.

/etc/services and the superdaemon configuration files have the appropriate Privilege Management for Unix and Linux configuration lines removed. The appropriate superdaemon processes are requested to reload their configuration files.

Syntax

```
pbuninstall [options]
```

> ℹ️ *For a **pbuninstall** execution example, see "Example of a pbuninstall Execution" on page 235.*

Arguments

-a	Explicitly sets the computer architecture.
-A appid	Allow the cleanup of RNS on the policy server.
-b	Runs in batch mode (no confirmation prompts).
-K appkey	
-h	Displays the usage message and exits.
-O	Uninstall sudo wrapper and leave other Privilege Management for Unix and Linux installed components intact. 📌 *Note: If uninstalling Privilege Management for Unix and Linux, pbuninstall automatically uninstalls sudo wrapper.* ℹ️ *For more information, please see the Privilege Management for Unix and Linux*

	ℹ️ *Administration Guide*.
-p prefix	Sets the Privilege Management for Unix and Linux installation prefix.
-s suffix	Sets the Privilege Management for Unix and Linux installation suffix.

Files

Not applicable

> ℹ️ *For more information, please also see the following:*
> - *"pbmakeremotetar" on page 217*
> - *"pbinstall" on page 212*

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

231

Upgrades and Reinstallations

The Privilege Management for Unix and Linux installers are designed to enable easy upgrades of an installed version to a new version. During an upgrade, the current Privilege Management for Unix and Linux configuration can be retained, or a new Privilege Management for Unix and Linux configuration can be put in place.

Privilege Management for Unix and Linux installation scripts **pbinstall** and **pbmakeremotetar** can also be used to perform upgrades and reinstallations.

If you want to return to an older version of Privilege Management for Unix and Linux or reinstall the current version with a different configuration, Privilege Management for Unix and Linux can be reinstalled to the current or older version without uninstalling, as long as the older version is 2.8.1 or later.

Pre-upgrade Instructions

Before performing an upgrade or reinstallation, do the following:

1. Obtain the new release, either on a CD or using FTP.
2. Read the release notes and installation instructions.
3. Determine the order for updating the policy server host machines. Note that **pbrun** clients need to be redirected to a new policy server host while their primary policy server host is updated. If your current Privilege Management for Unix and Linux installation includes policy server host failover machines, you may want to consider upgrading the policy server hosts failover machines first, followed by the submit hosts and run hosts, followed by the primary policy server hosts.

> 📌 **Note:** *The Privilege Management for Unix and Linux settings files on the policy server hosts may need to be updated as each policy server host is upgraded.*

4. If your current Privilege Management for Unix and Linux installation includes one or more policy server host failover machines, then ensure that the security policy files on the primary policy server host and the policy server host failover machines are synchronized.
5. Verify the current location of the Privilege Management for Unix and Linux administration programs, user programs, and log files. This information is in the **pb.cfg** file (**/etc/pb.cfg** or **pb/install/pb.cfg.{flavor}**) and the settings file, **/etc/pb.settings**.
6. If you do not have a recent backup of the host, or if it is imperative that no log entries can be lost, then create a save directory (for example, **/var/tmp/pb.{rev_rel}**) that can be used to restore Privilege Management for Unix and Linux files from in case the upgrade fails. After creating the directory, copy (do not use move) the files that are listed below to the new save directory (a shell script can be created to copy the necessary files).

Privilege Management for Unix and Linux files for all host types
/etc/services
/etc/pb.settings
/etc/pb.cfg (and **pb.cfg.*** on older installations)
/etc/pb.key (if encryption is in use on the system)
pb* log files (typically in **/var/adm**, **/var/log** or **/usr/adm**)

Privilege Management for Unix and Linux files Policy Server
/opt/pbul/policies/pb.conf
All included Security Policy Sub Files
Privilege Management for Unix and Linux database files (contents of **databasedir** which default to **/opt/pbul/dbs**)
/etc/inetd.conf (or your **xinetd**, **launchd**, or SMF configuration file)
Any event log or I/O log files to save

Privilege Management for Unix and Linux Submit Host and Run Host files
/etc/inetd.conf (or your **xinetd**, **launchd**, or SMF configuration file)

Privilege Management for Unix and Linux Log Server files
/etc/inetd.conf (or your **xinetd**, **launchd**, or SMF configuration file), **/etc/inetd.conf**
Any event log or I/O log files to save

Privilege Management for Unix and Linux GUI Host files
/etc/inetd.conf (or your **xinetd**, **launchd**, or SMF configuration file), **/etc/inetd.conf**

7. Determine in which directories to install the new Privilege Management for Unix and Linux log files, administration programs, and user programs. If you choose different directories for the Privilege Management for Unix and Linux programs, you might need to update the path variable for the root user and other users.

8. Be aware that users cannot submit monitored task requests while Privilege Management for Unix and Linux updates are in progress. Consider writing a Privilege Management for Unix and Linux configuration policy file that rejects all users from executing **pbrun** and echoes a print statement to their screen, informing them that a Privilege Management for Unix and Linux upgrade is in progress.

9. Privilege Management for Unix and Linux releases are always upward-compatible when encryption is not used. We recommend that you perform an uninstall if a release is replaced by a Privilege Management for Unix and Linux version older than 2.8.1.

10. If you use an encrypted settings file and intend to do an upgrade or reinstall, then the unencrypted version of the settings file needs to be restored before performing an upgrade or reinstall; otherwise, the settings file cannot be read.

11. If you have a previous installation of Privilege Management for Unix and Linux for v5.1 or earlier and your encryption is set to **none**, then when you install Privilege Management for Unix and Linux v5.2, all the encryption options (options 98 through 103) are set to **none**. You can change these options during installation.

ℹ️ *For more information on changing these options, please see* .

---

pbinstall Install Upgrades

To upgrade or reinstall Privilege Management for Unix and Linux with the same configuration as the currently installed version, run **pbinstall** in batch mode:

```
./pbinstall -b
```

If you perform a reinstall of an older version, be aware that the older version may not have the same features as the newer version. In this case, the upgrade process discards the configuration of the features that are not available in the older version of Privilege Management for Unix and Linux. When you upgrade to the newer version, make sure to configure the newer features when running **pbinstall**.

To change the configuration of Privilege Management for Unix and Linux during the upgrade or reinstall, run pbinstall in interactive mode:

```
./pbinstall
```

The present configuration is read into **pbinstall**. Make the desired configuration changes and then use the **c** command to continue. **pbinstall** then installs Privilege Management for Unix and Linux with the new configuration.

> **i** For step-by-step instructions for using pbinstall, please see *"Step-by-Step Instructions for a Basic Installation Using pbinstall" on page 42*.

pbmakeremotetar Install Upgrades and Reinstallations

Upgrading or reinstalling Privilege Management for Unix and Linux with **pbmakeremotetar** is the same process as installing with **pbmakeremotetar**. There is one difference to be aware of. In **pbinstall**, the in-place files are backed up as sybak files during the upgrade process; whereas in a **pbmakeremotetar** upgrade or reinstall, the files are overwritten.

Post-Upgrade Instructions

If you want to encrypt your settings file after upgrading Privilege Management for Unix and Linux, then save a copy of the unencrypted file (for future upgrades) and re-encrypt the settings file.

Patch Installations

> **i** For information on how to perform a patch installation, please see *"pbpatchinstall" on page 220*.

Uninstall Privilege Management for Unix and Linux

If **pbinstall** and **pbmakeremotetar** were used to install Privilege Management for Unix and Linux on the host, then use **pbuninstall** and the supporting files that were saved from the original **pbinstall** and **pbmakeremotetar** session to remove Privilege Management for Unix and Linux.

Privilege Management for Unix and Linux can be uninstalled by running the uninstall script **pbuninstall**. The uninstall scripts are located in the **powerbroker/<version>/<flavor>/install** directory. Running the uninstall script removes the appropriate product only from the machine that it runs on. Other Privilege Management for Unix and Linux hosts and concurrent (prefixed and/or suffixed) installations are not affected unless the other hosts rely upon the host that is performing the uninstall for Privilege Management for Unix and Linux services.

For example, uninstalling Privilege Management for Unix and Linux from the only (or last) policy server host will probably severely impact Privilege Management for Unix and Linux functionality on your network.

To successfully uninstall Privilege Management for Unix and Linux, you need access to the directory from which **pbinstall** was executed, and to the **pb.cfg** file. If the installation was from a CD-ROM, then the CD must be mounted. If the distribution was using FTP, then the original installation tree must exist or be restored if it was removed.

You should back up the installation directory tree and the directory that contains the created **pb.cfg** file before you remove them. If you remove these directories without first performing a backup, then contact BeyondTrust Technical Support for help.

If the distribution uses FTP and the environment variable **TMPDIR** is not set during the installation, then these two directory trees are the same. If the distribution uses a CD-ROM and **TMPDIR** is not set during the installation, then these files are created in **/tmp**.

The uninstall succeeds if the original files were not cleaned up before the uninstall or if the defaults were accepted during installation. If you intend to reinstall Privilege Management for Unix and Linux after the uninstall, then save copies, under different names, of any files you may want to look at later (for example, **/etc/pb.settings**).

The **pbuninstall** scripts, like the rest of the Privilege Management for Unix and Linux uninstallation suite, does not work with an encrypted settings file.

