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

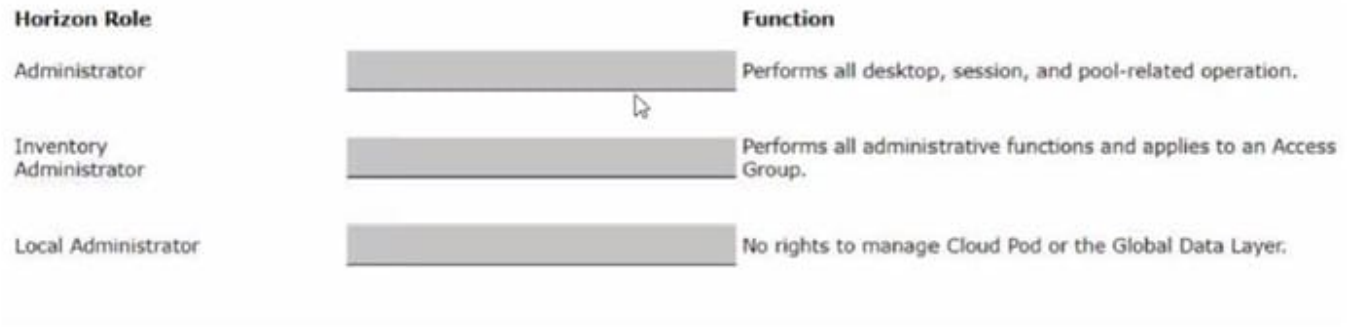
Following Questions and Answers are all new published by VMware Official Exam Center

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

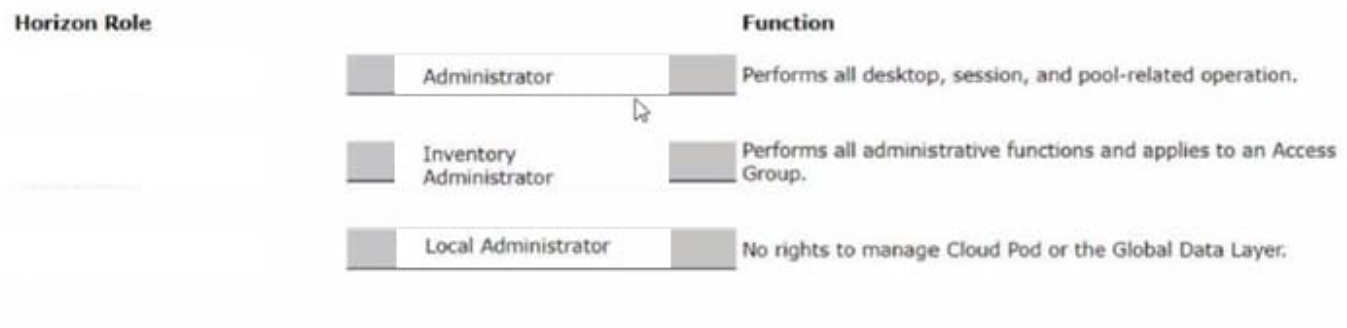
QUESTION 1

Drag and drop each Horizon console predefined role on the left to its matching function on the right.

Select and Place:



Correct Answer:



The following is the correct answer for the drag and drop question:

Administrator -> Performs all desktop, session, and pool-related operation.

Inventory Administrator -> Performs all administrative functions and applies to an Access Group.

Local Administrator -> No rights to manage Cloud Pod or the Global Data Layer.

Predefined Administrator Roles (vmware.com)

The predefined administrator roles in Horizon console are designed to provide different levels of access and control over the Horizon environment. Each role has a set of privileges that grant the ability to perform specific actions or view certain

information. You can assign these roles to users or groups on the root access group, which gives them access to all inventory objects in the system, or on a specific access group or federation access group, which limits their scope to the

objects within that group. You cannot modify the predefined roles, but you can create custom roles by selecting individual privileges.

The Administrator role is the most powerful role in Horizon console. It allows the user to perform all administrative operations, including creating and managing desktop pools, sessions, farms, applications, global settings, and other

administrators. In a Cloud Pod Architecture environment, this role also enables the user to configure and manage a pod federation and manage remote pod sessions. The Administrator role on the root access group is equivalent to a super

user role, as it gives full access to everything in the system. Therefore, you should assign this role to a limited number of users.

The Inventory Administrator role is similar to the Administrator role, but it applies only to an access group. This means that the user can perform all administrative functions on the inventory objects that belong to that access group, such as

desktop pools, farms, applications, and sessions. However, the user cannot manage global settings or other administrators. This role is useful for delegating administration of specific resources to different users or groups.

The Local Administrator role is a restricted version of the Inventory Administrator role. It applies only to an access group and does not grant any rights to manage Cloud Pod Architecture features or the Global Data Layer. This means that the

user can only manage local inventory objects within that access group, such as desktop pools, farms, applications, and sessions. This role is suitable for administrators who do not need to access or modify global settings or cross-pod

resources.

The Help Desk Administrator role is a specialized role that allows the user to perform desktop and application actions for troubleshooting and support purposes. These actions include shutting down, resetting, restarting, logging off,

disconnecting, and sending messages to users

QUESTION 2

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 3

End-users are complaining that they are frequently being asked for credentials when opening additional apps. Which step should the administrator take to resolve the issue?

