International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 4 Issue 5, May 2015

REPLICATION BASED DISASTER RECOVERY IN VIRTUAL MACHINES

Nethra H L
Dept. of CSE, CIT, Gubbi.

Prof. Shantala C P
Vice principal and HOD
Dept. of CSE, CIT, Gubbi.

***Abstract*:** Disaster means any event that brings down the system. Disasters may be human made or natural disasters. Human made disasters like power outage, cyber security attacks and when several people access some particular web site at the same time causes software corruption. Natural calamities like storm, cyclone, typhoon, earthquake, Tsunami and floods may cause hardware disasters in turn software also. When a physical server fails we can back up the data from virtual machines but what to do when virtual machines also goes down because although the virtual machine is decoupled from the hardware, it is still dependent on the working of the hardware. By having a replica of virtual machine we can get back our data and brings system back to normal working. Replication means copying data between two or more storages to prevent data loss in case of disasters. Replication can be synchronous or asynchronous. We are adopting asynchronous replication because it works over wide range.

Keywords: virtualization, virtual machine, disaster recovery, replication**.**

I. INTRODUCTION

Virtualization is a futuristic buzzword, broadly used in today's IT environment. Virtualization has a longer history, it was first developed in 1960's by IBM Corporation, originally to partition large mainframe computer into several logical instances and to run on single physical mainframe hardware as the host. Cause for inventing this feature was maintaining the larger mainframe computers became burdensome [1]. In today's new age of "always-on" business, prolonged downtime or even brief outages are no longer acceptable, all are expected to have their core information systems up and running all the time. Disaster Recovery has become an important part of today's computing world. Where, computing has now moved from physical servers to cloud and virtual machines (VM). Virtualization refers to the abstraction of computer resources means hiding the physical characteristics of computing resources from the way in which other systems, applications, or end users interact with those resources. By virtualizing the machine, we are able to run several operating systems (and all of their applications) at the same time. Virtual machine is representation of a real machine using software that provides an operating environment which can run or host a guest operating system [9] [10]. Virtualization is the foundation for all that is possible through the Cloud that is scalability, automation, and standardized services are all possible only because of underlying virtualization.

Disaster means any event, occurs suddenly and causes great loss to daily life, it also affect business. Disasters may be human made or natural disasters, human made, for example fire, power outage, cyber security attacks and when several people access some particular web site at the same time causes software corruption this also stops working of system. Natural calamities like storm, cyclone, typhoon, earthquake, Tsunami and floods may cause hardware disasters in turn software also. With the concept of Virtualization and virtual machine, if disaster occurs in physical machine we recover easily.

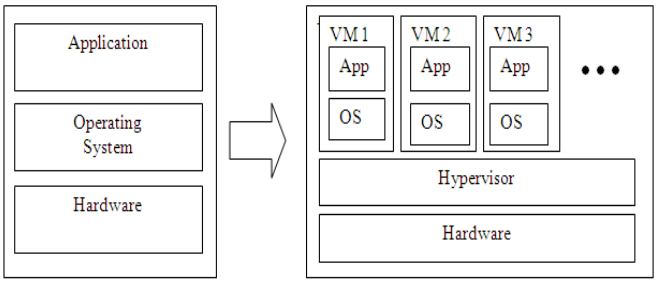

Fig .1 Physical to virtual machine

Having essential DR solutions on virtualized environment is the need because it is easier to build a virtual machine on a hypervisor than rebuilding a physical infra from the scratch in the event of failures. It adds higher operational and capital expenditures. But, the question is, how to recover virtual machine when it crashes. Disaster recovery solutions are essential to ensure business continuity and high availability. We are providing an automated disaster recovery solution that ensures that system is up and running by using replication and migration technique.

This paper presents a recovery solution for disaster occurred in virtual machine by means f natural or any man made. The report is organized as follows. Section 2 depicts the literature survey. Section 3 gives existing system, section 4 describes proposed system, section 5 is of implementation part, section 6 gives modules, section 7 gives advantages of proposed system, and section 8 concludes our work.

II. RELATED WORK

This section gives an overview on the context of our topic disaster recovery in virtual machine.

