Belisama

April Newsletter

Subscribe/Unsubscribe

Greetings all,
Just a quick update, in between reading the new VM Recovery Manager Cookbook (draft has just been published – again Dino and Tim have done a magnificent job) and looking at preparing a 3 day PowerSC course.

2 Questions
These are the two questions I often ask my customers, and I think that they are well worth revisiting:

- **Are you making full use of all your packages and all their new features?**
  IBM often bundles in other software components with AIX (Security and Compliance, VM management…). Now is a good time to check your software entitlement and if it can make you job easier / environment more secure!
- **Are you making full use of your hardware?**
  I often work with customers who's Power Systems have significant resources available. They have a well maintained, secure and reliable environment – why not move other applications onto their Power infrastructure for little extra work and a greater saving? Linux systems running on other hardware is an obvious choice – providing greater RAS and reducing costs!.

Quick bites

Automating Oracle and AIX Installation with Ansible Tools
Ansible offers significant benefits by providing fast and repeatable installations and configurations for AIX and the Oracle Database, including the RAC feature.
Download this presentation which covers the available AIX and Oracle Ansible automation tools, and how they can be used to achieve better and more reliable installations.
Link

Are you having trouble getting your adapters to come up?
Have you found that the link of PCIe3 2 PORT 25/10/1 Gb NIC&ROCE SFP28 ADAPTER (feature code EC2U) takes a long time to come up if at all?

The answer lies in the fact that Mellanox adapters and switch use a low frequency communication method for auto-negotiation during the link up process. However, some switches have compatibility issues and do not support the low frequency communication in their hardware. In order to overcome the switch port speed getting locked to the negotiation signal, Cisco Nexus 9000 switches have a **dfe-tuning-delay** command that enables them to start locking to the signal only after a predefined delay time to avoid trying to lock on the low frequency signal. For more details see the support note.
Link

IBM AIX - Network Routing Explained
IBM Support has prepared a technote covering what a route is in AIX and how the OS uses it. Routing is a critical component of networking, and understanding how to manage routes is essential for system administrators working with AIX.
Link

In case you missed ….

AIX Operating System Enhancements and Update
This PowerVUG was held on 27th April, and the AIX operating system was discussed. Jayen Shah, Ian Robinson, and Isabella Richard from the IBM AIX team each presented and covered the AIX roadmaps, announcements and updates.
The presentation will be loaded into box shortly, check details in the VUG site.
Link

Coming soon

- **IBM TechXchange**
  This year will be held in Las Vegas from 11-14 September. This is an event that brings together industry experts, thought leaders, clients & partners to discuss and share knowledge on the latest technology from IBM. The Call for Speakers has just been released, please contact me if you are interested in presenting – otherwise add the dates to your calendar.
- **ASEANZK AIX/IBM i/Linux on Power Meetup Group**
  This meetup will look at Antivirus Protection for IBM i, AIX and Linux and will be held on Friday, 12th May 10:30 - 11:30 SG / 12:30 – 13:30 AU
  Summary:
  > No OS can afford to be unprotected. IBM i, IBM AIX and Linux on Power systems are typically known for running critical workloads and applications. This means the threat of viruses, malware, and ransomware pose a significant risk to your organisation. This Meetup will cover Powertech Antivirus that is designed to provide the level of protection your Power Systems servers need.

  Speaker:
  > This meetup features Rohit Mathur, Senior Director for APJ & MENA at Fortra. Rohit is responsible for building new markets, partner alliances and developing regional and large accounts for cybersecurity & IBM power portfolio. He has more than 20 years of experience in the fast-changing software arena, and has helped numerous customers manage, automate and secure their business applications

  Meetup Link
  IBM Community Link

Redbooks and Redpapers

- **VM Recovery Manager Cookbook**, draft Redbook, last updated on 26 April 2023
  Link
- **IBM Power Systems Virtual Server Guide for IBM AIX and Linux**, draft Redbook, last updated on 25 April 2023
  Link

IBM alerts and notices

AIX and PowerVM VIO Server alerts:

- **APAR IJ46487 potential undetected data loss after running chvg -ky or chvg -g**
  Potential undetected data loss can occur on disks larger than 2 TB if 'chvg -ky' is run to make the VG encryption capable, or if 'chvg -g' is run on a VG that is encryption capable. On AIX 7.3, VGs are created as encryption capable by default. For encryption capable VGs, 'lsvg <vgname>' shows:
  ENCRYPTION: yes
  If the 'chvg' commands above are run, a variable size block of LVM metadata can overwrite user data on disks in the VG that are larger than 2 TB. This can occur during the chvg command execution, and also could reoccur later if the metadata is updated on disk.
  Recommended Action
  Avoid the above 'chvg' commands until the following fix has been applied.
  Affected AIX Levels and Recommended Fixes (bos.rte.lvm)

Minimum Affected Level	Maximum Affected Level	Fixing Level
7300-01-00	7300-01-02-2320	7.3.1.2
7300-00-00	7300-00-03-2246	7300-00-04
7200-05-00	7200-05-06-2320	7200-05-07

