2V0-51.23Q&As

VMware Horizon 8.x Professional

Pass VMware 2V0-51.23 Exam with 100% Guarantee

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

https://www.passapply.com/2v0-51-23.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

Where are exclusions specified for Writable Volumes to prevent App Volumes from persisting specific data between sessions?

A. snapvol.cfg

B. config.ini

C. svservice.log

D. json.cfg

Correct Answer: A

Explanation: Writable Volumes are user-specific virtual disks that store user-installed applications, data, and settings. App Volumes is a real-time application delivery system that uses Writable Volumes to deliver applications that are not multiuser aware. However, sometimes it might be necessary to prevent App Volumes from persisting specific databetween sessions, such as temporary files, application updates, or registry keys. To do this, administrators can specify exclusions

for Writable Volumes in a policy file called snapvol.cfg.

The snapvol.cfg file is a text file that contains policy settings for App Volumes. These settings determine which files and registry keys are captured or excluded by App Volumes. The snapvol.cfg file can be customized by administrators to suit

different needs and scenarios. The snapvol.cfg file can be applied to both application packages and Writable Volumes.

To specify exclusions for Writable Volumes, administrators can use the following keywords in the snapvol.cfg file:

exclude_uwv_file: This keyword excludes a file or folder path from being persisted on a Writable Volume. For example, exclude_uwv_file=\Program Files (x86)\Notepad++ excludes the folder location of Notepad++ from being overwritten

during an update.

exclude_uwv_reg: This keyword excludes a registry key or value from being persisted on a Writable Volume. For example,

exclude_uwv_reg=\REGISTRY\MACHINE\SOFTWARE\Notepad++ excludes the registry location of Notepad++ from being overwritten during an update. The snapvol.cfg file must be uploaded to the Writable Volume by using the Update

Writable Volumes feature in App Volumes Manager. The exclusions will take effect after the user logs off and logs back in to the desktop.

The other options are not valid files for specifying exclusions for Writable Volumes:

config.ini: This file is used to configure the App Volumes agent settings, such as the App Volumes Manager address, the logging level, and the SSL certificate validation.

svservice.log: This file is used to record the App Volumes agent log messages, such as the agent status, the package attachment, and the error messages. json.cfg: This file does not exist in App Volumes. References: Writable Volume

Exclusions, Policy Files (snapvol.cfg) in App Volumes, and [VMware Horizon 8.x Professional Course]

QUESTION 2

Refer to the exhibit.

An administrator prepared a golden image based on a Windows Server Operating System.

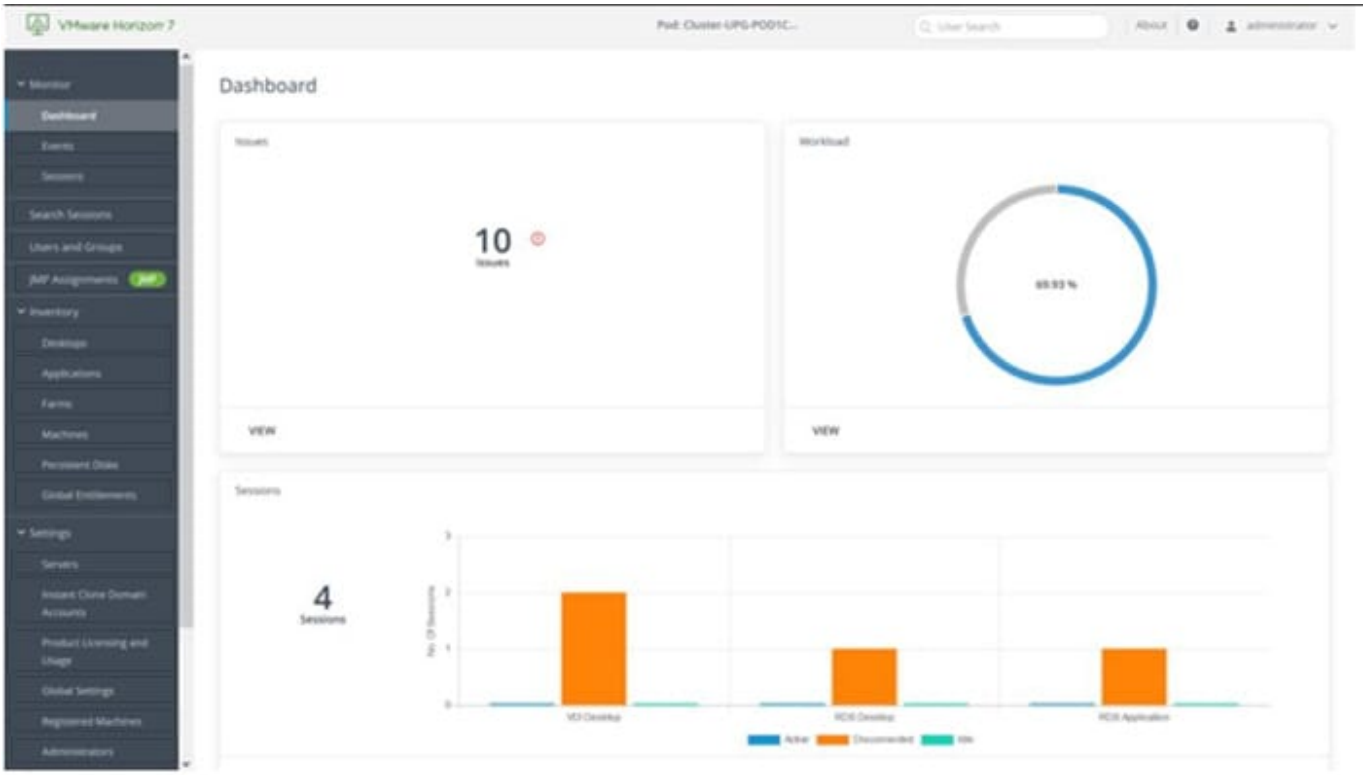
They plan to use this image to create a single-session virtual desktop pool. The installation is completed, the virtual machine is turned off, and the snapshot has been created. When the administrator creates the desktop pool, they are unable

