IBM AIX Operating System Service Strategy and Best Practices

AIX Development

2016

Evan Zoss
evanzoss@us.ibm.com

Introduction

This paper describes the current AIX Service Strategy and Best Practices for maintaining AIX.

New Developments

AIX 7.2 Live Update

New in AIX 7.2 the AIX Live Update function lets you apply iFixes without rebooting! For more details, please see the AIX 7.2 release notes:
http://www.ibm.com/support/knowledgecenter/ssw_aix_72/com.ibm.aix.rnbase720/rnbase720.htm

Security iFixes

Security Alerts which publish iFixes to patch the vulnerability will now include iFixes for the most recent 3 Service Packs (the latest SP, n-1, and n-2) on each active Technology Level, whenever possible.

Connect

Facebook

- IBM AIX and Power Systems: https://www.facebook.com/groups/poweraix/

LinkedIn Groups

- IBM PowerVM: https://ibm.biz/powervmgrp
- AIX Techonology Forum: https://ibm.biz/aixgroup
- PowerHA SystemMirror: https://www.biz/powerhagrp
- PowerVC: https://ibm.biz/powervclink

developerWorks

- IBM PowerVM: https://ibm.biz/powervmwiki
- IBM AIX: https://ibm.biz/aixwiki
- PowerHA SystemMirror: https://ibm.biz/powerhawiki
- PowerVC Service Management Connect: https://ibm.biz/smcpowervc

Twitter

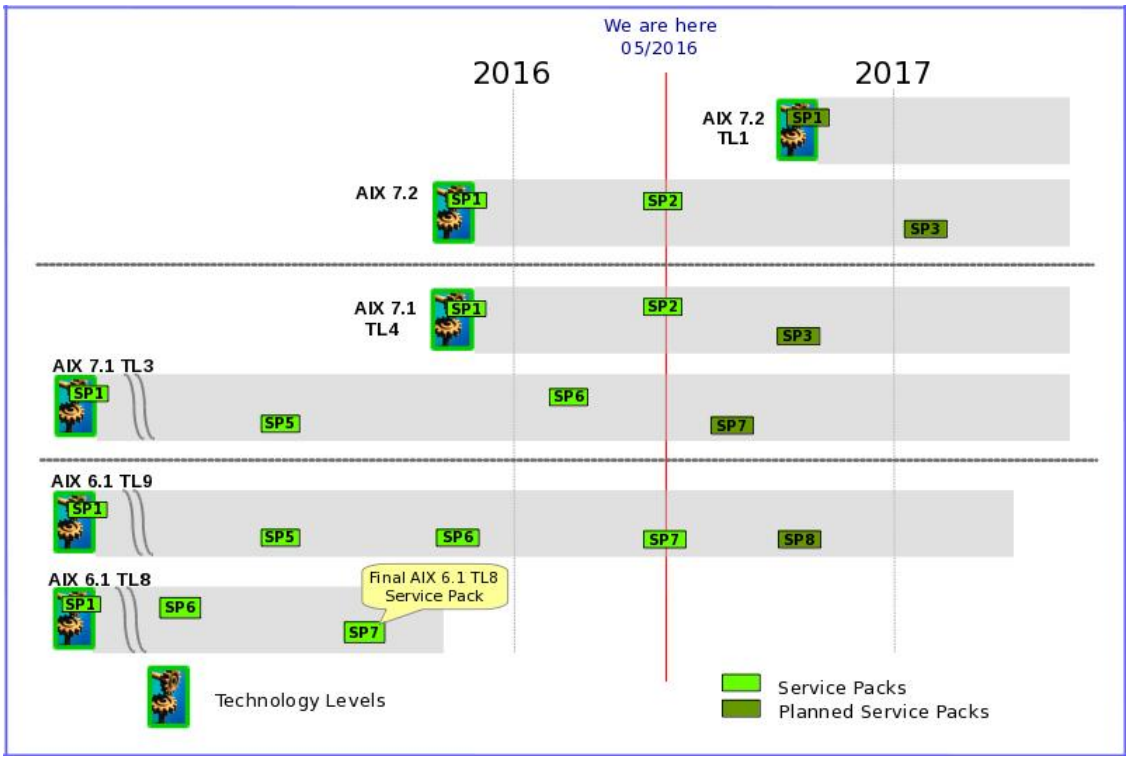
- @IBMAIXeSupp - https://twitter.com/IBMAIXeSupp
  AIX eSupport for important AIX Notifications including Security Advisories, HIPERs, latest Service Packs, and more.
- @mr_nmon - https://twitter.com/mr_nmon
  Nigel Griffiths works at IBM on AIX & Linux, Power Systems in Advanced Technology Europe.

