



Bharatiya Vidya Bhavan's
SARDAR PATEL INSTITUTE OF TECHNOLOGY
(Autonomous Institute Affiliated to Mumbai University)
Munshi Nagar, Andheri (West), Mumbai-400058
Information Technology Department

Academic Year: 2022-2023


Class: TE Sem.: VI

Name	Prathamesh Rajan Pawar
UID	2020400040
Course	Cloud Computing
Lab	1

Objective : Install Virtual machine and run Ubuntu & Windows on virtual machine

1. Ubuntu 22.04 Steps

Create Virtual Machine



Unattended Guest OS Install Setup

You can configure the unattended guest OS install by modifying username, password, and hostname. Additionally you can enable guest additions install. For Microsoft Windows guests it is possible to provide a product key.

Username and Password

Username: prathamesh

Password: ●●●●

Repeat Password: ●●●●

Additional Options

Product Key: #####-#####-#####-#####-;

Hostname: Ubuntu

Domain Name: myguest.virtualbox.org

☐ Install in Background

☐ Guest Additions

Guest Additions ISO: C:\Program Files\Oracle\VirtualBox\VBBoxGuestAdditions.iso


Help

Back

Next

Cancel

Create Virtual Machine



Hardware

You can modify virtual machine's hardware by changing amount of RAM and virtual CPU count. Enabling EFI is also possible.

Base Memory: 2048 MB

Processors: 1

☐ Enable EFI (special OSes only)

Help

Back

Next

Cancel

Create Virtual Machine

Virtual Hard disk

If you wish you can add a virtual hard disk to the new machine. You can either create a new hard disk file or select an existing one. Alternatively you can create a virtual machine without a virtual hard disk.

☒ Create a Virtual Hard Disk Now

Disk Size:
10.20 GB

☐ Pre-allocate Full Size

☐ Use an Existing Virtual Hard Disk File

☐ Do Not Add a Virtual Hard Disk

Help

Back

Next

Cancel

General

Name: Ubuntu
Operating System: Ubuntu (64-bit)

System

Base Memory: 2048 MB
Boot Order: Hard Disk, Optical, Floppy
Acceleration: Nested Paging, KVM Paravirtualization

Display

Video Memory: 16 MB
Graphics Controller: VMSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: IDE
IDE Secondary Device 0: [Optical Drive] Unattended-e5ad803d-e590-4823-8e36-61968e5e8ee9-aux-iso.iso (0 B)
Controller: SATA
SATA Port 0: Ubuntu.vdi (Normal, 10.20 GB)

