UNIVERSITI PUTRA MALAYSIA

ARCHITECTURE FOR HIGH DATA AVAILIBILITY USING SERVER VIRTUALIZATION FOR DISASTER RECOVERY

MAZNIFAH BINTI MOHD SAHALAN @ SALAM

FSKTM 2015 29

ARCHITECTURE FOR HIGH DATA AVAILIBILITY USING SERVER VIRTUALIZATION FOR DISASTER RECOVERY

By

MAZNIFAH BINTI MOHD SAHALAN @ SALAM

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Master of Science

November 2015

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the Master of Science

ARCHITECTURE FOR HIGH DATA AVAILIBILITY USING SERVER VIRTUALIZATION FOR DISASTER RECOVERY

By

MAZNIFAH BINTI MOHD SAHALAN @ SALAM

November 2015

Chair : Nur Izura Udzir, PhD
Faculty : Computer Science and Information Technology

Data, information and knowledge are becoming the most valuable commodity in everyday business exchange and transactions. Information availability has become increasingly central to organizations' success. Organizations have been targeted by attackers for the value of their data and information. These profound evolutions has changed and challenged the aspects of information security in ensuring organizations information are secure and be made available when needed. By using virtualization as a recovery platform, organization can protect a larger share of data center workloads without having to invest in costly duplicate hardware and software. This research proposes an architecture using server virtualization to provide high availability of data, through fast and high data through fast and high data recovery on virtual infrastructure for disaster recovery. The proposed architecture uses multi side network RAID to achieved return of time objectives (RTO) and return of point objectives (RPO) of the application in the organization. In server consolidation, multiple physical server applications are deployed onto the virtual machines (VM), which then would run on a single or fewer real high-end servers to achieve better performances compared to utilizing several or even hundreds of traditional servers. In addition, data protection becomes a big problem where the organizations are responsible to overcome the problem of data loss due either intentionally or unintentionally. Security perimeters are used in the proposed architecture to maximize the data protection in the organization.

To evaluate the proposed architecture, experiments using existing tools with virtualization technologies such as VMWare, Ranger Pro for backup and Trend Micro Deep Security have been carried out. This research proposes an architecture which simulates automated data replication from production site to disaster recovery site that creates an active-active environment. The proposed architecture contributed good result in Recovery Point Objective (RPO), Recovery Time Objective (RTO), data loss and data availability at 99.91 % of data are recovered during recovery process. Recovery platform using virtualization technology can protect a larger share of disaster recovery workloads in terms of high availability and data protection.

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia
sebagai memenuhi keperluan untuk Ijazah Master Sains.

SENI BINA PERLINDUNGAN DATA MENGGUNAKAN TEKNOLOGI PEMAYAAN PELAYAN UNTUK PEMULIHAN BENCANA

Oleh

MAZNIFAH BINTI MOHD SAHALAN @ SALAM

November 2015

Pengerusi: Nur Izura Udzir, PhD
Fakulti : Sains Komputer dan Teknologi Maklumat

Data, maklumat dan pengetahuan adalah komoditi yang paling bernilai untuk sesebuah organisasi. Ketersediaan maklumat telah menjadi semakin penting kepada kejayaan organisasi. Organisasi telah menjadi sasaran penyerang bagi mendapatkan data dan maklumat. Bagi proses sandaran data dan pemulihan data yang tidak cekap dan tidak selamat, organisasi menghadapi kesukaran apabila berlaku insiden dan proses pemulihan data tidak berfungsi. Dengan menggunakan teknologi virtualisasi sebagai salah satu platform pemulihan, organisasi boleh melindungi sebahagian besar daripada beban kerja pusat data tanpa perlu melabur lagi dalam perkakasan, perisian dan proses penduaan yang mahal. Kajian ini mencadangkan satu seni bina menggunakan virtualisasi pelayan untuk menyediakan ketersediaan data yang tinggi dan pemulihan data yang cepat melalui infrastruktur maya bagi pemulihan bencana. Seni bina yang dicadangkan menggunakan RAID sebelah rangkaian adalah untuk mencapai objektif pulangan masa (RTO) dan pulangan objektif titik (RPO) bagi sesebuah sistem aplikasi dalam organisasi. Dalam gabungan server, beberapa aplikasi server fizikal telah dimasukkan ke dalam beberapa mesin maya yang kemudiannya akan dijalankan oleh satu atau beberapa fizikal server sebenar yang mempunyai spesifikasi tinggi bagi mencapai prestasi yang lebih baik berbanding menggunakan beberapa buah atau bahkan ratusan server tradisional. Tambahan pula, perlindungan data menjadi masalah besar di mana organisasi bertanggungjawab untuk mengatasi masalah kehilangan data sama ada secara sengaja atau tidak sengaja. Perimeter keselamatan yang digunakan dalam seni bina yang dicadangkan digunakan untuk memaksimumkan perlindungan data dalam organisasi.

