2V0-51.23$^{Q\&As}$

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.pass2lead.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

QUESTION 1

What are two Cloud Pod Architecture feature limitations? (Choose two.)

A. Cloud Pod Architecture does not support Active Directory two-way trusts between domains.

B. Cloud Pod Architecture is not supported with Unified Access Gateway appliances.

C. Kiosk mode clients are not supported unless a workaround has been implemented.

D. Cloud Pod Architecture cannot span multiple sites and data centers simultaneously.

E. The Cloud Pod Architecture feature is not supported in an IPv6 environment.

Correct Answer: AC

Explanation: Cloud Pod Architecture is a feature that allows administrators to link multiple Horizon pods across sites and data centers to form a single logical entity called a pod federation. Cloud Pod Architecture enables global entitlements,

which allow users to access desktops and applications from any pod in the pod federation. Cloud Pod Architecture also provides load balancing, high availability, and disaster recovery capabilities for Horizon deployments.

However, Cloud Pod Architecture has some feature limitations that administrators should be aware of. Two of these limitations are:

Cloud Pod Architecture does not support Active Directory two-way trusts between domains: This means that the domains that contain the Horizon pods in the pod federation must have a one-way trust relationship, where the domain that

contains the Cloud Pod Architecture home site trusts all the other domains, but not vice versa. A two-way trust relationship, where each domain trusts and is trusted by all the other domains, is not supported by Cloud Pod Architecture and can

cause authentication and entitlement issues.

Kiosk mode clients are not supported unless a workaround has been implemented:

This means that users who log in to Horizon Client in kiosk mode, which is a mode that allows users to access a single desktop or application without entering credentials, cannot access desktops or applications from a Cloud Pod Architecture

implementation. Kiosk mode clients are not compatible with global entitlements and load balancing features of Cloud Pod Architecture. However, there is a workaround that involves creating a dedicated user account and a dedicated desktop

pool for each kiosk mode client and using a script to launch Horizon Client with the appropriate parameters. For instructions, see VMware Knowledge Base (KB) article 21488881.

The other options are not limitations of Cloud Pod Architecture:

Cloud Pod Architecture is supported with Unified Access Gateway appliances:

Unified Access Gateway is a platform that provides secure edge services for Horizon deployments, such as secure remote access, load balancing, and authentication. Unified Access Gateway is compatible with Cloud Pod Architecture and can be configured to route user requests to the appropriate pod in the pod federation based on global entitlements and load balancing policies. Cloud Pod Architecture can span multiple sites and data centers simultaneously:

This is one of the main benefits of Cloud Pod Architecture, as it allows administrators to scale up and out their Horizon deployments across different geographic locations and network boundaries. Cloud Pod Architecture can support up to 15

pods per pod federation andup to 5 sites per pod federation, with a maximum of 200,000 sessions per pod federation.

The Cloud Pod Architecture feature is supported in an IPv6 environment: IPv6 is the latest version of the Internet Protocol that provides a larger address space and enhanced security features for network communication. Cloud Pod

Architecture supports IPv6 environments and can operate in mixed IPv4 and IPv6 environments as well.

References: Cloud Pod Architecture Limitations in Horizon 8 and [VMware Horizon 8.x Professional Course]

QUESTION 2

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]

QUESTION 3

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 4

To reduce the risk of users downloading malware to the corporate network, an administrator wants to allow end-users to open only intranet websites inside their virtual desktop. Additionally, the administrator wants to configure all other URLs to automatically open in a browser on the end-user\\'s client machine.

Which steps should the administrator take to meet the requirements? (Choose two.)

