Lab 1 Answers

1. Check Processor Support for Intel/AMD Virtualization Technology and Enable It in BIOS

(1) Check Virtualization Support

Windows System:

Press Win + R, type msinfo32, and press Enter to open "System Information".

In the left navigation pane, select "System Summary". On the right, look for the "Virtualization Technology" entry: if it shows "Enabled", virtualization is supported and active; if it shows "Disabled", virtualization is supported but needs to be enabled in BIOS; if the entry is missing, your processor may not support virtualization.

Linux System:

Open the terminal and run the command: grep -E 'vmx|svm' /proc/cpuinfo.

If the output contains vmx (for Intel processors) or svm (for AMD processors), your processor supports virtualization; no output indicates no support.

macOS System:

Click the Apple icon in the top-left corner, select "About This Mac", then click "System Report".

Under "Hardware" in the left pane, select "Processor". On the right, check if "Virtualization Support" is set to "Yes".

(2) Enable Virtualization in BIOS (Intel Example; Similar for AMD)

When the computer boots, press the corresponding key to enter BIOS (common keys: Del, F2, F10; the key varies by motherboard brand and is displayed on the screen during boot).

In the BIOS interface, use the arrow keys to find the "Advanced" menu, then select "CPU Configuration" or "Processor Settings".

Locate the "Intel Virtualization Technology" (VT-x for Intel) or "AMD-V" (for AMD) option and set it to "Enabled".

Press the save key (usually F10) as prompted, select "Yes" to save settings, and restart the computer. Virtualization will then take effect.

2. Fundamental Reasons for Cloud Computing’s Success and Its Pros/Cons

(1) Fundamental Reasons for Success

Efficient Resource Utilization: Cloud computing pools physical hardware resources (CPU, memory, storage) via virtualization and allocates them to users on demand. This eliminates resource idleness caused by the traditional "one server per application" IT architecture, significantly improving hardware utilization.

Optimized Cost Model: Enterprises no longer need large upfront investments in purchasing, deploying, and maintaining physical hardware. Instead, they use a "Pay-as-you-go" model, paying only for the resources they actually use (e.g., computing hours, storage capacity). This reduces both capital expenditure (CAPEX) and operational expenditure (OPEX).

Elasticity and Scalability: To handle traffic fluctuations (e.g., peak sales during "Double 11" for e-commerce platforms, surges in users for short-video apps), cloud computing can quickly scale up resources (e.g., adding server nodes, expanding storage) and scale down when traffic decreases. This ensures stable business operations while avoiding resource waste.

Simplified Operations and Agile Innovation: Cloud service providers manage underlying operations such as hardware maintenance, system updates, and security patches. Enterprise IT teams can focus on core business development. Additionally, cloud platforms enable rapid deployment (e.g., creating VMs or deploying apps in minutes), accelerating product iteration and innovation.

(2) Pros and Cons of Cloud Computing

Category Details

Pros 1. Controllable Costs: The pay-as-you-go model reduces hardware procurement and operational costs, especially beneficial for SMEs and startups.

2. High Availability and Fault Tolerance: Cloud providers use multi-region and multi-availability zone deployments to offer 99.9% or even 99.99% service availability. Automatic resource switching during hardware failures prevents business interruptions.

3. Global Access: Users can access cloud resources from any location and device (computers, mobile phones) via the internet, supporting remote work and distributed team collaboration.

Cons 1. Data Security and Privacy Risks: Data stored on third-party cloud servers may face risks like data breaches or unauthorized access, which is particularly critical for sensitive industries (finance, healthcare).

2. Dependence on Network Connectivity: Cloud computing relies entirely on the internet. Network outages (e.g., insufficient bandwidth, disconnections) prevent users from accessing cloud resources, disrupting business operations.

3. Vendor Lock-in: Technical architectures (APIs, storage formats, virtualization technologies) vary across cloud providers. Migrating from one provider to another may incur high migration costs and technical compatibility issues.

