the Availability Digest

www.availabilitydigest.com
@availabilitydig

@availabilitydig – Our March Twitter Feed of Outages

March 2016

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.

Cyberattacks beginning to affect mobile service, too, study says

Distributed Denial of Service (DDoS) attacks are beginning to show up as a cause of mobile phone outages, according to respondents of a recent survey. Fifty-four global Mobile Network Operators (MNO) were polled on their experiences with outages and service degradations. The survey found that DDoS attacks showed up for the first time in this year's report.

https://t.co/NclHGSHhmf

The Reason SpaceX Keeps Aborting Launches

In February within a four-day period, SpaceX aborted three attempts to launch the SES-9 satellite. The aborts bode ill for a company that is hoping to demonstrate a speedy and predictable pace of rocket launches in 2016. After bad weather on the first attempt, the last two failures to launch were linked to the upgraded rocket SpaceX is using. The rocket relies on "superchilled" liquid oxygen to get an extra thrust into orbit.

https://t.co/0hIIJHxhNv

The IRS Hack Was Twice as Bad as We Thought

On 26 February, for the second time in six months, the Internal Revenue Service revised its estimate of the scale of a cyber attack on its systems, announcing that a total of about 724,000 individuals may have had their personal information stolen by hackers last year. That's more than twice as many as the agency said were impacted after an investigation that concluded last August – and a whopping six times larger than the original estimate of the damage.

https://t.co/RtAhDK9KwY

Disaster Recovery-as-a-Service: A Beginner's Guide, Part 1 -- Virtualization Review

Recent events, ranging from terrorist attacks to weather emergencies, have many business and IT planners concerned about the readiness of their facilities and processes for unplanned interruptions (aka disasters). While hypervisor vendors and their paid analysts have contended that high availability trumps DR, that failover clusters eliminate the need for disaster recovery planning, more sensible counsel says otherwise. Enter Disaster Recovery as a Service (DRaaS).

https://t.co/LEutdUvnYb

IRS outage caused by back-to-back failures, not cyberattack

The computer outage that halted IRS tax return processing for more than a day resulted from not just one hardware failure but two. An electrical voltage regulator on the computer server that handles tax returns for millions of Americans started to fail on February 3rd. As a technician worked to address the problem, a backup voltage regulator also failed.

https://t.co/Bp4isHH4xb

Glitch in Hive smart thermostat sends temperatures soaring to nearly 90 degrees

While you don’t want to freeze in the winter, there’s a big difference between being toasty in your home and being roasted alive. Yet some British Gas customers who have adopted Hive smart thermostats were at the mercy of a glitch that sent temperatures soaring to nearly 90 degrees Fahrenheit.

https://t.co/UEQpeokKO1

The EU General Data Protection Regulation is now law: here is what you need to know

The EU’s General Data Protection Regulation (GDPR) has achieved final approval after a long two year process. With the final draft clearing up a few ambiguities and loose ends, many are calling it a 'milestone of the digital age.'

https://t.co/YEYcEQ7kzt

VSI OpenVMS V8.4-2 Field Test Wrap up message (a retweet from @ianopenvmsorg)

VSI is wrapping up efforts on the external field test of our latest release, with active participation from 42 testers around the world. The release, which will officially be called VSI OpenVMS V8.4-2 when it becomes generally available in late March, offers some exciting new features, including 64 core support for BL890c i4 systems, inclusion of the latest UEFI 2.3 platform firmware (modernization that was long overdue), and tunable backup compression.

https://t.co/4Rw9MshJJu

An Availability Digest Oldie But Goodie: "Critical Date Testing – Leap Day and More"

Even with everything we learned from the Y2K experience, many failures due to date and time bugs still occur. However, products are available to thoroughly test applications to ensure that they handle critical dates and times successfully. These products are by and large noninvasive and require no program modifications. They can be used to offset times for testing or to simulate multiple time zones for system consolidation.

https://t.co/jZ9gfXEvDt

Political campaigns collect tons of data, but they’re terrible at protecting it

Over the last three months, more than 100 million US voters have had their data exposed online. These data breaches weren’t caused by a sophisticated hack or malware. Instead, political campaigns' abysmal cybersecurity practices are to blame.

https://t.co/3fOs0JGfxP

This is How Leap Year Can Ruin a Developer's Life

February 29th presents a perfect trial for developers. It enforces the idea that programmers must take into account rare yet inevitable events in their application testing. How is it that this one extra day can cause so much trouble? Most systems account for a 365 day year. If anything is set up on an annual basis, it counts down from 365 and then repeats itself. But there are 366 days in a leap year. If this isn't taken into account, events might occur too early on the backend of an application – or not at all. On the front-end, users might be served inaccurate data or become locked out of a system. This is certainly not the experience for which any developer wants to be responsible.

https://t.co/lyLpZN35jv

Apple Is Fixing That 1970 Bug In The Next iOS

The 1970 bug is a slightly annoying and mostly entertaining software glitch that bricks any iPhone by setting the date back before May 1970. Unsurprisingly, Apple's correcting that glitch in the next version of iOS.

https://t.co/1dp3g9Ex4L

Join the Continuous Availability Forum on LinkedIn.

