the Availability Digest

www.availabilitydigest.com
@availabilitydig

@availabilitydig – Our April Twitter Feed of Outages

April 2018

A challenge every issue for the Availability Digest is to determine which of the many availability topics out there win coveted status as Digest articles. We always regret not focusing our attention on the topics we bypass. With our new Twitter presence, we don't have to feel guilty. This article highlights some of the @availabilitydig tweets that made headlines in recent days.

NYSE's lapses lead to first enforcement under 'Reg SCI' continuity rule

In the first case involving a rule aimed at ensuring the stability of financial market operations, three NYSE exchanges agreed to pay a fine of $14 million to settle allegations by the Securities and Exchange Commission that due to a variety of lapses from 2008 through 2016, they failed to comply with laws and regulations governing registered securities exchanges.

https://t.co/5QkMfFq6Uu

The pain of replatforming: Inside Aviva's tumultuous tech upgrade

Advisers disillusioned by ongoing issues with Aviva's replatforming project say they are reconsidering recommending the platform to clients. Aviva moved clients to its new FNZ-backed platform in January, but the project has been beset with problems; and advisers are still frustrated by not being able to carry out key jobs for their clients.

https://t.co/WLn58dRH9B

5 of the world's biggest network outages

The typical cause of a mass outage varies. According to the Ponemon Institute, the three most common causes are power supply failure (25%), cybercrime (22%), and accidental human error (22%). In this post, we look at some of the most notable network outages in recent years, what caused them, and how to be prepared in the event of a future reoccurrence.

https://t.co/82WprfSP7s

Barclays to shut off online services during weekend for maintenance work

Barclays customers were unable to manage their accounts online, by phone or by app, over parts of the Easter weekend when the bank carried out work on its systems to meet now regulations. From 11.30pm on Saturday until 3.30pm the next day, millions of people were unable to check their balances, make new payments or transfer money via the Pingit app.

https://t.co/vNOyrSkL5X

Are Clouds the New Open Systems?

ICT practitioners have used the term “open system” for a long time – at last 40 years. Yet its meaning continues to be relatively fuzzy. The whole concept of openness for computer systems has picked up a lot of baggage over the years and continues to evolve! Today, the term “cloud” is arguably just as confusing, although some experts claim it’s just IT history repeating itself. Cloud computing represents shared, service-based systems such as are provided by companies like Amazon AWS, Microsoft Azure and Google Cloud. The question is: are these clouds “open”? And the follow-up question is what is open cloud interconnection?

https://t.co/2f0ZVHqzbA

Coinbase Bug Allowed Users To Steal Unlimited ETH, Wallet Paid $10K Bounty For Discovery

Major US crypto wallet provider and exchange service Coinbase has rewarded a Dutch company with a $10,000 bounty after it discovered a smart contract glitch allowing users to steal “as much as they want” in Ethereum, according to a report made public on March 21. The issue, which VI Company reported to Coinbase December 27 of last year, revolved around exploiting a smart contract that involved a faulty wallet.

https://t.co/8c8jlUEsDT

Don’t forget to lock the door

Using a piecemeal "set and forget" approach to maintaining your DNS security puts thousands of businesses at risk of cyber-attacks every year. It is akin to closing the vault door but not checking that it has actually been locked! An alarming number of organisations are still leaving themselves wide open to cyber-crime and Distributed Denial of Service (DDoS) attacks by not prioritising domain name system (DNS) security.

https://t.co/W1SK0M5CnT

Cyberattackers strike city of Atlanta

In mid-March, the United States city of Atlanta's computer network was targeted by hackers demanding ransom, prompting an investigation by the FBI and the U.S. Department of Homeland Security. The attack caused outages to multiple internal and external applications for the city, including apps people use to pay bills and view court-related information.

https://t.co/JpZn5OKRqE

ANZ online and phone banking crash fixed after customers left in limbo

A "technical fault" that ANZ customers said left them stranded at the checkout on 22 March caused chaos for customers around Australia. Just before noon, angry customers took to social media to report they couldn't withdraw money, process payrolls or pay for groceries. An ANZ spokesman said a "technical fault" was to blame for the outage that affected internet banking, goMoney and the ANZ app.

https://t.co/KCa8J1wZi4

Why Do Legacy and Cloud Mix Well?

