CHAPTER – 3

Methodologies

The main goal of my project is to implement and test failover and load balancing using a highly available clustered environment with respect to hardware and applications by using Oracle Linux Servers, Linux virtual machines, OHS (HTTP) Server, Hardware Load Balancer (BigIp) and Database.

3.1 Objective

This chapter will explain the methodologies used, including the hardware, software, design and analysis and validation methodology.

Review all the previous work done in the field of high availability clustered and virtualization and then develop an experimental testing alternate highly available clustered virtual environment with more advantages. Do the validation with native approach to validate the setup and then analyze the results[7].

So, I have formalized three objectives and going to use them throughout the project –

1) Review previous works.

2) Developed and test experimental solution.

3) Analyze the system and results.

So, the different phases are:-

1) Phase I   - Proof of technology

2) Phase II  - Discovery / Recommendations

3) Phase III - Pilot

4) Phase IV  - Production
3.2 Shared Storage System

Below is the example of shared storage in virtual environment.

![Shared Storage System Diagram](image)

For all nodes, disk images are stored in shared location which is available for all of the physical nodes. This will allow all the physical nodes to run all of the virtual machines and because of this the live migration of services is possible. In this example we have nine virtual machines running on three physical servers and sharing the same shared storage.

Virtual machine runs on a hypervisor layer on each of the physical host which allows virtual machines to migrate to different node in case of failure of that particular node.

The main requirement for this live migration of services is, all nodes should share the same storage area where all the file system and data partition resides[7][8].

Virtual machine running on a physical system can be decoupled anytime and the services of that particular machine will takeover by the other system on same cluster. Even a physical machine can be decoupled from the cluster physical
machines and the corresponding virtual machines will be failover to the other physical systems in the same cluster.

In case of failure of one of the physical system the virtual systems of that physical will be unaffected and will migrate to other physical machines on the same cluster.

By developing this kind of system we hope that we can create a alternate solution for the application or services to achieve failover capabilities with redundant low cost and efficient solution. To achieve this automated failover capabilities there is a term called heartbeat is there, all the machines in the cluster will talk with each other by sending heartbeat or called a signal to ensure his availability, in case any of the server missed to send heartbeat the other servers will take that server as failed and will automatically migrate the services of that system to other available clustered system.

![Diagram of resource sharing](image.png)

Resource Sharing

**Fig 2**

Hardware like cpu, memory, nic and disk space distributed between the number of virtual machines hosted by that particular server. As shown in fig 3.2.b, physical server hosting the two virtual machines having own virtual hardware. There should be a hypervisor layer between physical server and virtual machines which act as mediator between them.
3.3 Hardware, Software and Tools

3.3.1 Hardware

I have done all my experiments using the standard X86 Oracle Linux servers because they are globally used by all of the organizations in the market as well as fully certified by the Oracle itself for virtualization.

All machines are connected using the APAC power distribution unit which makes it possible to remotely control the servers in case of failure. I can able to start and stop the server without knowingly the physical location of the servers.

All testing equipment is almost resemblance to the equipments we used in the production environment and if got success then we can implement the same solution to the production without introducing any new technology or equipment[9].

3.3.2 Hardware Architecture of Testing Machines

Two Oracle Enterprises Linux Servers (X86)

Each one with configuration:-

1) 16GB of RAM
2) Multiprocessors (Total 12)
3) 2 NIC Cards
4) 500GB of disk space
The main requirement of the live application migration is the share storage for the application binaries and data which is shared between all physical machines so the 500 GB of storage has been shared between both physical machine using NFS.

Since storage is shared, so the necessary components need to failover during migration is cpu, memory and user connection states.

3.3.3 VMware vSphere Hypervisor ( ESXi )

VMware vsphere hypervisor is based on VMware ESXi, it's a solution to virtualized a physical node in different virtual machines. It allows you to create and run a virtual machine from scratch in minutes and make it operational.

Installed on both of the physical servers and each of the physical server distributed in two virtual machines so all in four virtual machines on two physical hosts.

3.3.4 Software’s

Database

Oracle 11.2.0.2

Database is the main important part of any business environment. It's used to the physical data of any organization. I have used oracle database version 11.2.0.2 [10].

Application Server

Oracle Weblogic Server 11G

Weblogic server is the Java J2EE based application servers.
**OHS (HTTP) Server**

Oracle OHS server

It’s a oracle web server just like attaché http server

**Hardware Load Balancer**

BigIP

It’s a hardware load balancer tool from F5.

**Development Software**

Developed in java J2EE and deployed on weblogic application server.

### 3.3.5 Testing Environment Setup

Fig 4 shows the architecture setup for the test of failover & load balancing testing on the LAB environment.

![Load Balancing and Failover Setup](image)
There were four virtual machines and out of four, two machines exist in the DMZ public zone and the other two machines exist in the private internal zone.

Database has been installed on two different virtual machines as a RAC (Real Application Cluster) setup.

Weblogic server, OHS server installed on both internal machines and only OHS server installed on the DMZ zone machines.

Under weblogic server, created four clustered managed servers on which deployed the web portal application. So total we have eight managed servers where we have equally deployed the web portal application.

Two hardware load balancers are there, one at the public zone level and other one at internal zone level.

Deployed application will access from the internet via DMZ zone load balancer and internally from the internal hardware load balancer.

OHS server from the public machines will redirect the request to the internal servers and for that need to open the ports at firewall between DMZ and private zone.