This forum provides a venue for discussion of high availability and continuously available topics, including active/active architectures, case studies, and implementation issues.

https://t.co/BjygkjAcHn

Nigerian air traffic controllers cry for radar equipment backup

The Nigeria Air Traffic Controllers Association (NATCA) has raised a red flag concerning the radar equipment that presently serves air traffic controllers in carrying out their duties. The Association has cried out that since the equipment has no backup, despite being installed 10 years ago, its failure will mean the total collapse of air traffic control services.

https://t.co/wZi4e2yj57

This is why your phone told you the Tube was closed today

Several popular London travel apps informed commuters all Tube lines were down during morning rush hour on 25 February. Transport for London (TfL) blamed a software bug for the mass confusion. The glitch meant many of the most popular travel apps for smart phones were showing all Underground lines as well as the Overground were running no services – just when millions of people were leaving the house for work at around 8am.

https://t.co/0jwcWkRQgx

The 15 worst data security breaches of the 21st Century

Data security breaches happen daily in too many places at once to keep count. But what constitutes a huge breach versus a small one? For some perspective, this article takes a look at 15 of the biggest incidents in recent memory.

https://t.co/evPNz5nNIV

When Malware Becomes a Service, Anyone Can Be a Hacker

For quite a while, online criminals have been moving to service models - DDoS attacks as a service, banking trojans as a service, and ransom trojans as a service, among others. What was once being operated behind the curtains - on Dark Web - is now being marketed publicly on popular platforms such as Facebook, Twitter, and YouTube.

https://t.co/2X5zPRLxNt

13 new sessions added to the HP-UX Boot Camp! Check them out, and register TODAY. Call for Papers is open until 3/15.

Connect's HP-UX runs from 24 – 26 April in Chicago, Illinois USA. Click link for more information.

https://t.co/IFgvixYNFT

Get connected with the HPE User community of over 70,000! Register today to become a member of CONNECT.

Select your member type: Individual (USD $0), Corporate (USD $500), HP Employee (USD $0) or Chapter Affiliate (USD $0). Click link for more information.

https://t.co/iJYHuytItH

Stratus Technologies' everRun Solution Prevents Downtime And Data Loss For Critical Physical Security Applications

Building security – especially high-security installations – requires technology that is reliable and minimizes downtime. In some physical security installations, access control and video surveillance solutions are required to function uninterruptedly to ensure business continuity and maintain data integrity. While it may not be a household name in the security industry, Stratus Technologies, a provider of "always-on" technology, helps to ensure the running of mission-critical applications.

https://t.co/9uoBPowXsS

2016: The year the branch router will RIP

2015 will likely be seen as the year when enterprises pushed aside their fears of cloud computing. Over 70% of companies now utilise cloud-based applications and services, although these companies still keep some critical systems and information stored in the data centre. The widespread adoption of this hybrid IT infrastructure model will lead to 2016 becoming the year when the branch office ends its relationship with an old friend – the router.

https://t.co/pZrcCnZjus

How to Survive the Zombie Apocalypse (and Other Disasters) with Business Continuity and Security Planning

Business interruptions come in all shapes and sizes. In today's landscape, the lack of business continuity planning not only puts companies at a competitive disadvantage, but it also can spell doom for the company as a whole. Careful consideration of disaster recovery planning in the areas of host configuration, defense, authentication and proactive monitoring will ensure the integrity of your DR systems and will effectively prepare for recovery operations while keeping security at the forefront.

https://t.co/GEkzjjabZ1

How IBM Plans To Innovate Past Moore's Law

In 1965, Intel cofounder Gordon Moore published a remarkably prescient paper. It observed that the number of transistors on an integrated circuit was doubling every two years. Moore predicted that this pace would lead to computers becoming embedded in homes, cars and communication systems. That simple idea is known today as Moore's Law. Yet the law has been fraying for years, and experts predict that it soon will reach its theoretical limits. However, Bernie Meyerson, IBM's Chief Innovation Officer, feels strongly that the end of Moore's Law doesn't mean the end of progress. Not by a long shot.

https://t.co/FmmA92qNou

How to fix the six biggest software performance issues

The legacy software problem is endemic, with nine out of ten IT decision makers being held back by systems that aren't performing up to scratch. There are many ways in which software can be underperforming, but what is important is that the signs indicating as such are noted and reacted to accordingly.

