

Automate infrastructure updates in NIM environment

AIX patch management with Chef

February 7, 2017

Updating AIX at a large scale infrastructure is easier than ever with the use of Chef. One may either upgrade to latest or specific SP or TL and/or apply recommended security and HIPER fixes to all its NIM clients.

Introduction

This article details how to use [Chef](#) for **patch management automation** on IBM® AIX® systems. The hardware configuration, the installation process and the nominal use case are detailed.

Our development supports a NIM (Network Installation Management) environment in **PUSH mode**. Pull operations from NIM client is already available at the [Chef Supermarket](#). Patch management cookbook is available as a GitHub repository at <https://github.com/aix-chef>.

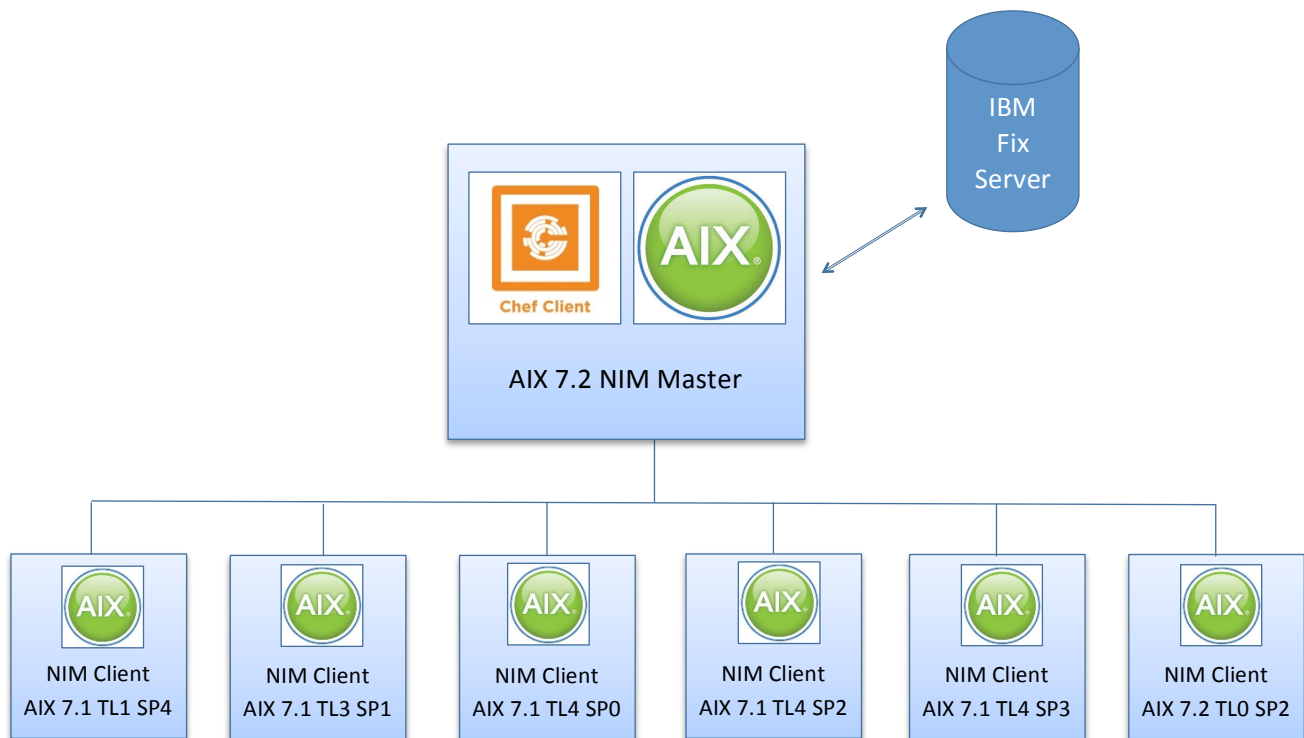
The NIM server/master takes the role of the chef client or node. It must be able to connect to IBM Fix Server in order to download SPs or TLs through **SUMA** (Service Update Management Assistant). It can install those updates on its clients through **NIM** either by NFS or HTTP. The method is described in [Managing AIX Updates Best Practices](#). It is also possible to patch NIM clients with recommended security and High Impact PERvasive fixes through **FLRTVC** ([Fix Level Recommendation Tool Vulnerability Checker](#)).

