March Newsletter

Subscribe/Unsubscribe

Greetings all,
I hope you are all keeping well and adjusting to the new normal? I must say however, that as much as I like working from home, it has been great to be able to get out and into data centres again, to mix with people, not just images on a screen. It has also been a pleasant change to be able to travel and meet my overseas customers.

A few updates to share

- Do you feel that everyone is talking about containers and you may be missing out on something? Have a look at opensource.com, which has a quick and easy introduction (https://opensource.com/article/22/2/start-running-containers) amongst other useful resources (for example a cool *grep* cheat-sheet that can be downloaded)
- We now have 5 useful presentations prepared by Satid (See the "i Series" Series at https://www.belisama.com.sg/publications).
- April ASEAN Meetup – we hope to have Satid talking about "Using IBM i PDI charts to answer performance questions" and Simon Hutchinson (of RPGPGM.COM fame) on "Speeding Up Your RPG and SQL". Details will be available soon through our page in IBM Community, or through Meetup.
- The Redbook editors have been working overtime and turned a couple of pig's ears into silk purses – or turned 2 of the Redpapers that I worked on into much more readable publications. Yes, the GLVM and HA/DR on prem and in the cloud are now no longer in draft.

Quick bites

AIX ulimit and maxuproc
IBM Support has just published a quick Q&A about the change in "ulimit -a" that was introduced in AIX 7.2 TL5 and 7.3
See: https://www.ibm.com/support/pages/node/6561649?myns=aix&mynp=OCSWG10&mync=E&cm_sp=aix-_-OCSWG10-_-E

The new ethernet device driver attribute "autoconfig" in AIX 7.3
IBM Support has just published a quick update on the feature introduced in 7.3 to allow the use to specify which port to bring into an available state or defined state. This will avoid problems that may occur when unused ports are queried or monitored.
See: https://www.ibm.com/support/pages/node/6527662?myns=aix&mynp=OCSWG10&mync=E&cm_sp=aix-_-OCSWG10-_-E

How malware is reshaping IBM i Security

Deploy robust, multi-layered and resilient defences to protect your business against advanced threats.
See: https://more.techchannel.com/precisely-how-malware-is-reshaping-ibm-i-security

The top 10 reasons to love AIX

IBM Champion Rob McNelly highlights his top reasons to love the AIX and Power Systems.
See: https://techchannel.com/SMB/02/2022/top-reasons-aix

How to rename a shared volume group in a PowerHA Cluster

IBM Support published a short article on the simple steps to rename a shared volume group used in a PowerHA Cluster.
See: https://www.ibm.com/support/pages/node/6564017?myns=swgother&mynp=OCSSPHQG&mync=E&cm_sp=swgother-_-OCSSPHQG-_-E

Power VUG

Sadly Joseph Armstrong has stepped down as the organiser of the Power Systems VUG. His role will be taken over by Ross Coniglio and Brian McDonald, so is still in capable hands. Joseph went out with a bang, as his last VUG was an SME Round table with an impressive group of SME's sharing their top hints and tips
See the Power Systems VUG Wiki site for past and future topics:
http://ibm.biz/powersystemsvug

The impact of log4j in the Open Source ecosystem

IBM i open-source leader Jesse Gorzinski discusses the log4j vulnerability, outlines software maintenance best practices and explains why open-source users should give back to the community.
See: https://techchannel.com/Trends/03/2022/log4j-open-source-ecosystem

A new home for the RFE community

Rob McNelly covers the "Request for Enhancement" (RFE) process in IBM and the new IBM Power Systems Ideas portal.
See: https://techchannel.com/Trends/03/2022/new-rfe-community

Ansible automation for Oracle Database on IBM Power

Ansible automation eliminates repetitive IT management tasks and provides a repeatable process reducing the risk of errors. Code is available from the AIX Oracle Collection on GitHub (https://github.com/IBM/ansible-power-aix-oracle).
See:
https://mediacenter.ibm.com/media/Ansible+Automation+for+Oracle+Database+on+IBM+Power/1_0zskjfjx

IBM Semeru Runtime Certified Edition V11 is certified for Power systems running Oracle WebLogic Server V 14.1

On March 1, 2022, Oracle announced the support of Semeru Runtime Certified Edition V11 with Oracle WebLogic Server 14.1.1.0.0.
See: https://www.ibm.com/support/pages/system/files/inline-files/Flash_Oracle_%20WLS_%2014.1%20AIX.pdf

