IBM BigFix Patch

Patching AIX Systems Using BigFix

Best Practices Guide

Version 1
August 8, 2016

Table of Contents

1.0 Overview

This document contains a compilation of best practices, assumptions, and requirements to help both AIX system administrators and BigFix console operators to successfully patch AIX endpoints using BigFix.

This document was written with the assumption that its readers possess basic knowledge of the AIX operating system, the patch management lifecycle, and BigFix. It covers some basic concepts and features provided by BigFix Patch for AIX. However, it does not provide information about AIX operating system migration or the Service Update Management Assistant (SUMA).

Note that the Fixlets and tasks mentioned in this document are available from the **Patches for AIX** site, unless stated otherwise.

2.0 Concepts and Capabilities

2.1 AIX Lifecycle

This section was taken from the *IBM AIX Operating System Service Strategy and Best Practices Guide*.

An AIX Release lifecycle is approximately 10 years:

6 years of usage and fix support under standard SWMA

3 years of optional, separately priced Extended Support

1 year of self-assist service on the Internet

AIX technology levels (TL) remain “active” for 3 years.

During this active period, new fixes will be released in the form of service packs (SP).

Also, during this active period, interim fixes (iFixes) can be provided.

2.2 AIX OS Level Format

AIX determines the OS Level by comparing the installed filesets to a list of known APARs. This means that OS levels can change by installing new packages.

The AIX OS level is in the following format:
<OS Version>-<TL>-<SP>-<BUILD DATE>

For example:
7100-01-03-1207
| | | '---------- Release Date: Week 07, of Year 2012
| | '----------Service Pack 3
| '---------- Technology Level 1

Use the **Determine OS Level** Fixlet (ID #6) from the **Patches for AIX** site to determine the current OS level of an endpoint.

2.3 AIX Patch Types in BigFix

2.3.1 Technology Level

Technology levels (TLs) contain all fixes from the previous service pack (SP) levels. They are released twice a year and require a reboot.

TLs use the following naming convention: *<OS release>-<TL number>*. For example, 6100-01 and 6100-02.

BigFix provides Fixlets to deploy TLs to endpoints, either through the download plug-in or NFS share.

2.3.2 Service Pack

Service packs (SPs) contain all Program Temporary Fixes (PTFs) for highly pervasive issues and interim fixes. They are released several times a year (every 4 to 6 weeks) and require a reboot.

SPs are named based on Release, Technology Level, Service Pack, and Release Date: *<RELE>-<TL>-<SP>-<YYWW>*. For example, 6100-06-07-1207 is AIX 6.1 TL 6 SP 7 and was released in the 7th week of 2012.

The concluding SP is the final service pack for a TL. It usually contains fixes for critical problems or security patches.

SPs always require a reboot, so they are recommended for planned maintenance windows or when the application of the fix will still require a reboot at the end of the upgrade.

BigFix provides Fixlets to deploy SPs to endpoints, either through the download plug-in or NFS share.

2.3.3 Interim Fix

An interim fix, or ifix (previously called an emergency fix or efix) is a code update to resolve a specific known problem, or APAR, while an official PTF is undergoing the formal development process.

Interim fixes are labeled as follows:

<APAR>[s|m]*<SP><sequence>*

IV14130s5a

| || '--------- sequence letter

| | '---------- Service Pack

| '------------ (s)ingle or (m)ulti fix.

'-- APAR Number

Interim fixes are intended as temporary fixes and are released as needed. They can be requested if the TL or SP is not applicable.

AIX provides the following interim fix content:

