2V0-621Q&As

VMware Certified Professional 6 – Data Center Virtualization

Pass VMware 2V0-621 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/2v0-621.html

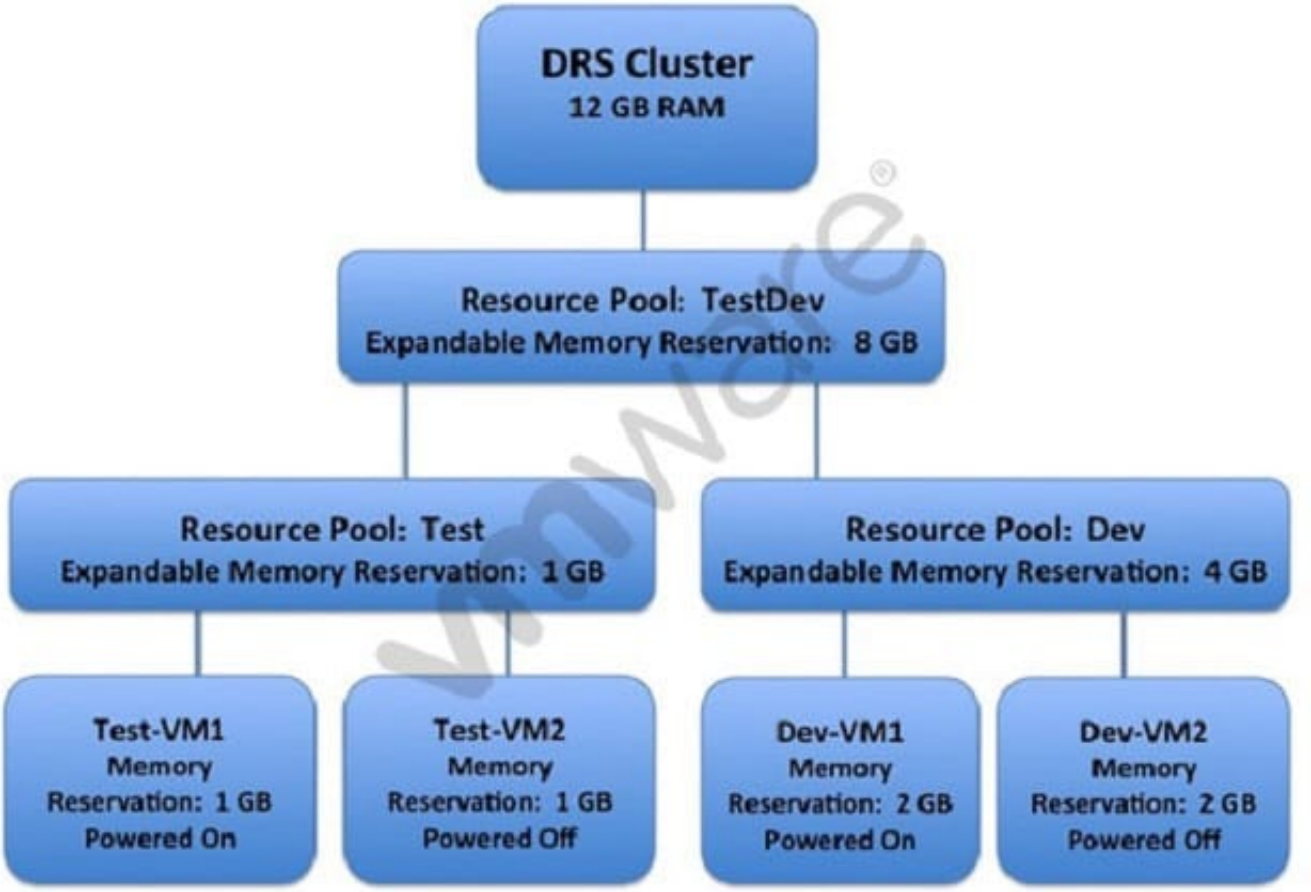
100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by VMware Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Refer to the Exhibit.



An administrator has configured a vSphere 6.x DRS cluster as shown in the Exhibit.

Based on the exhibit, which statement is true?