https://t.co/DodpawQ4M6

Legacy thinking, not legacy systems, is the biggest threat to the financial industry

The power of the cloud is now such that just as software is eating the world, the cloud is eating infrastructure. By virtualising the data currently locked in legacy systems, the same banks that are struggling now will be able to use their greater reach, customer numbers, and resources to leapfrog the agile new competition – to connect with them through open APIs and secure data integration.

https://t.co/6pXwdWztpr

The IRS's No Good Day

The U.S. Internal Revenue Service (IRS) had bad news for taxpayers — a "hardware failure" left the agency temporarily unable to process returns filed electronically. The agency's e-file program was just one of the systems to go down in February.

https://t.co/jvPAloYgzE

Xero back online after two-hour outage triggered by 'hardware failure'

Xero experienced its worst-ever outage following a "hardware failure" that took its accounting software service offline for about two hours at lunchtime on 24 February.

https://t.co/02tFJYmpU0

Lessons learned in business continuity planning

Many IT managers tasked with developing business continuity plans overlook or underestimate some key areas. They include: missing digital IDs, incomplete backups, too few remote user licenses, seasonality, backups that are hard to validate, weak notification systems, electronics vulnerable to "falling water," and overly optimistic testing plans.

https://t.co/qnCudEjcr5

Cellphone not working? Verizon Wireless suffers outage in New York City area

Verizon Wireless customers in the New York City area were left without data service after a network outage Wednesday morning, 24 February. A chart from downdetector.com, which tracks online service outages, showed outage reports starting as early as 6 a.m., with the most reports coming in just before 9 a.m. According to Verizon, "A hardware failure is suspected as the culprit. We're doing a full investigation."

https://t.co/JazNUkKsnA

From the Availability Digest: "Hacktivism"

Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially motivated purpose. The individual who performs an act of hacktivism is said to be a hacktivist. Hacktivists are not cybercriminals. They do not hack into computer systems to steal money or data. Rather, they hack into computer systems - typically websites - to make a statement.

https://t.co/BYxUQ1sYXB

Your infrastructure's in the cloud and the Internet goes down. Now what?

We've come to expect Internet connectivity to be available because the provision of it has become so cheap. And that expectation has led us to become reliant on it. When the Internet is down for us, many of the things we do are unavailable. This reliance on the Internet has made planning for the lack of it complicated. Many organizations are, in effect, crossing their fingers rather than planning in earnest.

https://t.co/jkvNIl637F

Avoid outages and achieve the fabled 'four nines'

The decision to aim for 100 percent uptime is not an easy one for everyone. It’s a matter of determining acceptable risk in the event of a cloud failure. Nor is it a matter of flicking a switch: it takes careful planning and consideration, accounting for the peculiarities of each company’s cloud environment. For some businesses, it may become too expensive to make everything 100 percent available all of the time; but it is important that businesses recognise what aspects of their online services must be available to ensure they run smoothly and without fault.

https://t.co/otfrl3hcc4

T-Mobile reports voice outage across LTE and Wi-Fi

T-Mobile US confirmed that it suffered a network outage during a weekend in late February. The outage appeared to affect customers' ability across the country to make voice calls over Wi-Fi and LTE. Details remain unclear on the outage, including how many customers were affected and what the reason was behind the problem. Based on some anecdotal evidence on social media, T-Mobile customers across the country could not make or receive phone calls over either their own Wi-Fi networks or over T-Mobile's LTE network, which may have been due to T-Mobile's Voice over LTE technology.

https://t.co/Ii2DZpsVLF

From the Availability Digest: "The U.S. Government's IT Fossils"

Aging federal IT systems are seen as a security risk. The U.S. government operates 28 systems that are at least 25 years old and eleven systems that are more than 35 years old. It spends USD $60 billion, 75% of its IT budget, each year to keep these systems running. Just finding the skill sets to maintain the systems is becoming increasingly difficult. Less than 25% of college computer-science programs teach old-school skills such as COBOL.

https://t.co/sksPesXWf2

Don't be duped by dedupe: Understanding data deduplication for backup

Today, new technology advances are needed to combat the unstoppable and exponential growth of virtual machines and data. There are many out there, and it's not always easy to tell which is right for your data. The article focuses on two competing dedupe technologies for backup to help shine a light on what they bring to the backup process.

https://t.co/ZMoaB5fbK7

Why Ford's CIO is shifting gears to bimodal IT

Ford's technology department has officially shifted into second gear under CIO Marcy Klevorn. The automobile maker has restructured its IT processes to incorporate technology experiments that can be hastily abandoned alongside more traditional, measured technologies and systems that fuel the company's operations. Klevorn says Ford's adoption of bimodal IT, as it is known in some tech circles, is designed to help Ford winnow out bureaucracy, making IT service delivery more efficient.