A. Enable the URL Content Redirection feature in Horizon Agent.

B. Disable the Allow External Website feature in Horizon Agent.

C. Enable secure website settings in the Global Settings Security menu.

D. Configure group policy settings to indicate how Horizon Agent redirects the URL

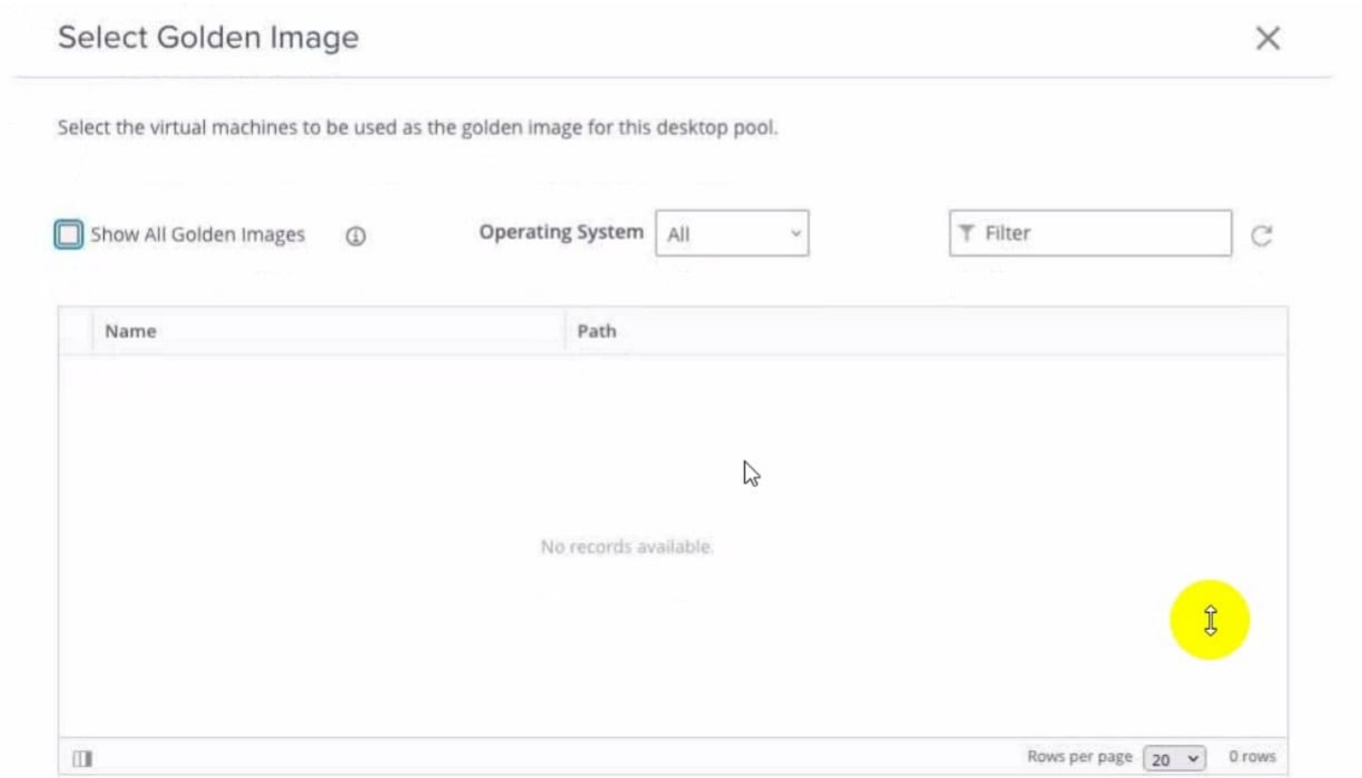
E. Enable the URL Content Redirection feature on the desktop pool settings.