A. DISASTER RECOVERY

Disaster recovery is forecasting the process that protects and recovers the resources of the firm in the event of disaster. It ensures high availability and business continuity. The purpose of a disaster recovery is to begin again usual computing capabilities in as little time as possible.

The key requirements for an effective DR solution:

1. RTO (Recovery Time Object)
2. RPO (Recovery Point Object)

RTO (Recovery Time Object): The RTO is a business decision that specifies a bound on how long it can take for an application to come back online after a failure occurs. This includes the time to detect the failure, prepare any required servers in the backup site (virtual or physical), initialize the failed application, and perform the network reconfiguration required to reroute requests from the original site to the backup site so the application can be used. Having a very low RTO can enable business continuity.

RPO (Recovery Point Object): The RPO of a DR system represents the point in time of the most recent backup prior to any failure. The necessary RPO is generally a business decision—for some applications absolutely no data can be lost (RPO=0), requiring continuous synchronous replication to be used, while for other applications, the acceptable data loss could range from a few seconds to hours or even days.

B. HYPERVISOR

Hypervisor is also called virtual machine monitor (VMM). A hypervisor or virtual machine monitor (VMM) is a piece of computer software, hardware or firmware that creates and runs virtual machines. It generally provides partitioning capabilities. Virtual Machine Monitor is the heart of Virtual Machine technology. The Virtual Machine Monitor determines how to map virtual resources to physical resources [3].

There are two types of hypervisors:

Type 1: Native or bare metal Hypervisor

Hypervisors runs directly on the host's hardware. It controls the hardware and manages the guest OS. A guest OS thus runs on another level above the hypervisor.

Example: Hyper-v, VMware ESX/ESXi, XenServer.

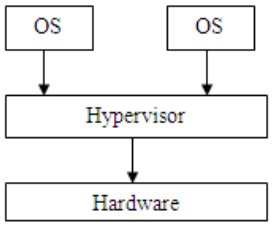

Fig 2. Type 1- Native or bare metal.

Type 2: Hosted Hypervisor

Hypervisor runs on Host OS. Hypervisor run within a conventional OS with Hypervisor layer as a distinct second software level.

Example: VMware workstation, Virtual Box, bhyve.

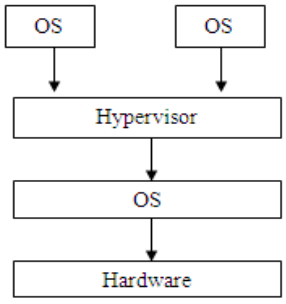

Fig 3. Type 2 - Hosted.

In our work we are using VMware vSphere hypervisor. It is also called ESX/ESXi. VMware vSphere replication is a virtual machine data protection and disaster recovery solution. It is fully integrated with VMware vCenter Server and VMware vSphere Web Client, providing host-based, asynchronous replication of virtual machines. VSphere Replication is a proprietary replication engine developed by
VMware [2].

C. REPLICATION

In general replication means creating a mirror image of the same i.e., duplication process. There are two types of replication [4].

1. Synchronous and
2. Asynchronous

Synchronous: Synchronous replication writes data to the primary and secondary sites at the same time so that the data remains current between sites. It works over distances up to 300 km.

Asynchronous: Asynchronous replication writes data to the primary storage array first and then to replication targets.

We are adopting asynchronous replication. Reasons for adopting asynchronous are its less costly than synchronous and it covers wide areas.

D. MIGRATION

The process of moving a virtual machine from one host to another host is referred as migration.

Migration can be divided into three phases [5]:

Push phase: The source VM continues running while certain pages are pushed across the network to the new destination. To ensure consistency, pages modified during this process must be resent.

Stop-and-copy phase: The source VM is stopped, pages are copied across to the destination VM, and then the new VM is started.

Pull phase: The new VM starts its execution and, if it accesses a page that has not yet been copied, this page is faulted in across the network from the source VM.

Most migration strategies select either one or two of the above phases. While the pre-copy approach combines push with stop-and-copy, the post-copy approach combines pull with stop-and-copy.

We are using live migration technique it involves migrating a virtual machine from one host to another while it is running.

III. EXISTING SYSTEM

In traditional server concept system administrators often talk about servers as a whole unit that includes the hardware, OS, storage, and applications.