Nigel’s brief history of AIX

If you have ever wondered when key features of AIX arrived, or what new features are available in a newer AIX release, then have a look at this quick summary published by IBM Support.
See: https://www.ibm.com/support/pages/brief-history-aix

IBM Expert TV

Catch up with their latest presentations, which include:

- High Performance Computing in the IBM Cloud
- SocialNot: AI Ethics with IBM Experts and their families
- IBM Security: Behind the Shield with Nick Bradley and Mitch Mayne
- Update from IBM Centre for Cloud Training

See: https://techtv.bemyapp.com/#/event

Bullfeeware now a git repository

For those fans of Bullfreeware, who were concerned last month at the announcement of it’s demise, worry no more!.
See: https://github.com/power-devops/bullfreeware

Planning to use memory-backed volumes in Kubernetes?

Pradipta Banerjee provides a very useful summary of emptyDir volumes and important things to look our for.
See: https://www.linkedin.com/pulse/planning-use-memory-backed-volumes-kubernetes-read-once-banerjee/

Handling Different Container Runtimes and Configurations in Kubernetes?

If you have been transitioning workloads to Kubernetes, I am sure that you have wondered how you can manage conflicting workloads in the cluster? Pradipta Banerjee provides a very clear guide for you.
See: https://www.linkedin.com/pulse/handling-different-container-runtimes-configurations-banerjee/

In case you missed ….

- **IBM Power Systems VUG (March)**
  As mentioned above the last VUG was a round table with IBM SMEs discussing their experiences.
  See: http://ibm.biz/powersystemsvug

Coming soon

- **IBM Power and Red Hat: Modernisation, Simplified**
  Friday 29/4/22 at 01:00 UTC +8
  As enterprises look to deliver the personalised, responsive, mobile experiences that many millennials expect - from their banks, their clothing brands, and everything in between - enabling that transformation in a timely manner is critical.
  Presented by: Chuck Bryan, Joe Cropper and Ramon Villarreal
  See: https://event.webcasts.com/starthere.jsp?ei=1535614&tp_key=d20f2f40d9

- **IBM Spectrum Scale Webinars: HDFS**
  Friday 1/4/22 23:00 UTC+8
  This webinar will focus on HDFS in IBM Spectrum Scale ;
  - A brief overview of the Hadoop Distributed File System (HDFS) architecture.
  - How Spectrum Scale implements HDFS services on top of a GPFS file system, known as HDFS Transparency.
  - How Cluster Export Services (CES) provides high availability.
  - Integration with Cloudera Data Platform (CDP) Private Cloud Base.
  - Tips for troubleshooting and debugging HDFS Transparency.
  - Tips for configuration and tuning.

  Register: https://www.ibm.com/support/pages/node/6557068?myns=s033&mynp=OCSTXKQY&mynp=OCSTHMCM&mync=E&cm_sp=s033-_-OCSTXKQY-OCSTHMCM-_-E

- **Best Practices for Protecting IBM i Data with Field Encryption**
  Friday 1/4/22 05:00 UTC +8
  Lloyd Ramdarie discusses best practices to effectively encrypt your IBM i sensitive data columns while at rest as well as in transit
  Register: https://lp.seasoft.com/webinar-signup-best-practices-for-protecting-ibm-i-data-with-field-encryption

Redbooks and Redpapers

- **IBM Tape Library Guide for Open Systems**, Redbook, Published: March 9, 2022
  http://www.redbooks.ibm.com/abstracts/sg245946.html?Open
- **IBM Spectrum Archive Enterprise Edition V1.3.2.2: Installation and Configuration Guide**, Redbook, Published: March 10, 2022
  http://www.redbooks.ibm.com/abstracts/sg248333.html?Open

- **Implementation Guide for IBM Spectrum Virtualize for Public Cloud on Microsoft Azure Version 8.4.3**, Redbook, Published: March 15, 2022
  http://www.redbooks.ibm.com/abstracts/sg248510.html?Open
- **High Availability and Disaster Recovery Options for IBM Power Cloud and On-Premises**, Redpwper, Published: March 17, 2022
  http://www.redbooks.ibm.com/abstracts/redp5656.html?Open
- **Asynchronous Geographic Logical Volume Mirroring Best Practices for Cloud Deployment**, Redpater, Published: March 18, 2022
  http://www.redbooks.ibm.com/abstracts/redp5665.html?Open
- **IBM Power Systems Private Cloud with Shared Utility Capacity: Featuring Power Enterprise Pools 2.0**, draft Redbook, Revised: March 24, 2022
  http://www.redbooks.ibm.com/abstracts/sg248478.html?Open

