Academic Year: 2022-23
Semester: VIII
Class / Branch: BE- IT
Subject: Cloud Computing Lab
Name of Instructor: Yaminee Patil

Name of Student:
Student ID:
Roll No.:
Date of Submission:

Experiment No.:02.

Aim: To create and execute Bare-metal Virtualization using Xen, HyperV or VMware Esxi.

Software Used: Virtual Box.

Theory:

Bare-metal hypervisor

A bare-metal hypervisor, also known as a Type 1 hypervisor, is virtualization software that has been installed directly onto the computing hardware.
This type of hypervisor controls not only the hardware, but one or more guest operating systems (OSes). In comparison, a hosted hypervisor, or Type 2 hypervisor, runs within the host OS, so the underlying hardware is managed by the host OS.
Bare-metal hypervisors feature high availability and resource management; they also provide better performance, scalability and stability because of their direct access to the hardware. On the other hand, the built-in device drivers can limit hardware support.
Examples of popular bare-metal hypervisors are Microsoft Hyper-V, Citrix XenServer and VMware ESXi.

What is the difference between bare-metal and hosted hypervisors?

A bare-metal or Type 1 hypervisor is significantly different from a hosted or Type 2 hypervisor. Although both are capable of hosting virtual machines (VMs), a hosted hypervisor runs on top of a parent OS, whereas a bare-metal hypervisor is installed directly onto the server hardware. This difference in the way that the hypervisors are installed leads to several other key differences.

One of the biggest differences between a bare-metal hypervisor and a hosted hypervisor lies in the way that VMs consume hardware resources. Because a bare-metal hypervisor is installed directly on the server hardware, a VM can access the hardware directly. Conversely, a VM that is running on a hosted hypervisor must pass hardware requests through the parent OS. This means that a bare-metal hypervisor generally offers far better VM performance than a hosted hypervisor.

Similarly, a bare-metal hypervisor offers better security than a hosted hypervisor. Because a hosted hypervisor is dependent on an underlying OS, security vulnerabilities within that OS could potentially be used to penetrate VMs and the guest OSes running on them.

Bare-metal hypervisor use cases

Bare-metal hypervisors are best suited for organizations that require high performance, management capabilities, scalability and strong security.

As bare-metal hypervisor is installed directly on the server hardware the VMs run at the hardware's native speed, as opposed to having their performance affected by an OS that is running on the host.

Bare-metal hypervisors also tend to be more scalable than hosted hypervisors. Hosted hypervisors' scalability is limited by the underlying OS. If the OS doesn't support clustering or if it only supports a relatively small amount of memory, then a hypervisor running on top of the OS will also be subject to those limitations. Because bare-metal hypervisors aren't installed on top of a host OS, they tend to be highly scalable.

The bare-metal hypervisor vendors also generally offer a management console that is designed to support large-scale hypervisor deployments. Some examples are VMware vCenter Server or Microsoft System Center Virtual Machine Manager. These consoles make it practical to manage large-scale deployments.

Finally, because a bare-metal hypervisor isn't running on top of an underlying OS, it tends to be far more secure than a hosted hypervisor.

Bare-metal virtualization is ideally suited to large organizations or to those organizations with significant performance or security requirements. Hosted hypervisors tend to be a better fit for lab environments or for use in SMB environments.

Benefits and drawbacks of bare-metal hypervisors

Like any other technology, there are benefits and drawbacks to bare-metal virtualization. These include:

Benefits

1. Performance: VMs can run at native hardware speeds.
2. Security: VMs aren't affected by vulnerabilities that might exist in an underlying OS, as would be the case for a hosted hypervisor.
3. Scalability: Enterprise grade bare-metal hypervisors support the creation of large failover clusters, and can generally take advantage of all a server's hardware resources -- memory, CPU, etc.
4. Manageability: Bare-metal hypervisor vendors offer management consoles that enable virtualization hosts to be collectively managed through a single console.

Drawbacks

1. Cost: Bare-metal hypervisors tend to be significantly more expensive than hosted

hypervisors. They also require dedicated hardware.

2. Complexity: Enterprise class bare-metal hypervisors can be quite complex and there might be a substantial learning curve associated with their use.

Top bare-metal hypervisor vendors and products

There are several major vendors that produce bare-metal hypervisors. Here are some of the leading bare-metal hypervisors:

- Citrix XenServer
- Linux KVM
- Microsoft Hyper-V
- Nutanix AHV
- VMware ESXi

Xen

Xen is an open source hypervisor based on paravirtualization. It is the most popular application of paravirtualization. Xen has been extended to compatible with full virtualization using hardware-assisted virtualization. It enables high performance to execute guest operating system. This is probably done by removing the performance loss while executing the instructions requiring significant handling and by modifying portion of the guest operating system executed by Xen, with reference to the execution of such instructions. Hence this especially support x86, which is the most used architecture on commodity machines and servers.

