the Availability Digest™
--- achieving 100% uptime
Volume 10
Issue 9
September 2015

The digest of 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

Follow us
@availabilitydig

Thanks to This Month's Availability Digest Sponsor

OmniPayments

OmniPayments is a financial-transaction switch that routes transactions from POS terminals and ATMs to the issuing banks. It is popular as a BASE24 replacement. It uses HP NonStop technology to provide a switch that is always up and that requires no downtime for upgrades. OmniCloudX running on NonStop X provides low cost virtual transaction switches for small retailers.

In this issue:

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.

Check out our consulting services.

Disaster Recovery Plans Are a Disaster

A Disaster Recovery Plan (DRP) is the IT portion of a Business Continuity Plan. However, an adequate DRP requires a great deal of effort to create and a continuing effort to update and test. Estimates indicate that a DRP for a large corporation can take a year or two to write and that it will consume the time of several subject matter experts in the firm's business processes.

The creation of a DRP begins with a Business Impact Analysis (BIA) that establishes the criticality of each business process, how long it can be down, and how much data can be lost as the result of an outage. Based on the BIA, the facilities required for recovery will be specified (e.g., redundant IT servers); and the recovery procedures will be set forth.

Unfortunately, many organizations go without a DRP. Even if they have one, they are reluctant to test it because of the risk that the testing itself may cause an outage. Rather, they are willing to "wing it" in the event of an outage. The survival of their businesses is based on faith and hope.

Contact us to schedule your customized seminar on this and other availability and security topics.

Dr. Bill Highleyman, Managing Editor

Best Practices

The Big One – Are You Ready?

Is it safe to build a datacenter on the Ring of Fire, that line of earthquakes and volcanos that surrounds the Pacific Ocean? We are well overdue for the mother of all earthquakes in the Pacific Northwest of North America. The culprit? - the Cascadia Subduction Zone.

The Pacific Northwest has seen little in the way of earthquake activity over the two-hundred years or so that it has been settled by the U.S. or Canada. This can lull us into a sense of security that it is an earthquake-safe area. Nothing can be further from the truth.

The area has seen little earthquake activity because the tectonic plates in the Cascadia Subduction Zone upon which it rests are pushing harder and harder against each other without moving. At some point, this pressure will release; and the tectonic plates will rush into new positions. This will generate an earthquake that may well represent the worst disaster in North American history.

A wide swath of the upper Northwest coast will be demolished, including many datacenters that may be located there. The area is home to many large data centers operated by companies such as Microsoft, Boeing, Amazon, and Starbucks. Now is the time to plan for how your organization will handle this disaster. Otherwise, once the “big one” hits, your organization may simply disappear.

--more--

Multifactor Authentication

Authentication is the process of verifying that a person is who he says he is. In today’s online technology, authentication of a user is often accomplished by requiring that he log onto a system with his username and password. However, usernames and passwords can be stolen, rendering this form of authentication risky.

The use of a username and password is a form of single-factor authentication. Only one factor is required – the knowledge of the password. The authentication process can be significantly strengthened by requiring additional identifications. This is multifactor authentication. With multifactor authentication, two or more factors are required for identification – something you know, something you possess, and/or something you are (like a fingerprint).

Multifactor authentication brings a great deal of additional security to applications. It can drastically reduce the incidence of online fraud because stealing a victim’s password will no longer be enough to support a malicious logon.

Each additional authentication factor makes a system more secure. Because the factors are independent, the compromise of one should not lead to the compromise of others.

--more--

Availability Topics

Upgrades Can Take You Down

In our recent article “Human Triple Whammy – NYSE, UA, WSJ,” we noted that humans cause about 40% of all outages. Another major cause of outages is software upgrades gone wrong.

The major challenge with upgrades is that the systems being upgraded have grown ever more complex. Each component of a system has many points of integration with other components. It’s hard to predict how a little change to one component might affect the overall system or how that system interacts with other systems. Because of system complexity, it is difficult to thoroughly test an upgrade before it goes into service. Therefore, there exists a real chance that the upgrade may cause the system to fail.

In this article, we review several major outages caused by upgrades gone wrong. There are two lessons to be learned from these outages. One is that upgrades must be thoroughly tested before they are put into production. The other is that no matter how much testing is performed on an upgrade, upgrades will fail. Therefore, there must be a fallback plan that is known to work. Successful fallback plans require a great deal of planning to ensure their reliability.

--more--

Recommended Reading

IT Disaster Recovery Planning for Dummies

Over time, the requirements for IT outage recovery have shrunk from days to hours and in some cases even minutes. However, many data center managers have been unable to effectively address disaster recovery because of a lack of knowledge or a lack of resources.

Peter Gregory’s book, “IT Disaster Recovery Planning for Dummies,” provides IT management with the knowledge required to develop a disaster recovery plan (DRP). The book carries on the Dummies-series tradition of being easy to read and complete in detail. The over 300 pages of this book offer insight into disaster-recovery planning. It becomes clear that the creation of a good DRP requires a great deal of time of many subject-matter experts in the organization and therefore must be supported actively by upper management.

The other major consideration in a good DRP is testing. Disaster-recovery procedures are not of much value if they do not work. However, testing a DRP can be a risky venture. Therefore, several levels of testing are described. The final level is a full cutover that if unsuccessful could take down IT services. However, the alternative is to rely on faith and hope when a disaster hits.

--more—

Tweets

@availabilitydig – The Twitter Feed of Outages

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.

Now with our Twitter presence, we don't have to feel guilty. This article highlights some of the @availabilitydig tweets that made headlines in recent days.

--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.