the Availability Digest

www.availabilitydigest.com
@availabilitydig

@availabilitydig – Our April Twitter Feed of Outages

April 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.

How Utilities Are Using Blockchain to Modernize the Grid

In the U.S. state of New York, neighbors are testing their ability to sell solar energy to one another using blockchain technology. In Austria, the country's largest utility conglomerate, Wien Energie, is taking part in a blockchain trial focused on energy trading with two other utilities. Meanwhile in Germany, the power company Innogy is running a pilot to see if blockchain technology can authenticate and manage the billing process for autonomous electric-vehicle charging stations. Blockchain has grabbed the attention of the heavily regulated power industry as it braces for an energy revolution in which both utilities and consumers will produce and sell electricity.

https://t.co/ItENELBelr

Archive or backup – now that's the question!

It is easy to confuse archiving with backup – and no wonder. Both activities are broadly related to data protection, but they each serve two very different purposes. Which is why, before deciding which approach to take, your first step should be to figure out exactly what your organisation requires and why. In other words, what is the use case?

https://t.co/hd6SuUASQ3

Google and Symantec go to war over our Internet security

Google and Symantec are engaged in a war about each other's security practices, with all of us caught in the crossfire. Google believes that Symantec has been improperly issuing security certificates for tens of thousands of websites. If the search engine follows through with its threat, Chrome will soon no longer place the same level of trust in Symantec's certificates.

https://t.co/xIoyuslB3k

Amazon Web Services fixes 't2.micro instances' capacity issues affecting London data centres

Amazon Web Services (AWS) has fixed a capacity issue affecting one of its instances. The issue had prevented users from using a particular service. The capacity issue affected t2.micro instances; but the Amazon insists that its London data centres, which only opened in December 2016, are not suffering from capacity issues. According to sources who contacted *V3*, attempts to expand their usage in the EU-West-2a zone had been rebuffed due to capacity issues: "We currently do not have sufficient t2.micro capacity in the Availability Zone you requested (eu-west-2a)."

https://t.co/BfKrfuIvvY

Bringing Legacy Control to the Internet of Things

When it comes to implementing the Internet of Things concept as a means of collecting data for analysis, the manufacturing and processing industries are better suited than most others. The reason for this is that the Internet of Things requires an essential ingredient—data. And that's something the manufacturing and processing industries have always had in abundance because of their vast base of installed sensors, controllers and actuators. However, therein lies the problem.

https://t.co/dx1UJfp9se

Oracle Cloud Plugs into Smart Grid

In an ongoing effort to boost its share of the public cloud market, Oracle has rolled out a cloud service geared toward the smart grid and Internet of Things device management. The Oracle Utilities Operational Device Cloud Service announced at a recent company event looks to boost automation of smart grid infrastructure and IoT device management.

https://t.co/SeRAm6DiVX

Saks self-leaked customer data unencrypted, violating multiple rules

With so many retailers being impacted by cyber attacks, it's easy to conclude that thieves are necessary for data breaches. Not necessarily. Saks in March made clear that it can breach itself quite efficiently.

https://t.co/Kx86fqwgZ6

Disaster recovery: How is your business set up to survive an outage?

Asynchronous vs synchronous. Dark disaster recovery vs. active architecture. Active/active vs. active/passive. No setup is objectively better or worse than another. The best one for you primarily depends on your level of tolerance for what happens when the server goes down.

https://t.co/M6wVRFcnhg

Google to Symantec: We don't trust you anymore

Security teams, network administrators, and operations teams have busy days ahead. Google's Chrome development team is fed up with Symantec as a certificate authority and has announced plans to no longer trust current Symantec certificates.

https://t.co/b89TOhOBXk

World War Three, by Mistake

On June 3, 1980, at about two-thirty in the morning, computers at the National Military Command Center beneath the Pentagon, at the headquarters of the North American Air Defense Command (NORAD) deep within Cheyenne Mountain, Colorado, and at Site R, the Pentagon's alternate command post center hidden inside Raven Rock Mountain, Pennsylvania, issued an urgent warning: the Soviet Union had just launched a nuclear attack on the United States. The Soviets had recently invaded Afghanistan, and the animosity between the two superpowers was greater than at any other time since the Cuban Missile Crisis.

https://t.co/EEJH1MmJND

Backup vs. Business Continuity: Using RTO to Better Plan for Your Business

In this white paper, TechMD discusses what's at stake when it comes to not just protecting but also managing your data (hint: your business). The authors explain why it's important to think in terms of business continuity rather than simply data backup. They look at how to calculate the all-important Recovery Time Objective (RTO) and Recovery Point Objective (RPO) so that you can get what you need from your business continuity vendor.