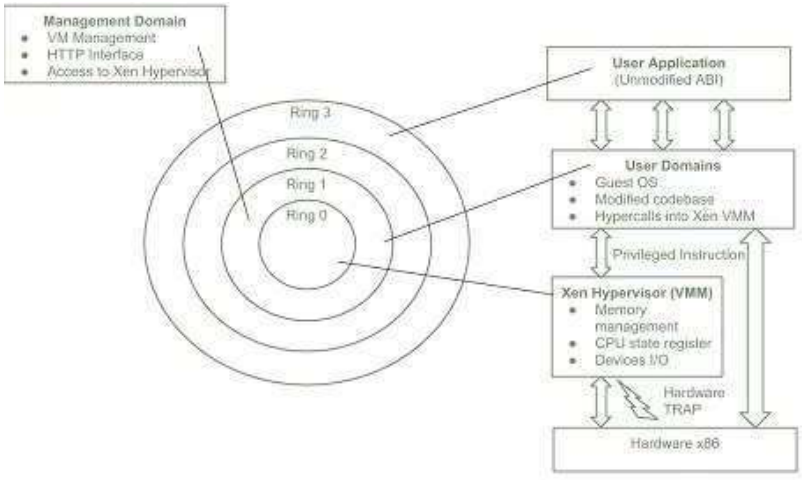


Figure – Xen Architecture and Guest OSnManagement

Above figure describes the Xen Architecture and its mapping onto a classic x86 privilege model. A Xen based system is handled by Xen hypervisor, which is executed in the most privileged mode and maintains the access of guest operating system to the basic hardware. Guest operating system are run between domains, which represents virtual machine instances.

Installation of Citrix Xenserver 6.5 Guide

1. The first step in the installation is to download the **XenServer ISO** file. This can easily be accomplished by visiting the link above or using the '**wget**' utility on a Linux system.

wget -c
http://downloadns.citrix.com.edgesuite.net/10175/XenServer-6.5.0-xenserver.org-install-cd.iso

Now burn the ISO to a CD or using '**dd**' to copy the ISO to a flash drive.

dd if=XenServer-6.5.0-xenserver.org-install-cd.iso of=</path/to/usb/drive>

2. Now place the media into the system that **XenServer** will be installed and boot to that media. Upon successful boot the user should be greeted by the wonderful **Citrix XenServer** boot splash.

XenServer Boot Menu

3. At this point simply press **enter** to begin the booting process. This will boot the user into the XenServer installer. The first screen will ask the user to provide a **language** selection.

Select XenServer Installation Language

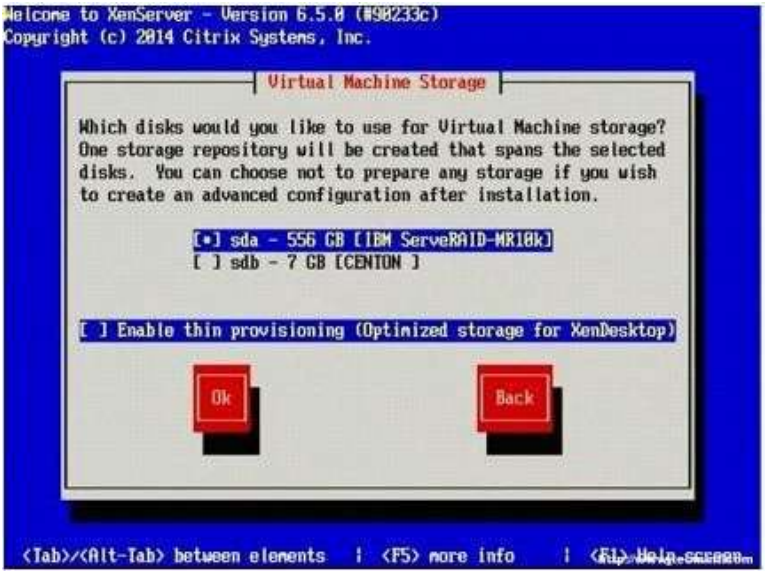
4. The next screen asks the user to confirm the reason for booting to this media as well as provide the option to load extra hardware drivers if needed. In this particular case, it is to install XenServer to the machine so it is safe to click "**OK**".

Load XenServer Device Driver

5. The next prompt is the obligatory **EULA** (End User License Agreement). Feel free to read the whole thing, as your supposed to anyways right, otherwise using the keyboard arrows move the cursor over to the "**Accept EULA**" button and hit enter.

Accept License Agreement

6. The next screen requests the installation device. In this example the **RAID** setup onthe server is where XenServer will be installed.
The **RAID** system is reflected as "**sda – 556 GB [IBM ServeRAID-MR10k]**" For this guide, thin provisioning is not necessary. Make sure the the asterisk **(*)** character is next to the hard drive selection to install XenServer and tab to the "**OK**" button.