Untuk menilai simulasi, eksperimen menggunakan alatan yang mempunyai teknologi virtualisasi seperti *VMware*, *Ranger Pro* untuk sandaran dan *Trend Micro Deep Security* telah dijalankan. Kajian ini mencadangkan satu seni bina yang mensimulasi replikasi data secara automatik dari tapak pengeluaran ke pemulihan bencana. Ia mewujudkan persekitaran yang aktif-aktif dengan mereplikasi data dari tapak pengeluaran ke pemulihan bencana. Seni bina yang dicadangkan menyumbang hasil yang baik dalam objektif pulangan masa (RTO), pulangan objektif titik (RPO), kehilangan data dan ketersediaan data selepas proses pemulihan, iaitu 99.91% daripada data yang diperolehi setelah proses pemulihan dilakukan. Ia juga menghasilkan keputusan yang baik selepas pemulihan dengan menggunakan teknologi virtualisasi dalam melindungi bahagian yang lebih besar daripada beban kerja pemulihan bencana dari segi ketersediaan yang tinggi dan perlindungan data.

ACKNOWLEDGEMENTS

All praise is due to Almighty Allah as He is all merciful, most gracious and most compassionate and it is He who gathered all knowledge in its essence and our Messenger the prophet Muhammad (peace and blessings be upon him) and his progeny, companions and followers. All grace and thanks belong to Almighty Allah.

I would like to take this opportunity to record my gratitude towards the great people who has supported me during the phases of this research. Special thanks to my supervisor, Associate Professor Dr. Nur Izura Udzir who has always the time when I have a problem in this research. She has patiently answered my questions, giving valuable comments, guidance and advice through the course of this research.

Also, my deepest appreciation to my supervisory committee members Associate Professor Dr. Md Nasir Sulaiman and Puan Zaiton Muda for their cooperation, efforts and valuable comments.

Great thanks to the Faculty of Computer Science and Information Technology for the facilities and also the university library and Universiti Putra Malaysia for providing the working environment to me to perform this research.

I want to express my special thanks to my mother and my late father, who never let me believe I could not succeed in this research. Also, special thanks to my husband Norol Aizam, my kids and my special friends Puan Salwa Ab Rahman and En Mohd Hairy Mohammadiah for their support, love and encouragement during my research. Finally, I am grateful to my entire friends for their impressive help in my research.

I certify that a Thesis Examination Committee has met on (date of viva voce) to conduct the final examination of Maznifah binti Salam @ Mohd Sahalan on her thesis entitled Architecture Of Data Protection Using Server Virtualization Technology For Disaster Recovery in accordance with the Universities and University Colleges Act 1971 and the Constitution of the Universiti Putra Malaysia [P.U.(A) 106] 15 March 1998. The Committee recommends that the student be awarded the Master of Science.

Members of the Thesis Examination Committee were as follows:

Fatimah bt Sidi, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Mohd Taufik b Abdullah, PhD
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Osman bin Ghazali, PhD
Title (Associate Professor)
School of Computing
Universiti Utara Malaysia
Malaysia
(External Examiner)

ZULKARNAIN ZAINAL, PhD
Professor and Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date: 21 April 2016

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirement for the Master of Science. The members of the Supervisory Committee were as follows:

Nur Izura Udzir, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Md Nasir Sulaiman, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Zaiton Muda
Senior Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

BUJANG KIM HUAT
Professor and PhD
Dean School of Graduate Studies
Universiti Putra Malaysia

Date:

Declaration by graduate student

I hereby confirm that:

- this thesis is my original work;
- quotations, illustrations and citations have been duly referenced;
- this thesis has not been submitted previously or concurrently for any other degree at any other institutions;
- intellectual property from the thesis and copyright of thesis are fully-owned by Universiti Putra Malaysia, as according to the Universiti Putra Malaysia (Research) Rules 2012;
- written permission must be obtained from supervisor and the office of Deputy Vice-Chancellor (Research and Innovation) before thesis is published (in the form of written, printed or in electronic form) including books, journals, modules, proceedings, popular writings, seminar papers, manuscripts, posters, reports, lecture notes, learning modules or any other materials as stated in the Universiti Putra Malaysia (Research) Rules 2012;
- there is no plagiarism or data falsification/fabrication in the thesis, and scholarly integrity is upheld as according to the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) and the Universiti Putra Malaysia (Research) Rules 2012. The thesis has undergone plagiarism detection software.

Signature: _____ Date: _____

Name and Matric No.: Maznifah binti Salam @ Mohd Sahalan GS23265

Declaration by Members of Supervisory Committee

This is to confirm that:

- the research conducted and the writing of this thesis was under our supervision;
- supervision responsibilities as stated in the Universiti Putra Malaysia (Graduate Studies) Rules 2003 (Revision 2012-2013) are adhered to.

Signature: _____	Signature:_____
Name of Chairman of Supervisory Committee: Associate Professor Dr Nur Izura Udzir	Name of Member of Supervisory Committee: Associate Professor Dr Md Nasir Sulaiman

Signature: _____
Name of Member of Supervisory Committee: Puan Zaiton Muda

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVATIONS

BCE	Basic Consolidation Estimate
BCDR	Business Continuity and Disaster Recovery
BC	Business Continuity
CPU	Central Processing Unit
CDP	Continue Data Protection
CA	Continuous Access
CIA	Confidentiality, Integrity And Availability
DVWA	Damn Vulnerable Web Application
DPA	Data Protection Architecture
DRM	Data Repository Model
DSA	Deep Security Agent
DSM	Deep Security Manager
DPI	Deep Packet Inspection
DAS	Direct Attached Storage
DR	Disaster Recovery
HA	high availability
IP	Internet Protocol
ICMP	Internet Control Message Protocol
IM	Integrity Monitoring
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
iSCSI	Internet Small Computer System Interface
LTO	Linear Tape-Open
LAN	Local Area Networks
LUN	Logical Unit Network
OS	Operating System
P2V	Physical To Virtual
RTO	Return Of Time Objectives
RPO	Return Of Point Objectives
RAID	Redundant Array Of Independent Disks
RABC	Real-time Assurance of Business Continuity
SAS	Serial Attached SCSI
SLA	Service Level Agreement
SCSI	Small Computer System Interface
SMB	small and medium-sized businesses
SAN	Storage Area Network
SSSU	Storage System Scripting Utility
VM	Virtual Machine
VMM	Virtual Machine monitor
VMDK	Virtual Machine Disk
VSA	Virtual Storage Appliance
VSE	Virtual Server Environment
V2V	Virtual-to-virtual
WAN	wide area network

CHAPTER 1

INTRODUCTION

This chapter provides the general idea about the current research where it explains the research background, problem statement, research questions and objectives and research scope. This chapter is considered to be crucial since it provides important information for applying data protection using server virtualization for disaster recovery (DR).

1.1. Research Background

Data protection systems include high availability (HA), backup, disaster recovery, and archive and security systems. Each of these systems is attempting to give a particular business unit access to the data that it needs within a timeframe acceptable for that particular business unit (Curtis, 2012). Such events can include natural disasters, hardware failures, software failures, errors by user admin, and malicious attacks. Given these threats, most businesses protect their data by using techniques such as remote mirroring, point-in time copies (e.g., snapshots), and periodic backups to tape or disk. These techniques have different properties, advantages, and costs. For example, using synchronous remote mirroring permits applications to be quickly failed over and resumed at the remote location. Snapshots internal to a disk array are space-efficient and permit fast recovery of a consistent recent version of the data. Backups to the tape or disk allow an older version of the data to be recovered. These techniques have limitations. Remote mirroring usually has high resource requirements, local snapshots do not protect against failure of the disk array, and recovering from backups can result in significant loss of recent updates (Gaonkar et al., 2010).

