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.pass4itsure.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

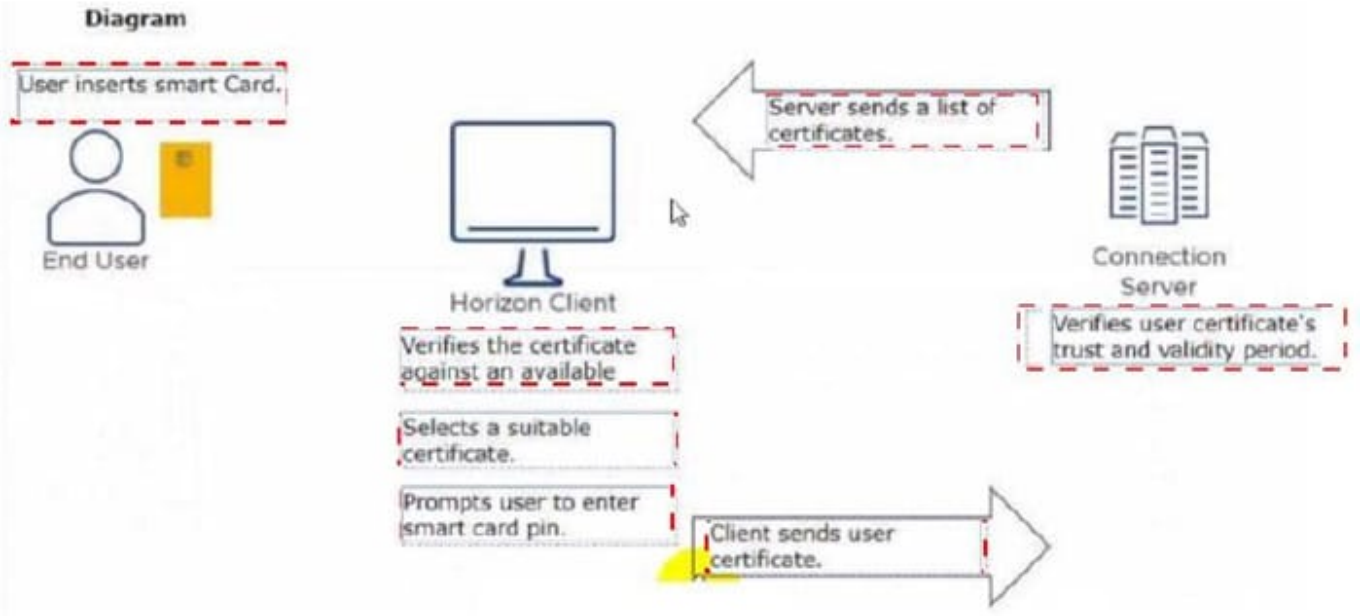
QUESTION 1

Refer to the exhibit.

Drag and drop the labels on the left for the authentication flow for smart cards into the correct location in the diagram on the right.

Select and Place:

Correct Answer:



QUESTION 2

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 3

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 4

What is the effect of changing any VMware Blast policy that cannot be changed in real time?

A. Horizon Client detects the change and prompts the user to reboot once every 480 seconds.

B. VMware Tools services is restarted by Microsoft GPO Update service.

C. VMware Tools detects the change and immediately applies the new setting within 480 seconds.

D. Microsoft GPO update rules apply and GPOs are updated manually or by restarting the Horizon Agent.

Correct Answer: D

Explanation: VMware Blast policy settings are stored in the registry key HKLM\Software\Policies\VMware, Inc.\VMware Blast\Config on the remote desktops or RDS hosts that use the VMware Blast display protocol. These settings can be configured by using the VMware Blast ADMX template file (vdm_blast.admx) and applying it through Microsoft Group Policy Object (GPO). Some of these settings can be changed in real time, which means that they take effect immediately after the policy is applied, without requiring a reboot or a reconnection of the Horizon Client. However, some of these settings cannot be changed in real time, which means that they require a reboot or a reconnection of the Horizon Client to take effect. The effect of changing any VMware Blast policy that cannot be changed in real time is that the Microsoft GPO update rules apply and GPOs are updated manually or by restarting the Horizon Agent. This means that the new policy settings will not be applied until one of the following events occurs: The Horizon Agent service is restarted on the remote desktop or RDS host. This can be done manually by using the Services console or the command-line tool sc.exe, or automatically by using a scheduled task or a script. The remote desktop or RDS host is rebooted. This can be done manually by using the Restart option in Windows, or automatically by using a scheduled task or a script. The Group Policy refresh interval is reached. This is a configurable time interval that determines how often the system checks for and applies new or changed GPOs. By default, this interval is 90 minutes for domain members and 5 minutes for domain controllers, with a random offset of 0 to 30 minutes. This interval can be modified by using the Group Policy refresh interval for computers setting in the ComputerConfiguration\Administrative Templates\System\Group Policy folder of the Group Policy Management Console. Therefore, to ensure that the VMware Blast policy settings that cannot be changed in real time are applied as soon as possible, it is recommended to restart the Horizon Agent service or reboot the remote desktop or RDS host after applying the policy. References: VMware Blast Policy Settings, Group Policy refresh intervals, and [VMware Horizon 8.x Professional Course]

QUESTION 5

Which three VMware Horizon based resources does Unified Access Gateway (UAG) provide access to? (Choose three.)

A. virtual desktops

B. RDSH-based applications

C. physical Windows machines

D. IOT devices

E. thin clients

Correct Answer: ABC

Explanation: Unified Access Gateway (UAG) is a secure gateway appliance that provides access to VMware Horizon based resources such as virtual desktops, RDSH-based applications, and physical Windows machines. UAG supports multiple authentication methods and protocols, such as SAML, OAuth, and RADIUS, to provide secure access to end users from any device and location. UAG also provides edge services such as load balancing, high availability, and firewall rules to optimize the performance and availability of Horizon based resources12. References := 1: VMware Horizon Architecture Planning: Unified Access Gateway 2: VMware Unified Access Gateway Administration Guide: Introduction to Unified Access Gateway