



2V0-621^{Q&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.passapply.com/2v0-621.html>

100% Passing Guarantee
100% Money Back Assurance

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

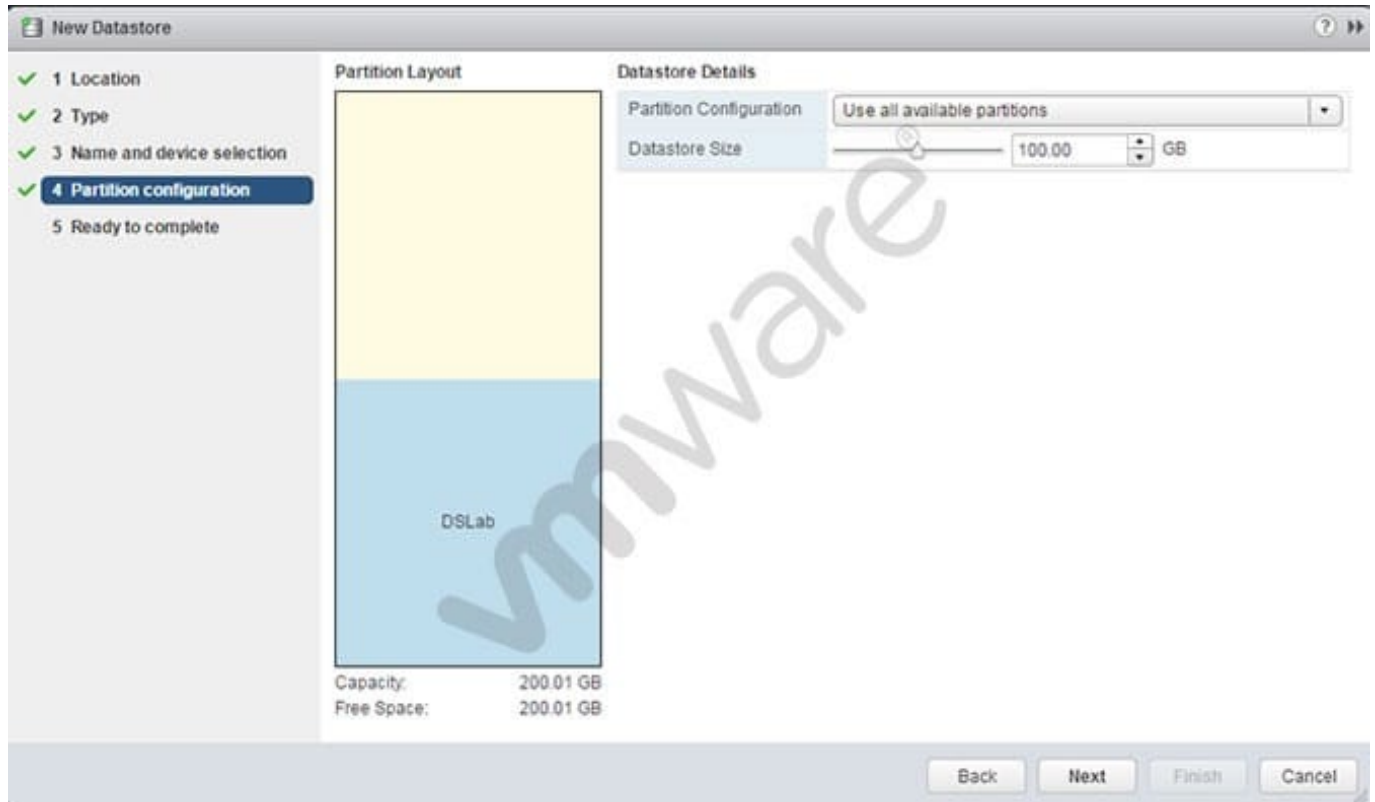
- ⚙ **Instant Download** After Purchase
- ⚙ **100% Money Back** Guarantee
- ⚙ **365 Days** Free Update
- ⚙ **800,000+** Satisfied Customers





QUESTION 1

Refer to the Exhibit.



What will be created upon completion of the steps in this wizard?

