

LIQUIDIQ[®] BUSINESS CONTINUITY

Disaster Recovery Made Simple

Introduction

Business Continuity Planning (BCP) is a subject of increasing importance for most enterprises today. The events of 9/11 and hurricane Katrina are front page examples of our vulnerability to disaster, but data centers are hit on a regular basis by power outages, tornadoes, floods, and earthquakes. Even something as mundane as a communications “back-hoe” outage can isolate your data center from your customers. Human errors inside the data center also cause major system outages. Some BCP plans even account for disease outbreaks.

The cost of an outage varies by industry. Businesses that manage a high volume of financial transactions, for example, encounter down time costs as high as millions of dollars per hour. Industries that link system and service availability to contractual obligations lose customers, reputation and revenue during protracted outages. Regulatory and compliance implications due to downtime and data loss have severe costs for most large enterprises, as well. With the first wave of virtualization, enterprises are consolidating resources on x86 based servers. This concentration of resources makes disaster recovery all the more critical. Less data center equipment provides savings in terms of capital and operating expenses, power and cooling, and real-estate. However, single system outages can now affect widespread user bases and enterprise resources.

Today's solutions

It's not surprising that established and new vendors alike are responding to the need for effective Disaster Recovery (DR) and Business Continuity (BC) solutions with new products. Storage and virtualization vendors specifically are leading the charge to new solutions, but these solutions have some limitations.

Virtualization

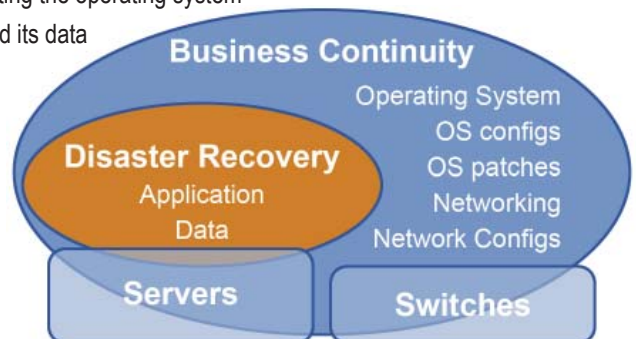
Traditional DR solutions back up the application and its data. Extra care must be taken to make sure the disaster recovery site has suitable hardware, and the same version, patch level and configuration settings for the operating systems on local disk. The second wave of virtualization is enabling more effective disaster recovery solutions by encapsulating the operating system

(OS) environment with the application and its data into a file that can be easily backed up.

There are limitations with this approach, however. First, not all applications are suitable for virtualization, and second, network configurations must be captured by another method.

Network configuration

In a typical data center, network equipment and networking configurations are managed by separate systems and different administrators. Continuity of the application at the DR site is also dependent on these network configurations. Applications such as Oracle RAC, for example, require several separate networks with very specific configuration requirements. VMware features like VMotion also require several separate networks.



Typically, this network configuration data is not included in an application data back-up image, and must be manually re-configured by network administrators on the DR site when a disaster strikes or when the BCP process needs to be verified. The considerable manual effort makes it difficult to achieve a business Recovery Time Objective (RTO).

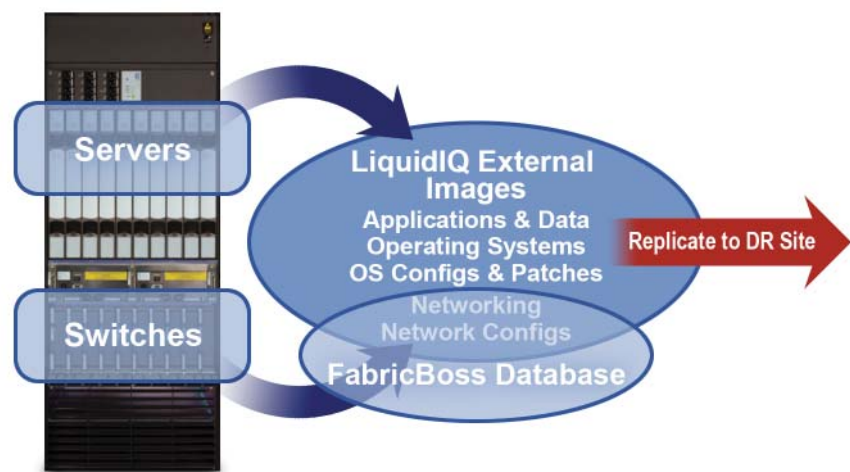
Verification

Since BCP plans require manual procedures by a team of system and network administrators, verifying the BCP process is costly and time consuming. In many cases, this phase of the BCP cycle is not properly tested or kept current with the changing applications and environment in the data center.



