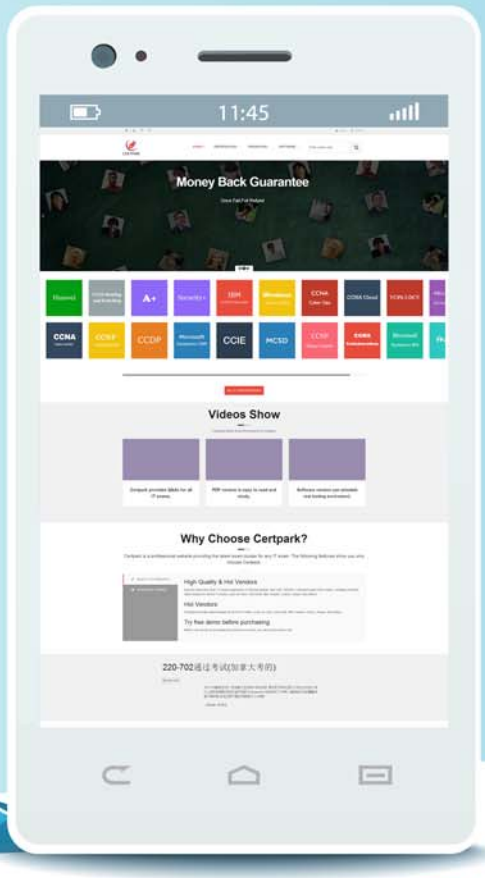
CERTPARK

QUESTION & ANSWER

CERTPARK.COM

Accurate Study Guides,
High Passing Rate!
provides update
free of charge
in one year!



https://www.certpark.com

Exam : **2V0-51.23**

Title : VMware Horizon 8.x Professional

Version : DEMO

1.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.
Answer: A D
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 established between 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]

2.Drag and drop each Desktop Persistence type on the left to its matching description on the right.

Desktop Persistence type		Description
Floating assignment		Each user is assigned a particular remote desktop and returns to the same desktop at each login.
Dedicated assignment		With every login, users get a random desktop. When a user logs out, the desktop is returned to the pool.
Automatic assignment		Horizon finds an available, unassigned desktop and creates an assignment when a user connects to a pool for the first time. Thereafter, this user always gets the same desktop after logging in, and this desktop is not available to any other user.
Multi-User assignment		Manually assign multiple users to each machine in the dedicated-assignment desktop pool. If an assigned user has a connected or disconnected session on a multi-user assignment machine, other assigned users cannot launch a session on that machine.

Answer:

Desktop Persistence type		Description
Floating assignment	Dedicated assignment	Each user is assigned a particular remote desktop and returns to the same desktop at each login.
Dedicated assignment	Floating assignment	With every login, users get a random desktop. When a user logs out, the desktop is returned to the pool.
Automatic assignment	Multi-User assignment	Horizon finds an available, unassigned desktop and creates an assignment when a user connects to a pool for the first time. Thereafter, this user always gets the same desktop after logging in, and this desktop is not available to any other user.
Multi-User assignment	Automatic assignment	Manually assign multiple users to each machine in the dedicated-assignment desktop pool. If an assigned user has a connected or disconnected session on a multi-user assignment machine, other assigned users cannot launch a session on that machine.

3.What are two best practices for Windows Golden Image Optimization? (Choose two.)

A. Activate Windows OS paging.

B. Turn on automatic Windows maintenance (scheduled tasks).

C. Turn on automatic Windows Updates.

D. Disable unnecessary services.

E. Disable power options.

Answer: D E

Explanation

Windows golden image optimization is the process of reducing the size and improving the performance of the Windows OS image that is used as the base for the desktop pools.

Some of the best practices for Windows golden image optimization are:

- Disable unnecessary services: Services that are not required for the desktop functionality or user experience should be disabled to reduce the resource consumption and potential security risks.

For example, services such as Windows Search, Windows Defender, Windows Update, and Superfetch can be disabled for better performance and stability.

