Belisama

October Newsletter

Subscribe/Unsubscribe

Greetings all,
I trust you are all keeping well? Please enjoy the interesting updates I found in October...

A few interesting updates for October

- For those in Sydney, there is a TechXchange Nov 28-29 at the International Convention Centre. Unfortunately it is still very AI focused, but I am trying to get some sessions on what is happening on the infrastructure side and so that IBM can share with the participants the exciting Power and AIX updates. Register
- I have been tidying up my "sanitisation script" – designed to help quickly and consistently remove corporate sensitive details from PD data before you send it to support. Hope to publish it soon on the IBM support site, but in meantime you can contact me for a copy.
- Working with PowerVS testing a quick and simple way to get your AIX workloads moved to Power in the IBM Cloud – transfer your mksysb to an existing image (at the same level of AIX) with a spare LUN for the new OS and then *alt_disk_install* is you friend!

Quick bites

AIX New features

Some of the new features in AIX:

- JFS2 now supports per file system configuration of the base number of *bufstructs* as a mount option. This support allows tuning a select JFS2 file system for improved performance when there are many concurrent large I/O operations;
- AIX multi-path IO (MPIO) is enhanced to throttle IO traffic on congested paths relative to good paths when FPIN (Fabric Performance Impact Notification) congestion notifications are received from fabric switches.
- AIX adds support to collect and display Fibre Channel optical transceiver information for diagnostic purposes. The information can be retrieved with the *fcstat* command for adapters that support data rates of 16Gb or higher.
- The AIX *vmo*, *ioo*, *raso*, *schedo*, and *asoo* commands are enhanced to allow collection of tunable values as non-root using a new aix.system.tune.display RBAC authorisation.
- The Ansible collections include the following updates in 2023
  AIX Collection:
  - New Modules: Bosboot, Physical and Logical Volume Encryption.
  - New Roles: nim_client_registration, nim_master_migration.
  - Feature enhancements in alt_disk and nim modules.
  - Enhanced use cases in existing playbooks.

VIOS

- Enhancements in VIOS backup and restore (*viosbr*) module.
- Enhanced documentation.

LINK

Intel based Servers out perform IBMPower!!!

Yes you read this correctly (Thank you Andrey for pointing this out):

> **IBM POWER5 (2005) delivers almost the same performance as modern Dell PowerEdge R960 with the latest generation of Intel CPUs.**

Check the latest SAP benchmark figures to confirm!

Link

Interested in becoming an IBM Champion

I have found it very useful to have a foot in the door with the IBM Developers to be able to influence the direction of the products we love and use. If you are interested see:

More information

or

Nominate

PowerVS synchronous replication

PowerVS now has synchronous replication within metro distances (30 to 60km) – but not yet in AP!

Link

Preparing a VIOS for maintenance using the HMC

In this tutorial, Chris Gibson explains how to prepare a VIOS for maintenance with the HMC, from validation to error detection and post-maintenance activity

Link

VIOS to NIM Mapping

If using NIM to backup, install or update a VIOS partition, the NIM master be at the correct AIX level based on the VIOS version.

Link

How to use MTU 9000 (jumbo frame) in environment with AIX LPAR and VIOS

This Technote from IBM Support explains how to use MTU 9000 (jumbo frame) in a virtualised AIX LPAR.

Link

Changes required in your firewall for Call Home and Electronic fix distribution

Check the link for details of the required changes.

Link

AIX PowerDraw

PowerDraw provides customers with an interactive graphical representation of their Power Systems. It collects all the information about the server, VIOS, and partitions from the HMC, and then creates interactive drawings of the components and their connections.

Link

Adding new binaries to the AIX Trusted Signature Database

IBM support has published a Technote outlining the steps to add new entries in the Trusted Signature Database.

Link

In case you missed ….

