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.leads4pass.com/2v0-51-23.html

100% Passing Guarantee
100% Money Back Assurance

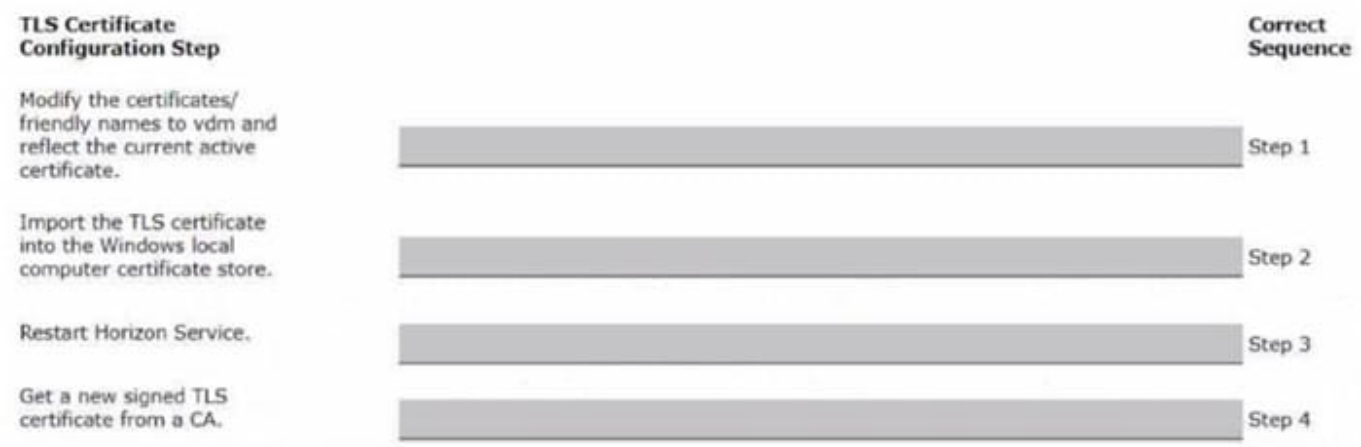
Following Questions and Answers are all new published by VMware Official Exam Center

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

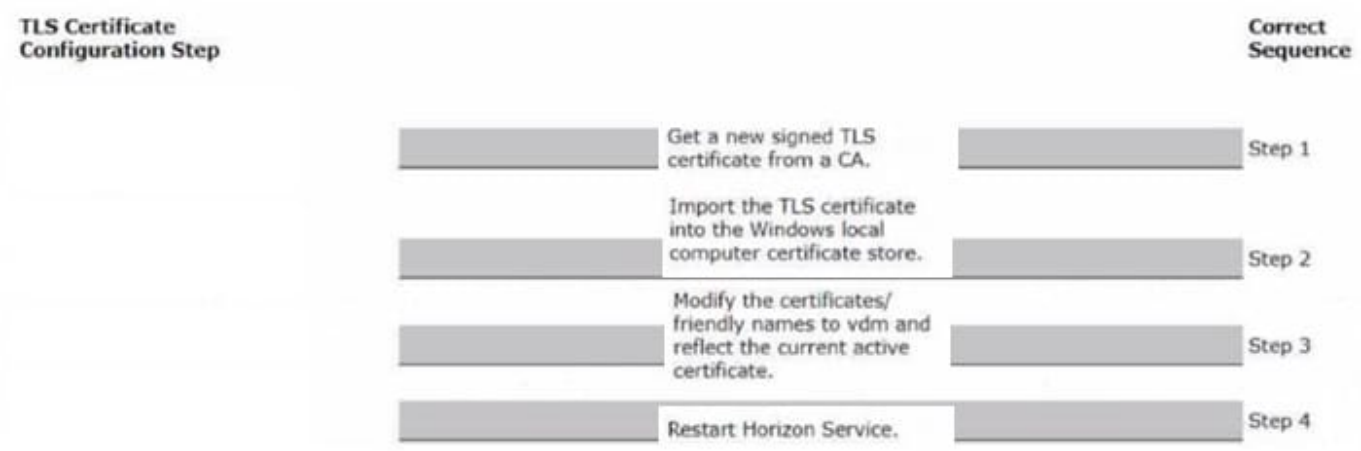
QUESTION 1

Drag and drop 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.

QUESTION 2

Which three of the following are benefits of using Virtual Machines? (Choose three.)

