Chapter 16

Enhancing the Disaster Recovery Plan through Virtualization

Dennis C. Guster
St. Cloud State University, USA

Olivia F. Lee
Northwest University, USA

ABSTRACT

Currently, organizations are increasingly aware of the need to protect their computer infrastructure to maintain continuity of operations. This process involves a number of different concerns including: managing natural disasters, equipment failure, and security breaches, poor data management, inadequate design, and complex/impractical design. The purpose of this article is to delineate how virtualization of hosts and cloud computing can be used to address the concerns resulting in improved computer infrastructure that can easily be restored following a natural disaster and which features fault tolerant hosts/components, isolates applications security attacks, is simpler in design, and is easier to manage. Further, because this technology has been out for a number of years and its capabilities have matured an attempt has been made to describe those capabilities as well as document successful applications.

INTRODUCTION

Numerous types of disasters, both natural and manmade, can be catastrophic to businesses. Without a well thought out disaster recover (DR) plan, such events can seriously disrupt routine business operations. Often times, it is difficult to comprehend the devastation of an unknown future event, let alone create a comprehensive approach to meet and survive it. The most critical challenges are related to understanding the scope and complexity of DR requirements and the risk of inadequate deployment of recovery efforts. Too often in the past companies have
Enhancing the Disaster Recovery Plan through Virtualization

relied on specific vendors and the architecture they provide. However, with virtualization the architecture tends to be more open and it is critical that business adopt a structure independent approach (Zheng & Fang, 2009). This lack of understanding is especially applicable to small or medium size businesses (Hill, 2008) due to the limited IT resources they have available. Larger firms are able to apply economy of scale to develop an information technology (IT) department that equips them with the basic infrastructure to support the addition of DR mechanisms. Small and medium sized businesses, on the other hand, often do not have adequate infrastructure and since, they operate on smaller profit margins, devising and supporting a DR plan can be a huge burden. While outsourcing has been an option for some time for small companies, there are options that build on the advantages of a virtual cloud environment. Wood, Cecchet, Ramakrishnan, Shenoy, van der Merwe, and Venkataaramani (2010) report the technical advantages of this architecture as well as its cost effectiveness for small business. No matter the model used a business must realize that they need to invest in DR. Recently, Search Security. com reported that disaster recovery often accounts for as much as 25% of the IT budget. Hence, sound disaster recovery planning is a very important undertaking not only due to what might be lost, but also from a budget perspective. Hence, devising a strong DR infrastructure is further justified by the “information intensity” structure of many companies in the 21st century.

Specifically, for many companies in the 21st century, information resources are their livelihood. The loss or unexpected long term disruption of information or data could have a detrimental effect on business operations. Phillippi (2008) reports that 92% of small businesses that experience significant data loss due to a major disaster go out of business within five years. Indeed, due to the high level of internet connectivity required by most operation functions today, the risks are high and warrant a well thought-out plan with appropriate risk assessment (e.g., Hiles, 1992; Jones & Keyes, 2001; Stephens, 2003). There are success stories in regard to the successful application of virtualization to business applications. A great example is reported by Maitra, Shanker, and Mudholker (2011) in which they describe how virtualization was applied to the banking industry and how secure connectivity was achieved.

Although security risks of the internet increase the need for an effective disaster recovery mechanism, the internet connectivity is nevertheless advantageous as it can be effectively used in the data replication process. If the data is not available it could have far reaching effects particularly in mission critical application such as health care. Therefore, it is crucial that the design focus on the concept of high availability (Adeshiyan et al., 2009). Given this need to ensure high availability, an efficient and cost-effective disaster recovery strategy is to utilize the geographic distribution of the critical components model (Adam, 2002). The connectivity can be inexpensively provided by the internet provided secure transmission methods, such as virtual private networks or VPNs (a way of isolating and double encrypting data sent across the internet), are used, and using the internet can minimize the huge cost of leasing dedicated lines (such as T1 a non-switched digital phone line). The data replicas should be at least 150 miles from the data center headquarters (Phillippi, 2008).

Information resource or data recovery can take many forms. In the past, pools of computers, on which a few members worked together and shared resources, could be used to house backup systems. While this approach still has merit and fits reasonably within a service oriented architecture approach (SOA), for small businesses with remote sites and existing corporate partners, there are major trust issues to resolve in regard to the partners that make up the pool. An alternative is the use of virtualization which can potentially minimize costs and server density (Safigan, 2008). This approach has been refined and the work of Calzolari, Arezzini, Ciampa, Mazzoni, Domenici,