3. Primary Function of a Hypervisor in Virtualization

The hypervisor is the core component of virtualization technology. Its primary function is to create and manage multiple virtual machines (VMs) on physical hardware (the host). Specific responsibilities include:

Resource Abstraction and Allocation: It abstracts physical hardware resources (CPU, memory, storage, network interface cards) into "virtual resources" and dynamically allocates them to each VM based on demand (e.g., assigning 2 CPU cores and 4GB memory to VM1, 4 CPU cores and 8GB memory to VM2).

VM Scheduling and Isolation: Using CPU scheduling algorithms (e.g., time-sharing), it enables the operating systems (Guest OS) of multiple VMs to "simultaneously" use the physical CPU. It also strictly isolates resources between VMs to prevent failures or malicious behavior in one VM from affecting others or the host (e.g., a memory overflow in VM1 will not crash VM2).

Hardware Access Mediation: It intercepts VMs’ direct requests to access physical hardware and allows VMs to use physical hardware indirectly via "hardware emulation" or "passthrough" (e.g., when a VM needs to read/write to a hard disk, the hypervisor forwards the request to the physical storage device), avoiding conflicts from direct hardware operations.

VM Lifecycle Management: It provides functions to create, start, pause, restart, and delete VMs. Some hypervisors also support VM migration (e.g., moving a running VM from Host A to Host B).

4. Definition of a Virtual Machine (VM)

A virtual machine is a "virtual computer system" created on a physical computer (host) using virtualization technology. It has independent virtual hardware (virtual CPU, virtual memory, virtual hard disk, virtual network card), an operating system (Guest OS), and applications, and behaves almost identically to a physical computer.

Logically, a VM is an "isolated software container": when installing an OS or software in a VM, users do not need to focus on the underlying physical hardware. During operation, all VM activities (e.g., file storage, software execution) are confined to its own virtual environment and do not directly modify the host’s system or data. For example, you can create a VM with the Linux OS on a Windows 11 host, run Linux-exclusive software in the VM, and a Linux system failure (e.g., virus infection) will not affect the Windows host.

5. Benefits of Using Virtual Machines

Resource Isolation and Security Protection: VMs are fully isolated from the host and other VMs. Failures, virus infections, or malicious attacks in one VM will not spread to other environments. This is ideal for testing suspicious software (e.g., unknown EXE files) or running high-risk applications.

Coexistence of Multiple OS Environments: Without purchasing multiple physical computers, you can run multiple different OSes (Windows, Linux, macOS) on one host, meeting diverse development or usage needs. For example, developers can compile Linux programs in a Linux VM on a Windows host and test iOS apps in a macOS VM.

Reduced Hardware Costs: A high-performance physical machine can host multiple VMs, replacing multiple low-config physical machines. This reduces hardware procurement, server room space, power consumption, and maintenance costs—especially useful for enterprise server deployment (e.g., running VMs for multiple services on one physical server).

Environmental Consistency and Rapid Deployment: A configured VM (e.g., with specific development tools or databases) can be saved as an "image file". When the same environment is needed later, new VMs can be quickly created from the image, eliminating tedious repetitive configurations and ensuring consistency across development, testing, and production environments.

Flexible Resource Adjustment and Migration: Virtual hardware resources (e.g., increasing memory, expanding virtual hard disks) can be adjusted at any time based on VM needs. Some hypervisors support "live migration", allowing running VMs to be moved between physical machines, ensuring uninterrupted business during hardware maintenance.

6. Five Use Cases of Virtual Machines

Software Development and Testing:

Developers can create a VM with an OS consistent with the production environment (e.g., Linux CentOS 7 for both production and testing), avoiding "works in development, fails in production" issues caused by environment differences.

Testers can simulate environments with different OSes and browser versions in VMs to test software compatibility (e.g., testing web page display on Chrome for Windows, Firefox for Linux, and Safari for macOS).

Server Virtualization and Resource Consolidation:

Enterprises replace multiple traditional physical servers (Web servers, database servers, email servers) with multiple VMs on one physical machine, reducing hardware quantity and lowering operational costs and energy consumption. For example, a company that previously used 3 physical machines for Web, MySQL, and OA systems can host 3 corresponding VMs on one high-performance physical machine, increasing resource utilization from 30% to 80%.