A. Difficult to move or copy.

B. Independent of physical hardware.

C. Faster to provision.

D. Bound to a specific set of hardware components.

E. Easy to move or copy.

Correct Answer: BCE

Explanation: One of the benefits of using virtual machines is that they are independent of physical hardware. This means that they can run on any compatible host machine, regardless of the underlying hardware components. This also enables them to be migrated, moved, or copied easily from one host to another, without requiring any reconfiguration or installation. This enhances the flexibility and portability of virtual machines, as well as their availability and disaster recovery. Another benefit of using virtual machines is that they are faster to provision than physical machines. This is because they can be created from templates or snapshots, which contain preconfigured operating systems and applications. This reduces the time and effort needed to install and configure software on each machine. Moreover, virtual machines can be cloned or duplicated quickly, allowing for rapid scaling and deployment of multiple identical instances. References := Virtual Machines Overview Creating and Provisioning Virtual Machines Migrating Virtual Machines

QUESTION 3

In a load balanced Horizon POD with three Connection Servers, there are 450 active Blast sessions connected. What happens if one of these Connection Servers runs into an unplanned outage?

A. All 450 active sessions are disconnected, and have to re-connect again by the end-user.

B. All active sessions will stay connected, because HTTPS Secure Tunnel and Blast Secure Gateway are disabled.

C. All 450 active session are logged off immediately.

D. Only the active sessions from the failed Connection Server are disconnected, because HTTPS Secure Tunnel is disabled.

Correct Answer: D

In a load balanced Horizon POD with three Connection Servers, there are 450 active Blast sessions connected. If one of these Connection Servers runs into an unplanned outage, only the active sessions from the failed Connection Server are disconnected, because HTTPS Secure Tunnel is disabled. This means that the other two Connection Servers can still handle the remaining sessions without interruption. The HTTPS Secure Tunnel is a feature that allows Horizon Client devices to establish secure connections to virtual desktops and applications through the Connection Server.

When this feature is enabled, all the display protocol traffic is tunneled through the Connection Server, which acts as a proxy between the client and the desktop. This increases the security and simplifies the network configuration, but also adds some overhead and dependency on the Connection Server availability1. When this feature is disabled, the Horizon Client devices connect directly to the desktops using their IP addresses or hostnames, bypassing the Connection Server. This reduces the load and dependency on the Connection Server, but also requires more network configuration and firewall rules to allow direct access to the desktops2. The Blast Secure Gateway is a similar feature that allows Horizon Client devices to establish secure connections to virtual desktops and applications using the Blast Extreme protocol through the Connection Server. When this feature is enabled, the Blast Extreme traffic is tunneled through the Connection Server, which acts as a gateway between the client and the desktop. When this feature is disabled, the Horizon Client devices connect directly to the desktops using Blast Extreme3. In this scenario, both HTTPS Secure Tunnel and Blast Secure Gateway are disabled, which means that the Horizon Client devices connect directly to the desktops using Blast Extreme. Therefore, if one of the Connection Servers fails, only the sessions that were authenticated by that Connection Server are affected. The other sessions can continue without interruption, as long as they can reach their desktops directly4. The other options are not correct for this scenario: All 450 active sessions are disconnected, and have to re-connect again by the end-user. This would be true if HTTPS Secure Tunnel or Blast Secure Gateway were enabled, and all the display protocol traffic was tunneled through the Connection Server. In that case, any failure of a Connection Server would disconnect all the sessions that were using it as a proxy5. All active sessions will stay connected, because HTTPS Secure Tunnel and Blast Secure Gateway are disabled. This would be true if there was no dependency on the Connection Server after authentication. However, even with HTTPS Secure Tunnel and Blast Secure Gateway disabled, there is still some communication between the Horizon Client and the Connection Server for session management and heartbeat monitoring. If a Connection Server fails, these communications are lost and the sessions are terminated. All 450 active session are logged off immediately. This would be true if there was a global setting in Horizon Console to log off users when a Connection Server fails. However, there is no such setting in Horizon Console. The default behavior is to disconnect users when a Connection Server fails, not log them off. References: Configuring HTTPS Secure Tunnel Configuring Network Ports for Direct Connections Configuring Blast Secure Gateway Load Balancing Across Multiple Pods Horizon 7: Monitoring health of Horizon Connection Server using Load Balancer [Horizon 7 Pods] [Global Settings for Client Sessions in Horizon Console] [VMware Horizon Architecture Planning]

QUESTION 4

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 5

An IT support center has been tasked with helping with Horizon desktop user issues.

What is the minimal level of Horizon Console access they would need to perform this action?

A. Help Desk Administrators

B. Local Administrators

C. Global Help Desk Administrators

D. Inventory Administrators

E. Administrators

Correct Answer: A

Explanation: The minimal level of Horizon Console access that the IT support center would need to help with Horizon desktop user issues is the Help Desk Administrators role. This role allows the IT support center to view and troubleshoot

user sessions, reset user passwords, send messages to users, and perform other help desk tasks. The Help Desk Administrators role can be assigned to users or groups on any access group that contains the desktop pools or farms that the

IT support center needs to support. The other options are not the minimal level of Horizon Console access for this scenario:

Local Administrators: This role allows full administration rights on a specific access group and its sub-access groups. This role can perform all the tasks of the Help Desk Administrators role, as well as create, edit, and delete desktop pools,

farms, applications, entitlements, and other objects. This role is more than what the IT support center needs to help with user issues.