Ensuring data availability in back up and restoring processes and securing data from attackers are the focus of this research. The restoration processes need to overcome the issue of unavailability of data to ensure successful data restore and recovery process. To mitigate the risk of losing data, administrators typically make backup copies of data stored on various storage devices. Users sometimes have no mechanism to test the backup data and once the backup doesn't work it turns to disaster when the backup process is not able to be used. During the gathering information from reference, it found that certain organisation mentioned and worries of data loss if anything happen to the application system.

For over twenty years, information security has held three key concepts which form the core principles of information security: confidentiality, integrity and availability (CIA) (Parker, 2002). Data availability is important to ensure no disruption of data in a long run. One of the elements on disaster recovery plan is to ensure availability of data after any incident/disaster happen to make sure no disruption in business operation. Disaster recovery (DR) is the process in which an organization can recover the data after any disaster events happened (Sindoori *et al.*, 2012). Disaster recovery configurations are used in some cases to provide additional protection against loss of data due to failures, not only in the computer system themselves but in the surrounding environment (Parker, 2002).

Information security is defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. It means

to protect the data and the systems from those who would seek to misuse it and even more from every unauthorized person (Parker, 2002).

Availability refers to the ability to access the data when it needed. Loss of availability can refer to a wide variety of breaks anywhere in the chain that allows access to the data.

In information security, integrity means that data cannot be created, changed, or deleted without authorization. It also means that data stored in one part of a database system, is in agreement with other related data, stored in another part of the database system (or another system). For example, the loss of integrity can occur when a database system is not properly shut down before maintenance or the database server suddenly loses its electrical power (Parker, 2002).

There was a promising and positive impact from data protection for organizations in Malaysia and other countries. Without data, system cannot be operated and it will affect the whole operation cycle. Due to unavailability of data, organisation will suffer and may cause the business closure and lead to unemployed workers.

Back up and restoration process include of data availability to complete the cycle. Incomplete data cycle will cause the data loss and system cannot be operated as the previous operation.

Data protection methods can be classified into three categories: restore, recover, and overcome. Restore methods can restore the systems' functionality after an incident or event occurred but the organizations require a significant amount of time to do so. Recovery methods allow the organizations or business unit to continue functioning after such an event, but would require a minor disruption in service before doing so. Finally, methods that allow to completely overcome an event are typically the most expensive, but this method would allow the organizations or business unit to continue functioning uninterrupted through any kind of event (Curtis, 2012).

Traditional method requires same hardware specification and configuration, periodic management, high power and cooling costs. Traditional method creates bottleneck and performance problem and take more time to complete. Application and data recovery process through image tools and tape backups are complex and slow. Traditional backup and recovery methods involve complex procedure operating system backup agents, scheduling and performing backups, restoring data, testing and verification of backups (Sindoori *et al*., 2012).

Data protection is a critical aspect of all computing environments. Over the years, it has changed with the goal of protecting an enterprise's data from device failure expanding to encompass software failure, human error, site outages and theft.

The term data protection for an IT department is to ensure the data that the organization needs is available when it is needed and is not made available to those entities that should not be given access. Data protection system includes high availability (HA), backup, disaster recovery, and archive and security systems (Curtis, 2012).

Data protection is very important for the commercial sectors where data recovery is crucial in case of disaster to minimize data losses. In fact, many companies like small

and medium-sized businesses (SMB) nowadays still rely on the traditional backup technology like tape data storage backup for data protection.

Nowadays, there were limited ways of architectures for backup to recover data. Most people think that, once the backup was successful, the data are always available, whenever disaster happens. Therefore, many organizations have turned to corresponding replication and high availability solutions to minimize downtime and ensure critical applications and important data is protected (Curtis, 2012).

The ever-increasing amount of data imposes challenges for traditional data protection during a disaster. Thus, the information technology (IT) department needs to ensure the availability of data with larger backup set and need longer recovery time.

Due to the global demand, the IT department must ensure:

i. Shorter recovery time to restore the information after disaster occurs.
ii. Using the existing resources to manage more backup with less time.
iii. Protect the data due to the attackers' activity.

