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

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 2

What is the default URL used to access the Horizon Console?

A. https:///admin

B. https:///default

C. https:///administrator

D. https:///login

Correct Answer: A

Explanation: The default URL used to access the Horizon Console is https:///admin, where is the fully qualified domain name of the Connection Server instance. This URL allows you to log in to Horizon Console by using a secure (TLS) connection. You can also use the IP address of the Connection Server instance instead of the FQDN, but this might result in blocked access or reduced security due to certificate mismatch. You cannot use https://localhost to connect fromthe Connection Server host, but you can use https://127.0.0.1 instead. The other options are not valid URLs for Horizon Console. References: Log In to Horizon Console

QUESTION 3

A junior-level Horizon administrator is not able to see all RDS farms.

Where would a high-level administrator need to make changes to correct the issue?

A. Category Folder

B. Access Groups

C. Global Entitlements

D. Global Policies

Correct Answer: B

Explanation: Access groups are a way of organizing and delegating the administration of machines, desktop pools, application pools, and farms in Horizon. By default, all these objects reside in the root access group, which appears as / or Root (/) in Horizon Console. A high-level administrator can create sub-access groups under the root access group and assign different permissions to different administrators for each access group. For example, a high-level administrator can create an access group called RDS Farms and assign the Inventory Administrators role to a junior-level administrator for that access group. This way, the junior-level administrator can see and manage all the RDS farms that are in the RDS Farms access group, but not the ones that are in other access groups or the root access group. Therefore, to correct the issue of a junior-level administrator not being able to see all RDS farms, a high-level administrator needs to make changes to the access groups and the permissions associated with them. References: Understanding Permissions and Access Groups and [VMware Horizon 8.x Professional Course]

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 is configuring load-balancing settings in Horizon Console for a RDSH Farm. Which two check boxes can be selected to influence the load balancing behavior? (Choose two.)

A. The floating dynamic host profile setting, created in the vSphere profile section.

B. The use custom script setting for customized RDSH load balancing.

C. The Include Session Count setting to include the session count on the RDSH for load balancing.

D. The Horizon DRS setting for fully automated vSphere load balancing.

Correct Answer: BC

Explanation: Load balancing is a feature that allows administrators to distribute the load of published desktop and application sessions across multiple RDS hosts in a farm. Load balancing can improve the performance and availability of the sessions and the hosts. Horizon offers two ways of configuring load balancing for RDS hosts: using load balancing settings in Horizon Console or using custom load balancing scripts. The load balancing settings in Horizon Console allow administrators to define how Horizon calculates the server load index, which indicates the load on each RDS host. The server load index can range from 0 to 100, where 0 represents no load and 100 represents full load. A server load index of -1 indicates that load balancing is disabled. Horizon uses the server load index to determine which RDS host is the best candidate for placing a new session request. The load balancing settings in Horizon Console include the following check boxes that can be selected to influence the load balancing behavior: The use custom script setting for customized RDSH load balancing: This setting allows administrators to override the default behavior of the load balancing settings and control the placement of new sessions by writing and configuring custom load balancing scripts. The custom scripts must write the server load index to a specific registry key on each RDS host. Horizon will use the value from the registry key instead of calculating it from the other settings. The Include Session Count setting to include the session count on the RDSH for load balancing: This setting allows administrators to include the number of sessions (connected, pending, and disconnected) on each RDS host as a factor in calculating the server load index. By

