8.1.7 Lesson Review

Date: 12/6/2025, 4:43:44 PM

Time Spent: 13:50

Score: 100%

Passing Score: 80%

Question 1 ✓ Correct

Which of the following is a key consideration for ensuring security in a client-side virtualization environment?

- Using 32-bit hypervisors to limit the number of guest OSs that can be installed
- Disabling virtualization extensions in the CPU to prevent unauthorized access
- Ensuring the host OS and hypervisor are regularly updated with security patches ✓ Correct
- Avoiding the use of snapshots to reduce storage requirements

Explanation

Regularly updating the host OS and hypervisor with security patches is essential for maintaining a secure virtualization environment. Vulnerabilities in the hypervisor or host OS can be exploited by attackers to compromise the entire system, including all guest OSs. Keeping the software up-to-date ensures that known vulnerabilities are addressed, reducing the risk of exploitation.

While 32-bit hypervisors may limit the number of guest OSs due to resource constraints, this is not a security measure. Security in virtualization is more about protecting the integrity of the host and guest OSs, as well as ensuring proper isolation between them, rather than limiting the number of VMs.

Disabling virtualization extensions in the CPU would degrade the performance of virtual machines and is not a security best practice. These extensions are designed to enhance virtualization performance and are not inherently a security risk when properly configured.

Snapshots are a useful feature for testing and rollback purposes, and while they do consume additional storage, avoiding them does not contribute to security. Instead, proper management of snapshots and ensuring they are not exposed to unauthorized access is a better approach to maintaining security.

Related Content

8.1.5 Virtualization Security Requirements
resources\questions\q_virtualization_security_requirements_02.question.xml

Question 2 ✓ Correct

Which key advantages do containers have over virtual machines? (Select two.)

- [ ] Hardware optimization
- [x] Smaller size and may only require a few megabytes ✓ Correct
- [ ] The ability to run legacy software on an updated operating system
- [x] Faster start times for containerized applications ✓ Correct
- [ ] Portability between hypervisor environments

Explanation

The key advantages of virtualized containers include:

- A container might only occupy a few megabytes, while a virtual machine might take up several gigabytes.
- A virtual machine may take several minutes to boot, while a containerized application only takes a few seconds to initialize.

Virtual machines are portable between different hypervisors, while containers are only portable between different families of operating systems.

Containerized applications depend on the operating system running on the host machine. They do not include their own operating system. This means that updating the operating system on the host machine could prevent a containerized legacy application from running properly.

Virtualization is a great way to use your physical hardware efficiently. Instead of sitting idly by, waiting for something to do, your processor can perform several tasks at a time. However, this applies to both containerized applications and virtual machines and is not an advantage of one over the other.

Related Content

8.1.2 Uses for Virtualization
resources\questions\q_uses_for_virtualization_04.question.xml

Question 3 Correct

A developer wants to ensure that all the clients using their application always use the latest, most updated version. How can the developer make sure of this?

- Server-side virtualization
- Client-side virtualization
- Application virtualization ✓ Correct
- Container virtualization

Explanation

Application virtualization means that the client either accesses an application hosted on a server or streams the application from the server, ensuring that they are always using the latest version.

Client-side virtualization refers to any solution designed to run on "ordinary" desktops or workstations. Each user will be interacting with the virtualization host directly.

Server-side virtualization means deploying a server role as a virtual machine. For server computers and applications, the main use of virtualization is better hardware utilization through server consolidation.

Container virtualization dispenses with the idea of a hypervisor and instead enforces resource separation at the OS level. The OS defines isolated containers for each user instance to run in.

Related Content

8.1.2 Uses for Virtualization
resources\questions\q_uses_for_virtualization_01.question.xml

Question 4 ✓ Correct

You want to create a virtualization environment that runs directly on the host machine's hardware to manage the virtual machines.

Which of the following virtualization types should you use?