Audio

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

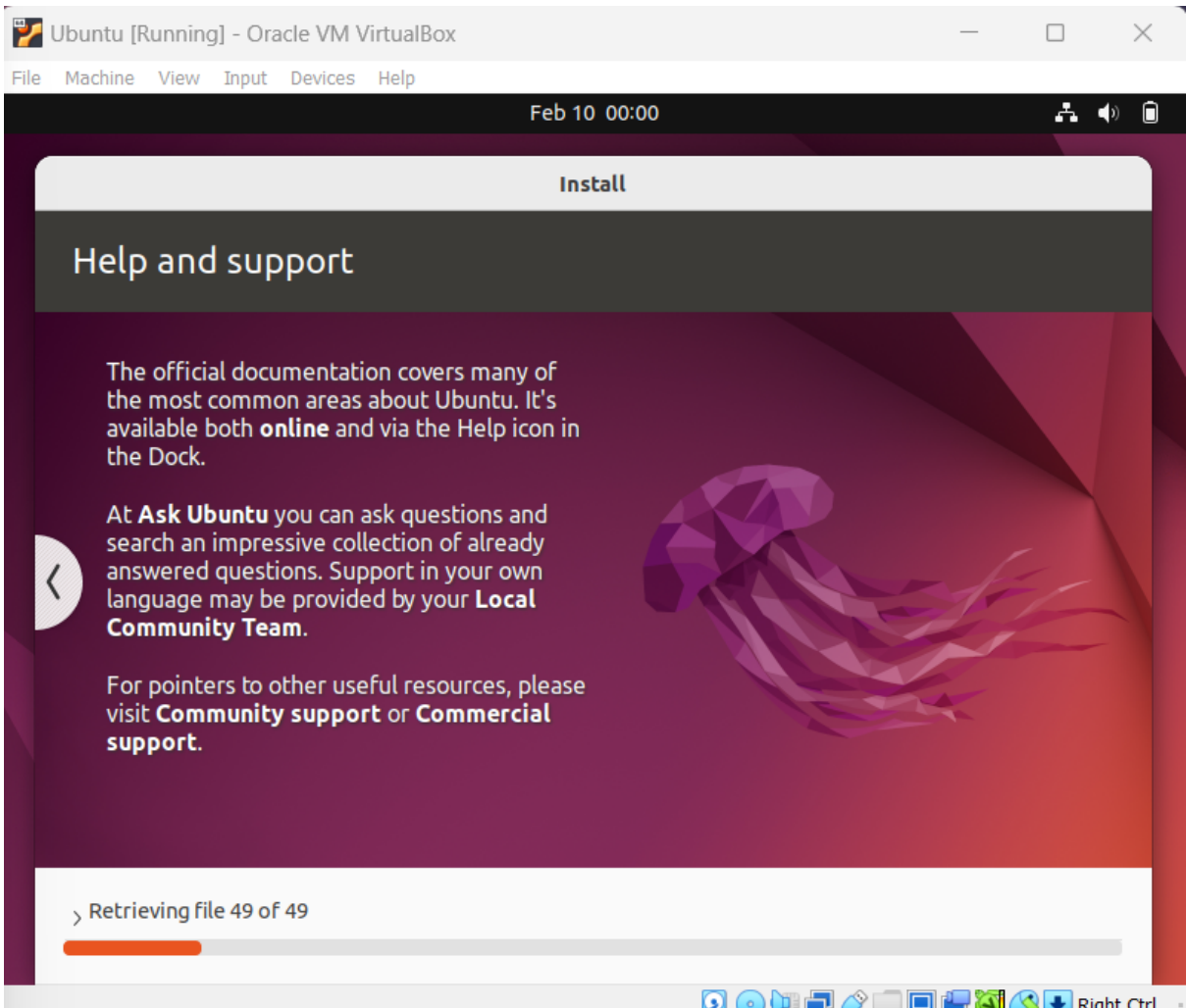
Shared folders

None

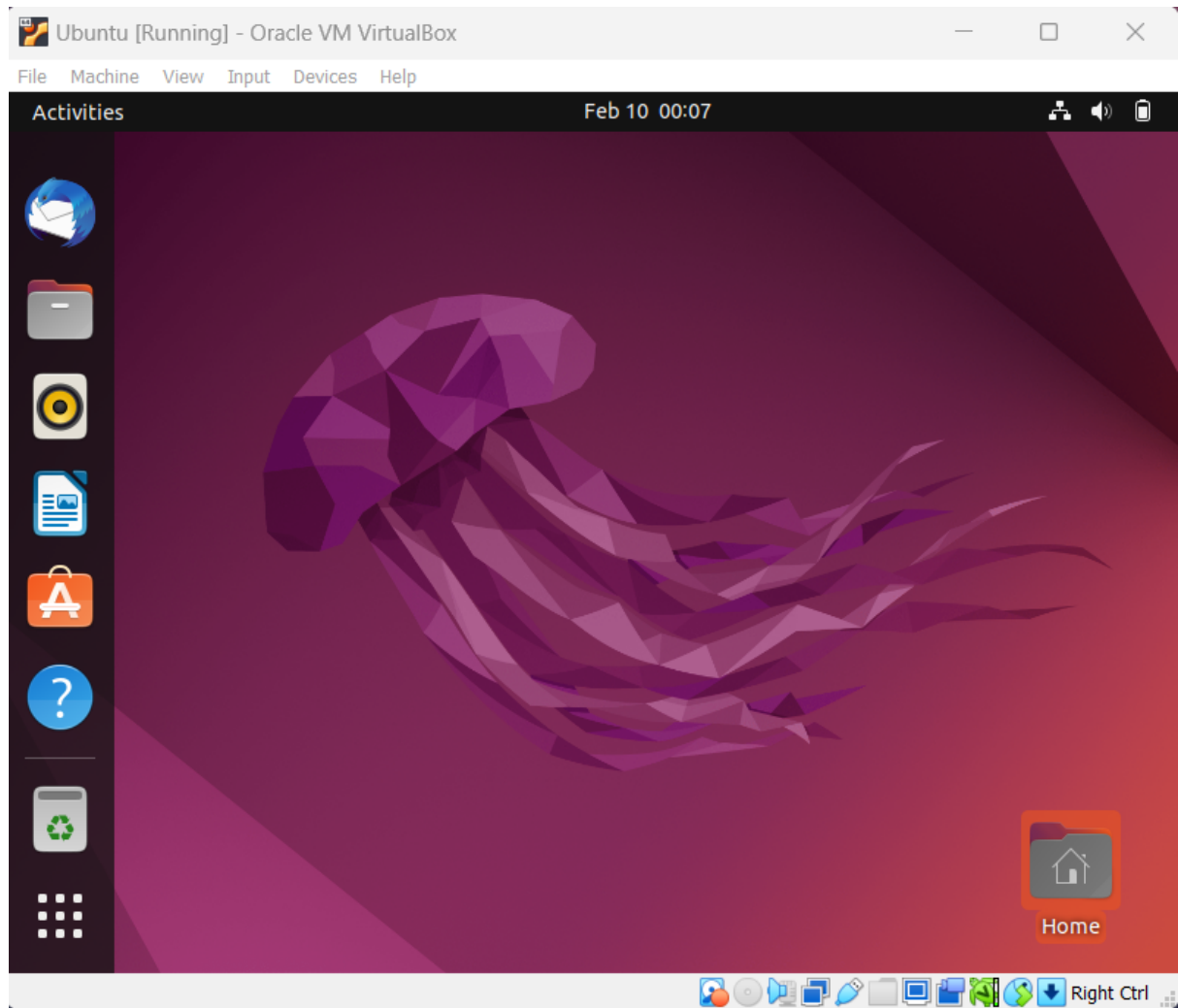
Description

None







Preview

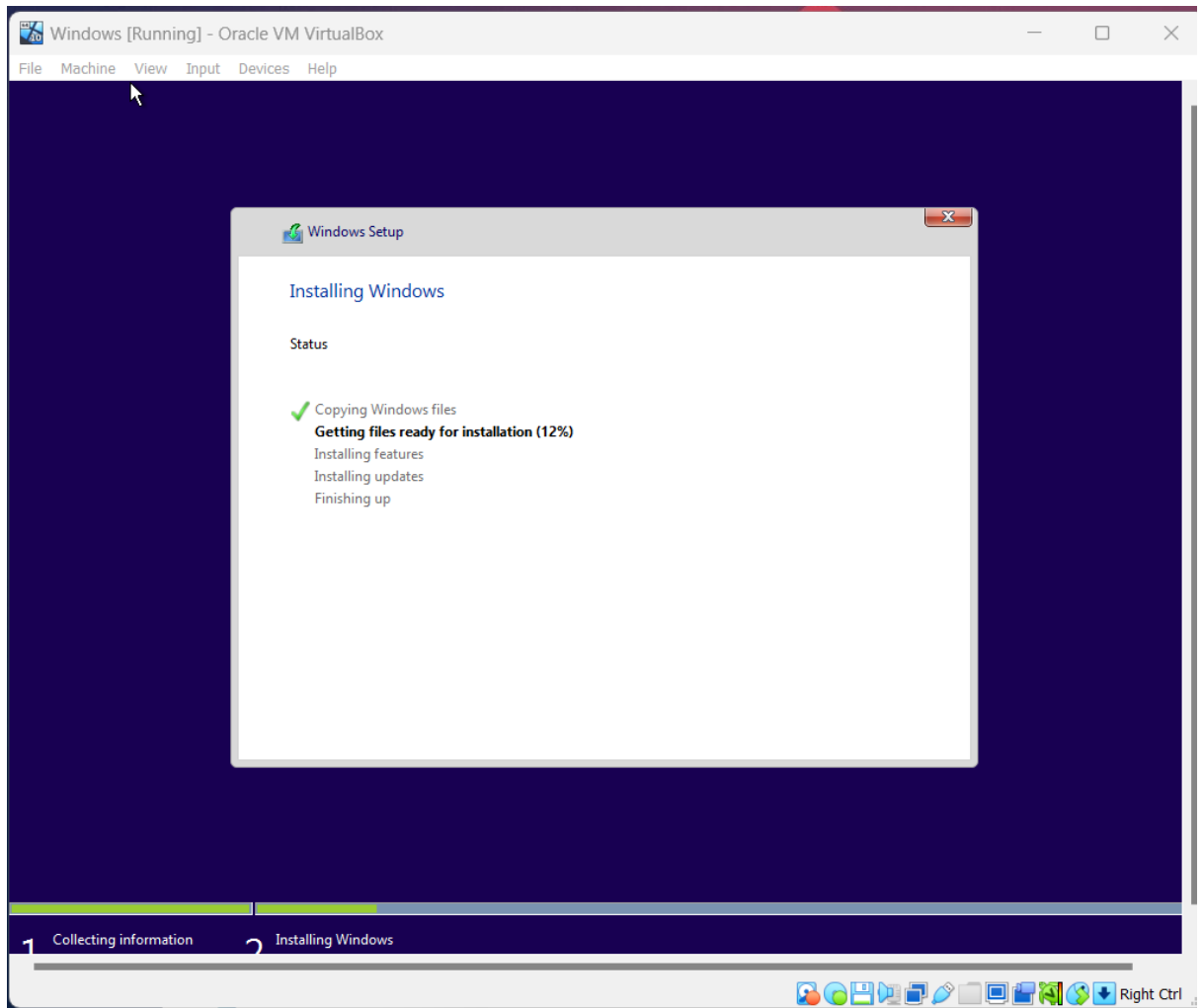


Running Ubuntu 22.04 on Oracle VM virtualbox

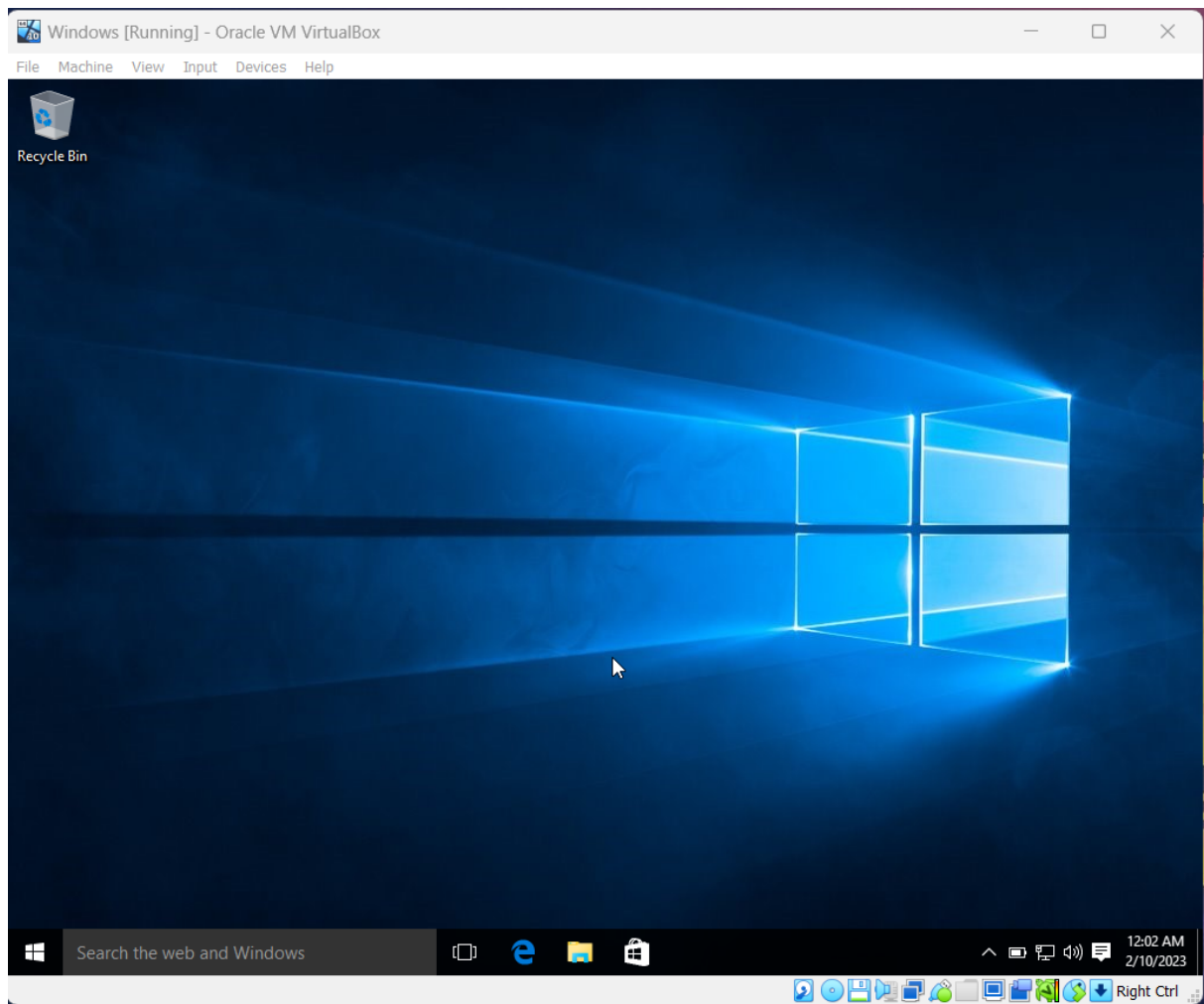


2. Windows steps

    	
General	Preview
Name: Windows Operating System: Windows 10 (64-bit)	
System	
Base Memory: 2048 MB Boot Order: Hard Disk, Optical, Floppy Acceleration: Nested Paging, Hyper-V Paravirtualization	
Display	
Video Memory: 128 MB Graphics Controller: VBoxSVGA Remote Desktop Server: Disabled Recording: Disabled	
Storage	
Controller: SATA SATA Port 0: Windows.vdi (Normal, 50.00 GB) SATA Port 1: [Optical Drive] en_windows_10_multiple_editions_x64_dvd_6846432.iso (3.80 GB) Controller: Floppy Floppy Device 0: Unattended-e808a006-97e4-45e1-9472-3ec1a86c9297-aux-floppy.img (1.41 MB)	
Audio	
Host Driver: Default Controller: Intel HD Audio	
Network	
Adapter 1: Intel PRO/1000 MT Desktop (NAT)	
USB	
USB Controller: xHCI Device Filters: 0 (0 active)	
Shared folders	
None	
Description	
None	



Running Windows 10 on oracle VM virtualbox