For ease of use, Chef will be used in **local (or standalone) mode** on the NIM master. But, it may also be configured with a Linux Chef server.

Configuration

The NIM master has access to the internet in order to download fixes and updates through HTTP and FTP protocol. It has several clients which are at different AIX releases and levels. It needs to be at a level at least as high as the highest level client. As a prerequisite to this demo, it needs to have *wget* and *git* tools installed in order to easily install Chef and AIX patch management cookbook and recipes example. But one may also download and transfer the repository on the NIM client.

The diagram below describes the hardware configuration for the test use case.



Installation

- 1) Download and install latest version of chef client for AIX from <https://downloads.chef.io/chef-client/> depending on your NIM server level. Or you can use wget.

```
$ wget --no-check-certificate https://packages.chef.io/files/stable/chef/12.18.31/aix/7.1/chef-12.18.31-1.powerpc.bff
--2017-01-31 07:42:28-- https://packages.chef.io/files/stable/chef/12.18.31/aix/7.1/chef-...
Resolving packages.chef.io... 151.101.68.65
Connecting to packages.chef.io[151.101.68.65]:443... connected.
WARNING: cannot verify packages.chef.io's certificate, issued by 'CN=GlobalSign Organization Validation CA - SHA256 - G2,O=GlobalSign nv-sa,C=BE':
  Unable to locally verify the issuer's authority.
HTTP request sent, awaiting response... 200 OK
Length: 77785088 (74M) [application/octet-stream]
Saving to: 'chef-12.18.31-1.powerpc.bff'

chef-12.18.31-1.powerpc.bff
100%[=====] 74.18M 1.11MB/s in 68s

2017-01-31 07:43:38 (1.09 MB/s) - 'chef-12.18.31-1.powerpc.bff' saved [77785088/77785088]
```



Page 3 of 15



+-----+ Summaries: +-----+				
Installation Summary -----				
Name	Level	Part	Event	Result

chef	12.18.31.1	USR	APPLY	SUCCESS
chef	12.18.31.1	ROOT	APPLY	SUCCESS

- ```
$ /opt/chef/embedded/bin/gem install aix-wpar
Successfully installed aix-wpar-0.1.0
Parsing documentation for aix-wpar-0.1.0
Done installing documentation for aix-wpar after 1 seconds
1 gem installed
```

- ```
$ mkdir -p /chef/cookbooks
$ cd /chef/cookbooks
$ git clone https://github.com/aix-chef/aix.git aix
Cloning into 'aix'...
remote: Counting objects: 2163, done.
remote: Compressing objects: 100% (130/130), done.
remote: Total 2163 (delta 87), reused 0 (delta 0), pack-reused 2033
Receiving objects: 100% (2163/2163), 474.52 KiB | 289.00 KiB/s, done.
```

```
Resolving deltas: 100% (1431/1431), done.  
Checking connectivity... done.  
$ git clone https://github.com/aix-chef/nim.git ohai_nim  
Cloning into 'ohai_nim'...  
remote: Counting objects: 78, done.  
remote: Total 78 (delta 0), reused 0 (delta 0), pack-reused 78  
Unpacking objects: 100% (78/78), done.  
Checking connectivity... done.
```

- 4) Create the configuration file `client.rb` by providing the path to the cookbooks and the path to our Ohai plugin. Again, that file may be placed anywhere in the filesystem as long as you provide the right path to it during step 6.

```
$ cat > /chef/client.rb  
cookbook_path '/chef/cookbooks'  
ohai.plugin_path << '/chef/cookbooks/ohai_nim/ohai/plugins'  
Ctrl+D
```

- 5) The [README.md](#) file describes how to create your own recipes. For example, to download AIX 7.1 TL3 SP4 update needed to upgrade all NIM standalone clients to that version, use `suma` Chef Resource.

```
$ cat > aix/recipes/my_own_recipe.rb  
aix_suma 'Suma recipe example' do  
  oslevel '7100-03-04'  
  targets '*'  
end  
Ctrl+D
```

