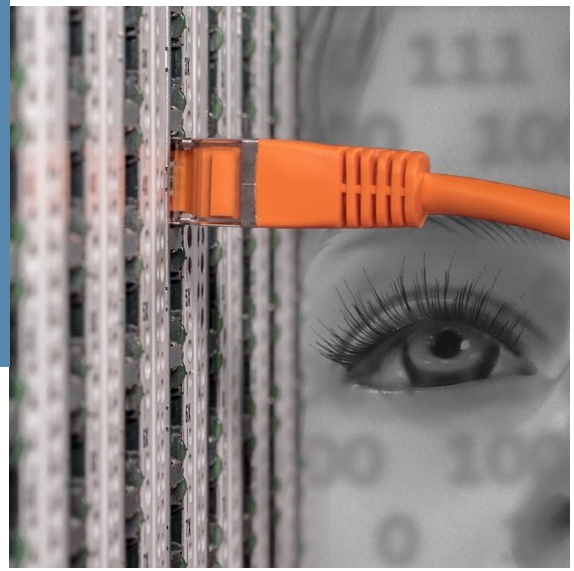
IBM AIX Patch Management. Automated?

Common Europe Congress 2026, Lyon

Andrey Klyachkin

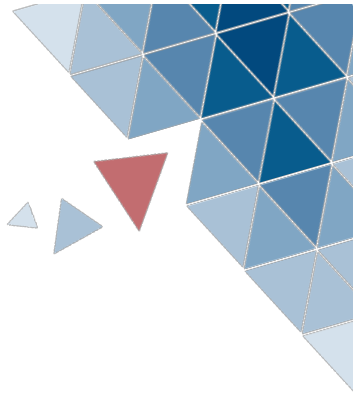
andrey.klyachkin@enfence.com

eNFence



— Obélix, more or less, every week at patch day

Today: how to stop being crazy.

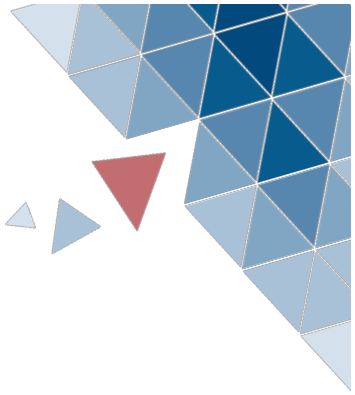


Patch management is concerned with the identification, acquisition, distribution, and installation of patches to systems. Proper patch management can be a net productivity boost for the organization. Patches can be used to defend against and eliminate potential vulnerabilities of a system, so that no threats may exploit them. Problems that can arise during patch management, including buggy patches that either fail to fix their problem or introduce new issues. **Patch management tools** can help orchestrate all of the procedures involved in patch management.

A **patch** is data that is intended to be used to modify an existing software resource such as a program or a file, often to fix bugs and security vulnerabilities.[1][2] A patch may be created to improve functionality, usability, or performance. A patch is typically provided by a vendor for updating the software that they provide.

ENFENCE

Before you start automating



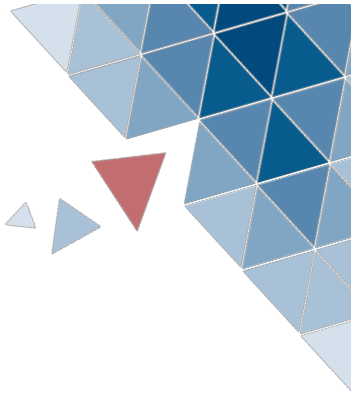
- Understand how it works
- Standardize
- Define your strategy and make a process out of it

Before you start automating

- How oft should you patch?
- How fast should you install patches?
- Where do you get patches from?
- Do you have downtime?
- How big is the downtime?
- How many environments do you have?
- Do you have sandbox systems?
- How do you check if patches are installed?

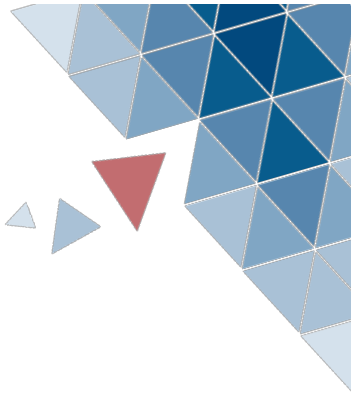
ENFENCE

How many packaging formats are there in IBM AIX?



ENFENCE

How many packaging formats are there in IBM AIX?



My answer:

BFF

RPM

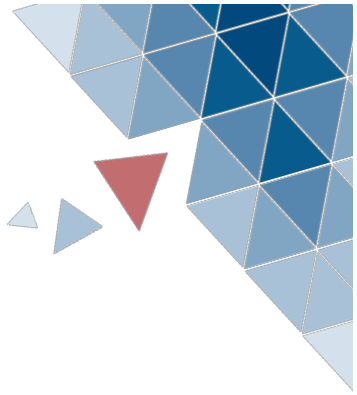
ISMP

epkg.Z

tar.gz, zip, ...

ENFENCE

What parts has IBM AIX?



ENFENCE

What parts has IBM AIX?

My answer:

BOS (Base Operating System)

OpenSSL

OpenSSH

GSKit

IBM Directory Server

Network Authentication Service

Db2

Bash

Python

Perl

Java

XL C/C++ Runtime

XL Fortran Runtime

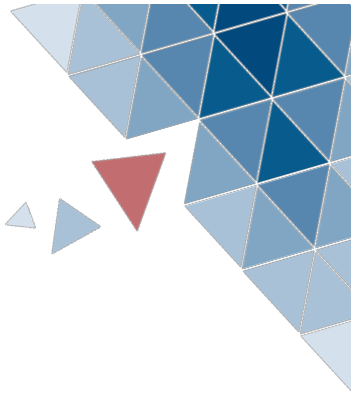
RSCT

Adapter Microcode

AIX Toolbox (RPM Pakete)

ENFENCE

Which channels do you know to get AIX updates and patches?



ENFENCE

Which channels do you know to get AIX updates and patches?

My answer:

IBM ESS

IBM FixCentral

IBM Webpack for AIX

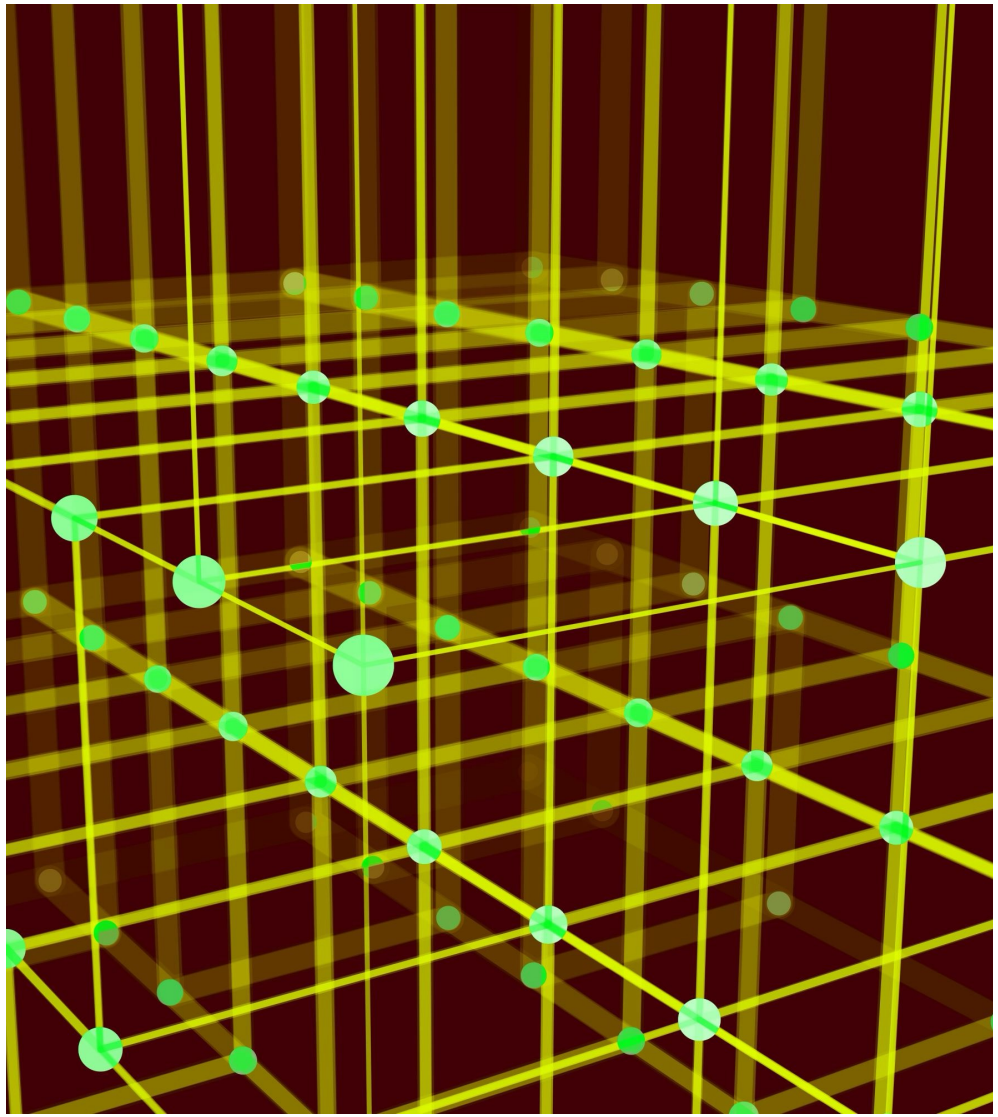
AIX Toolbox for Opensource Apps

IBM ~~FTP~~ Site

IBM HTTPS Site

ENFENCE

Bonus Question: Do you have NIM?



Theory

and a little bit practice

The most important question: What should I patch?

New TLs and SPs?

Security Fixes? (efixes)

RPM Updates?

Updates for additional components, like OpenSSH, Java, Python, ...

ENFENCE

Entitled Systems Support

https://www.ibm.com/servers/eserver/ess/landing/landing-page

- Login manually, choose software, download to local workstation and then upload to AIX

API? CLI?

🧐 What is this? Never heard...

- Choose HTTP Downloads and copy the links to the server
- Download with curl or wget

ENFENCE

Fix Central

https://www.ibm.com/support/fixcentral

Login manually, choose software, download to local workstation, then upload to AIX NIM

No published API, but there should be...

CLI: suma

ENFENCE

Webpack for IBM AIX

https://www.ibm.com/resources/mrs/assets?source=aixbp

Login manually, choose software, download to local workstation, then upload to AIX NIM

API? CLI?

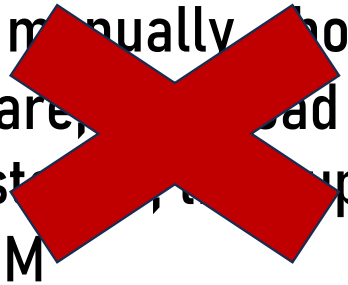
🧐 What is this? Never heard...

ENFENCE

AIX Toolbox for Opensource Applications

https://www.ibm.com/support/pages/aix-toolbox-open-source-software-downloads-alpha

Login manually, choose software, download to local workstation, then upload to AIX NIM



Use DNF, Luke!

Hint:
https://blog.power-devops.com/p/update-aix-with-ansible-part-3a
https://blog.power-devops.com/p/update-aix-with-ansible-part-3b
https://blog.power-devops.com/p/update-aix-with-ansible-part-3c
https://blog.power-devops.com/p/update-aix-with-ansible-part-3d

ENFENCE

IBM HTTPS Site with Security Fixes

https://aix.software.ibm.com/aix/efixes/security/

Choose [illegible]s, d[illegible]load them to local w[illegible]ion, then upload [illegible]X f[illegible]

https://e[illegible]upport.ibm.com/customercare/flrt/[illegible]-security

Sort acc[illegible]g [illegible]he date and choose the suitable fixes

ENFENCE

IBM HTTPS Site with Security Fixes

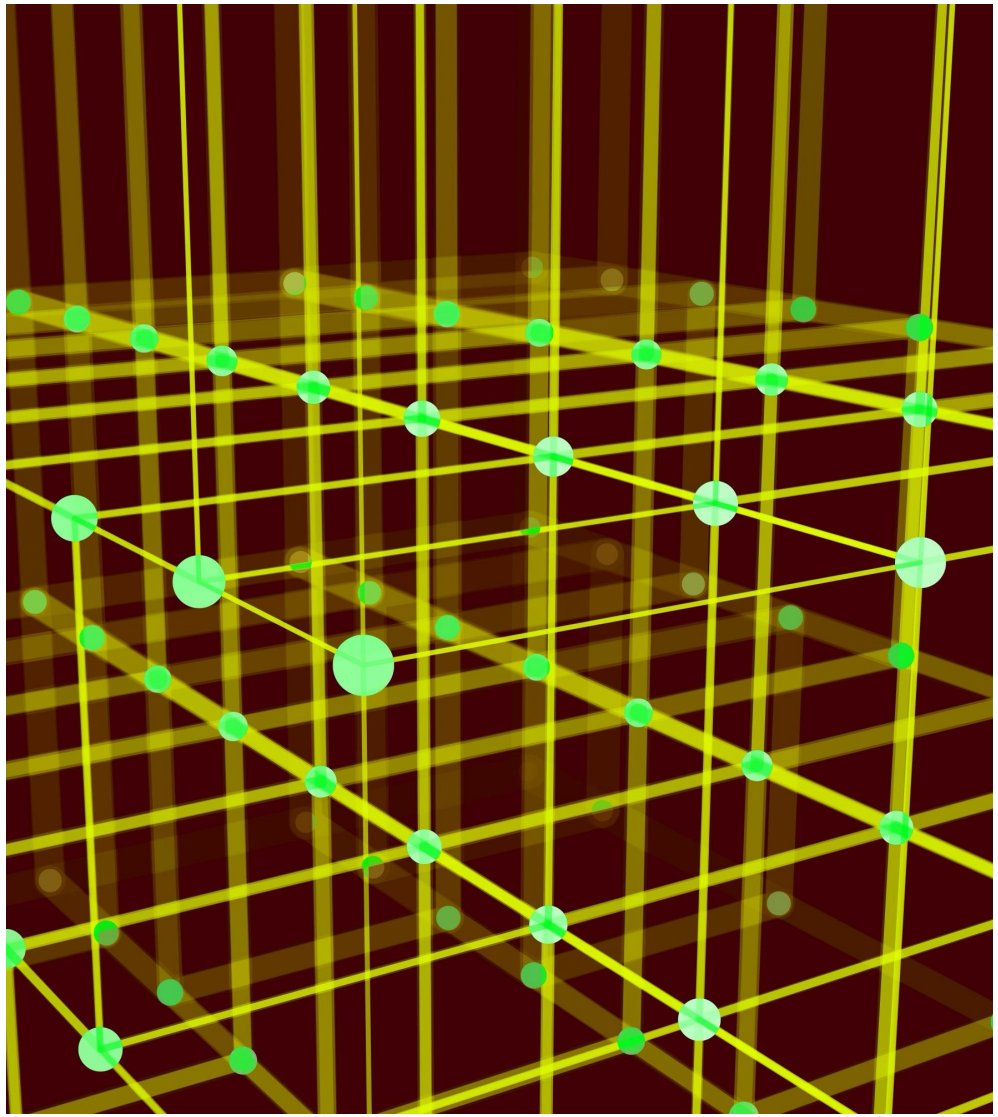
https://github.com/Kristijan/aix_security_advisories