Scott Jeschonek, Director of Cloud Solutions at Avere Systems, thinks that although oil and water don’t mix, legacy and cloud do. Despite the hype about moving applications to the cloud and about turning legacy applications into cloud natives, he finds that legacy systems are alive and well; and he believes they aren’t going anywhere anytime soon. “Though the cloud promises the cost savings and scalability that businesses are eager to adopt, many organizations are not yet ready to let go of existing applications that required massive investments and have become essential to their workflows.”

https://t.co/tewUP1GCZ6

Software bug in server behind SingPass outages

A software bug in the server of a vendor was behind two recent SingPass outages that disrupted hundreds of essential e-government services. It was the longest disruption to SingPass since it was set up in 2003.

https://t.co/kTQYQawXIW

What to do if your cloud provider stops offering its services

The cloud is a new market that continues to grow, and there are more small players offering their services. As the market matures, it's only natural that some of these organizations will disappear or stop offering certain services. In 2013, Nirvanix stopped offering its cloud services and gave customers only two weeks’ notice to move their data off of the Nirvanix platform. What would your organization do if your cloud provider were to go out of business? What happens if your cloud provider suddenly stops offering critical services that your organization requires for its business to function properly? Businesses need to start asking these important questions and develop plans to address these scenarios.

https://t.co/v6iwz0QENZ

How 4 Companies Readied Their Infrastructure to Weather Any Storm

By plotting out technology and policy strategies, businesses establish continuity plans to prepare for any disaster.

https://t.co/jloivrKPXq

Mediacom Missouri outage caused by the ‘rarest of rare situations’

Two separate construction-related accidents caused Mediacom customers across the U.S. state of Missouri to be without Internet and voice service in mid-March. In the first incident, a construction crew of unspecified origin working in northwest Missouri accidentally severed a buried Mediacom fiber conduit. Network traffic was supposed to be rerouted through an aerial backup rented from another unspecified cable company. But the connection to the backup was taken down by a “dump truck or heavy vehicle” in a different area of the state.

https://t.co/kp74g4dv3T

Dozens of Aussie banks go down after supplier outage

As many as 27 smaller Australian banks and credit unions were offline for much of a mid-March weekend after a network outage left their supplier scrambling to restore services. The affected banks are all customers of Data Action, an Australian banking and IT solutions provider. Services appeared to first fall over early on a Saturday morning, when many of the banks took to social media to advise customers of an "unexpected issue" with online and mobile banking and their websites. The issues stretched into Saturday night and early Sunday morning. Systems were restored at around 7am AEDT. Data Action's own website was similarly offline for the same period. Many of the banks blamed either Data Action or Telstra for the problems, advising their customers that the issues were national and not isolated to the individual bank. However, later in the day Telstra clarified that the problems did not stem from a Telstra outage but rather a network problem within Data Action's infrastructure.

https://t.co/Sem6IRQ6EG

Astronauts on the space station are getting a new friend: A floating, talking robotic head that follows them around

When German astronaut and scientist Alexander Gerst rockets to the International Space Station in June, he'll bring along an unusual friend: a flying, talking, intelligent robot. Called the Crew Interactive Mobile Companion, or CIMON, the orb-shaped device weighs about 11 pounds and displays an expressive digital face. CIMON will use IBM Watson software to interact with astronauts. It will be the first [artificial intelligence]-based mission and flight assistance system.

https://t.co/1Q2lf5w2qj

3 years after data breach, OPM still struggling to modernize IT

The massive data breach the U.S. government's Office of Personnel Management suffered in 2015 was due in part because of old technology systems and software. One of OPM's first actions to clean up the breach was to accelerate its efforts to modernize its aging technology infrastructure. Nearly three years later and tens of millions of dollars spent, OPM's efforts to bring its software and hardware into the modern era continue to struggle.