With the challenges mentioned, it will pave ways for an alternative approaches to data protection**.** Solutions of architectures of data protection using server virtualization technology in disaster recovery were proposed in this research.

1.2. Problem Statement

Presently, there are still many legacy applications which were running on old machines in many large organizations. Many administrative and maintenance efforts, and also huge space of capacity were required for those applications. A study by Tan *et al*. (2003), virtualization can be used to improve the performance and efficiency and effectiveness of server virtualization through the use of "live" migration and dynamic resource allocation. For the purpose of higher resource utilization and smaller space organization's requirement, server consolidation, which consolidates multiple physical servers into a single or fewer real machines were proposed. Thus, using virtualization technology for data centre is not a new concept or theory anymore. Currently, there are tools that can manage virtualized environments as specified by Tan *et al*. (2003).

The performance of virtualization technology and efficient utilization of physical equipment were the main concerns by academicians and industries. There were only few researches on the performance benchmark of server consolidation and those researches concentrated on the static performance of server consolidation (Cherkasova & Gardner, 2005). Few researches were involved in the performance change during creating and killing of virtual machine (VM) under different workloads, namely dynamic performance. The VSCBenchmark is a benchmark for stability and dynamic performance of virtualization technology where it measures the dynamic performance and stability of VM and the influence between VM. It was also used to observe the results when the VM or the tasks changed (Jin *et al*., 2008).

The business operations and the types of services are not always the same where the services may be started and closed frequently according to the users' requirements.

Current situation in the organization, data recovery is done via traditional architecture (e.g.: backup tape). Traditionally, this functionality is provided by a backup and recovery system that does one of the following:

1. Backup to tapes that are sent off site
2. Backup to disk, copies to tapes that are sent off site
3. Backup to disk, replicates to other disks that are located off site.

Regardless which method is chosen to ensure that copies of data are stored away from the servers the organizations are protecting, the restore method is always the same: copy significant amounts of data from the backup medium to the system to be restored. This is why it is said that very little has changed in backup and restore in multiple decades. But in the end, restore methods still require significant amounts of downtime to perform their function (Curtis, 2012).

Key findings indicate that the vast majority of organizations identify backup as critical, yet most also believe that current methodologies are incomplete. Furthermore, the current solutions for backup and recovery is complex with 90 percent of IT professionals using multiple backup and recovery tools, and 91 percent report that using multiple tools causes issues. With increasingly complex and critical IT environments, the organization looking for ways to fully protect their business, while at the same time providing easier and faster recovery times. To cope, an overwhelming 90 % report that they have multiple backup and recovery tools in place and more than 60 % say that these tools have duplicate functionality. To make matters worse, 91 % of organizations report that there are challenges in using multiple tools, including the learning curve of utilizing multiple solutions, increased cost of licenses and maintenance, or the management of multiple solutions of backup and recovery (Axcient, 2014).

Based on current practice at the existing organisation, the researcher found that the Storage Area Network (SAN) replication for data drive was currently being deployed for some of the servers, however it does not provide 100% recovery as the operating system (OS) volume is not being replicated to the DR site. Daily observation resulted the error message appear at the server during back up process. As a result the organizations rely on the tape backup for restoration of data. Some of the servers may not be connected to SAN at all; hence a total tape backup of the server was required. In order to connect the server to the SAN and to ease the server management, server virtualization technology is proposed.

Currently, only antivirus software is provided to the organisation. Antivirus software is a type of utility used for scanning and removing viruses from your computer. While many types of antivirus (or "anti-virus") programs exist, their primary purpose is to protect computers from viruses and remove any viruses that are found (TechTerms, 2010). None of the security perimeter is provided for data protection for virtualised environment.

1.3. Research Questions

Based on the problem statements in the previous sections, the research questions that this research attempts to solve is:

i. What is the best architecture to ensure high availability (HA) of data in the organisation after disaster occurs?
ii. What is the most efficient mechanism in terms of time and speed to ensure the high availability of data in back up and restoration?
iii. How to ensure the data are secured from attackers by using server virtualization security technology?

1.4. Research Objectives

This study aims to answer three fundamental research questions leading to the development of the research objectives and the outcome of this research.