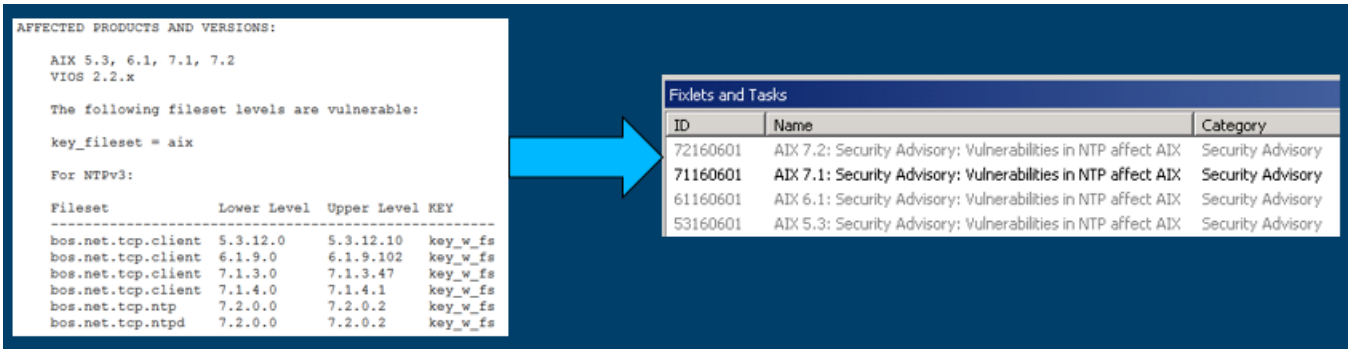
- High Impact PERvasive (HIPER)
  Resolves defects that have a combination of both high impact and pervasiveness. It indicates an Authorized Program Analysis Report (APAR) that contains an untested fix.
- PTF in Error (PE)
  Resolves functional regression. It indicates a Program Temporary Fix that contains a tested fix. It is usually released to close the APAR. Interim fixes for PE are usually under another HIPER.
- Security Advisories
  Indicates several security issues rather than a bug. A security advisory might be applicable to multiple AIX versions, but an interim fix might not necessarily be provided for all the versions listed.

Two types of Fixlet content are available in the BigFix console, and can be used to ensure that endpoints are secure and contain the fixes based on an endpoint's APAR applicability:

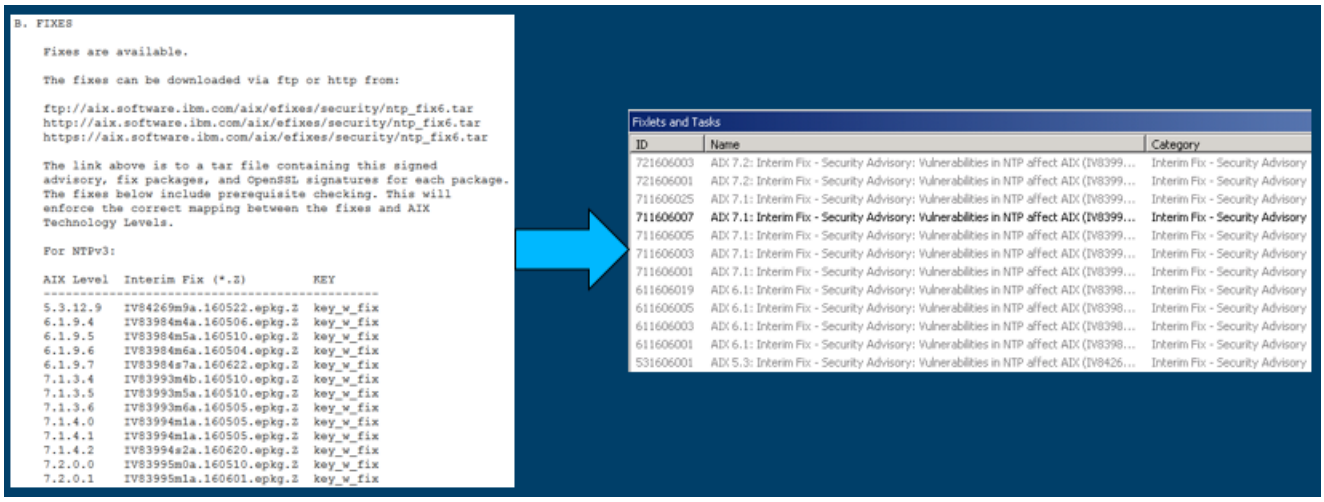
- Audit Fixlet
    - Mainly for inventory and tracking purposes, which means that it doesn't contain the patch to apply the fix. However, it does provide a link to retrieve more information about the APAR, as well as steps about how to manually create a custom Fixlet through the AIX Interim Fix Management Wizard. For more information about the wizard, see

Creating Fixlets by using the AIX Interim Fix Management Wizard

- Displays as relevant if the APAR is applicable to an AIX system (OS-version specific).
- Includes HIPER, PE, and Security Advisories.
- Affected products and versions are mapped to BigFix Audit Fixlets, which means there is one Fixlet for each affected AIX version.



- Interim Fix Fixlet
  - Provides a way to automatically apply the fix to the endpoints directly from the BigFix console. The interim fix package (.epkg.Z file) is downloaded from Fix Central and deployed to the targeted endpoints.
  - Displays as relevant if the APAR is applicable to an AIX system based on its current SP level.
  - Includes Security Advisories (SA) and High Impact/Highly Pervasive Fixes (HIPER) interim fixes for IBM AIX versions that are active in the last three years. These Fixlets check for locked filesets or earlier installed interim fixes and uninstalls them before installing the fix.
  - BigFix maps interim fixes with the Interim Fix Fixlets, this means that there is one Fixlet for each interim fix.