Question & Answers

1. Why does an organization use a hypervisor?

An organization may use a hypervisor, also known as a virtual machine manager, for several reasons, including:

- **Server Consolidation:** By creating virtual machines, a hypervisor can enable multiple virtual servers to run on a single physical server, increasing the utilization of hardware resources and reducing hardware costs.
- **Improved Resource Allocation:** A hypervisor can help manage and allocate hardware resources (such as CPU, memory, and storage) more effectively, so that each virtual machine gets the resources it needs to run efficiently.
- **Improved Availability:** By using a hypervisor to create virtual machines, organizations can improve the availability of their services. For example, if one virtual machine experiences an issue, the others can continue to operate normally, reducing downtime and improving overall reliability.
- **Improved Security:** A hypervisor can be used to isolate virtual machines from each other, reducing the risk of a security breach spreading from one virtual machine to another.
- **Easy Deployment and Management:** Hypervisors provide a centralized management console for virtual machines, making it easy for administrators to deploy new virtual machines, manage existing ones, and monitor overall system performance.

In summary, a hypervisor provides an organization with the ability to virtualize their computing infrastructure, enabling them to improve resource utilization, increase availability, improve security, and make deployment and management easier.

2. What is Full and Para virtualization? Which is better? Why?

Full virtualization and Paravirtualization are two methods of virtualizing computer systems, specifically virtualizing operating systems.

Full virtualization provides a completely isolated environment for a guest operating system, allowing it to run as if it were on its own physical hardware. The virtualization software provides virtual versions of all the physical hardware components to the guest operating system, including a virtual CPU, memory, storage, network interface, etc. This means that the guest operating system can run any operating system or application without modification, as if it were installed on a physical machine.

Para-virtualization, on the other hand, involves the guest operating system being modified to run in a virtual environment. The guest operating system is aware that it is running in a virtual environment and communicates with the virtualization software to access the underlying physical resources. Para-virtualization is typically faster and more efficient than full virtualization, as the guest operating system can make direct use of the physical resources, bypassing the virtualization layer.

It is difficult to say which method is "better" as it depends on the specific use case. Full virtualization is better suited for environments where it is important to maintain compatibility with existing operating systems and applications, as no modification is required. Para-virtualization is better suited for environments where performance is a concern, such as high-performance computing or big data processing, as the direct access to physical resources results in lower overhead.

Ultimately, the choice between full virtualization and paravirtualization will depend on the specific requirements of the virtualization deployment, including performance, compatibility, and ease of management.