The main objective of this research is to propose an architecture using virtualization technology with a recovery system management to minimize data losses, increase data availability and to protect information systems.

In this research, there are specific objectives to be achieved are:
i. To propose an efficient architecture in time and speed in server virtualization technology.
ii. To propose a secure virtualised environment architecture that can protect data from attackers by adding security parameter i.e agent-less anti-malware protection, deep packet inspection (DPI) rules, IDS/IPS, web application control, application control, firewall rules, log inspection rules and integrity monitoring rules.

1.5. Research Scopes

The research is limited to the simulation of architectures and proposed architecture in terms of return of time objectives (RTO) and return of point objectives (RPO) of the application in the organization. It focuses on high availability of data for disaster recovery (DR). The research scope does not include the cost of hardware, energy consumption, human intervention issues and cloud computing technology.

1.6. Thesis Organization

This thesis is organized in six chapters where:
Chapter 2 presents an overview of availability, disaster recovery, the purpose of disaster recovery centre, data protection architecture, backup and restore using traditional architecture, storage area network (SAN) to SAN replication and auto replication, the meaning of virtualization, previous researches related to server virtualization and data protection in disaster recovery.

Chapter 3 provides research methodology about the server virtualization for disaster recovery. The information includes explanation on the type of architectures used in this research, the theoretical architecture underpinning the research, the instruments adapted, and the process of data collection and analysis.

Chapter 4 presents the implementation design of all architectures and the proposed architecture for the organization.

Chapter 5 discusses the outcome and comparison of the proposed approach, which is the combination of multi side network RAID and backup method.

Chapter 6 the results of this research were concluded and future works were briefly discussed.

REFERENCES

Ahmed, M., Zahda, S., & Abbas, M. (2008). Server Consolidation Using OpenVZ: Performance evaluation. In Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference on (pp. 341-346). IEEE.

Aguilera, M. K., Keeton, K., Merchant, A., Muniswamy-Reddy, K. K., & Uysal, M. (2007). Improving Recoverability in Multi-Tier Storage Systems. In Dependable Systems and Networks, 2007. DSN'07. 37th Annual IEEE/IFIP International Conference on (pp. 677-686). IEEE.

Apparao, P., Iyer, R., Zhang, X., Newell, D., & Adelmeyer, T. (2008). Characterization & Analysis of a Server Consolidation Benchmark. In Proceedings of The Fourth ACM Sigplan/Sigops International Conference on Virtual Execution Environments (pp. 21-30). ACM.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud Computing And Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility. Future Generation Computer Systems, 25(6), 599-616.

Cherkasova, L., & Gardner, R. (2005). Measuring CPU Overhead for I/O Processing in the Xen Virtual Machine Monitor. In USENIX Annual Technical Conference, General Track (Vol. 50).

Crump, G. (2009). Five Questions to Ask in a Disk Array Data Replication Project. Retrieved from http://searchitchannel.techtarget.com/tip/Five-questions-to-ask-in-a-disk-array-data-replication-project?.

Curtis, P. W. (2012). Data Protection Strategies In Today's Data Center. Oracle Whitepaper. Retrieved from http://www.oracle.com/us/products/servers-storage/storage/truthinit-data-protection-wp-1535962.pdf

Gaonkar, S., Keeton, K., Merchant, A., & Sanders, W. H. (2010). Designing Dependable Storage Solutions for Shared Application Environments. Dependable and Secure Computing, IEEE Transactions on, 7(4), 366-380.

Goth, G. (2007). Virtualization: Old Technology Offers Huge New Potential. IEEE Distributed Systems Online, (2), 3.

Gupta, D., Gardner, R., & Cherkasova, L. (2005). Xenmon: Qos Monitoring and Performance Profiling Tool. Hewlett-Packard Labs, Tech. Rep. HPL-2005-187.

Gupta, D., Cherkasova, L., Gardner, R., & Vahdat, A. (2006). Enforcing Performance Isolation Across Virtual Machines in Xen. In Middleware 2006 (pp. 342-362). Springer Berlin Heidelberg.

HP (2009). Rethinking Server Virtualization Breaking Performance and Manageability Barriers, HP. Retrieved from www.hp.com/learn/storage.