IBM alerts and notices

AIX alerts:

- **Vulnerability in AIX audit commands (CVE-2021-38955)**
  IBM AIX could allow a local user with elevated privileges to cause a denial of service due to a file creation vulnerability in the audit commands.
  See: https://www.ibm.com/support/pages/node/6560236?myns=aix&mynp=OCSWG10&mync=E&cm_sp=aix-_-OCSWG10-_-E
  Applies to:

Version	From	To	APAR	Service Pack
AIX 7.1	7.1.5.0	7.1.5.37	IJ38113	SP10
AIX 7.2	7.2.4.0	7.2.4.4	IJ38115	SP06
	7.2.5.0	7.2.5.2	IJ38117	SP04
	7.2.5.100	7.2.5.101	IJ38117	SP04
AIX 7.3	7.3.0.0	7.3.0.0	IJ38121	SP02
VIOS 3.1.1			IJ38115	3.1.1.60
VIOS 3.1.2			IJ38119	3.1.2.40
VIOS 3.1.3			IJ38117	3.1.3.20

- **Vulnerabilities in AIX CAA (CVE-2022-22350, CVE-2021-38996)**
  There are two vulnerabilities, IBM AIX could allow a non-privileged local user to exploit a vulnerability in CAA or the AIX kernel to cause a denial of service.
  See: https://www.ibm.com/support/pages/node/6560390?myns=aix&mynp=OCSWG10&mync=E&cm_sp=aix-_-OCSWG10-_-E
  Applies to:

Fileset	Lower level	Upper level
bos.cluster.rte	7.1.5.0	7.1.5.38
bos.cluster.rte	7.2.4.0	7.2.4.4

bos.cluster.rte	7.2.5.0	7.2.5.1
bos.cluster.rte	7.2.5.100	7.2.5.101
bos.cluster.rte	7.3.0.0	7.3.0.0

APAR:

AIX	APAR	Service Pack
7.1.5	IJ37355	SP10
7.2.4	IJ37496	SP06
7.2.5	IJ36682	SP04
7.3.0	IJ36596	SP02
VIOS		
3.1.1	IJ37496	3.1.1.60
3.1.2	IJ37512	3.1.2.40
3.1.3	IJ36682	3.1.3.20

- **Vulnerability in the AIX kernel (CVE-2021-38988)**
There is a ulnerability in the AIX pfcdd kernel extension that could be exploited to cause a denial of service.
See: https://www.ibm.com/support/pages/node/6561281?myns=aix&mynp=OCSWG10&mync=E&cm_sp=aix-_-OCSWG10-_-E
Applies to:

Fileset	Lower level	Upper level
bos.pfcdd.rte	7.1.5.0	7.1.5.32
bos.pfcdd.rte	7.2.4.0	7.2.4.0
bos.pfcdd.rte	7.2.5.0	7.2.5.0
bos.pfcdd.rte	7.3.0.0	7.3.0.0

APAR:

AIX	APAR	Service Pack
7.1.5	IJ37508	SP10
7.2.4	IJ37504	SP06
7.2.5	IJ37494	SP04
7.3.0	IJ37403	SP02
VIOS		
3.1.1	IJ37504	3.1.1.60
3.1.2	IJ37779	3.1.2.40
3.1.3	IJ37494	3.1.3.20

- **Vulnerability in the AIX kernel (CVE-2021-38989)**
  There is a ulnerability in the AIX pmsvcs kernel extension that could be exploited to cause a denial of service.
  See: https://www.ibm.com/support/pages/node/6561277?mynns=aix&mynp=OCSWG10&mync=E&cm_sp=aix-_-OCSWG10-_-E
  Applies to:

Fileset	Lower level	Upper level
bos.pmapi.pmsvcs	7.1.5.0	7.1.5.36
bos.pmapi.pmsvcs	7.2.4.0	7.2.4.4
bos.pmapi.pmsvcs	7.2.5.0	7.2.5.1
bos.pmapi.pmsvcs	7.2.5.100	7.2.5.100
bos.pmapi.pmsvcs	7.3.0.0	7.3.0.0

