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.pass4itsure.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

What are two best practices for Windows Golden Image Optimization? (Choose two.)

A. Activate Windows OS paging.

B. Turn on automatic Windows maintenance (scheduled tasks).

C. Turn on automatic Windows Updates.

D. Disable unnecessary services.

E. Disable power options.

Correct Answer: DE

Explanation: Windows golden image optimization is the process of reducing the size and improving the performance of the Windows OS image that is used as the base for the desktop pools. Some of the best practices for Windows golden image optimization are: Disable unnecessary services: Services that are not required for the desktop functionality or user experience should be disabled to reduce the resource consumption and potential security risks. For example, services such as Windows Search, Windows Defender, Windows Update, and Superfetch can be disabled for better performance and stability. Disable power options: Power options such as hibernation and sleep mode should be disabled to free up disk space and avoid potential issues with the desktop state. Hibernation can consume a large amount of disk space by creating a hiberfil.sys file that stores the system memory contents when the desktop is powered off. Sleep mode can cause problems with network connectivity and user sessions when the desktop is resumed from a low-power state. Other best practices for Windows golden image optimization include: Activate Windows OS paging: Paging is a mechanism that allows the OS to use a portion of the disk as virtual memory when the physical memory is insufficient. Paging can improve the performance and stability of the desktops by preventing out-of-memory errors and reducing memory contention. However, paging can also increase disk I/O and wear, so it should be configured with caution and monitored regularly. Turn off automatic Windows maintenance (scheduled tasks): Automatic Windows maintenance is a feature that runs various tasks such as disk defragmentation, disk cleanup, security scanning, and system diagnostics in the background. These tasks can consume a lot of CPU, memory, and disk resources and interfere with the user experience and desktop performance. Therefore, it is recommended to turn off automatic Windows maintenance and run these tasks manually or on a scheduled basis when the desktops are not in use. Turn off automatic Windows Updates: Automatic Windows Updates is a feature that downloads and installs updates for the OS and other Microsoft products in the background. These updates can consume bandwidth, disk space, and CPUresources and cause compatibility issues with some applications or drivers. Therefore, it is recommended to turn off automatic Windows Updates and manage the updates manually or through a centralized tool such as VMware Update Manager or Microsoft WSUS. References: [Optimizing Your VMware Horizon View 7.x Golden Image] and [VMware Horizon 8.x Professional Course]

QUESTION 2

Having configured two standalone Horizon pods, what steps should be taken to join them in a Cloud Pod Architecture (CPA) deployment?

A. On one pod, initialize the CPA. On the second pod, join the CPA. On one pod, create Global Entitlements, and add local pools from each pod.

B. Initialize the CPA on both Pods. On the second pod, sync the CPA. On one pod, create Global Entitlements, and add local pools from each pod.

C. On one pod, initialize the CPA. On the second pod, join the CPA. On one pod, create Cloud Entitlements, and sync

pools from each pod. Initialize the CPA on both Pods.

D. On the second pod, sync the CPA. On one pod, create Cloud Entitlements, and add local pools from each pod.

Correct Answer: A

Explanation: To join two standalone Horizon pods in a Cloud Pod Architecture (CPA) deployment, the administrator needs to perform the following steps:

On one pod, initialize the CPA. This step creates a pod federation and enables global data replication among all pods in the federation. The pod that initializes the CPA becomes the first pod in the federation67.

On the second pod, join the CPA. This step adds an existing standalone pod to an existing pod federation. The pod that joins the CPA inherits the global data from the federation89.

On one pod, create Global Entitlements, and add local pools from each pod. This step allows users to access desktops or applications from any pod in the federation based on their entitlements and load-balancing policies . The other options

are not correct or complete because:

Initializing the CPA on both pods is not necessary or possible. Only one pod can initialize the CPA and create a pod federation. The other pods must join an existing pod federation68.

Syncing the CPA on the second pod is not a valid step. Syncing is a process that occurs automatically among all pods in a pod federation to ensure data consistency and availability.

Creating Cloud Entitlements is not a valid term. The correct term is Global Entitlements, which are used in CPA to entitle users to desktops or applications across multiple pods.

References := 6: VMware Horizon 8 Documentation: Initialize Cloud Pod Architecture 7:

VMware Horizon 8 Documentation: Understanding Cloud Pod Architecture in Horizon 8 8:

VMware Horizon 8 Documentation: Join a Pod to an Existing Pod Federation 9: VMware Horizon 8 Documentation: Understanding Cloud Pod Architecture in Horizon 8 : VMware Horizon 8 Documentation: Create a Global Entitlement :

VMware Horizon 8Documentation:

Understanding Global Entitlements in Cloud Pod Architecture : VMware Horizon 8 Documentation: Understanding Cloud Pod Architecture in Horizon 8

QUESTION 3

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 4

An administrator has been tasked with determining the type of VMware Horizon deployment for their organization.

These requirements have been provided to the administrator:

It must support Windows 10 Enterprise multi-session desktops.