3. How does cloud computing relate to virtualization?

- Cloud computing and virtualization are closely related concepts in the field of computing. Virtualization provides a layer of abstraction between a physical server and its operating system, allowing multiple virtual machines to run on the same physical hardware. This enables greater resource utilization, easier management of IT infrastructure, and better scalability.
- Cloud computing builds upon the foundation of virtualization to deliver computing resources as a service over the internet. In a cloud computing environment, virtualized computing resources, such as virtual machines, storage, and network bandwidth, are made available to users on-demand. This enables organizations to dynamically allocate and scale computing resources as needed, without the need to invest in and maintain their own physical infrastructure.

Therefore, virtualization is a key component of cloud computing, as it enables the pooling and allocation of physical resources in a dynamic and scalable manner. This allows cloud service providers to offer their customers the ability to easily provision and manage virtualized computing resources on an as-needed basis.

4. What's the difference between Type 1 and Type 2 hypervisors?

Feature	Type 1 Hypervisor	Type 2 Hypervisor
Location	Runs directly on host's physical hardware	Runs as software application on top of host operating system
Hardware Access	Direct access to host's physical resources	Access to physical resources through host operating system
Security	High	Low
Performance	High	Low
Examples	VMware ESXi, Microsoft Hyper-V, Xen	VMware Workstation, Oracle VirtualBox, Parallels Desktop

5. Give examples of commercial hypervisors available today?

- Microsoft Hyper-V: A Type 1 hypervisor from Microsoft, which is integrated into Windows Server operating system.
- Citrix Hypervisor: A Type 1 hypervisor from Citrix, which provides virtualization solutions for enterprise-level applications.
- Oracle VM Server: A Type 1 hypervisor from Oracle, which is designed for use with Oracle's enterprise-level applications.
- KVM: A Type 1 hypervisor that is open-source and included in the Linux kernel, providing virtualization for Linux systems.
- VMware Workstation: A Type 2 hypervisor from VMware, which allows users to run multiple virtual machines on a single physical machine.
- Oracle VirtualBox: A Type 2 hypervisor from Oracle, which is popular for use in testing and development environments.
- VMware ESXi: A Type 1 hypervisor from VMware, one of the leading companies in the virtualization market.

These are some of the most widely used commercial hypervisors

6. Can you name some free or open source hypervisors?

Here are some popular free and open-source hypervisors:

- **KVM (Kernel-based Virtual Machine):** An open-source Type 1 hypervisor that is included in the Linux kernel and provides virtualization for Linux systems.
- **Xen:** An open-source Type 1 hypervisor that provides virtualization for multiple operating systems, including Linux, Windows, and Unix.
- **VirtualBox:** An open-source Type 2 hypervisor developed by Oracle that allows users to run multiple virtual machines on a single physical machine.
- **QEMU:** An open-source hypervisor that can be used as a standalone virtualization solution or as a component in other virtualization solutions.
- **libvirt:** An open-source virtualization management library that supports multiple hypervisors, including KVM, Xen, and QEMU.

These open-source hypervisors provide an alternative to commercial hypervisors and can be a cost-effective solution for small to medium-sized virtualization deployments. They also offer a large community of users and developers, which can provide support and resources for deployment and management.

7. Is it possible to run multiple instances of an OS on more than one physical machine? If yes, how?

Yes, it is possible to run multiple instances of an operating system on more than one physical machine. This is achieved through the use of a technology called "clustering". Clustering involves grouping multiple physical machines together to form a single, unified computing resource.

The operating system instances running on each physical machine are coordinated so that they appear to be running on a single, virtual machine. In this way, multiple instances of an operating system can run on multiple physical machines, providing improved reliability, availability, and scalability.

There are several methods to implement clustering, including:

- **Network Load Balancing (NLB):** A Microsoft technology that allows multiple instances of an operating system to run on multiple physical machines, with traffic to the virtual machines distributed across the physical machines.
- **Heartbeat and failover:** A method that uses a software component to monitor the health of the virtual machines and automatically fail over to another physical machine in the event of a failure.
- **Distributed Resource Scheduler (DRS):** A VMware technology that automatically distributes workloads across multiple physical machines in a virtualized environment.
- **Grid computing:** A method of clustering that allows multiple instances of an operating system to work together to solve complex problems, with workloads divided across multiple physical machines.

8. Is it possible to create backups of running VMs? If yes, then how?

Yes, it is possible to create backups of running virtual machines (VMs). There are several methods for creating backups of running VMs, including:

Snapshotting: This method involves taking a point-in-time "snapshot" of the virtual machine's disk image, which can then be used to revert the virtual machine to that state in the event of a failure.