The LiquidIQ Solution

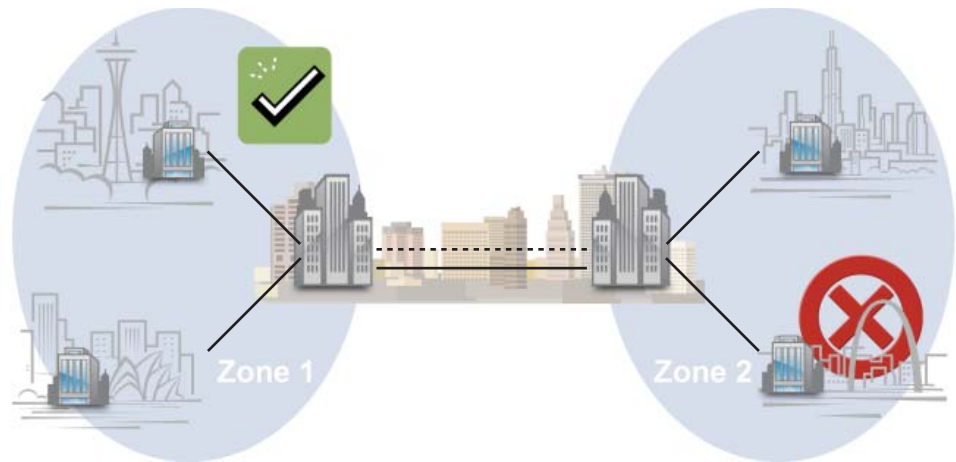
Liquid Computing’s converged compute and networking architecture removes typical DR limitations by providing a holistic view and centralized control of the entire IT infrastructure. Our LiquidIQ® solution encapsulates and virtualizes all compute, networking and I/O resources in the same system. All server operating system instances, native bare-metal or virtualized, are defined and contained in a LiquidIQ “logical server“ which is abstracted from the physical hardware and portable to another LiquidIQ system. In addition, all network configuration settings are also virtualized and stored in the LiquidIQ FabricBoss™ database. All operating system images, all application images, the most recent patches, all data, as well as all network configuration settings are saved on external storage. This information is replicated to a DR site leveraging storage vendor features and tools at intervals driven by a business Recovery Point Objective (RPO).



BCP process verification is as simple as applying a “source” LiquidIQ configuration on a “destination” LiquidIQ system and booting the servers. There are no manual server or networking configuration procedures that can become error-prone or obsolete.

A LiquidIQ Disaster Recovery Scenario

Let's examine a typical DR scenario and then show the benefits of adding LiquidIQ to the environment. For example, let's say a service provider has two main data centers connected by redundant links. They also manage several distributed smaller points of presence (POP) which can be grouped into independent geographically isolated management zones. (See diagram below.)



Designated individual POP sites in one geographically clustered zone operate as disaster recovery centers for all POP sites in peer geographic zones. A small number of designated 'DR-enabled' POP sites support a large number of distributed systems, where there is only an N+1 incremental equipment acquisition required per zone. There is no need for 1:1 hardware duplication for all supported sites. This maximizes business continuity with minimal cost, effort, and downtime.

With LiquidIQ in the production environment, virtualized and non-virtualized applications, and the complete computing infrastructure are automatically recovered on a LiquidIQ DR site. This includes all networking and I/O configuration settings. The entire IT Infrastructure is captured and replicated on Network Attached Storage (NAS) or Storage Area Networks (SANs) at the remote site using existing and well-known file synchronization tools. LiquidIQ enables verification and validation of the complete IT infrastructure at the DR site. This minimizes service disruptions and allows the service provider to maintain business continuity while meeting SLAs and legal obligations.

Liquid Computing's unique architecture enables robust DR infrastructure and simplified resource management that can be handled by fewer, less qualified admin employees. This is critical as more and more enterprises move to virtualized computing infrastructures. Our LiquidIQ solution in particular makes IT infrastructures easy to manage and reduces the complexity of DR schemes. The complete solution reduces operating expenses, consolidates space, reduces energy consumption and maintains business continuity.

To learn how to make disaster recovery much simpler, please email info@liquidcomputing.com or call 1-877-592-2666 for more information.

About Liquid Computing, Inc.

Liquid Computing has delivered a new generation of IT infrastructure that is transforming the traditional server and switch configurations commonplace in data centers. LiquidIQ, the world's first fully converged communications and computing platform, provides flexible pools of computing, networking and switching resources and makes data center IT infrastructure easy to manage. For more information, visit www.liquidcomputing.com.