Example of a pbuninstall Execution

Example: The following listing shows the **pbuninstall** and execution:

```
# ./pbuninstall
Starting pbuninstall main() from /opt/beyondtrust/powerbroker/v6.0/pbx86_linuxB-6.0.0-
01/install/.
x86_linuxB

BeyondTrust PowerBroker Installation Removal

This script will remove PowerBroker programs and files from the system.
Hit return to continue

Looking for SuperDaemons to configure...
Finished looking for SuperDaemons to configure... Reading /etc/pb.cfg

Trying /etc/pb.settings

De-configuring system /etc/services and superdaemon configurations.
```

```
Removing PowerBroker 'prefix ' service definitions (if any) from /etc/services. Removing
any PowerBroker definitions from SuperDaemon xinetd file /etc/xinetd.conf

Restarting superdaemons

Reloading SuperDaemon Configurations...
Done Reloading SuperDaemon Configurations... Moving /etc/pb.settings to /tmp
Moving /etc/pb.conf to /tmp Moving /etc/pb.key to /tmp Moving /etc/pb.key to /tmp
Removing /usr/sbin/pbmasterd...
Removing /usr/local/man/man8/pbmasterd.8 ... Removing /usr/sbin/pblocald...
Removing /usr/local/man/man8/pblocald.8 ... Removing /usr/sbin/pbguid...
Removing /usr/local/man/man8/pbguid.8 ... Removing /usr/sbin/pblogd...
Removing /usr/local/man/man8/pblogd.8 ... Removing /usr/sbin/pbreport...
Removing /usr/local/man/man8/pbreport.8 ... Removing /usr/sbin/pbuvqrpg...
Removing /usr/local/man/man8/pbuvqrpg.8 ... Removing /usr/sbin/pbsyncd...
Removing /usr/local/man/man8/pbsyncd.8 ... Removing /usr/sbin/pbhostid...
Removing /usr/local/man/man8/pbhostid.8 ... Removing /usr/sbin/pbkey...
Removing /usr/local/man/man8/pbkey.8 ... Removing /usr/sbin/pbpasswd...
Removing /usr/local/man/man8/pbpasswd.8 ... Removing /usr/sbin/pbsum...
Removing /usr/local/man/man8/pbsum.8 ... Removing /usr/sbin/pblog...
Removing /usr/local/man/man8/pblog.8 ... Removing /usr/sbin/pbencode...
Removing /usr/local/man/man8/pbencode.8 ... Removing /usr/sbin/pblicense...
Removing /usr/local/man/man8/pblicense.8 ... Removing /usr/sbin/pbsync...
Removing /usr/local/man/man8/pbsync.8 ... Removing /usr/local/bin/pbcall...
Removing /usr/sbin/pbcheck...
Removing /usr/local/man/man8/pbcheck.8 ... Removing /usr/sbin/pbprint...
Removing /usr/local/man/man8/pbprint.8 ... Removing /usr/sbin/pbreplay...
Removing /usr/local/man/man8/pbreplay.8 ... Removing /usr/sbin/pbmerge...
Removing /usr/local/man/man8/pbmerge.8 ... Removing /usr/local/bin/pbrun...
Removing /usr/local/man/man1/pbrun.1 ... Removing /usr/local/bin/pbbench...


Removing /usr/local/man/man1/pbbench.1 ... Removing /usr/local/bin/pbksh...
Removing /usr/local/bin/pbsh...
Removing /usr/local/man/man8/pbinstall.8 ... Removing /usr/local/man/man8/pbuninstall.8
... Removing /usr/local/man/man8/pbmakeremotetar.8 ... Removing
/usr/local/man/man8/pbversion.8 ...
Removing /usr/local/man/man8/pbpatchinstall.8 ... Removing /usr/local/bin/pbless...
Removing /usr/local/man/man1/pbless.1 ... Removing /usr/local/bin/pbmg...
Removing /usr/local/man/man1/pbmg.1 ... Removing /usr/local/bin/pbnvi...
Removing /usr/local/man/man1/pbnvi.1 ... Removing /usr/local/bin/pbumacs...
Removing /usr/local/man/man1/pbumacs.1 ... Removing /usr/local/bin/pbvi...
Removing /usr/local/man/man1/pbvi.1 ... Moving /var/log/pbmasterd.log to /tmp Moving
/var/log/pblocald.log to /tmp Moving /var/log/pblogd.log to /tmp Moving
/var/log/pb.eventlog to /tmp Moving /var/log/pbguid.log to /tmp Moving /etc/pb.cfg to
/tmp
Moving /var/log/pbksh.log to /tmp Moving /var/log/pbsh.log to /tmp Moving
/var/log/pbsync.log to /tmp Moving /var/log/pbsyncd.log to /tmp
Removing pbguid html help and policy example files from '/usr/local/lib/pbbuilder'
Removing /usr/local/lib/pbbuilder -- empty BeyondTrust Created Directory
```

```
BeyondTrust PowerBroker Installation Removal was successful
PowerBroker configuration files and logs were moved to /tmp for removal
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

237

TC: 12/7/2022

Solr Installations

Solr can be used to index Privilege Management for Unix and Linux I/O logs to provide improved search capability. Indexing can be done on the I/O log files on the Privilege Management for Unix and Linux log server.

Installation Considerations

Solr is installed in a user-defined directory, and logs to a second user-defined directory. The defaults are **/opt/pbul-Solr** and **/var/log/Solr**.

Supported Platforms

Solr is supported on various Linux, AIX, HPUX and Solaris platforms.

> ℹ️ *For more information on the specific platforms supported, please see the Privilege Management for Unix and Linux ReadMe.*

Solr Java Requirements

- Solr 4.1 (included)
- Java 1.6+ JRE or JDK

System Requirements

- Disk: pmul Solr 4.1: 18MB
- Disk: Java 1.7: 58MB
- RAM: Solr - 2GB dedicated
- RAM: Java 1.7 - 64MB

Unix/Linux Utilities

The Privilege Management for Unix and Linux installer requires the following Unix and Linux utilities and built-in commands:

awk	cut	getopt	ps	sort	unset
basename	date	grep	pwd	stty	vi
cat	diff	id	read	tar	wc
cd	dirname	kill	rm	tee	xargs
chmod	df	ls	rmdir	touch	
chown	echo	mkdir	sed	tr	
cksum	eval	more	set	trap	
clear	exec	mv	shift	umask	
cp	export	od	sleep	uname	

System File Modifications

AIX: **/etc/inittab** modified, backed up prior as **inittab.bak.####**.

SSL Certificates and Search Interface

Solr can be installed with either BeyondInsight, or BeyondInsight for Unix and Linux. At this time, Solr cannot work with both, and cannot be changed from working with one to working with the other.
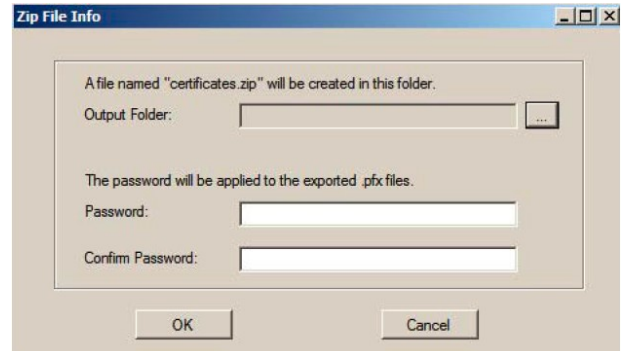
Prerequisites when Installing with BeyondInsight

Obtain the BeyondInsight Cert and CA files by copying the certificates from the BeyondInsight Windows Server machine to the Solr host machine:

1. Start the BeyondInsight Configuration Tool on the BeyondInsight Windows Server machine.
2. Click **Generate Certificate Zip** in the BeyondInsight Configuration Tool.
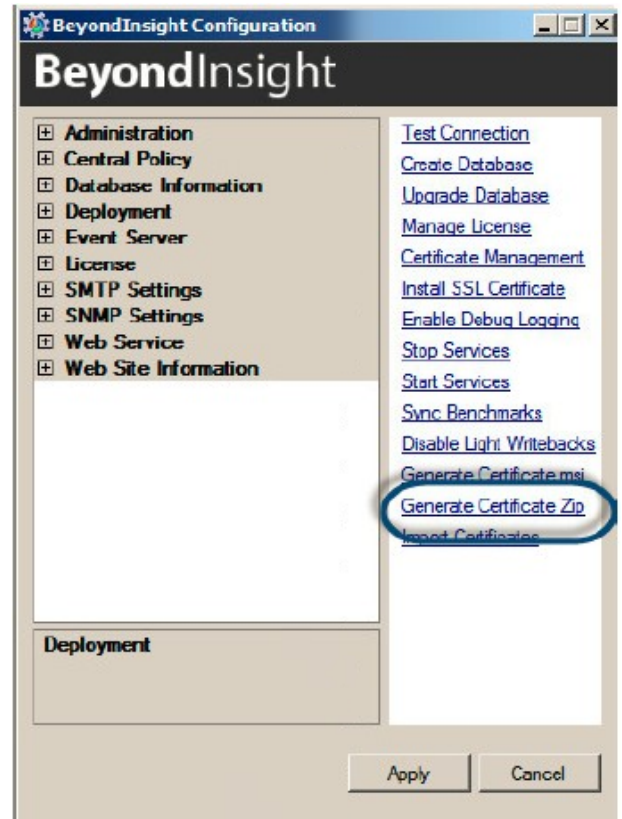
3. Select the output folder for the ZIP file and a password to apply to the exported .pfx file. This password is not used during the Solr install.

4. Select a folder where you can securely copy the file, and move it to your Unix or Linux server where you are planning to install Solr.

Command Line Options

When installing with BeyondInsight, an installation menu can be used to specify all options. When installing with BeyondInsight for Unix and Linux, or with manually generated certificates, the **-M** option at a minimum must be specified on the command line. Other options are available both on the command line and via menu.

Options for Use with BeyondInsight

-a rcsuser	Specify RCS Admin user.
-A file	Specify file containing rcs admin password.
-s	Configure local **pb.settings**.
-r	Re-install with BeyondInsight, without generating new certificates.

Options for Use with BeyondInsight for Unix and Linux

-M	Install via BeyondInsight for Unix and Linux (skip BeyondInsight registration and certficates).
-K	Filename of SSL Server certificate PEM file containing the private key. May also contain the public certificate.
-k	Filename of SSL Server certificate PEM file containing public certificate.
-C	Filename of any CA certificate PEM file containing the CA public certificate. May be used multiple time for multiple CA files.
-o	Fully qualified path for **openssl**.

Command Options

-b basedir	Set Solr installation base directory.
-p port	Set Solr/jetty port.
-j javahome	Set **JAVA_HOME**.
-u user	Set Solr user.
-c	If specified, create Solr user.
-I uid	If creating Solr user, specify the UID.
-G gid	If creating Solr user, specify the GID.
-i	Configure init **script/SMF/inittab**.
-l logdir	Specify Solr log directory.
a rcsuer	Specificy RCS Admin user.
s	Configure local **pb.settings**.
A file	Specify file containing the RCS admin password.
-P file	Specify file containing java keystore password.
M	Install via PBSMC (skip BI registration and certificates).
K	Specify the filename of the SSL server certificate PEM file containing the private key. 📌 *Note: This may also contain the public key.*
k	Specify the filename of any CA certifcate PEM file contain the CA public certificate. 📌 *Note: This filename may be used multiple times for multiple CA files.*
o	Specify the fully qualified path for **openssl**.
t tmpdir	Specify the **TMPDIR** directory for **Solrinstall** temporary files.
r	Re-install.
-q	Quiet mode.
-h	Display help.

Installation

Solr is provided as a tarball named **pmul-Solr_multiarch-{version}.tar.Z**. As root:

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

241

1. Make sure you have Java 1.6+ installed and know the home directory of Java.

2. Create directory **/opt/beyondtrust** and **cd** to that directory.

3. Extract the Solr installation files:

```
# gunzip -c pmul-Solr_multiarch-{version}.tar.Z | tar xvf -
```

4. Navigate to the install directory:

```
# cd powerbroker-Solr/v7.5/install
```

5. Copy the file **certificate.zip** generated by BeyondInsight.

6. Start the **Solrinstall** script with the following command; **Solrinstall** has no command line options:

```
# ./Solrinstall
```

The **Solrinstall** menu displays options similar to the following:

Solr Installation Menu		
Opt	*Description*	*[Value]*
1	Solr installation directory	[/opt/pbul-Solr]
2	Solr SSL port number	[8443]
3	JAVA_HOME environmental variable	[/usr/java/jre1.7.0_40]
4	Solr user	[Solr]
5	Create Solr user?	[yes]
6	Solr user UID	[]
7	Solr user GID	[]
8	Configure init?	[yes]
9	Solr log directory	[/var/log/Solr]
10	BeyondInsight certificate admin user name	[administrator]*
11	Configure local pb.settings with Solr	[no]
C to continue, X to exit		
Please enter a menu option		

7. During the install, you are prompted for the keystore password:

   Enter a keystore password (minimum 6 characters).

> 📌 *Note:* *This is a new password you must provide. Enter this password during the Post-Install when you import the Solr certificates using the BeyondInsight Configuration Tool.*

> ℹ️ *For more information, please see "Prerequisites when Installing with BeyondInsight" on page 239.*

SALES: www.beyondtrust.com/contact   SUPPORT: www.beyondtrust.com/support   DOCUMENTATION: www.beyondtrust.com/docs

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

242

TC: 12/7/2022

Menu Options

```
1. PowerBroker Solr installation directory
```

This is the directory where the Solr installation files are placed. The default value is **/opt/pbul-Solr.**

```
2. Solr port number
```

The port number to be used for the Solr service. The default is **8983**.

```
3. JAVA_HOME environmental variable
```

The value of **$JAVA_HOME**. This is set if environmental variable **$JAVA_HOME** is set. Prior to installation, **$JAVA_HOME/bin/java** is tested for version compatibility.

```
4. Solr user
```

The non-root user that runs the Solr server. The default is **Solr**. If user **Solr** does not exist, the menu displays options 5, 6, and 7 specifying whether to create the Solr user, and optionally specifying the uid/gid. The Solr user requires bash shell in order to run the Solr (jetty) startup script.

```
8. Configure init (Linux/HP-UX; AIX uses inittab, Solaris 10+ uses SMF)
```

Solr startup and shutdown are accomplished via init. Selecting **yes** to this menu option configures init to startup and shutdown Solr.

```
9. Solr log directory
```

This is the directory where the Solr log files are placed. The default value is **/var/log/Solr** (Linux). Other operating systems may use **/var/adm** or **/usr/adm** rather than **/var/log**.

```
10. BeyondInsight Certificate Administrator user name
```

The BeyondInsight Admin user; admin user password is prompted for.

```
11. Configure local pb.settings with Solr
```

Answering **yes** configures the local **pb.settings** file with the Solr related keywords, configured for this Solr installation. The keywords are:

- **Solrhost**
- **Solrport**
- **Solrcafile**
- **Solrclientkeyfile**
- **Solrclientcertfile**

SALES: www.beyondtrust.com/contact   SUPPORT: www.beyondtrust.com/support   DOCUMENTATION: www.beyondtrust.com/docs

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

243

TC: 12/7/2022

# Post-Install when Installing with BeyondInsight

After **SolrInstall** has installed and started Solr, Solr is registered with BeyondInsight.

To give the Solr server a heartbeat, a script called **pbrcsSolrupdate** is launched at the Solr installation, and with each restart of Solr services (jetty), where a Solr asset update event is sent to BeyondInsight daily.

Follow the instructions as listed after a successful Solr install are displayed at the end of the installation.

In order for the log server and policy server hosts to communicate with this Solr server, for indexing Privilege Management for Unix and Linux I/O log data, you must do the following:

1. On your BeyondInsight Windows server, start the BeyondInsight Configuration Tool.

2. Click **Import Certificates** to import the certificates created during the Solr install and grant privileges to the certificates for use by the Solr search.
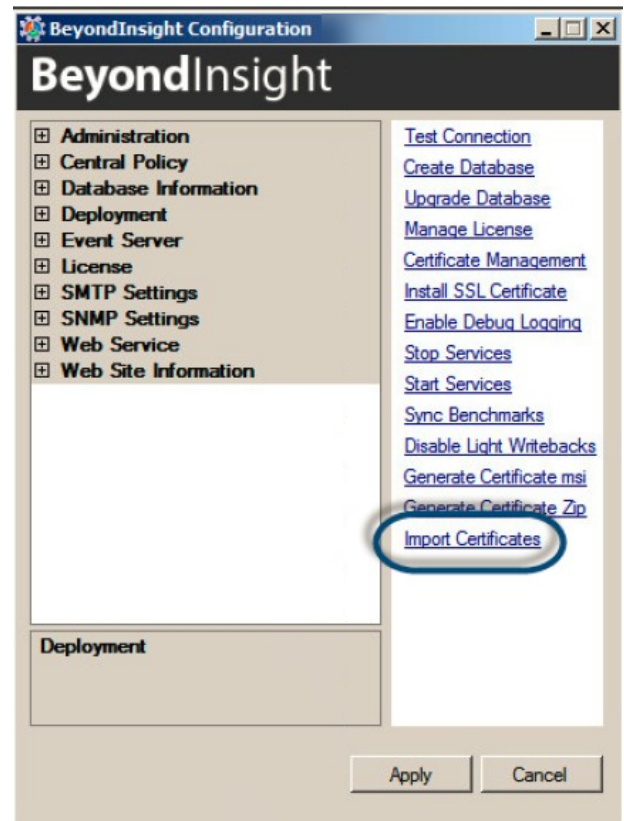
3. Enter the password that you provided when you created the Certificates ZIP file.
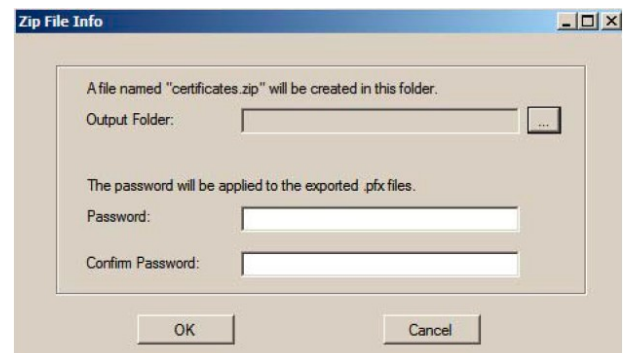
4. Securely copy the following files from **/opt/pbul-Solr/etc** to a secure directory on the Privilege Management for Unix and Linux policy server and log server hosts:

- **Solr.<host>.client.pem**
- **Solr.<host>.ssl.CA.pem**

> 📌 *Note: A tarball (**Solr.${shorthostname}.pbsettings.tar**) is created with the certificate files and related settings, for convenient copying to other hosts. When the tarball is extracted from the root directory, the certificate files and **Solr.pb.settings** are placed in **/etc/**. The settings contained in **/etc/Solr.pb.settings** must be manually merged into **/etc/pb.settings**.*

5. In **pb.settings** of the policy server or log server hosts, add the following parameters:

```
Solrhost <host>
Solrport 8443
Solrcafile <secure_directory>/Solr.<host>.ssl.CA.pem
Solrclientkeyfile <secure_directory>/Solr.<host>.client.pem
Solrclientcertfile <secure_directory>/Solr.<host>.client.pem
```

> 📌 *Note: A tarball (**Solr.${shorthostname}.pbsettings.tar**) is created with the certificate files and related settings, for convenient copying to other hosts. When the tarball is extracted from the root directory, the certificate files and **Solr.pb.settings** are placed in **/etc/**. The settings contained in **/etc/Solr.pb.settings** must be manually merged into **/etc/pb.settings**.*

Re-Installation when Installing with BeyondInsight

Starting with v9.4, when re-installing Solr, the installation script recognizes that certificates have already been generated, and the registration with BeyondInsight is skipped. This prevents regeneration of certificates by BeyondInsight. In the case where regeneration of certificates is desired, the certificates must be manually cleared from BeyondInsight, and removed from the **etc** directory of the Solr installation (default: **/opt/pbul-Solr/etc**).

Solr Uninstall

As root:

1. Create directory **/opt/beyondtrust** and **cd** to that directory.
2. Extract the Solr installation files:

```
# gunzip -c pmul-Solr_multiarch-{version}.tar.Z | tar xvf -
```

3. Navigate to the install directory:

```
# cd /opt/beyondtrust/powerbroker-Solr/v7.5/install
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

245

TC: 12/7/2022

4. Start the **Solruninstall** script with either of the following commands; **Solruninstall** has 1 command line option:

```
# ./Solruninstall
```

```
# ./Solruninstall -clean
```

Install ODBC Connectors

Oracle and MySQL ODBC connectors are only supported on Linux and Solaris platforms.

Install MySQL ODBC Connector on Linux

1. Create the database and grant user privileges. On the host where MySQL server is installed, run:

```
# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 11
Server version: 5.6.45 MySQL Community Server (GPL)
Copyright (c) 2000, 2019, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> use mysql;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> create database pbtest;
Query OK, 1 row affected (0.00 sec)

mysql> create user 'testuser'@'locahost' identified by '<passwd>';
Query OK, 0 rows affected (0.00 sec)

mysql> grant all on pbtest.* to 'testuser' identified by '<passwd>';
Query OK, 0 rows affected (0.00 sec)

mysql> grant all on pbtest.* to 'root' identified by '<passwd>';
Query OK, 0 rows affected (0.00 sec)

mysql> ^DBye
```

2. The steps below are to be done on the log server, where only MySQL ODBC connector needs to be installed. The example below is from a CentOS 6 system:

```
# yum install mysql-connector-odbc
```

> 📌 **Note: mysql-connector-odbc** *version 5.3.14 is not supported.*

3. In **pb.settings** set:

```
eventdestinations authevt=odbc=MySQL
odbcinidir  /opt/pbul/etc
```

If you are using **mysql-connector-odbc** version 5.3.x with SSL enabled on MySQL server or **mysql-connector-odbc** version 8.0.x (with or without SSL), in **pb.settings** file, you need to configure the setting **loadssllibs** to **yes**.

```
cat /etc/pb.settings | grep loadssllibs
loadssllibs                          yes
```

4. Copy **/etc/odbcinst.ini** to **/opt/pbul/etc**.
5. Make sure the libraries are set correctly (if 64-bit machine, **driver64** and **setup64**).