- 6) Run `chef-client` from command line by providing the configuration file, the cookbook and the recipe.

```
$ chef-client --local-mode -c /chef/client.rb --runlist 'recipe[aix::my_own_recipe]'  
Starting Chef Client, version 12.18.31  
resolving cookbooks for run list: ["aix::my_own_recipe"]  
Synchronizing Cookbooks:  
- aix (1.0.0)  
Installing Cookbook Gems:
```

```

Compiling Cookbooks...
Converging 1 resources
Recipe: aix::my_own_recipe
  * aix_suma[Suma recipe example] action download
[2017-02-01T04:32:52-06:00] WARN: The oldest machine is at level 7100-01.
[2017-02-01T04:32:52-06:00] WARN: Preview: 1773 downloaded (7.1 GB), 0 failed, 0 skipped fixes

Start downloading 1773 fixes (~ 7.1 GB) to '/usr/sys/inst.images/7100-03-04-1441-lpp_source' directory.
SUCCEEDED: 1773/1773   FAILED: 0/0   SKIPPED: 0/0. (Total time: 22 mins 29 secs).
Finish downloading 1773 fixes (~ 7.1 GB).

- download 1773 fixes to '/usr/sys/inst.images/7100-03-04-1441-lpp_source'
- define nim lpp source '7100-03-04-1441-lpp_source'

Running handlers:
Running handlers complete
Chef Client finished, 1/1 resources updated in 25 minutes 48 seconds

```

7) Observe idempotency by running the same recipe once again.

```

$ chef-client --local-mode -c /chef/client.rb --runlist 'recipe[aix::my_own_recipe]'
Starting Chef Client, version 12.18.31
resolving cookbooks for run list: ["aix::my_own_recipe"]
Synchronizing Cookbooks:
  - aix (1.0.0)
Installing Cookbook Gems:
Compiling Cookbooks...
Converging 1 resources
Recipe: aix::my_own_recipe
  * aix_suma[Suma recipe example] action download
[2017-02-01T03:38:30-06:00] WARN: The oldest machine is at level 7100-01.
[2017-02-01T03:38:30-06:00] WARN: Preview: 0 downloaded (0.0 GB), 0 failed, 1773 skipped fixes
(up to date)

Running handlers:
Running handlers complete
Chef Client finished, 0/1 resources updated in 02 minutes 31 seconds

```

Watch this video to learn more.



To view this video, [AIX Patch Automation with Chef – Installation](#), please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

