close window

Web Exclusive   Print 🖶

The Complete Guide to System Maintenance

August 2016 | by Jaqui Lynch

Taking care of your servers is crucial. It's important to stay as current as possible to ensure you have the best security and performance. Additionally, the further back you are the more likely that the response will be to upgrade when you call in with a problem. The key items to upgrade include LPARs, VIO servers, HMCs and server and I/O firmware.

First, planning is critical. Many find it challenging to get a maintenance window at all so the plan is often to cram as much into it as possible. But that's almost a guarantee that something will get broken and, worst of all, it'll be difficult to figure out the cause. It's important to separate times for network, storage and system updates. For example, if you're using LPM (Live partition mobility) to move LPARs to prepare for maintenance and someone starts performing maintenance on the network, then you'll have a problem. It happens all the time. The same applies to active directory server maintenance, if that's how you authenticate for your LPARs, and to things like citrix servers, if that's how you access them from outside. I've lost count of the times I've had an upgrade go south because someone rebooted the citrix server I was using. So planning should include the timing of the upgrades and those of anything you're depending on for your upgrade to work.

Before any update, you must download the files and read all of the readme files. This ensures that you install any patches in the right order. Typically, you upgrade the HMC,then the firmware and then the operating system, however the readme will make clear what the prerequisites are.

IBM also requires that you have a valid hardware maintenance agreement (HWMA) to download and install firmware and a valid software maintenance agreement (SWMA) to download and upgrade software. You can check entitlements on the IBM entitled software site under "my entitled software". You'll need the server model and serial number, i.e. 8205-e6d serial 06abcd1. For some products you'll need all seven characters.

Determine the Levels

To figure out what levels you should install, determine current installed levels by doing the following as root:

```
oslevel -s
```

The above will show you the oslevel as something like:

```
7100-01-04-1216
```

The above is AIX 7.1 tl01 sp4

For a VIO you run the above after entering oem_setup_env but you also run the following as padmin

```
ioslevel
```

```
2.2.3.52
```

For a VIO, oslevel will normally show something like: 6100-09-05-1524 with ioslevel showing something like 2.2.3.52 You can check the VIOS to NIM mapping table to find out how these should match

```
lsmcode -A
```

The above will provide you with the firmware level for the server and also for any I/O that is attached to it i.e. fibre cards, network cards, disks, etc. These adapters will need updating regularly as IBM brings out mandatory updates from time to time. This applies especially to the 10Gb network and 8/16Gb fibre cards. For example the 5735 2 port 8Gb fibre card has a mandatory update as of January 2016 – the level needs to be at 203305.

Before Starting

Now that you have your starting points, you can use FLRT (fix level recommendation tool) or FLRT Lite to figure out what updates need to be applied, download the operating system ones and then look at the readme documents. In the readme you will either find a change history with a list of all the changes incorporated in these fixes or a link to the firmware history which lists the changes in every firmware release from your installed one to the one you're going to. Once you have the list of potential levels then you must determine what combination to install. Typically, most people want to wait two to three months after a level is released before installing it unless it's mandatory.

Step 1: always run errpt if this is an operating system or to check error logs prior to starting any update. No point in trying to update a system that has problems. Step 2: take a backup–for AIX or the VIO this would be a mksysb to an external resource, for the HMC this would involve running a save upgrade data to the hard drive and then backing up the management console data. This second backup can be done to the USB key if you have one or to a remote FTP server. Use of the DVD is no longer supported. Once the backup is complete you are ready to go.

Prior to starting any firmware updates you may want to use LPM to move any affected LPARs to a new server, especially if you are going to have to power cycle the server for a deferred or disruptive update.

HMC (Hardware Management Console) Updates

I try to keep my HMC at the absolute latest level that will support my servers and that's supported on the HMC. Right now the latest version of the HMC software is v8.8.5.0 (MH01616) with iFix MH01649 applied. This level requires that the HMC must be at least a CR8 deskside or a CR5 rack mount. Earlier HMCs are not supported on v8. Additionally, POWER5 servers are not supported on v8. There are also prerequisites prior to upgrading to v8.8.5 that are further explained in the readme. For older HMCs or for POWER5 server support the most current version is v77.7.9.0M3 (MH01546) with iFix MH01635.