Security Testing and Malware Analysis:

Security researchers run suspicious files (e.g., virus samples, phishing programs) in isolated VMs to observe behavior (e.g., modifying system files, stealing data), analyze malware mechanisms, and prevent malware from infecting the host system.

Education and Training Labs:

Schools or training institutions can create VM images with preconfigured lab environments (e.g., with network device simulation software or programming tools) on teacher machines and distribute them to student VMs. Students can freely perform experiments (e.g., configuring routers, writing code) in VMs without risking damage to the physical machine’s system due to operational errors.

Legacy System Migration and Operation:

Some outdated software (e.g., industrial control software, traditional office systems for government agencies) only supports obsolete OSes like Windows XP or Windows Server 2003. These OSes no longer receive security updates, making them high-risk to run directly on physical machines. Running these obsolete OSes and legacy software in VMs meets business needs while isolating security risks.

7. Guest Operating System in Virtualization (Multiple Choice)

Answer: b) The operating system installed on a virtual machine

Explanation:

Option a describes the "Host Operating System"—the OS that runs directly on physical hardware.

Option c describes a "remote server OS", which is unrelated to the definition of a guest OS.

Option d describes a "mobile device OS" (e.g., Android, iOS), which is not a guest OS in virtualization.

The core of a guest OS is that it is "installed on a VM" and runs on virtual hardware allocated by the hypervisor. Thus, option b is correct.

8. Virtual Machine Isolation (Multiple Choice)

Answer: c) Virtual machines run independently and are isolated from each other and the host system

Explanation:

Option a is incorrect: VMs cannot directly communicate with physical hardware; they require mediation by the hypervisor. Direct access would cause hardware conflicts.

Option b is incorrect: While VMs share the host’s physical resources, the hypervisor isolates and allocates resources. A VM cannot occupy resources of other VMs or be affected by their failures.

Option d is incorrect: VMs can be accessed remotely via the network (e.g., SSH access to a Linux VM), not just locally.

The core of VM isolation is "independent operation, isolation from each other, and isolation from the host", ensuring no external interference with a VM’s runtime environment. Thus, option c is correct.

9. Benefit of Virtual Machine Portability (Multiple Choice)

Answer: c) It allows virtual machines to be moved between different physical machines with compatible hypervisors

Explanation:

Option a is incorrect: VM-to-VM communication relies on network configuration (e.g., being in the same virtual LAN) rather than portability.

Option b is incorrect: Faster VM boot times depend on factors like VM resource allocation and OS optimization, not portability.

Option d is incorrect: Portability has no connection to reducing the need for hardware virtualization; hardware virtualization is a prerequisite for running most VMs.

The core of VM portability is the ability to migrate VMs across physical machines (as long as hypervisors are compatible, e.g., VMware ESXi to VMware ESXi). Thus, option c is correct.

10. Purpose of Cloning a Virtual Machine

Cloning a VM refers to creating an exact copy (clone) of an existing VM (including the guest OS, installed software, configurations, and data). Its main purposes are:

Rapid Deployment of Consistent Environments: Instead of repeatedly installing the OS, software, and configurations for new VMs (a process that takes hours), you can clone a pre-configured "template VM" (e.g., a VM with a Windows Server OS and SQL Server database) to create new VMs in minutes. This ensures consistency across multiple VMs (e.g., all web server VMs have the same software version).

Disaster Recovery and Backup: A VM clone can serve as a backup. If the original VM fails (e.g., system corruption, data loss), the clone can be activated immediately to restore business operations, minimizing downtime.

Safe Testing and Experimentation: Before making changes to the original VM (e.g., upgrading software, modifying system settings), you can clone it and test the changes in the clone. If the test fails (e.g., software incompatibility causes crashes), the original VM remains unaffected.

Scaling Workloads Efficiently: When business demands increase (e.g., more web servers are needed to handle traffic surges), cloning existing VMs allows quick scaling of the VM cluster, avoiding the inefficiency of manual configuration for each new VM.