Servers are often referred to by their function i.e. the Exchange server, the SQL server, the File server, etc. If the File server fills up, or the Exchange server becomes overtaxed, then the System administrators must add in a new server. Unless there are multiple servers, if a service experiences a hardware failure, then the service is down. System admin can implement clusters of servers to make them more faults tolerant. However, even clusters have limits on their scalability, and not all applications work in a clustered environment. But, virtual servers seek to encapsulate the server software away from the hardware and can be scaled out easily.

Drawbacks of this virtual machine concept are:

1) Potential Downtime and
2) Oversubscription.

Potential Downtime – it can be more difficult to reboot virtual machines in the event of a catastrophic hardware failure. Virtual machines can power on and off just as easily as a physical machine,

but a VM coming online from a host crash will need to wait for their physical infrastructure to boot, plus the time it takes for your virtual machines to boot.

Oversubscription – if you have 5 VMs using 2GB RAM running on a physical machine with 8GB RAM, you've oversubscribed that hardware.

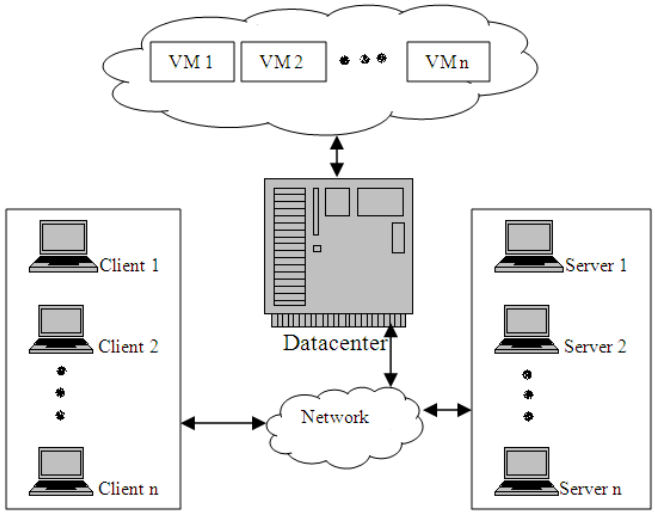

Fig 4. Existing system architecture

IV. PROPOSED SYSTEM

In this paper we are proposing a disaster recovery system that overcomes the disadvantage of existing system that is potential downtime. The architecture of the proposed system is shown in fig 5.

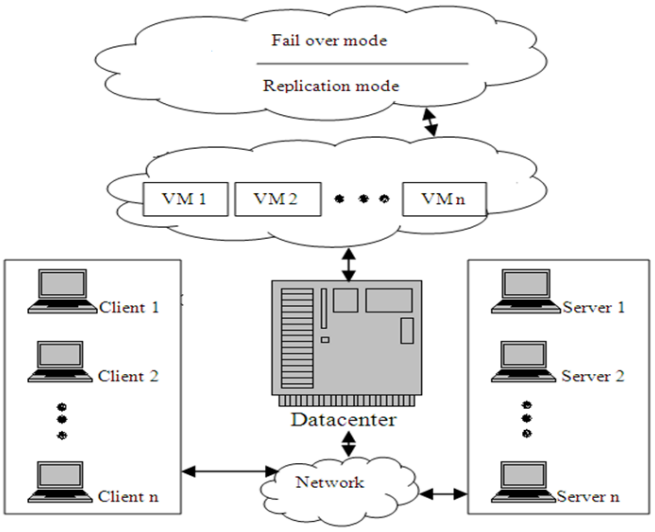

Fig 5. System architecture.

A virtual server can be serviced by one or more hosts, and one host may house more than one virtual server. Hosts may be introduced almost at will to accommodate maintenance. Virtual servers themselves can be migrated from one host to another host. In the architecture the data is replicated between primary and secondary sites. Virtual host and virtual machines are replicated to prevent data loss in case of failures. Here we are applying asynchronous replication and taking periodic snapshots to recover and provision the virtual machine and virtual host. There are two modes, failover mode and replication mode. In replication mode the virtual machines and the secondary sites are creating the replicas of primary site. If any disaster occurs in primary site and it goes down means it will switch to failover mode and then migrate the virtual host or virtual machine as needed. Suppose, while migrating the replica crashes means we will be having one more replica. So we will be having total of two replicas. To overcome potential downtime we adopted asynchronous replication and live migration techniques.