There are three kinds of updates for the HMC and they are handled a little differently. Two of them (updates and fixes) are handled as general updates where the HMC is updated via the GUI. You need to know if the update is an update or a fix -- this is detailed in the readme and determines the location you point to in order to obtain the update. When I select Update HMC on the HMC I use the FTP option, point to ftp.software.ibm.com and login as anonymous. If this is an update I point to /software/server/hmc/updates. If it's a fix, the directory is usually /software/server/hmc/fixes. The HMC prompts you with a list of patches with names like MH01567.iso and you pick the correct one.

The other option is a more major upgrade. Typically I do these by using SSH to the HMC. If I was going to upgrade to v8.8.3.0 I would open two SSH sessions to the HMC. On one I would run the following script to monitor the upgrade:

```
while true ; do
date
```

```
ls -la /hmcdump
sleep 60
done
```

On the other I would be downloading the software. Once it's downloaded you won't see the files in /hmcdump which is why the monitor script above is helpful in knowing when it has ended. On the actual download session, you would do the following:

```
chhmcfs -o f -d 0
```

The above clears out all temp files

```
getupgfiles -h public.dhe.ibm.com -u anonymous --passwd anonymous -d /software/server/hmc/network/v8830
```

The above downloads the actual upgrade files. Once that's done you can exit the first session and type in the following two commands to tell the HMC to perform the upgrade:

```
chhmc -c altdiskboot -s enable --mode upgrade
```

The above tells it to set up to upgrade on boot

```
hmcshutdown -r -t now
```

It takes about 20 to 30 minutes to actually perform the upgrade. Once it's done you must install any required upgrades or fixes. Each upgrade or fix will take at least 20 minutes as a reboot of the HMC is required for each. If you have redundant HMCs you should do them both the same day as problems can occur when they are out of sync.

Server and I/O Firmware

If you have an HMC, then firmware is very easy to install. There are three types of installs: concurrent, deferred and disruptive. Concurrent updates can be installed with no downtime. Deferred updates can be installed but will not be activated until the system is powered off and on. Disruptive updates require an immediate power off and on. The readme will tell you what kind of updates these are and the HMC process will also flag the updates before you click on the final ok. When using the HMC to install firmware, you can also choose to have it install any I/O firmware at that time. Without an HMC you need to download the updates and follow the manual process.

At install time you have the option to install both server and I/O firmware; I recommend doing both if you can. Some updates (boot disks for example) may require that the LPARs using them are shut down. If you have LPM you can move any active LPARs to another server during this time and that will allow you to power off the server releasing those resources. If the updates are deferred or disruptive you will need to perform a power recycle of the server anyway.

Operating Systems (AIX and VIO Servers)

Upgrading the operating system is something that should be planned and tested ahead of time. There are several kinds of upgrades – this is regardless of whether we are talking about AIX or VIO servers. The upgrades can be as small as an eFix (which is an individual temporary fix applied with emgr) and as large as a whole version upgrade with service packs and technology levels fitting in the middle.

With the possible exception of the eFix, most of these will require a reboot at the end. Backups should be taken regularly but definitely before any changes are made.

The first step is to identify and download the fixes or maintenance to be applied. If this is a version upgrade, you must go to the entitled software page, login using your IBM id and then you can download the necessary image. On the entitled software page you can find your AIX and VIO server base images. You can download as .iso images and then either burn them to a DVD or use FBO (file backed optical) on your VIO or mount them using loopmount. If you use loopmount on the NIM (network install manager) server then you can use that image to create an lppsource and spot to use for NIM controlled upgrades.