Internal load balancer will redirect the requests to one of the internal OHS server and OHS server redirect to the managed servers where application were deployed.

At last, request to access portal will redirect to any one of the managed server out of the eight.
3.3.6 Failure

As discussed earlier, all the servers in the cluster communicate with each other by using the heartbeat mechanism and the same mechanism used to know the shutdown or crashed events. In case of failure of a machine failover happened when other machines in the cluster are not able to listen the heartbeat of the crashed server[11].

With respect to the failures in terms of the heartbeats, we can divided the failure in two major category –

1) Planned or Graceful
2) Unplanned or Uncontrolled

And each outage can be due to any of the below factor

1) Software ( Application )
2) Hardware ( Machines and operating systems )

A planned outage which is pre planned and decided by the management on specific day and time, in that case during of planned outage applications are failover to the secondary available environment to continue the business activity.

An unplanned outage which is not pre planned and caused by due to failover of either hardware or software. This directly related with the ETA (estimated recovery time ) and financial implications to the organization according to the service level agreement signed with the customer.

There is a connection between outages type and the cause of outages like planned outages can be due to Software or Hardware or unplanned outages can be due to Software or Hardware failure[12].
3.3.7 Validation Methodology

3.3.7.1 Validation Using OHS (Oracle HTTP Server)

Load balancing testing carried out at the first entry point called Oracle HTTP server (OHS).

Hardware load balancer were configure in conjunction with OHS server where –

1) Any request will come to the public zone bigip should forward to any one of the public zone MT OHS servers and further ohs servers should forward request to any one of the managed servers.

2) Any request will come to the internal bigip should forward to any one of the internal MT OHS servers and further ohs servers should forward request to any one of the managed servers.
Fig 5

Configuration on httpd.conf on HTTP server –

```xml
<IfModule weblogic_module>
  Debug OFF
  WLLogFile /tmp/ohs.log
  WebLogicCluster
    DynamicServerList Off
    MatchExpression /portal/*
  </IfModule>

<Location /console24>
  SetHandler weblogic-handler
  WebLogicCluster xyzabcd24.mukeshnegi.com:40010
</Location>

<Location /console26>
  SetHandler weblogic-handler
  WebLogicCluster xyzabcd26.mukeshnegi.com:40010
</Location>

3.3.7.2 Validations Using Weblogic Server & Access Logs
DMZ (Public Zone)

Request was distributed from hardware load balancer any one of the OHS server in dmz zone and from OHS server to any one of the internal managed server among eight managed servers. If there is firewall then internal managed server ports need to be open from public zone to internal servers. Once the request full, the portal page will display to the end user. To avoid extra burden on the network, SSL configured at bigip (hardware load balancer) level[12].

![Public DMZ Zone](image)

DMZ (Public) Zone

Fig 6

Internal Zone

Fig 7 represents the internal architecture where request from internet will come to internal OHS server via firewall and from internal OHS will be redirect to internal managed servers via another firewall.

![Internal Zone](image)

Internal (Private) Zone with firewall

Fig 7
3.3.7.3 Validations Using JMETER

Validating the proper load balancing is yet another typical and important part. If you will not be able to judge load balancing properly then your system is not perfect.

Jmeter is a openly available tool for the load balancing testing and can be integrate with any application server with web server features as well with any of the web server. You application either can deploy on application server or can place on web server in case of some static or dynamic contents only.

During testing, you need to provide the context of your application including the server ip or dns and the port on which your web or application server is running or either it will take default 80 in case of nonssl and 443 in case of ssl[13][14].

![HTTP Proxy Server]

Http proxy server

Fig 8
Once the server, port and context information provided, you can hit the number of physical requests to the ohs server, which will further redirect request to the designated managed servers where your application were deployed and you can verify if proper load balancing is working or not under sufficient load of the requests.

### 3.3.7.4 Virtual Machine Fault Tolerance Testing

VMWare fault tolerance provides you the high availability by running a parallel virtual machine to take over the services from primary machine just in case of the failure of that machine.

The reason behind the failure is same as when machines in the cluster not able to communicate with each other.

Below three scenarios may occur:

**Deterministic Scenario**

1) ESX host failure which would cause complete host failure.
2) Any of the primary server process will be unresponsive.

**Reactionary Scenario**

1) Communication of NIC may be interrupted
2) Communication of NIC may be slow

**No Action Taken scenario**

Where failover not happened because of FT cannot monitor such type of events

- Interruption or failure of management network
- Interruption or failure of virtual machine network
- HBA failures that do not affect the entire host
Any n number of combinations of all of the above

To test FT failover, the synchronization between primary and secondary machine must fail. There is a inbuilt functionality added with the VMware to test the fault tolerance failover[15].

3.3.7.5 VMware High Availability (VMHA) Test

VMHA (virtual machine high availability) allow virtual machine migration from one machine to other in case of failover of a machine.

You have to perform few steps or need to configure few things before you test and implement the VMHA.

1) You need vmware enterprises suite
2) 2 ESX host servers
3) Shared storage between both two servers to store the data.
4) You need to make sure cpu compatibility also between the machines.

To test it, use VMotion of a machine from one to other, Fig 3.3.7.5.a showing the results.
Test VM High Availability – Machine Failover

Create a new cluster

HA cluster

Give a name to the cluster and choose option VMWare HA
Do the optional configuration

Add the servers to the cluster
Before failover primary machine was on esx4

When I had shutdown primary machine then I saw Win2008 failover to esx3
Fig 15