> *Example:*
>
> ```
> [MySQL]
> Description= ODBC for MySQL xml:space="preserve">
> Driver= /usr/lib/libmyodbc5.so
> Setup= /usr/lib/libodbcmyS.so
> Driver64 = /usr/lib64/libmyodbc5.so
> Setup64= /usr/lib64/libodbcmyS.so
> FileUsage = 1
> UsageCount = 3
> trace = no
> tracefile = stderr
> ```

6. Create **/opt/pbul/etc/odbc.ini:**

```
[MySQL]
Description = ODBC for MySQL
Driver = MySQL
server = <ip-address>
port = 3306
user = root
password = <passwd>
database  = pbtest
trace = no
tracefile = stderr
```

> *Note: In the file above, **<ip-address>** is the IP address of the host where the database was created (in step 1). **<passwd>** is the root password as set up on that host.*

7. On some Linux platforms, such as Debian, you might also need to add the following highlighted line to **/etc/systemd/pblighttpd.service**. In the example below, **/usr/local/unixODBC** is where unixODBC was installed, and **/usr/local/MySQL/lib** is where the MySQL libraries **libmyodbc5.so** is located:

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

248

> **Example:**
>
> ```
> # cat /etc/systemd/system/pblighttpd.service
> [Unit]
> Description=BeyondTrust PowerBroker REST services
> After=network.target
>
> [Service]
> ExecStart=/usr/lib/beyondtrust/pb/rest/sbin/pblighttpd-svc
> ExecReload=/bin/kill -HUP $MAINPIDEnvironment="LD_LIBRARY_
> PATH=/usr/lib:/usr/local/lib:/usr/local/unixODBC/lib:/usr/local/MySQL/lib:"
>
> [Install]
> WantedBy=multi-user.target
> ```

8. Restart **pblighttpd**.

9. Run pbrun and verify using:

```
# pblog --odbc -f MySQL
```

10. Check **pbrest.log** and other logs to make sure there is no error.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

249

TC: 12/7/2022

Install MySQL ODBC on Solaris

The MySQL ODBC connector can be installed on Solaris 10 and 11 (sparc and x86).

To install the database/server, follow the MySQL instructions (or see above on Linux).

📌 *Note: PMUL binaries are 32-bit. You must ensure a 32-bit version of ODBC is installed on Solaris 10 and 11.*

1. Install the MySQL package (output of the command is in the attached file):

```
# pkgadd -d http://get.opencsw.org/now
# /opt/csw/bin/pkgutil -U -u -y
# /opt/csw/bin/pkgutil -y -i myodbc
```

📌 *Note: Mysql-connector-odbc version 5.3.14 is not supported.*

2. In **pb.settings** set:

```
eventdestinations authevt=odbc=MySQL
odbcinidir  /opt/pbul/etc
```

If you are using **mysql-connector-odbc** version 5.3.x with SSL enabled on MySQL server or **mysql-connector-odbc** version 8.0.x (with or without SSL), in **pb.settings** file, you need to configure the setting **loadssllibs** to **yes**.

```
cat /etc/pb.settings | grep loadssllibs
loadssllibs                          yes
```

3. Configure **Odbc.ini:**

```
[MySQL]
Description = ODBC for MySQL
Driver = MySQL
server = <ip_of_MYSQL_host>
port = 3306
user = root
password = <passwd>
database = <database>
```

4. Create **/opt/pbul/etc/odbc.ini:**

```
[MySQL]
Description  = ODBC for MySQL
Driver = /opt/csw/lib/libmyodbc3.so
FileUsage = 1
```

```
UsageCount = 3
trace = no
tracefile = stderr
```

5. Set **LD_LIBRARY_PATH** to:

```
LD_LIBRARY_PATH=/opt/csw/lib:/usr/lib:/lib:/usr/local/lib
```

6. Restart **pblighttpd**.

Install Oracle ODBC Connector on Linux

1. On the Oracle database/server, log in to the server where the Oracle database is installed as root, then **su** to oracle, and create your user (replace <user> by your name) as follows:

Example:

```
# su - oracle
Last login: Wed Sep  4 17:28:54 PDT 2019 from jurel.pbse.lab on pts/0
$ sqlplus / as sysdba
SQL*Plus: Release 19.0.0.0.0 - Production on Thu Sep 5 15:21:24 2019
Version 19.3.0.0.0
Copyright (c) 1982, 2019, Oracle.  All rights reserved.
Connected to:
Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 - Production
Version 19.3.0.0.0
SQL> alter session set "_ORACLE_SCRIPT"=true;
Session altered.
SQL> create user mdavis identified by mdavis;
User created.
SQL> GRANT CONNECT,RESOURCE,DBA to mdavis;
Grant succeeded.
SQL> GRANT UNLIMITED TABLESPACE to mdavis;
Grant succeeded.
SQL> Disconnected from Oracle Database 19c Enterprise Edition Release 19.0.0.0.0 -
Production
Version 19.3.0.0.0
```

2. Run the following steps on the log server, where only the Oracle ODBC connector needs to be installed. Steps shown below are on a CentOS 6 system:

   Oracle InstantClient (basic and ODBC) can be downloaded from https://www.oracle.com/database/technologies/instant-client/downloads.html.

   Download the file to a directory. For example, **/tmp/Oracle**.

   On RHEL 6, install **oracle-instantclient<version>-basic…** and **oracle-instantclient<version>-odbc** v18.5. Version 19.3 does not work on RHEL 6, but works on RHEL 7:

```
# cd /tmp/Oracle
# yum install oracle-instantclient18.5-basic-18.5.0.0.0-3.x86_64.rpm oracle-
instantclient18.5-odbc-18.5.0.0.0-3.x86_64.rpm
```

   Install unixODBC needed by Oracle ODBC:

```
# yum install unixODBC
```

   unixODBC is installed in **/usr/lib64**.

3. In **pb.settings** set:

```
eventdestinations authevt=odbc=Oracle
odbcinidir  /opt/pbul/etc
```

4. Create **/etc/tnsnames.ora:**

```
# cat /etc/tnsnames.ora
ORCLCDB=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=moonfish)(PORT=1521)))
(CONNECT_DATA=(SID=ORCLCDB)))
```

> 📌 ***Note:*** *The **tnsnames.ora** file needs to be in **/etc**. Copying it elsewhere and setting environment variable TNS_ADMIN to the new directory does not work.*

5. Create **/opt/pbul/etc/odbcinst.ini:**

```
[oracle]
Description = Oracle 18
Driver      = /usr/lib/oracle/18.5/client64/lib/libsqora.so.18.1
ServerName  = ORCLCDB
```

6. Create **/opt/pbul/etc/odbc.ini:**

```
[oracle]
Description = Oracle
Driver      = oracle
DSN         = ORCLCDB
ServerName  = ORCLCDB
UserID      = mdavis
Password    = mdavis
```

Use the user name created in step 1.

7. The following library is required for **pblighttpd** to connect to the Oracle ODBC: **/usr/lib/oracle/18.5/client64/lib/libsqora.so.18.1**. With Oracle ODBC, some of the paths of the dependent libraries are not set and setting LD_LIBRARY_PATH doesn't work. The following error is displayed:

```
Sep  6 09:08:18 [12974] 6339.32 Failed to connect to ODBC DSN 'Oracle' - [unixODBC][Driver
Manager]Can't open lib '/usr/lib/oracle/18.5/client64/lib/libsqora.so.18.1' : file not found
```

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

253

©2003-2022 BeyondTrust Corporation. All Rights Reserved. Other trademarks identified on this page are owned by their respective owners. BeyondTrust is not a chartered bank or trust company, or depository institution. It is not authorized to accept deposits or trust accounts and is not licensed or regulated by any state or federal banking authority.

TC: 12/7/2022

⚠ **IMPORTANT!**

Solution 1

1. Set the library path system wide in **ld.so**. For that, create a file **oracle-instantclient.conf** with the path in it, and do the following:

    ```
    # cat oracle-instantclient.conf
    /usr/lib/oracle/18.5/client64/lib
    # cp oracle-instantclient.conf /etc/ld.so.conf.d
    # ldconfig
    ```

2. Verify it's loaded:

    ```
    # ldconfig -p|grep sqora
    libsqora.so.18.1 (libc6,x86-64) => /usr/lib/oracle/18.5/client64/lib/libsqora.so.18.1
    ```

Solution 2

Use **patchelf** to set the path for all the Oracle libraries.

If **patchelf** is not on your machine, download **patchelf rpm** from https://pkgs.org/search/?q=patchelf.

Do the following:

```
# service pblighttpd stop
# cd /usr/lib/oracle/18.5/client64/lib
# for i in *.so*
do
patchelf --set-rpath /usr/lib/oracle/18.5/client64/lib $i
done
# service pblighttpd start
Starting pblighttpd-svc service.
```

📌 *Note: You might prefer the second solution because the lib path is set only for the Oracle libraries and is not system-wide.*

8. To use oracle SSL authentication, create **sqlnet.ora** file, update **TNS_NAMES** configurations for **pblighttpd** and restart **pblighttpd**.

    -   Create **/etc/sqlnet.ora**.

        ```
        #cat /etc/sqlnet.ora
        SQLNET.AUTHENTICATION_SERVICES= (TCPS)
        SSL_CLIENT_AUTHENTICATION = FALSE
        ```

```
SSL_CIPHER_SUITES = (SSL_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA)
SSL_SERVER_DN_MATCH = no
WALLET_LOCATION = (SOURCE =(METHOD = FILE)(METHOD_DATA =(DIRECTORY =
/home/oracle/app/oracle/wallet)) )
```

```
ls /etc/*.ora
/etc/sqlnet.ora   /etc/tnsnames.ora
```

- If **pblighttpd** is running as deamon: edit the **/etc/init.d/pblighttpd** file.

Add an entry to export the **TNS_ADMIN** environmental variable.

🔍 ***Example:***

```
cat /etc/init.d/pblighttpd | grep TNS_ADMIN
TNS_ADMIN=/etc/
export PBLIGHTTPD_PRG PBLIGHTTPD_ROOT PBLIGHTTPD_PID PBLIGHTTPD_BIN PBLIGHTTPD_CONF
RETVAL PATH TNS_ADMIN
```

- If it is a service, edit **/etc/systemd/system/pblighttpd.service** and add the text below the **[Service]** tag.