- ○ Container virtualization
- ○ Type 2 hypervisor
- ○ VDI
- ◉ Type 1 hypervisor ✓ Correct

Explanation

A hypervisor is a virtualization component that allows virtual machines to interact with hardware on the host machine. Type 1 runs directly on the host machine's hardware to manage the guest VMs.

Type 2 runs on an operating system to manage the guest VM(s) and does not run directly on the host machine's hardware.

A VDI (virtualization desktop infrastructure) is designed to be the end user's main computer system, which can be accessed from something like a tablet or thin client. In addition, a VDI can be hosted by a cloud service provider. A VDI does not run directly on the host machine's hardware.

Container virtualization is focused on providing a virtual environment for a single application and requires a host machine operating system to run.

Related Content

8.1.1 Hypervisors

8.3.3 Exercise: Exploring Hypervisors

resources\questions\q_hypervisors_04.question.xml

Question 5 ✓ Correct

Rachel, an employee in the support department, wants to run a virtual machine on her computer to troubleshoot customer issues.

Which of the following must she complete before virtualization will work on her computer?

- ○ Install an extra hard disk that the new virtual machine will run on.
- ○ Flash the computer's BIOS to add virtualization support.
- ○ Install additional memory.
- ◉ Enable virtualization support in the BIOS settings. ✓ Correct

Explanation

For virtualization to work on Rachel's PC, she must ensure that virtualization support is enabled in the BIOS settings. Some CPUs will have virtualization support turned on by default, and others will not.

Most modern CPUs support virtualization and do not require the BIOS to be flashed.

Adding an additional hard disk may be advantageous in storing or running virtual machines, but additional hard disks are not a requirement.

Although additional memory will increase the performance of a computer using virtualization, this memory may not be required, depending on the amount currently installed.

Related Content

resources\questions\q_virtualization_resource_requirements_02.question.xml

Question 6 Correct

A network technician gathers requirements to implement virtualization of multiple guest VMs that will need to communicate.

Which of the following resource requirements will the technician need to employ? (Select three.)

- [x] A virtual network environment ✓ Correct
- [ ] Low storage requirements
- [x] Virtualization support enabled on the CPU ✓ Correct
- [x] Memory above what the OS requires ✓ Correct

Explanation

Most virtualization software requires a central processing unit (CPU) with virtualization support enabled as the performance of the virtual machines will be impaired if hardware-assisted virtualization is not available.

Each guest OS requires sufficient system memory over and above what the host OS/hypervisor requires to support the VMs.

A hypervisor will be able to create a virtual network environment through which all the VMs can communicate, and a network shared by the host and by VMs on the same host and on other hosts.

Virtual machines will need mass storage as each guest OS takes up a substantial amount of disk space. The host stores each of the VM's "hard disks" as an image file on the host.

Related Content

resources\questions\q_virtualization_resource_requirements_01.question.xml

Question 7 ✓ Correct

What is the primary benefit of server-side virtualization?

- It eliminates the need for a hypervisor by isolating resources at the OS level.
- It allows users to access applications without installing them locally.
- It simplifies the process of creating isolated environments for testing and development.
- It improves hardware utilization through server consolidation. ✓ Correct

Explanation

Server-side virtualization allows multiple server instances to run on the same hardware, significantly improving hardware utilization. This is achieved by consolidating multiple server roles onto fewer physical machines, which reduces hardware costs and increases efficiency.

Simplifying the process of creating isolated environments for testing and development describes a use case for client-side virtualization, particularly sandboxing, which is used for testing and development. It is not the primary benefit of server-side virtualization.

Allowing users to access applications without installing them locally describes application virtualization, where applications are streamed or accessed from a server. While related to virtualization, it is not specific to server-side virtualization.

Eliminating the need for a hypervisor by isolating resources at the OS level describes container virtualization, which operates at the OS level without requiring a hypervisor. Server-side virtualization, on the other hand, typically involves the use of a hypervisor to manage virtual machines.

Related Content

resources\questions\q_uses_for_virtualization_08.question.xml

Question 8 Correct

You are tasked with setting up a virtualization environment for a team of developers who need to test applications on their existing desktop computers.

