the Availability Digest

www.availabilitydigest.com
@availabilitydig

@availabilitydig – Our December Twitter Feed of Outages

December 2017

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.

Computer glitch giving American Airlines pilots Xmas holiday at once jeopardises thousands of flights

Thousands of American Airlines' flights over the Christmas period have no pilots assigned to them after a computer glitch gave time off to too many cockpit crew. The union for the pilots says that possibly as many as 15,000 flights between 17 and 31 December will not have adequate crew numbers.

https://t.co/bMZkO8nj5K

Obsolete, outdated software puts Victorian hospitals and police at risk of cyber attacks

Outdated computer systems are putting Victoria's (Australian state) most critical services (including hospitals, police and child protection) at risk of cyber hackers and fraudsters. The obsolete IT systems leave the state exposed to a disastrous hardware crash and computer virus attacks, the Victorian Auditor-General's Office says. Audits also found that systems for criminal justice services, marine safety and bushfire management are operating without key back-up capabilities

https://t.co/qUx56kqqr4

Human error causes Australian Broadcasting Corporation breach

Ukranian cybersecurity firm Kromtech discovered an unsecured cache of files related to the commercial operations of the Australian Broadcasting Corporation, stored with Amazon Web Services' S3 'buckets'. The contents allegedly included several thousand emails, customer logins and passwords, requests for licensed content, and 1,800 daily database backups made since 2015. The misconfigured repositories were left publicly visible, only discovered during a routine check.

https://t.co/9nmjrsLh0Q

Top-secret spy data exposed on misconfigured Amazon cloud instance

Top-secret data belonging to the United States Army Intelligence and Security Command, a joint U.S. Army and National Security Agency Defense Department command that gathers intelligence data, has been found exposed and open to the public. It was yet another case of a misconfigured Amazon Web Services S3 storage instance and included more than 100 gigabytes of data.

https://t.co/3l2SZrFrlc

TalkTalk customers left without broadband after major 'outage'

Thousands of Talk Talk customers were left without broadband in November after the internet giant suffered a "major outage." Users in London, Birmingham, Manchester and Glasgow appeared to be the worst affected, although problems also were reported elsewhere in the UK.

https://t.co/fzRKuKB9l4

Apple rushes to fix major password bug

A flaw in a recent version of MacOS High Sierra made it possible to gain entry to the machine without a password and also to have access to powerful administrator rights. The bug was discovered by Turkish developer Lemi Ergin. He found that by entering the username "root," leaving the password field blank, and hitting "enter" a few times, he was granted unrestricted access to the target machine.

https://t.co/UlZBkLPMnX

New IBM platform turns your data center into a cloud

What if you could flip a switch and turn your stodgy old data center full of legacy apps into a cloud-enabled one capable of migrating apps and data to the public cloud with ease by containerizing your legacy apps? IBM says it has just such an offering in IBM Cloud Private, a platform focused on assisting private data centers looking for a relatively simple way to move into the cloud.

https://t.co/DUZ42qrLxK

How a Tiny Error Caused Internet Outages Across the US

A year ago. a DDoS attack caused internet outages around the US by targeting the internet-infrastructure company Dyn, which provides Domain Name System services to look up web servers. Recently, the US saw yet another nationwide series of outages but with a more pedestrian cause: a misconfiguration at Level 3, an internet backbone company and enterprise ISP that underpins other big networks. Network analysts say the misconfiguration was a routing issue that created a ripple effect, causing problems for companies like Comcast, Spectrum, Verizon, Cox, and RCN.

https://t.co/v3qVNPNIws

Google Cloud Spanner update includes SLA that promises less than five minutes of downtime per

Cloud Spanner, Google's globally distributed cloud database, got an update that includes multi-region support, meaning the database can be replicated across regions for lower latency and better performance. It also got an updated Service Level Agreement (SLA) that should please customers. The latter states Cloud Spanner databases will have 99.999% (five nines) availability, a level of downtime that translates into less than five minutes per year

https://t.co/yx5G4wV4ag

Report finds millions of insecure devices in European cities

Millions of unsecured smart-home gadgets are vulnerable to attack in European cities, according to a recent report from computer security company Trend Micro. Berlin has more than 2.8 million vulnerable devices, the largest number in a European city. London is a close second, with more than 2.5 million devices that could be attacked.