Select XenServer Virtual Machine Storage

7. The next screen will prompt the user for the location of the installation files. Since the installer was boot locally with a CD/DVD/USB, make sure to select the "**Local Media**" option.

Select XenServer Installation Source

8. The next step allows for the installation of **Supplemental Packs** (SP) at the time of install. For this guide, none of the supplemental packs available will be installed at this point but will be covered later once XenServer is up and running.

Select Supplemental Packs

9. The next screen will ask if the user wishes to verify that the installer media is not corrupt. Generally, this is a good idea but is a personal choice. All in all the verification on this test server took about 3 minutes from a CD.

Verify XenServer Installation Media

Checking Base Pack

Verification Successful

10. Once the verification is completed, if selected during install, the XenServer installer will ask the user to setup some system information.

The first prompt will be to set the root user's password. Now, since XenServer will be the underlying system to potentially several important virtualized servers, it is imperative that the password be secured as well as sufficiently complex!

Important: Do not forget this password either as there will not be any other users on the system once the installer finishes!

Set XenServer Root Password

11. The next screen will ask the user to chose a management interface. The number of interfaces that shows up will vary from system to system and the management interface doesn't have to be a separate interface. A separate interface can be used to secure administrative access to the hypervisor itself.

12. Once the management interface is selected, the system will prompt for how to obtain an IP address for the management interface. This step will obviously vary from site to site as well.

Set XenServer IP Address

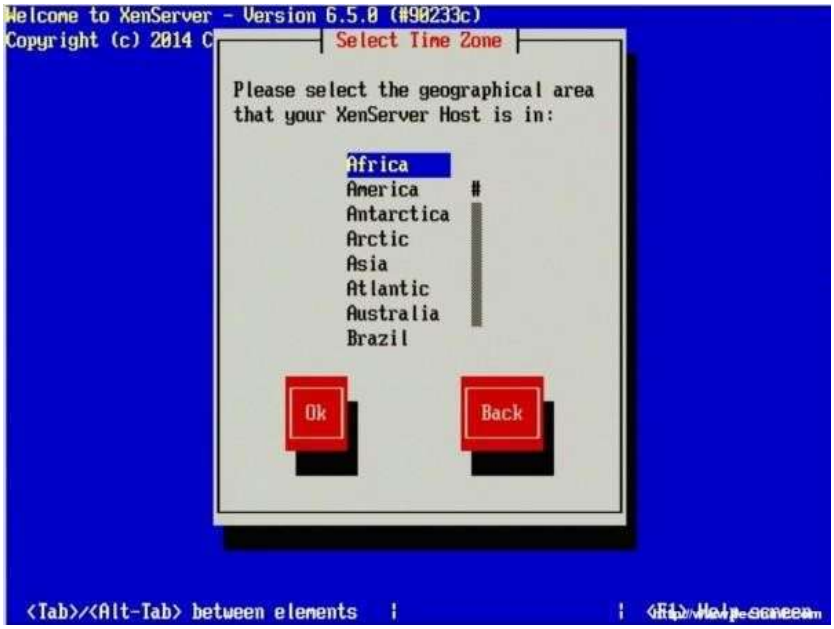
13. After determining the IP address information for the XenServer, the system will ask for a

hostname to be set as well as **DNS** server configuration.

Hostname and DNS Configuration

14. The next three screens will go through the steps of setting up time zones as well as the method for keeping track of time. Generally, **Network Time Protocol** is suggested for keeping system time synchronized on systems but again this will vary from location to location.

If a network time server isn't available or the XenServer doesn't have access to the Internet time servers, the installer will allow for manual time setting.



Set Time Zone

Add NTP Servers

15. At this point all of the initial configuration parameters will be complete and the XenServer installer will be ready to begin the installation of the hypervisor.

WARNING – Continuing at this point **WILL ERASE ALL DATA** on the target disks!

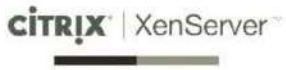
Confirm XenServer Installation Drive

16. The installation will take some time but a progress bar will be displayed. Once the installer is done, it will prompt the user to restart the system to boot to the newly installed hypervisor (be sure to remove the XenServer installation disk upon reboot).

Preparing XenServer Installation

XenServer Installation Complete

17. Upon removing the installation media and rebooting the system, the user should be presented with the **Citrix XenServer** splash page. Allow the system to continue booting.



Citrix XenServer Booting

18. Once the booting has completed, the system will present the **XenServer control** page.

XenServer Configuration Page

XenServer was successfully installed and is now ready to have any hotfixes/supplemental packs applied, storage repositories designated, and ultimately virtual machines created. The next step in this series will address the methods available to patch a XenServer system with patches from Citrix.

Conclusion: Thus, we have successfully implemented Hosted Virtualization using KVM