https://t.co/8yBf6nhAdR

The End of Backup

Like insurance policies, backups are expensive; and they don't add any additional functionality. Your car doesn't go any faster because you're insured, and your production system doesn't run any better with backup. As many IT professionals have discovered too late, backups also are unreliable, a situation made even worse by the fact that bad backups typically aren't discovered until there's a need to restore. Fortunately, backup as we have known it is ending. Significant improvements in virtualization, synchronization and replication have converged to deliver production systems that incorporate point-in-time recovery and data protection as an integral component. These new data protection technologies are no longer engaged only when a system fails. Instead, they run constantly within live production systems.

https://t.co/WQkswpQHFK

NYSE glitch sends traders scrambling as ETF auctions derailed

NYSE Arca, the largest U.S. listing venue for ETFs, left traders scrambling at the end of a trading day in mid-March after a system upgrade went awry. An upgraded version of its software went live and derailed closing auctions for certain securities, a key moment at the end of the trading day.
The exchange shifted to backup methods for calculating the closing prices for most names and went back to using an old version of its software, according to an email to clients. A total of 341 symbols did not complete their closing auctions.

https://t.co/8iET646F6c

How the Sun messes with your TV, radio and internet

A sun outage is when the energy from the Sun disrupts the signal from a satellite. All satellites can be affected by sun outages, but geostationary satellites are particularly vulnerable. These satellites orbit the equator at an altitude of about 36,000 kilometres and take 24 hours to complete an orbit. That means from the ground, they appear to be stationary in the sky. Geostationary satellites provide a wide variety of services — including TV and radio broadcasts, telecommunications, and for regional and remote parts of Australia, the Internet. But when the Sun traverses the equator during an equinox, it also passes briefly behind geostationary satellites – about 10 minutes at most. But that 10 minutes is enough to degrade or completely disrupt radio and television broadcasts as well as satellite Internet.

https://t.co/I9tANLaCJo

Microsoft Probes Cause of Global Web Outage

Microsoft's massive outage in mid-March disrupted user access to Office 365, Skype, Xbox Live and other online services, in some cases for more than 16 hours. The outage, which affected large swaths of the U.S. and Europe, was the second that month of Microsoft's online services; though a disruption on March 7 only lasted about an hour. Unclear is how or if the outages were related to a simultaneous problem with Azure cloud.

https://t.co/WRDWzXnQZH

The Internet of bad things

On a Tuesday evening in late September 2016, Brian Krebs, one of the Internet's most prominent cybercrime reporters, noticed a startling surge in his blog traffic. It did not take him long to realize that he was under attack. Someone had seized control of hundreds of thousands of internet-connected devices, including home routers, video cameras, DVRs, and printers, to create a botnet, a sort of digital zombie army. Instead of performing their normal functions, these various devices, all of which were capable of transmitting data to the Internet, obeyed a command to pummel the server that hosted Krebs' blog. The assault, called a distributed denial of service, or DDoS attack, overwhelmed the server and knocked Krebs' blog off the Internet for three days.

https://t.co/HxveQtRMXA

African governments learn to block the Internet

Since 2015, about a dozen African countries have had wide-ranging Internet shutdowns, often during elections. Rights defenders say the blackouts are conducive to carrying out serious abuses.
The Internet outages also can inflict serious damage on the economies of African countries that desperately seek growth. In February 2016, amid a tight election, Ugandan authorities shut down access to Facebook and Twitter as anger swelled over delayed delivery of ballots in opposition strongholds. During the blackout, the police arrested the president's main challenger. Over $2 million was shed from the country's GDP in just five days of internet restrictions.

https://t.co/Ta0ke4eQ7P

Another 911 outage. Does any accountability exist?

AT&T Wireless customers who tried to reach 911 in the evening hours of Wednesday, March 8, were left stranded in more than a dozen major U.S. cities. Based on unconfirmed but widespread reports, the problem may have affected callers nationwide. What failed? The public may never know.

https://t.co/A6XihK8B5S

AWS Outage: Implications for Internet, Enterprise Cloud Customers

February's hours-long Amazon Web Services (AWS) outage provided a vivid illustration of how much large parts of the Internet depend on the cloud service. It also presented a puzzle for many users: because the AWS health dashboard itself depends on the cloud service, the status messages failed to indicate any signs of trouble throughout the outage.

https://t.co/kP3RSAwIXI

Jersey City neighborhood's Internet outage enters 2nd week

Residents of Jersey City's (New Jersey USA) Liberty Harbor neighborhood are on their eighth day of an Internet outage that is affecting residents of the area and some local businesses.
The outage, which began mid-March and has also affected telephone and cable television service, has Liberty Harbor residents questioning why they are forced to use a single internet provider, Gold Coast Broadband, that is tied to Liberty Harbor developer Peter Mocco.