A. A virtual machine can be powered on in the Test Resource Pool with a 6 GB Memory Reservation.

B. A virtual machine can be powered on in the Dev Resource Pool with a 8 GB Memory Reservation.

C. A virtual machine from both the Test Resource Pool and the Dev Resource Pool can be powered on with a 4 GB Memory Reservation.

D. No more virtual machines can be powered on due to insufficient resources.

Correct Answer: A

A virtual machine can be powered on in the Test Resource Pool with a 6 GB Memory Reservation because: Total is 8GB 1Gb used by test resource pool VM which is powered on and 2gb by Test dev pool VM powered on hence distribution is less and expandable memory quota is more/left.

To understand limits and theory check the information given below: Memory Maximums The ESXi host maximums represents the limits for ESXi host memory. Table 3-2. ESXi Host Memory Maximums Item Maximum RAM per host 6

TB 12 TB is supported on specific OEM certified platform. See VMware Hardware Compatibility Limits for guidance on the platforms that support vSphere 6.0 with 12 TB of physical memory. Number of swap files 1 per virtual machine

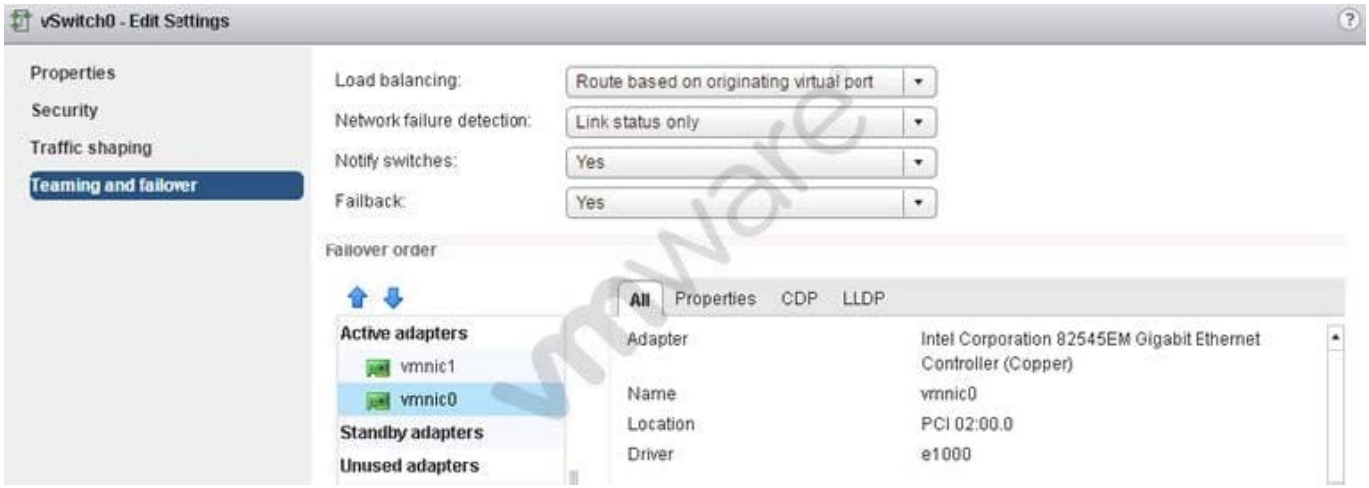
And, Resource Pool Resource pools per host 1600 Children per resource pool 1100 Resource pool tree depth 8 Additional 4 resource pools are used by system internals. Resource pools per cluster 1600

Configuration Maximums - vSphere 6.0 - VMware https://www.vmware.com/pdf/vsphere6/r60/vsphere-60-configuration-maximums.pdf

QUESTION 2

An administrator has recently configured HA on a cluster. After reviewing the summary tab on one of the hosts, the warning in Exhibit 1 is displayed:

The administrator proceeds to view the management network port group data shown in Exhibit 2:



The administrator then views the management network vSwitch as shown in Exhibit 3:

Based on the exhibits, which two steps should be taken to ensure redundancy on the management network? (Choose two.)