- A. 100GB VMFS5 datastore with free space available for expansion
- B. 100GB VMFS5 datastore with free space available for a second datastore
- C. 100GB VMFS3 datastore
- D. 200.01 GB VMFS5 datastore

Correct Answer: A

Explanation: The datastore size selected is 100GB. On completion of this step, 100 GB VMFS datastore will be created.

QUESTION 2

An administrator has a virtual machine configured with the following settings:

1.

ESXi version: 5.1



2.

CPU: vCPUs 6

3.

Memory: 48GB

4.

Hardware version: 7

5.

VMware Tools: Installed

Which two actions must the administrator take in order to utilize vNUMA? (Choose two.)

A. Upgrade the ESXi host to vSphere 5.5 or later.

B. Upgrade to Virtual Hardware version 8.

C. Configure numa.vcpu.min to 5

D. Configure numa.vcpu.min to 6

Correct Answer: BD

Using Virtual NUMA vSphere 5.0 and later includes support for exposing virtual NUMA topology to guest operating systems, which can improve performance by facilitating guest operating system and application NUMA optimizations. Virtual NUMA topology is available to hardware version 8 virtual machines and is enabled by default when the number of virtual CPUs is greater than eight. You can also manually influence virtual NUMA topology using advanced configuration options. You can affect the virtual NUMA topology with two settings in the vSphere Client: number of virtual sockets and number of cores per socket for a virtual machine. If the number of cores per socket (cpuid.coresPerSocket) is greater than one, and the number of virtual cores in the virtual machine is greater than 8, the virtual NUMA node size matches the virtual socket size. If the number of cores per socket is less than or equal to one, virtual NUMA nodes are created to match the topology of the first physical host where the virtual machine is powered on. Reference: <https://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.resmgmt.doc/GUID-17B629DE75DF-4C23-B831-08107007FBB9.html>

-----note-----Also, Check Page 21,22

https://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.1.pdf D-) Size your virtual machines so they align with physical NUMA boundaries. For example, if you have a host system with six cores per NUMA node, size your virtual machines with a multiple of six vCPUs (i.e., 6 vCPUs, 12 vCPUs, 18 vCPUs, 24 vCPUs, and so on). Hence answer is D Also, Check Page 41,42 https://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.1.pdf

QUESTION 3

Which three services can be enabled/disabled in the Security Profile for an ESXi host? (Choose three.)

A. CIM Server

B. Single Sign-On

C. Direct Console UI



D. Syslog Server

E. vSphere Web Access

Correct Answer: ACD

**ESXi Services in the Security Profile**

Service	Default	Description
Direct Console UI	Running	The Direct Console User Interface (DCUI) service allows you to interact with an ESXi host from the local console host using text-based menus.
ESXi Shell	Stopped	<p>The ESXi Shell is available from the Direct Console User Interface and includes a set of fully supported commands and a set of commands for troubleshooting and remediation.</p> <p>You must enable access to the ESXi Shell from the direct console of each system.</p> <p>You can enable access to the local ESXi Shell or access to the ESXi Shell with SSH.</p>
SSH	Stopped	The host's SSH client service that allows remote connections through Secure Shell.
Load-Based Teaming Daemon	Running	Load-Based Teaming.
Local Security Authentication Server (Active Directory Service)	Stopped	Part of Active Directory Service. When you configure ESXi for Active Directory, this service is started.
I/O Redirector (Active Directory Service)	Stopped	Part of Active Directory Service. When you configure ESXi for Active Directory, this service is started.
Network Login Server (Active Directory Service)	Stopped	Part of Active Directory Service. When you configure ESXi for Active Directory, this service is started.