Update by SUMA example

In the 'examples' directory, you can find an **interactive recipe** called 'update_by_suma.rb' which will ask you which client(s) you want to upgrade at which SP or TL level and where you want the downloaded packages to be saved. You just have to copy that file to the 'recipes' directory and run it as is.

```
update_by_suma.rb
1 # recipe example update using suma and nim
2 # This recipe is interactive and allows upgrade of AIX 7.1 and 7.2 machines
3
4 Chef::Recipe.send(:include, AIX::PatchMgmt)
5
6 puts '#####'
7 puts 'Available machines and their corresponding oslevel are:'
8 puts clients(node)
9 puts 'Choose one or more (comma or space separated) to update?'
10 client = STDIN.readline.chomp
11
12 puts '#####'
13 puts 'Available SP/TL levels are:'
14 puts levels(node)
15 puts 'Choose one to download and install?'
16 level = STDIN.readline.chomp
17
18 puts '#####'
19 puts 'Where to download? (default to /export/extra/lpp_source)'
20 directory = STDIN.readline.chomp
21 directory = '/export/extra/lpp_source' if directory.empty?
22
23 ohai 'reload_nim' do
24   action :nothing
25   plugin 'nim'
26 end
27
28 aix_suma "Downloading '#{level}' installation images to '#{directory}'" do
29   oslevel level
30   location directory
31   targets client
32   action :download
33   notifies :reload, 'ohai[reload_nim]', :immediately
34 end
35
36 aix_nim "Updating machine(s) '#{client}'" do
37   lpp_source "#{level}-lpp_source"
38   targets client
39   async false
40   action [:update, :reboot]
41   only_if "lsnim -t lpp_source #{level}-lpp_source"
42   notifies :reload, 'ohai[reload_nim]', :immediately
43   ignore_failure true
44 end
45
46 aix_nim 'Check update status' do
47   action :check
48 end
49
```




```
$ cp aix/examples/update_by_suma.rb aix/recipes
$ chef-client --local-mode -c /chef/client.rb --runlist 'recipe[aix::update_by_suma]'
Starting Chef Client, version 12.18.31
resolving cookbooks for run list: ["aix::update_by_suma"]
Synchronizing Cookbooks:
  - aix (1.0.0)
Installing Cookbook Gems:
Compiling Cookbooks...
#####
Available machines and their corresponding oslevel are:
+-----+-----+-----+
| machine | oslevel | Cstate |
+-----+-----+-----+
| quimby01 | 7100-01-04-1216 | ready for a NIM operation |
| quimby02 | 7100-03-01-1341 | ready for a NIM operation |
| quimby03 | 7100-04-00-0000 | ready for a NIM operation |
| quimby04 | 7100-04-02-1614 | ready for a NIM operation |
| quimby05 | 7100-04-03-1642 | ready for a NIM operation |
| quimby06 | 7200-00-02-1614 | ready for a NIM operation |
| quimby07 | 7200-01-00-0000 | ready for a NIM operation |
| quimby08 | 7100-04-02-1614 | ready for a NIM operation |
| quimby09 | 7100-04-01-1543 | ready for a NIM operation |
| quimby10 | 7100-04-01-1543 | ready for a NIM operation |
| quimby11 | 7100-04-01-1543 | ready for a NIM operation |
| quimby12 | 7200-01-00-0000 | ready for a NIM operation |
| master | 7200-01-00-0000 |
+-----+-----+-----+
Choose one or more (comma or space separated) to update?
quimby01 quimby02 quimby03 quimby04 quimby05 quimby06
#####
Available SP/TL levels are:
+-----+-----+-----+-----+-----+-----+
| 7.1 TL0 | 7.1 TL1 | 7.1 TL2 | 7.1 TL3 | 7.1 TL4 | 7.2 TL0 | 7.2 TL1 |
+-----+-----+-----+-----+-----+-----+