***TIP**: To differentiate between these two types of content, note that the interim fix Fixlet uses the following prefix in the title:*

- *Interim Fix – Security Advisory*
- *Interim Fix - HIPER*

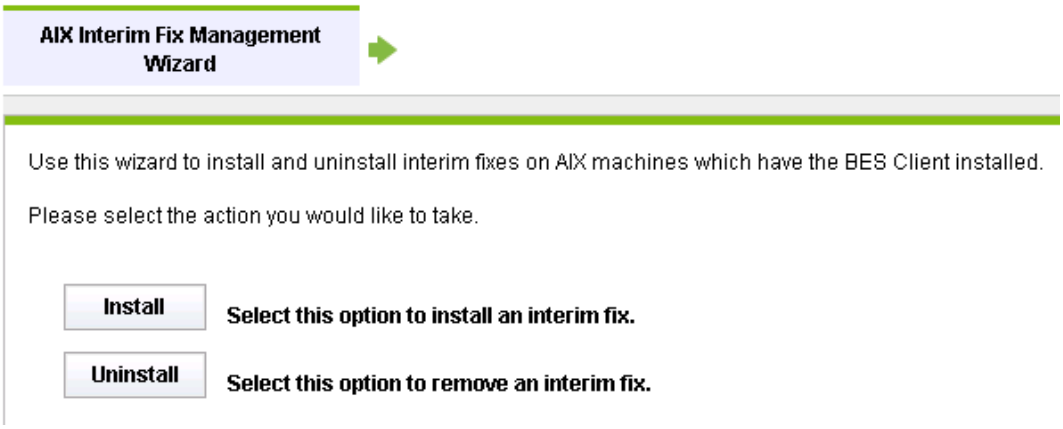
Interim fixes lock their target filesets preventing any changes from being made while the interim fix is being installed.

Starting with 5.3 TL10 and 6.1 TL3, interim fixes are automatically removed by an update if the TL or SP that is being applied contains the permanent fix for the defect. In cases where the TL or SP does not contain the permanent fix (commonly occurs for open source applications), it is recommended that all interim fixes be uninstalled prior to deploying any TL or SP update. To facilitate this process, use the **Uninstall All Interim Fixes** Fixlet (ID #63) to remove all interim fixes that are installed. The applicable interim fixes must then be applied right after the TL or SP update to ensure secure endpoints.

To find more information about interim fixes from IBM Knowledge Center, see Interim Fix support.

Creating Fixlets by using the AIX Interim Fix Management Wizard

Use the **AIX Interim Fix Management Wizard** to create Fixlets to install customized interim fixes (.epkg.Z file types) on AIX systems. This wizard also provides options to remove individual interim fixes.



For more information about the wizard, see Creating Fixlets for interim fixes.

2.3.4 PTFs

A PTF is a Program Temporary Fix and provides a solution for a problem.

AIX provides individual downloads for certain PTFs only. For example, PTFs containing bos.rte.install, bos.alt_disk_install.rte, or PTFs that are released between Service Packs. Otherwise, the TL or SP must be downloaded.

BigFix provides Fixlets to deploy PTFs to endpoints, either through the download plug-in or NFS share.

2.3.5 Firmware Updates

BigFix provides a firmware update solution to endpoints that are not managed by IBM Hardware Management Console (HMC). If the system is managed by HMC, apply the server firmware from HMC.

Note: When a system is running in an LPAR and a firmware upgrade is initiated, a system reboot will be required. This means that the entire server along with all the LPARs will be unavailable during the downtime, so deploy firmware updates at a time when it is less disruptive to the users.

3.0 Prerequisites and Recommendations

3.1 Required Packages

Ensure that the following packages exist on all the target endpoints.

- Bash
- Expect 5.4 or later (required for compliance patch management)

3.2 Relay Infrastructure

Use a relay to cache content closer to the endpoints that are being updated. A cache at the top-end can speed things up. Consider a relay to cache the content in the same data center or WAN link, or similar, to greatly increase the speed.

3.3 Disk Space

3.3.1 BigFix Server and Relays

Ensure that the BigFix root server and BigFix relays have enough space to cache packages. A package is cached during its initial download, and subsequent downloads of that same package will come from the root cache or relay. It is recommended to set the BigFix server and BigFix relay cache size to 30 GB by using the **BES Relay/ BES Server Setting: Download Cache Size** Fixlet (ID #148) from the **BES Support** site.