https://t.co/yLu3VCFiLd

Level 3 technician's misstep causes largest outage ever reported

On Oct. 4, 2016, phone service on Level 3's network was blocked for nearly an hour and a half across the nation. Level 3 shortly thereafter copped to "a configuration error" but said little more publicly. The company got more specific with its customers, revealing a Level 3 technician made a clerical error. The specific mechanism has just been made public by the Federal Communications Commission.

https://t.co/jTca0j0Usq

Availability Digest Oldie but Goodie: "Backup Is More Than Backing Up"

If your company's survival depends upon its data (as many do), proper backup/restore procedures are a matter of corporate life or death. This requires not only that the backup strategy support the required RPO but that all backup and restore procedures be documented, tested, and audited.

https://t.co/gQikYFeg7X

Rebuilding Puerto Rico's Power Grid: The Inside Story

The restoration of Puerto Rico's power grid is a timely object lesson on the vulnerabilities of modern electrical networks and on the emerging technological options for minimizing those vulnerabilities. Power experts are now not just repairing Puerto Rico's grid but doing so with an eye toward a future that portends storms of increasing intensity and frequency. Grid operators around the world are considering the merits of microgrids, utility-scale energy storage, and distributed and renewable generation. But for Puerto Rican officials trying to rebuild their shattered electrical infrastructure, these possibilities are of much more than abstract interest.

https://t.co/fqlhuxFX6J

The State of Oregon’s New Phone System Doesn’t Work—And It’s Beginning to Echo Previous Tech Fiascos

The state of Oregon has spent $46 million on a new phone system for more than 30,000 state employees in 400 offices. It doesn't work. Non-working phones have been a regular complaint at many state agencies over the past two years, although the trouble-plagued system has until now received little public attention. But on January 26th, the state issued a formal notice of default to IBM, the contractor that built and installed that new phone system.

https://t.co/BPs1i7lUO3

Scientists say power utilities need to adapt to climate change, wilder weather

The increasing intensity of storms that lead to massive power outages highlights the need for Canada’s electrical utilities to be more robust and innovative, climate change scientists say.

https://t.co/dk1Gc6ou8n

How a Mysterious Case of ‘Missing Energy’ Caused Europe’s Clocks to Run 6 Minutes Slow

Europe’s integrated electricity network is getting back on track after a bizarre and unprecedented episode that caused clocks across the region to run at a delay of around six minutes. Continental Europe boasts the world’s largest synchronous electricity grid--energy flows freely across the borders of 25 countries at a fixed frequency of 50 Hz that is maintained by close coordination between the region’s power companies. Maintaining the grid’s frequency is extremely important. If it were to drop below 47.6 Hz or go above 52.5 Hz, the whole grid will automatically shut down along with everything connected to it. However, much smaller deviations can also have an effect. What happened here is that from mid-January until early March, energy was “going missing” from the huge, interconnected system--by a tiny margin, more energy was being consumed than was being produced, leading the average frequency over that period to be 49.996 Hz rather than 50 Hz.

https://t.co/Zrpwz06uXp

How do you service a computer server? Send in the robots, Amazon patent says

Does something need checking out in your data center? Before you send out a technician, why not send out a robot? That’s the upshot of a newly published Amazon patent for mobile robots that are designed to respond to the report of a glitch, check out the computer server that may be having an issue, hook into it if necessary, and gather data for a fix. The system, described in an application that was filed back in 2014, even calls for having the machine use its robotic manipulator to pull out a suspect part and install a replacement if need be.

https://t.co/fhIeXX5MfC

Operation Bayonet: Inside the Sting That Hijacked an Entire Dark Web Drug Market

For anyone who has watched the last few years of cat-and-mouse games on the dark web's black markets, the pattern is familiar. A contraband bazaar like the Silk Road attracts thousands of drug dealers and their customers along with intense scrutiny from police and three-letter agencies. Authorities hunt down its administrators and tear the site offline in a dramatic takedown—only to find that its buyers and sellers have simply migrated to the next dark-web market on their list. So when Dutch police got onto the trail of the popular dark-web marketplace Hansa in the fall of 2016, they decided on a different approach: Not a mere takedown, but a takeover.