https://t.co/rD3kUBZQUp

Why the mainframe is still going strong

Mainframe technology has played a crucial role in the business world for decades. Yet as computing technology has become more mobile over the years, many have predicted its downfall. Despite these gloomy predictions, it still appears to be going strong. Indeed, mainframe technology has evolved greatly in the five decades since it first appeared; and many organisations, including 70% of Fortune 500 businesses, are still using mainframe systems to power core business operations.

https://t.co/HP7CzzQC9V

OVH to Disassemble Container Data Centers after Epic Outage in Europe

OVH, the quickly growing French cloud provider that's been aggressively going after US market share of giants like Amazon and Microsoft, is planning to shut down and disassemble two of the three data centers on its campus in Strasbourg, France, following a power outage that brought down the entire campus in November. The outage lasted throughout the day and well into the evening and caused prolonged disruption to customer applications.

https://t.co/AMO7mrcPqM

"Hacking the Lights Out"

It recently was reported that North Korea is exploring ways to penetrate the U.S. electrical grid – most likely to position the country to launch a preemptive or retaliatory cyber-attack. An article available at www.securityinfowatch.com/12374400 describes a spear phishing attack that used fake fundraiser invitations containing malware. The story suggests that this was the first such attempt by the North Koreans, although this technique has been used previously by Russian hackers. As a refresher, *spear phishing* is the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.

https://t.co/656SHEKYGQ

Space missions that dodged disaster

A tiny problem can have huge consequences for a space mission. Sometimes a huge endeavor hinges on the smallest detail — three seconds' worth of fuel, an engineer's stubbornness, a speck of paint, or a 1.3-millimeter calibration. When surprise glitches revealed themselves after launch, it took massive efforts to save the missions that gave us a closer look at Mercury, a tour of the outer solar system, our only glimpse of Titan's surface, and an incredible view of the early universe. But even with hundreds of people putting in months of work, a few of these missions only succeeded by a razor-thin margin.

https://t.co/iBrNsRAIzV

Snapchat had an outage yesterday, and the grown-up Internet didn't notice:

Snapchat was down for four hours on a Monday in November, apparently preventing users from signing into the app. The outage, which began at around 3:30 p.m., prompted teens and junior millennials to express their panicked chagrin on Twitter. Gen X was conspicuously absent from the brouhaha. It seems that everyone else—i.e., grownups—only found out about the outage from news reports the day after it happened, another brutal reminder that we drift further and further from the digital vogue as we age.

https://t.co/AbhRymaVOR

Google’s Halloween lock-out caused by false positive

Who is in charge of files created and stored on Google Docs and Drive? Most people assume it’s the user or team sharing them. But an incident affecting these services on Halloween reminded everyone that there is always a super user with absolute power sitting above this – Google itself.
On that particular day, some Docs users started finding themselves blocked from opening or editing specific documents. Many reported seeing the following message: *This item has been flagged as inappropriate and can no longer be shared.* Except the files were wholly innocent of the charge, something that was quickly pointed out to Google using the preferred medium of modern complaint, Twitter. A few hours later, access to the files was restored. All back to normal? Not exactly.

https://t.co/oP2hiivxiz

'$300m in cryptocurrency' accidentally lost forever due to bug

More than $300m of cryptocurrency was lost after a series of bugs in a popular digital wallet service led one curious developer to accidentally take control of and then lock up the funds, according to reports. Unlike most cryptocurrency hacks, however, the money wasn’t deliberately taken: it was effectively destroyed by accident.

https://t.co/M7BKOybetR

Comcast's nationwide outage was caused by a configuration error

In early November, folks across the U.S. reported that Comcast Internet services were down -- an unusually large outage that lasted around 90 minutes. It turns out that the problem was caused by Level 3, an enterprise ISP that provides the backbone for other internet providers like Verizon, Comcast and RCN. The outage shows yet again just how vulnerable the Internet is.

https://t.co/QmkBP6lMGg

IT infrastructure failing as if the past two decades never happened

In Greek mythology, King Sisyphus was an arrogant ruler who believed he was smarter than Zeus. As punishment for his hubris, Sisyphus was tasked with pushing a boulder up a hill in the underworld, only to have it spin out of his control and roll back down. Based on recent data centre downtime events, we can only describe the process of keeping IT infrastructure running as Sisyphean. Data centre owners and operators repeatedly watch as the boulder slips from their grasp and back down the hill.