APAR:

AIX	APAR	Service Pack
7.1.5	IJ37507	SP10
7.2.4	IJ37503	SP06
7.2.5	IJ37488	SP04
7.3.0	IJ37411	SP02
VIOS		
3.1.1	IJ37503	3.1.1.60
3.1.2	IJ37778	3.1.2.40
3.1.3	IJ37488	3.1.3.20

- **Vulnerability in AIX nimsh (CVE-2022-22351)**
  There is a vulnerability in the AIX nimsh daemon that could be exploited in the nimsh daemon on another host to cause a denial of service.
  See: https://www.ibm.com/support/pages/node/6561275?myns=aix&mynp=OCSWG10&mync=E&cm_sp=aix-_-OCSWG10-_-E
  Applies to:

Fileset	Lower level	Upper level
bos.sysmgt.nim.client	7.1.5.0	7.1.5.37
bos.sysmgt.nim.client	7.2.4.0	7.2.4.4
bos.sysmgt.nim.client	7.2.5.0	7.2.5.1
bos.sysmgt.nim.client	7.2.5.100	7.2.5.100
bos.sysmgt.nim.client	7.3.0.0	7.3.0.0

APAR:

AIX	APAR	Service Pack

7.1.5	IJ37419	SP10
7.2.4	IJ37705	SP06
7.2.5	IJ36681	SP04
7.3.0	IJ36593	SP02
VIOS		
3.1.1	IJ37705	3.1.1.60
3.1.2	IJ37706	3.1.2.40
3.1.3	IJ36681	3.1.3.20

- **Vulnerability in BIND affects AIX (CVE-2021-25219)**
  ISC BIND is vulnerable to a denial of service, caused by a flaw in response processing. By abusing a lame cache, an attacker could exploit this vulnerability to cause a named resolver to spend most of its CPU time on managing and checking the lame cache and severely degrade resolver performance.
  See: https://www.ibm.com/support/pages/node/6561275?myns=aix&mynp=OCSWG10&mync=E&cm_sp=aix-_-OCSWG10-_-E
  Applies to:

Fileset	Lower level	Upper level
bos.net.tcp.server	7.1.5.0	7.1.5.35
bos.net.tcp.client	7.1.5.0	7.1.5.40
bos.net.tcp.bind	7.2.4.0	7.2.4.1
bos.net.tcp.bind_utils	7.2.4.0	7.2.4.3
bos.net.tcp.bind	7.2.5.0	7.2.5.1
bos.net.tcp.bind_utils	7.2.5.0	7.2.5.2
bos.net.tcp.bind	7.2.5.100	7.2.5.100
bos.net.tcp.bind_utils	7.2.5.100	7.2.5.100
bos.net.tcp.bind	7.3.0.0	7.3.0.0
bos.net.tcp.bind_utils	7.3.0.0	7.3.0.0

APAR:

AIX	APAR	Service Pack
7.1.5	IJ37222	SP10
7.2.4	IJ37225	SP06
7.2.5	IJ37223	SP04
7.3.0	IJ37226	SP02
VIOS		
3.1.1	IJ37225	3.1.1.60
3.1.2	IJ37224	3.1.2.40

3.1.3	IJ37223	3.1.3.20

- **High Impact / Highly Pervasive APAR IJ38518**
  In AIX 7.3, some performance tuning commands' default output changed when called with the -x option. Live Update stats were added to default -x output for commands such as "vmo". This change in output may break some applications that depend on it, such as Oracle RAC tuning pre-checks.
  See: https://www.ibm.com/support/pages/node/6563017?myns=aix&mynp=OCSWG10&mync=E&cm_sp=aix-_-OCSWG10-_-E
  Affected levels and recommended fixes

Minimum Affected Level	Maximum Affected Level	Fixing Level	Interim Fix
7300-00-00 bos.perf.tune 7.3.0.0	7300-00-01-2148 bos.perf.tune 7.3.0.0	7300-00-02 IJ38518: http://www-01.ibm.com/support/docview.wss?uid=isg1IJ38518	http://aix.software.ibm.com/aix/ifixes/ij38518/

PowerHA alerts:

- **Lodash versions prior to 4.17.21 vulnerability in PowerHA System Mirror for AIX**
  Node.js lodash module could allow a remote authenticated attacker to execute arbitrary commands on the system, caused by a command injection flaw in the template.
  See: https://www.ibm.com/support/pages/node/6524656?myns=swgother&mynp=OCSSPHQG&mync=E&cm_sp=swgother-_-OCSSPHQG-_-E
  Applies to:
  - 7.2.1 *
  - 7.2.2 *
  - 7.2.3
  - 7.2.4
  - 7.2.5

  * Versions out of support as on Dec-2021
  Remediation / Fixes:
  The service packs of PowerHA 7.2.5 SP1, 7.2.4 SP4 & 7.2.3 SP6 are upgraded to latest version of lodash which remediates this vulnerability.

ESS notices:

- **ESS_DME_BASEIMAGE_3000-6.1.2.2-x86_64-Linux**
  This fixpack is cumulative and includes all fixes completed since the last release.
  See: http://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FStorageSoftware%2FIBM+Elastic+Storage+Server+%28ESS%29&fixids=ESS_DME_BASEIMAGE_3000-6.1.2.2-x86_64-Linux&source=myna&myns=s033&mynp=OCSTHMCM&mync=E&cm_sp=s033-_-OCSTHMCM-_-E

- **ESS_DME_BASEIMAGE_5000-6.1.2.2-ppc64LE-Linux**
  This fixpack is cumulative and includes all fixes completed since the last release.
  See: https://www.ibm.com/support/fixcentral/swg/selectFixes?product=ibm%2FStorageSoftware%2FIBM+Elastic+Storage+Server+%28ESS%29&fixids=ESS_DME_BASEIMAGE_5000-6.1.2.2-ppc64LE-Linux&source=myna&myns=s033&mynp=OCSTHMCM&mync=E&cm_sp=s033-_-OCSTHMCM-_-E&function=fixId&parent=Software%20defined%20storage

- **ESS_DAE_BASEIMAGE_5000-6.1.2.2-ppc64LE-Linux**
  This fixpack is cumulative and includes all fixes completed since the last release.
  See: http://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FStorageSoftware%2FIBM+Elastic+Storage+Server+%28ESS%29&fixids=ESS_DAE_BASEIMAGE_5000-6.1.2.2-ppc64LE-Linux&source=myna&myns=s033&mynp=OCSTHMCM&mync=E&cm_sp=s033-_-OCSTHMCM-_-E
  •

- **ESS_DAE_BASEIMAGE_3000-6.1.2.2-x86_64-Linux**
  This fixpack is cumulative and includes all fixes completed since the last release.
  See: http://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FStorageSoftware%2FIBM+Elastic+Storage+Server+%28ESS%29&fixids=ESS_DAE_BASEIMAGE_3000-6.1.2.2-x86_64-Linux&source=myna&myns=s033&mynp=OCSTHMCM&mync=E&cm_sp=s033-_-OCSTHMCM-_-E

- **ESS_FIRMWARE-6.0.0.17-ppc64LE-Linux**
  This fixpack is cumulative and includes all fixes completed since the last release.
  See: http://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FStorageSoftware%2FIBM+Elastic+Storage+Server+%28ESS%29&fixids=ESS_FIRMWARE-6.0.0.17-ppc64LE-Linux&source=myna&myns=s033&mynp=OCSTHMCM&mync=E&cm_sp=s033-_-OCSTHMCM-_-E

- **IBM Spectrum Scale Software Version Recommendation Preventive Service Planning**

This generalised recommendation is made available to assist clients in implementing a code update strategy.
See: http://www.ibm.com/support/fixcentral/quickorder?product=ibm%2FStorageSoftware%2FIBM+Elastic+Storage+Server+%28ESS%29&fixids=ESS_FIRMWARE-6.0.0.17-ppc64LE-Linux&source=myna&myns=s033&mynp=OCSTHMCM&mync=E&cm_sp=s033-_-OCSTHMCM-_-E

