



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.geekcert.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

An administrator wants to ensure that user's desktop experience is consistent regardless of the desktop they connect to. What solution should be used to meet the requirement?

- A. Persona Management
- B. Temporary Profiles
- C. Dynamic Environment Manager
- D. Local Profiles

Correct Answer: C

VMware Horizon's Dynamic Environment Manager (DEM) is designed to provide a consistent and personalized desktop experience for users across different sessions and desktops. DEM manages user profiles and policies dynamically, ensuring that user settings, preferences, and application configurations are consistent no matter which desktop a user connects to, thus meeting the requirement for a uniform desktop experience.

QUESTION 2

A user is complaining that each time they logon they need to change the settings for the e-mail client.

Which three options can an administrator deploy to make sure the user's settings are being saved? (Choose three.)

- A. VMware App Volumes Writable Volumes
- B. Roaming Profiles
- C. Persona Management
- D. VMware Dynamic Environment Manager
- E. Flexible profiles

Correct Answer: ACD

The user's problem is that their settings for the e-mail client are not being saved across sessions. This means that their user profile, which contains their personal data, settings, and preferences, is not being preserved or synchronized properly. To solve this problem, the administrator can deploy one or more of the following options to manage user profiles in Horizon:

- VMware App Volumes Writable Volumes:** This option allows users to store user-installed applications, data, and settings on a disk independent of the VM. Writable volumes can be attached to desktops along with application packages, and they can isolate the user-installed applications from the system-installed applications. Writable volumes can also be configured to capture specific files and registry keys by using the snapvol.cfg policy file. This option can help users retain their e-mail client settings on a writable volume that is attached to their desktop at each login.
- Persona Management:** This option allows administrators to manage user profiles by using a remote repository that stores user profiles. Persona Management synchronizes the user profile between the remote repository and the local desktop at login, logout, and at regular intervals during the session. Persona Management also supports profile redirection, which allows administrators to redirect certain folders in the user profile to a network share or a writable volume. This option can help users access their e-mail client settings from the remote repository or the redirected folder at each login.
- VMware Dynamic Environment Manager:** This option allows administrators to manage user profiles and policies by using a central share that stores user configuration files. Dynamic Environment Manager



captures and applies user settings and preferences based on conditions and triggers, such as location, device, or application launch. Dynamic Environment Manager also supports profile archives, which allow administrators to back up and restore user profiles on demand or on schedule. This option can help users apply their e-mail client settings from the central share or the profile archive at each login. The other options are not valid options for managing user profiles in Horizon: Roaming Profiles: This option is a native Windows feature that allows users to access their user profile from any computer in a domain by storing it on a network share. However, this option is not recommended for Horizon because it can cause long login times, profile corruption, and data loss due to its synchronous and overwrite behavior. Roaming profiles are also incompatible with instant clones and linked clones. Flexible profiles: This option does not exist in Horizon or Windows. It might be confused with Flex Profiles, which is a third-party product from Liquidware that provides profile management solutions similar to Dynamic Environment Manager.

References: Writable Volumes Overview, Configuring User Profiles with Horizon Persona Management, VMware Dynamic Environment Manager Overview, 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