https://t.co/GYgy6rbrkY

Availability Digest Oldie but Goodie: "Availability versus Performance"

Increased availability usually does not come for free. There are hardware approaches that increase cost, and there are software techniques that reduce performance. Because of the tremendous improvements in system performance over the years as compared to the modest improvements in system availability, it often is desirable to trade off some of these performance gains for improved availability. This is especially true for applications that are involved in the 24x7 operations of today's enterprises. The techniques for availability improvement at the expense of performance are substantially software-based. They improve the availability of a single system. However, improved single system availability translates to much higher availability for multinode systems.

https://t.co/AzPO4QlfVY

Microsoft finally fixes 'critical' Windows security flaw after patch delay

The software giant made customers wait a month before rolling out a fix for a serious Windows security flaw with public exploit code. Patch Tuesday, 14 March, saw the fix of a Windows SMB bug. The memory corruption bug could allow a remote, unauthenticated attacker to crash an affected machine.

https://t.co/gH3ywmXSNJ

This startup lets you collect and trade solar power, bypassing the grid

A new startup in Brooklyn, New York (USA) is bringing solar panels to rooftops while letting local residents buy and sell electricity among their neighbors. The project, named Brooklyn Microgrid, aims to create a peer-to-peer trading system built on blockchain, the distributed ledger technology behind Bitcoin and other cryptocurrencies. Although it boasts just 50 participants so far, the Brooklyn experiment offers the chance to bypass electricity companies and create a viable generation and storage network that functions independently even during broad power failures.

https://t.co/xWOJx55irq

Huge database leak reveals 1.37 billion email addresses and exposes illegal spam operation

A faulty backup inadvertently exposed the entire working database of notorious spam operator River City Media (RCM). In all, the database contains more than 1.37 billion email addresses. For some records, there are additional details such as names, real-world addresses, and IP addresses. It's a situation that's described as "a tangible threat to online privacy and security."

https://t.co/Pus71ag38s

Federal Agencies Hacked 31,000 Times in 2016

U.S. federal agencies faced almost 31,000 “cyber incidents” in fiscal 2016, incidents that led to “compromise of information or system functionality,” the U.S. Office of Management and Budget stated in its annual cyber security report to Congress. “Sixteen of these incidents met the threshold for a major incident, a designation that triggers a series of mandatory steps for agencies, including reporting certain information to Congress,” the report stated.

https://t.co/XlyCdNMdod

Gas Turbine Microgrids: What’s Next as They Become Smarter?

Gas turbine microgrids are growing in sophistication as microgrid controllers become more advanced. Control technology tends to accomplish such functions as islanding and frequency control. More advanced controls offer the ability to automatically leverage energy prices. They can calculate best pricing among on-site resources at any given moment or between the grid and the microgrid. The bottom line is that an advanced microgrid is ultimately a technology tailored to solve a customer problem. As a result, microgrids are rarely developed in a plug-and-play fashion. Instead, they often require a great deal of pre-installation study by an experienced and knowledgeable energy company.

https://t.co/Nu3TpcGVuk

Microsoft says Google's cloud reliability claim vs. Azure and Amazon Web Services does not compute

With March's Amazon Web Services outage still fresh in the minds of many people, Google senior vice president Diane Greene took a few moments at the Google Cloud Next conference to address the issue of reliability. "I just learned yesterday that we were recognized as having the highest availability of any cloud over the course of 2016," Greene said on stage. She paused before adding with a chuckle, "I think 2017 will be promising, too." Greene was referring to new numbers from CloudHarmony, a unit of the Gartner research firm. CloudHarmony revealed that Google Cloud had 74 minutes of "total time lost" in 2016, compared with 270 minutes for Microsoft Azure and 108 for Amazon Web Services. Microsoft responded by declaring that comparing downtime alone doesn't take into account the larger number of regions operated by Azure, which Microsoft says provides a more accurate picture of cloud reliability.

https://t.co/VO9ZASnZHX

Sneaky adware exploits Android users with precision targeting

Malware using new precision-targeted tactics to distribute adware hid on the Google Play store for two months and infected over 10,000 Android users before being removed. Called 'Skinner', the malware will display unwanted ads to users; but it does so in a way that avoids raising suspicion. Skinner is far from the first instance of malware to be discovered on the Google Play store - but this one uses sophisticated new tactics.

https://t.co/w2PEWEk0Y8

How to Survive a Cloud Meltdown

One of the biggest questions following Amazon's cloud outage in March was whether you can use the world's biggest cloud provider and still avoid downtime when the provider has a major outage – a common if infrequent occurrence. If you can, how to do it? And if there is a way to do it, why isn't everybody doing it?

