An Overview of Disaster Recovery in Virtualization Technology

R. Sindoori, V. Preetha Pallavi and P. Abinaya
M. Tech Advanced Computing, SASTRA University, Thanjavur, India

Corresponding Author: R. Sindoori, M. Tech Advanced Computing, SASTRA University, Thanjavur, India
Tel: 9976844230

ABSTRACT
In IT Business organisations, accessing and maintaining of data plays a vital role. Data disaster will occur due to human prone and natural hazards, so disaster recovery is important for IT business. Virtualization is one of the best technologies for disaster recovery because of high resource utilization, high availability, ease of power management, recovery management and dynamic infrastructure. This study describes some disaster recovery mechanisms in major virtualization technologies such as VMware, Citrix, Microsoft, Oracle VM, and Parallel workstation.

Key words: Backup, hypervisor, migration, data recovery, virtual machines, snapshots, system isolation

INTRODUCTION
Virtualization is a software technique in which a single physical resource appears as multiple logical resources. Some of the advantages of virtualization are easier bare metal restores easier backup verification, backup usability, multiple backup methods, agent less, resource free backup, network free backup, easy snapshots, application item recovery. Disaster recovery is the process in which an organisation can recover the data after any catastrophic events occur.

Traditional method requires same hardware configuration, periodic management, high power and cooling costs. Traditional method create bottleneck and performance problem and take more time to complete. Application and data recovery through image tools and tape backups are complex and slow process. Traditional backup and recovery methods involves complex procedure operating system backup agents, scheduling and performing backups, restoring data, testing and verification of backups. Thus, it leads to high cost to manage these features.

Nowadays virtualization solutions decrease the customer burden by reducing the data center complexity, management, cost and providing dynamic, flexible access, energy, space efficiency, centralized management. Because of this, virtualization is 700-800% better than traditional method. Only 15-20% of IT workloads are virtualized for the past three years, but now that percentage increased to 50-60%. For example, 97 virtual servers can run on 3 physical machines, thereby it saves 97% reduction of physical server machines. Hence, it saves £20,000 per year by decreasing power consumption from 34 to 1.1 kWh.

There is an architecture Virtualization based Recovery Intrusion Tolerance (VRIT) for recovery which strengthens the cluster's availability, event driven and dependability through periodic. Deeper security and service was managed by this algorithm (Philpott, 2006). Encapsulate and shield distribution of collaborative manufacturing resources as service is done by this virtualization technology. This virtualization plays an important layer of cloud computing architecture.
The virtualization also plays important role in grid and distributed computing. Logical Petri Nets (LPNs) model is used in grid computing with virtualization which creates a single system image and implements virtual applications in the user level. It manages and monitoring the applications and mapping and allocate the resources (Du et al., 2006).

The best virtualization disaster recovery solutions will have the following features: full data protection, virtualization vendor support, and integration with virtualization management platform, easy installation and use, secured, flexible backup storage options, intended use of storage, live migration, and considerable cost. The data can be recovered after performing some essential tasks like Risk Assessment, Business Impact Analysis, Recovery Time Object (RTO) and Recovery Point Object (RPO). This study focusing on disaster recovery methods of three innovative virtualization technologies such as VMware, Citrix, and Microsoft.

VMWARE

VMware’s disaster recovery mechanisms are cost effective, fast and reliable. It is also applicable for tier 0, 1, 2 applications.

Core Properties of VMware

- **Partitioning**: Each system has ability to run multiple operating systems and applications; thereby it increases the server utilization. This decreases the cost and disaster recovery affordable
- **Hardware independence**: Here, virtual machines are run on any x86 systems without any modifications on host and remote system. Due to this, recovery can be done easily by system start up and configurations at problem area. It also avoids the necessity of identical systems and result in low cost
- **Encapsulation**: Encapsulation represents that the entire operating system data, application, images are transferred as a single file on disk and it is mobilable. There is no need for server migration, backup and recovery, replication. Instead of these processes, it can be carried out by data migration and file copy. Image tools and tape systems are also not necessary
- **Isolation**: Problems or instability in one virtual machine does not affect the other virtual machines in there same host

Physical recovery process versus virtual recovery process: Physical recovery process requires 40+hours to recover the entire applications and data. The steps involved are hardware configuration, OS installation, OS configuration, backup installation, and then automatic recovery. But, in virtual recovery process requires only 4 hours recovering the applications and data. Here, the steps involved are restore VM, power on VM. Because operating system files are stored in shared storage and it can be easily transformed to recovery site.

End to end disaster recovery solutions: VMware enables the organisation to perform backup and restore process are the foremost step for disaster recovery. For reliable recovery method, testing should be carried out periodically.

Backup and recovery for disaster recovery: The backup method involves image and file level backups, snapshots, consistent backup states, VCB and VStorage API, scheduling and performing
backups. For virtual machine backups, three methods are used and it depends on recovery and protection needs:

- Within a virtual machine
- VMware ESX server service console
- VMware consolidated backup

**Within a virtual machine:** The file level backup is done, when third party backup is run in a virtual machine with same configuration and procedure.