to select the created image and snapshot. They do see other previously created golden images, based on Desktop Operating Systems.

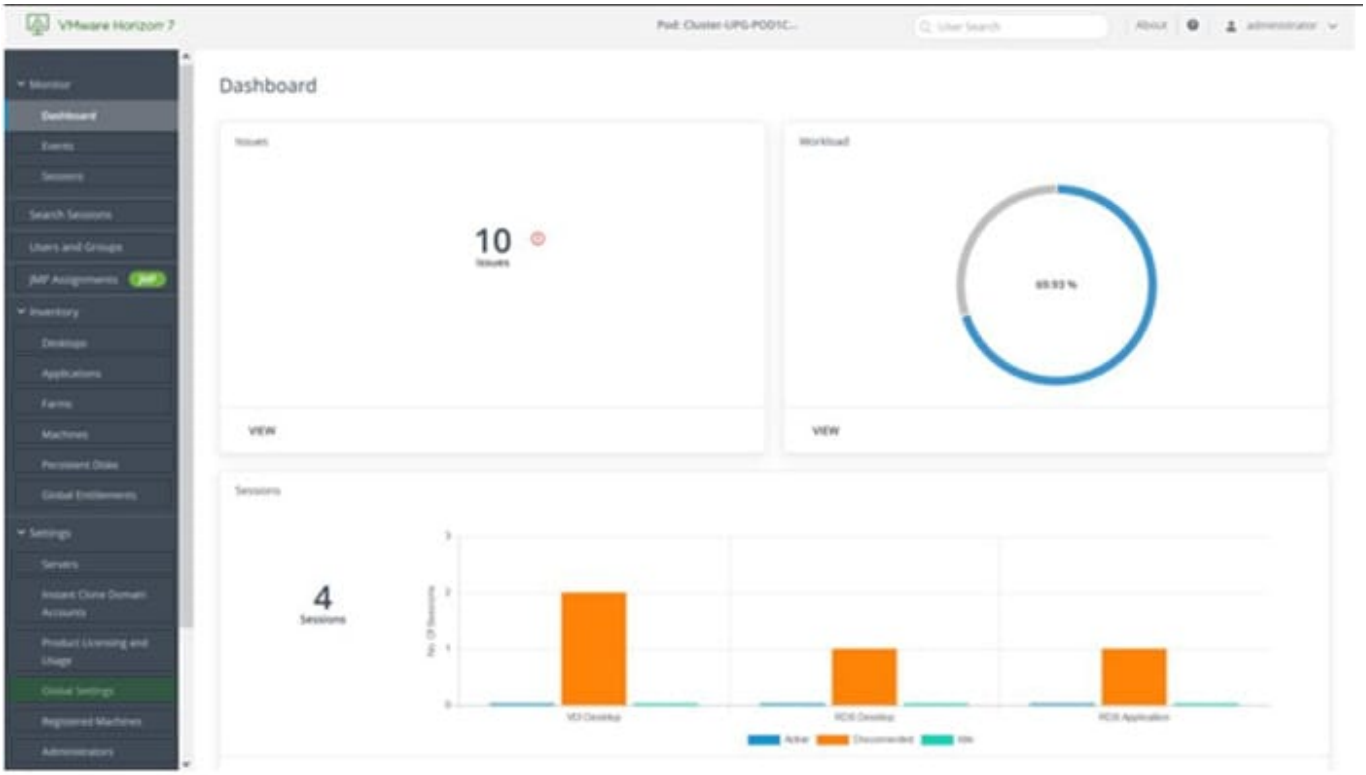
The administrator has opened the Horizon Console.

