CRITICAL NATIONAL NEED IDEA

Multiple Location Model for Disaster Prevention and Rapid Information Deployment

Submitting Organization
Twin Peaks Software

Contact
John Wong
Twin Peaks Software
46732 Fremont Blvd.
Fremont CA 94538
Tel: (510) 438-0536
Fax: (717) 427-3470
Email: John.Wong@TwinPeakSoft.com

Key words:

Data Center, Disaster Prevention, Moore's Law, Multiple Location, Operating System

Table of Contents

A Multiple Location Model for Disaster Prevention and Rapid Information Deployment

An Area of Critical National Need

Moore's law still applies to computer hardware, especially certain components, but has never accurately described the growth of the software industry. Although CPU power, network speed and storage capacity have consistently exceeded Moore's law in the last two decades, and the Internet can move Gigabits of data per second from coast to coast, the software that utilizes and controls this fast and capable infrastructure lags considerably in its rate of growth and economies of scale, and the gap is increasing, especially in the areas of:

1) Disaster Recovery (DR) or Disaster Prevention (DP)

2) Rapid, real-time distribution and deployment of mission-critical information at multiple, geographically-dispersed locations

During the week of September 11, the widespread destruction of physical infrastructure supporting financial institutions in and around the World Trade Center and extensive telecommunications breakdowns throughout the region caused dislocation in financial markets. U.S. equity markets were closed for four days and most bond trading, including securities trading halted for two days. There were significant disruption in the clearing and settlement mechanisms for government securities, repurchase agreements, and commercial paper. [1, pg 2-3].

Yet, as of today, DR technology has made little progress since September 11, 2001 [4], despite calls to learn appropriate lessons [1].

Why?

It is the goal of this White Paper to analyze the problems and provide a direction for further research and development in this critical area.

Magnitude of the Problem

During the week of September 11, most financial institutions in and around the World Trade Center had disaster recovery procedure to ensure business continuity. Some used an active backup model, many used a split operation model. Other models were also in use. But they all failed, some miserably [1].

The world Trade Center disaster, concentrated in a few city blocks of Lower Manhattan, caused the nation's financial system to shut down for days. If the Greater New York City region had been hit by natural disaster of the magnitude of the 1906 San Francisco earthquake, all the redundancies provided by disaster recovery technology and solutions then current in the region would also have been knocked out, and the catastrophe would have been immeasurable.

Why did the disaster recovery technologies that we spent years of effort and resources to develop not work when we needed them?

The crux of the problem is that conventional software — the Operating System (OS) and the applications empowered by the OS — can only process mission-critical data in a single data center at a single physical location. All Disaster Recovery solutions developed to this day [4] are harnessed to and dependent upon the single data center model. They proved deficient, however, when trying to provide backup solutions at remote locations when their primary data center was knocked out by the September 11 disaster. This painful demonstration showed that the single location data center model is highly vulnerable: disaster recovery technology and plans based it were unable to protect the single data center or the data in it.

Unfortunately, all computer OS and applications designed and developed since the emergence of this single location information model half a century ago continue to be based upon it

Mapping to National Objectives

Critical Infrastructure Protection or CIP is a concept that relates to the preparedness and response to serious incidents that involve the critical infrastructure of a region or nation. The US CIP is a national program to assure the security of vulnerable and interconnected infrastructures of the United States. In May 1998, President Bill Clinton issued Presidential directive PDD-63 [2] on the subject of Critical Infrastructure Protection. This recognized certain parts of the national infrastructure as critical to the national and economic security of the United States and the wellbeing of its citizenry, and required steps to be taken to protect it.

Presidential Decision Directive/NSC-63 addressed vulnerability of the nation's critical infrastructure (cyber-based information systems and others), and called for "Critical Infrastructure Protection" as "A National Goal" that requires "flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security."

the directive was updated on December 17, 2003 by President Bush, through Homeland Security Presidential Directive HSPD-7 for Critical Infrastructure Identification, Prioritization, and Protection[3]. The directive broadened the definition of infrastructure in accordance with the Patriot Act, as the physical and virtual systems that are “so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety.”