Code	Recommendation
IBM Spectrum Scale	5.0.x stream: 5.0.5.91 [Aug 2021] EOS April 2022 5.1.x stream: 5.1.1.4 [Oct 2021] 5.0.x stream: 5.0.5.131 2 [Mar 2022] EOS April 2022 5.1.x stream: 5.1.2.34 (Mar 2022) 5.1.x stream: 5.1.3.0 (Mar 2022)
IBM Spectrum Scale for ESS	5.0.x stream: ESS 5.3.7.3 [Nov 2021] EOS April 2022 5.1.x stream: ESS 6.1.1.23 [Sept 2021] 5.0.x stream: ESS 5.3.7.4 [Jan 2022] EOS April 2022 5.1.x stream: ESS 6.1.2.2 [Feb 2022]
IBM Elastic Storage System 3000 and 5000	5.0.x stream: ESS 6.0.2.3 [Nov 2021] EOS April 2022 5.1.x stream: ESS 6.1.1.23 [Sept 2021] 5.0.x stream: ESS 6.0.2.4 [Jan 2022] EOS April 2022 5.1.x stream: ESS 6.1.2.2 [Feb 2022]
IBM Elastic Storage System 3200	5.1.x stream: ESS 6.1.1.23 [Sept 2021] 5.1.x stream: ESS 6.1.2.2 [Feb 2022]

ESS alerts:

- **Daemon restart or failure to mount file system when using RDMA**
  The following symptoms could be seen on a system with Infiniband or RoCE interconnect with RDMA enabled:
  - Intermittent restart of the Spectrum Scale daemon
  - File system fails to mount at the client

  The Spectrum Scale log shows entries like this:

  ```
  logAssertFailed: wcOpcode == IBV_WC_SEND || wcOpcode ==
  IBV_WC_RDMA_READ || wcOpcode == IBV_WC_RDMA_WRITE
  ```

  See: https://www.ibm.com/support/pages/node/6558812?myns=s033&mynp=OCSTHMCM&mync=E&cm_sp=s033-_-OCSTHMCM-_-E

- **Security Bulletin: Ansible vulnerability affects IBM Elastic Storage System (CVE-2021-3583)**
  See: https://www.ibm.com/support/pages/node/6560038?myns=s033&mynp=OCSTHMCM&mync=E&cm_sp=s033-_-OCSTHMCM-_-E
  IBM Elastic Storage System is shipped with ansible, for which a fix is available.

The following versions are affected and it is recommended to upgrade your ESS 3000, 3200, or 5000 to the following levels:

  - for 6.0.0 – 6.0.2.3
    V6.0.2.4
    See: https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=Software%20defined%20storage&product=ibm/StorageSoftware/IBM+Elastic+Storage+Server+(ESS)&release=6.0.0&platform=All&function=all
  - for 6.1.0 – 6.1.2.1
    V6.1.2.2
    See: https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=Software%20defined%20storage&product=ibm/StorageSoftware/IBM+Elastic+Storage+Server+(ESS)&release=6.1.0&platform=All&function=all

- **Security Bulletin: glibc vulnerability affects IBM Elastic Storage System (CVE-2021-27645)**
  See: https://www.ibm.com/support/pages/node/6560036?myns=s033&mynp=OCSTHMCM&mync=E&cm_sp=s033-_-OCSTHMCM-_-E
  IBM Elastic Storage System is shipped with GNU glibc, for which a fix is available.
  The following versions are affected and it is recommended to upgrade your ESS 3000, 3200, or 5000 to the following levels:
  - for 6.0.0 – 6.0.2.3
    V6.0.2.4
    https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=Software%20defined%20storage&product=ibm/StorageSoftware/IBM+Elastic+Storage+Server+(ESS)&release=6.0.0&platform=All&function=all
  - for 6.1.0 – 6.1.2.1
    V6.1.2.2
    https://www.ibm.com/support/fixcentral/swg/selectFixes?parent=Software%20defined%20storage&product=ibm/StorageSoftware/IBM+Elastic+Storage+Server+(ESS)&release=6.1.0&platform=All&function=all

- **Vulnerability in Apache Log4j affects IBM Elastic Storage System (CVE-2021-4104)**
  See: https://www.ibm.com/support/pages/node/6565395?myns=s033&mynp=OCSTHMCM&mync=E&cm_sp=s033-_-OCSTHMCM-_-E
  A vulnerability in Apache Log4j could allow an attacker to execute arbitrary code on the system.
  The following versions are affected and it is recommended to apply the listed APAR to your 3000, 3200, or 5000:
  - for 6.0.0 – 6.0.2.4 APAR IJ38352

- for 5.3.0 – 5.3.7.4 APAR IJ38352

Keep safe and hope to see you soon,
Red, Belisama