| 7100-00-00-0000 | 7100-01-00-0000 | 7100-02-00-0000 | 7100-03-00-0000 | 7100-04-00-0000 | 7200-00-00-0000 | 7200-01-00-0000* |
| 7100-00-01-1037 | 7100-01-01-1141 | 7100-02-01-1245 | 7100-03-01-1341 | 7100-04-01-1543* | 7200-00-01-1543 | 7200-01-01-1642 |
| 7100-00-02-1041 | 7100-01-02-1150 | 7100-02-02-1316 | 7100-03-02-1412* | 7100-04-02-1614 | 7200-00-02-1614* | |
| 7100-00-03-1115 | 7100-01-03-1207 | 7100-02-03-1334 | 7100-03-03-1415 | 7100-04-03-1642 | 7200-00-03-1642 | |
| 7100-00-04-1140 | 7100-01-04-1216 | 7100-02-04-1341 | 7100-03-04-1441 | | | |
| 7100-00-05-1207 | 7100-01-05-1228 | 7100-02-05-1415 | 7100-03-05-1524 | | | |
| 7100-00-06-1216 | 7100-01-06-1241 | 7100-02-06-1441 | 7100-03-06-1543* | | | |
| 7100-00-07-1228 | 7100-01-07-1316 | 7100-02-07-1524 | 7100-03-07-1614 | | | |
| 7100-00-08-1241 | 7100-01-08-1334 | | | | | |
| 7100-00-09-1316 | 7100-01-09-1341 | | | | | |
| 7100-00-10-1334 | 7100-01-10-1415 | | | | | |
+-----+-----+-----+-----+-----+-----+
Choose one to download and install?
```

```
7100-04-02-1614
#####
Where to download? (default to /usr/sys/inst.images)

Converging 4 resources
Recipe: aix::update_by_suma
  * ohai[reload_nim] action nothing (skipped due to action :nothing)
  * aix_suma[Downloading '7100-04-02-1614' installation images to '/usr/sys/inst.images'] action download[2017-02-03T02:59:14-06:00] WARN: The oldest machine is at level 7100-01.
[2017-02-03T02:59:44-06:00] WARN: Preview: 1806 downloaded (8.18 GB), 0 failed, 0 skipped fixes

Start downloading 1806 fixes (~ 8.18 GB) to '/usr/sys/inst.images/7100-04-02-1614-lpp_source' directory.
SUCCEEDED: 2088/1806   FAILED: 0/0   SKIPPED: 0/0. (Total time: 25 mins 34 secs).
Finish downloading 2088 fixes (~ 9.34 GB).

- download 1806 fixes to '/usr/sys/inst.images/7100-04-02-1614-lpp_source'
- define nim lpp source '7100-04-02-1614-lpp_source'
* ohai[reload_nim] action reload

- re-run ohai and merge results into node attributes
* aix_nim[Updating machine(s) 'quimby01 quimby02 quimby03 quimby04 quimby05 quimby06'] action update
Start updating machine(s) 'quimby01' to 7100-04-02-1614-lpp_source.
Finished processing all filesets. (Total time: 1 hrs 54 mins 48 secs).
Finish updating quimby01 synchronously.

- nim: perform synchronous software customization for client 'quimby01' with resource '7100-04-02-1614-lpp_source'
Start updating machine(s) 'quimby02' to 7100-04-02-1614-lpp_source.
Finished processing all filesets. (Total time: 1 hrs 36 mins 21 secs).
Finish updating quimby02 synchronously.

- nim: perform synchronous software customization for client 'quimby02' with resource '7100-04-02-1614-lpp_source'
Start updating machine(s) 'quimby03' to 7100-04-02-1614-lpp_source.
Finished processing all filesets. (Total time: 1 mins 3 secs).
Finish updating quimby03 synchronously.

- nim: perform synchronous software customization for client 'quimby03' with resource '7100-04-02-1614-lpp_source'[2017-02-03T07:04:50-06:00] WARN: Machine quimby04 is already at same or higher level than 7100-04-02-1614
[2017-02-03T07:04:50-06:00] WARN: Machine quimby05 is already at same or higher level than 7100-04-02-1614
[2017-02-03T07:04:50-06:00] WARN: Machine quimby06 has different release than 7100-04-02-1614

Running handlers:
Running handlers complete
Chef Client finished, 3/4 resources updated in 04 hours 12 minutes 57 seconds
```

