The digest of current topics on Continuous Availability. More than Business Continuity Planning.

Follow us

BCP tells you how to *recover* from the effects of downtime.
CA tells you how to *avoid* the effects of downtime.
www.availabilitydigest.com

@availabilitydig

Technical Writing

The articles you read in the Availability Digest result from years of experience in researching and writing a variety of technical documents and marketing content. It's what we do best, and we provide our services to others who value high-quality content created by IT specialists. **Ask us** about • articles • white papers • case studies • web content • manuals • specifications • patent disclosures

Browse through our Useful Links.

See our article archive for complete articles.

Sign up for your free subscription.

Visit our Continuous Availability Forum.

Check out our seminars.

Check out our technical writing services.

In Memory of OpenVMS

HP's announcement of its end of support for OpenVMS may not come as a surprise to many, but it is shocking to us all in its finality. Further sales of OpenVMS on Integrity i2 servers will end in eighteen months (December 31, 2015) as will support for all previous versions. Integrity i2 server upgrades will be available for another year, and hardware support will continue through the end of 2020. OpenVMS then will be only a memory.

This takes me back to the early days of my data-processing career. As a research assistant at MIT, my first supervisor was Ken Olsen. Our group was working on the first transistorized computer, TX-0, for the U.S. Air Force. Ken devised a way to package transistorized logical units (gates, flip-flops, etc.) into pluggable units and went on to start Digital Equipment Corporation. He used these "flip chips" to build DEC's early range of computers.

Digital evolved into a major force in the computer industry. Its split-site clusters were arguably the ultimate in high-availability distributed architectures.

The later acquisition of DEC by Compaq and then by HP was the beginning of the end for DEC. Many of us may never find a suitable replacement.

Dr. Bill Highleyman, Managing Editor

Never Again

New York City's New 911 System Goes Down Four Times

After limping along for decades on an aging 911 Computer-Aided Dispatch (CAD) system, New York City finally commissioned a brand new, state-of-the-art 911 system. The new 911 system had undergone extensive testing, but this did not prevent it from failing four times in its first three days of operation during late May, 2013.

It seems that this project suffered from several faults. First is the question of redundancy. A 911 system is certainly a mission-critical system deserving an availability of four or five 9s (just minutes of downtime per year). Where was the redundancy that would keep the system operating during these component failures?

A major error – true for any upgrade – was in not maintaining a path to return to the original, known working system if problems occurred. There should have been a way to keep the original system operational and on standby so that 911 operators and dispatchers could return to that system and use it until the new system had undergone further testing in the areas of failure.

Fortunately, the city had the ultimate backup – manual operation. According to the city administration, no one was ever in danger of being denied care by New York City's emergency services.

--more--

Best Practices

Superstorm Sandy Survivors

Superstorm Sandy, with its high winds and severe storm surge, hit the New Jersey and New York shores and lower Manhattan with devastating force on Monday, October 29, 2012. It flooded streets, tunnels, and subway lines in New York City. It disrupted power in and around the city for weeks and cut communications when they were most needed. Sandy leveled homes, businesses, and even entire communities along the shore line.

Melissa Delaney, writing for Biztech Magazine, has published an insightful series of case studies describing how three companies in Superstorm Sandy's path weathered the disaster relatively unscathed. These companies relied on multilayered disaster recovery plans and business continuity strategies. They remained in operation even though they never anticipated the length of the outage, the disruption to power and communications, and the length that some of their facilities remained dark.

In this article, we review Delaney's case studies. They provide valuable guidance for other companies that are reviewing their business continuity plans in the light of recent disasters such as Hurricane Sandy, the Oklahoma City tornadoes, and the California wildfires.

As one executive commented, when it comes to disaster planning, "Think bigger. Mother Nature is pretty powerful."

--more--

Enterprise Availability Architectures for Business-Critical Services

Large enterprises continue to search for an approach to supporting business-critical processing with the right balance of risk and cost. Industry experience shows that companies that lose critical data-processing capabilities for an extended time may be unable to ever recover from the impact of an outage. At the other extreme, it is easy to overspend on availability to provide extra assurance of recoverability or merely to simplify the operational aspects of availability.

Architected availability and disaster recovery are undoubtedly significant aspects of the compute strategy in any large enterprise. A risk-based analysis of the requirements and potential solutions can result in differentiated implementations, resulting in significant cost savings over simple replication-centered implementations while providing better levels of support for the organization's actual needs. Understanding availability implications enables business and technical communities to define and fulfill appropriate application and infrastructure requirements. Architectural methods, including categorization of availability requirements, analysis of relevant technology and attendant costs, and planning processes and implementations, are the main steps in achieving the appropriately balanced solution.

Written by our guest author, Arvin Levine, PhD, this paper offers an approach to risk-based availability architecture and analysis.

--more--

Availability Topics

Sophos Security Threat Report 2013

Every year, Sophos Ltd., a major security firm based in the U.K., publishes a report that highlights the security threats of the past year and the threats that seem likely in the coming year. In this article, we summarize the findings of Sophos' Security Threat Report 2013.

IT security is evolving from a device-centric view to a user-centric view, bringing many new security challenges. Users are fully embracing the power to access data from anywhere. The rapid adoption of bring-your-own-devices (BYOD) is accelerating this trend and is providing new malware attack vectors.

Another trend is the transformation of endpoint devices from homogeneous Windows systems to an environment of diverse systems. Predominant among exploits of such devices is Android malware, a serious and growing menace.

The web remains the dominant source for malware. Social engineering and targeting vulnerabilities in browsers and applications represent the primary attack vectors launched from the web.

A modern security policy must focus on all areas of vulnerability – enforcement of BYOD policies, data encryption, secure access to corporate networks, content filtering, patch management, and threat and malware protection.

--more--

Sign up for your free subscription at http://www.availabilitydigest.com/signups.htm

Would You Like to Sign Up for the Free Digest by Fax?
Simply print out the following form, fill it in, and fax it to:
Availability Digest
+1 908 459 5543

Name: _____

Email Address: _____

Company: _____

Title: _____

Telephone No.: _____

Address: _____

_____

_____

_____