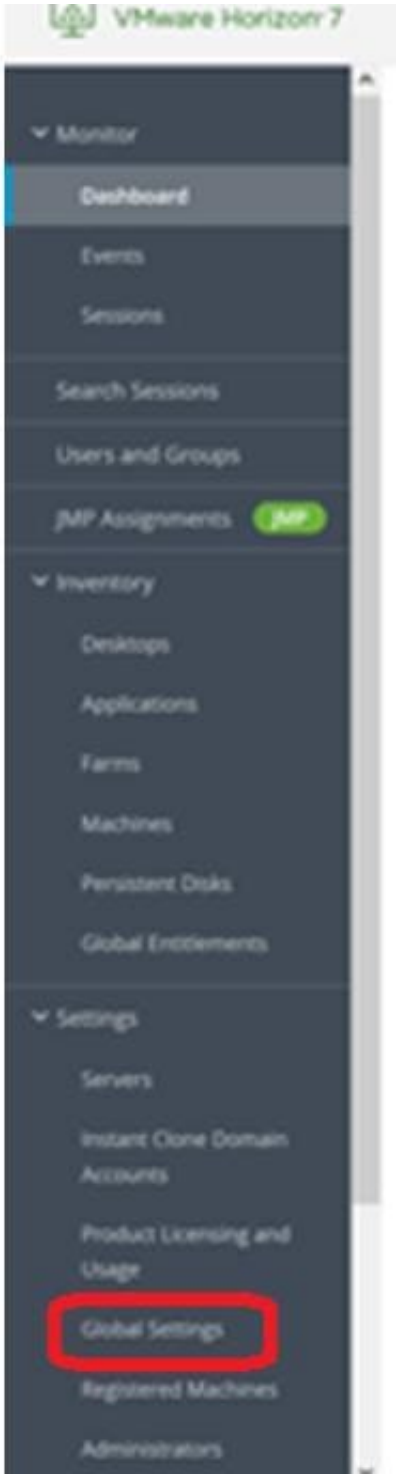
Mark the correct menu option where the administrator can enable Windows Server Operating Systems to be used as single-session desktops by clicking on it.

Hot Area:



Correct Answer:


Dashboard
10
VIEW
VIEW
4
Sessions



QUESTION 3

Which three steps are required to entitle user and groups to pools? (Choose three.)

A. Run the Active Directory entitlement script in the golden master, when preparing if for the pool.

B. During pool creation in the entitlement pane, click on add, search for users and groups in the Active Directory, continue and finish the pool creation.

C. During the Pool creation the desired Active Directory OU for the VMs will be specified. This will automatically add the preconfigured associated user group to the Horizon entitlements.

D. Navigate to Inventory > Desktops > check mark a pool > click on Add Entitlement.

E. Navigate to Users and Groups > Entitlements > click on Entitlements > click on Add Entitlements, search for users and groups in the Users pane and add the desired desktop pool in the next pane Desktop Pools.

