the Availability Digest™

Volume 7
Issue 11

--- achieving 100% uptime

November 2012

The digest of current topics on Continuous Availability. More than Business Continuity Planning.
BCP tells you how to *recover* from the effects of downtime.
CA tells you how to *avoid* the effects of downtime.

www.availabilitydigest.com

In this issue:

Browse through our Useful Links.

Check our article archive for complete articles.

Sign up for your free subscription.

Join us on our Continuous Availability Forum.

Check out our seminars.

Check out our technical writing services.

Our Presentation at the NonStop Boot Camp Gets a Rave Review

The 2012 NonStop Boot Camp, held in October in San Jose, was a great success based on all of the user feedback received at the conference and in follow-on surveys. Connect has just distributed a newsletter advertising the 2013 NonStop Boot Camp, to be held November 3-5, 2013, again in San Jose. The fifteen things that attendees liked best in the recent Boot Camp were listed, and #2 on that list was "Bill Highleyman's presentation: Excellent!!"

My talk, "Help! My Data Center is Down," related horror stories of events that disabled entire data centers not only for hours but in some cases for days. Many causes were involved – people, failed upgrades, failover faults, and network outages. Many lessons can be learned from these unfortunate experiences.

I will be giving an updated version of this talk with new Never Again stories at Discover 2013 and at the 2013 NonStop Boot Camp. Come attend, and see what you can learn from the misfortune of others.

The fundamentals behind these failures are what we cover in our seminars on "Availability Concepts and Practices." Please contact us to arrange a seminar online or at your facility. We tailor our seminars to your needs.

Dr. Bill Highleyman, Managing Editor

Case Studies

How Does Google Do It? (part 2)

Google has transformed our relationship with information. No longer do we go to the library to do our research or consult an encyclopedia. We type in a query for Google and instantly get a long list of postings on the topic that can be found on the Web.

Today, Google indexes twenty million web pages every day to support its searches. It handles three billion daily search queries. It provides free email to 425 million Gmail users.

How Google does this has been a closely guarded secret, and much of it still is. However, Google is strongly committed to green practices. It has made major inroads on energy savings in its data centers and feels that the extreme security regarding its progress in this area undercuts that commitment. So Google has now opened its doors to provide an insight into its energy-conservation practices.

Google manages its massive data-processing requirements by building large data centers that behave as a single computer. Applications are distributed across the entire server floor. Google achieves industry-leading energy efficiencies with particular attention to cooling, server design, battery backup, and other initiatives to minimize the energy overhead required to operate a major data center.

--more--

Never Again

Orca – The Outage That May Change History

The Romney campaign looked forward with confidence to the November 6, 2012, U.S. presidential election. Not only were many polls improving in its favor, but it had a secret weapon that it did not disclose until just before Election Day. Orca!

Orca was a massive, technologically sophisticated tool that was aimed at GOTV – Get Out The Vote – in the critical swing states that would decide the election outcome. In elections that are as close as this one was predicted to be, outperforming polls by a single point can mean that entire states and all their Electoral votes can be won.

But Orca failed. It never got off the ground on Election Day. Was this outage the cause of Governor Romney's loss to President Obama? We will never know the answer to this question, but it was quite likely a factor.

What would be different one hundred years from now if Governor Romney had won this election? We will never know, but certainly history would have taken a different path. And Orca would perhaps have played a role, a role that was denied it by incompetency.

--more--

Amazon Downed by Memory Leak

On Monday, October 22, 2012, Amazon Web Services (AWS) suffered a major multi-hour outage in one of the Northeastern Availability Zones. The problem began in a noncritical program that had no significant role in the ongoing operations of AWS. It was a memory leak whose impact cascaded unnoticed over several hours to critical components and finally disabled most of an entire Availability Zone.

As can be seen from the Amazon AWS outage, clouds are extremely complex. Bugs will always be lurking in their depths, but with experience they will be slowly flushed out over time and will be eradicated. Of course, new features will always add new bugs; so this will be a never-ending experience.

Amazon’s transparent approach to bug reporting is refreshing. It helps customers to know exactly what happened and what is being done to correct the problem.

Nonetheless, the complexity of clouds and the propensity of bugs as evidenced in this outage emphasize the need to have an effective and tested business continuity plan to guide you when your critical cloud-based applications suddenly become unavailable.

--more--

Best Practices

FBI Warns Employees Are New Targets

A recent joint report issued by several U.S. government agencies concerned with cybersecurity has warned that individual employees rather than companies are being more frequently targeted by cybercriminals. Prepared by the FBI (the U.S. Federal Bureau of Investigation), FS-ISAC (the Financial Services – Information Sharing and Access Center), and IC3 (the Internet Crime Complaint Center), the report notes that cybercriminals are using a variety of malware to obtain employees’ login credentials. The stolen credentials have been used, for instance, to initiate unauthorized wire transfers ranging up to USD one million dollars.

Cybercriminals are now directly targeting a company’s employees rather than going after corporate systems because law enforcement has become more successful at prosecuting cybercriminals who succeed in large attacks, and individual employee attacks garner less law-enforcement notice. Even so, the stealing of employee credentials can result in successful major assaults. This trend is aggravated by the off-the-shelf availability of powerful malware that can be used by cybercriminals to wage successful attacks with little effort.

No matter how smart we are at defending ourselves against malicious assaults, it seems that cybercriminals are always smarter. Whatever defenses we throw up are quickly thwarted by rapidly evolving malware. However, though endless, the fight must go on.

--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: ______________________________

____

____

____

The Availability Digest is published monthly. It may be distributed freely. Please pass it on to an associate.
Managing Editor - Dr. Bill Highleyman editor@availabilitydigest.com.