Concepts

AIX Life Cycle

AIX supports multiple Releases and multiple Technology Levels on each Release in parallel to give customers flexibility when selecting what levels to run.

Here is an example of AIX Lifecycle and supported releases, with more details explained below. A current version of this chart can always be found on Fix Central (select Product=AIX, Version=(Release), Function=Fix packs, and scroll to the bottom of the page).



AIX Level Naming

AIX Levels are named based on Release, Technology Level, Service Pack, and Build Sequence Identifier

```
RELE-TL-SP-BBBB
```

The command `'oslevel -s'` will print out the current AIX Level.

```
# oslevel -s
7100-01-07-1316
|      |   |     '---------------------- Build Sequence Identifier
|      |   '-----------------Service Pack 3
|      '---------- Technology Level 1
'-- Release 7.1
```

Note: `` `oslevel -s` `` will show the latest full Service Pack that has been applied.
If individual fileset updates have been applied, consider the –g or –q options along with -s.
See oslevel man page in the Information Center for more details.

Releases

AIX Releases contain new software features as well as the latest fixes for defects and exploitation of new hardware.

New Releases are shipped approximately every 4 years

They are supported for usage and debug for 10 years under standard SWMA, plus 3-5 years of optional, separately priced, extended support.
https://www-01.ibm.com/software/support/lifecycle/

Fixes are available for supported Releases on all Technology Levels that are still active for Service Pack Support (see below).

Technology Levels (TLs)

Technology Levels contain fixes for defects found by customers and internal testing, exploitation of new hardware, and may contain software enhancements.

New Technology Levels generally ship yearly for new Releases. We then transition to shipping new Technology Levels approximately every 2 years as the Release matures.

They are supported with fixes provided through Service Packs and iFixes for 3 years initially. Support increases to 4 years for TLs that have transitioned to the 'every 2 years' release cadence.
http://www-01.ibm.com/support/docview.wss?uid=isg3T1012517

Usage and debug support is still available even after the End of Service Pack Support.

Service Packs (SPs)

Service Packs contain fixes for defects impacting customers, fixes for critical defects found in internal testing, and may contain enablement for new hardware.

In general, changes that are allowed in a Service Pack are minimal defect fixes that do not change default behavior nor add new functionality.

New Service Packs are released approximately twice a year for each TL that is still active for Service Pack Support.

APARs

(Authorized Program Analysis Reports)

An APAR is a record of a problem reported with AIX, and also associated with the fix for that problem. Each APAR applies to a specific Technology Level. If the same problem is reported and/or fixed on other Technology Levels, there will be different APARs for each of them. It is important to understand this when tracking and managing a fix across multiple levels of AIX.

When an APAR has shipped, the Technology Level to which it applies is noted in the Abstract.

```
APAR=iz98260
    request for vgsa update of concurrent vg hangs
    applies to aix 6100-06
```

APARs fixing the same problem on other Technology Levels are noted in the Comments.

```
COMMENTS:
    6100-05 - use AIX APAR IZ98619
    6100-06 - use AIX APAR IZ98260
```

iFixes

(Interim Fixes)

iFixes are temporary relief for defects, which can be used to fix especially critical problems that cannot be avoided until the permanent fix can be installed. These are custom built one-off fixes that patch only the required files. iFixes are tested for functionality and some regression, but generally not exposed to full regression testing or system test.

There can only be one iFix installed at a time for any given file, though there can be multiple iFixes installed for the same fileset. Installing an iFix will lock the entire fileset from being updated except by an update containing the fix for the same APAR(s) resolved by the ifix.

More information about managing iFixes is available in the Technote "Managing Interim Fixes on AIX" (http://www.ibm.com/support/docview.wss?uid=isg3T1012104).

Security iFixes

Security iFixes are a special set of iFixes published when a security vulnerability in AIX is fixed. The published Security Vulnerability Alert will include an initial set of iFixes to provide immediate relief for most systems. We have recently expanded this list to include iFixes for the latest 3 Service Packs of each active Technology Level. It is important to stay current to have immediate access to security iFixes.

