the Availability Digest™

Volume 7
Issue 9

--- achieving 100% uptime

September 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 Managing Editor Will Speak at the NonStop Boot Camp

The NonStop Advanced Technical Boot Camp is coming up. It will be held in San Jose, California, USA, from October 14th through October 16th. In addition to four full-day HP educational seminars, the Boot Camp features three dozen breakout sessions. There will be dozens of NonStop vendors participating in the Partner Pavilion. NonStop Boot Camp is Coming in October, an article in our August *Availability Digest*, has further details.

I will be presenting one of the breakout sessions. My talk is entitled "Help! My Data Center is Down!" Nothing strikes fear in the hearts of management so much as losing a company's entire corporate IT infrastructure. To make sure this never happens, companies invest heavily in their data centers with technologies ranging from fault-tolerant systems to redundant architectures and even redundant data centers.

However, the unexpected happens. In this presentation, I will review from the archives of the *Availability Digest* many horror stories that highlight unlikely events that have taken down entire data centers and the lessons that can be learned from such disasters. These lessons apply to any data center, including those with NonStop systems.

I look forward to seeing you at my talk.

Dr. Bill Highleyman, Managing Editor

Never Again

Go Daddy Takes Down Millions of Web Sites

At about 10 AM EDT on Monday, September 10, 2012, companies and individuals around the world (including the *Availability Digest*) began to lose their web sites and email services. Ultimately, an estimated fifteen million web sites and an untold number of email accounts suffered failure and did not recover until six hours later.

This catastrophe was caused by an outage incurred by Go Daddy. Go Daddy hosts more than five million web sites on its server farms.

The problem was with Go Daddy's DNS (Domain Name System) servers. They were largely inaccessible. With no access to its DNS servers, web sites and email domains hosted by Go Daddy could not be reached.

Several theories in the press took form during the outage, starting with a DDoS attack by Anonymous. It then appeared that an attack by an individual was the cause. However, the root cause of the outage turned out to be a failure in Go Daddy's networks connecting its DNS servers.

With all of its redundancy, the Internet is nevertheless a fragile ecosystem. Companies must have a plan for continuing their business in the absence of the Internet or be willing to face the consequences.

--more--

More Never Agains VII

Since our Never Agains VI summary was published in the April 2012 issue, catastrophes have continued to plague the IT industry. We already have reported on several – the DNS-Changer and Flame viruses, Royal Bank of Scotland's two-week outage due to a software bug, Knight Capital's disastrous high-frequency-trading algorithmic bug that literally destroyed the company, and in this issue, the Go Daddy outage that took down millions of web sites worldwide. In this article, we summarize some others that have made headlines during the last four months.

Half of the outages that we describe were caused by power failures – Amazon, Salesforce.com, Hosting.com, and half of India. Others were plagued with failover faults, either because the failover was compromised (Amazon, Twitter) or because the backup system was damaged (Calgary).

The experience of the city of Calgary shows the foolishness of depending upon a backup system that is not remote enough from its production system so as to be unaffected by an event that takes down the production system.

--more--

Availability Topics

The Malware Threat to Android

Can smart phones be infected by malware? You bet! Furthermore, studies by many security firms show that Android is the primary mobile target of hackers.

The fact that the majority of malware versions and attacks have been aimed at Android mobile devices is not surprising, as Android has become the world's leading smartphone platform. As of the beginning of 2012, Android had a 59% share of the worldwide smartphone market. As of the third quarter, there were 500 million Android devices in use; and 1.3 million were being added every day.

Android is particularly susceptible to malicious attacks because it is open source and because there is little control over the apps written by the large community of Android developers. Because Android is open source, the various manufacturers using it make their own significant modifications that often add security vulnerabilities not in the base operating system. Cyber criminals can easily add malicious software to otherwise appealing apps that exploit these vulnerabilities and provide them to users via unregulated third-party app sites.

Apple's iOS does not have these problems yet. iOS is a closed system, and Apple will only allow certified apps to be downloaded to its devices.

--more--

The Geek Corner

The Cost of RPO and RTO

The purpose of availability analysis is to determine how to limit downtime and data loss. Both cost a corporation money and reputation. But improving them also costs money. Improvement generally means adding redundancy to the corporate systems. How does one balance the cost of availability improvement against the savings of reduced downtime and lost data?

For every application, the company should set certain objectives for lost downtime and lost data. The objective for lost downtime is called the Recovery Time Objective, or RTO. The objective for lost data is called the Recovery Point Objective, or RPO.

The techniques for minimizing downtime and lost data are, in general, largely independent. Redundancy is used to minimize downtime. Data replication is use to minimize lost data. Downtime is minimized by providing geographically dispersed redundant servers and storage. Lost data is minimized by maintaining a copy of the data at a safe site

In this article, we look at relationships between costs and savings; and we generate some rules of thumb for arriving at the best compromise. The analysis is the same for both RPO and RTO. Therefore, we focus on RPO as an example.

--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