3.3.2 BigFix Clients

Most AIX deployments have a limited amount of space available in the /var filesystem. This can be a problem when deploying TLs that are very large in size. TLs can be larger than 6 GB, which means that the /var filesystem needs to have free space of at least twice the size of the TL to extract the filesets and to complete the installation.

The Fixlets for TL and SP deployment contain a check for available disk space, but this check is performed only after the filesets are downloaded and are cached. The cached filesets are copied to the /var/opt/BESClient as part of the deployment process. If the /var/opt/BESClient has insufficient disk space to store the filesets, the Fixlet action fails.

Patching via the download plug-in directly from the BigFIx server requires at least 10 GB on the endpoint. If that much space is not available, patching can be done via NFS.

If patches are deployed using the AIX download plug-in, it is recommended that you create a dedicated filesystem for /var/opt/BESClient to provide it with sufficient free space. As a best practice, to prevent the AIX operating system from running out of disk space, allocate the additional dedicated space out of a volume group other than rootvg.

3.3.3 Available Content for Disk Space Configuration

BigFix provides Fixlets to help ensure that sufficient space is available in the BigFix server, relays, and clients to successfully patch systems.

The following Fixlets are available in the **Patches for AIX** site to modify the BigFix client settings. These configuration changes are necessary only if patches are deployed using the direct download via the download plug-in.

- **AIX: Set Disk Space - BES Data Folder** Fixlet (ID #57)
  Addresses the disk space limitation on the BigFix client by increasing the space of the BES data folder (if available). It is recommended that the BES Data directory have at least 10 GB of free space.
- **AIX: Remove File Size Limit for Root User** Fixlet (ID #60)
  Addresses the file size limitation on the BigFix client by removing the file size limits for root user.
- **AIX: Change BES Client Download Limits** Fixlet (ID #59)
  Addresses the BES Client download limitation by changing the download Limit to allow downloads that are of 10 GB in size.

The following Fixlets are available in the **BES Support** site to manage the BigFix server and relay cache size and BigFix client CPU usage.

- **BES Relay/ BES Server Setting: Download Cache Size** Fixlet (ID #148)
  Addresses patching issues with large downloads by increasing the disk cache on the BigFix server and relays to accommodate the patches being deployed.
- **BES Client Setting: CPU Usage** task (ID #168)
  Addresses slow response issues between the BigFix Server and the client by increasing the allowed CPU usage on the client.

3.4 Repositories (NFS/NIM)

According to the guide called *Best Practices: Managing AIX Updates using SUMA, NIM, and AIX Service Tools*, keeping updates in separate repositories is ideal if only specific updates are to be applied to the endpoints.

There are two important things to keep in mind when using a remote repository over an NFS mount.

- The required files must already be stored in the remote repository before running the install action. There are no checks or verifications of required packages performed by the install action. Use the NFS Repository Management feature from the **AIX Advanced Deployment Wizard** to download the fix packs. Repositories can also be built though a NIM server (an existing lpp_souce directory works well) or by running the AIX Download Cacher with the "--repo" parameter.
- Remote repositories are mounted in a read-only state so a current .toc file must exist in the remote directory prior to running the update action. It is not necessary to rebuild the .toc file before every update installation. If using a NIM server, this .toc file is created automatically. Use the **Generate Fileset Repository TOC file** task (ID #55) to create the table of contents.

3.5 Rebooting

Certain packages and patches require a reboot to activate the update or fix, especially for kernel and library patches.

Fixlets for TL or SP updates and interim fixes report back as 'Pending Restart' when the patch has run successfully. It does not report back the final status until the system is restarted. Use the **Restart Computer** task (ID #62) to reboot AIX systems.

3.6 Testing AIX Patches

It is recommended that you test the patches through the released Fixlets before installing them on the endpoints. This is to ensure that all possible conflicts have been identified in a test environment before installing the patches in the production environment.

3.7 Previewing Updates

Always perform a preview installation before attempting any software installation to verify that all of the updates, including any requisite updates, are available (downloaded from Fix Central, installation media, NFS share).

A preview installation or update of an actual TL or SP update, can help foresee issues that will likely occur during the actual installation, especially failures due to locked filesets. When running a preview, a list of interim fixes is provided. This list includes both interim fixes that can be automatically removed and those that are installed but cannot be removed because the corresponding fix is not available in the updates that are currently installing. Preview installations are always highly recommended, even if there are no interim fixes applied.

Create Fixlets to preview the installation or update of TLs, SPs, PTFs, filesets and firmwares from the **AIX Advanced Deployment Wizard**. For more information, see Creating verification checks (preview).