- Disable power options: Power options such as hibernation and sleep mode should be disabled to free up disk space and avoid potential issues with the desktop state. Hibernation can consume a large amount of disk space by creating a hiberfil.sys file that stores the system memory contents when the desktop is powered off. Sleep mode can cause problems with network connectivity and user sessions when the desktop is resumed from a low-power state.

Other best practices for Windows golden image optimization include:

- Activate Windows OS paging: Paging is a mechanism that allows the OS to use a portion of the disk as virtual memory when the physical memory is insufficient. Paging can improve the performance and stability of the desktops by preventing out-of-memory errors and reducing memory contention. However, paging can also increase disk I/O and wear, so it should be configured with caution and monitored regularly.
- Turn off automatic Windows maintenance (scheduled tasks): Automatic Windows maintenance is a feature that runs various tasks such as disk defragmentation, disk cleanup, security scanning, and system diagnostics in the background. These tasks can consume a lot of CPU, memory, and disk resources and interfere with the user experience and desktop performance. Therefore, it is recommended to turn off automatic Windows maintenance and run these tasks manually or on a scheduled basis when the desktops are not in use.
- Turn off automatic Windows Updates: Automatic Windows Updates is a feature that downloads and installs updates for the OS and other Microsoft products in the background. These updates can consume bandwidth, disk space, and CPUresources and cause compatibility issues with some applications or drivers. Therefore, it is recommended to turn off automatic Windows Updates and manage the updates manually or through a centralized tool such as VMware Update Manager or Microsoft WSUS.

References: [Optimizing Your VMware Horizon View 7.x Golden Image] and [VMware Horizon 8.x Professional Course]

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.