A. Configure SSO Timeout by modifying the Global Settings in Horizon Administrator.

B. Configure a time limit by modifying the Horizon GPO.

C. Configure Desktop Timeout by modifying the Pool Settings in Horizon Administrator.

D. Configure Session Timeout by modifying the Client Settings in Horizon Client.

Correct Answer: A

Explanation: Single sign-on (SSO) is a feature that allows users to log in to Horizon Client once and launch remote desktops and applications without being prompted for credentials again. SSO is enabled by default and can be configured in the Global Settings of Horizon Administrator. One of the settings is SSO Timeout, which determines how long the user\\'s credentials are cached before they expire. If the SSO Timeout is too short, users might be frequently asked for credentials when opening additional apps. To resolve this issue, the administrator can increase the SSO Timeout value or set it to -1, which means that no SSO timeout limit is set. References: Global Settings for Client Sessions in Horizon Console and [VMware Horizon 8.x Professional Course] https://docs.vmware.com/en/VMware-Horizon-7/7.13/horizon-console-administration/GUID- E2A7CA32-193D-43D9-B08E-DD20CAE9CA28.html

QUESTION 4

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

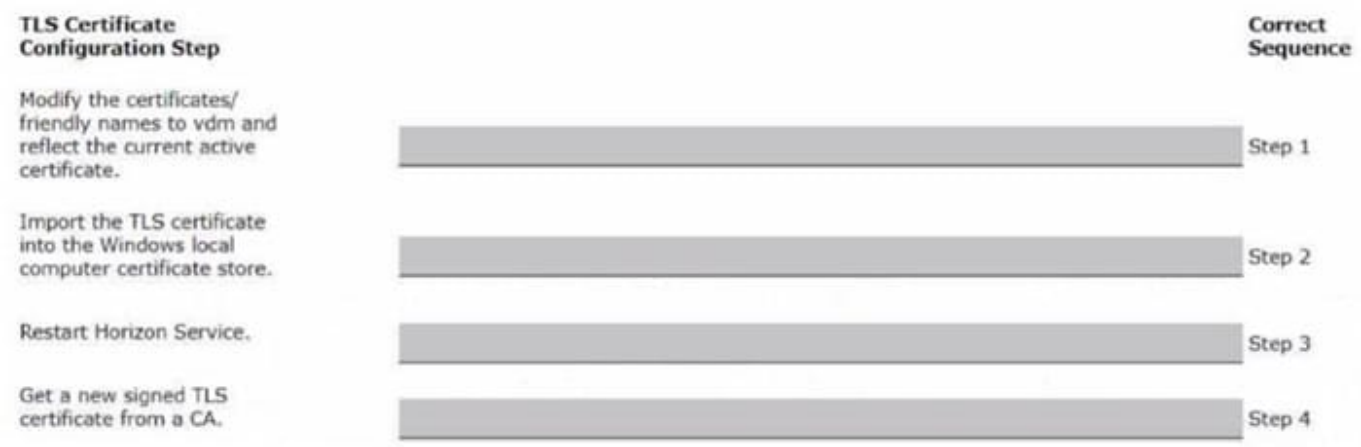
Architecture supports IPv6 environments and can operate in mixed IPv4 and IPv6 environments as well.

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

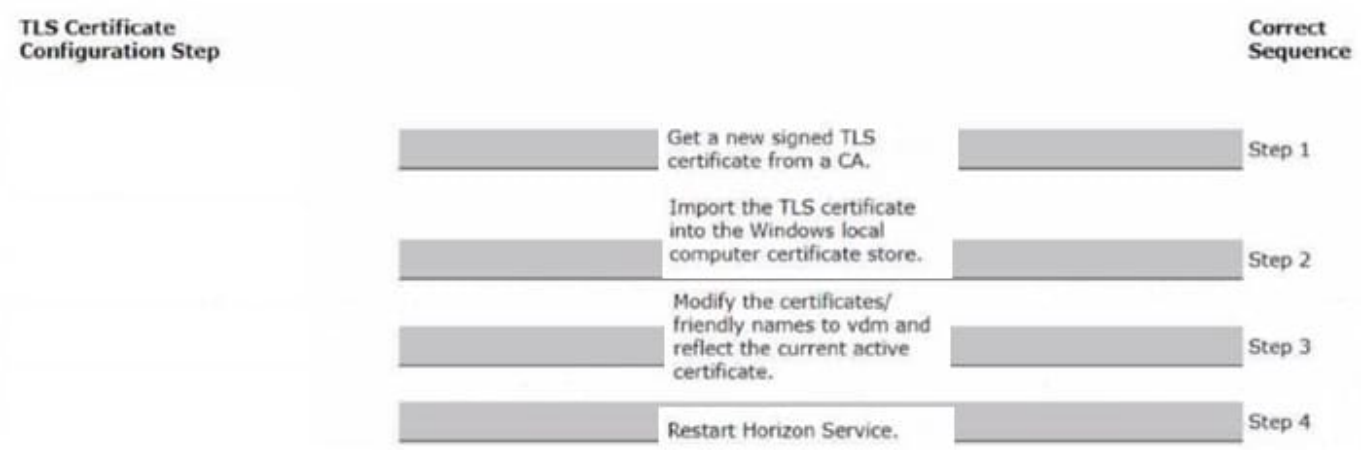
QUESTION 5

Drag and drop the TLS Configuration steps on the left into the correct sequential order on the right.

Select and Place:



Correct Answer:



To correctly sequence the TLS Certificate Configuration Steps:

Get a new signed TLS certificate from a CA.Before making any modifications or importing the certificate, you\\'ll first need to obtain a new signed TLS certificate from a Certificate Authority (CA). So, this should beStep 1.

Import the TLS certificate into the Windows local computer certificate store.After obtaining the new signed TLS certificate, the next logical step is to import this certificate into the Windows local computer certificate store. This would beStep 2.

Modify the certificates/ friendly names to vdm and reflect the current active certificate.Once the certificate is imported, the next step is to modify its friendly names to ensure the Horizon Service recognizes and uses this certificate. This

becomesStep 3.

Restart Horizon Service.Finally, after all the modifications and configurations are done, you should restart the Horizon Service to apply the changes. This isStep 4.