You can view the results of the preview from the **AIX Pre-Install Verification Results** analysis or in the **Deployment AIX Health Checks** Dashboard. See Deployment AIX Health Checks Dashboard overview.

For customized interim fixes that were created from the **AIX Interim Fix Management Wizard**, manual configuration of the available Fixlets is required to include the -p option in the actionscript. For more information, see Creating Fixlets for customized interim fixes.

3.8 Baseline

Limit the number of components in a baseline to ensure the best possible performance on the clients and relays. Having a baseline that's too large can lead to performance issues that could affect the client and relays ability to gather, evaluate, and report. To know more about the best practices for creating, using, and maintaining baseline actions, see Baseline Best Practices.

Other articles that might come in handy are as follows:

- Best practices for baselines from the devWorks wiki
- Running Baselines in Sequence

4.0 Deploying AIX Patches

BigFix provides different methods of deploying AIX patches. The correct method to use depends on the type of patch that must be updated.

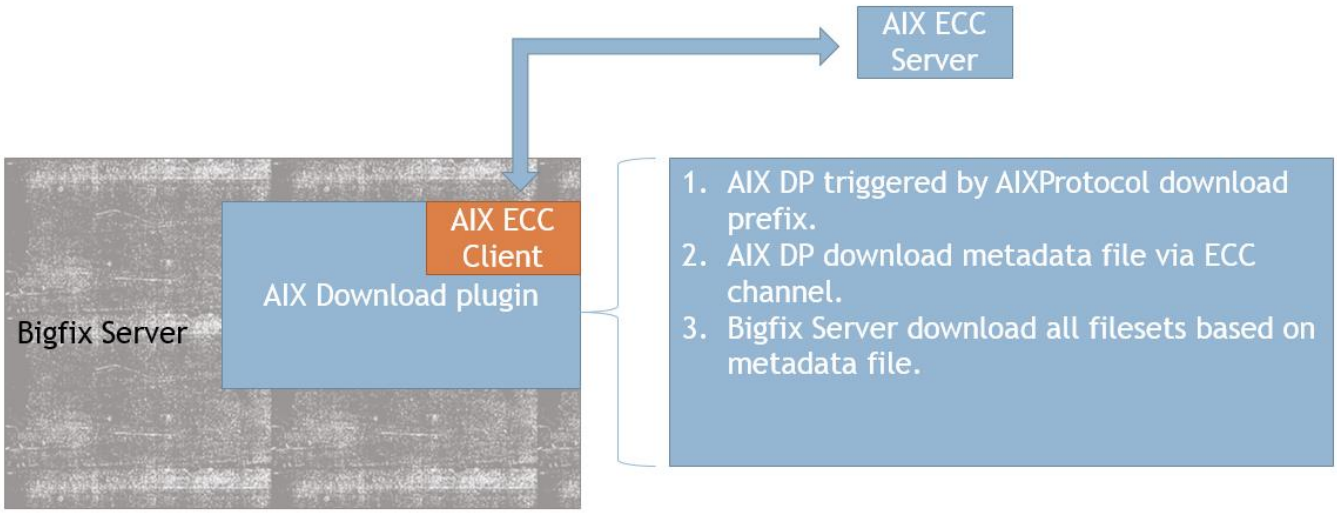
AIX Patch	BigFix Content	Deployment Options
Fix pack for Technology Level / Service Pack	Fixlet	Download plug-in / NFS
Interim fix for Security Advisory	Audit Fixlet / Fixlet	Direct download via BigFix
Interim fix for HIPER	Audit Fixlet / Fixlet	Direct download via BigFix
Fix pack for open source package & Java SDK	Audit Fixlet	AIX Deployment Wizard

Each patching method has its own set of advantages and disadvantages, which we will attempt to cover in this section.

4.1 Patching Methods

4.1.1 Direct Download using the Download Plug-in

The AIX download plug-in is an external executable program that uses the Electronic Customer Care (ECC) services to download AIX updates from IBM. Filesets are downloaded and cached on the BigFix server, allowing them to be reused for later deployment. The files are then downloaded to the targeted endpoint (/var/opt/BESClient) and installed from there. This approach can help save time from having to download the same set of filesets every time an action is taken against a Fixlet.



The default action in all the available Fixlets for TL and SP uses the download plug-in to download the necessary filesets.

This method is the easiest one to set up, in terms of maintenance cost, although it requires at least 10 GB of free disk space on the endpoint (/var/opt/BESClient) to accommodate the downloaded patch content.