V. IMPLEMENTATION

The above said two modes that is replication and failover modes can be better understood by analyzing the below diagram.

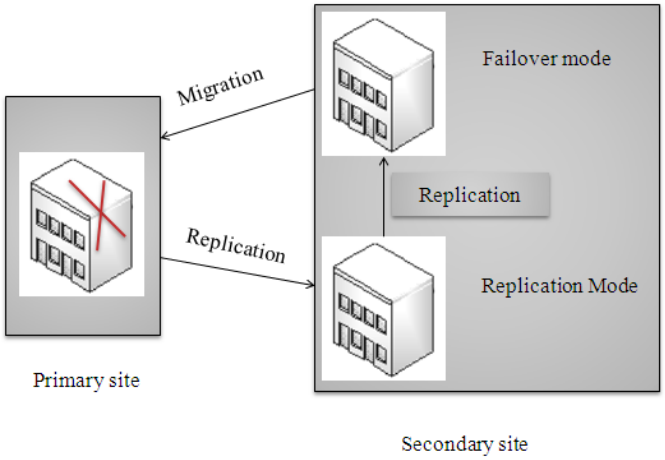

Fig 6. Site recovery

Key work flow:

1. Get the statistics of the virtual machines present in the data center.
2. Ping all the available virtual machines.
3. If VM responds to ping consider it to be alive if its not responding means consider it to be dead.
4. If VM is dead check weather it is powered off by the user, if so no action will be taken.
5. If the VM is dead because of disaster occurrence, check the virtual host containing to the VM is alive or not by sending the ping message.
6. If the vHost is alive make the VM alive by using snaphot.
7. If the vHost is dead try making it alive using the vHost snapshot.
8. Making vHost alive fails, check anyother vHost connected to that vHost.
9. If no such vHost is present, add new vHost make the VM alive.

By considering the below scenarios we can test and understand the working of the system [7]:

1. Scenario 1: vHost and VM are Running.
   Action: No action is performed by Health Manger.
2. Scenario 2: vHost is Running, VM is Down (i.e. not responding to ping)
   Action:
   a. First get the alarm status of VM.
   b. If user had shutdown the application, then no action is performed. However, if the machine was shut down because of failure, go to next step.

c. Check whether vHost is powered on and responding to ping
   - Yes- recover the VM using the replica of the VM.
   - No- Go to next scenario, to know the steps for vHost recovery.

3. Scenario 3: vHost is Down, VM is Down.
   Action:
   a. First gets the alarm status of the VM.
   b. If user had shutdown the application, then no action is performed. But, if the machine was shut down because of failure, go to next step.
   c. Check If vHost is powered on and responding to ping.
      - Yes- recover the vHost using the replica of the vHost.
      - No- Go to next step
   d. Try to make the vHost alive using vHost snapshot.
      - Successful- recover the VM using the snapshot.
      - Failed- Go to next step
   e. Check whether another vHost is alive and the current vHost is connected
      - Yes- recover the VM using he snapshot.
      - No- Add a new vHost and recover the VM using the snapshot.
   f. Check whether another vHost is alive and the current vHost is not connected
      - Yes- recover the VM using the snapshot and migration technique.
      - No- add a new vHost and recover the VM using by migrating the snapshot.

VI. MODULES

1. Availability Administrator (AA)

   In current solution, Availability administrator is responsible for getting the inventory list in terms of vHost and its VMs. Each VM is identified using a key value pair i.e. name and IP mapping, which is stored in distributed hash map. The VMs that do not have an IP assigned are not considered as a part of this solution. Once, the list of VMs present in the inventory is fetched, the AA does the primary task of spanning Health Administrator Thread for each virtual machine. It also spawns two more threads for virtual machine snapshot and vHost snapshot i.e. Snapshot Manager and Snapshot vHost Manager respectively.