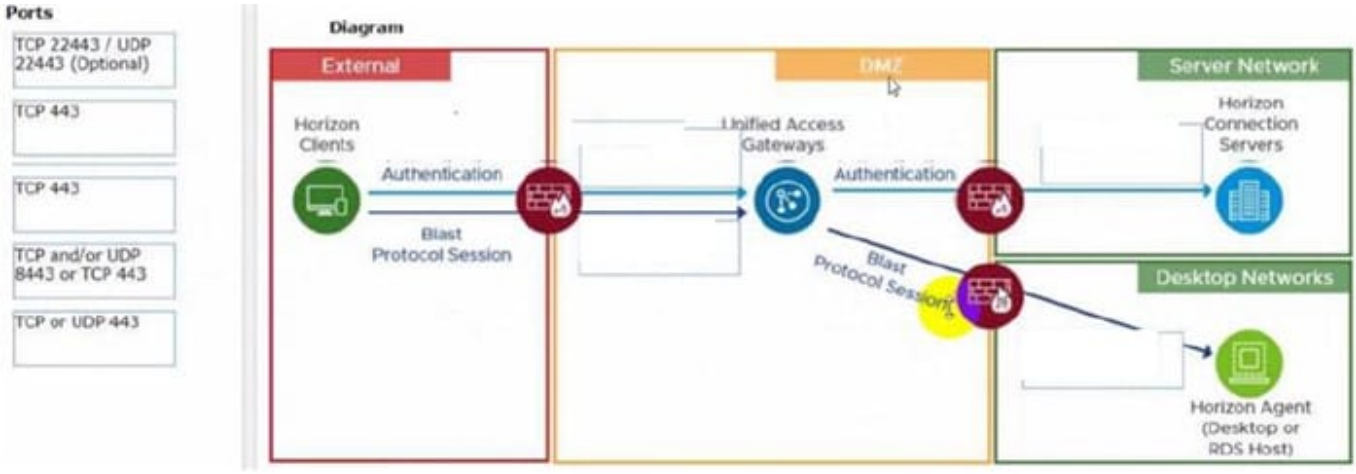
default, Horizon uses the following formula to calculate the server load index based on the session count: (connected sessions + pending sessions + disconnected sessions)/ (maximum session count). If the maximum session count is configured as unlimited, Horizon falls back to using the absolute number of total sessions. The other options are not check boxes that can be selected in the load balancing settings in Horizon Console: The floating dynamic host profile setting, created in the vSphere profile section: This option is not related to load balancing for RDS hosts, but rather to dynamic environment manager for instant-clone desktops. A dynamic host profile is a vSphere profile that contains configuration settings for instant-clone desktops, such as network settings, domain join settings, and customization scripts. A floating dynamic host profile is a type of dynamic host profile that applies to floating desktop pools, where users are assigned a random desktop from a pool at each login. The Horizon DRS setting for fully automated vSphere load balancing: This option is not related to load balancing for RDS hosts, but rather to distributed resource scheduler (DRS) for vSphere clusters. DRS is a feature that monitors and balances the CPU and memory resources across multiple ESXi hosts in a cluster. DRS can also migrate virtual machines between hosts using vMotion to optimize resource utilization and performance. Horizon DRS is an extension of DRS that integrates with Horizon and provides additional capabilities, such as affinity rules, maintenance mode, and power management. Horizon DRS can be configured with different automation levels, such as fully automated, partially automated, or manual. References: Configuring Load Balancing for RDS Hosts in Horizon Console, Load Balancing Settings, Load Balancing Scripts, [Dynamic Host Profiles], and [VMware Horizon 8.x Professional Course]

QUESTION 6

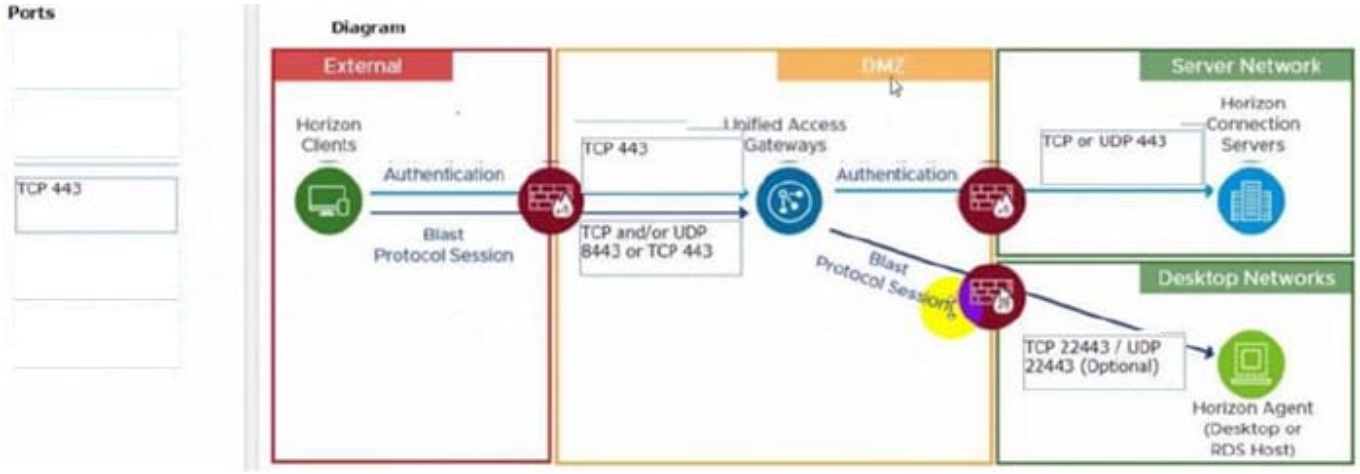
Refer to the exhibit.