Watch this video to learn more.



To view this video, [AIX Patch Automation with Chef – Suma example](#), please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.

Patch by FLRTVC example

In the 'examples' directory, you can find an **recipe** called 'patch_by_flrtvc.rb' which will ask you which client(s) you want to patch with recommended emergency fixes. You just have to copy that file to the 'recipes' directory and run it as is.

```
$ emgr -P
There is no efix data on this system.
$ cp aix/examples/patch_by_flrtvc.rb aix/recipes
$ cat aix/recipes/patch_by_flrtvc.rb
aix_flrtvc 'patch local aix machine' do
  path '/flrtvc'
  action [:install, :patch]
end
$ chef-client --local-mode -c /chef/client.rb --runlist 'recipe[aix::patch_by_flrtvc]'
Starting Chef Client, version 12.18.31
resolving cookbooks for run list: ["aix::patch_by_flrtvc"]
Synchronizing Cookbooks:
  - aix (1.0.0)
Installing Cookbook Gems:
Compiling Cookbooks...
Converging 1 resources
Recipe: aix::patch_by_flrtvc
  * aix_flrtvc[patch aix machine(s)] action install
    * remote_file[/chef/local-mode-cache/cache/FLRTVC-latest.zip] action create
      - create new file /chef/local-mode-cache/cache/FLRTVC-latest.zip
      - update content in file /chef/local-mode-cache/cache/FLRTVC-latest.zip from none to eda11e
      (new content is binary, diff output suppressed)
    * execute[unzip -o /chef/local-mode-cache/cache/FLRTVC-latest.zip -d /usr/bin] action run
      - execute unzip -o /chef/local-mode-cache/cache/FLRTVC-latest.zip -d /usr/bin
    * file[/chef/local-mode-cache/cache/FLRTVC-latest.zip] action delete
      - delete file /chef/local-mode-cache/cache/FLRTVC-latest.zip
    * file[/usr/bin/flrtvc.ksh] action create
      - change mode from '0644' to '0755'

  * aix_flrtvc[patch aix machine(s)] action patch[2017-02-09T08:24:44-06:00] WARN: [master] Flrtvc report has been
saved to '/flrtvc/master.flrtvc'
[2017-02-14T07:38:00-06:00] WARN: [master] Found 11 different download links over 18 vulnerabilities and 9
filesets

Checking 1/11 fixes. (https://aix.software.ibm.com/aix/efixes/security/openssh_fix9.tar:6202_ifix.160830.epkg.Z)... NO MATCH
Checking 2/11 fixes. (https://aix.software.ibm.com/aix/efixes/security/openssh_fix8.tar:IV84698m9a.160513.epkg.Z)... MATCH PREREQ
Checking 3/11 fixes. (https://aix.software.ibm.com/aix/efixes/security/openssh_fix7.tar:IV80743m9a.160127.epkg.Z)... MATCH PREREQ
Checking 4/11 fixes. (https://aix.software.ibm.com/aix/efixes/security/openssh_fix6.tar:6201_ifix.151009.epkg.Z)... MATCH PREREQ
Checking 5/11 fixes. (http://aix.software.ibm.com/aix/ifixes/iv91511/IV91511s1a.161214.72TL01SP00-01.epkg.Z)... MATCH PREREQ
Checking 6/11 fixes. (http://aix.software.ibm.com/aix/ifixes/iv91020/IV91020s0a.161125.72TL01SP00.epkg.Z)... MATCH PREREQ
```

```
Checking 7/11 fixes. (http://aix.software.ibm.com/aix/ifixes/iv90451/IV90485s0a.161104.72TL1SP0-1.epkg.Z)... MATCH PREREQ
Checking 8/11 fixes. (ftp://aix.software.ibm.com/aix/ifixes/iv91432/IV91432s1a.161209.72TL01SP01.epkg.Z)... NO MATCH
Checking 9/11 fixes. (ftp://aix.software.ibm.com/aix/efixes/security/bind_fix14.tar:IV91257m0a.161212.epkg.Z)... MATCH PREREQ
Checking 10/11 fixes. (ftp://aix.software.ibm.com/aix/efixes/security/bellmail_fix2.tar:IV92242m1a.170112.epkg.Z)... MATCH PREREQ
Checking 11/11 fixes. (ftp://aix.software.ibm.com/aix/efixes/security/bellmail_fix.tar:IV91011s1a.161125.epkg.Z)... MATCH PREREQ
```

```
[2017-02-14T07:40:53-06:00] WARN: [master] Found 9 fixes to install
```

```
- create directory '/chef/local-mode-cache/cache/2017_02_14_07_37_48__0600/lpp_sources/master-lpp_source/emgr/ppc'
- [master] sec fix 'IV84698m9a.160513.epkg.Z' meets level pre-requisite for fileset 'openssh.base.client'
- [master] sec fix 'IV80743m9a.160127.epkg.Z' meets level pre-requisite for fileset 'openssh.base.client'
- [master] sec fix '6201_ifix.151009.epkg.Z' meets level pre-requisite for fileset 'openssh.base.client'
- [master] hiper fix 'IV91511s1a.161214.72TL01SP00-01.epkg.Z' meets level pre-requisite for fileset
'devices.vdevice.ibm.vfc-client.rte'
- [master] hiper fix 'IV91020s0a.161125.72TL01SP00.epkg.Z' meets level pre-requisite for fileset
'devices.vdevice.ibm.l-lan.rte'
- [master] hiper fix 'IV90485s0a.161104.72TL1SP0-1.epkg.Z' meets level pre-requisite for fileset
'rsct.basic.rte'
- [master] sec fix 'IV91257m0a.161212.epkg.Z' meets level pre-requisite for fileset 'bos.net.tcp.client_core'
- [master] sec fix 'IV92242m1a.170112.epkg.Z' meets level pre-requisite for fileset 'bos.net.tcp.client_core'
- [master] sec fix 'IV91011s1a.161125.epkg.Z' meets level pre-requisite for fileset 'bos.net.tcp.client_core'
```

Start patching nim master or local machine.