   The AA also checks after a configurable interval of time if any new vHost and VMs are added. In scenarios, when new vHost and VM is added, a thread is spawned for the new VM only. This functionality is achieved using distributed hash map that keeps track of old and new VMs.

2. Health Administrator (HA)

   Health Administrator (HA) is the core for this project. It performs the following tasks:
   - Creates an alarm for the virtual machine using Ping Administrator. In case, an alarm is already present, the alarm is not created again.
   - Gather vital status of the virtual machine, such as I/O, CPU, Network and Storage.
   - Performs ping test on the Virtual Machine and vHost.
   - Checks Alarm status of the virtual machine.
   - Performs recovery and provisioning using Cloning with Snapshots and Cold Migration, depending on the failure scenario of vHost and VM.
   - Function to add a new vHost that is already present in the inventory, but not added to the vCenter.

   The Health Administrator thread is specific for each virtual machine and monitors the VM's health after every configurable amount of time.

3. Snapshot Creator (SC):

   Snapshot Creator is responsible for maintain the snapshot of the virtual machines. It performs two main functions:
   - Delete all previous snapshots (this is done to overcome resources constraints.)
   - Create a new snapshot

4. Snapshot Creator vHost (SCV)

   Snapshot Creator is responsible for maintain the snapshot of the vHost machines. It performs two main functions:
   - Delete all previous snapshots (this is done to overcome resources constraints.)
   - Create a new snapshot

5. Ping Administrator (PA)

   Alarm Manager is responsible for event and alarm management of the virtual machine. It performs the following tasks.
   - Create a new alarm for the VM
   - Check alarm state for the VM

6. Inventory Administrator

   Inventory Administrator is responsible for reading the configurable properties such as vCenter URL, username and password, sleep interval for monitoring the VM and managing the snapshot interval. It has been designed such that, even if during the program execution the property is changed, it is able to read the new values.

VII.ADVANTAGES

Like every system our proposed has advantages:

1. It ensures business continuity and access to data even in serious failure modes.
2. It can lower the operational and capital expenditures to disaster recovery.
3. This can be applied across any distance because we adopted asynchronous replication.
4. It is quite flexible, it allows to continuosly replicate the files that user thinks critical to business.

VIII. CONCLUSION AND FUTURE WORK

The proposed disaster recovery system ensures business continuity and high availability. It allows applications to rapidly come back online after a failure occurs. Minimizes the RTO , RPO and potential downtime. Reduces the data lost due to disaster and also the CAP and OP expenditures.

Future work involves expanding the technique to datacenter now its limited to only for VM and vHost. And also to take meaures to remove zombie and orphan VMs these are of no use but acquired system resources.

ACKNOWLEDGEMENT

We are pleased to acknowledge all who supported our work. Am very thankful to my guide Prof. Shantala C P, vice principal and HOD of dept. CSE, CIT Gubbi. And and all the authors of the papers i have reffered. Thank you one and all.

REFERENCES

[1] "*VM AND THE VM COMMUNITY: Past, Present, and Future*", Melinda Varian.
[2] "VMware vSphere Replication 6.0" TECHNICAL OVERVI EW REVI S E D FEB RUARY 2015.
[3] "*Virtual Machine (Google/image)*", Dongpu Jin, University of Nebraska-Lincoln.
[4] http://www.computerweekly.com/answer/Synchronous-vs-asynchronous-replication-Order-of-events-during-data-writes
[5] *"A Brief Tutorial on Live Virtual Machine Migration From a Security Perspective",* Diego Perez-Botero.
[6] "*Disaster Recovery as a Cloud Service: Economic Benefits & Deployment Challenges*" Timothy Wood, Emmanuel Cecchet, K.K. Ramakrishnany, Prashant Shenoy, Jacobus van der Merwey, and Arun Venkataramani.
[7] http://www.slideshare.net/akshaywattal/disaster-recovery-solution-for-vmware-vcenter-vhost-and-vms
[8] Project report document.
[9] *"Survey of Server Virtualization",* Radhwan Y Ameen, Asmaa Y. Hamo. (IJCSIS) International Journal of Computer Science and information Security, Vol.11, No. 3, 2013.
[10] *"Virtualization Concepts and Applications",* YashJain, DA-IICT (DCOM Research Group).