Considerations when using this approach:

- Register and configure the AIX download plug-in from the **Manage Download Plug-in** dashboard (available in the Patching Support site). See Registering the AIX download plug-in.
- Register the AIX download plug-in only on the IBM BigFix server.
- In case of insufficient disk space, use the available Disk Space Configuration to adjust the space and size limitations.
- When using proxies, verify that:
    - The proxy is working and does not block traffic.
    - The proxy user account has rights to the IBM site to download the packages.
    - The AIX download plug-in (under the Patching Support site) is registered and configured.

4.1.2 Direct Download using the Download Cacher

The AIX download cacher is a stand-alone executable tool that runs on a Windows operating system. The tool downloads filesets for TLs or SPs to a user specified location in either an individual fileset format or archived into a single .aix file.

The sha1 filename for each fileset is not generated by the tool, which means that the filesets cannot be directly cached on the BigFix server. However, the filesets can stored on an NFS share or used by the AIX Deployment Wizard to deploy the TL or SP fix packs.

It is recommended that you use this tool for air-gapped environments.

For more information about the download cacher, see Using the AIX download cacher.

4.1.3 Network File System (NFS) Share

NFS is a distributed file system that allows users to access files and directories that are on remote computers and handle those files and directories as if they were local.

All the available Fixlets for TL and SP provide an option to install the packages from an accessible NFS share. Because these patches can be large, downloading and extracting them directly to the endpoint can take some time. Deploying patches from an NFS share shortens the installation time, decreases bandwidth usage, and reduces storage costs.

This approach works well with systems that have limited storage because the fix packs that are to be deployed and installed on the endpoints can be accessed by mounting the NFS share. This approach minimizes the space disk requirement on the target systems because the Fixlets access the NFS share for the required files. No local storage is needed.

Considerations when using this approach:

- The specified NFS share must be pre-populated with required filesets and built days before the actual patching.
  Use the NFS Repository Management feature in the **AIX Advanced Deployment Wizard** to manage the TL and SP fix packs on registered NFS repositories.

Alternatively, use the AIX Download Cacher (without creating an archive file) to download the filesets, and then copy them to the NFS share.

- Verify the fix packs stored in the NFS share to ensure that the content is complete and valid before installation.

  Use the NFS Repository Management solution in the **AIX Advanced Deployment Wizard** to verify the integrity of the fix packs in an NFS share to prevent installation failures caused by missing or outdated fix packs.

- Setting up and maintaining multiple NFS shares is required for endpoints that are distributed over a wide area network.

4.1.4 Network Installation Manager (NIM)

Use NIM to remotely manage upgrades on multiple AIX systems while reducing down time.

Note: This section mainly covers the capabilities of BigFix to integrate with existing NIM environments.

BigFix provides an alternative solution for updating and managing multiple AIX systems through NIM, which is an AIX native tool. BigFix supports the NIM patch management features to remotely manage AIX installations and updates in multiple AIX systems in an environment.

NIM uses NFS-based repositories that contain the filesets to deploy; it does not provide control over individual patches.

To use existing NIM setups, use the functions that are available in the NIM Management Dashboard to install, configure, and manage NIM server and clients. For more information, see NIM dashboards overview.

With NIM, download the latest TL or SP to the NIM server and by using BigFix, either mount the NFS export from the NIM server and do an installp update_all operation (through the **NIM Management Dashboard > NIM Update Operations > Update NIM Components from NIM Master**), or run the NIM command on the NIM server to push the updates (through the **NIM Management Dashboard > General NIM Management Operations > Enable/Disable Push Permissions**).

4.2 Applying Technology Level and Service Pack updates

When to patch

Consider performing a TL upgrade in the following three cases:

- The currently installed TL is going out of the available support period.
- To test a new technology level that is going to go into production and needs to get the longest period of fix support.
- To use the new features and functionality of the TL.

However, there is really no such thing as a right or wrong time to perform an upgrade. It all depends on your requirements and priorities.

If the requirement is to have a stable environment that has maximum uptime, then wait until new TLs have been out for at least six months to a year before applying them.

To take advantage of new features and ensure that the systems have the latest security patches, install new TL updates soon after they come out.

Overall, as a best practice to obtain a better, secure, and reliable environment, upgrade TLs and SPs as soon as they come out.

How to patch

BigFix provides out-of-the-box Fixlets to deploy TL and SP updates.

For planned maintenance windows, apply SPs as a group to simplify inventory and make it easier to report levels to auditors. It is not recommended that you apply individual filesets because this might cause unexpected results. It is recommended that you apply the whole SP or TL as a full fix pack bundle instead of just individual PTFs or filesets.