Correct Answer: AD

Explanation: The URL Content Redirection feature allows administrators to configure specific URLs to open on the client machine or in a remote desktop or published application. This can help reduce the risk of users downloading malware to the corporate network, as well as improve the user experience and performance of certain web applications. To meet the requirements of the scenario, the administrator needs to enable the URL Content Redirection feature in Horizon Agent when installing or upgrading it on the instant- clone desktops. This will allow Horizon Agent to send or receive URLs from Horizon Client, depending on the redirection direction. The administrator also needs to configure group policy settings to indicate how Horizon Agent redirects the URL. Specifically, the administrator needs to enable agent-to-client redirection, which means that Horizon Agent sends the URL to Horizon Client, which opens the default application for the protocol in the URL on the client machine. The administrator also needs to specify which URLs are redirected from a remote desktop to a client, and which URLs are not redirected. In this case, the administrator needs to configure a whitelist of intranet websites that are allowed to open inside the virtual desktop, and a blacklist of all other websites that are automatically redirected to a browser on the client machine. The other options are not relevant or sufficient for meeting the requirements. Disabling the Allow External Website feature in Horizon Agent will prevent users from accessing any external websites from their virtual desktops, which might not be desirable or practical. Enabling secure website settings in the Global Settings Security menu will not affect how URLs are redirected, but only how secure connections are establishedbetween Horizon components. Enabling the URL Content Redirection feature on the desktop pool settings will not work unless it is also enabled in Horizon Agent and configured with group policy settings. References: Configuring URL Content Redirection and [VMware Horizon 8.x Professional Course]

QUESTION 5

Refer to the exhibit.



Select Golden Image

Select the virtual machines to be used as the golden image for this desktop pool.

□ Show All Golden Images

Operating System: All

Filter

Name	Path

No records available.

Rows per page 20 · 0 rows

An administrator is tasked with creating an instant clone pool for their sales department. During the creation of the pool the administrator saw that there is no golden image available, as seen in the exhibit.

Which two actions can an administrator take so that the golden image is showing up in the Golden Image selection window? (Choose two.)

A. Login to the vSphere Client, select the Golden Image virtual machine and delete all snapshots.

B. Login to the vSphere Client, select the Golden Image virtual machine and create a snapshot

C. Refresh the Select Golden Image view and select the Golden Image.

D. Login to the vSphere Client, select the Golden Image virtual machine and clone it to a new virtual machine.

E. Login to the vSphere Client, select the Golden Image virtual machine and convert it to a template.

Correct Answer: BE

Explanation: The administrator can take two actions to make the golden image show up in the Golden Image selection window. First, they can login to the vSphere Client, select the Golden Image virtual machine and create a snapshot. This will make the golden image available in the selection window. Second, they can login to the vSphere Client, select the Golden Image virtual machine and convert it to a template. This will also make the golden image available in the selection window. A golden image is a virtual machine that contains the operating system, applications, and settings that are required for an instant clone desktop pool. To create an instant clone desktop pool, the administrator must select a golden image and a snapshot from the vSphere inventory. The snapshot must be taken after installing and configuring the Horizon Agent on the golden image1. If there is no snapshot or no template available, the golden image will not show up in the selection window. The other options are not correct for this scenario: Login to the vSphere Client, select the Golden Image virtual machine and delete all snapshots. This option is not correct because deleting all snapshots will not make the golden image show up in the selection window. In fact, it will prevent the administrator from creating an instant clone desktop pool, as a snapshot is required for instant cloning2. Refresh the Select Golden Image view and select the Golden Image. This option is not correct because refreshing the view will not change the availability of the golden image in the selection window. The administrator must create a snapshot or a template of the golden image before it can be selected. Login to the vSphere Client, select the Golden Image virtual machine and clone it to a new virtual machine. This option is not correct because cloning the golden image to a new virtual machine will not make it show up in the selection window. The administrator must still create a snapshot or a template of the cloned virtual machine before it can be selected. References: Preparing a Golden Image Virtual Machine for Instant-Clones Snapshot vmdk files of the golden image used to publish Instant clone ... Create an Automated Instant-Clone Desktop Pool Instant Clone Desktop Pools [VMware Horizon 8.x Professional]

Latest 2V0-51.23 Dumps   2V0-51.23 PDF Dumps   2V0-51.23 Study Guide