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>

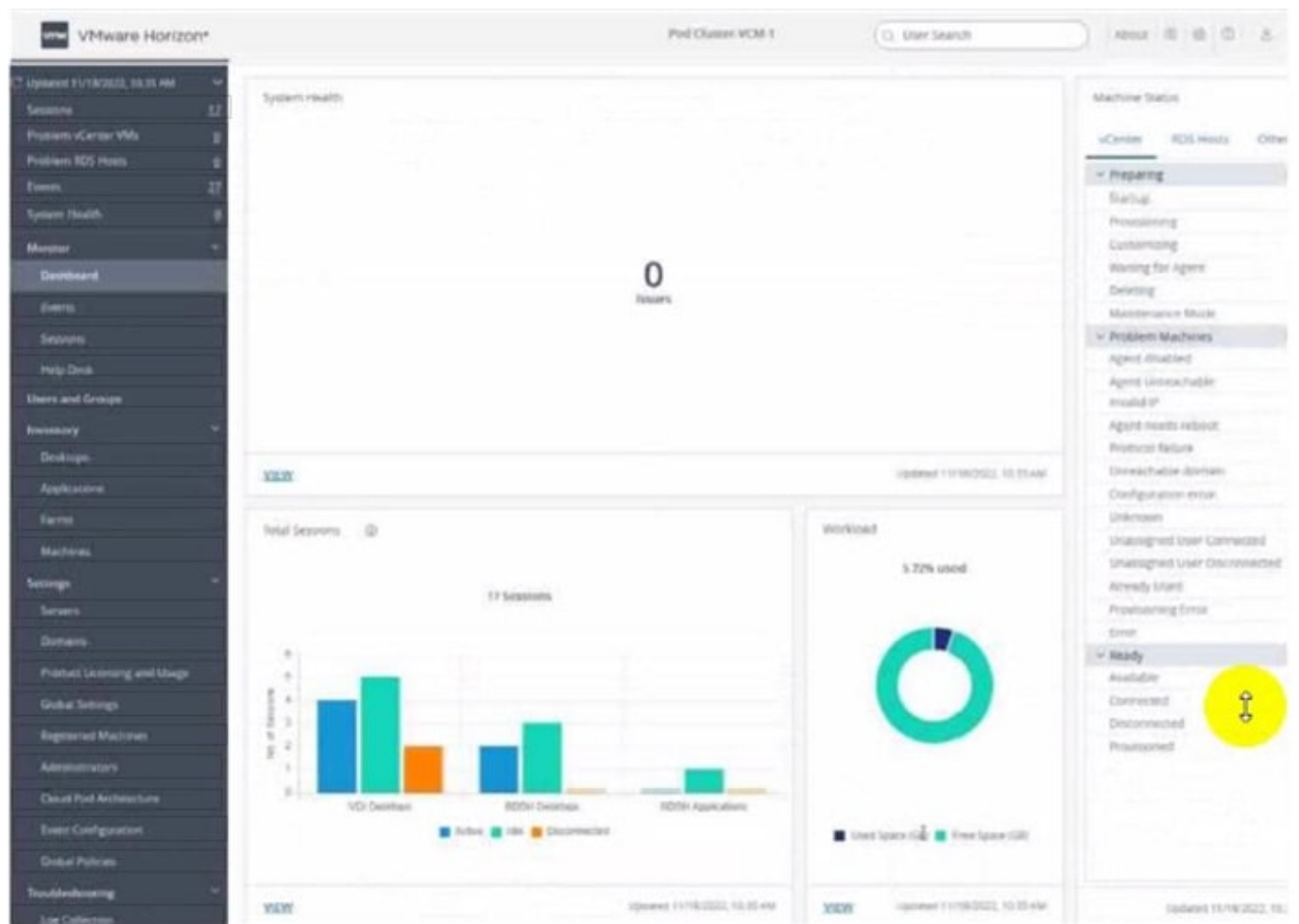
QUESTION 4

HOTSPOT

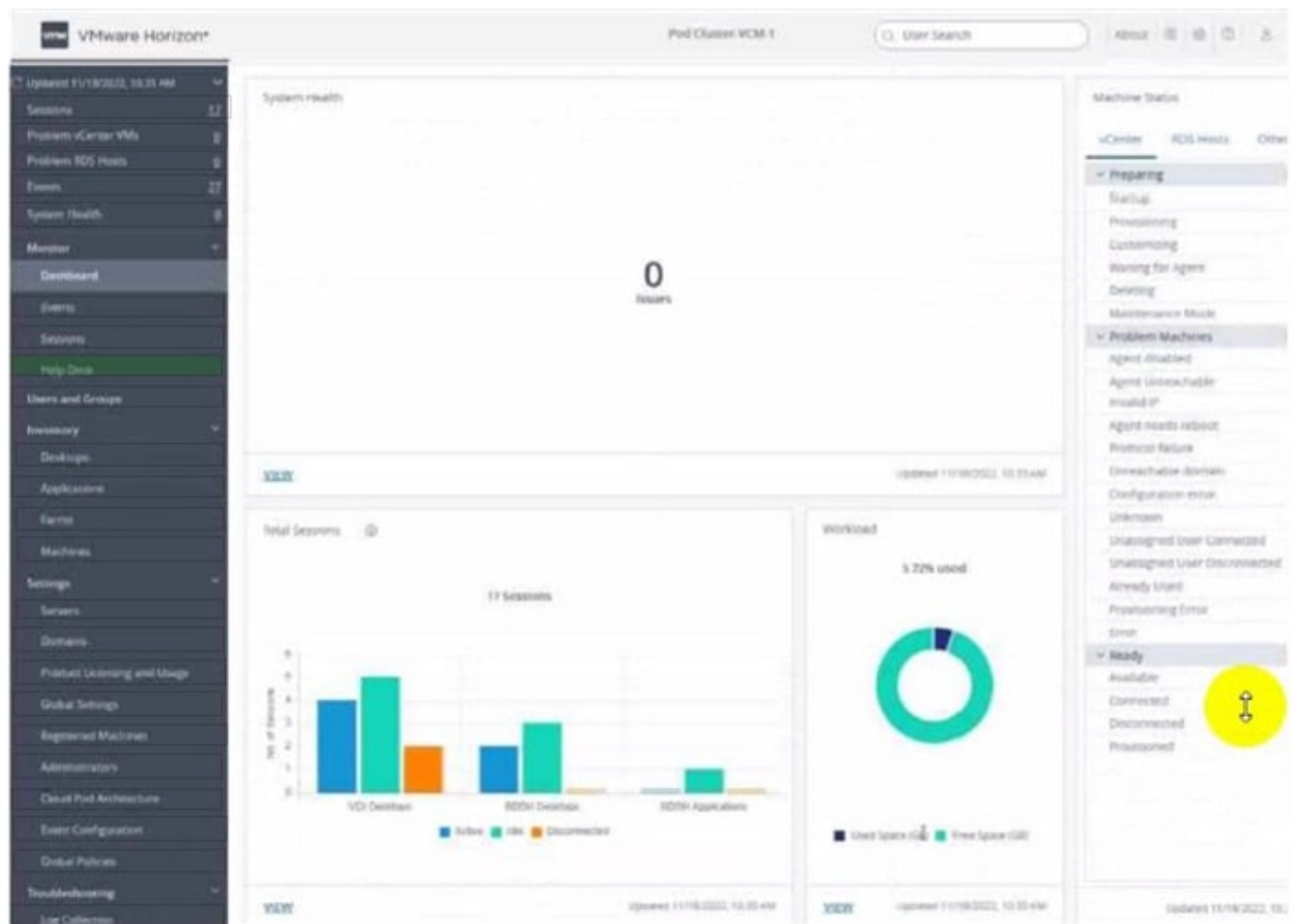
An administrator needs to monitor the advanced metrics of desktop sessions in Horizon Console.