You can deploy a TL or SP update by using either the AIX Download Plug-in or an NFS share. To compare the advantages and disadvantages of each approach, see Patching Methods. For more information about deploying Fixlets, see Deploying technology level and service pack updates.

***Note**: Installing a subset of a TL using the* **AIX Deployment Wizard** *is not recognized from a support standpoint due to complications of circular requisites.*

Starting with 5.3 TL10 and 6.1 TL3, interim fixes are automatically removed by the update if the TL or SP that is being applied contains the permanent fix that the interim fix was patching.

4.3 Applying Interim Fixes

When applying interim fix Fixlets, ensure that the systems have internet access; otherwise, the interim fix download fails.

For more information about interim fixes, see the following resources:

- Interim fix overview

- Interim fix support
- Deploying interim fixes

For customized interim fixes that are unique to a customer's environment, use the **AIX Interim Fix Management Wizard** to create Fixlets to deploy the interim fixes. For more information about the wizard, see Creating Fixlets for interim fixes.

4.4 Applying Open Source Filesets

Use the **AIX Deployment Wizard** to update individual open source filesets such as OpenSSL and IBM Java.

Download the filesets that you want to apply and use the Folder option in the **AIX Deployment Wizard** to distribute them across your endpoints. For more information, see the steps in Creating Fixlets for AIX fileset updates.

4.5 Applying Firmware Updates

Use the **AIX Deployment Wizard** to deploy packages for firmware updates on endpoints that are not managed by IBM Hardware Management Console (HMC).

Download the .iso or .rpm files from Fix Central without renaming the files because firmware information is parsed from the file names.

For information about applying firmware updates, see the following topics in IBM Knowledge Center:

- Creating Fixlets for firmware updates
- Deploying Fixlets for firmware updates

For more information about the firmware update solution, see http://www-01.ibm.com/support/knowledgecenter/POWER7/p7ha5/fix_firm_no_hmc_aix.htm?cp=POWER7 "Committing" filesets.

5.0 System Backup and Recovery

One of the most important aspects of patching is to have a backup and recovery plan in place. When things go wrong (power outages, disk drive failures, and more), the aim is to decrease the downtime and bring the system back up to a stable state as quickly as possible.

Alternate disk and multibos are used to apply TL and SP updates to AIX endpoints without disruption, only rebooting after the upgrade is done.

Alternate Disk	Multibos
A free disk is needed to clone the primary disk	Create another bootable instance of Base operation system (BOS) on the same disk
Everything is copied	Copy the following logical volumes (LV): /; /usr; /var; /opt; hd5. All other LVs are shared

5.1 Alternate Disk

BigFix provides the **AIX Advanced Deployment Wizard** to manage and patch alternate disk images instead of the active or booted operating system. With the alternate disk solution, the operating system can be updated to the next TL or SP without disrupting the machine or having to take it down for an extended period of time.

Alternate disk patching creates a mirror image of the rootvg and patches. Maintaining an active mirrored copy of the rootvg volume on another disk ensures the continuous operation of the AIX operating system in event of a disk failure. Note that BigFix supports two-way mirror only.

As a best practice, break the root disk mirrors before any OS patches are deployed in case issues occur during or after patching.

Having an alternative disk or mirror management solution in place can help save time and cost during system recovery or roll back due to issues encountered post patch.

Considerations when using this approach:

- A secondary disk to clone the current disk is required.
- Run the **Deploy AIX Startup/Shutdown script for alt disk reboot** Fixlet (ID #84) before running any alt disk task, or the task will fail after a reboot.

For more information about alternate disk patching and mirror management, see the following topics in IBM Knowledge Center:

- Alternate disk solution in the AIX Advanced Deployment Wizard
- Mirror management solution

5.2 Multibos

BigFix provides the **AIX Advanced Deployment Wizard** to deploy TL or SP updates (either by the AIX Download Plug-in or an AIX NFS mount) to endpoints with a standby BOS instance without impacting the active BOS instance. By using the multibos solution, you can ensure continuous operation of the AIX operating system on the endpoint.

With multibos, two separate bootable instances of the base operating system (BOS) within the same root volume group (rootvg) can be created, saving costs from maintaining a separate disk.

Use multibos in environments with tight maintenance windows to manage system downtime and risk when upgrading endpoints.