Python script to show the latest advisories

```
#/opt/freeware/bin/python3 aix_security_advisories.py -d 30
                                                    AIX/VIOS Security Advisories
```

Issued	Updated	Abstract	URL	Reboot	CVE	CVSS
15/05/2024	N/A	AIX is vulnerable to arbitrary command execution due to invscout (CVE-2024-27260)	https://aix.software.ibm.com/aix/ef…	no	CVE-2024-27260	8.4
03/06/2024	N/A	AIX is vulnerable to information disclosure due to openCryptoki (CVE-2024-0914)	https://aix.software.ibm.com/aix/ef…	no	CVE-2024-0914	5.9
04/06/2024	05/06/2024	AIX is vulnerable to denial of service due to ISC BIND	https://aix.software.ibm.com/aix/ef…	no	CVE-2023-4408 CVE-2023-50387 CVE-2023-50868 CVE-2023-5517 CVE-2023-5679 CVE-2023-6516	7.5 7.5 7.5 7.5 7.5 7.5

ENFENCE



Practice

and a lot of theory

emgr_check_ifixes in Ansible

```yaml
---
- name: Show available fixes
  hosts: all
  gather_facts: true
  become: true

  tasks:
    - name: Ensure wget is installed (AIX 7.2)
      ansible.builtin.dnf:
        name: wget
        use_backend: dnf4
      vars:
        ansible_python_interpreter: /opt/freeware/libexec/python3.12_32
      when: ansible_facts.distribution_version == "7.2"

    - name: Ensure wget is installed (AIX 7.3)
      ansible.builtin.dnf:
        name: wget
        use_backend: dnf4
      when: ansible_facts.distribution_version != "7.2"

    - name: Get FLRTVC information
      ibm.power_aix.flrtvc:
        apar: sec
        check_only: true
      environment:
        PATH: /usr/bin:/opt/freeware/bin
      register: flrtvc

    - name: Output
      ansible.builtin.debug:
        var: flrtvc.meta['0.report']
```


ENFENCE

emgr_install_ifixes in Ansible

```yaml
---
- name: Install available fixes
  hosts: all
  gather_facts: true
  become: true

  tasks:
    - name: Ensure wget is installed (AIX 7.2)
      ansible.builtin.dnf:
        name: wget
        use_backend: dnf4
      vars:
        ansible_python_interpreter: /opt/freeware/libexec/python3.12_32
      when: ansible_facts.distribution_version == "7.2"

    - name: Ensure wget is installed (AIX 7.3)
      ansible.builtin.dnf:
        name: wget
        use_backend: dnf4
      when: ansible_facts.distribution_version != "7.2"

    - name: Install security fixes
      ibm.power_aix.flrtvc:
        apar: sec
        force: true
      environment:
        PATH: /usr/bin:/opt/freeware/bin
      register: flrtvc

    - name: Show installed fixes
      ansible.builtin.debug:
        var: flrtvc.meta['5.install']

    - name: Reboot server
      ibm.power_aix.reboot:
        reboot_timeout: 600
      when: "'REBOOT REQUIRED' in ( flrtvc.meta['5.install'] | join )"
```


ENFENCE

Can I do it with NIM? check_ifixes_nim

```yaml
---
- name: Show available fixes
  hosts: all
  gather_facts: true
  become: true

  tasks:
    - name: Ensure wget is installed (AIX 7.2)
      ansible.builtin.dnf:
        name: wget
        use_backend: dnf4
      vars:
        ansible_python_interpreter: /opt/freeware/libexec/python3.12_32
      when: ansible_facts.distribution_version == "7.2"

    - name: Ensure wget is installed (AIX 7.3)
      ansible.builtin.dnf:
        name: wget
        use_backend: dnf4
      when: ansible_facts.distribution_version != "7.2"

    - name: Get FLRTVC information
      ibm.power_aix.nim_flrtvc:
        targets: ALL
        apar: sec
        check_only: true
      environment:
        PATH: /usr/bin:/usr/sbin:/opt/freeware/bin
      register: flrtvc

    - name: Output
      ansible.builtin.debug:
        var: item.value['0.report']
      loop: "{{ flrtvc.meta | dict2items }}"
      loop_control:
        label: "{{ item.key }}"
      when: item.value['0.report'] is defined
```


ENFENCE

Can I do it with NIM? install_ifixes_nim

```yaml
---
- name: Install available fixes
  hosts: all
  gather_facts: true
  become: true

  tasks:
    - name: Ensure wget is installed (AIX 7.2)
      ansible.builtin.dnf:
        name: wget
        use_backend: dnf4
      vars:
        ansible_python_interpreter: /opt/freeware/libexec/python3.12_32
      when: ansible_facts.distribution_version == "7.2"

    - name: Ensure wget is installed (AIX 7.3)
      ansible.builtin.dnf:
        name: wget
        use_backend: dnf4
      when: ansible_facts.distribution_version != "7.2"

    - name: Install security fixes
      ibm.power_aix.nim_flrtvc:
        targets: ALL
        apar: sec
        force: true
      environment:
        PATH: /usr/bin:/usr/sbin:/opt/freeware/bin
      register: flrtvc

    - name: Show installed fixes
      ansible.builtin.debug:
        var: item.value['5.install']
      loop: "{{ flrtvc.meta | dict2items }}"
      loop_control:
        label: "{{ item.key }}"
```


ENFENCE

Am I secure? — what is installed

```
"EPKG NUMBER       LABEL              OPERATION          RESULT          ",
"===========       ==============     =================  ==============  ",
"1                 IJ58140m2a         INSTALL            SUCCESS         ",
"2                 14524ma            INSTALL            SUCCESS         ",
"3                 IJ55897m1a         INSTALL            SUCCESS         ",
"4                 3272897ma          INSTALL            SUCCESS         ",
"",
"Return Status = SUCCESS"
# ls -l /var/adm/ansible/work/*tar
-rw-r--r--    1 root     system      1413120 Jun 10 2025  /var/adm/ansible/work/curl_fix7.tar
-rw-r--r--    1 root     system      1423360 Dec 10 23:02 /var/adm/ansible/work/curl_fix8.tar
-rw-r--r--    1 root     system      1413120 Apr 15 21:02 /var/adm/ansible/work/curl_fix9.tar
-rw-r--r--    1 root     system     25610240 Mar 13 19:01 /var/adm/ansible/work/libxml2_fix10.tar
-rw-r--r--    1 root     system     20490240 May 28 20:02 /var/adm/ansible/work/libxml2_fix11.tar
-rw-r--r--    1 root     system     41943040 Jul 17 2025  /var/adm/ansible/work/libxml2_fix9.tar
-rw-r--r--    1 root     system      8376320 Dec 02 2025  /var/adm/ansible/work/nim_fix2.tar
-rw-r--r--    1 root     system     25159680 Mar 17 2025  /var/adm/ansible/work/openssh_fix18.tar
-rw-r--r--    1 root     system     25159680 Jun 10 2025  /var/adm/ansible/work/openssh_fix19.tar
-rw-r--r--    1 root     system     13690880 Jan 06 21:02 /var/adm/ansible/work/openssh_fix20.tar
-rw-r--r--    1 root     system     13670400 May 28 20:01 /var/adm/ansible/work/openssh_fix21.tar
-rw-r--r--    1 root     system     34304000 Dec 10 23:02 /var/adm/ansible/work/openssl_fix45.tar
-rw-r--r--    1 root     system     30341120 Mar 09 20:02 /var/adm/ansible/work/openssl_fix46.tar
-rw-r--r--    1 root     system     30361600 May 04 21:01 /var/adm/ansible/work/openssl_fix47.tar
-rw-r--r--    1 root     system    191477760 Jun 26 2025  /var/adm/ansible/work/perl_fix10.tar
-rw-r--r--    1 root     system    291276800 Sep 16 2025  /var/adm/ansible/work/perl_fix11.tar
-rw-r--r--    1 root     system    191508480 Feb 05 22:02 /var/adm/ansible/work/perl_fix12.tar
-rw-r--r--    1 root     system    191508480 Mar 17 21:02 /var/adm/ansible/work/perl_fix13.tar
-rw-r--r--    1 root     system    259563520 May 20 2025  /var/adm/ansible/work/python_fix15.tar
-rw-r--r--    1 root     system    258344960 Aug 20 2025  /var/adm/ansible/work/python_fix16.tar
-rw-r--r--    1 root     system    258324480 Nov 19 2025  /var/adm/ansible/work/python_fix17.tar
-rw-r--r--    1 root     system    164956160 Mar 17 21:02 /var/adm/ansible/work/python_fix18.tar
-rw-r--r--    1 root     system    164904960 Apr 15 21:01 /var/adm/ansible/work/python_fix19.tar
```