Meeting a Timely Need Not Met by Others

Given that the conventional, static, single location information model in use for the last 50 years is fragile, vulnerable, and inefficient, there is a clear national need for a new information model that enables multiple data centers to be deployed at geographically dispersed locations so that:

1) Each data center can contain and process identical copies of mission-critical information

2) Each data center updates the other data centers to which it is connected with the latest-processed mission-critical data, so that all connected data centers remain synchronized nationwide.

This new information model enables every data center to operate independently as the primary production data center for the region it server, in sync with other data centers in real time. When one data center is struck by disaster or needs to be taken out of service for maintenance, there are still other data centers up and running, so any disaster hit on one or two regions is restricted to the local or regional level, and catastrophic damage to mission-critical data can be effectively prevented.

Another advantage of this dynamic multiple location information model is that a new data centers can be added at other geographically-dispersed locations as needed, on the fly, without disrupting the normal operations of other data centers.

The new dynamic multiple location information model can solve many problems that have persisted in the industry for decades. In addition to disaster recovery, it can also help to eliminate the problem of single points of failures in both hardware and software and to enable real-tine file backup between systems.

It is hoped that research and development in this area will unlock and alter the "DNA" of computer systems to make them more robust, resilient, and efficient. Adequate funding from private sources has not been forthcoming in recent years. Nevertheless, the national need for technical solutions to the inherent risks of the single location information remains as critical today as it was 10 years ago. Investment in further investigation has the potential to address this weakness in the national infrastructure may also lead to considerable commercial benefits.

Benefits

The result of this high-risk, high-reward research in the new information model can empower many things, including:

- Enterprise data processing
- Manufacturing processing
- Communication infrastructure
- Defense systems

Virtually every entity, from large-scale enterprises and government agencies to end users, that uses computer systems to control and process information can benefit from research and development of the new information model. For instance, it can empower end users to back up (replicate) a copy of their files from the laptop or desktop to either a data center or a remote server in the Cloud transparently and seamlessly. It can also help industry to distribute information rapidly to multiple geographically-dispersed location automatically and efficiently.

Summary

Computer software, especially Operating System software, has made only incremental, not fundamental progress in the last two decades, causing a gap between drastic improvements in CPU power, network speed, and storage capacity on one hand and their utilization on the other. In some case, the legacy of the conventional, single location information model has inhibited new technology or solutions from developing and left the nation's information infrastructure vulnerable to human and natural disaster. The static, single location information model needs to be replaced by a dynamic, multiple-location model.

It is anticipated that research and development in this area will lead to further possibilities and solutions as well.

References

[1] Summary of lessons learned from September 11 and implication for business continuity. US Securities and Exchange Commission: Washington, DC. February 13, 2002.
http://www.sec.gov/divisions/marketreg/lessonslearned.htm

[2] Corp, E. Sysmetrix remote data facility.
http://www.emc.com/products/family/srdf-family.htm last accessed June, 2009.

[3] PARSON,H., MANLEY,S. , FEDERWISCH, M,, MOORE, T. HITZ, D., KLEIMAN, S., AND OWARA, S. Snapmirror: File System based asynchronous mirroring for Disaster recovery. In Proc. of USENIX FAST (January 2002).

[4] KEETON, K., SANTOS, C., BEYER,D., CHASE, J., AND WILKES,J., Designing for disasters. In Proc. of USENIX FAST (Berkeley, CA, USA, 2004) USENIX Association

[5] PRESIDENTIAL DECISION DIRECTIVE/NSC-63, May 22, 1998.
http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

[6] Homeland Security Presidential Directive / HSPD-7, December 17, 2003
http://www.fas.org/irp/offdocs/nspd/hspd-7.html