If you want to put on a service pack or technology level, go to fix central to download the necessary code. Again you can usually download as an iso image or you can download the update files into a directory. If you use NIM you should then create a new lppsource and spot that you then update using the downloaded software. Once that is done you can use it to update the LPARs. Alternatively, you can use the downloaded software and install to update the LPAR directly without NIM.

Typically, after the backups are done, the upgrade is a two-step process if you're not using NIM. For both the VIO and AIX you will need to uninstall any iFixes or eFixes that were installed by emgr. Run emgr -l to get a list and then remove them using emgr (as root). For AIX you then install the updated bos.rte.install by itself. Then you can use smitty update_all or install to apply the updates from the directory or CD. For a VIO server you have to accept all prior patches and then run the update. You don't need to install bos.rte.install separately.

```
On my vio I download the patches into a directory on the VIO. Then as padmin:
updateios -commit
```

The above commits all previous patches on the VIO

```
updateios -accept -install -dev /directorywithpatches
```

The above installs the patches from the directory into which they were downloaded.

Post Install

Once the updates are applied you should check a few things. I use the following:

```
oslevel -s
```

Make sure you see the expected OS level. If you see something like 7100-00-00-0000 then you most likely have some missing filesets that need to be corrected.

```
instfix -I | grep ML
```

This will tell you if you have missing filesets and which level they apply to

```
lppchk -v
lppchk -vm3
```

The above will tell you about issues with filesets

```
oslevel -sq
```

Lists known service packs – you use the highest level of these in the command below

```
oslevel -s -l 6100-09-02-1412
```

The above would list any filesets that were not at least at this level. You now know the filesets that need correcting.

```
errpt
```

Check for Errors

At this point you're done or you have missing fixes to resolve. For a VIO you would use the same commands as the above (using oem_setup_env to become root) and you would also issue ioslevel as padmin to check the VIO shows as the correct level.

If you do have missing or incorrect filesets you can remove them or correct them. For AIX this is done using smitty or installp but for the VIO server you should be using updateios. As an example the following will remove bos.suma if it is backlevel:

```
updateios -remove bos.suma
```

If you have missing filesets for the VIO server put them in their own directory with nothing else and then run updateios -commit and then updateios -accept pointing to that directory. Don't ever update the VIO by pointing to a full AIX LPP directory.

At this point you should run flrtvc to identify security patches that must be updated. You can download them and use emgr to install them. For Java and SSL you use installp on the new version. Once all patches are on it is time to reboot. Prior to rebooting I always run bosboot to reinitialize the boot sector on each boot disk and the bootlist command to ensure the bootlist is correctly set. Then it's time to reboot and test. Remember to back everything up after the updates are completed.

Summary

System maintenance is a time-consuming process that takes planning. However, so many problems are fixed in firmware, HMC and operating system updates that there really needs to be a regular schedule for applying these. It's important to have a maintenance plan that incorporates these three kinds of updates in a stand-alone manner. They should not be combined with storage, switch, network, oracle, application, etc updates. The key to a successful update is to have a well planned out update strategy. I pre-document every step including the commands before I do any upgrade – that way I am not searching for commands or trying to remember the next step. I go through the readmes and incorporate their notes into the plan and I include steps in the plan for what to do when or if things go wrong. Maintenance is a

necessary process and it can be done in a very painless manner if proper planning is done. With the advent of fix central, flrt, flrtvc and other updates on the IBM tool site this process has become much simpler to perform.

References

Fix Central

www-945.ibm.com/support/fixcentral/

Entitled Software

https://www-304.ibm.com/servers/eserver/ess/ProtectedServlet.wss/

FLRT (fix level recommendation tool)

http://www14.software.ibm.com/webapp/set2/flrt/home

FLRT Lite

http://www14.software.ibm.com/webapp/set2/flrt/liteHome

FLRT VC (FLRT Vulnerability checker)

http://www14.software.ibm.com/webapp/set2/flrt/vc

VIOS to NIM mapping table

http://www14.software.ibm.com/webapp/set2/sas/f/flrt/viostable.html