ENFENCE

Am I secure? — what FLRTVC says

```
"EPKG NUMBER       LABEL           OPERATION          RESULT       ",
"============     ==============  =================  ==============",
"1                 IJ58140m2a      INSTALL            SUCCESS      ",
"2                 14524ma         INSTALL            SUCCESS      ",
"3                 IJ55897m1a      INSTALL            SUCCESS      ",
"4                 3272897ma       INSTALL            SUCCESS      ",
"",
"Return Status = SUCCESS"
```


```
    "flrtvc.meta['0.report']": [
        "Fileset|Current Version|Type|EFix Installed|Abstract|Unsafe Versions|APARs|Bulletin URL|Download URL|CVSS Base Score|Reboot Required|Last Update|Fixed In",
        "openssh.base.client|9.7.3013.1000|sec||NOT FIXED - AIX is vulnerable to potential code execution (CVE-2025-61984 CVE-2025-61985) due to OpenSSH|9.2.112.0-9.7.3013.1000|35414ma / 61985sa / CVE-2025-61984 / CVE-2025-61985|https://aix.software.ibm.com/aix/efixes/security/openssh_advisory20.asc|https://aix.software.ibm.com/aix/efixes/security/openssh_fix20.tar|CVE-2025-61984:3.6 CVE-2025-61985:3.6|NO|01/06/2026|See Bulletin",
        "openssh.base.client|9.7.3013.1000|sec||NOT FIXED - Multiple vulnerabilities in OpenSSH affect AIX|9.2.112.0-9.7.3013.1000|35414ma / CVE-2026-35385 / CVE-2026-35386 / CVE-2026-35387 / CVE-2026-35388 / CVE-2026-35414|https://aix.software.ibm.com/aix/efixes/security/openssh_advisory21.asc|https://aix.software.ibm.com/aix/efixes/security/openssh_fix21.tar|CVE-2026-35385:8.1 CVE-2026-35386:8.1 CVE-2026-35387:6.5 CVE-2026-35388:2.5 CVE-2026-35414:8.1|NO|05/28/2026|See Bulletin",
        "openssh.base.server|9.7.3013.1000|sec||NOT FIXED - AIX is vulnerable to potential code execution (CVE-2025-61984 CVE-2025-61985) due to OpenSSH|9.2.112.0-9.7.3013.1000|35414ma / 61985sa / CVE-2025-61984 / CVE-2025-61985|https://aix.software.ibm.com/aix/efixes/security/openssh_advisory20.asc|https://aix.software.ibm.com/aix/efixes/security/openssh_fix20.tar|CVE-2025-61984:3.6 CVE-2025-61985:3.6|NO|01/06/2026|See Bulletin",
        "openssh.base.server|9.7.3013.1000|sec||NOT FIXED - Multiple vulnerabilities in OpenSSH affect AIX|9.2.112.0-9.7.3013.1000|35414ma / CVE-2026-35385 / CVE-2026-35386 / CVE-2026-35387 / CVE-2026-35388 / CVE-2026-35414|https://aix.software.ibm.com/aix/efixes/security/openssh_advisory21.asc|https://aix.software.ibm.com/aix/efixes/security/openssh_fix21.tar|CVE-2026-35385:8.1 CVE-2026-35386:8.1 CVE-2026-35387:6.5 CVE-2026-35388:2.5 CVE-2026-35414:8.1|NO|05/28/2026|See Bulletin",
        "openssl.base|3.0.15.1001|sec||NOT FIXED - AIX is vulnerable to an out-of-bounds read (CVE-2025-9230 CVE-2025-9232) due to OpenSSL|3.0.0.0-3.0.16.1000|301610sa / 301610mc / 301610mb / CVE-2025-9230 / CVE-2025-9232|https://aix.software.ibm.com/aix/efixes/security/openssl_advisory45.asc|https://aix.software.ibm.com/aix/efixes/security/openssl_fix45.tar|CVE-2025-9230:7.5 CVE-2025-9232:5.9|NO|12/10/2025|See Bulletin",
        "openssl.base|3.0.15.1001|sec||NOT FIXED - Multiple vulnerabilities impact AIX due to OpenSSL|3.0.0.0-3.0.16.1000|301610mc / 301610mb / CVE-2025-15467 / CVE-2025-68160 / CVE-2025-69418 / CVE-2025-69419 / CVE-2025-69420 / CVE-2025-69421 / CVE-2026-22795 / CVE-2026-22796|https://aix.software.ibm.com/aix/efixes/security/openssl_advisory46.asc|https://aix.software.ibm.com/aix/efixes/security/openssl_fix46.tar|CVE-2025-15467:9.8 CVE-2025-68160:4.7 CVE-2025-69418:4 CVE-2025-69419:7.4 CVE-2025-69420:7.5 CVE-2025-69421:7.5 CVE-2026-22795:5.5 CVE-2026-22796:5.3|NO|03/09/2026|See Bulletin",
        "openssl.base|3.0.15.1001|sec||NOT FIXED - Multiple vulnerabilities impact AIX due to OpenSSL|3.0.0.0-3.0.16.1000|301610mc / CVE-2026-28387 / CVE-2026-28388 / CVE-2026-28389 / CVE-2026-28390 / CVE-2026-31789 / CVE-2026-31790|https://aix.software.ibm.com/aix/efixes/security/openssl_advisory47.asc|https://aix.software.ibm.com/aix/efixes/security/openssl_fix47.tar|CVE-2026-28387:8.1 CVE-2026-28388:7.5 CVE-2026-28389:7.5 CVE-2026-28390:7.5 CVE-2026-31789:9.8 CVE-2026-31790:7.5|NO|05/04/2026|See Bulletin",
        "perl.rte|5.38.2.1|sec||NOT FIXED - AIX is vulnerable to denial of service and possible code execution due to Perl (CVE-2024-8176 CVE-2024-56406)|5.38.0.0-5.38.2.2|CVE-2024-56406 / CVE-2024-8176|https://aix.software.ibm.com/aix/efixes/security/perl_advisory10.asc|https://aix.software.ibm.com/aix/efixes/security/perl_fix10.tar|CVE-2024-56406:8.6 CVE-2024-8176:7.5|NO|06/26/2025|See Bulletin",
        "perl.rte|5.38.2.1|sec||NOT FIXED - AIX/VIOS is vulnerable to a race condition in directory handling due to Perl (CVE-2025-40909)|5.38.0.0-5.38.2.2|CVE-2025-40909|https://aix.software.ibm.com/aix/efixes/security/perl_advisory11.asc|https://aix.software.ibm.com/aix/efixes/security/perl_fix11.tar|CVE-2025-40909:5.9|NO|09/16/2025|See Bulletin",
        "perl.rte|5.38.2.1|sec||NOT FIXED - AIX is vulnerable to denial of service and possible code execution due to Perl (WS-2025-0004)|5.38.0.0-5.38.2.3|WS-2025-0004|https://aix.software.ibm.com/aix/efixes/security/perl_advisory12.asc|https://aix.software.ibm.com/aix/efixes/security/perl_fix12.tar|WS-2025-0004:7.5|NO|02/05/2026|See Bulletin",
        "perl.rte|5.38.2.1|sec||NOT FIXED - AIX Perl is vulnerable to a null pointer dereference (CVE-2026-24515) and an integer overflow (CVE-2026-25210)|5.38.0.0-5.38.2.4|CVE-2026-24515 / CVE-2026-25210|https://aix.software.ibm.com/aix/efixes/security/perl_advisory13.asc|https://aix.software.ibm.com/aix/efixes/security/perl_fix13.tar|CVE-2026-24515:2.5 CVE-2026-25210:6.9|NO|03/17/2026|See Bulletin",
        "python3.11.base|3.11.10.0|sec||NOT FIXED - AIX is affected by a denial of service (CVE-2024-8176) due to Python|3.11.0.0-3.11.10.0|CVE-2024-8176|https://aix.software.ibm.com/aix/efixes/security/python_advisory15.asc|https://aix.software.ibm.com/aix/efixes/security/python_fix15.tar|CVE-2024-8176:7.5|NO|05/20/2025|See Bulletin",
        "python3.11.base|3.11.10.0|sec||NOT FIXED - AIX/VIOS is affected by arbitrary code execution (CVE-2025-47273 CVE-2025-4330 CVE-2024-12718 CVE-2025-4138 CVE-2025-4517) due to Python|3.11.0.0-3.11.10.1|CVE-2024-12718 / CVE-2025-4138 / CVE-2025-4330 / CVE-2025-4517 / CVE-2025-47273|https://aix.software.ibm.com/aix/efixes/security/python_advisory16
```