https://t.co/X59MErQbbk

Microsoft outage leaves users without access to services for hours

Microsoft experienced an issue with its authentication platform across some services in early March. Users faced problems signing in or creating accounts on Xbox Live, Skype, Outlook, Hotmail, and more for a couple of hours. Microsoft's outage follows last week's AWS blackout that left a substantial part of the Internet without media to display. Both situations lasted only a couple of hours and had no significant consequences, but some speculate there might be something more behind these issues.

https://t.co/HXgPN7SK67

Recent Amazon outage highlights need for cloud automation

In early March, Amazon faced one of its largest service outages since the launch of Amazon Web Services (AWS). The list of disrupted businesses read like a dire Who's Who of the Internet, from Netflix to Pinterest to Airbnb. The cause of the AWS S3 outage appears to be a fat-finger typo by an authorized Amazon system administrator who was troubleshooting an unrelated problem. According to research from Ponemon Institute, at least 22 percent of data center outages each year are caused by human error. The fact that Amazon has not experienced many more outages like this so far is a testament to just how good their processes truly are. Apparently, though, the public cloud is not going to save us from human error.

https://t.co/P8imWiW8FU

FCC Investigating AT&T's Massive 911 Outage

Federal regulators are investigating the source of an outage that left millions of AT&T wireless customers in 14 states and the District of Columbia without access to 911 emergency services for several hours on 8 March. It took five hours to resolve.

https://t.co/pTkPuZsZsu

We can't see inside Fukushima Daiichi because all our robots keep dying

Tepco, the utility company tasked with overseeing cleanup and waste processing for the former Fukushima Daiichi nuclear plant, recently hit another snag. Reactor #2 is far more radioactive inside than previously measured, and the contamination exceeds the tolerance levels of the robotic probes that Tepco sends into the reactor to find the estimated 600 tons of fuel and debris that fill the reactor's concrete lining.

https://t.co/Q6fNBHnHn9

Security check bug sparks luggage mayhem at Israel's main airport

A technical fault with Ben Gurion Airport's automatic screening system led to delays and massive lines in early March, disrupting baggage distribution at Israel's international airport.

https://t.co/lMhvs8AX9E

The Internet was meant to resist nuclear strikes. Now it can't handle a power outage

When a cloud-storage malfunction at Amazon temporarily knocked out services, including Netflix, Slack, the Securities and Exchange Commission's website, "smart" thermostats and email servers, it demonstrated how much we've all come to depend on one company's infrastructure. It also shows how the centralization of data has made the Internet — at least the part that most of us use — more vulnerable than it was designed to be.

https://t.co/Nk1n0VXrlu

AWS blames a typo for Tuesday's outage

Amazon Web Services announced that its 28 February outage that affected major websites and apps was caused by human error. Sites including Netflix, Reddit and the Associated Press struggled for hours -- all because of a simple typo. "While we are proud of our long track record of availability with Amazon S3, we know how critical this service is to our customers, their applications and end users, and their businesses," the company wrote in an online message. "We will do everything we can to learn from this event and use it to improve our availability even further."

https://t.co/nnUvvwYTg8

Amazon and the $150 Million Typo

On Tuesday, 28 February, a typo caused part of Amazon Web Services to fail. In an online statement, Amazon described the circumstances of the disruptive typo this way: "The Amazon Simple Storage Service (S3) team was debugging an issue causing the S3 billing system to progress more slowly than expected. At 9:37AM PST, an authorized S3 team member using an established playbook executed a command which was intended to remove a small number of servers for one of the S3 subsystems that is used by the S3 billing process. "Unfortunately, one of the inputs to the command was entered incorrectly and a larger set of servers was removed than intended."

https://t.co/8eIER7uC6q

Torvalds unhappy with sloppy Unix Millennium Bug patches for Linux kernel

Along similar lines to the Y2K bug, there is a new challenge faced by Unix-like operating systems - the year 2038 problem or 'Unix Millennium Bug'. Under these operating systems, date values are stored in a signed 32-bit integer indicating the number of seconds since January 1, 1970. A problem arises with the 32-bit integer overflowing at approximately 0314 hours on January 19, 2038, causing systems to interpret the date value as December 13, 1901. Unsurprisingly, Linus Torvalds himself is keeping a very close eye on Linux kernel code changes.

https://t.co/Rfp1YcNer1

Massive Amazon cloud service outage disrupts sites

It didn't quite break the Internet, but a 4-hour outage on 28 February at Amazon's AWS cloud computing division caused headaches for hundreds of thousands of websites across the United States.

https://t.co/LzvstKq5Wu