- **Backup and restore:** This method involves creating a backup of the virtual machine's disk image and configuration, which can then be used to restore the virtual machine in the event of a failure.
- **Replication:** This method involves creating a duplicate of the virtual machine and keeping it updated in real-time, so that the duplicate can be used in the event of a failure.
- Each of these methods has its own advantages and disadvantages, and the specific method used will depend on the requirements of the virtualization deployment. For example, snapshotting is quick and easy to perform, but may not capture all of the data that is necessary for a full restore. Backup and restore provides a complete backup of the virtual machine, but can take longer to perform and may require more storage space. Replication provides real-time protection, but can be resource-intensive and may impact the performance of the virtual machines.

Most hypervisors and virtualization management platforms provide tools for creating backups of running VMs, and there are also many third-party backup and recovery solutions available that are specifically designed for use with virtual environments.

9. Give me some examples of real-time scenarios where virtualization makes sense?

Virtualization is a powerful technology that can bring many benefits to an organization, including improved resource utilization, reduced costs, and increased flexibility and scalability. Here are some real-world scenarios where virtualization makes sense:

- **Server consolidation:** When an organization has many underutilized servers, virtualization can be used to consolidate multiple physical servers onto a smaller number of more powerful physical servers, reducing the cost and complexity of server management.
- **Test and development environments:** Virtualization can be used to create isolated test and development environments that are separate from production environments. This allows developers to test their code and configurations without risking harm to the production environment.
- **Disaster recovery:** Virtualization can be used to create disaster recovery solutions that allow an organization to quickly recover from a disaster by starting virtual machines on alternative physical servers.
- **Application isolation:** Virtualization can be used to isolate different applications from each other, providing security and stability benefits.

- **Cloud computing:** Virtualization is the foundation of cloud computing, allowing cloud providers to offer multiple virtual machines to multiple customers on shared physical resources.
- **Business continuity:** Virtualization can be used to provide business continuity by allowing virtual machines to be quickly moved from one physical server to another in the event of a failure.

10. What are the advantages and disadvantages of using third-party software like Puppet or Ansible over native virtualization solutions provided by VMware or Microsoft?

Third-party software like Puppet and Ansible provide a number of advantages and disadvantages when compared to native virtualization solutions provided by VMware and Microsoft.

Advantages of third-party software:

- **Flexibility:** Third-party software like Puppet and Ansible can be used to automate tasks across a variety of operating systems, hypervisors, and cloud platforms, making them more flexible than native virtualization solutions that are tied to a specific vendor's technology.
- **Customizability:** Third-party software is often more customizable than native virtualization solutions, allowing administrators to tailor the automation and management process to meet the specific needs of their environment.
- **Cost:** Third-party software is often less expensive than native virtualization solutions, particularly for smaller organizations.

Disadvantages of third-party software:

- **Learning curve:** Third-party software can require a significant investment in time and resources to learn and implement, particularly for organizations that are already familiar with native virtualization solutions.
- **Integration challenges:** Third-party software may not integrate as smoothly with existing virtualization solutions and management tools, leading to compatibility and interoperability issues.
- **Support:** Third-party software may have limited support and documentation compared to native virtualization solutions, which are supported by the vendor.

Ultimately, the choice between using third-party software like Puppet and Ansible, or native virtualization solutions like those provided by VMware and Microsoft, will depend on the specific needs and resources of the organization.

Organizations that are already familiar with native virtualization solutions and are looking for a cost-effective solution may find that third-party software provides a good alternative, while organizations that require a high level of integration and support may be better served by native virtualization solutions.

11. What are the security issues associated with virtualization?

Virtualization brings many benefits to organizations, but it also introduces a number of security risks that must be carefully managed. Some of the key security issues associated with virtualization include:

- **Hypervisor security:** The hypervisor is the core component of virtualization and must be carefully secured to prevent unauthorized access or tampering. This includes securing the hypervisor against attacks such as malware or malicious code that could be used to compromise the virtual environment.
- **Virtual machine isolation:** Virtual machines must be isolated from each other to prevent security breaches. If one virtual machine is compromised, it must not be able to access or compromise other virtual machines or the physical host.
- **Network security:** Virtual networks must be carefully managed to prevent unauthorized access and to ensure that data transmitted between virtual machines is protected. This includes securing virtual switches, virtual network adapters, and virtual network segments.
- **Storage security:** Virtual storage solutions must be secured to prevent unauthorized access to virtual disk images and to ensure that data stored in the virtual environment is protected.
- **Patch management:** Virtual environments must be kept up-to-date with the latest security patches and updates to prevent security breaches. This includes ensuring that the hypervisor, virtual machines, and associated software are all patched and updated regularly.
- **Insider threat:** Virtual environments must be protected against insider threats, such as employees or contractors who have access to virtual resources and could potentially misuse or compromise them.