HP (2011). Hp Enterprise Virtual Array Family with Vmware Vsphere 4.0, 4.1 and 5.0 Configuration Best Practices. Technical white paper. Retrieved from http://www.h20565.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c02018828.

HP (2009). Fundamentals of a Well-Built SAN. Retrieved from www.hp.com/go/P4000.

HP (2013). HP StoreVirtual Storage for Server and Client Virtualization with VMware vSphere. Retrieved from http://www8.hp.com/h20195/V2/

Harter, I. B. B., Schupke, D., Hoffmann, M., & Carle, G. (2014). Network Virtualization for Disaster Resilience of Cloud Services. Communications Magazine, IEEE, 52(12), 88-95.

Jian-hua, Z., & Nan, Z. (2011). Cloud Computing-Based Data Storage and Disaster Recovery. In Future Computer Science and Education (ICFCSE), 2011 International Conference on (pp. 629-632). IEEE.

Jin, H., Cao, W., Yuan, P., & Xie, X. (2008). VSCBenchmark: Benchmark for Dynamic Server Performance of Virtualization Technology. In Proceedings of the 1st International Forum on Next-Generation Multicore/Manycore Technologies (p. 5). ACM.

Kahane, Y., Neumann, S., & Tapiero, C. S. (1988). Computer Backup Pools, Disaster Recovery, and Default Risk. Communications of the ACM, 31(1), 78-83.

Keeton, K., Santos, C. A., Beyer, D., Chase, J. S., & Wilkes, J. (2004). Designing for Disasters. In FAST (Vol. 4, pp. 59-62).

Keeton, K. and Merchant, A. (2004) "A Framework for Evaluating Storage System Dependability," Proc. Intl. Conf. Dependable Systems and Networks (DSN '04), pp. 877-886, June 2004.

Kernsafe, 2011. iStorage Server iSCSI SAN for VMWare ESX Sever. Retrieved from http://www.kernsafe.com/white-papers/iscsi-san-for-vmware-esx-esxi-server.aspx.

Kim, S. K., Ma, S. Y., & Moon, J. (2015). A Novel Secure Architecture of the Virtualized Server System. The Journal of Supercomputing, 1-14.

Klein, B (2012). Leveraging the Cloud for Data Protection and Disaster Recovery. White Paper. Retrieved from http://www.cloudtss.com/content/Leveraging%20the%20Cloud%20for%20Data%20Protection%20and%20Disaster%20Recovery.pdf

Libre Solutions Pty Ltd (2013). Hardware RAID Disadvantages. Retrieved from http://raid6.com.au/posts/hardware_RAID_disadvantages/

Lin, Q., Qi, Z., Wu, J., Dong, Y., & Guan, H. (2012). Optimizing Virtual Machines Using Hybrid Virtualization. Journal of Systems and Software,85(11), 2593-2603.

M.F. Mergen, V. Uhlig, O. Krieger, J. Xenidis (2006). Virtualization for High-Performance Computing. ACM SIGOPS Operating Systems Review, 40 (2) , pp. 8–11.

Mikkilineni, R., & Kankanhalli, G. (2010). Using Virtualization to Prepare Your Data Center for "Real-Time Assurance of Business Continuity". In Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE), 2010 19th IEEE International Workshop on (pp. 76-81). IEEE.

NetApp SnapMirror (2012). Retrieved from www.symantec.com/business/support/resources/.../288533.pdf.

Padala, P., Zhu, X., Wang, Z., Singhal, S., & Shin, K. G. (2007). Performance Evaluation of Virtualization Technologies for Server Consolidation. HP Labs Tec. Report.

Parker, Donn B. Fighting Computer Crime: A New Framework for Protecting Information. John Wiley & Sons, Inc., 1998.

Rao, M & Gopal, M (2010). Using Virtualization to Prepare Your Data Center for “Real-time Assurance of Business Continuity”. 2010 Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises.

Roselinda R. S. (2004). Disaster Recovery Issues and Solutions A White Paper from Hitachi Data Systems.

Routray, A. V. K. V. R., & Jain, R. (2008). Sweeper: An Efficient Disaster Recovery Point Identification Mechanism.