- **Scrunching with Scaled Throughput Mode with Earl Jew**
  Scrunching with Scaled Throughput Mode – is about a Power AIX tactic; a tactic that we all can follow. The schedo tuneable *vpm_throughput_mode* (options 0,1,2,4,8) has been a feature of AIX since 2013 (that is also called Scaled Throughput Mode). Since its announcement in 2013, this feature was rarely discussed and virtually. never used.
  Link

Coming soon

- **November ASEANZK Power (AIX, i, Linux) Meetup,**
  Our next meeting in on Friday, 17th 10:00 SG/13:00 AEDT and in this session Shamsul discuss **Achieving Operational Excellence in SAP Environments with SUSE Trento and Monitoring**
  Shamsul Zulkifli is a Solutions Architect working with the SUSE ASEAN team. He plays a crucial role in identifying, testing, and delivering solutions that bring immense value to SUSE in the marketplace.
  Meetup
  IBM Community

Redbooks and Redpapers

- **IBM Power S1014, S1022s, S1022, and S1024 Technical Overview and Introduction** , Redpaper, revised: 06 October 2023
  Link

IBM alerts and notices

AIX and PowerVM alerts:

- **AIX is vulnerable to sensitive information exposure due to Perl (CVE-2023-31484 and CVE-2023-31486)**
  Multiple vulnerabilities in AIX's Perl could allow an attacker to launch a man-in-the attack to obtain sensitive information or further compromise the system (CVE-2023-31484 and CVE-2023-31486). AIX uses Perl in various operating system components.
  iFixes are now available for Perl 5.28.1 and 5.34.1. The fixes are offered in lieu of updating to Perl 5.28.1.8 and 5.34.1.4, which have a dependency on OpenSSL 3.0.
  The iFixes may be downloaded from iFixes
  Vulnerability Details
  CVEID: CVE-2023-31484- CPAN.pm is vulnerable to a man-in-the-middle attack, caused by improper validation of TLS certificates when downloading distributions over HTTPS. An attacker could exploit this vulnerability to

launch a man-in-the-middle attack and gain access to the communication channel between endpoints to obtain sensitive information or further compromise the system.
CVE-2023-31486 - Perl HTTP::Tiny module is vulnerable to a man-in-the-middle attack, caused by an insecure default TLS configuration. An attacker could exploit this vulnerability to launch a man-in-the-middle attack and gain access to the communication channel between endpoints to obtain sensitive information or further compromise the system.

Affected Products and Versions

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

The following fileset levels are vulnerable:

Fileset	Lower Level	Upper Level
perl.rte	5.28.0.0	5.28.1.7
perl.rte	5.34.0.0	5.34.1.3

Link

- **AIX is vulnerable to a denial of service due to NTP (CVE-2023-26551, CVE-2023-26552, CVE-2023-26553, CVE-2023-26554)**

Multiple vulnerabilities in NTP could allow a remote attacker to cause a denial of service (CVE-2023-26551, CVE-2023-26552, CVE-2023-26553, CVE-2023-26554).

Vulnerability Details

CVE-2023-26551 - NTP is vulnerable to a denial of service, caused by an out-of-bounds write in mstolfp in libntp/mstolfp.c. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-26552 - NTP is vulnerable to a denial of service, caused by an out-of-bounds write in mstolfp in libntp/mstolfp.c. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-26553 - NTP is vulnerable to a denial of service, caused by an out-of-bounds write in mstolfp in libntp/mstolfp.c. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a denial of service.
CVE-2023-26554 - NTP is vulnerable to a denial of service, caused by an out-of-bounds write in mstolfp in libntp/mstolfp.c. By sending a specially-crafted request, a remote attacker could exploit this vulnerability to cause a denial of service.

Affected Products and Versions

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

VIOS 3.1

The vulnerabilities in the following filesets are being addressed:

Fileset	Lower Level	Upper Level
ntp.rte	7.4.2.8100	7.4.2.8153
ntp.rte	73.4.2.8151	73.4.2.8154

Link

ESS and GPFS:

- **The following fixpacks are now available**

  These fixpacks are cumulative and include all fixes completed since the last release.

  - ESS_DAE_UNIFIED-6.1.8.3-x86_64-EMS
  - ESS_DME_UNIFIED-6.1.8.3-ppc64LE-EMS
  - ESS_VM-6.1.8.3-x86_64-BYOE-EMS
  - ESS_VM-6.1.8.3-x86_64-UTILITY-EMS
  - ESS_DAE_UNIFIED-6.1.8.3-ppc64LE-EMS
  - ESS_DME_UNIFIED-6.1.8.3-x86_64-EMS

Keep safe and hope to see you at TechXChange Sydney.
Red, Belisama