the **Availability Digest**™

Volume 12
Issue 4

- - - achieving 100% uptime

April 2017

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

Follow us

@availabilitydig

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 writing services.

Digital Certificates Drive the Internet

A digital certificate is an electronic document used to prove ownership of a public encryption key. It is issued by a Certificate Authority (CA) and allows software to communicate securely with the certificate's subject, typically another computer.

Many companies have thousands of digital certificates. However, should the certificate expire, the public key no longer is available to the company; and the document or documents that it has encrypted may be lost. It is mandatory that records of all such certificates be maintained so that their expiration dates can be tracked. Only in this way can they be renewed on a timely basis.

Our article entitled "Epidemic of Certificate-Related Outages" exposes the difficulty organizations are having with maintaining their certificates. "Google and Symantec Spar Over Digital Certificates" shows the confusion that can result when digital certificates are issued.

These articles are an example of the stories we write for the Digest and for others. If you have an article, a case study, or a white paper that you would like written, come talk to us. We also provide consulting services and seminars on high- and continuous availability. We will be glad to help you.

Dr. Bill Highleyman, Managing Editor

Case Studies

Google and Symantec Spar Over Digital Certificates

Symantec is considered by many to be the largest digital certificate authority (CA) on the Internet. A CA issues digital certificates that authenticate the ownership of public keys used by organizations for encryption. A digital certificate allows software to communicate securely with the certificate's subject – typically another computer.

Symantec and the brands that it controls (such as VeriSign) account for 30 percent of the valid certificates used on the Internet.

However, Symantec has an unfortunate history of issuing improper digital certificates. In 2015, it terminated several employees involved in issuing unauthorized certificates for Google web pages.

In early 2017, an independent researcher determined that Symantec had issued 108 invalid Transport Layer Security (TLS) certificates. Ninety-nine were issued to companies with data that was obviously fraudulent. Nine were issued without the knowledge or permission of the affected domains.

Mis-issued certificates pose a critical threat because certificate holders can impersonate legitimate sites. To protect themselves and their customers, every organization needs to be able to quickly detect, remove, and/or replace unauthorized certificates issued by any CA. Businesses that are unprepared to detect and respond to CA errors threaten the integrity of encrypted and authenticated Internet traffic.

--more--

Never Again

GitLab Suffers Massive Backup Failure Due to a Fat Finger

GitLab offers a web-based Git repository manager. *Git* is an open-source program code repository for tracking changes in computer files. It is used primarily for software development.

GitLab offers several online and on-premises applications that allow users to code, test, and deploy software projects. It has over 1,400 open-source contributors.

On January 31, 2017, GitLab suffered a massive data loss when a technician accidentally deleted 300 GB of data from a production database. This error was compounded by the inability to restore the database from the company's backups. GitLab was down for about 36 hours before it was able to recover its database.

Statistics show that human error is the main cause of data loss. That was certainly true in GitLab's case. This is a further example of a caution we have expressed many times in the *Availability Digest*. Humans need redundancy, too. If a critical command to be entered could wreak havoc with your system, it should be entered by two people – one to type the command and the other to check it before it is executed. If GitLab had followed this simple procedure, its outage would not have happened.

--more--

Best Practices

Accounting for Non-Accountants

Years ago, I realized that many of we techies did not understand the fundamentals of dual-entry bookkeeping. I therefore wrote an article entitled “Accounting for Non-Accountants.” As an ‘oldie but goodie,’ I am republishing that article in this issue of the *Digest*.

Programmer types sometimes get called upon to implement or maintain a financial accounting system from time to time. At first, the job sounds relatively dull. Then we find ourselves scratching our heads and asking ourselves:

- Why are assets equal to the sum of net worth and liabilities? Are liabilities an asset?

- Why is an increase to a liability a credit? Sounds bad to me. Should be a black mark.

- If we increase an asset, we debit it. If we increase a liability, we credit it. But if we increase an expense, we debit it. Why is an expense treated like an asset? By the same token, if we increase revenue, we credit it. Are revenues like liabilities?

How can we remember these simple rules if they don’t make sense? Well, it turns out that a little simple logic and a little simple algebra can be used to make sense of accounting.

--more--

Availability Topics

Epidemic of Certificate-Related Outages

The use of digital certificates is skyrocketing as companies use more cloud services, IoT devices, and DevOps automation. A digital certificate is an electronic document used to prove ownership of a public key. It is issued by a certificate authority (CA) and allows software to communicate securely with the certificate’s subject.

Certificates and their corresponding keys are the foundation of all cyber security. They are the identity and access management facilities for machines, just like user names and passwords are for humans. Certificates allow machines to communicate securely.

The increase in certificates and their corresponding keys compounds the serious security vulnerabilities associated with cryptographic key and digital certificate management. When a digital certificate expires, the related public key no longer is effective. Communication with the certificate’s encrypted subject no longer is possible. The encrypted subject is effectively lost. This is a certificate-related outage.

Organizations must automate the discovery, issuance, lifecycle, and remediation of all keys. This process must start with a central record of digital certificates and their keys. Facilities must be in place to provide notification about the expiration of certificates so that they can be renewed in a timely fashion.

--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.