  Link
- **Security Bulletin: CVE-2023-30441 affects IBM SDK, Java Technology Edition**
  CVE-2023-30441 affects IBM SDK, Java Technology Edition. An update has been released to address the vulnerability.
  Vulnerability Details
  CVEID: CVE-2023-30441 - IBM Runtime Environment, Java Technology Edition IBMJCEPlus and JSSE components could expose sensitive information using a combination of flaws and configurations.
  Affected Products and Versions
  8.0.7.0 - 8.0.7.11
  Link
- **Security Bulletin: AIX is vulnerable to an SSL server spoof due to Apache Commons HttpClient (CVE-2012-5783)**
  A vulnerability in Apache Commons HttpClient could allow a remote attacker to conduct spoofing attacks (CVE-2012-5783). AIX ships Apache Commons HttpClient as part of Electronic Customer Care.
  Vulnerability Details
  CVEID: CVE-2012-5783 - Apache Commons HttpClient, as used in Amazon Flexible Payments Service (FPS) merchant Java SDK and other products, could

allow a remote attacker to conduct spoofing attacks, caused by the failure to verify that the server hostname matches a domain name in the subject's Common Name (CN) field of the X.509 certificate. By persuading a victim to visit a Web site containing a specially-crafted certificate, an attacker could exploit this vulnerability using man-in-the-middle techniques to spoof an SSL server.

Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.1.5
AIX	7.2.5
AIX	7.3.0
AIX	7.3.1
VIOS	3.1

Link

- **Security Bulletin: AIX is vulnerable to arbitrary command execution (CVE-2023-26286)**

  A vulnerability in the AIX runtime services library could allow a non-privileged local user to execute arbitrary commands (CVE-2023-26286).

  Vulnerability Details

  CVEID: CVE-2023-26286 - IBM AIX could allow a non-privileged local user to exploit a vulnerability in the AIX runtime services library to execute arbitrary commands.

  Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.1
AIX	7.2
AIX	7.3
VIOS	3.1

  Link

- **Security Bulletin: AIX is vulnerable to arbitrary command execution due to invscout (CVE-2023-28528)**

  A vulnerability in the AIX invscout command could allow a non-privileged local user to execute arbitrary commands (CVE-2023-28528).

  Vulnerability Details

  CVEID: CVE-2023-28528 - IBM AIX could allow a non-privileged local user to exploit a vulnerability in the invscout command to execute arbitrary commands.

  Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.1
AIX	7.2
AIX	7.3
VIOS	3.1

  Link

- **Security Bulletin: AIX is vulnerable to denial of service vulnerabilities**
  UPDATED Apr 5
  > See 'Change History' for full update history. Current update corrected the affected upper fileset levels for VIOS to show that VIOS 3.1.2.50 and 3.1.3.30 are affected. Added iFixes for VIOS 3.1.2.50 and 3.1.3.30. This update applies to the kernel, perfstat, and pfcdd portions of the bulletin.

  Vulnerabilities in the AIX kernel and kernel extensions could allow a non-privileged local user to cause a denial of service (CVE-2022-43380, CVE-2022-40233, CVE-2022-39165, CVE-2022-43848, CVE-2022-43849, CVE-2022-39164).
  Vulnerability Details

  > CVEID: CVE-2022-43380 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX NFS kernel extension to cause a denial of service. IBM X-Force ID: 238640.
  > CVEID: CVE-2022-40233 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 235599.
  > CVEID: CVE-2022-39165 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in CAA to cause a denial of service. IBM X-Force ID: 235183.
  > CVEID: CVE-2022-43848 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX perfstat kernel extension to cause a denial of service. IBM X-Force ID: 239169.
  > CVEID: CVE-2022-43849 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX pfcdd kernel extension to cause a denial of service. IBM X-Force ID: 239170.
  > CVEID: CVE-2022-39164 - IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to cause a denial of service. IBM X-Force ID: 235181.

  Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.1
AIX	7.2
AIX	7.3
VIOS	3.1

  Link
- **Security Bulletin: AIX is vulnerable to arbitrary code execution due to libxml2 (CVE-2022-40303 and CVE-2022-40304)**
  UPDATED Apr 5:
  > Corrected the affected upper fileset levels for AIX 7.3 TL0 to show that SP03 is affected. Corrected the affected upper fileset levels for VIOS to show that VIOS 3.1.2.50 and 3.1.3.30 are affected. Added iFixes for AIX 7.3 TL0 SP03 and VIOS 3.1.2.50 and 3.1.3.30.

Vulnerabilities in libxml2 could allow a remote attacker to execute arbitrary code (CVE-2022-40303 and CVE-2022-40304). AIX uses libxml2 as part of its XML parsing functions.
Vulnerability Details

CVEID: CVE-2022-40304 - Gnome ibxml2 could allow a remote attacker to execute arbitrary code on the system, caused by a dict corruption flaw. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system.
CVEID: CVE-2022-40303 - Gnome libxml2 could allow a remote attacker to execute arbitrary code on the system, caused by an integer overflow in the XML_PARSE_HUGE function. By persuading a victim to open a specially-crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system.

Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.2
AIX	7.3
VIOS	3.1

Link

- **Security Bulletin: AIX is vulnerable to denial of service due to ISC BIND (CVE-2022-38178, CVE-2022-3080, CVE-2022-38177, CVE-2022-2795)**

UPDATED Apr 5

Corrected the affected upper fileset levels for AIX to show that AIX 7.1 TL5 SP11 and 7.3 TL0 SP03 are affected. Corrected the affected upper fileset levels for VIOS to show that VIOS 3.1.2.50 and 3.1.3.30 are affected. Added iFixes for AIX 7.1 TL5 SP11 and 7.3 TL0 SP03. Added iFixes for VIOS 3.1.2.50 and 3.1.3.30.

A vulnerability in ISC BIND could allow a remote attacker to cause a denial of service (CVE-2022-38178, CVE-2022-3080, CVE-2022-38177, CVE-2022-2795). AIX uses ISC BIND as part of its DNS functions.
Vulnerability Details

CVEID: CVE-2022-38178 - ISC BIND is vulnerable to a denial of service, caused by a memory leak in the DNSSEC verification code for the EdDSA algorithm. By spoofing the target resolver with responses that have a malformed EdDSA signature, a remote attacker could exploit this vulnerability to cause named to crash.
CVEID: CVE-2022-3080 - ISC BIND is vulnerable to a denial of service, caused by an error when stale cache and stale answers are enabled, option stale-answer-client-timeout is set to 0 and there is a stale CNAME in the cache for an incoming query. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause named to crash.
CVEID: CVE-2022-38177 - ISC BIND is vulnerable to a denial of service, caused by a small memory leak in the DNSSEC verification code for the ECDSA algorithm. By spoofing the target resolver with responses that have a malformed ECDSA signature, a remote attacker could exploit this vulnerability to cause named to crash.
CVEID: CVE-2022-2795 - ISC BIND is vulnerable to a denial of service, caused by a flaw in resolver code. By flooding the target resolver with queries, a remote

attacker could exploit this vulnerability to severely degrade the resolver's performance, effectively denying legitimate clients access to the DNS resolution service.

Affected Products and Versions

Affected Product(s)	Version(s)
AIX	7.1
AIX	7.2
AIX	7.3
VIOS	3.1

Link

Informational and software updates:

- **IBM Spectrum Scale Software Version Recommendation Preventive Service Planning**
  Support has provided their latest IBM Spectrum Scale Software Version Recommendation
  Link
- **PowerHA fix information for PowerHA 7.2.5 Service Pack 4**
  PowerHA 7.2.5 Service Pack 4 is now available for download as of October 2022.
  NOTE: PowerHA SystemMirror 7.2.5 SP4 testing has been done on the following AIX levels and are recommended:
  AIX7.3 TL01 SP1 (requires a critical AIX APAR IJ44756 for PowerHA GUI Cluster discovery to work.)
  AIX7.3 TL00 SP2
  AIX7.2 TL05 SP4
  AIX7.2 TL04 SP6
  AIX7.2 TL03 SP7
  AIX7.2 TL02 SP6
  AIX7.2 TL01 SP6
  AIX7.1 TL05 SP10
  Link
- **PowerHA fix information for PowerHA 7.2.4 Service Pack 6**
  PowerHA 7.2.4 Service Pack 6 is now available for download as of October 2022.
  NOTE: PowerHA SystemMirror 7.2.4 SP6 testing has been done on the following AIX levels and are recommended:
  AIX7.3 TL01 SP1 (requires a critical AIX APAR IJ44756 for PowerHA GUI Cluster discovery to work)
  AIX7.3 TL00 SP2
  AIX7.2 TL05 SP4
  AIX7.2 TL04 SP6
  AIX7.2 TL03 SP7
  AIX7.2 TL02 SP6
  AIX7.2 TL01 SP6
  AIX7.1 TL05 SP10
  Link

Product announcements:

- **Java SDK on AIX**
  Download and service information for IBM® Semeru Runtimes and the IBM SDK, Java™ Technology Edition (IBM SDK).
  Link

Technotes:

- **IBM AIX: NFS support for Encrypted File System (EFS) enabled J2 File system**
  Support has provided a detailed answer to whether EFS file systems can be supported by NFS Exports.
  In brief – No, due to the fact that:
  > The Encrypted Files System (EFS) enables individual users on the system to encrypt their data on J2 filesystem through their individual key stores. Also, file encryption information is further encrypted as users' and groups' public keys, and those encrypted keys would be stored in the file's Extended Attribute (EA).
  > Each J2 EFS-activated file is associated with a special Extended Attribute (EA) which contains EFS meta-data. The EA content is hidden from J2. Also, user's keystore password could be either tied to user's login password to load keystore at the time of login or an alternate password to manually load the keystore and thus, the EFS filesystems cannot be exported through NFS, and cannot be locally mounted through NFS.

  It would be a major enhancement to support and accomplish data encryption & decryption on NFS.
  Link

Keep safe and may the 4th be with you.
Red, Belisama