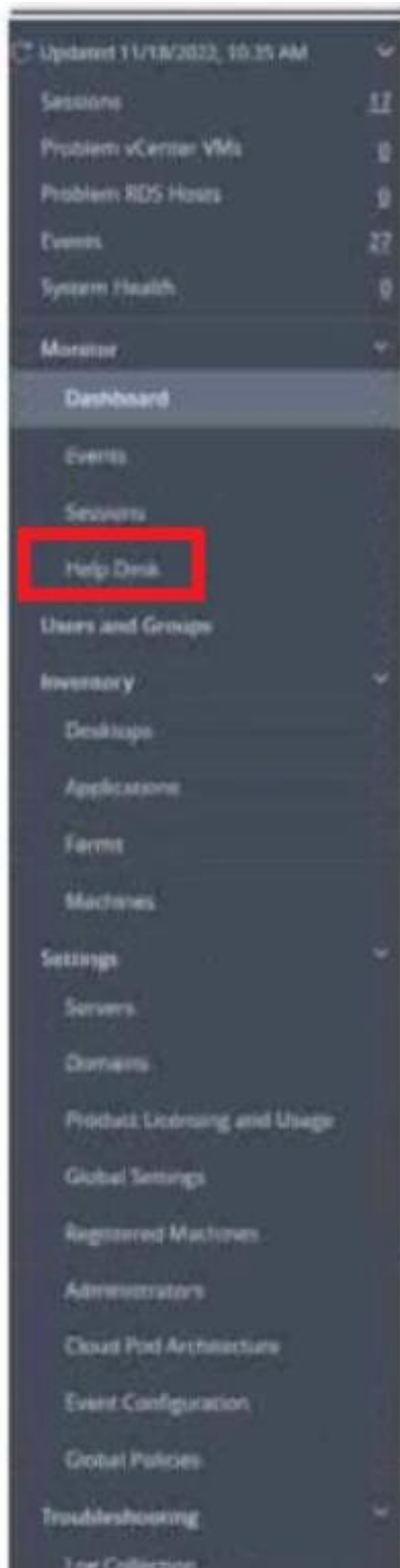
Mark where the administrator would navigate in the Horizon Console by clicking on it.

Hot Area:



Correct Answer:





To monitor the advanced metrics of desktop sessions in Horizon Console, you need to use the Horizon Help Desk Tool. This is a web application that you can use to get the status of Horizon 8 user sessions and to perform troubleshooting and maintenance operations¹. You can also view performance details for a virtual or published desktop session that



uses the PCoIP or VMware Blast display protocol2.

To access the Horizon Help Desk Tool, you need to click on the Monitoring tab on the left side of the Horizon Console. Then, you need to select Help Desk from the drop-down menu. This will open the Horizon Help Desk Tool in a new

browser tab. You can then search for a user, machine, or pool and view the session details. You can also click on More to see the advanced metrics such as latency, bandwidth, protocol, and frame rate1.

QUESTION 5

DRAG DROP

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

Select and Place:

| TLS Certificate Configuration Step | Correct Sequence |
|--|------------------|
| Modify the certificates/ friendly names to vdm and reflect the current active certificate. | Step 1 |
| Import the TLS certificate into the Windows local computer certificate store. | Step 2 |
| Restart Horizon Service. | Step 3 |
| Get a new signed TLS certificate from a CA. | Step 4 |

Correct Answer:

| TLS Certificate Configuration Step | Correct Sequence |
|--|------------------|
| Get a new signed TLS certificate from a CA. | Step 1 |
| Import the TLS certificate into the Windows local computer certificate store. | Step 2 |
| Modify the certificates/ friendly names to vdm and reflect the current active certificate. | Step 3 |
| Restart Horizon Service. | Step 4 |

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 be Step 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 be Step 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 becomes Step 3.

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

[Latest 2V0-51.23 Dumps](#)

[2V0-51.23 PDF Dumps](#)

[2V0-51.23 VCE Dumps](#)