ENFENCE

Am I secure? — when installs fail

```
        "",
        "EPKG NUMBER       LABEL              OPERATION          RESULT          ",
        "===========       ==============     =================  ==============  ",
        "1                 IJ50424s7a         INSTALL            FAILURE         ",
        "2                 IJ50428s1a         INSTALL            SUCCESS         ",
        "3                 IJ50432s3a         INSTALL            FAILURE         ",
        "4                 IJ50433s4a         INSTALL            FAILURE         ",
        "5                 IJ50508s1a         INSTALL            FAILURE         ",
        "",
        "Return Status: FAILURE"
    ]
}

PLAY RECAP *********************************************************************************************
nim                        : ok=4    changed=1    unreachable=0    failed=0    skipped=1    rescu
ed=0    ignored=0
```


ENFENCE

Other options? ibm.power_aix.emgr

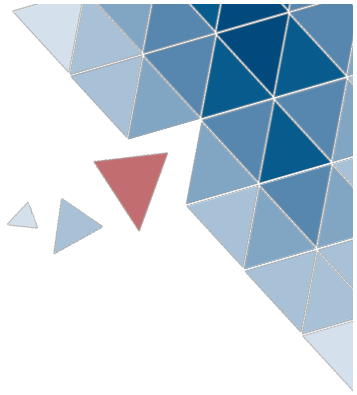
```yaml
---
- name: Install epkg
  hosts: all
  gather_facts: false
  become: true

  tasks:
    - name: Install security fix
      ibm.power_aix.emgr:
        action: install
        ifix_package: /tmp/301610mc.260424.epkg.Z
        from_epkg: true
        extend_fs: true
      register: emgr

    - name: Show result
      ansible.builtin.debug:
        var: emgr
```


ENFENCE

Can I do it better?



Repository with fixes?

Information about OS-versions?

Analyze security advisories?

Check signatures?

Automatically download fixes?

ENFENCE

Repository with all fixes for my systems? Part 1.

```yaml
---
- name: Create AIX fixes repository
  hosts: nim
  gather_facts: false

  tasks:
    - name: Check prereqs
      ansible.builtin.include_tasks: prereqs.yml

    - name: Create filesystem
      ansible.builtin.include_tasks: fixes_fs.yml

    - name: Analyze our clients and download fixes
      ibm.power_aix.nim_flrtvc:
        targets: ALL
        apar: sec
        download_only: true
        extend_fs: true
        path: /nim/fixes
      register: flrtvc

    - name: Build fixes list
      ansible.builtin.include_tasks: get_fix_info.yml
      loop: "{{ flrtvc.meta | dict2items }}"
      loop_control:
        label: "{{ report.key }}"
        loop_var: report
      when: report.value['0.report'] is defined
```


ENFENCE

Repository with all fixes for my systems? Part 2.

```
- name: Check that fixes are downloaded
  ansible.builtin.stat:
    path: "/nim/fixes/work/{{ item }}"
  register: fix_exist
  loop: "{{ fixes }}"

- name: Stop if some fix is not found
  ansible.builtin.fail:
    msg: "{{ item.item }} was not found"
  when: not item.stat.exists
  loop: "{{ fix_exist.results }}"

- name: Unpack fixes
  ansible.builtin.command:
    cmd: "tar xf /nim/fixes/work/{{ item }}"
    chdir: /nim/fixes
  loop: "{{ fixes }}"

- name: Find directories
  ansible.builtin.find:
    paths: /nim/fixes
    file_type: directory
    recurse: false
  register: fix_dirs
```


ENFENCE

Repository with all fixes for my systems? Part 3.

You can find IBM public key in /etc/security/certificates/AIX_PSIRT_pubkey.txt since AIX 7.2 TL5 SP3.
Thanks to Sascha Korzen (OEDIV) for the tip.

```
    - name: Set correct permissions on directories
      ansible.builtin.file:
        path: "{{ item.path }}"
        mode: "0755"
        owner: root
        group: system
      loop: "{{ fix_dirs.files }}"
      loop_control:
        label: "{{ item.path }}"

    - name: Find advisories
      ansible.builtin.find:
        paths: /nim/fixes
        file_type: file
        recurse: true
        depth: 2
        patterns: Advisory.asc
      register: advisories

    - name: Check signature on advisories
      ansible.builtin.command:
        cmd: "openssl dgst -sha256 -verify /etc/security/certificates/AIX_PSIRT_pubkey.txt -signatur
e {{ item.path }}.sig {{ item.path }}"
      changed_when: false
      loop: "{{ advisories.files }}"
      loop_control:
        label: "{{ item.path }}"
```


ENFENCE

Repository with all fixes for my systems? Part 4.

```
    - name: Find fixes
      ansible.builtin.find:
        paths: /nim/fixes
        file_type: file
        recurse: true
        depth: 2
        patterns: '*.epkg.Z'
      register: epkg

    - name: Check signature on fixes
      ansible.builtin.command:
        cmd: "openssl dgst -sha256 -verify /etc/security/certificates/AIX_PSIRT_pubkey.txt -signatur
e {{ item.path }}.sig {{ item.path }}"
      changed_when: false
      loop: "{{ epkg.files }}"
      loop_control:
        label: "{{ item.path }}"
```