🔍 ***Example:***

```
cat /etc/systemd/system/pblighttpd.service
[Unit]
Description=BeyondTrust PowerBroker REST services
After=network.target
[Service]
ExecStart=/usr/lib/beyondtrust/pb/rest/sbin/pblighttpd-svc
ExecReload=/bin/kill -HUP $MAINPID
Environment=TNS_ADMIN=/etc/
[Install]
WantedBy=multi-user.target
```

📌 ***Note: TNS_ADMIN** is the location from where odbc drivers will read **sqlnet.ora** and **tnsnames.ora**.*

- Restart **pblighttpd**.

9. Run **pbrun** and verify using:

```
# pblog --odbc -f Oracle
```

📌 ***Note: Export **TNS_NAME=/etc/** to use oracle SSL connections.*

Install Oracle ODBC Connector on Solaris

The following install was on x86 Solaris 10. The steps are similar on a Sparc Solaris 10 and on Solaris 11. Download the appropriate ZIP files (**instantclient-basic** and **instantclient-odbc**) to a directory. For example, **/tmp/Oracle**.

For Solaris Sparc 10, the 2 hosts **pbul-qa-spsol11z-01** and **pbul-qaspsol11z-02** already have Oracle ODBC installed. When installing PMUL, you must create **odbc.ini** in **/opt/<prefix>pbul<suffix>/etc**.

> 📌 *Note: PMUL binaries are 32-bit. You must ensure 32-bit versions of unixODBC and Oracle ODBC connectors are installed on Solaris 10 and 11.*

1. Step 1 is the same as for Linux. Use the existing Oracle database/server and create your user.
2. Run the following steps on the log server:

```
# pkgadd -d http://get.opencsw.org/now
# export PATH=$PATH:/opt/csw/bin
# pkgutil -U -u -y
# pkgutil -i -y unixodbc
# mkdir /opt/oracleODBC
# cd /opt/oracleODBC/
# unzip /tmp/Oracle/instantclient-basic-solaris.x32-18.3.0.0.0dbru.zip
# unzip /tmp/Oracle/instantclient-odbc-solaris.x32-18.3.0.0.0dbru.zip
# unzip /tmp/Oracle/instantclient-sqlplus-solaris.x32-18.3.0.0.0dbru.zip
```

3. In **pb.settings** set:

```
eventdestinations authevt=odbc=Oracle
odbcinidir  /opt/pbul/etc
```

4. Create **/etc/tnsnames.ora:**

```
# cat /etc/tnsnames.ora
ORCLCDB=(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=moonfish)(PORT=1521)))
(CONNECT_DATA=(SID=ORCLCDB)))
```

> 📌 *Note: The **tnsnames.ora** file needs to be in **/etc**. Copying it elsewhere and setting **TNS_ADMIN** to the new directory does not work.*

5. Create **/opt/pbul/etc/odbcinst.ini:**

```
[oracle]
Description = Oracle 18
Driver      = /opt/oracleODBC/instantclient_18_3/libsqora.so.18.1
ServerName  = ORCLCDB
```

6. Create **/opt/pbul/etc/odbc.ini:**

```
[oracle]
Description = Oracle
Driver      = oracle
DSN         = ORCLCDB
ServerName  = ORCLCDB
UserID      = mdavis
Password    = mdavis
```

Use the user name you created in step 1.

7. Set **LD_LIBRARY_PATH** and **TNS_ADMIN** for the **pblighttpd** service:

```
svccfg -s application/security/pblighttpd setenv LD_LIBRARY_PATH
/opt/oracleODBC/instantclient_18_3:/opt/csw/lib
svccfg -s application/security/pblighttpd setenv TNS_ADMIN /etc
svcadm refresh pblighttpd
svcadm restart pblighttpd
```

8. Set **LD_LIBRARY_PATH** in the environment for **pblog** to work. Add the following to **/etc/profile:**

```
LD_LIBRARY_PATH="/usr/lib:/lib:/opt/oracleODBC/instantclient_18_3:/opt/csw/lib"
export LD_LIBRARY_PATH
TNS_ADMIN=/etc
export TNS_ADMIN
```

> **(!) IMPORTANT!**
>
> *Make sure /usr/lib is first in LD_LIBRARY_PATH.*

9. To use oracle SSL authentication, create **sqlnet.ora** file, update **TNS_NAMES** configurations for **pblighttpd** and restart **pblighttpd**.

   - Create **/etc/sqlnet.ora**.

```
#cat /etc/sqlnet.ora
SQLNET.AUTHENTICATION_SERVICES= (TCPS)
SSL_CLIENT_AUTHENTICATION = FALSE
SSL_CIPHER_SUITES = (SSL_RSA_WITH_AES_256_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA)
SSL_SERVER_DN_MATCH = no
WALLET_LOCATION = (SOURCE =(METHOD = FILE)(METHOD_DATA =(DIRECTORY =
/home/oracle/app/oracle/wallet)) )
```

```
ls /etc/*.ora
/etc/sqlnet.ora  /etc/tnsnames.ora
```

- Set the environment variable **TNS_ADMIN=/etc/** to **pblighttpd** service.

Use the below commands to set the variable:

```
svccfg -s pblighttpd setenv TNS_NAME /etc/
svcadm refresh pblighttpd
```

Validate the configuration using below command:

```
svcprop -p start/environment pblighttpd
```

> 📌 *Note: TNS_ADMIN is the location from where ODBC drivers read **sqlnet.ora** and **tnsnames.ora**.*

- Restart **pblighttpd**.

10. Run **pbrun** and verify using:

```
# pblog --odbc -f Oracle
```

> 📌 *Note: Export **TNS_ADMIN=/etc** if you are using oracle SSL connections.*

11. Check **pbrest.log** and other logs to make sure there is no error.

> ⚠ **IMPORTANT!**
>
> Set **LD_LIBRARY_PATH** with **/opt/csw/lib:**
>
> When **LD_LIBRARY_PATH** is set to contain **/opt/csw/lib** without **/usr/lib** first, and we either validate or import **pblighttpd-smf.xml**, **svccfg** segfault on Solaris:
>
> ```
> # LD_LIBRARY_PATH=/opt/oracleODBC/instantclient_18_3:/opt/csw/lib
> # svccfg validate /usr/lib/beyondtrust/pb/rest/etc/pblighttpd-smf.xml
> Segmentation Fault (core dumped)
> #
> # LD_LIBRARY_PATH=/opt/oracleODBC/instantclient_18_3
> # svccfg validate /usr/lib/beyondtrust/pb/rest/etc/pblighttpd-smf.xml
> ```
>
> Or
>
> ```
> # LD_LIBRARY_PATH=/usr/lib:/opt/oracleODBC/instantclient_18_3:/opt/csw/lib
>       # svccfg validate /usr/lib/beyondtrust/pb/rest/etc/pblighttpd-smf.xml
> ```
>
> The reason for the segfault is a library conflict in **/usr/lib** and **/opt/csw/lib**.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

258

TC: 12/7/2022

```
# ldd /usr/sbin/svccfg
libxml2.so.2 =>  /usr/lib/libxml2.so.2
libscf.so.1 =>   /usr/lib/libscf.so.1
libl.so.1 =>     /usr/lib/libl.so.1
libuutil.so.1 =>          /usr/lib/libuutil.so.1
libumem.so.1 =>  /usr/lib/libumem.so.1
libdoor.so.1 =>  /usr/lib/libdoor.so.1
libmd5.so.1 =>   /usr/lib/libmd5.so.1
libtecla.so.1 =>          /usr/lib/libtecla.so.1
libc.so.1 =>     /usr/lib/libc.so.1
libpthread.so.1 =>        /usr/lib/libpthread.so.1
libz.so.1 =>     /usr/lib/libz.so.1
libm.so.2 =>     /usr/lib/libm.so.2
libsocket.so.1 =>         /usr/lib/libsocket.so.1
libnsl.so.1 =>   /usr/lib/libnsl.so.1
libgen.so.1 =>   /usr/lib/libgen.so.1
libcurses.so.1 =>         /usr/lib/libcurses.so.1
libmp.so.2 =>    /usr/lib/libmp.so.2
libmd.so.1 =>    /usr/lib/libmd.so.1
/platform/sun4v/lib/libc_psr.so.1
/lib/libm/libm_hwcap1.so.2
/platform/sun4v/lib/libmd_psr.so.1
```

If **LD_LIBRARY_PATH** does not have **/usr/lib** first, we get:

```
# LD_LIBRARY_PATH=/opt/oracleODBC/instantclient_18_3:/opt/csw/lib
# ldd /usr/sbin/svccfg
libxml2.so.2 =>  /usr/lib/libxml2.so.2
libscf.so.1 =>   /lib/libscf.so.1
libl.so.1 =>     /usr/lib/libl.so.1
libuutil.so.1 => /lib/libuutil.so.1
libumem.so.1 =>  /lib/libumem.so.1
libdoor.so.1 =>  /lib/libdoor.so.1
libmd5.so.1 =>   /lib/libmd5.so.1
libtecla.so.1 => /usr/lib/libtecla.so.1
libc.so.1 =>     /lib/libc.so.1
libpthread.so.1 =>  /lib/libpthread.so.1
libz.so.1 =>     /opt/csw/lib/libz.so.1
libz.so.1 (SUNW_1.1) =>  (version not found)
libm.so.2 =>     /lib/libm.so.2
libsocket.so.1 => /lib/libsocket.so.1
libnsl.so.1 =>   /lib/libnsl.so.1
libgen.so.1 =>   /lib/libgen.so.1
libcurses.so.1 => /lib/libcurses.so.1>
libmp.so.2 =>    /lib/libmp.so.2
libmd.so.1 =>    /lib/libmd.so.1
/platform/sun4v/lib/libc_psr.so.1
/lib/libm/libm_hwcap1.so.2
/platform/sun4v/lib/libmd_psr.so.1
```

ℹ️ *For more information, please see* .

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

259

Install Sudo Policy Server

Privilege Management for Unix and Linux Sudo Manager, hereinafter Sudo Manager, provides improved management and maintenance of sudo files and data, while leveraging some of the features of Privilege Management for Unix and Linux without replacing sudo itself.

There are two components to install to use Sudo Manager:

- Sudo Manager policy server
- Sudo Manager plugin client

This section guides you through installing the Sudo Manager policy server.

Sudo Manager Installation Considerations

Sudo Manager is a non-intrusive software program that does not require kernel reconfiguration, system reboot, or to replace system executable files. The items in this section contain information you should consider when planning your implementation.