https://t.co/X5l4ZpbHoQ

Amazon’s Alexa emits creepy, unprompted laughs. Now the company is stepping in with a fix

Amazon has a fix in to repair its Echo devices, which is outfitted with the Amazon AI Alexa.
Alexa, much to the chagrin of consumers, is apparently laughing at inappropriate times and reportedly in menacing-sounding ways on occasion.

https://t.co/lcxu7Gj2zW

Hundreds stranded at Sydney Airport after technical failure

Hundreds were left stranded at Sydney Airport after a technical issue caused flight delays before dawn on a Friday in early March. The airport a statement about six am, blaming 'technical issues' at T1 and T2, which were causing interruptions to passenger processing and delays.

https://t.co/65CITMAoLS

Every Oculus Rift VR headset bricked due to expired certificate

If you're had trouble with your Oculus Rift in March, you were not alone not alone. Many users received error messages saying, "Can't Reach Oculus Runtime Service.” Because Oculus failed to renew this certificate, the Oculus Runtime Service was being viewed as invalid.

https://t.co/EAnqZF1yWi

123 Reg backup cockup wipes out users' websites since August last year

In March, webhost 123 Reg suffered something of an issue that caused it to replace some users' websites with backups dating back to August 2017. Other website owners complained that their sites had been taken offline completely. Changes made since August appeared to have been lost forever. Unsurprisingly, customers were more than a little irked. At the time, 123 Reg did not give much information about what happened, simply referring to a "hardware failure" that affected a "small number of customers.” As well as irritating customers by wiping out their websites, 123 Reg caused frustration by failing to communicate effectively. The company's service status page made reference to a problem affecting some sites, but there is no reference to the backup SNAFU.

https://t.co/yqtaayyMLL

Amazon Web Services power outage took hundreds of sites offline

Earlier this year, an Amazon datacentre power outage affected scores of online services, including GitHub and Slack. The incident occurred almost exactly a year after a similar failure in the same region of Amazon's cloud. Service was quickly restored. The unplanned downtime affected

Amazon's US-East-1 region. The service hosts thousands of web services for consumers on the U.S. East Coast, so prolonged outages had a knock-on impact across the Internet.

https://t.co/D4XcARr73J

GDPR And Tape: The Elephant in The Room Is Ransomware

It's Monday, and your manager asks you to delete someone's personal data from your backup copies because the data protection officer received an email asking the company to follow the "right to be forgotten." So you grab a coffee and start figuring out where to find the data—but how can you delete a single file in a tape? You can't. You'll need to wipe the entire tape. Should you restore everything? Delete the personal information and backup the remaining data again? Sounds complex. Now imagine that this happens many times per day because of this new regulation—the GDPR. Kind of scary, right?

https://t.co/DFTc7ttdPo

Why is tape declining in the backup world?

Multiple data points show a steady decline in the use of tape for backup and recovery purposes, but why is that? There are a lot of reasons, many of which are justified and some of which are not.

https://t.co/MkDmGIGemS

Availability Digest Oldie but Goodie: Data Deduplication

Data deduplication is a technology that can reduce disk storage-capacity requirements and replication bandwidth requirements by a factor of 20:1. This is certainly a very powerful marketing statement, and it is generally accurate. However, data deduplication comes with a lot of ifs, ands, and buts. In this article, we explore what data deduplication is and its many strengths, along with some caveats.

https://t.co/TLf8PY4stF

Eliminating storage failures in the cloud

Cloud vendors make much of storage redundancy, but it takes more than multiple copies to protect data. Storage needs a reliable way to recover from corruption or loss - and current methods aren't reliable. Here's how to harden cloud storage.