These iFixes have had limited functional and regression testing but not the full regression testing that takes place for Service Packs. See the 'Reactive Maintainence' section below for more information on security vulnerabilities.

iFix Naming

iFixes are labeled as follows to help quickly identify some key information:
Label: <APAR>[s|m]<SP><seq>, for example:
IV24230s5a
^^^^^^^ APAR Number (specific to the Technology Level on which the iFix can be applied)
^ (s)ingle or (m)ulti fix (if it's multi, inspect the iFix description or aparref with emgr for the full list of APARs)
^ Service Pack (iFix will apply to this SP at least, possibly others if the code is common across multiple SPs)
^ sequence letter (to ensure each ifix has a unique label)

Sometimes this naming convention cannot be followed and the detailed iFix description should be consulted for more details about the contents. This is viewable with:
`` `emgr -l -v3 -L <iFix Label>` `` for installed iFixes, or
`` `emgr -d -v3 -e <iFix filename>` `` for iFix package files.

Debug Packages

Sometimes debug/test patches are sent out in the same packaging that iFixes use, but not following the standards above. These packages will be labeled beginning with "dbg" to distinguish them and will not usually contain APAR numbers. These should be removed as soon as debug/testing is complete, and replaced by an Interim Fix if appropriate.

Planned Maintenance

Service Pack Updates

Planned Service Pack updates are driven by requiring a software fix and/or new hardware enablement that is shipped in a Service Pack.

Contents of new Service Packs should be reviewed as they are published by IBM by examining the 'Fix details' on Fix Central (http:// www.ibm.com/support/fixcentral/). If the Service Pack contains fixes for problems (documented by APAR numbers) that might be encountered in your particular environment, then a planned update to apply that Service Pack should be considered to avoid encountering the problem. Important Security, HIPER, and PE resolving APARs are highlighted for careful consideration. More information on these 'Critical APARs' below.

New hardware enablement might also exist in a new Service Pack, and would be documented in the hardware announcement. More information about the levels required to support a specific system is located in the System to AIX maps page (http://www.ibm.com/support/docview.wss?uid=ssm1platformaix).

New Service Packs require a reboot.

When updating Service Packs, the release date should be considered. The Fix Level Recommendation Tool (http://www.ibm.com/support/customercare/flrt) should be used to plan the update. IBM will generally mark an AIX Service Pack recommended 90 days after it is released. However Security Vulnerability and HIPER APARs should also be evaluated before updating to a recommended level. FLRT has links to "AIX/VIOS Security Tables" and "AIX HIPER Tables" which provide a very useful view of what HIPER or Security problems each release is exposed to, and where to get fixes.

Technology Level Upgrades

Technology Level upgrades are initiated to receive the new software enhancements and new hardware exploitation they contain; or because your current Technology Level is approaching or past the active period for new fixes.

Contents of new Technology Levels are available on Fix Central just as for Service Packs. New features and benefits of updating to a new TL can be found in the publication "AIX - From Strength to Strength" (http://public.dhe.ibm.com/common/ssi/ecm/en/poo03022usen/POO03022USEN.PDF).

If your current Technology Level is no longer active for new fixes, or is about to become inactive, a Technology Level upgrade should be considered. This will ensure that if any unexpected problems are encountered, a fix for the problem can be applied without any major update being required.

New Technology Levels require a reboot.

When upgrading Technology Levels, the release date and active life should be considered. When a new Technology Level is released, testing continues both internally and externally, and the first Service Pack is usually mandatory. The Fix Level Recommendation Tool (http://www.ibm.com/support/customercare/flrt) should be used to plan the upgrade. IBM will generally mark a Technology Level recommended 90 days after its first Service Pack has been released. However, the same evaluations of critical HIPER/PE/Security fixes should be made, as described above for Service Pack Updates.

Applying the Updates

Technology Levels must be applied as a group, using the 'smitty update_all' or 'install_all_updates' commands. Installing a partial Technology Level will not be recognized from a support standpoint. Technology Level updates should always be committed and cannot be rejected. Because of that, you should always create a backup and plan on restoring that backup if you need to rollback to your previous level, or use tools like alt_disk_install or multibos as a way to get back to your previous level. After the Technology Level has been successfully applied and tested, a backup should be taken for disaster recovery situations.

Service Packs should generally be applied as a whole to simplify inventory and for risk reduction, because the filesets in a Service Pack are regression tested as a group, not as individual updates. Service Packs can be applied but not committed at first to ensure there are no problems after updating.