ENFENCE

Repository with all fixes for my systems? Part 5.

```
- name: Analyze fixes
  ansible.builtin.include_tasks: fix_analyze.yml
  loop: "{{ epkg.files }}"
  loop_control:
    label: "{{ item.path }}"

- name: Save information about all fixes
  ansible.builtin.copy:
    content: "{{ epkgs | to_nice_json }}"
    dest: /nim/fixes/fixes.json
    owner: root
    group: system
    mode: "0644"
```


ENFENCE

Repository with all fixes for my systems? Appendix A. get_fix_info.yml

```
---
- name: Get available fixes
  ansible.builtin.set_fact:
    fixes: "{{ fixes | d([]) + [ item | regex_search('https://aix.software.ibm.com/aix/efixes/sec
urity/([A-Za-z0-9_]+.tar)', '\\1') ] }}"
  loop: "{{ report.value['0.report'] }}"

- name: Remove duplicates and nulls
  ansible.builtin.set_fact:
    fixes: "{{ fixes | flatten | unique | select() | sort }}"
```


ENFENCE

Repository with all fixes for my systems? Appendix B. fix_analyze.yml

```yaml
---
- name: Get efix information
  ansible.builtin.command:
    cmd: "emgr -d -v3 -e {{ item.path }}"
  changed_when: false
  register: efix_info

- name: Parse information
  ansible.utils.cli_parse:
    text: "{{ efix_info.stdout }}"
    parser:
      name: ansible.netcommon.native
      template_path: epkg_template.yml
    set_fact: epkg_info

- name: Get data
  ansible.builtin.set_fact:
    epkg_data: "{{ epkg_info.data }}"
  when: epkg_info.data is defined

- name: Add path information into data
  ansible.builtin.set_fact:
    epkg_data: "{{ epkg_data | combine( { 'path': item.path } ) }}"
  when: epkg_data is defined

- name: Add epkg information
  ansible.builtin.set_fact:
    epkgs: "{{ epkgs | d([]) + [ epkg_data ] }}"
  when: epkg_data is defined
```


ENFENCE

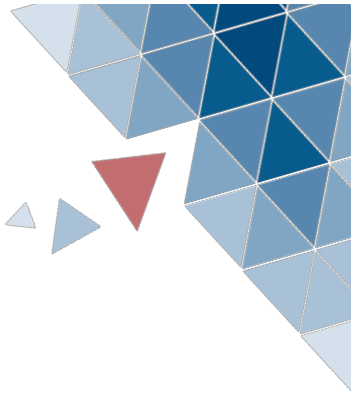
Repository with all fixes for my systems? Appendix C. epkg_template.yml

```
---
- example: 'LABEL:            IJ55968mAa'
  getval: 'LABEL: +(?P<label>[A-Za-z0-9]+)'
  result:
    data:
      label: "{{ label }}"
  shared: true

- example: 'bos.sysmgt.nim.client 7.2.5.202 7.2.5.204'
  getval: '(?P<fileset>[A-Za-z0-9_.]+) (?P<minver>[0-9.]+) (?P<maxver>[0-9.]+)'
  result:
    data:
      "{{ fileset }}":
        fileset: "{{ fileset }}"
        minver: "{{ minver }}"
        maxver: "{{ maxver }}"
```


ENFENCE

OK, I have my repository. How do I install the fixes?



EASY!
Mount the NFS share and run emgr!

ENFENCE

Installation of fixes. Part 1.

```yaml
---
- name: Install fixes on AIX
  hosts: all
  gather_facts: false
  vars:
    reboot_reqd: false

  tasks:
    - name: Get LPP information
      ibm.power_aix.lpp_facts:

    - name: Create temporary directory
      ansible.builtin.tempfile:
        path: /tmp
        prefix: emgr.
        state: directory
      register: emgr_mnt_dir

    - name: Mount fixes repo
      ibm.power_aix.mount:
        state: mount
        node: nim
        mount_dir: /nim/fixes
        mount_over_dir: "{{ emgr_mnt_dir.path }}"

    - name: Read fixes information
      ansible.builtin.slurp:
        src: "{{ emgr_mnt_dir.path }}/fixes.json"
      register: fixes_json

    - name: Set variables
      ansible.builtin.set_fact:
        fixes: "{{ fixes_json.content | b64decode | from_json }}"
```


ENFENCE

Installation of fixes. Part 2.

```
- name: Find installable fixes
  ansible.builtin.include_tasks: check_fix.yml
  loop: "{{ fixes }}"
  loop_control:
    label: "{{ fix.label }}"
    loop_var: fix

- name: Simplify list of fixes to install
  ansible.builtin.set_fact:
    install_list: "{{ install_list | sort(attribute='path') }}"

- name: Show fixes to install
  ansible.builtin.debug:
    var: install_list

- name: Install fix
  ansible.builtin.include_tasks: install_emgr.yml
  loop: "{{ install_list }}"
  loop_control:
    label: "{{ item.path }}"

- name: Unmount fixes repo
  ansible.posix.mount:
    state: unmounted
    path: "{{ emgr_mnt_dir.path }}"
    fstab: /dev/null

- name: Remove temporary directory
  ansible.builtin.file:
    path: "{{ emgr_mnt_dir.path }}"
    state: absent

- name: Reboot system
  ibm.power_aix.reboot:
    reboot_timeout: 600
  when: reboot_reqd
```


ENFENCE

Installation of fixes. Appendix A. check_fix.yml

```yaml
---
- name: Get list of filesets to patch
  ansible.builtin.set_fact:
    filesets: "{{ fix.keys() | list | difference( [ 'label', 'path' ] ) }}"

- name: Add fix to the list to be installed
  ansible.builtin.include_tasks: check_fileset.yml
  loop: "{{ filesets }}"
  loop_control:
    loop_var: fileset
  when: fileset in ansible_facts.filesets
```


ENFENCE

Installation of fixes. Appendix B. check_fileset.yml

```
---
- name: Get current installed fileset version
  ansible.builtin.set_fact:
    curver: "{{ ansible_facts.filesets[fileset].levels.keys() | first }}"

- name: Add fixes to installation list
  ansible.builtin.set_fact:
    install_list: "{{ install_list | d([]) + [ { 'path': fix.path | regex_replace('/nim/fixes', e
mgr_mnt_dir.path), 'fileset': fileset } ] }}"
  when: |
    curver is version(fix[fileset].maxver, '<=') and
    curver is version(fix[fileset].minver, '>=')
```


ENFENCE

Installation of fixes. Appendix C. install_emgr.yml

```yaml
---
- name: Install security fix (1st attempt)
  ibm.power_aix.emgr:
    action: install
    ifix_package: "{{ item.path }}"
    from_epkg: true
    extend_fs: true
  failed_when: false
  register: emgr1

- name: Check if the fileset is locked
  ansible.builtin.shell:
    cmd: "/usr/sbin/emgr -P | grep ^{{ item.fileset }}"
  changed_when: false
  failed_when: false
  register: check_result
  when: |
    "'return code 1' in emgr1.msg and
     'is locked by efix' in emgr1.stderr"

- name: Remove installed fixes if needed
  ibm.power_aix.emgr:
    action: remove
    ifix_label: "{{ label | split | last }}"
  loop: "{{ check_result.stdout_lines }}"
  loop_control:
    loop_var: label
  when:
    - "'return code 1' in emgr1.msg and 'is locked by efix' in emgr1.stderr"
    - check_result.rc == 0

- name: Install security fix (2nd attempt)
  ibm.power_aix.emgr:
    action: install
    ifix_package: "{{ item.path }}"
    from_epkg: true
    extend_fs: true
  register: emgr2
  when: "'return code 1' in emgr1.msg and 'is locked by efix' in emgr1.stderr"

- name: Check if reboot required
  ansible.builtin.set_fact:
    reboot_reqd: true
  when: |
    (emgr1.reboot_required is defined and emgr1.reboot_required) or
    (emgr2.reboot_required is defined and emgr2.reboot_required)
```


ENFENCE

Done?