A. Move vmnic1 to Standby adapters.

B. Add an additional vmknic to the Network Adapters and move it to Active adapters.

C. Set the advanced HA configuration parameter das.ignoreRedundantNetWarning to True.

D. Uncheck the Override Failover Checkbox on the management network port group.

Correct Answer: AD

Explanation: A and D

Use Load Balancing and Failover policies to determine how network traffic is distributed between adapters and how to reroute traffic in the event of an adapter failure.

The Failover and Load Balancing policies include the following parameters:

Load Balancing policy: The Load Balancing policy determines how outgoing traffic is distributed among the network adapters assigned to a standard switch. Incoming traffic is controlled by the Load Balancing policy on the physical switch.

Failover Detection: Link Status/Beacon Probing

Network Adapter Order (Active/Standby)

In some cases, you might lose standard switch connectivity when a failover or failback event occurs. This causes the MAC addresses used by virtual machines associated with that standard switch to appear on a different switch port than they previously did. To avoid this problem, put your physical switch in portfast or portfast trunk mode.

Link:

https://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.networking.doc%2FGUID-D5EA6315-5DCD-463E-A701-B3D8D9250FB5.html

QUESTION 3

An administrator decides to change the root password for an ESXi 6.x host to comply with the company\\'s security policies.

What are two ways that this can be accomplished? (Choose two.)

A. Use the Direct Console User Interface to change the password.

B. Use the passwd command in the ESXi Shell.

C. Use the password command in the ESXi Shell.

D. Use the vSphere client to update local users.

Correct Answer: AB

Explanation: Limit ESXi Access By default, the ESXi Shell and SSH services are not running and only the root user can log in to the Direct Console User Interface (DCUI). If you decide to enable ESXi or SSH access, you can set timeouts to

limit the risk of unauthorized access. ESXi enforces password requirements for direct access from the Direct Console User Interface, the ESXi Shell, SSH, or the vSphere Client. Reference: https://pubs.vmware.com/vsphere-60/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenterserver-60-security-guide.pdf

QUESTION 4

An administrator is having a problem configuring Storage I/O Control on a Datastore.

Which two conditions could explain the issue? (Choose two.)