Correct Answer: BDE

Explanation: To entitle users and groups to pools, you need to perform the following steps: During pool creation in the entitlement pane, click on add, search for users and groups in the Active Directory, continue and finish the pool creation. This option allows you to entitle users and groups to a desktop or application pool at the same time as you create the pool3. Navigate to Inventory > Desktops > check mark a pool > click on Add Entitlement. This option allows you to add entitlements to an existing desktop or application pool after you create the pool4. Navigate to Users and Groups > Entitlements > click on Entitlements > click on Add Entitlements, search for users and groups in the Users pane and add the desired desktop pool in the next pane Desktop Pools. This option allows you to review and manage the entitlements for users and groups from a single location5. The other options are not required or valid for entitling users and groups to pools. Running the Active Directory entitlement script in the golden master is not necessary as Horizon 8 automatically synchronizes with Active Directory domains that are configured in Horizon Console6. Specifying the desired Active Directory OU for the VMs during pool creation does not automatically add the preconfigured associated user group to the Horizon entitlements as you still need to select the users or groups from the search results7. References := 3: VMware Horizon 8 Documentation: Add Entitlements During Pool Creation 4: VMware Horizon 8 Documentation: Add Entitlements After Pool Creation 5: VMware Horizon 8 Documentation: Review and Manage Entitlements 6: VMware Horizon 8 Documentation: Active Directory Requirements forHorizon Connection Server 7: VMware Horizon 8 Documentation: Create an Automated Desktop Pool

QUESTION 4

An administrator is preparing to upgrade Horizon Connection Servers in parallel.

What action must first be performed to ensure that there are no issues with Horizon LDAP replication within the Pod?

A. Execute repadmin.exe/showrepl localhost:389.

B. Execute ViewDBChk.cmd --scanMachines.

C. Execute vdmexport.exe -f Myexport.lDF.

D. Execute vdmadmin.exe -S.

Correct Answer: A

Explanation: The action that must first be performed to ensure that there are no issues with Horizon LDAP replication within the Pod is to execute repadmin.exe/showrepl localhost:389. This command will display the replication status of the local Connection Server instance and show any errors or warnings that might affect the replication process1. The administrator should run this command on each Connection Server instance in the Pod before upgrading them in parallel, and resolve any issues that are reported. The other options are not valid or feasible because: Executing ViewDBChk.cmd --scanMachines will not check the Horizon LDAP replication status, but rather scan the vCenter Server inventory for virtual machines that are managed by Horizon and report any inconsistencies or errors2. This command is useful for troubleshooting virtual machine issues, but not for verifying LDAP replication. Executing vdmexport.exe -f Myexport.lDF will not check the Horizon LDAP replication status, but rather export the Horizon LDAP configuration data to a file named Myexport.lDF3. This command is useful for backing up or restoring the Horizon LDAP data, but not for verifying LDAP replication. Executing vdmadmin.exe -S will not check the Horizon LDAP replication status, but rather display the health status of the Connection Server instances in the Pod4. This command is useful for monitoring the

Connection Server performance and availability, but not for verifying LDAP replication. References: Repadmin Examples1 ViewDBChk Tool2 Back Up Horizon Configuration Data3 Display Health Status Information4

QUESTION 5

An administrator has added a supported PCI graphics accelerator to a virtual machine configuration. When the administrator tries to power on the virtual machine, an error is displayed and the virtual machine remains powered off.

Which of the following virtual machine configuration settings needs to be applied to enable the virtual machine to power on?

A. Enable Video Card 3D Graphics.

B. Reserve all guest memory.

C. Set Memory Shares to High.

D. Disable CPU Hot Plug.

Correct Answer: B

Explanation: To enable a virtual machine to power on with a PCI graphics accelerator, such as a GPU, attached to it, the administrator needs to reserve all guest memory for that virtual machine. This is because PCI devices require direct memory access (DMA) to function properly, and memory overcommitment can interfere with DMA operations. Reserving all guest memory ensures that no memory swapping or ballooning occurs on the virtual machine, and that the memory address space is contiguous and available for DMA56. The other options are not required or valid because: Enabling Video Card 3D Graphics is not necessary for using a PCI graphics accelerator. This option is for using software-accelerated graphics or virtual shared graphics acceleration (vSGA) on a virtual machine7. Setting Memory Shares to High does not guarantee that all guest memory will be reserved. Memory shares only affect how memory resources are distributed amongcompeting virtual machines when there is memory contention on the host. Memory shares do not prevent memory overcommitment or swapping. Disabling CPU Hot Plug does not affect the use of a PCI graphics accelerator. CPU Hot Plug allows adding or removing virtual CPUs from a powered-on virtual machine. It has no relation to PCI devices or DMA operations. References := 5: VMware vSphere 7 Documentation: Add a PCI Device to a Virtual Machine 6: VMware Knowledge Base: Enabling DirectPath I/O causes virtual machines to fail to power on (1010789) 7: VMware Workstation Pro Documentation: Prepare a Virtual Machine to Use Accelerated 3D Graphics : VMware vSphere Resource Management Documentation: Memory Resource Management : VMware vSphere Virtual Machine Administration Documentation: Hot Add Memory and CPU Resources