There are some filesets which should be updated individually, without applying the entire Service Pack or updating to a new Technology Level. These include, but are not limited to: bos.rte.install, bos.alt_disk.install.rte, bos.alt_disk_install.boot_images, RSCT filesets, LDAP filesets, Tivoli agents, and IBM Systems Director agents.

Other Considerations

When moving up to a new Technology Level, you must move to a Service Pack that has the same or later Build Sequence Identifier than your current Service Pack. The Service Pack number itself will not be the same, because the Service Packs will be numbered consecutively as they are released, but the dates will tell you where you need to be on the new Technology Level. The update process will not allow an earlier built Service Pack to be applied to avoid the chance of regression.

When updating in any form, any installed iFixes should be evaluated to know if the permanent fix will be installed in the new update, or if another iFix will need to be requested, to be applied after updating. iFixes will be automatically removed by the update if the Technology Level or Service Pack being applied contains the permanent fix (APAR) that the interim fix was patching. An installp preview will output which iFixes will be automatically removed.

Doing a "Fix search" on Fix Central for an APAR number will usually present a "Sibling information" page in the search results. This page shows, in one place, all the Service Packs which contain fixes for the same problem, and what the specific APAR numbers are for each Technology Level. This can be useful especially when planning an update or upgrade if you have iFixes installed and would like to know which Service Packs (on various Technology Levels) contain the permanent APAR fix.

Release Migrations

When migrating the operating system to a new version or release of AIX, you must be careful to not down-level the operating system by migrating to a previously built level (that may not contain all your current fixes). When applying updates, we use build dates to prevent down-leveling, but a migration ignores build dates because once it's started, it must complete as cleanly as possible. So you must manually verify build dates before migrating, to be sure the target media build date is equal or greater than what is currently running. Compare the build dates of what is currently installed on your system (using `` `oslevel` ``, see 'AIX Level Naming' above) with what is printed on the media to be used for migration.

If using a NIM lpp_source for migration, you must check the build date of the media it was created from. If your lpp_source was created from, for example, 7100-00 base images, and has updates for 7100-01, then you are actually migrating to 7100-00, and then updating to 7100-01. So be sure the base install level you are migrating to is a later build date.

Always run the pre_migration script on the system you are planning to migrate, and the post_migration script after migrating. This will catch some potential failures before migrating, and tell you of any software that did not migrate correct afterwards, which can possibly be corrected. These two scripts are found on physical media in <mount_point>/usr/lpp/bos, or in a NIM SPOT in <spot_location>/lpp/bos.

As always, backup the system before migrating in case of an unrecoverable failure in the migration of the operating system.

Reactive Maintenance

iFixes

When an especially critical problem is encountered that cannot be avoided by some workaround, and the permanent fix cannot be applied via Service Pack update, an iFix can be requested for temporary relief.

iFixes are available by request for active Technology Levels only. If the fix requested is shipped in a later Service Pack on your current Technology Level, you will be told to update to that Service Pack instead of getting an iFix. If you cannot update to the Service Pack at this time, and the fix is very critical, the iFix request can sometimes still be made. Once a request is made it will be evaluated for feasibility. IBM will make every effort to supply an iFix for a particular issue; however, there may be some that cannot be provided due to risk or complexity.

It is recommended to update to the Technology Level or Service Pack containing the permanent fix during the next planned maintenance window.

Critical APARs

IBM highlights three categories of APARs as especially critical for customers to be aware of:

Security APARs
These resolve security vulnerabilities in AIX. They are reported as soon as IBM is aware and a fix is available.

HIPER (High Impact PERvasive) APARs
These resolve defects which have a combination of both high impact and pervasiveness such that IBM thinks all customers exposed to the issues should proactively apply the fix to avoid encountering the problem.

PE (PTF in Error) resolving APARs
These resolve issues where a prior PTF caused a regression in functionality, breaking something that used to work.

Fix Central (http:// www.ibm.com/support/fixcentral/) has information on all these critical APARs for each Service Pack in the 'Fix details' link. This page lists all APAR fixes in the Service Pack, starting with Security APARs, HIPER APARs, and APARs resolving PEs. At the bottom of the page, filesets in this Service Pack that cause regressions are listed as 'Known problems with this package', along with a link to the PE resolving APAR.