https://t.co/ckN93apBtM

Loss of Hewlett-Packard Archive a Wake-Up Call for Computer Historians

Some 100 boxes of correspondence, speeches, and other documents created by William Hewlett and David Packard as they built the company considered to be the grandfather of what we think of as Silicon Valley were burned to ash by the recent Sonoma County fires.

https://t.co/hVHRSh3R7K

The big opportunities in serverless computing

Serverless computing is a type of cloud service where the hosting provider allocates adequate resources for you on the fly rather than making you pay for dedicated servers or capacity in advance. It's a major technological breakthrough, and we expect to see a significant inflection point soon in this nascent market.

http://bit.ly/2yHpkDo

A new Dummies book: Beginners Guide to Hyperconverged Infrastructure

Powerful IT doesn't have to be complicated. Hyperconvergence puts your entire virtualized infrastructure and advanced data services into one integrated powerhouse. This easy-to-understand guide will help you a) understand the basic tenets of hyperconvergence and the software-defined data center and b) solve for common virtualization roadblocks.

https://t.co/NApDyUXDv0

The incredible shrinking operating system: Containers and serverless computing are changing the cloud

For years, Microsoft and Linux vendors have fought for control of the operating system, this basic and lucrative part of "the stack." But as cloud computing evolves, we're starting to see other parts of the stack take on greater prominence. Containers — which allow applications to run independently of the operating system — were the spark for this evolution; and the growing importance of container orchestration software means that a certain amount of the resource management once done by the operating system can now be handled in other places.

https://t.co/RHEYVuJZDd

What Are Azure Availability Zones?

An Azure region is made up of several data centers. Each data center, or group of data centers, has its own resources such as power and networking. Each set of independent data centers, or group of data centers, that does not share resources with others is called an availability zone.

https://t.co/e0AGqDqRRC

Time to Update Your Vacuum Cleaner -- Hack Turns LG Robot Hoover Into A Spy

Got a robot hoover buzzing around your home? It's time to take a look at its security, especially if it's an LG device. Researchers from Israeli firm Check Point reported a hack of the LG SmartThinQ app that allowed them to remotely take control of the manufacturer's hoover and use the video feed to spy on anything in the device's vicinity. And, the researchers said, the attack could also compromise refrigerators, ovens, dishwashers, washing machines, dryers and air conditioners -- any connected thing controlled by the LG app.

https://t.co/CaRYBBPwCD

Dell web address grabbed by a third party for a month

A web address used by Dell to help customers restore their data was taken over by a third party for a month last summer. The backup and recovery program installed on Dell computers periodically checks a web address called DellBackupandRecoveryCloudStorage.com. A software backup and imaging company called SoftThinks, one of Dell's partners, previously had control of this address but it appears it forgot to renew the domain in mid-June.

https://t.co/VgVEKbB9hE

1% downtime is too high for compliance: The benefits of continuous availability in access control

Continuous availability solutions can deliver 99.999% uptime – equivalent to just five minutes of downtime per year. Continuous availability means that no single point of failure can stop a security software platform from running. And unlike high availability, back-up and clustering solutions, there is no failover or reboot required and therefore minimal downtime. In a business environment where non-compliance can have serious consequences, adding a continuous availability solution to support an existing or new access control system would seem to be one of the easiest decisions to make.

https://t.co/4PeyR3BNvX

Blockchain Takes Away a Cybercriminal's Greatest Edge

Centralized architectures—which account for most of today's Internet services—concentrate data, hardware, and other vital resources in a small number of physical and virtual servers. This structure burdens Amazon, Google, Microsoft, and other large public cloud companies hosting large numbers of critical websites and services with the heavy responsibility of securing all of these resources and keeping them running in the face of an ever-evolving threat landscape. Many experts and organizations believe that decentralizing vital services will make them more resilient against cyberattacks. Blockchain, the decentralized technology that ushered in the era of cryptocurrencies, has already begun to re-shape the digital landscape.

https://t.co/n8CoBJNRF5

Airline system glitches - is the chaos avoidable through better testing & QA?