Drag and drop the ports on the left to allow an external Blast Extreme connection through Unified Access Gateway (UAG) into the diagram on the right.

Select and Place:



Correct Answer:



C:\Users\Waqas Shahid\Desktop\Mudassir\Untitled.jpg

QUESTION 7

Adobe Acrobat 11 has been assigned to a user. VM25 already has Adobe Acrobat 11 and is natively installed. What happens when the user logs on to VM25?

A. The App Volume package does not get attached because the natively installed application has priority.

B. The user-assigned application is attached to VM25. When the user clicks on the application shortcut, the App Volume package for Adobe Acrobat 11is opened.

C. Although a shortcut to the App Volume package is created on the user desktop, the application does not get attached to VM25.

D. A shortcut to the user-assigned application is created on the user desktop, and when they click on the shortcut, the application gets attached to VM25.

Correct Answer: B

Explanation: App Volumes is a real-time application delivery system that allows administrators to assign applications to users and groups in Horizon. App Volumes uses virtual disks called packages to store and deliver applications. When a user logs on to a desktop, the App Volumes agent attaches the assigned packages to the desktop and merges them with the OS disk. The user can then access the applications as if they were natively installed. In this scenario, Adobe Acrobat 11 has been assigned to a user as an App Volumes package. When the user logs on to VM25, which already has Adobe Acrobat 11 natively installed, the App Volumes agent attaches the package to VM25 and creates a shortcut on the user desktop. However, the package does not overwrite or conflict with the natively installed application. Instead, when the user clicks on the shortcut, the App Volumes package for Adobe Acrobat 11 is opened and runs in an isolated environment. This allows the user to use different versions of the same application without affecting each other or the OS. References: App Volumes Architecture and [VMware Horizon 8.x Professional Course]

QUESTION 8

An administrator wants to deploy a RDS farm which can be patched in a rolling process with zero downtime. Which of the following statements is true in this scenario?

A. This cannot be done as updating a Farm always incurs downtime.

B. Create an instant-clone RDS desktop farm.

C. Create a manual RDS desktop farm.

D. Nothing needs to be done. All RDS farms can be patched in a rolling process with zero downtime.

Correct Answer: B

Explanation: Instant clones are a type of virtual machines that are created by cloning a running parent VM in memory, without requiring a full disk copy. This allows for faster provisioning and updating ofRDS hosts in a farm. Instant clones can be patched in a rolling process with zero downtime by using the push-image operation, which replaces the existing instant clones with new ones that have the latest patches applied. The push-image operation can be performed on a per-farm basis or on multiple farms at once. The push- image operation preserves the user sessions and data on the existing instant clones until they are logged off or disconnected, and then deletes them. The new instant clones inherit the same settings and assignments as the old ones. Therefore, to deploy a RDS farm that can be patched in a rolling process with zero downtime, the administrator should create an instant-clone RDS desktop farm. References: Instant Clones for RDSH in VMware Horizon 7.1 and [VMware Horizon 8.x Professional Course]

QUESTION 9

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

QUESTION 10

What are the steps to create a custom role?

A. In the navigation pane under the Settings section dick on Administrators > Roles and Permission > Add. Once the Add Role pane opens, add a name for the role and select the specific privileges.

B. In the navigation pane under the Settings section click on Administrators > Roles and Permission > Users and groups > Add. Once the Add Role pane opens, add a name for the role and select the specific privileges.

C. In the navigation pane under the Settings section click on Administrators > Entitlements > Add. Once the add Role pane opens, add a name for the role and select the specific privileges.

D. In the navigation pane under the Settings section click on Administrators > Users and Groups > Add. Once the Add Role pane opens, add a name for the role and select the specific privileges.

Correct Answer: A

Explanation: Roles and permissions are a way of controlling the access and actions of administrators and users in Horizon. By default, Horizon provides two predefined roles:

Administrators and Read Only Administrators. However, a high-level administrator can create custom roles with specific privileges to suit different needs and scenarios. To create a custom role, the administrator needs to follow these steps:

In the navigation pane under the Settings section, click on Administrators > Roles and Permissions.

In the Roles and Permissions page, click on Add. In the Add Role pane, enter a name for the role in the Role Name text box. In the Privileges section, select the checkboxes for the privileges that you want to assign to the role. You can

expand or collapse the categories to view or hide the sub-privileges. You can also use the Select All or Deselect All buttons to select or clear all the privileges in a category.

Click on Save to create the custom role.

The custom role will appear in the Roles and Permissions page, where you can edit or delete it as needed. You can also assign the custom role to users or groups in the Users and Groups page. References: [Create Custom Roles] and

[VMware Horizon 8.x Professional Course]