A. A host is running ESXi 4.0.

B. An ESXi host does not have appropriate licensing.

C. The vCenter Server version is 5.0.

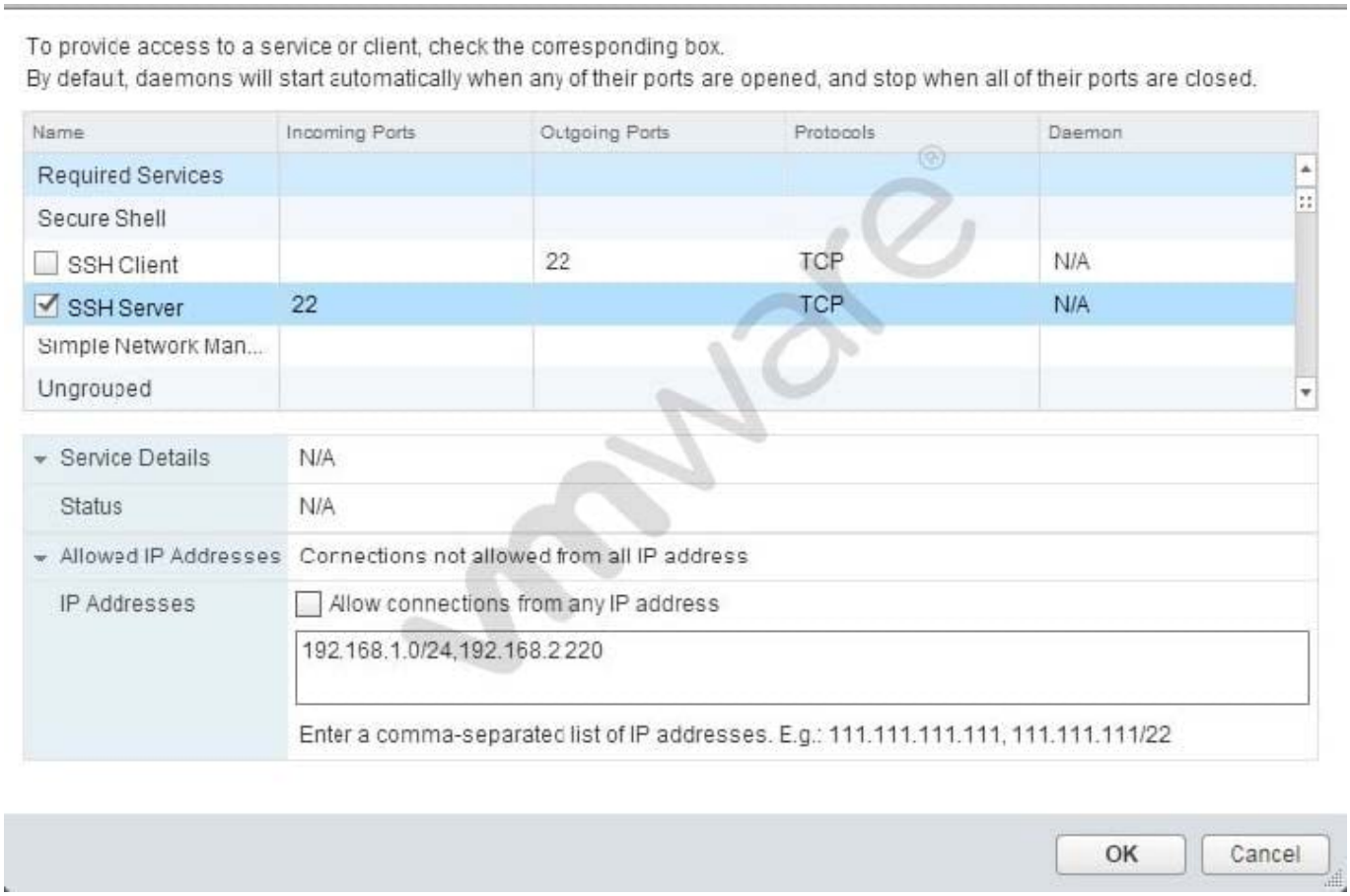
D. The vCenter Server License is Standard.

Correct Answer: AB

A-) Storage I/O Control was introduced in vSphere 4.1, taking storage resource controls built into vSphere to a much broader level. In vSphere 5, Storage I/O Control has been enhanced with support for NFS data stores and clusterwide I/O shares. Check vmware.com esxi versions enhancements, for further troubleshooting https://kb.vmware.com/kb/1022091 B-) If hosts are not licensed at the appropriate level, the option to enable Storage I/O control is grayed out. Check: https://kb.vmware.com/kb/2021530

QUESTION 5

Refer to the Exhibit.



An administrator has configured a firewall rule as shown in the Exhibit. Which statement best describes the ESXi 6.x firewall rule?

A. Connections from the ESXi host to all devices on the 192.168.1.0 network and 192.168.2.220 on port 22 are allowed.

B. Connections coming from IP addresses from the 192.168.1.0 network and 192.168.2.220 on port 22 are allowed.

C. TCP Connections coming from IP addresses from the 192.168.1.0 network and 192.168.2.220 on port 22 are not allowed.

D. TCP Connections from the ESXi host to all devices on the 192.168.1.0 network and 192.168.2.220 on port 22 are not allowed.

Correct Answer: B

PoRT 22 SSH on ESXi allowed : "Allow connections from any IP address," or, you can select "Only allow connections from the following networks" and enter an IP address or subnet. You can enter multiple IP addresses and subnets, separated with a comma. By default, there is a set of predefined firewall rules that can be enabled/disabled for the ESXi host from the vSphere Client. These firewall services can be enabled/disabled for the defined ports (UDP/TCP) from the vSphere Client. However, if you need to enable the service on a protocol that is not defined, you must create new firewall rules from the command line. For example, the DNS Client service can be enabled/disabled only on UDP port 53.

To enable DNS for TCP:

Open an SSH connection to the host. For more information, see Using ESXi Shell in ESXi 5.0 and 6.0

(2004746).

List the firewall rules by running the command:

esxcli network firewall ruleset list

https://kb.vmware.com/selfservice/microsites/search.do?

language=en_USandcmd=displayKCandexternalId=2008226