https://t.co/RaIIsND8pc

Hackers exploiting memory cache for massive denial-of-service attacks

Multiple security companies are reporting on a new type of distributed denial-of-service attack that exploits unprotected servers to launch massive attacks against organizations. The servers use Memcached, a popular open source distributed memory caching system. It's used in turn to speed up dynamic database-driven websites by caching data and objects in temporary memory to reduce the number of times an external data source must be read when delivering a webpage. Those behind the attacks have worked out a way to exploit a setup issue with the UDP protocol in some Memcached installations to cause Memcached to respond with data packets thousands of times bigger than a usual request. That multiplies the volume of data in the given DDoS attack, sort of like giving a megaphone to a mouse.

https://t.co/gAZN4LDI5p

Another massive DDoS internet blackout could be coming your way

A massive internet blackout similar to the Dyn DNS outage in 2016 could easily happen again, despite relatively low-cost countermeasures. The growing legion of insecure IoT devices--insecure out of the box, and often unpatchable--means that the next DDoS attack on the domain name system could be much more severe. The centralization of DNS providers is largely to blame.

https://t.co/F8N6rsvQGw

Spaceborne computer set to teraFLOP its way across the Solar System

HPE recently posted an update about their super space computer on their website. The Spaceborne computer is supposedly running like a dream and has even achieved one teraFLOP status, meaning that it can calculate over one trillion calculations per second. The goal is to operate seamlessly in the harsh conditions of space for one year, which is roughly the amount of time it will take to travel to Mars.

https://t.co/RBKqHS87C9

Pushed to The Edge

Computing, which always includes storage and networking, evolves. Just like everything else on Earth. Anything with a benefit in efficiency will always find its niche, and it will change to plug into new niches as they arise and make use of ever-cheaper technologies as they advance from the edges. It is with this in mind that we ponder the datacenter.

https://t.co/orjJ8Qy8K7

Serious quantum computers are finally here. What are we going to do with them?

Quantum computers promise to run calculations far beyond the reach of any conventional supercomputer. They might revolutionize the discovery of new materials by making it possible to simulate the behavior of matter down to the atomic level. Or they could upend cryptography and security by cracking otherwise invincible codes. There is even hope they will supercharge artificial intelligence by crunching through data more efficiently. Yet only now, after decades of gradual progress, are researchers finally close to building quantum computers powerful enough to do things that conventional computers cannot.

https://t.co/nZZoJLSzCW

What's old is new again: Why the mainframe thrives

Sure, the mainframe platform has more than 50 years of history. Sure, the first mainframes were designed to serve Cold War clients like the Department of Defense. And yes, the mainframe was the number-crunching system that helped propel John Glenn into orbit (as shown in the recent hit film, *Hidden Figures*). But, this is a system of unequaled staying power that has adapted and evolved incredibly well to serve a very different world and economy. Mobile transactions comprised 50 percent of U.S. digital commerce revenue by the end of last year, and the vast majority of these ballooning transaction volumes rely on the serious computing muscle of mainframes.

https://t.co/HNp3tCGChF

Last of the mainframers: Big Iron's Big Crisis

Modern mainframes are unrecognizable from the ones seen in those early days of the technology. The IBM z14, which Big Blue shipped to Australia in October, has up to 32 terabytes of memory and boasts the world's fastest microprocessor, according to its maker, at 5.2GHz. But the people that work with the machines are very much the same. While mainframes look set to run core processes within Australia's biggest businesses for many years to come, the staff that keep them running are about to retire. A skills crisis, feared for a decade or more, is now beginning to bite. And hard.

https://t.co/Lv83dG3xd6

Read Gravic's new website section on HPE Shadowbase use case solutions for finance. Industrial, healthcare and telco enterprises on a variety of platforms and databases.