No 😢

We are missing:

- Additional components like OpenSSH and OpenSSL
- RPMs
- Service Packs and TLs Updates
- AIX Upgrade

ENFENCE

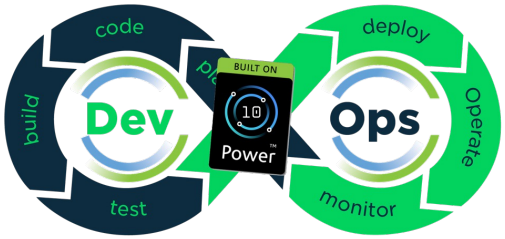
Done!

See my posts 🤗

https://blog.power-devops.com/p/upgrade-aix-72-to-73-with-ansible
https://blog.power-devops.com/p/update-aix-with-ansible
https://blog.power-devops.com/p/update-aix-with-ansible-part-2
https://blog.power-devops.com/p/update-aix-with-ansible-part-3a
https://blog.power-devops.com/p/update-aix-with-ansible-part-3b
https://blog.power-devops.com/p/update-aix-with-ansible-part-3c
https://blog.power-devops.com/p/update-aix-with-ansible-part-3d
https://blog.power-devops.com/p/update-aix-with-ansible-part-4

ENFENCE

About me



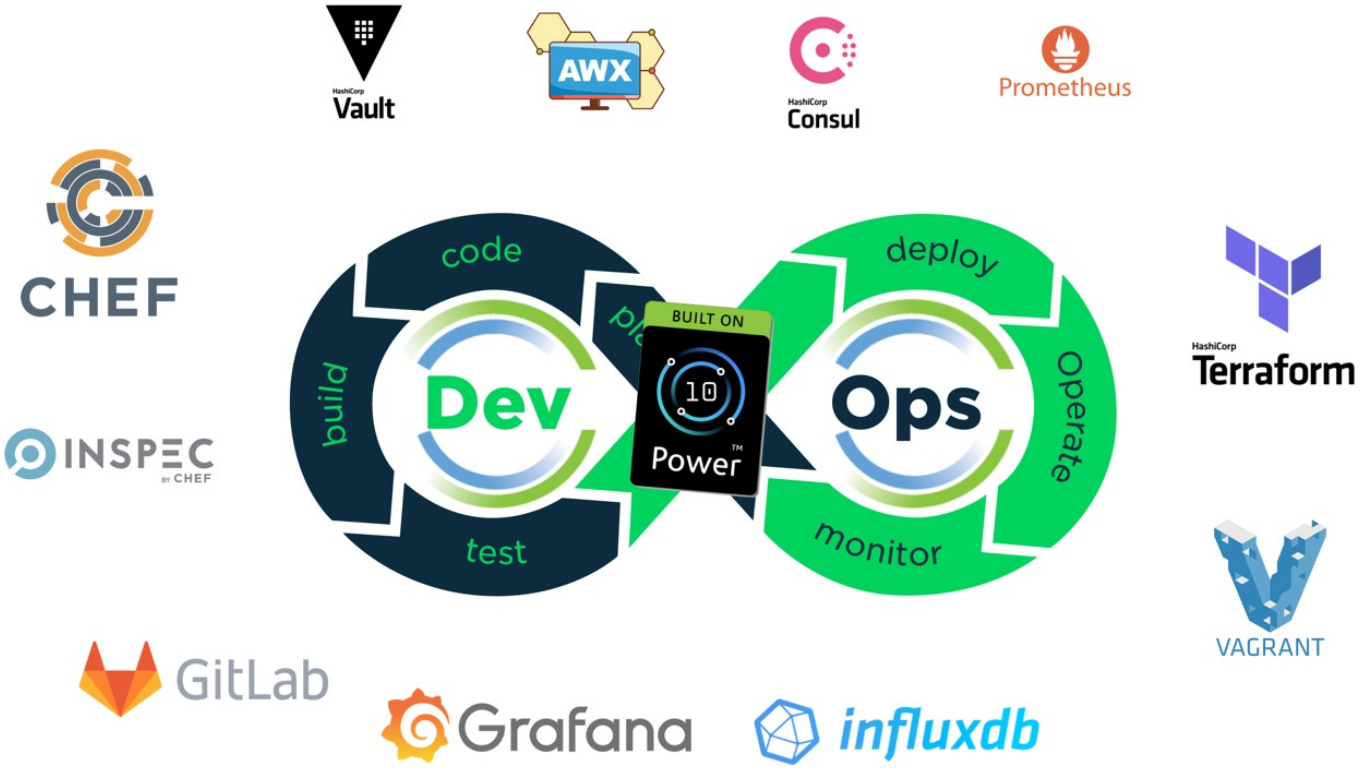
- Andrey Klyachkin
- IBM Champion on IBM Power
- IBM AIX Community Advocate
- IBM Certified Advanced Technical Expert, Red Hat Certified Engineer
- Author of different IBM AIX and IBM Power certifications
- IBM Redbooks Author
- Founder of power-devops.com (DevOps tools for IBM Power)
- E-mail: andrey.klyachkin@enfence.com
- LinkedIn: https://www.linkedin.com/in/aklyachkin/
- Youtube: https://www.youtube.com/@powerdevops
- Newsletter: https://blog.power-devops.com

ENFENCE

eNFence portfolio

- IBM Power and AIX Managed Services
- IT Automation and DevOps
- Security Audits and Hardening
- Private, Public and Hybrid Clouds
- Porting Software to IBM Power (IBM AIX, Linux on IBM Power)

ENFENCE



ENFENCE

IBM HTTPS Site with Security Fixes

man emgr_check_ifixes
Checks the availability of security interim fixes for the current operating system level.

```
# oslevel -s
7300-02-01-2346
# emgr_check_ifixes
Gathering system information
+-------------------------------------------------------------------------------+
p0.mtm=9040-MR9
p0.fw=VM950_145
p0.parnm=is3197
p0.os=aix
p0.aix=7300-02-01-2346
+-------------------------------------------------------------------------------+
Checking interim fixes on the system ...
+-------------------------------------------------------------------------------+
There is no efix data on this system.

Searching for AIX security fixes ...
+-------------------------------------------------------------------------------+
ERROR: HTTP connection failed. Data cannot be extracted
ERROR: failed to download CRL, http status log in  /tmp/ifix/crl.der
```


ENFENCE

IBM HTTPS Site with Security Fixes

man emgr_download_ifix
Downloads individual security patches and interim fixes.