Considerations when using this approach:

- The current rootvg must have enough space for a new BOS logical volume.
- Run the **Deploy AIX Startup/Shutdown script for multibos reboot** Fixlet (ID #92) before running any multibos task, or the task might fail after reboot

For more information, see the following topics in IBM Knowledge Center:

- Multibos support
- Multibos solution in the AIX Advanced Deployment Wizard

6.0 Reporting

6.1 Compare Report

BigFix provides Fixlets to help determine if any filesets are outdated or belong to earlier versions of a TL. Having the information available allows you to maintain a proactive fix strategy by providing a way to ensure that your systems are at an expected level. A comparison can be done between the filesets installed on a stand-alone system and the contents of a NIM lpp_source or fix repository (NFS or BigFix server).

To facilitate retrieval of the compare report, deploy the **Commit Applied Filesets** Fixlet (ID #3) and the appropriate Run Compare_Report Fixlets:

- **Run Compare_Report – AIX 5.2** (ID #15)
- **Run Compare_Report – AIX 6.1** (ID #39)
- **Run Compare_Report – AIX 7.1** (ID # 52)
- **Run Compare_Report – AIX 7.2** (ID #90)

View the results from the **Compare_Report Results** analysis (ID #17).

6.2 Instfix Report

Instfix determines if all files are up to the current maintenance level.

Run the report after deploying TL or SP updates. Use the **Run Instfix Command** Fixlet (ID #19) and the **Instfix Results** analysis (ID #20) to generate the report.

Appendix A: Logs

Collect the following logs and data for troubleshooting IBM BigFix Patch for AIX issues.

When problems occur, determine what went wrong by viewing messages in the appropriate log files, which provide information about how to correct errors.

Feature/Component	**Log directory and names**
AIX Download Plug-in	AIXProtocol/logs directory of the default DownloadPlugin directory on the IBM BigFix server For example, For Windows systems: C:\Program Files (x86)\BigFix Enterprise\BES Server\ DownloadPlugins\AIXProtocol\logs For Linux systems: /var/opt/BESServer/DownloadPlugins/AIXProtocol/logs
NIM operations	<Path to Endpoint Manager Data Directory>__NIM_Logs/NIM_Operations_*<yyyymmdd>*.log For example, /var/opt/BESClient/__BESData/__NIM_Logs/NIM_Operations_20130520.log.
Installation logs (admin)	/var/adm/ras on the target system
Interim fix installation log	/var/opt/BESClient/__BESData/__iFixInstall/*<ifix_number>*.epkg.Z_result.log
BES Data disk space	/var/opt/BESClient/__BESData/
AIX download cacher	Default log directory of the IBM BigFix client on the target system.
Preview deployment feature of the AIX Advanced Deployment Wizard	/var/opt/BESClient/__BESData/__MLPkgInstall/PreviewLog/preview_*<os_level>-<technology_level>-<service_pack>-<build_date>*
Fileset inventory	/var/opt/BESClient/__BESData/__AIXInventory
Breaking mirrors	/var/adm/ras/altDiskNewDeploy.log
Re-mirroring mirrors	/var/adm/ras/reMirror.log
Results of the reboot command for operating systems in an alternate disk environment	/var/adm/ras/KZCopyAltDiskBESDATA.log /var/adm/ras/SZCopyAltDiskBESDATA.log

Feature/Component	Log directory and names
Multibos	Log files (/var/adm/ras/Multibos*.log) of Multibos Tasks: MultibosExpress.log: the results of Multibos Express task MultibosCreateClone.log: the results of the standby BOS creation task MultibosFixPackDeploy.log: the results of the standby BOS update task MultibosExpress_emgr.log & MultibosFixPackDeploy_emgr.log: the results of the removal of interim fixes on the standby BOS before installing the updates MultibosDeleteClone.log: the results of the standby BOS removal action

Appendix B: Resources

IBM AIX in IBM Knowledge Center: http://www.ibm.com/support/knowledgecenter/ssw_aix/welcome?lang=en

AIX Support Lifecycle Information: http://www-01.ibm.com/support/docview.wss?uid=isg3T1012517

AIX Technology Level update strategies: http://www.ibm.com/developerworks/aix/library/au-aixtlupdate/

NIM Cheat Sheet: http://www.ibm.com/developerworks/aix/library/au-aix-nim-cheat-sheet/index.html

Managing Interim Fixes on AIX: http://www-01.ibm.com/support/docview.wss?uid=isg3T1012104

IBM Fix Central: https://www-945.ibm.com/support/fixcentral/

IBM BigFix Patch for AIX User Guide in IBM Knowledge Center: https://ibm.biz/BdrrLp

IBM AIX Operating System Service Strategy Details and Best Practices: https://ibm.biz/BdrrLh

Interim Fix Information: https://ibm.biz/BdrrLV

Listing Interim Fixes: https://ibm.biz/BdrrLg