Global Help Desk Administrators: This role allows full administration rights on all access groups in the Horizon environment. This role can perform all the tasks of the Local Administrators role, as well as create, edit, and delete access groups

and global entitlements. This role is more than what the IT support center needs to help with user issues.

Inventory Administrators: This role allows limited administration rights on a specific access group and its sub-access groups. This role can view and manage desktop pools, farms, applications, entitlements, and other objects, but cannot

create or delete them. This role can also perform some help desk tasks, such as viewing user sessions and sending messages to users, but cannot reset user passwords or troubleshoot sessions. This role is not sufficient for what the IT

support center needs to help with user issues.

Administrators: This role allows full administration rights on all access groups in the Horizon environment, as well as global settings, licensing, roles and permissions, events configuration, and other system-wide settings. This role can perform

all the tasks of theother roles, as well as configure and manage the Horizon infrastructure. This role is more than what the IT support center needs to help with user issues.

References: Understanding Permissions and Access Groups and [VMware Horizon 8.x Professional Course]

QUESTION 6

Users need to be able to log into VMware Workspace ONE Access and connect to remote desktops and applications without having to provide Active Directory credentials. Which VMware Horizon component needs to be deployed to allow this functionality?

A. Replica Server

B. Security Server

C. Enrollment Server

D. vCenter Server

Correct Answer: C

Explanation: The VMware Horizon component that needs to be deployed to allow users to log into VMware Workspace ONE Access and connect to remote desktops and applicationswithout having to provide Active Directory credentials is the Enrollment Server. The Enrollment Server is a standalone service that integrates with VMware Workspace ONE Access and enables True Single Sign-On (SSO) for Horizon clients that are using non-AD-based authentication methods such as RSA SecureID, RADIUS, or SAML1. The Enrollment Server requests short-lived certificates on behalf of the users from a certificate authority (CA), and these certificates are used for authentication to the Horizon environment2. The Enrollment Server must be installed and configured in the same domain or forest as the Connection Server, and it must have an enrollment agent certificate that authorizes it to act as an enrollment agent2. The other options are not valid or feasible because: A Replica Server is a Connection Server instance that replicates the Horizon LDAP configuration data from another Connection Server instance, and provides high availability and load balancing for user connections3. A Replica Server does not request or issue certificates for users, and it does not integrate with VMware Workspace ONE Access. A Security Server is a Connection Server instance that resides within a DMZ and acts as a proxy for external user connections to the Horizon environment4. A Security Server does not request or issue certificates for users, and it does not integrate with VMware Workspace ONE Access. Security Servers are deprecated in Horizon 8 and replaced by Unified Access Gateways (UAGs)4. A vCenter Server is a management platform that provides centralized control and visibility of vSphere hosts and virtual machines in the Horizon environment5. A vCenter Server does not request or issue certificates for users, and it does not integrate with VMware Workspace ONE Access. References: VMware Horizon 8.x Professional by Vmware1 Install and Set Up an Enrollment Server2 Install a Replica Connection Server Instance3 Install a Security Server4 vCenter Server Overview5

QUESTION 7

How do multiple Horizon Connection Server instances in a pod maintain synchronization?

A. Horizon Connection Server instances keep their data in an AD LDS database, which is automatically synchronized between the Connection Server.

B. Horizon Connection Server instances keep their data in an Oracle database, which works as the central hub.

C. Horizon Connection Server instances keep their data in a local MySQL DB. The data is synchronized once every 24h.

D. Horizon Connection Server instances keep their data in an MS SQL database, which works as the central hub.

Correct Answer: A

Explanation: Horizon Connection Server instances keep their data in an AD LDS database, which is automatically synchronized between the Connection Server. AD LDS is a Lightweight Directory Access Protocol (LDAP) directory service that provides flexible support for directory-enabled applications, without the dependencies that are required for Active Directory Domain Services (AD DS). AD LDS provides much of the same functionality as AD DS, but it does not require the deployment of domains or domain controllers. In a Horizon environment, each Connection Server instance has a copy of the AD LDS database and replicates changes to other Connection Server instances in the same pod. This ensures that the Connection Server instances have consistent and up-to- date information about the Horizon resources and user sessions12 References: Configuring Horizon Connection Server1 Understanding VMware Horizon Services2

QUESTION 8

An administrator is tasked with configuring VMware Integrated Printing. They enabled the VMware Integrated Printing feature during the installation of the Horizon Agent in the golden image, and created a Test Desktop Pool. On a physical end-point where the Horizon Client already is installed, the administrator added multiple network printers which are working perfectly. They test the configuration by connecting to the Horizon Desktop with the Horizon Client, unfortunately they do not see the printers within their Horizon Desktop.