It must support App Volumes.

It must support centralized brokering.

It must automatically route end-users to the most appropriate virtual workspace.

Which deployment solution meets the requirements?

A. VMware vSphere Desktop Edition

B. VMware Workspace ONE Unified Endpoint Management

C. VMware Horizon On-Premises

D. VMware Horizon Cloud on Microsoft Azure

Correct Answer: D

Explanation: VMware Horizon Cloud on Microsoft Azure is the only deployment solution that meets all the requirements. VMware Horizon Cloud on Microsoft Azure supports Windows 10 Enterprise multi-session desktops, which are a new Remote Desktop Session Host exclusive to Azure Virtual Desktop on Azure1. It also supports App Volumes, which is a real-time application delivery system that enables IT to instantly provision applications to users or desktops. VMware Horizon Cloud on Microsoft Azure supports centralized brokering, which means that the Horizon Cloud Service acts as a single point of entry for end users to access their virtual desktops and applications. VMware Horizon Cloud on Microsoft Azure also supports automatic routing of end-users to the most appropriate virtual workspace, using the Universal Broker feature. Universal Broker is a cloud-based brokering service that provides a unified user experience across multiple Horizon pods and clouds. VMware vSphere Desktop Edition does not support Windows 10 Enterprise multi-session desktops, as they are only available on Azure Virtual Desktop1. VMware Workspace ONE Unified Endpoint Management does not support App Volumes, as it is a different solution for managing devices and applications. VMware Horizon On-Premises does not support automatic routing of end-users to the most appropriate virtual workspace, as it requires manual configuration of load balancing and global entitlements. References: Profile production applications in Azure with Application Insights Profiler1 Using Application Profiler - VMware Docs2 First look at profiling tools - Visual Studio (Windows)3 App Volumes Overview Horizon Cloud Service on Microsoft Azure Architecture Universal Broker Overview Workspace ONE UEM Overview Load Balancing Across Pods and Sites in a Cloud Pod Architecture Environment

QUESTION 5

Which two scenarios are appropriate for a cloud implementation of a VDI solution over an on-premises solution? (Choose two.)

A. The organization already has infrastructure to support a VDI.

B. The organization needs to setup high availability and disaster recovery.

C. The organization needs to quickly scale-up in disparate geographical locations.

D. The organization has limited CapEx budget.

E. The organization controls highly confidential data.

Correct Answer: CD

Explanation: A cloud implementation of a VDI solution over an on-premises solution is appropriate for the following scenarios:

The organization needs to quickly scale-up in disparate geographical locations. A cloud VDI solution can provide faster provisioning, deployment, and management of virtual desktops and applications across multiple regions and data centers.

A cloud VDI solution can also offer better performance, availability, and user experience for remote and mobile workers who need to access their desktops and applications from anywhere and any device12.

The organization has limited CapEx budget. A cloud VDI solution can reduce the upfront capital expenditure (CapEx) required to purchase, install, and maintain the hardware and software infrastructure for a VDI solution. A cloud VDI solution

can also lower the operational expenditure (OpEx) by shifting the responsibility of managing, updating, and securing the VDI infrastructure to the cloud provider. A cloud VDI solution can offer flexible and predictable pricing models based on

usage, subscription, or consumption13.

The other scenarios are not appropriate for a cloud implementation of a VDI solution over an on-premises solution because:

The organization already has infrastructure to support a VDI. If the organization has already invested in the hardware and software resources to support a VDI solution, it may not be cost-effective or feasible to migrate to a cloud VDI solution.

The organization may also have existing policies, processes, and workflows that are tailored to the on-premises VDI solution and may not be compatible with the cloud VDI solution4.

The organization needs to setup high availability and disaster recovery. While a cloud VDI solution can provide high availability and disaster recovery capabilities, it may not be sufficient or reliable for some organizations that have strict

requirements for data protection, compliance, and business continuity. An on- premises VDI solution can offermore control, customization, and security over the backup, replication, and restoration of the VDI data and applications in the event

of a disaster5.

The organization controls highly confidential data. A cloud VDI solution may pose some risks or challenges for organizations that handle sensitive or regulated data, such as financial, healthcare, or government data. A cloud VDI solution may

not meet the compliance standards or regulations that apply to the organization\\'s data. A cloud VDI solution may also expose the organization\\'s data to potential breaches, leaks, or unauthorized access by third parties. An on-premises VDI

solution can provide more visibility, governance, and encryption over the organization\\'s data6.

References := 1: VMware: What is Desktop as a Service (DaaS)? 2: Parallels: VDI in the Cloud: Which Cloud VDI Product Is Right for You? 3: Microsoft Azure: What Is Virtual Desktop Infrastructure (VDI)? 4: VMware: On-Premise vs Cloud:

Which is Better for Your Business? 5: VMware: Disaster Recovery Solutions for Virtual Desktop Infrastructure (VDI) 6: Microsoft Azure: Virtual desktop infrastructure security best practices