Case studies include topics on application integration, asymmetric capacity expansion, and big data.

https://t.co/0xrSvogTGd

IBM uncovers phishing campaign that has stolen millions from Fortune 500 companies

Security researchers at IBM's X-Force Incident Response and Intelligence Services (IRIS) have discovered an incredibly sophisticated phishing campaign that has managed to make off with millions of dollars from companies around the world. The phishing campaign appears (based on IP addresses) to be based in Nigeria and has been using a technique known as business email compromise (BEC) to accomplish the bulk of its work. What's even more frightening about this BEC campaign is that it hasn't involved any malware or hacker intrusions into networks: just social engineering, phishing, fake login pages, and shell corporations to receive stolen money.

https://t.co/9fqLJdsbe7

Lack of funding exposes US federal agencies to high data breach risks

US federal agencies suffer the highest volume of data breaches out of government agencies worldwide, and budgets are part of the problem, new research suggests. The 2018 Thales Data Threat Report, Federal Edition, suggests that US federal agencies are experiencing a rise in data breaches not only from past years but are also reporting higher rates in comparison to non-US government counterparts.

https://t.co/Wehz1a475t

Google discloses 'high-severity' exploit in Windows 10 before it's patched

Google's Project Zero team of security researchers disclosed a "high-severity" vulnerability it found in Microsoft's Edge browser after the company failed to patch it within the allotted time of 90 days. The vulnerability can allow an attacker to gain administrator privileges if exploited. For those unfamiliar, Project Zero is a team of security analysts employed by Google to find zero-day vulnerabilities before they are found and exploited by malicious people. On finding and disclosing the vulnerability to the relevant company, Google gives them 90 days to fix the issue. However, if the company fails to issue a patch within the specified time period, the Project Zero team discloses the vulnerability to the public so that users can protect themselves by taking necessary steps.

https://t.co/erip0gr822

Quantum-as-a-Service not as crazy as it sounds

A fully-tolerant quantum computer complete with in-built error checking is a good few years off.

But given the speed at which we have progressed from the days when computers filled huge rooms and when “bugs” were actual bugs in the machinery, it may only be a dozen years until we can access the new generation of computing power. This will help us to solve those exponentially-based problems that are an intrinsic part of the natural world. We already have a decent infrastructure in the form of the Internet, and classical computing power (including breakthroughs in machine learning techniques) is robust enough to act as the interface between the frankly strange quantum universe and the way we all live and do business today.

https://t.co/7vXv77rHap

Navy looks to harden legacy software

A Government Accounting Office report released in May 2016 found that U.S. federal agencies rely far too heavily on legacy computing systems and software for critical missions, including a Defense Department's nuclear command and control system that was still using floppy disks from the 1970s. Replacing such systems is a top priority government-wide, but the Office of Naval Research is also exploring a different approach.

https://t.co/HnMeTWHXH1

Head in three clouds: ANAO finds ATO contracts missing service commitments

The Australian Taxation Office (ATO) has once again found itself the centre of an investigation, following a tumultuous 18 months of IT-related incidents and systems outages plaguing the agency. While probes into its physical equipment have previously been the focus, the Australian National Audit Office (ANAO) on Tuesday called out the taxation office for lacking on the service commitment front, particularly where cloud is concerned, noting a year-old agreement with Amazon Web Services (AWS) does not include service level provisions.

https://t.co/tokgzF8416

Using end of life software – what are the risks?

When software becomes End of Life (EOL), it can be tempting to delay the decision to find an alternative. And while you might be comfortable with no additional features being developed for your software, it pays to fully understand the dangers involved in using End of Life software. Associated risks include: security vulnerabilities, spiraling costs, software incompatibility, compliance issues, poor performance, and downtime.

https://t.co/zbbhHXSPdh

Availability Digest Oldie but Goodie: Avoiding "Notworks"

Network faults can cause problems in both active/active and active/backup configurations. In both scenarios, an available network is required if users are to be moved from an inoperative node or system to a functional one. If the network should fail and then a node in an active/active system or the active system in an active/backup pair should fail, users cannot be reconnected to an operating node or system to continue their service. A network that doesn’t work is a “notwork.”

https://t.co/Wp8gCU8OKn