> ℹ️ *For more detailed information about Sudo Manager, please see the Privilege Management for Unix and Linux Sudo Manager System Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

Flavor and Release Definitions

Flavor is a BeyondTrust term that defines a build of a BeyondTrust product, such as Sudo Manager, that is compiled and tested for a certain range of operating system versions and underlying hardware. The README file describes which flavor is the right match for specific combinations of hardware and operating systems in the **Release Identifier** column. The release identifier is the flavor plus the version of the Sudo Manager distribution.

During installation, the flavor of the distribution you are using will be compared to the flavor required for the operating system and hardware version combination you are installing on. If you believe that you are using the correct version for the machine you are installing on but the installer is returning a flavor mismatch, please contact BeyondTrust Technical Support for assistance.

Interactive Versus Packaged Installation

Sudo Policy Server

All Sudo Policy Server flavors can be installed by using an interactive program that presents you with a series of options. Your choices determine the details of the installation for a particular host.

The client registration facility can be used to automate the installation of new clients by downloading the default configuration from the primary Policy Server. Options are defaulted within the interactive installation, and shared encryption keys are copied over.

For certain flavors, the Sudo Policy Server can be installed by using package installers. Package installers enable you to choose the options once, and then install that configuration of Sudo Policy Server non-interactively on multiple identical hosts. Using package installers also takes advantage of the operating system's installation management system, which tracks the source of installed files and enables their safe removal.

Sudo Manager Clients

The Sudo Manager client is only supported on Linux x86_64.The installation method is through the interactive **sudomgrinstall** program. Package installers are not available.

> ℹ️ *For more information, please see Supported Platforms at https://www.beyondtrust.com/docs/privilege-management/unix-linux/supported-platforms.htm.*

Resource Overhead

There are not any start-up or shutdown programs associated with Sudo Manager client. From a system resource perspective, a basic Sudo Manager session uses about the same overhead as a telnet session with additional front-end work for processing the policy security file.

The Sudo Manager Policy Server is the pblighttpd/pbconfigd REST server daemon. The accept, reject and finish events are logged by the **pblogd** daemon on a Log Server. These resources are requested by the sudo manager plugin client. The REST services are started by a superdaemon, and normally run continuously. The **pblogd** daemon can be started by a superdaemon, or may itself run continuously as a daemon. The superdaemons include **systemd**, **inetd**, **xinetd**, **launchd**, or **SMF** depending on the platform.

For systems based on RedHat version 7+, **xinetd** is no longer installed by default since it has been superceded by **systemd**, which is an init system. The installation program performs a check to see if systemd exists and is functional. If it exists, it configures Sudo Manager daemons to be managed by **systemd**. If **systemd** is not present, the installation program checks if xinetd is installed and running and displays a warning message if it is not.

> ℹ️ *For more information, please see the Privilege Management for Unix and Linux Sudo Manager Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

> 📌 *Note: The terms **monitored task** and **secured task** are interchangeable.*

SSL adds some startup overhead for certificate exchange and verification. The encryption overhead is slightly larger than self-contained encryption technologies such as DES because of the use of packet checksums by SSL.

> 📌 *Note: Sudo Manager requires 10 to 50 MB of disk space, depending on the installation options selected.*

Installation Directories

Sudo Manager is not sensitive about the location of its binary files; you can place them in any convenient directory. However, there are a few points to consider when you are selecting installation directories:

- Online manuals such as user man pages and Sudo Manager documentation should be accessible from every computer to enable users to get online help for Sudo Manager programs.

Default Directories

The following table lists Sudo Manager components and their locations. The installation script uses these locations by default, but you can change them during installation. Usually **/usr/local/bin** is used for user programs and **/usr/sbin** for administrator and daemon programs, depending on the platform.

Default Directories for Sudo Manager Components

Directory	Files	Description
/etc	pb.keypb.settingspbsudo.settings	Encryption KeySudo Manager policy server config fileSudo Manager plugin config file
/usr/adm, /var/adm, or /var/log	pb.eventlogpblogd.log	Default event log filepblogd diagnostic log file
/usr/sbin	pbdbutil	Utility providing Sudo Manager database maintenance.
/opt/pbul/dbs	pbsvccache.db	

The default log directory varies by platform to match that platform's conventions. The directories **/usr/adm**, **/var/adm**, and **/var/log** are used interchangeably throughout as the default location of the database files generated and used by Sudo Manager log files.

Prefix and Suffix Installations

The Sudo Manager policy server or Sudo Manager clients do not support prefix and suffix installations.

System File Modifications

The Sudo Manager client modifies:

- **/etc/sudo.conf** to use the Sudo Manager plugin.
- **/etc/pam.d/sudo-l** might be copied from **/etc/pam.d/sudo**; and the necessary libraries and plugin are installed in **/usr/lib/beyondtrust/pb/**

Installation Preparation

This section lists the items that you need to plan for and be aware of before beginning your installation.

Pre-installation Checks

pbulpreinstall.sh performs some pre-installation checks such as:

- Checks Hostname resolution and DNS and name services resolution to verify that the default ports are not in use.
- Checks for sufficient disk space.
- Reports technical support-related information such as the Operating System, NIC information, gateway, and super daemon status. If Sudo Manager is already installed, the roles such as **submithost**, **runhost**, Policy Server, **logserver**, and **pbx** are reported.

This script has an optional **-t <datetime in UTC>** argument, which initiates a time verification check. This check simply validates that the host's time is within 60 seconds of the time specified. The time specified must be UTC and in the format 20130827154130, such as:

date -u '+%Y%m%d%H%M%S'

This script has an optional **-f** argument, which causes **pbulpreinstall.sh** to produce machine readable output intended for the BeyondInsight for Unix & Linux installation console.

Prior to installation, the **pbulpreinstall.sh** script is located in the Sudo Manager distribution in the following directory **powerbroker/<version>/<flavor>/install**. After installation, this script is installed in the **'$inst_admin'** directory. **/usr/sbin** is the default.

Obtain a License Validation Key

To install Sudo Manager, you need a license string, which is provided by your BeyondTrust sales representative.

Privilege Management for Unix and Linux Primary License Server hosts perform the license resolution functions for Sudo Manager and are the only Sudo Manager host types that require a license key. For a Policy Server host to accept a task, the Primary License Server must have a current valid license key. The distribution includes a temporary license key with a two-month expiration date from the date of the installation.

If installing using **pbinstall**, the license key may be configured during installation using the Sudo Manager **License** installation menu item. After the installation is complete, the Sudo Manager license can also be added using the **"pbadmin --lic -u"** command.

Obtain root Access

Installing Sudo Manager requires root access.

Plan Sudo Manager Hosts

A Sudo Manager installation includes several host types, each of which performs specific functions. Prior to installation, you need to determine which host type needs to be placed on the individual machines in your environment.

> 📌 **Note:** *Sudo Manager must be installed separately on each machine that will run any type of Sudo Manager host.*

Select License Servers

Determine which hosts to use as License Servers, the machines that perform the license resolution functions for Sudo Manager. These hosts are the only types that require a license key. They store and maintain the product license, parameters, and usage information.

The first installation of Sudo Manager becomes the Primary License Server. Subsequent License Server installations will obtain their data when the Primary License Server performs synchronization.

Select Sudo Policy Server Hosts

Determine which machines to use as sudo Policy Servers for Sudo Manager. These hosts act as central repositories of the sudoers policy files obtained from sudo client hosts. It is highly recommended that hosts designated as sudo Policy Servers are isolated from regular user activity to shield policies from users that can elevate their privileges.

Select Log Hosts

Using a log host to record event and I/O logs is optional. To use this feature, determine which machine to use as the Sudo Manager log host and the machines where pblogd will be installed and executed. As with sudo Policy Server hosts, multiple log hosts are recommended to provide redundancy. When there is a log host failover, the log synchronization utilities in Sudo Manager can be used to resynchronize the log entries.

The load on the log hosts varies with the amount of logging that is performed. I/O logs require greater resources on the log hosts. Additional log hosts can be added to your environment during installation, or afterward as needed.

Enable Log Synchronization Host

Log synchronization enables a log host, or a Policy Server host that is acting as a log host, to participate in log synchronization. Install the log synchronization component on any log host or Policy Server host that may participate in log synchronization. Log synchronization should be installed on each log and Policy Server host if you are installing primary and failover log hosts, or are installing Policy Server hosts that are acting as log hosts.

If log synchronization is used, then one or more machines need to have the ability to initiate log synchronization.

Select Sudo Hosts (Clients)

Determine which sudo hosts in the enterprise will have their sudoers files and generated data managed by Sudo Manager. Sudo on these hosts will be configured to use the customized plugin that Sudo Manager will install.

Select Port Numbers

You need to decide whether to use the Sudo Manager default port numbers or to specify your own. Sudo Manager uses the following default port numbers:

pblogd	24347
pbrestport	24351

If you decide to change the port number defaults, be sure to choose port numbers that do not conflict with those already in use. See **/etc/services**. Also, if present and active, review the services NIS map. Sudo Manager port numbers must use the non-reserved system ports. The allowed port numbers are 1024 to 65535.

Select Installation Directories

Decide whether to use the Sudo Manager default installation directories or to specify your own. Specifying your own installation directories allows for Sudo Manager optimization of the local installation.

Select Syslog

Use of syslog is optional. Determine if the log host should generate syslog records when system error conditions are encountered.

Select Encryption

By default, Sudo Manager installs with aes-256 encryption. Prior to version 8.0, the default was DES; however, it can support a large number of encryption technologies.

> *Prior to selecting which encryption technology you plan to use, please see the Privilege Management for Unix and Linux Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

Firewalls

Sudo Manager can be used in a firewall environment with special configuration.

> *If you are installing Sudo Manager into an environment where the components need to communicate across firewalls, please see the Privilege Management for Unix and Linux Administration Guide at https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.*

Use NIS

Privilege Management for Unix and Linux can use NIS to provide configuration services for Sudo Manager settings. Netgroups can be defined for the Log Host (pblogservers) settings. NIS can also be used to provide port lookup information for the Sudo Manager components. If NIS is running in your environment, consider using Sudo Manager netgroups and port definitions.

Verify Proper TCP/IP Operation

Privilege Management for Unix and Linux uses TCP/IP as its communication protocol. Therefore, it is essential that TCP/IP be working correctly before Sudo Manager installation. Use programs such as ping, netstat, route, or traceroute to verify correct TCP/IP operation among all hosts that will have Sudo Manager components installed.

Verify Network Host Information

Ensure that each network host knows the names and addresses of all other network hosts. Network host information is generally stored in the /etc/hosts file on each network host machine or in the NIS maps or DNS files on a server. Each submit host should resolve all of the Policy Server host names correctly. Each Sudo Policy Server host should resolve all log host names correctly. The resolution must work correctly in both directions: name-to-IP address and IP address-to-name.