To say the airline industry is beleaguered is putting it mildly. If it isn't Ryanair and its cancellation of thousands of flights or Monarch going into administration, it's an airline or airport tech issue hitting the headlines on almost a weekly basis. And the cause of most of these tech disasters? Almost all of them can be put down to undetected software bugs and inadequate testing and quality assurance (QA). If not tested properly, bugs can slip through the net and go into production, causing all manner of problems. Even the BA IT worker who took out the wrong plug – this was a failure in the QA process and methodology that should be part and parcel of testing strategy.

https://t.co/rlubIFS9xP

The ridiculously fast Marea transatlantic Internet cable is complete

Microsoft and Facebook may not be as cool as SpongeBob, but they do now have a mighty under-the-sea cable that is almost as impressive as a pineapple. The two companies have completed their Marea subsea cable, a groundbreaking – or should that be seabreaking? – infrastructure project that will funnel vast quantities of high-speed data more than 17,000 feet under the Atlantic Ocean.

https://t.co/bNUO1LgoiX

When system downtime simply isn't an option, Stratus ftServer is the answer

When superb processing performance is vital, and there is limited or no on-site IT support available, choose Stratus ftServer: the world's first, simple 'fault tolerance in a box' integrated solution. With three different models of ftServer, hardware-based fault tolerance is available to suit requirements and budget, no matter what. Each ftServer model is completely scalable and flexible, tailor-made to your own specific requirements.

https://t.co/bAU4ppQkey

Why tape is still strong

Tape storage is one of those technological hangovers from the early days of computing, associated in the minds of many with rooms full of massive mainframe cabinets. Somewhat like the mainframe, tape shows no signs of going away just yet, and ironically, could even be handed a new lease of life thanks to the burgeoning volumes of data that are being accumulated in modern data centers.

https://t.co/IEqrSDQoiF

National Electricity Grid Suffers System Collapse

The Transmission Company of Nigeria (TCN) said a total system collapse of the national electricity grid was recorded on September 28 at 8:03 p.m. It resulted in a temporary loss of electricity generation for the nation's power grid.

https://t.co/M7HCvwD5do

Gas suppression system, fire extinguisher cause outage in London college

A London college was forced to call in a team of technical cleaners after the fire suppression system in its server room unloaded inert gas and debris onto the live IT equipment, and a fire extinguisher was "accidentally deployed."

https://t.co/m4oaYAB1Bz

How New, Resilient Networks Change Data Center Design

There is a view among some data center industry insiders that, at a very basic level, software and networks will take on an even greater role when it comes to ensuring service availability. That could have significant long-term implications for how future data centers are designed and managed, with some types of site requiring less redundant power and cooling equipment.

https://t.co/WV1xrZ6gOv

"Yawn, another outage"

It's human nature to quickly become highly dependent on new innovations soon after they arrive — imagine mobile phones or the Internet were just taken away tomorrow. But we need to ensure this new wave of digital services and Internet-connected world is secure before we become fully reliant on it.

https://t.co/ghmukWMBRy

Australia headed for peak hour Internet collapse as Netflix use surges

Australia's Internet is at risk of collapse at peak hour as the public's love of Internet streaming outpaces the broadband network's capacity to handle the traffic, an expert has warned. "The network could effectively stop between 5pm to 9pm." The unprecedented uptake of high definition (HD) online streaming services, such as Netflix, put Australia in danger of a network collapse during peak time despite the nation's biggest-ever $49 billion infrastructure spend on the national broadband network (NBN).

https://t.co/OyRVn7kIN2

Availability Digest Oldie but Goodie: "Fire Suppressant's Impact on Hard Disks"

Occasional reports have surfaced in the last few years describing damage to hard-disk drives following a discharge of a gaseous fire-suppression system. Tests by major providers of these systems have confirmed that such damage can occur and that it is related to extreme noise generated during such a discharge. However, the noise specifically due to the discharge of gas is not the primary culprit. The biggest effect on disk drives is caused by the fire alarms that accompany the discharge. There are reasonably simple steps that a data center can take to minimize this damage.

https://t.co/cnstOfumsH

UK National Lottery Hit by Peak-Time DDoS Attack

The UK National Lottery has confirmed a distributed denial-of-service attack (DDoS) was behind an outage that took its website and mobile application offline for more than an hour during peak time on a Saturday evening in early October. The attack ran from 6 p.m. to 7:30 p.m. The lottery closes ticket sales on Saturday evenings at 7:30 p.m., meaning users were left unable to buy last-minute tickets on the day.

