BigFix Patch for RHEL best practices
This document provides best practices and tips for using BigFix Patch for Red Hat Enterprise Linux.

Deploying patches
Ensure that you have done the following steps to avoid deployment issues and errors.
- Gather the latest version of the Patches for RHEL site.
- Install and enable gpg keys.
- Ensure that bzip2 is installed if you are using native tools sites.

Supported updates
BigFix Patch for RHEL supports the following errata updates.
- Security Updates
  The Red Hat Enterprise Linux site indicates strong recommendation for these to be updated.
- Bug Fix updates
- Enhancement updates

BigFix Patch releases Fixlets for all errata updates of supported channels. These updates are based on errata advisories from Red Hat Enterprise Linux. For a list of Red Hat Enterprise Linux erratas, see https://rhn.redhat.com/errata/.

To see the versions and channels that BigFix Patch for RHEL supports, see http://www-01.ibm.com/support/knowledgecenter/SS6MER_9.2.0/com.ibm.tem.patch.doc_9.2/Patch_Man/Patch_Man_RH/c_supportedPlatforms.html

Updating RHEL packages
Install errata packages regularly.
It has been assumed that updating errata packages can lead to an unstable system or cause unnecessary risk but in fact the opposite is true. If these packages are not installed, many software bugs will stay unresolved. The best system administrators prefer to deploy all the errata packages diligently.

The probability of encountering a bug increases over time if updates are not installed. For example, there was a case where a new kernel was needed to resolve a security vulnerability. The kernel required a prerequisite bug fix IRQ package which was not listed as a dependency for the kernel package. Installation of the kernel without the required IRQ package resulted in widespread outages and performance issues. See https://rhn.redhat.com/errata/RHBA-2014-0489.html. This issue would not have occurred if errata packages had been installed along with the new kernel.

Previous Red Hat Enterprise versions better tolerated the installation of RHEL packages from multiple update levels onto a server. RHEL versions 6 and 7 are not as tolerant of mixing update levels. Little testing is performed by Red Hat and their partners for such uncommon patching scenarios. Most Red Hat packs now include disclaimers stating that ALL previously released patches applicable to that system should be applied prior to installation of that specific patch.

Red Hat download plug-in
- Ensure that you have the latest plug-in version and that the correct credentials are registered. This avoids the action reporting back a failed download.
- If the downloads must go through a proxy server, enter a well formed proxy server URL which contains a protocol and a host name. The URL is usually the IP address or DNS name of your proxy server and its port, which is separated by a colon. For example: http://192.168.100.10:8080.
RHEL Custom Repository Management dashboard

Check the following to avoid failed deployments in the dashboard:

- When registering the endpoints, add `gpgcheck=0` to Additional fields.
- The client setting setting `_BESClient_RHEL_AllowYumDownloads` in the endpoints is set to 1.

Patching baselines

For best practices about patching baselines, see the corresponding section in http://www-01.ibm.com/support/docview.wss?uid=swg21636385.

Auditing baselines

You can see the changes made to baselines in the `LOCAL_OBJECT_DEF` table. The table includes the history of the object (including custom Fixlets, groups, properties, and tasks) that provides in effect an audit trail.

Try `select * from LOCAL_OBJECT_DEFs where name = '`. Alternatively, if you export all content (including analyses, baselines, Fixlets, and tasks) as .xml BES files and check them into GIT source control daily using the REST API, only items that have been changed get checked in to the commit. This allows you to see the additions, deletions, and modifications that were made to serve as both backup and an audit trail.

Patching sources

External Red Hat Network accessed via the Internet (use of a forwarding proxy by endpoints that have no direct Internet access)

- Red Hat Network Proxy or Satellite Servers (may still require a forwarding proxy to obtain patches from Red Hat)
- Local patch repositories where endpoint entitlement is 100% verified before patch installation using guidance from the following Red Hat reference:
  - How to create a local mirror of the latest update for Red Hat Enterprise Linux 5, 6, 7 without using Satellite server: https://access.redhat.com/solutions/23016
  - How to use "createrepo" or "reposync" to create a local repository for updates: https://access.redhat.com/solutions/9892

Checking logs and configuration files

Refer to logs and configuration files:

Auditing baselines

You can see the history of an object, including baselines in the `LOCAL_OBJECT_DEF` table. To do so, try `select * from LOCAL_OBJECT_DEFs where name = '`

Deployment logs in the endpoints

Go to `/var/opt/BESClient/EDRDeployData`.

EDR_PackageSpec files (to check if sha1 is included)

To check if sha1 is included in the EDR_PackageSpec files, check the files in the `/var/opt/BESClient/_BESDATA/Patches` for RHEL x folder.

RHEL Custom Repository Management dashboard

- Service logs
  - `/var/opt/BESClient/EDRDeployData/register-repo.log`
  - `/var/opt/BESClient/EDRDeployData/register-satellite.log`
  - `/var/opt/BESClient/EDRDeployData/unregister-repo.log`

- Repository configuration
  Go to `/etc/yum.repos.d/`. The configuration includes the user name and password of your repositories.
**YUM transactions**

YUM log is the official log that YUM generates by default in `/var/log/yum.log`.

**Using Extended Update**

For RHEL versions that are no longer receiving updates from Red Hat, users can purchase the Extended Update Service (EUS) or Extended Lifecycle Support (ELS). The add-ons provide security packages and some bug fix packages for a finite period of time. Eventually the add-ons reach end of support and an upgrade is required.

For more information about ELS, see: [https://access.redhat.com/solutions/690063](https://access.redhat.com/solutions/690063)

For more information about EUS, see: [https://access.redhat.com/articles/rheus.BigFix](https://access.redhat.com/articles/rheus.BigFix)