**VMware ESX Server service console:** The agent runs in the service console and it provides the full system image and it does not affect the applications run on the another virtual machines.

**VMware consolidated backup (VCB):** An IT organisation allows us to:

- Full image and file level backup of virtual machine in its running state for recovery files are also supported with VCB
- Improves managability by single agent on proxy server
- To reduce the backup traffic in the local area network, it is connected to tape based devices

**Testing disaster recovery to ensure high availability:** Without testing, there is no use for disaster recovery plan. Testing is simple and it should be managed periodically. The testing steps includes snapshot and to create test virtual machines cloning of replicated data is needed and connect it to isolated network, powering it up to evaluate recovery and deleting virtual machine clones after testing. Thus, this testing is method using in IT organisation due to simplicity and reliable nature.

**CITRIX XENSERVER**

In Citrix, XenServer provides the disaster recovery. It integrates the software and compresses it as a small stream file for backup. It will simultaneously takes backup and restore it for multiple virtual machines and its nodes in XenServer. It takes backup in remote device and manages it by the main enterprise management console.

**Xen backup recovery:** The Xen provides a single interface for XenServer backup capabilities. The solutions for backup are:

- Encryption capabilities
- Agent less technique
- Guest VSS
- Independent platform
- Enterprise management interface

**XenServer backup methods:** There are several methods in XenServer using guest virtual machine. They are as follows:
• Offline backup
• Online live memory backup
• Online quiesced backup
• Online normal backup

These methods are integrated and managed into a different platform, heterogeneous, centralized backup solutions:

• **Offline backup:** The offline backup takes place after the operating system shutdown. This offline back occurs only when there is no change in the virtual guest. But this backup solution does not fulfill the high availability requirements. It is independent of both operating system and applications. All data is in consistent state.

• **Online live memory backup:** It will perform the backup for guest virtual machine and its memory. This will take the backup of the current state of the memory. This will provide consistency. In this method the virtual machine is in “frozen” at the time of backup. The guest virtual machine is in lock state.

• **Online quiesced backup:** It will use the Citrix Xen tool for backup. The guest virtual machine is in active state when performing the backup. There is no down time required for this method. It takes the advantages of citrix VSS which provide consistent application backups but it gives only for windows. It takes the backup of virtual machine configuration, storage information and VIPs.

• **Online normal backup:** This method is also like quiesced method performs back up in active state but it does not use only tools. It will provide backup for any type of guest virtual machine operating system. There is no consistency for data in active memory.

**Agent less technique:** Due to the presence of the hypervisor, there is no need for agent. Whatever maybe the virtual guest containing operating system it supports the direct communication by using hypervisor. It analyse the operating system of virtual guest with the help of the citrix Xen tool. By using the snapshot detection technique, VSS snapshot detection is used in windows guest.

**Restore:** The restore takes place using the management interface. If the virtual machines are connected in network when there is no downtime occurs in Citrix XenServer. The virtual machine is restored in same or different location. It will restore like a snapshot at any time if the backup is available. The user may use same UID or new ID for restored virtual guest.

**Key products of disaster recovery:**

• Citrix access gateway
• Citrix password manager
• Citrix net scalar application delivery system
• Citrix secure gateway
• Citrix licence server
Advantages:

- Rapid access application and data using a standard web browser
- Security over the public internet
- Centralized control over end point
- "Shadowing" capability for remote technical support.
- Remote conferencing over the internet

MICROSOFT

Microsoft is one among the major virtualization vendors. The end to end disaster recovery solution is achieved through the below listed component they are:

- Windows server 2008 with Hyper-V
- Windows server failover clustering
- Microsoft system center virtual machine manager

Features of windows server with hyper-V: Hypervisor based technology in Microsoft which is bundled with windows server 2008 and comes under x64 operating system. Hyper-V provides the user to run multiple operating systems and providing maximum advantage in server hardware. Hyper v in Microsoft windows server enables some features which add credit to Microsoft virtualization. As Hyper-V is integrated with Microsoft windows server it avoids the enterprise to go for any other virtualization technology. And also it supports the symmetric multi processors. The main key of virtualization is high availability, windows server 2008 clustering support the high availability which reduces the unexpected down time.

The full fledged virtualization is live migration. Windows server 2008 makes the things simple for live migration from one virtual machine to another which will be pillar for the business continuity, volume shadow copy service support in windows server 2008 which enables the healthy storage backup of virtual machine. Other than these features it includes ease extensibility, integrated management.

Features of windows server failover clustering: Fail-over clustering offers the critical application and services like email, line of business whenever required. It enables the cluster to communicate to network router without connecting VLANs. In windows server fail-over clustering it enables the cluster for maximum distance coverage this enables the fast recovery and minimize the failure. It also uses same set of management for local cluster. When a complete site let to disaster it enables the automatic failover. It provides the mirror storage for long distance. It also offers the replication tool by smooth collision with hardware or software based data replication solution.