https://t.co/XUAFNq24cp

Compuware CEO: Mainframes Can Be Agile

Compuware started selling software for mainframes more than 40 years ago. After years of expanding their efforts into software for other systems, the company has refocused on software for mainframe systems. And Chris O'Malley, Compuware's chairman and CEO, says that the big opportunities are in big iron.

https://t.co/7fLELBzJ6e

Why EHR Vendors Are Next Healthcare Data Breach Target

In 2015, we witnessed numerous hospital networks and health insurers fall victim to data breaches. Now with the growing sophistication of hackers and the amount of sensitive data stored, 2016 may be the year when EHR vendors become the next major target. Why EHR? Health data hackers are moving upstream: from hospital networks or insurers who might represent patients in a particular geographic area to EHR service providers with customers all over the country.

https://t.co/ARDKAkjRfE

Lessons Learned from 2015 Healthcare Data Breaches

Last year was filled with healthcare data breaches, with the top three alone combining to impact nearly 100 million individuals. Will 2016 hold the same potential threats to covered entities? How can healthcare organizations best prepare for cybersecurity threats while still implementing the latest technologies?

https://t.co/1cbwkHYGaO

"When the Single Point of Failure Actually Fails"

“Late yesterday afternoon, our trusted Cisco 5505 stopped working. Poof. Red Status light on; activity lights on the embedded switch ports blinking; no traffic. A few reboots and a few attempted hard resets later, we are still not working. A quick call and discussion, and our Cisco guru tells us “it’s a brick.” Covered by warranty and a solid support/service plan, a new unit will arrive in several days. In the meantime, we must continue to service our customers.”

https://t.co/5lDzB8Oj6r

The 99.999 percent cybersecurity problem

Near-perfection is a lofty goal, one for which utilities strive. “Five nines” has become, it’s said, the “holy grail” of reliability. Under this scenario, customers have service 99.999 percent of the time, with outages averaging only about five minutes per year. Now, *that's* service. A major telephone company set this standard, boasting of its 99.999-percent reliability. Now some are calling for “five nines” service from Internet providers and websites.

https://t.co/aYbEXnRFMK

Netflix cloud migration targets four 9s uptime

Netflix has confirmed it has finally completed its cloud migration and has shut down the last remaining data centre bits used by its streaming service. It began the process in August 2008, when it experienced a major database corruption and for three days could not ship DVDs to its members. Netflix suggests the development moves it nearer to its desired goal of four nines of service uptime.

https://t.co/JeSDKP5l15

Cloud disaster recovery on the increase but challenges remain, says CloudEndure

While the vast majority of organisations hope for 99.9% uptime throughout the year, 57% of companies polled by CloudEndure say they had at least one outage in the past three months. The survey, which quizzed 141 IT global IT professionals, found organisations are, in general, gaining confidence in cloud disaster recovery (DR) solutions. This is noticed in the key risks to system availability. The number one risk remains human error, followed by network failures and application bugs. Downtime of cloud providers fell from the third highest risk last year to #6 in 2016.

https://t.co/DEHRaZEjIt

Legacy storage under fire from software defined startup Infinit

Infinit, a French startup, has launched its second product, a decentralized file storage platform, making it possible to aggregate storage resources across on-premise servers and the cloud into a secure, fault-tolerant, and scalable file system.

https://t.co/5ufxbCtRmv

$17,000 bitcoin ransom paid by hospital to hackers sparks outrage

The malware ransom attack on Hollywood Presbyterian Medical Center — which prompted the facility to pay a $17,000 ransom in bitcoin to the hacker who seized control of the hospital's computer systems — is part of a larger problem that is generating outrage.

https://t.co/e5W3bdYqE5

HPE Cyber Risk Report 2016: Old problems and known issues still rampant (a retweet from XYPRO Technology)

The HPE Cyber Risk Report 2016 recently was released. Unfortunately, it details a threat landscape that remains rampant with old problems and known issues. The annual report, published by HPE Security Research, offers in-depth industry data and analysis on the most pressing security issues, providing business leaders and security professionals with actionable intelligence to better protect their digital enterprises and drive fearless innovation.

https://t.co/BnME7P1U5I

Space Is Cold, Vast, and Deadly. Humans Will Explore It Anyway

“But we didn’t stay there, not all of us—over thousands of years, our ancestors walked all over the continent and then out of it. And when they came to the sea, they built boats and sailed tremendous distances to islands they could not have known were there. Why? Probably for the same reason we look up at the moon and the stars and say, “What’s up there? Could we go there? Maybe we could go there. Because it’s something human beings do.” *Ann Leckie*

https://t.co/PTAsnJ3R2s