After installation, the pbbench utility generates warnings for any host name resolution issues on a host where components are installed.

Install Sudo Policy Server

The Sudo Policy Server supports interactive installation methods and package installation methods for its server components.

> ℹ️ *For more information, please see:*
>
> - *"Interactive Versus Packaged Installation" on page 260: review to help you decide on the right install for your Sudo Manager implementation.*
> - *"Basic pbinstall Information" on page 31: learn more about the pbinstall program.*
> - *"Advanced Installation Instructions Using pbinstall" on page 46: provides indepth details for install options.*

Install Sudo Policy Server Overview

If you are installing Sudo Policy Server using pbinstall, the menu options will look similar to the following table.

1. For option 9, **Install sudo Policy Server?**, enter **yes**. If Registry Name Service is enabled, you are also required to install the Registry Name Services Server. Review the section noted in the information box for more details.

Opt	Description	[Value]
1	Install Everything Here (Demo Mode)?	[no]
2	Install License Server?	[no]
3	Install Registry Name Services Server?	[no]
4	Install Client Registration Server?	[no]
5	Install Policy Server Host?	[yes]
6	Install Run Host?	[yes]
7	Install Submit Host?	[yes]
8	Install PBSSH?	[yes]
9	Install sudo Policy Server?	[yes]
10	Install Log Host?	[yes]
11	Enable Logfile Tracking and Archiving?	[yes]
12	Is this a Log Archiver Storage Server?	[no]
13	Is this a Log Archiver Database Server?	[no]
14	Install File Integrity Monitoring Polic...	[no]
15	Install REST Services?	[yes]
16	List of License Servers	[*]
54	sudo policy database file path and filename?	[/opt/pbul/dbs/pbsudo.db]

Opt	Description	[Value]
55	Directory location for sudo policy files?	[/opt/pbul/sudoersdir]?

2. Choose your options.

3. Use the **c** navigation command to continue the installation.

4. A prompt asks if you want to view the install script. Enter **n**.

⚠ **IMPORTANT!**

This option is intended for troubleshooting by BeyondTrust Technical Support. The generated install script contains thousands of lines of code.

---

5. A prompt asks if you want to install the product now. Enter **y**.

The pbinstall install script executes and installs components on this machine.

Upgrades and Reinstallations

The Sudo Policy Server installers are designed to enable easy upgrades of an installed version to a new version. During an upgrade, the current configuration can be retained, or a new Sudo Policy Server configuration can be put in place.

Sudo Policy Server installation scripts **pbinstall** and **pbmakeremotetar** can also be used to perform upgrades and reinstallations.

Pre-upgrade Instructions

Before performing an upgrade or reinstallation, do the following:

1. Obtain the new release, either on a CD or using FTP.
2. Read the release notes and installation instructions.
3. Determine the order for updating the Policy Server host machines. If your current installation includes Policy Server host failover machines, you may want to consider upgrading the Policy Server hosts failover machines first, followed by the submit hosts and run hosts, followed by the primary Policy Server hosts.

> 📌 **Note:** *The settings files on the Policy Server hosts may need to be updated as each Policy Server host is upgraded.*

4. If your current installation includes one or more Policy Server host failover machines, then ensure that the security policy files on the primary Policy Server host and the Policy Server host failover machines are synchronized.
5. Verify the current location of the administration programs, user programs, and log files. This information is in the **pb.cfg** file (**/etc/pb.cfg** or **pb/install/pb.cfg.{flavor})** and the settings file, **/etc/pb.settings**.
6. If you do not have a recent backup of the host, or if it is imperative that no log entries can be lost, then create a save directory (for example, **/var/tmp/pb.{rev_rel})** that can be used to restore Sudo Policy Server files from in case the upgrade fails. After creating the directory, copy (do not use move) the files that are listed below to the new save directory (a shell script can be created to copy the necessary files).

Sudo Policy Server files for all host types
/etc/services
/etc/pb.settings
/etc/pb.cfg (and **pb.cfg.*** on older installations)
/etc/pb.key (if encryption is in use on the system)
pb* log files (typically in **/var/adm**, **/var/log** or **/usr/adm**)

Files for Sudo Policy Server
Database files (contents of **databasedir** which default to **/opt/pbul/dbs)**
/etc/inetd.conf (or your **xinetd**, **launchd**, or SMF configuration file)
Any event log or I/O log files to save
Sudo Policy Server Log Server files
/etc/inetd.conf (or your **xinetd**, **launchd**, or SMF configuration file), **/etc/inetd.conf**
Any event log or I/O log files to save
Sudo Policy Server GUI Host files
/etc/inetd.conf (or your **xinetd**, **launchd**, or SMF configuration file), **/etc/inetd.conf**

7. Determine in which directories to install the new log files, administration programs, and user programs. If you chose different directories for the Sudo Policy Server programs, you might need to update the path variable for the root user and other users.

8. Be aware that users cannot submit monitored task requests while Sudo Policy Server updates are in progress. Consider writing a Sudo Policy Server configuration policy file that rejects all users from executing **pbrun** and echoes a print statement to their screen, informing them that a Sudo Policy Server upgrade is in progress.

9. Sudo Policy Server releases are always upward-compatible when encryption is not used. We recommend that you perform an uninstall if a release is replaced by a Sudo Policy Server version older than v2.8.1.

10. If you use an encrypted settings file and intend to do an upgrade or reinstall, then the unencrypted version of the settings file needs to be restored before performing an upgrade or reinstall; otherwise, the settings file cannot be read.

11. If you have a previous installation of Sudo Policy Server for v5.1 or earlier and your encryption is set to **none**, then when you install Sudo Policy Server v5.2, all the encryption options (options 98 through 103) will be set to **none**. You can change these options during installation.

ℹ️ *For more information on changing these options, please see .*

---

pbinstall Install Upgrades

To upgrade or reinstall Sudo Policy Server with the same configuration as the currently installed version, run **pbinstall** in batch mode:

```
./pbinstall -b
```

If you perform a reinstall of an older version, be aware that the older version may not have the same features as the newer version. In this case, the upgrade process discards the configuration of the features that are not available in the older version of Sudo Policy Server. When you upgrade to the newer version, make sure to configure the newer features when running **pbinstall**.

To change the configuration of Sudo Policy Server during the upgrade or reinstall, run pbinstall in interactive mode:

```
./pbinstall
```

The present configuration is read into **pbinstall**. Make the desired configuration changes and then use the **c** command to continue. **pbinstall** then installs Sudo Policy Server with the new configuration.

ℹ️ *For step-by-step instructions for using pbinstall, please see .*

Post-Upgrade Instructions

If you want to encrypt your settings file after upgrading Sudo Policy Server, then save a copy of the unencrypted file (for future upgrades) and re-encrypt the settings file.

Install Sudo Manager Plugin Client

This section provides details on install Sudo Manager plugin client.

Installation Programs

This section describes the Sudo Manager installation programs and their options.

sudomgrinstall

sudomgrinstall is an interactive script that is used to install the client-side component of Sudo Manager. The **sudomgrinstall** installer program registers the target sudo host and securely transfers the sudoers policy file, along with relevant include files, to the Sudo Manager Policy Server for storage and maintenance. It then lays down Sudo Manager's customized policy (**pbsudomgr.so**), hooking it into the sudo front end configuration (**sudo.conf**), simultaneously deactivating any pre-existing plugins for policy processing.

Syntax

```
sudomgrinstall [options]
```

Arguments

-a architecture	This option and its required argument explicitly specify which Unix or Linux architecture file to install. If the **-a** option is used, then the installer compares the expected flavor and the flavor that is specified with the **-a** option and displays a warning if they do not match.
-b	Runs **sudomgrinstall** in batch mode. In batch mode, the specified existing or default settings are automatically used. User intervention is not allowed and *hit enter* prompts are suppressed. This option also invokes **-e**.
-c	Perform or skip client registration for automatic configuration: **yes:** (default). Perform client registration. Required for initial installation. **no:** Skip client registration and only update local binaries. Use only in upgrade scenarios.
-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 production environment.
-e	Runs **sudomgrinstall** automatically by bypassing the menu step of **sudomgrinstall**. Bypassing the **sudomgrinstall** menu step makes it impossible to change installation options or configurations.
-p	Configures sudo to use Sudo Manager plugin for policy processing.
-C alias	Configures Sudo Manager to create a host alias for this sudo client.
-J alias	Configures Sudo Manager to join a host alias for this sudo client.
-U	Automatically upload the **sudoers** file to the Sudo Policy Server.

-F	Force **sudoers** file upload to the Sudo Policy Server. Any existing **sudoers** file in the repository will be replaced.
-A appid	Set the Application Id for client registration
-K appkey	Set the Application Key for client registration.
-D host	Set the address for the primary server for client registration.
-P port	Specify the port for the primary server for client registration.
-S y|n	Specify **y** or **n** to if Registry Name Service is enabled for your enterprise.
- t	Set the temporary directory to be used during installation. When a temporary directory is defined, **TMPDIR** is overwritten, and the **tempfilepath** is included in **pb.settings**. `-t /tmp/tempdir`
-h	Prints the usage information for **sudomgrinstall** and exits.
-v	Prints **sudomgrinstall** version information and exits.

sudomgruninstall

The **sudomgruninstall** program is an interactive script that is used to uninstall the client-side component of Sudo Manager. The **sudomgruninstall** program deregisters the target sudo host and removes its **sudoers** files from the repository maintained at the Sudo Policy Server. It attempts to restore the sudo host to its state prior to installation: the latest **sudoers** files are retrieved from the Sudo Policy Server and saved back to the original location (e.g., **/etc/sudoers**); references to the custom Privilege Management plugin in the sudo configuration file are removed; and files related to Sudo Manager are uninstalled.

Syntax

```
sudomgruninstall [options]
```

Arguments

-a architecture	This option and its required argument explicitly specify which Unix or Linux architecture file to uninstall. If the **-a** option is used, then the uninstaller compares the expected flavor and the flavor that is specified with the **-a** option and displays a warning if they do not match.
-b	Skip confirmation prompts.
-P	Preserve local **sudoers** policy files. During the uninstallation, by default, the latest **sudoers** file (along with associated include files) are first pulled from the Sudo Policy Server and saved back to the original location on the sudo host. Specifying this option skips this restoration step. 📌 *Note: After initial installation by **sudomgrinstall**, the original **sudoers** files are renamed*

	📌 *(with timestamp as a suffix) since the active sudoers files were automatically maintained by Sudo Manager.*
-A appid	Set the Application Id for client registration
-K appkey	Set the Application Key for client registration.
-h	Prints the usage information for **sudomgruninstall** and exits.
-v	Prints **sudomgruninstall** version information and exits.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

273

TC: 12/7/2022

Install Sudo Manager Sudo Clients

Sudo Manager on hosts with sudo will allow integration between sudo and Sudo Manager. Sudo clients will transfer the sudoers policy to the Sudo Policy Server, and sudo will be configured to use Sudo Manager plugins for policy processing.