What could be the reason that the administrator is not seeing the printers within his Horizon Desktop session?

A. Port TCP 9427 is disabled.

B. The VMware Integrated Printing feature is not installed in the Horizon Client.

C. Printing is disabled in the Horizon Desktop Pool.

D. Port TCP 32111 is disabled.

Correct Answer: C

Explanation: One of the possible reasons that the administrator is not seeing the printers within his Horizon Desktop session is that printing is disabled in the Horizon Desktop Pool. Printing is a feature that allows users to print from a remote

desktop to any local or network printer available on their client device. Printing can be enabled or disabled for each desktop pool by using the VMware Integrated Printing feature. VMware Integrated Printing is a feature that supports client

printer redirection, location- based printing, and persistent print settings. Client printer redirection enables users to print from a remote desktop to any local or network printer available on their client device. Location-based printing enables

users to print to network printers that are physically near their client device. Persistent print settings enable users to retain their print settings across sessions.

To enable or disable printing for a desktop pool, the administrator needs to follow these steps:

In Horizon Console, select Inventory > Desktops.

Select the desktop pool and click Edit.

In the Edit Desktop Pool dialog box, select the VMware Integrated Printing tab. Select or clear the Enable VMware Integrated Printing check box.

Click OK.

If printing is disabled for a desktop pool, users will not see any printers within their Horizon Desktop session, even if they

have installed the VMware Integrated Printing feature in the Horizon Agent and the Horizon Client. Therefore, to resolve

this issue, the administrator needs to enable printing for the desktop pool by selecting the Enable VMware Integrated Printing check box.

The other options are not likely to be the reason that the administrator is not seeing the printers within his Horizon Desktop session:

Port TCP 9427 is disabled: This port is used by the VMware Integrated Printing feature for communication between the Horizon Agent and the Horizon Client. If this port is disabled, users might experience printing errors or delays, but they

should still see the printers within their Horizon Desktop session. The VMware Integrated Printing feature is not installed in the Horizon Client: This feature is installed by default in the Horizon Client for Windows, Mac, Linux, Chrome, and

HTML Access. If this feature is not installed in the Horizon Client, users might not be able to print from their remote desktops, but they should still see the printers within their Horizon Desktop session. Port TCP 32111 is disabled: This port is

used by ThinPrint for communication between the Horizon Agent and the ThinPrint Client. ThinPrint is a legacy printing feature that has been replaced by VMware Integrated Printing. If this port is disabled, users might experience printing

errors or delays with ThinPrint, but they should still see the printers within their Horizon Desktop session if they use VMware Integrated Printing.

References: Configuring VMware Integrated Printing, Enable or Disable Printing for a Desktop Pool, and [VMware Horizon 8.x Professional Course]

QUESTION 9

Which vCenter privileges are required only for instant clones VMs with a Trusted Platform Module (vTPM) device?

A. Upgrade virtual machine compatibility

B. Manage KM5

C. Configure Host USB device

D. Manage custom attributes

Correct Answer: B

Explanation: A Trusted Platform Module (vTPM) is a virtualized version of a physical TPM device that provides enhanced security for virtual machines. A vTPM device can be added to a virtual machine to enable features such as encryption,

attestation, and key management. A vTPM device requires a Key Management Server (KMS) to store and manage the encryption keys.

To create instant clones VMs with a vTPM device, the vCenter Server user must have certain privileges in addition to those required for instant clones without a vTPM device. One of these privileges is Manage KMS, which allows the user to

perform cryptographic operations on the vTPM device, such as cloning, decrypting, encrypting, migrating, and registering. The Manage KMS privilege is part of the Cryptographic operations privilege group on vCenter Server.

The other options are not required only for instant clones VMs with a vTPM device:

Upgrade virtual machine compatibility: This privilege allows the user to upgrade the virtual hardware version of a virtual machine to support new features and capabilities. This privilege is required for instant clones VMs regardless of whether

they have a vTPM device or not.

Configure Host USB device: This privilege allows the user to configure USB devices on an ESXi host and attach them to a virtual machine. This privilege is not related to vTPM devices or instant clones VMs.

Manage custom attributes: This privilege allows the user to create, edit, and delete custom attributes for vCenter Server objects. Custom attributes are user-defined fields that can store additional information about objects. This privilege is not

related to vTPM devices or instant clones VMs.

References: Privileges Required for the vCenter Server User With Instant Clones, vSphere Virtual Machine Administration, and [VMware Horizon 8.x Professional Course]

QUESTION 10

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]