NTP Daemon	Stopped	Network Time Protocol daemon.
CIM Server	Running	Service that can be used by Common Information Model (CIM) applications.
SNMP Server	Stopped	SNMP daemon. See <i>vSphere Monitoring and Performance</i> for information on configuring SNMP v1, v2, and v3.
Syslog Server	Stopped	Syslog daemon. You can enable syslog from the Advanced System Settings in the vSphere Web Client. See <i>vSphere Installation and Setup</i> .
vSphere High Availability Agent	Stopped	Supports vSphere High Availability functionality.
vProbe Daemon	Stopped	vProbe daemon.
VMware vCenter Agent	Running	vCenter Server agent. Allows a vCenter Server to connect to an ESXi host. Specifically, vpxa is the communication conduit to the host daemon, which in turn communicates with the ESXi kernel.
X.Org Server	Stopped	X.Org Server. This optional feature is used internally for 3D graphics for virtual machines.

Reference: <https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUID37AB1F95-DDFD-4A5D-BD49-3249386FFADE.html>

QUESTION 4

Which Advanced Setting should be created for the vCenter Server to change the expiration policy of the vpxuser password?

- A. VimPasswordExpirationInDays
- B. VimExpirationPasswordDays
- C. VimPassExpirationInDays
- D. VimPasswordRefreshDays

Correct Answer: A



Important

To preclude the possibility that vCenter Server is locked out of the ESXi host, the password aging policy must not be shorter than the interval that is set to automatically change the vpxuser password.

Procedure

- 1 To change the password length policy, edit the `vpxd.hostPasswordLength` parameter in the vCenter Server configuration file on the system where vCenter Server is running.

Operating System	Default Location
Windows	C:\Documents and Settings\All Users\Application Data\VMware VirtualCenter\vpzd.cfg
Linux	/etc/vmware-vpx/vpzd.cfg

- 2 To change the password aging requirement, use the Advanced Settings dialog box in the vSphere Web Client.
 - a Browse to the vCenter Server system in the vSphere Web Client inventory.
 - b Click the **Manage** tab and click **Settings**.
 - c Select **Advanced Settings** and locate the `VirtualCenter.VimPasswordExpirationInDays` parameter.
- 3 Restart vCenter Server.

Reference: <https://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUID96210743-0C17-4AE9-89FC-76778EC9D06E.html>

QUESTION 5

An administrator would like to use the VMware Certificate Authority (VMCA) as an Intermediate Certificate Authority (CA). The first two steps performed are:

1.

Replace the Root Certificate

2.

Replace Machine Certificates (Intermediate CA)

Which two steps would need to be performed next? (Choose two.)

- A. Replace Solution User Certificates (Intermediate CA)
- B. Replace the VMware Directory Service Certificate (Intermediate CA)
- C. Replace the VMware Directory Service Certificate
- D. Replace Solution User Certificates

Correct Answer: AC

Use VMCA as an Intermediate Certificate Authority You can replace the VMCA root certificate with a third-party CA-signed certificate that includes VMCA in the certificate chain. Going forward, all certificates that VMCA generates include the full chain. You can replace existing certificates with newly generated certificates. This approach combines the security of thirdparty CA-signed certificate with the convenience of automated certificate management.



Procedure 1 Replace the Root Certificate (Intermediate CA) The first step in replacing the VMCA certificates with custom certificates is generating a CSR and adding the certificate that is returned to VMCA as a root certificate. 2 Replace Machine SSL Certificates (Intermediate CA) After you have received the signed certificate from the CA and made it the VMCA root certificate, you can replace all machine SSL certificates. 3 Replace Solution User Certificates (Intermediate CA) After you replace the machine SSL certificates, you can replace the solution user certificates. 4 Replace the VMware Directory Service Certificate If you decide to use a new VMCA root certificate, and you unpublish the VMCA root certificate that was used when you provisioned your environment, you must replace the machine SSL certificates, solution user certificates, and certificates for some internal services. 5 Replace the VMware Directory Service Certificate in Mixed Mode Environments During upgrade, your environment might temporarily include both vCenter Single Sign-On version 5.5 and vCenter Single Sign-On version 6.0, you have to perform additional steps to replace the VMware Directory Service SSL certificate if you replace the SSL certificate of the node on which the vCenter Single Sign-On service is running.

Reference: <https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUID5FE583A2-3737-4B62-A905-5BB38D479AE0.html>

[2V0-621 VCE Dumps](#)[2V0-621 Study Guide](#)[2V0-621 Braindumps](#)