Processing Efix Package 9 of 9.

EPKG NUMBER	LABEL	OPERATION	RESULT
=====	=====	=====	=====
1	IV84698m9a	INSTALL	SUCCESS
2	IV80743m9a	INSTALL	FAILURE
3	6201_ifix	INSTALL	FAILURE
4	IV91511s1a	INSTALL	SUCCESS
5	IV91020s0a	INSTALL	SUCCESS
6	IV90485s0a	INSTALL	SUCCESS
7	IV91257m0a	INSTALL	SUCCESS
8	IV92242m1a	INSTALL	SUCCESS
9	IV91011s1a	INSTALL	FAILURE

Finish patching nim master or local machine.

```
[2017-02-14T07:42:15-06:00] WARN: master failed installing some efixes. See /var/adm/ras/emgr.log for details
```

```
- geninstall: install all efixes from '/chef/local-mode-cache/cache/2017_02_14_07_37_48__0600/lpp_sources/master-lpp_source'
```

Running handlers:

Running handlers complete

Chef Client finished, 1/3 resources updated in 07 minutes 49 seconds

```
$ chef-client --local-mode -c /chef/client.rb --runlist 'recipe[aix::patch_by_flrtvc]'
```

Starting Chef Client, version 12.18.31



```
resolving cookbooks for run list: ["aix::patch_by_flrtvc"]
Synchronizing Cookbooks:
  - aix (1.0.0)
Installing Cookbook Gems:
Compiling Cookbooks...
Converging 1 resources
Recipe: aix::patch_by_flrtvc
  * aix_flrtvc[patch aix machine(s)] action install
  * file[/usr/bin/flrtvc.ksh] action create (up to date)
    (up to date)
  * aix_flrtvc[patch aix machine(s)] action patch[2017-02-14T07:44:08-06:00] WARN: [master] Flrtvc report has been
saved to '/flrtvc/master.flrtvc'
[2017-02-14T07:44:08-06:00] WARN: [master] Found 2 different download links over 6 vulnerabilities and 5 filesets

Checking 1/2 fixes. (https://aix.software.ibm.com/aix/efixes/security/openssh_fix9.tar:6202_ifix.160830.epkg.Z)... NO MATCH
Checking 2/2 fixes. (ftp://aix.software.ibm.com/aix/ifixes/iv91432/IV91432s1a.161209.72TL01SP01.epkg.Z)... NO MATCH

[2017-02-14T07:44:29-06:00] WARN: [master] Found 0 fixes to install
[2017-02-14T07:44:29-06:00] WARN: master have 0 vulnerabilities but none meet pre-requisites
  (up to date)

Running handlers:
Running handlers complete
Chef Client finished, 0/3 resources updated in 01 minutes 57 seconds
$ emgr -P

PACKAGE                                INSTALLER  LABEL
=====
openssh.base.client                    installp   IV84698m9a
openssh.base.server                    installp   IV84698m9a
devices.vdevice.IBM.vfc-client.rte     installp   IV91511s1a
devices.vdevice.IBM.l-lan.rte          installp   IV91020s0a
rsct.basic.rte                         installp   IV90485s0a
bos.net.tcp.bind_utils                 installp   IV91257m0a
bos.net.tcp.bind                       installp   IV91257m0a
bos.net.tcp.client_core                installp   IV92242m1a
```

Watch this video to learn more.



To view this video, [AIX Patch Automation with Chef – Flrtvc example](#), please access the online version of the article. If this article is in the developerWorks archives, the video is no longer accessible.