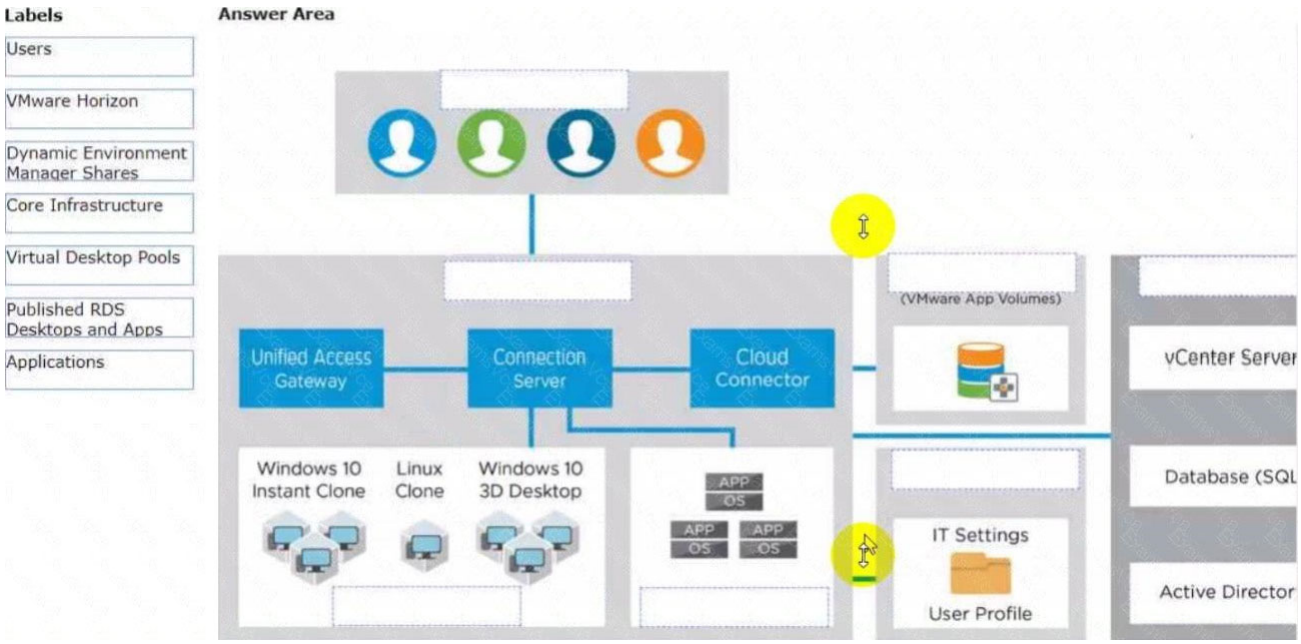
Answer: D

Explanation

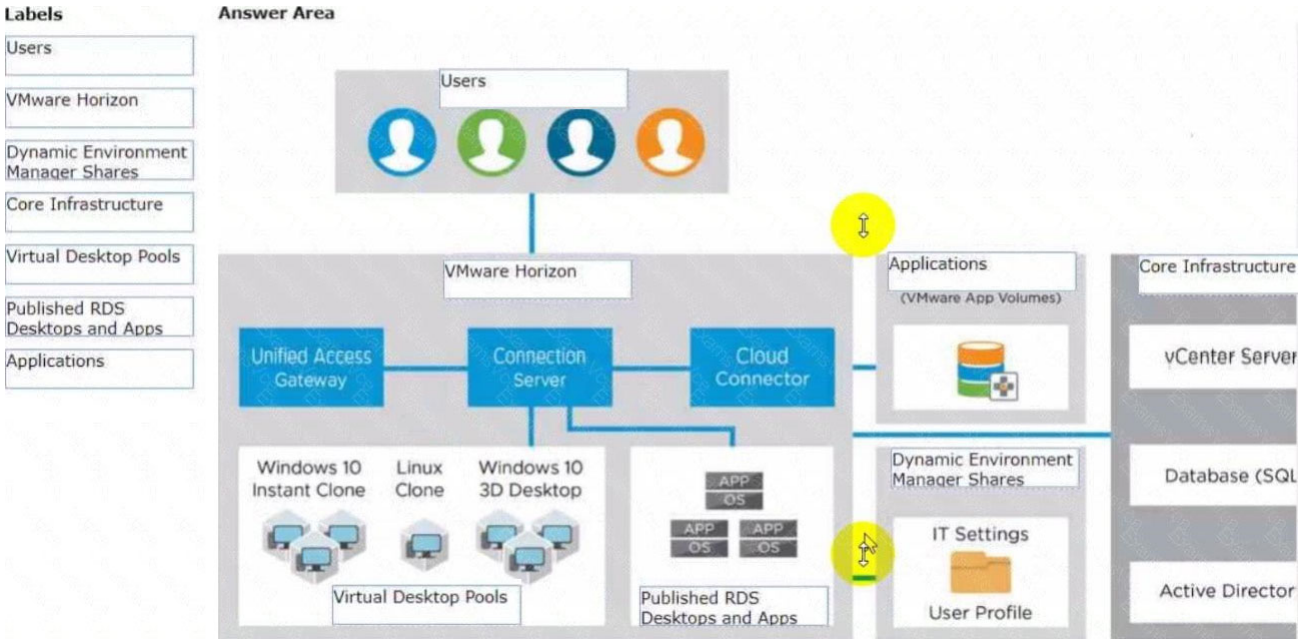
VMware Blast policy settings are stored in the registry key HKLM\Software\Policies\VMware, Inc.\VMware Blast\Config on the remote desktops or RDS hosts that use the VMware Blast display

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]

5.Refer to the exhibit.
Drag and drop the labels on the left into their correct location in the diagram of VMware Horizon Architecture on the right.



Answer:


Labels
Users
VMware Horizon
Dynamic Environment Manager Shares
Core Infrastructure
Virtual Desktop Pools
Published RDS Desktops and Apps
Applications
Answer Area
Users
VMware Horizon
Unified Access Gateway
Connection Server
Cloud Connector
Windows 10 Instant Clone
Linux Clone
Windows 10 3D Desktop
Virtual Desktop Pools
APP
OS
Published RDS Desktops and Apps
Applications
(VMware App Volumes)
Dynamic Environment Manager Shares
IT Settings
User Profile
Core Infrastructure
vCenter Server
Database (SQL
Active Director