Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 3/25/2022 8:27:42 pm • Time spent: 07:04

Score: 40% Passing Score: 80%

Question 1: ✔ Correct

Which of the following provides the network virtualization solution called XenServer?

- Microsoft
- VMWare
- Cisco
- Citrix

EXPLANATION

Citrix provides the virtualization solution called XenServer, also referred to as Citrix Hypervisor.

Microsoft provides a virtualization solution called Hyper-V Network Virtualization.

VMWare provides a virtualization solution called ESXi.

Cisco does not provide a virtualization solution but does offer a vSwitch platform called Nexus 1000v.

REFERENCES

9.2.4 Virtualization Implementation Facts

q_virt_impl_citrix_secp7.question.fex

Question 2: ✔ Correct

Which of the following is a network virtualization solution provided by Microsoft?

- VMware
- Hyper-V
- Citrix
- VirtualBox

EXPLANATION

Hyper-V Network Virtualization provides virtual networks to virtual machines. This is similar to the way in which server virtualization (hypervisors) provides virtual machines to the operating system. Hyper-V Network Virtualization has high scalability, with the capacity for over 1,000 virtual machines per host.

None of the other virtualization solutions are provided by Microsoft.

REFERENCES

9.2.4 Virtualization Implementation Facts

q_virt_impl_micro_secp7.question.fex

Question 3: ✔ Correct

What is the limit of virtual machines that can be connected to a virtual network?

- 16,777,214
- 65,534
- 54
- Unlimited

EXPLANATION

An unlimited number of virtual machines can be connected to a virtual network.

254 is the maximum hosts in a Class C network.

65,534 is the maximum hosts in a Class B network.

16,777,214 is the maximum hosts in a Class A network.

REFERENCES

9.2.4 Virtualization Implementation Facts

q_virt_impl_unlimited_secp7.question.fex

Question 4: ✕ Incorrect

You are an application developer. You use a hypervisor with multiple virtual machines installed to test your applications on various operating systems' versions and editions.

Currently, all of your virtual machines used for testing are connected to the production network through the hypervisor's network interface. However, you are concerned that the latest application you are working on could adversely impact other network hosts if errors exist in the code.

To prevent issues, you decide to isolate the virtual machines from the production network. However, they still need to be able to communicate directly with each other.

What should you do? (Select two. Both responses are part of the complete solution.)

- [ ] Disconnect the network cable from the hypervisor's network interface.
- [x] Connect the virtual network interfaces in the virtual machines to the virtual switch.
- [ ] Create a new virtual switch configured for host-only (internal) networking.
- [ ] Disable the switch port the hypervisor's network interface is connected to.
- [ ] Create MAC address filters on the network switch that block each virtual machine's virtual network interfaces.
- [x] ~~Create a new virtual switch configured for bridged (external) networking.~~

EXPLANATION

To allow the virtual machines to communicate with each other while isolating them from the production network, complete the following:

- Create a new virtual switch configured for host-only (internal) networking
- Connect the virtual network interfaces in the virtual machines to the virtual switch

Creating a bridged virtual switch would still allow the virtual machines to communicate on the production network through the hypervisor's network interface. Disconnecting the hypervisor's network cable, blocking the virtual machines' MAC addresses, or disabling the hypervisor's switch port would isolate the virtual machines from the production network, but this would also prevent them from communicating with each other.

REFERENCES

9.2.4 Virtualization Implementation Facts

q_virt_impl_virtualize_secp7.question.fex

Question 5: ✕ Incorrect

Which of the following statements about virtual networks is true? (Select two.)