The developers require the ability to run multiple operating systems simultaneously without replacing their current OS.

Which type of hypervisor would be the most appropriate for this scenario?

- Type 1 (Bare Metal Hypervisor)
- Virtual Desktop Infrastructure (VDI)
- Container virtualization
- Type 2 (Host-based Hypervisor) ✓ Correct

Explanation

Type 2 hypervisors are installed on top of an existing operating system, making them ideal for client-side virtualization on desktop computers. This allows developers to run multiple guest operating systems without replacing their current OS, meeting the requirements of the scenario.

Type 1 hypervisors are installed directly onto hardware and are typically used in server environments, not on existing desktop computers. This would not meet the requirement of running on the developers' current OS.

Containers isolate applications at the OS level and do not provide the ability to run multiple operating systems simultaneously, which is a key requirement in this scenario.

VDI is a server-side solution where desktops are hosted on a centralized server. It does not align with the need for client-side virtualization on existing desktop computers.

Related Content

8.1.1 Hypervisors

8.3.3 Exercise: Exploring Hypervisors

resources\questions\q_hypervisors_08.question.xml

Question 9 ✓ Correct

While creating a virtual machine, you decide to set it up to use an external network.

What else do you need to do to enable the external network configuration?

- ○ Configure the virtual machine to use Remote Desktop Protocol (RDP).
- ○ Make sure that you are using a Type 1 hypervisor.
- ○ Set the RAM on the virtual machine to match the host.
- ◉ Select a NIC using the virtual switch manager. ✓ Correct

Explanation

To enable an external network configuration for a virtual machine, you must connect the virtual machine to the host's physical network adapter (NIC). This is done using the virtual switch manager within the hypervisor software. The virtual switch manager allows you to create a virtual switch and associate it with the physical NIC of the host system. By selecting the appropriate NIC, the virtual machine can access the external network, enabling communication with other devices and systems outside the host machine. This step is essential for external network connectivity.

Setting the RAM on the virtual machine to match the host system is unrelated to enabling external network configuration. This step pertains to resource allocation and ensures that the virtual machine has enough memory to operate efficiently. While proper RAM allocation is important for the performance of the virtual machine, it does not affect its ability to connect to an external network.

Configuring the virtual machine to use Remote Desktop Protocol (RDP) is a step that allows remote access to the virtual machine. While RDP is useful for managing and accessing the virtual machine from another device, it is not a requirement for setting up external network connectivity. RDP configuration is a separate process that involves enabling the RDP service within the guest operating system and ensuring network settings allow RDP traffic.

Using a Type 1 hypervisor (bare-metal hypervisor) is not a requirement for enabling external network configuration. Both Type 1 and Type 2 hypervisors can support external network connectivity as long as the virtual switch manager is used to associate the virtual machine with the host's physical NIC. The choice of hypervisor type depends on the deployment environment and performance requirements, but it does not directly impact the ability to configure an external network for the virtual machine.

Related Content

8.1.5 Virtualization Security Requirements
resources\questions\q_virtualization_security_requirements_01.question.xml

Question 10 Correct

A network technician installs virtual machines in hypervisor software that runs directly onto a server. What kind of hypervisor setup is this? (Select two.)

- [x] Bare metal ✓ Correct
- [ ] Type 2
- [x] Type 1 ✓ Correct
- [ ] Guest OS

Explanation

A Type 1 hypervisor installs directly onto the computer and manages access to the host hardware without going through a host OS.

A bare metal virtual platform means that a Type 1 hypervisor installs directly onto the computer and manages access to the host hardware without going through a host OS.

In Type 2 hypervisors, the hypervisor application installs onto a host OS, and the computer must have resources to run the host OS, the hypervisor, and the guest operating systems.

In a guest OS (or host-based) system, the hypervisor application is itself installed onto a host OS. The hypervisor software must support the host OS.

Related Content

8.1.1 Hypervisors

8.3.3 Exercise: Exploring Hypervisors
resources\questions\q_hypervisors_01.question.xml