When configured for Sudo Manager policy processing, the Sudo Policy Server will store the sudoers policies in the Privilege Management sudoers database. When sudo is invoked, the policy plugin will contact the Sudo Policy Server to retrieve the latest sudoers policy for that client. The sudoers policy from the Sudo Policy Server is maintained in a cache on the client for sudo policy processing.

Sudo is configured to use the customized Privilege Management plugin that reads the sudoers policy from the client cache database. The Privilege Management client will initiate an accept event or a reject event based on the results of the sudoers policy processing.

Supported Platforms

ℹ️ For more information, please see *Supported Platforms* at *https://www.beyondtrust.com/docs/privilege-management/unix-linux/supported-platforms.htm*.

Unix and Linux Utilities

The Sudo Manager installer requires the following Unix and Linux utilities and built-in commands:

awk	cut	getopt	ps	sort	unset
basename	date	grep	pwd	stty	vi
cat	diff	id	read	tar	wc
cd	dirname	kill	rm	tee	xargs
chmod	df	ls	rmdir	touch	
chown	echo	mkdir	sed	tr	
cksum	eval	more	set	trap	
clear	exec	mv	shift	umask	
cp	export	od	sleep	uname	

System File Modifications

Privilege Management modifies **sudo.conf** and replaces **sudoers_policy** and **sudoers_audit** (for sudo v1.9.1+) plugins with the Sudo Manager plugins:

- Plugin **sudoers_policy /usr/lib/beyondtrust/pb/pbsudomgr.so sudoers_file=/etc/sudoers**
- Plugin **sudoers_audit /usr/lib/beyondtrust/pb/pbsudomgr.so sudoers_file=/etc/sudoers**

Prerequisites

Sudo Manager client requires v1.8.23 or higher installed and properly configured on the host prior to Privilege Management installation. Sudo must be built with shared library support to use shared library plugins. Currently Privilege Management does not support LDAP-enabled sudo. During the installation, the installer checks if sudo is configured to use LDAP, and if so, it will exit with an error.

Privilege Management installation uses the client registration capabilities, and requires an Application ID, Application Key, and Client Profile name and the hostname and port for a Sudo Manager Policy Server/REST server. The Sudo Manager Policy Server installation automatically creates two related Application IDs and keys: **PBSUDOADMIN** and **PBSDUOREAD** for administration and read-only access, respectively. The **PBSUDOADMIN** Application ID can be used when installing the Privilege Management client. Other Application IDs can be used as well, as long as the Application ID has the appropriate administration rights.

If, during the installation or upgrade of the Sudo Manager Policy Server/Log Server, the option **Install PBSUDO Policy Server?** is set to **yes**, the install creates a default registration profile **sudodefault** that can be used during the installation of Sudo Manager. The install also creates a file called **/etc/pbsudo.settings.default** stored as **/etc/pbsudo.settings** in **sudodefault** profile.

Although **sudodefault** registration profile created by **pbinstall** on the Policy Server is adequate to use, you can also create your own registration profile.

> ℹ️ *For more information on how to create a registration profile, please see the* [Privilege Management for Unix and Linux Sudo Manager Administration Guide](https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm) *at* https://www.beyondtrust.com/docs/privilege-management/unix-linux/index.htm.

Prior to running **sudomgrinstall**, you need to create an Application ID and Key on the Policy Server.

Run the following command on the Policy Server:

```
pbdbutil --rest -g <appid>
```

For example:

```
# pbdbutil --rest -g sudoappid
{ "appkey":"934bbab5-503e-4c40-8486-90c748142431"}
```

Make sure you copy the value of the appkey generated in a secure, safe file. This information cannot be retrieved after it is generated.

The **sudomgrinstall** default install (option **–d**) can be used to automatically select the default port 24351, the default profile name **sudodefault**, and to automatically execute the generated installation script.

Privilege Management host aliases (not to be confused with sudoers host aliases) can be used to group sudo client hosts that use the same sudoers policy.

Host aliases can be created on the Policy Server, or during **sudomgrinstall**. If a host alias is created, and the sudo client host is added to that host alias on the Policy Server prior to installing the client, that client will automatically detect that the alias is to be used.

If the client does not already belong to a host alias, the interactive installation will normally ask whether a host alias should be created or joined. The **sudomgrinstall** command line option **–C** can be used to create an alias, and the **–J** command line option can be used to join an alias (thus skipping the question during interactive installation).

When not using an alias, the first time the **sudomgr** client is installed on a host, that host's existing sudoers policy file (and any included files) are uploaded to the Policy Server. Any subsequent re-installations do not normally re-upload the sudoers files. The **–U** and **–F** command line options used together will force re-uploading the sudoers files.

Installation

Sudo Manager client is provided as a tarball named **sudomgr{arch}-{version}.tar.Z**.

Prior to running the install script, make sure the path where **sudo** binary is located is in the environment variable **PATH**, and you can successfully run **sudo –V**.

As root:

1. Create directory **/opt/beyondtrust** and **cd** to that directory.

2. Extract the Sudo Manager installation files:

```
# gunzip -c sudomgr{arch}-{version}.tar.Z | tar xvf -
```

3. Navigate to the install directory:

```
# cd sudomgr/{version}/pbsudo{arch}-{version}/install
```

4. Start the **sudomgrinstall** script with the following command:

```
# ./sudomgrinstall
```

The **sudomgrinstall** menu displays options similar to the following:

```
Client Registration provides a method of automatic configuration based upon
    a profile provided by your Primary Policy Server.
To use this functionality you will need to know specific parameters from
    your Primary Policy Server setup. Please see the installation guide for details.
```

5. For a new install, enter the Application ID created on the Policy Server, as well as the Application Key, the name of the host where the Policy Server is installed, the REST port (**pbrestport**) and the registration profile name (default **sudodefault**):

```
Enter the Application ID generated on the Primary Policy Server: PBSUDOADMIN
Enter the Application Key generated on the Primary Policy Server: cefd039d-
    966f-44e2-a2f8-c56804009cfb
Enter the Primary Policy Server address/domain name for registering clients: host1
Enter the Primary Policy Server REST TCP/IP port [24351]:
Enter the Registration Client Profile name [sudodefault]:
```

6. After Client registration, if the client host is not already a member of a host alias on the Sudo Policy Server, the install will ask if you want to join or create a Host Alias on the Sudo Policy Server for this host:

```
A Privilege Management for Unix and Linux Sudo Manager Host Alias, defined in the Policy
Server database, provides a way
    to group clients that must share a common set of sudoers policies.
Would you like to join an existing alias (j), create a new alias (c), or
    skip creating an alias (s) [s]:
```

If **join** is selected, a list of existing aliases is presented. Followed by:

```
Please enter the Privilege Management for Unix and Linux Sudo Manager Host Alias name to
join:
```

If **create** is selected, the installer prompts for the alias name:

```
Please enter the Privilege Management for Unix and Linux Sudo Manager Host Alias name to
create:
```

If **skip** (the default) is selected, or if the host alias requires a sudoers policy, and the client's sudoers policy cannot be located, the installer prompts for the sudoers location:

```
Enter the path of the primary sudoers policy [e.g. /etc/sudoers]:
```

Alternatively, for a fresh install, you can run **sudomgrinstall** with command line options providing the above values (in batch mode **-b** or interactive mode to get the default values of the above set to the command line arguments). For example:

```
./sudomgrinstall -A sudoappid -D host1 -K b3d6e2c0-aee6-493f-87a5-
    d7900d963028 -P 24351 -N sudodefault -S sudo_alias1 -b
```

7. For an upgrade, where **sudoers** file does not need to be re-imported, answer **no** to the prompt:

```
Do you wish to utilize Client Registration which will overwrite /etc/pbsudo.settings and re-
import the sudoers file? [no]?
```

8. A new install copies the files **/etc/pb.settings**, **/etc/pb.key**, **/etc/pbssl.pem** from the Sudo Policy Server to **/etc**.

   It will also import the sudoers file (sudoers and all the included files specified in **#includedir** and **#include**) to the Sudoers database on the Sudo Policy Server.

   It will then replace the **Plugin** variables in **sudo.conf** with Sudo Manager plugins:

   - Plugin **sudoers_policy /usr/lib/beyondtrust/pb/pbsudomgr.so sudoers_file=/etc/sudoers**
   - Plugin **sudoers_audit /usr/lib/beyondtrust/pb/pbsudomgr.so sudoers_file=/etc/sudoers**

Sudo Manager Client Uninstall

Sudo Manager client can be uninstalled by running **sudomgruninstall** located in the **sudomgr/{version}/sudomgr{arch}-{version}/instal**l directory.

Running **sudomgruninstall** will remove all files installed and remove **pbsudomgr.so** plugins from **sudo.conf**.

The **sudomgruninstall** file will normally restore the current sudoers policy (and included policy files) from the Sudo Policy Server, and if not using a host alias, remove the sudoers from the Sudo Policy Server's database. The **–P** command line option can be used to skip this step, thus preserving any local files.

> 📌 **Note:** If there are not any local files (**sudomgruninstall** renames the original), this option will leave sudo in an un-usable state.

Example of a **sudomgruninstall:**

```
BeyondTrust Privilege Management Installation Removal
Exporting latest /etc/pbsudo.settings from /etc/pb.db

This script will remove Privilege Management for Unix and Linux Sudo Manager programs and files
from the system.

Hit return to continue
```

```
Trying /etc/pbsudo.settings
Updating policy files:
/etc/sudoers
Removing PBUL plugin definitions (if any) from /etc/sudo.conf.
Removing plugin definitions (if any) from /etc/sudo.conf.
Removing /usr/sbin/pbdbutil...
Moving /etc/pb.rest.key to /tmp/beyondtrust_pbinstall
Moving /opt/pbul/dbs/pbsvccache.db to /tmp/beyondtrust_pbinstall

BeyondTrust Privilege Management for Unix and Linux Sudo Manager Installation Removal was
successful
Privilege Management for Unix and Linux Sudo Manager configuration files and logs were moved to
    /tmp/beyondtrust_ pbinstall for removal
```