- [x] Multiple virtual networks can be associated with a single physical network adapter.
- [ ] Each virtual network must be associated with a single physical network adapter.
- [ ] Accessing network resources requires that the operating system on the virtual machine be configured on an isolated network.
- [ ] A virtual network is dependent on the configuration and physical hardware of the host operating system.
- [x] ~~A virtual network is independent of the configuration and physical hardware of the host operating system.~~

EXPLANATION

A virtual network is made up of one or more virtual machines configured to access local or external network resources. Some important facts about virtual networks include:

- Virtual machines support an unlimited number of virtual networks, and an unlimited number of virtual machines can be connected to a virtual network.
- Multiple virtual networks can be associated with a single physical network adapter.
- When a virtual network is created, its configuration is dependent on the configuration and physical hardware (such as the type and number of network adapters) of the host operating system.
- Accessing a network and network resources requires that the operating system on the virtual machine be configured as a part of the network.

REFERENCES

9.2.5 Virtual Networking Facts

q_virt_net_network_secp7.question.fex

Question 6: ✕ Incorrect

Which of the following devices facilitates communication between different virtual machines by checking data packets before moving them to a destination?

- ~~Virtual router~~
- Hypervisor
- Virtual firewall
- Virtual switch

EXPLANATION

A virtual switch is software that facilitates the communication between different virtual machines. It does so by checking data packets before moving them to a destination. They may already be a part of software installed in the virtual machine, or they may be part of the server firmware.

REFERENCES

9.2.5 Virtual Networking Facts

q_virt_net_switch_secp7.question.fex

Question 7: ✕ Incorrect

What is a virtual LAN that runs on top of a physical LAN called?

- VMM
- VAN
- VFA
- ~~VLAN~~

EXPLANATION

A virtual area network (VAN) is a virtual LAN running on top of a physical LAN. This configuration enables guest virtual machines on separate physical hosts to communicate.

VLANs allow several physical LANs to function as a single logical LAN.

A VFA is a virtual firewall appliance. This is software that functions as a network firewall device.

A virtual machine monitor is software, firmware, or hardware that creates and runs virtual machines. This is also known as a hypervisor.

REFERENCES

9.2.5 Virtual Networking Facts

q_virt_net_van_secp7.question.fex

Question 8: ✕ Incorrect

Which of the following virtual devices provides packet filtering and monitoring?

- VLAN
- VMM
- VFA
- ~~vSwitch~~

EXPLANATION

A VFA is a virtual firewall appliance. This is software that functions as a network firewall device that provides the usual packet filtering and monitoring. A VFA can run as a traditional software firewall on a virtual machine.

VLANs allow several physical LANs to function as a single logical LAN.

A vSwitch is software that facilitates the communication between virtual machines by checking data packets before moving them to a destination.

A virtual machine monitor is software, firmware, or hardware that creates and runs virtual machines. This is also known as a hypervisor.

REFERENCES

9.2.5 Virtual Networking Facts

q_virt_net_vfa_secp7.question.fex

Question 9: ✕ Incorrect

Which of the following is an example of protocol-based network virtualization?

- ~~VMM~~
- VLAN
- vSwitch
- VFA

EXPLANATION

VLANs and VPNs are two examples of protocol-based network virtualization.

A vSwitch is software that facilitates the communication between virtual machines by checking data packets before moving them to a destination.

A VFA is a virtual firewall appliance. This is software that functions as a network firewall device.

A virtual machine monitor is software, firmware, or hardware that creates and runs virtual machines. This is also known as a hypervisor.

REFERENCES

9.2.5 Virtual Networking Facts

q_virt_net_vlan_secp7.question.fex

Question 10: ✔ Correct

Which of the following is used as a secure tunnel to connect two networks?

- VLAN
- VFA
- VPN
- VAN

EXPLANATION

A virtual private network (VPN) is usually used as a secure tunnel over another network, connecting multiple remote endpoints (such as routers). A multipoint VPN is a VPN connecting more than two endpoints.

VLANs allow several physical LANs to function as a single logical LAN.

A virtual area network (VAN) is a virtual LAN running on top of a physical LAN.

A VFA is a virtual firewall appliance. This is software that functions as a network firewall device.

REFERENCES

9.2.5 Virtual Networking Facts

q_virt_net_vpn_secp7.question.fex