Sengupta, S., & Annervaz, K. M. (2014). Multi-Site Data Distribution for Disaster Recovery - A Planning Framework. Future Generation Computer Systems, 41, 53-64.

Sindoori, R., Pallavi, V. P., & Abinaya, P. (2012). An Overview of Disaster Recovery in Virtualization Technology. J. Artificial Intelligence, 6, 60-67.

Tan, T., Simmonds, R., Arlt, B., Arlitt, M., & Walker, B. (2008). Image Management in a Virtualized Data Center. ACM SIGMETRICS Performance Evaluation Review, 36(2), 4-9.

Ta-Shma, P., Laden, G., Ben-Yehuda, M., & Factor, M. (2008). Virtual Machine Time Travel Using Continuous Data Protection and Checkpointing. ACM SIGOPS Operating Systems Review, 42(1), 127-134.

TechTerms. (2010). Definition of Anti-Virus. Retrieved from http://techterms.com/definition/antivirus

Trend Micro. (2012). Trend Micro Deep Security 8.0 Administrator Guide. (2012) Retrieved from http://downloadcenter.trendmicro.com/.

Trend Micro. (2009). Trend Micro Deep Security. A Trend Micro White Paper. Retrieved from http://la.trendmicro.com/media/wp/deep-security-whitepaper-en.pdf.

Van C. A., Pieters, W., & Wieringa, R. (2009). Security Implications Of Virtualization: A Literature Study. In Computational Science and Engineering, 2009. CSE'09. International Conference on (Vol. 3, pp. 353-358). IEEE.

VMWare. (2009). VMware Capacity Planner Optimize Business and IT Capacity Planning in your Data center and Desktop Environment. Retrieved from https://www.vmware.com/files/pdf/datasheet_capacity_planner.pdf.

VMWare (2009). User's Guide vCenter Converter Standalone 4.0.1. Retrieved from http://www.vmware.com/pdf/converter_standalone_guide401.pdf.

VMWare (2011). Distributed Resource Scheduler, Distributed Power Management. Retrieved from https://www.vmware.com/products/vsphere/features/drs-dpm

Voorsluys, W., Broberg, J., Venugopal, S., & Buyya, R. (2009). Cost of Virtual Machine Live Migration in Clouds: A Performance Evaluation. In Cloud Computing (pp. 254-265). Springer Berlin Heidelberg.

Wallace, M., & Webber, L. (2010). The Disaster Recovery Handbook: A Step-By-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets. AMACOM Div American Mgmt Assn.

Wei, X. (2011). Application of Server Virtualization Technology in Enterprise Information. In Internet Computing & Information Services (ICICIS), 2011 International Conference on (pp. 25-28). IEEE.

Weltzin, C., & Delgado, S. (2009). Using Virtualization to Reduce the Cost of Test. In 2009 IEEE AUTOTESTCON.

Whitehouse,L. (2011). Virtualization and Business Continuity using HP's Converged Storage to Develop/Enhance Business Resiliency in VMware Environments. Enterprise Strategy Group, Inc.

Wikipedia, 2011. BareMetal Restore. Retrieved from https://en.wikipedia.org/wiki/Bare-metal_restore#References.

Wood, T., Cherkasova, L., Ozonat, K., & Shenoy, P. (2008). Profiling and Modeling Resource Usage of Virtualized Applications. In Proceedings of the 9th ACM/IFIP/USENIX International Conference on Middleware (pp. 366-387). Springer-Verlag New York, Inc.

Yu, H., Xiang, X., Zhao, Y., & Zheng, W. (2014). Birds: a bare-metal recovery systemfor instant restoration of data services. *Computers, IEEE Transactions on*, *63*(6), 1392-1407.

Yuan, P., Huang, Y., Jin, H., & Cao, W. (2009). Evaluating dynamic performance of VMM in server consolidation. In Web Society, 2009. SWS'09. 1st IEEE Symposium on (pp. 81-85). IEEE.

Zahed, S. K., Rani, S. P., Saradhi, V. U., & Potluri, A. (2009). Reducing Storage Requirements of Snapshot Backups Based on Rsync Utility. In Communication Systems and Networks and Workshops, 2009. COMSNETS 2009. First International (pp. 1-2). IEEE.