Features of system centre virtual machine manager: This feature enables to manage effectively for both physical and virtual environment. The features of system centre virtual machine manager are it manages both the Hyper-V and VMware ESX virtual environment. It manages the environment for both physical and virtual environment through single console the
power to influence performance and resource optimization. It also offers the original capability for live migration from physical to virtual similarly for virtual to virtual environment. And also it supports the failover and automation features. Depending on needs, it can be configured in many ways.

The combination of Hyper-V and windows server fail-over cluster reduces the hardware component failure by assigning the hardware failure virtual machine to another virtual machine. By using the above specified Microsoft virtualization component in Microsoft virtualization environment we can achieve the high availability, reduce the unexpected down time for user, live migration.

**COMPARISON OF VMWARE, XEN, MICROSOFT**

Table 1 compares some of the important features of three vendors. Guest OS licensing is included in Microsoft but it is licensed separately in VMware and Xen. In VMware, Storage VMotion allows the whole content migration, while in Microsoft Quick storage migration is allows the majority process but this is not available in Xen. Number of nodes in VMware is 32 but for Xen and Microsoft are 16. Integrated High Availability and snapshot are present in all the three technologies. VMware and Microsoft have a capability to restart automatically when VM is unresponsive but it is not in the case of Xen. Fault tolerance is occurred through 'shadow' secondary VM in VMware but not in other technologies. Site failover has to purchase separately in VMware, in Xen integrated disaster recovery (array storage control) is used, in Microsoft basic MS recovery is used. A Hypervisor upgrade is available in VMware and Microsoft, but it is limited in Xen through rolling pool upgrade wizard. The patching process is used in Microsoft but it is limited in VMware. It is not used in Xen. Snapshots play a vital role in three vendors. RAM size is maximum in VMware and minimum in Microsoft. Thus, the Table 1 compares some of the important features of three vendors.

Figure 1 represents the four parameter performance for five different vendors. The four parameters are consolidation, CPU performance, RAM capacity, and disaster recovery. Vmware is leading in all these parameters. Next to Vmware, Microsoft has higher values.

<table>
<thead>
<tr>
<th>Features</th>
<th>VMware</th>
<th>XEN</th>
<th>Microsoft</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest OS licensing</td>
<td>Not included</td>
<td>Not included</td>
<td>Yes</td>
</tr>
<tr>
<td>Storage migration</td>
<td>Yes</td>
<td>No</td>
<td>Limited</td>
</tr>
<tr>
<td>Number of nodes</td>
<td>32</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>Integrated HA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatic restart</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Fault tolerance</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Site failover</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Hypervisor upgrades</td>
<td>Yes</td>
<td>Limited</td>
<td>Yes</td>
</tr>
<tr>
<td>Patching</td>
<td>Limited</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Snapshot</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Maximum RAM per VM</td>
<td>1 TB</td>
<td>128 GB</td>
<td>64 GB</td>
</tr>
</tbody>
</table>
OTHER VENDORS

Some of the other vendors for virtualization technology are Oracle VM and Parallel workstation.

Oracle VM: In Oracle VM X-86 has architecture which includes design and process for disaster recovery. Disaster recovery requirements are calculated through RTO and RPO. It implies the concept of resource pool and it manages one or more clustered Oracle VM server by grouping it together. When it is created, it isolates and manages the virtual and physical resources. The resource pool can be copied from one site to another site for disaster recovery. For restoring process, same type of resources must be used. For consistent installation configuration using automated PXE boot configuration Oracle VM server is installed.

Oracle VM server 3.1 server virtualization is the newest technology of Oracle VM which has additional advantages compared to another technology. It has the capability to deploy both X-86-64 server and support wide range of storage and network devices. The key features are easy to use, support backup, hardware and application workloads. The key benefits are no licensing cost, free download. Thus, it helps the customer to achieve high availability and thereby it improves the performance and reduces the cost.

Parallel workstation: Parallel workstation is software product developed by Parallels, Inc. It also uses hypervisor, which forms a layer between OS and host computer. It is used to deploy faster desktops and protect from failure.

Parallels Virtuozzo container is OS virtualization, which creates separate partitions or virtual environments on a physical server. It enables continues data protection to assure disaster recovery through peer software products. It jobs is to monitor the virtual OS and provide replication for disaster recovery. This software is not tied to particular hard disk. When hard disk is seen as local drive by container, peer software has a capacity to read and monitor it.

In hardware virtualization, it consolidates servers to solve the cost of infrastructure and hardware, but it leads to a new problem called OS or VM sprawl. Thus, OS virtualization is used to solve the problem. Parallels Virtuozzo container can resolved this problem by using template based approach.
CONCLUSION

Thus, IT organisations enhance their business continuity by providing effective disaster recovery through virtualization technology. Virtualization is the essential technology for cloud computing. So the initial step to virtualize the most of the elements, which makes the disaster recovery in effective manner.

ACKNOWLEDGMENTS

We thank the anonymous reviewers for giving comments that helped to improve the study. We also thank Dr. N. Sairam, Professor, School of Computing, SASTRA University, Thanjavur for giving support to do this work.

REFERENCES