My Notifications (http://support.ibm.com/) is the primary way that IBM will notify customers of these critical APARs. Signing up for each AIX release will ensure you are notified of all Security, HIPER, and PEs reported. When a notification is received, it should be evaluated immediately to determine if it applies to your environment. If so, the fix will be available either via iFix or APAR, as documented in the notification.
Past notifications can also be reviewed at any time via Power Server Bulletins (http://www14.software.ibm.com/webapp/set2/subscriptions/onvdq).

FLRT (Fix Level Recommendation Tool - http://www.ibm.com/support/customercare/flrt) can help determine if a system is exposed to one of these critical APARs by inputting the current system level, or examining the "AIX/VIOS Security Tables" and "AIX HIPER Tables".

Resources

Fix Central
http:// www.ibm.com/support/fixcentral/
Central site for AIX update distribution. Here you can find details of Technology Levels and Service Packs that have been released, and you can download them. There are also links to this Best Practices doc and other service related documents.

My Notifications
http://support.ibm.com/ - Sign in, under "Notifications" click "Manage all my subscriptions"
Sign up for Update Notifications for AIX and other products. This is the primary way customers will be notified of any critical AIX fixes including HIPER and Security Vulnerabilities.

Power Server Bulletins
http://www14.software.ibm.com/webapp/set2/subscriptions/onvdq
Archive site for the HIPER/PE/Security Vulnerability notifications that are sent out. This is a good reference to re-vist what the latest critical fixes are, even those not yet available in a Service Pack on Fix Central.

Fix Level Recommendation Tool (FLRT)
http://www.ibm.com/support/customercare/flrt
Tool for recommending upgrades and updates for AIX as well as other products. This is a good place to check when planning what level to roll out in the next planned maintainence window. FLRT also has links to the "AIX HIPER Tables" and "AIX/VIOS Security Tables" which provide a very useful view of what HIPER and Security problems each release is exposed to, and where to get fixes. This includes links to the Bulletin with more information and links to download the fix either as an Interim Fix or Service Pack.

Managing Interim Fixes on AIX
http://www.ibm.com/support/docview.wss?uid=isg3T1012104
Detailed document for how to install and manage Interim Fixes on AIX

IBM System to AIX maps
http://www.ibm.com/support/docview.wss?uid=ssm1platformaix
Information on the AIX levels required to support different hardware

AIX Technology Level Lifecycles
http://www.ibm.com/support/docview.wss?uid=isg3T1012517
Life Cycle of AIX Releases and Technology Levels, including dates for release dates and end of support dates.

Entitled Software Support (Ordering Product Media)
https://www.ibm.com/servers/eserver/ess/ProtectedServlet.wss
Place to order product media.

AIX from Strength to Strength – A summary of AIX upgrade benefits
http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=RG&htmlfid=POO03022USEN
Summary of the benefits of upgrading AIX to various TLs

IBM Enhances AIX Service Strategy in 2011
http://www.ibm.com/systems/power/software/aix/whitepapers/release_strategy.html
Summary of the changes with the last AIX Service Strategy changes.

Product Support Lifecycles
http://www.ibm.com/software/support/systemsp/lifecycle
Life Cycle information for AIX and other products.

AIX Support Center Tools
http://www.ibm.com/support/aixtools
Tools that IBM support will ask you to install and run to help gather information to aid in problem determination.

Power 7 Performance Best Practices
http://www14.software.ibm.com/webapp/set2/sas/f/best/power7_performance_best_practices.pdf
Best Practices checklist and links for optimizing performance of AIX on Power.

Power 8 Performance Best Practices
http://www14.software.ibm.com/webapp/set2/sas/f/best/power8_performance_best_practices.pdf
Best Practices checklist and links for optimizing performance of AIX on Power

VIOS Best Practices
http://www-304.ibm.com/webapp/set2/sas/f/vios/svcstrategy.html
Best Practices for VIOS. This information is also available in VIOS Release Notes.

Service and Support Best Practices for Power Systems
http://www.ibm.com/support/customercare/sas/f/best/home.html
Best Practices for other Power Systems products.

IBM Corporation
Marketing Communications
Systems Group
Route 100
Somers, New York 10589

Produced in the United States of America

June 2009

The IBM home page on the Internet can be found at http://www.ibm.com.

The IBM System p home page on the Internet can be found at http://www.ibm.com/systems/p.

The IBM AIX home page on the Internet can be found at: http:///www.ibm.com/servers/aix.

PSW03011-USEN-00