By carefully managing these security risks, organizations can reduce the likelihood of a security breach in their virtual environment and ensure that their virtual infrastructure is secure and reliable.

12. What are some ways to ensure high availability of virtual machines?

High availability of virtual machines is important for ensuring that business-critical applications and services are always available to users, even in the event of hardware failures or other disruptions. Some of the key strategies for ensuring high availability of virtual machines include:

- **Redundant hardware:** This involves using redundant components such as redundant power supplies, network adapters, and storage to ensure that virtual machines remain available even if one component fails.
- **Live migration:** This involves moving running virtual machines from one physical host to another without any downtime, which can help ensure that virtual machines remain available even if a host fails.

- **Load balancing:** This involves distributing workloads across multiple virtual machines to ensure that resources are used efficiently and to reduce the risk of a single virtual machine becoming a bottleneck.
- **Clustering:** This involves grouping virtual machines together in a cluster, so that if one virtual machine fails, another can take over its workload automatically.
- **Backups and snapshots:** Regularly creating backups and snapshots of virtual machines can help ensure that the virtual environment can be quickly restored in the event of a failure.
- **Monitoring and alerting:** Monitoring the virtual environment and setting up alerts can help quickly identify any issues and resolve them before they become major disruptions.

By implementing these and other high availability strategies, organizations can ensure that their virtual machines remain available and that their business-critical applications and services are always accessible to users.

13. How does virtualization affect performance?

Virtualization can have both positive and negative effects on performance, depending on various factors such as the hardware resources available, the workload being run, and the virtualization technology being used. Some of the key ways in which virtualization can affect performance include:

- **Overhead:** Virtualization introduces overhead due to the extra layer of abstraction between the physical hardware and the virtual environment. This overhead can result in slower performance compared to running applications directly on physical hardware.
- **Resource contention:** Virtual environments can compete for physical resources such as CPU, memory, and storage, which can result in resource contention and reduced performance.
- **Network performance:** Virtual networks can introduce network overhead and latency compared to physical networks, which can affect network performance.
- **I/O performance:** Virtual environments can also introduce I/O overhead, especially when accessing virtual storage, which can result in reduced I/O performance.

However, virtualization can also bring performance benefits, such as:

- **Resource utilization:** Virtual environments can help to better utilize hardware resources, which can result in improved performance compared to underutilized physical servers.
- **Scalability:** Virtual environments can be easily scaled up or down to meet changing workload demands, which can result in improved performance compared to physical environments that are more difficult to scale.
- **Isolation:** Virtual environments can be isolated from each other, which can result in improved performance compared to physical environments where applications can interfere with each other.

14. Difference between docker and VM?

Docker and Virtual Machines (VMs) are both virtualization technologies, but they differ in several key ways.

- **Abstraction level:** Docker provides operating-system-level virtualization, whereas VMs provide full virtualization, including a separate operating system for each VM.
- **Resource utilization:** Docker containers share the host operating system and can run multiple containers on a single host, making them more lightweight and efficient with regards to resource utilization compared to VMs.
- **Portability:** Docker containers are designed to be highly portable, allowing them to be easily moved from one host to another, whereas VMs can be more challenging to move between hosts due to differences in hardware and software configurations.
- **Isolation:** Docker containers are isolated from each other and from the host operating system, but they do not provide the same level of isolation as VMs, which are completely isolated from each other and from the host.
- **Scalability:** Docker containers can be easily scaled up or down, whereas VMs can be more challenging to scale due to their larger resource requirements and the overhead of running multiple operating systems on a single host.

In conclusion, Docker and VMs have different use cases and trade-offs. VMs are often used for running applications and services that require a full operating system and a higher level of isolation, whereas Docker containers are often used for applications that require a more lightweight and portable solution. The choice between Docker and VMs often depends on the specific requirements and constraints of the environment and the applications being run.