https://t.co/n08QClSTpC

Microsoft Says Azure Outage Caused by Accidental Fire-Suppression Gas Release

An accidental release of fire-suppression agent into the data center environment in Europe triggered a chain of events that led to an Azure cloud outage for a group of customers on September 29. In what has become common practice for cloud providers, Microsoft said customers with redundant virtual machines deployed across multiple isolated hardware clusters would not have been affected by the outage. The Azure-specific name for this high-availability feature is "Availability Sets."

https://t.co/vLER1aZTvb

Why Wind Operators Need Predictive Analytics Right Now

Last March in northwest Iowa. was a typical late-winter day. The temperature wouldn't break the freezing mark. Snow fell off and on throughout the day. The wind blew, turning the blades of wind turbines that punctuate the region's horizon. Although things seemed normal, something remarkable was happening. Four-hundred miles away, predictive analytics software had been monitoring data from the wind turbines. As the software's data science models combed through the data, it spotted an anomaly in one wind turbine's gearbox. The data insight predicting a future gearbox failure led the owner of the turbine to perform a few hours of predictive maintenance that cost $5,000. In the end, that work saved the owner from having a more catastrophic, $250,000 problem and at least several days of downtime.

https://t.co/B8sATOnyBb

It's worse than you think. The Equifax breach shows the dystopian gap between wealth and competence in America

Former Equifax CEO Richard Smith essentially blamed a cyberattack that hit 145 million Americans on one employee who "owns the patch process" for fixing known vulnerabilities.

https://t.co/HHTrGVsDfd

How will the cloud be able to handle the emergence of IoT

Cloud computing and the Internet of Things (IoT) have spent the last several years in a sort of maximum-acceleration race where they've lapped the other players several times over and have only one another against which to measure.

https://t.co/t7iiIPwqJE

Not All Carriers are Equal When Addressing Network Outages

In an effort to stem the financial loss from an outage - not to mention the impact on angry, frustrated customers and potential PR fallout - companies have tried to enforce network safeguards. However, despite best efforts, an industry survey analysis found mobile operators suffer from an average of five network outages or degradations every year. Despite precautions that are being implemented, it has historically been a very real challenge to quickly reroute voice traffic to resolve an outage and prevent further impairment. With the heavy financial risks associated with network outages, it's becoming critical for businesses of all sizes to analyze available telecom solutions and select a carrier option that works best for your industry, company size, and customer base.

https://t.co/IkeE2y4dla

Login credentials of over 6,000 Indian government departments, businesses put up for sale on DarkNet

The login credentials and other confidential data of more than 6,000 Indian ISPs, government departments and private businesses were put up for sale on DarkNet. Seqrite Cyber Intelligence Labs and seQtree InfoServices discovered an advertisement on DarkNet allegedly selling access to the servers and database dump of an unspecified "internet registry." The researchers identified the affected agency as India's National Internet Registry - Indian Registry for Internet Names and Numbers (IRINN) - which falls under the National Internet Exchange of India (NIXI). The team said the hackers were selling the allegedly stolen data for 15 Bitcoins.

https://t.co/4VVmV9TKyx

Interesting article - "A Flaw in the Design"

Those who helped design the Internet over subsequent decades focused on the technical challenges of moving information quickly and reliably. When they thought about security, they foresaw the need to protect the network against potential intruders or military threats. However, they didn't anticipate that the Internet's own users would someday use the network to attack one another.

https://t.co/oofDYjU6ef

Oracle debuts autonomous cloud database for data warehouse workloads

Oracle Autonomous Database Cloud uses machine learning to eliminate human maintenance and error, offering self-driving, self-scaling and self-repairing database functions. The company claims performance 10 times faster than and half the cost of Amazon's RedShift system. The autonomous cloud service offers customer simpler service and instant elasticity, according to the announcement. The database comes with a 99.995% availability guarantee.

https://t.co/0POnC5qvd3

The Sky Fell in Puerto Rico. The Microgrid Argument is not Chicken Little

Hurricane Maria showed that warnings about the vulnerabilities of centralized electric grids – and the need for microgrid development — are not overstated. When the hurricane hit the U.S. territory on September 20th, it knocked out power to 100 percent of 1.57 million accounts served by the Puerto Rico Electric Power Authority (PREPA), the island's utility. This kind of scenario is exactly what microgrid proponents have described as possible anywhere when electric reliability depends almost solely on an interconnected central grid without the support of microgrids and related distributed energy. Before, the argument may have sounded hypothetical, improbable, maybe even apocalyptic. Puerto Rico made it real.

https://t.co/jXhy9PCHOz