NB: APAR IJ49379:
https://www.ibm.com/support/pages/apar/IJ49379
Fixed in AIX 7.3 TL2 SP2, AIX 7.2 TL5 SP8.

```
# oslevel -s
7300-02-01-2346
# emgr_download_ifix -L https://aix.software.ibm.com/aix/efixes/security/bind_fix26.tar
ssl connection failed, logs saved in  /tmp/ifix_22020366/ssl_connection_software.log
# grep error /tmp/ifix_22020366/ssl_connection_software.log
verify error:num=19:self-signed certificate in certificate chain
00000001:error:0A000086:SSL routines:tls_post_process_server_certificate:certificate verify failed:ssl/statem/statem_clnt.c:1890:
Verification error: self-signed certificate in certificate chain
```

```
# lslpp -w /var/ssl_aix/certs/DigiCert_Global_Root_CA.crt
  File                                        Fileset              Type
  ----------------------------------------------------------------------------
  /var/ssl_aix/certs/DigiCert_Global_Root_CA.crt
                                             bos.rte.install       File
# cp /var/ssl/certs/DigiCert_Global_Root_G2.crt /var/ssl_aix/certs/
# ln -s /var/ssl_aix/certs/DigiCert_Global_Root_G2.crt /var/ssl_aix/certs/607986c7.0
# emgr_download_ifix -L https://aix.software.ibm.com/aix/efixes/security/bind_fix26.tar
HTTP connection error. Data cannot be extract
error downloading CRL, http status log in  /tmp/ifix_14680380/crl.der
```


ENFENCE

IBM HTTPS Site with Security Fixes

wget or curl just works...

```
# wget https://aix.software.ibm.com/aix/efixes/security/bind_fix26.tar
--2024-06-08 15:02:08--  https://aix.software.ibm.com/aix/efixes/security/bind_fix26.tar
Resolving aix.software.ibm.com... 170.225.126.13
Connecting to aix.software.ibm.com|170.225.126.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 409989120 (391M) [application/x-tar]
Saving to: 'bind_fix26.tar'

bind_fix26.tar                      100%[=================================================================>] 391.00M   275KB/s    in 24m 25s

2024-06-08 15:26:33 (273 KB/s) - 'bind_fix26.tar' saved [409989120/409989120]
```


ENFENCE

Security Fixes: Installation

man emgr_sec_patch

the emgr_sec_patch command extracts the .tar file, identifies the applicable interim fixes for the current operating system level and installs the individual security interim fixes.

```
# emgr_sec_patch bind_fix26.tar
Downloaded Tar file name is: /tmp/fix/bind_fix26.tar
+-------------------------------------------------------------+
Verifying contents of /tmp/fix/bind_fix26.tar
+-------------------------------------------------------------+
+-------------------------------------------------------------+
Verifying integrity of Advisory.asc
+-------------------------------------------------------------+
Advisory.asc integrity verification passed
ERROR: 71bind.rte is not found in the tar file
```

IBM packed the fix another way!

ENFENCE

Security Fixes: Installation

I have many more fixes to test 😅

```
# emgr_sec_patch invscout_fix6.tar
Downloaded Tar file name is: /tmp/fix/invscout_fix6.tar
+-----------------------------------------------------------------------------+
Verifying contents of /tmp/fix/invscout_fix6.tar
+-----------------------------------------------------------------------------+
+-----------------------------------------------------------------------------+
Verifying integrity of Advisory.asc
+-----------------------------------------------------------------------------+
Advisory.asc integrity verification passed
+-----------------------------------------------------------------------------+
Checking System Level Prerequisites
+-----------------------------------------------------------------------------+
calling emgr -p -e /tmp/emgr_14680436/invscout_fix6/is22026s1a.240514.epkg.Z
Found the ifix /tmp/emgr_14680436/invscout_fix6/is22026s1a.240514.epkg.Z for the
+-----------------------------------------------------------------------------+
Verying signature of ifix
+-----------------------------------------------------------------------------+
ifix: /tmp/emgr_14680436/invscout_fix6/is22026s1a.240514.epkg.Z
Signature file found
Certificate found
Verified OK
Signature verification passed for /tmp/emgr_14680436/invscout_fix6/is22026s1a.24
Installing ifix /tmp/emgr_14680436/invscout_fix6/is22026s1a.240514.epkg.Z ...
+-----------------------------------------------------------------------------+
```


ENFENCE

Bonus: What is wrong with bind_fix26.tar?

This is not emgr.Z, but BFF!

```
# tar xvf bind_fix26.tar
x bind_fix26/71bind916.tar, 128491520 bytes, 250960 tape blocks
x bind_fix26/71bind916.tar.sig, 256 bytes, 1 tape blocks
x bind_fix26/72bind916.tar, 140738560 bytes, 274880 tape blocks
x bind_fix26/72bind916.tar.sig, 256 bytes, 1 tape blocks
x bind_fix26/73bind916.tar, 140738560 bytes, 274880 tape blocks
x bind_fix26/73bind916.tar.sig, 256 bytes, 1 tape blocks
x bind_fix26/Advisory.asc, 12424 bytes, 25 tape blocks
x bind_fix26/Advisory.asc.sig, 256 bytes, 1 tape blocks
```

```
# cd bind_fix26
# tar xvf 73bind916.tar
x 73bind916/73bind.rte, 140729344 bytes, 274862 tape blocks
```

```
# cd 73bind916
# installp -Ld 73bind.rte
bind.rte:bind.rte:7.3.916.4800::I:T:::::N:BIND Domain Name System::::0::
```


ENFENCE

Can I install the same fix twice?

No! Return Code == 0!

```
# emgr_sec_patch invscout_fix6.tar
Downloaded Tar file name is: /tmp/fix/invscout_fix6.tar
+-------------------------------------------------------------------------------+
Verifying contents of /tmp/fix/invscout_fix6.tar
+-------------------------------------------------------------------------------+
+-------------------------------------------------------------------------------+
Verifying integrity of Advisory.asc
+-------------------------------------------------------------------------------+
Advisory.asc integrity verification passed
/tmp/emgr_19071308/invscout_fix6/is22026s1a.240514.epkg.Z is already installed
# echo $?
0
```


ENFENCE

What happens if there is nothing to patch?

Nothing! Return Code == 0!

```
# emgr_sec_patch invscout_fix6.tar
Downloaded Tar file name is: /tmp/fix/invscout_fix6.tar
+-------------------------------------------------------------------------------+
Verifying contents of /tmp/fix/invscout_fix6.tar
+-------------------------------------------------------------------------------+
+-------------------------------------------------------------------------------+
Verifying integrity of Advisory.asc
+-------------------------------------------------------------------------------+
Advisory.asc integrity verification passed
+-------------------------------------------------------------------------------+
Checking System Level Prerequisites
+-------------------------------------------------------------------------------+
calling emgr -p -e /tmp/emgr_15532396/invscout_fix6/is22026s1a.240514.epkg.Z
Skipping ifix
See /var/adm/ras/emgr.log for more details
# echo $?
0
```


ENFENCE

Older patches?

Failed! Return Code == 1!

```
# emgr_sec_patch sendmail_fix3.tar
Downloaded Tar file name is: /tmp/fix/sendmail_fix3.tar
+-------------------------------------------------------------------------------+
Verifying contents of /tmp/fix/sendmail_fix3.tar
+-------------------------------------------------------------------------------+
+-------------------------------------------------------------------------------+
Verifying integrity of Advisory.asc
+-------------------------------------------------------------------------------+
00000001:error:02000068:rsa routines:ossl_rsa_verify:bad signature:crypto/rsa/rsa_sign.c:430:
00000001:error:1C880004:Provider routines:rsa_verify:RSA lib:providers/implementations/signature/rsa_sig.c:774:
ERROR: /tmp/emgr_15270376/sendmail_fix3/Advisory.asc integrity verification failed
# echo $?
1
```


ENFENCE

Use-cases from practice, which I did not test.

An older version of the fix is already installed. Will it be automatically uninstalled?

Two almost identical fixes – one for AIX and one for VIOS, with the same Dependencies section. Which fix will be installed?

ENFENCE