

VMware.2V0-51.23.by.Kent.39q

Number: 2V0-51.23  
Passing Score: 800  
Time Limit: 120  
File Version: 4.0

**Exam Code: 2V0-51.23**

**Exam Name: VMware Horizon 8.X Professional**



## Exam A

### QUESTION 1

An administrator has added a supported PCI graphics accelerator to a virtual machine configuration. When the administrator tries to power on the virtual machine, an error is displayed and the virtual machine remains powered off.

Which of the following virtual machine configuration settings needs to be applied to enable the virtual machine to power on?

- A. Enable Video Card 3D Graphics.
- B. Reserve all guest memory.
- C. Set Memory Shares to High.
- D. Disable CPU Hot Plug.

**Correct Answer: B**

**Section:**

**Explanation:**

To enable a virtual machine to power on with a PCI graphics accelerator, such as a GPU, attached to it, the administrator needs to reserve all guest memory for that virtual machine. This is because PCI devices require direct memory access (DMA) to function properly, and memory overcommitment can interfere with DMA operations. Reserving all guest memory ensures that no memory swapping or ballooning occurs on the virtual machine, and that the memory address space is contiguous and available for DMA56.

The other options are not required or valid because:

Enabling Video Card 3D Graphics is not necessary for using a PCI graphics accelerator. This option is for using software-accelerated graphics or virtual shared graphics acceleration (vSGA) on a virtual machine7.

Setting Memory Shares to High does not guarantee that all guest memory will be reserved. Memory shares only affect how memory resources are distributed among competing virtual machines when there is memory contention on the host. Memory shares do not prevent memory overcommitment or swapping.

Disabling CPU Hot Plug does not affect the use of a PCI graphics accelerator. CPU Hot Plug allows adding or removing virtual CPUs from a powered-on virtual machine. It has no relation to PCI devices or DMA operations.

### QUESTION 2

DRAG DROP

Refer to the exhibit.

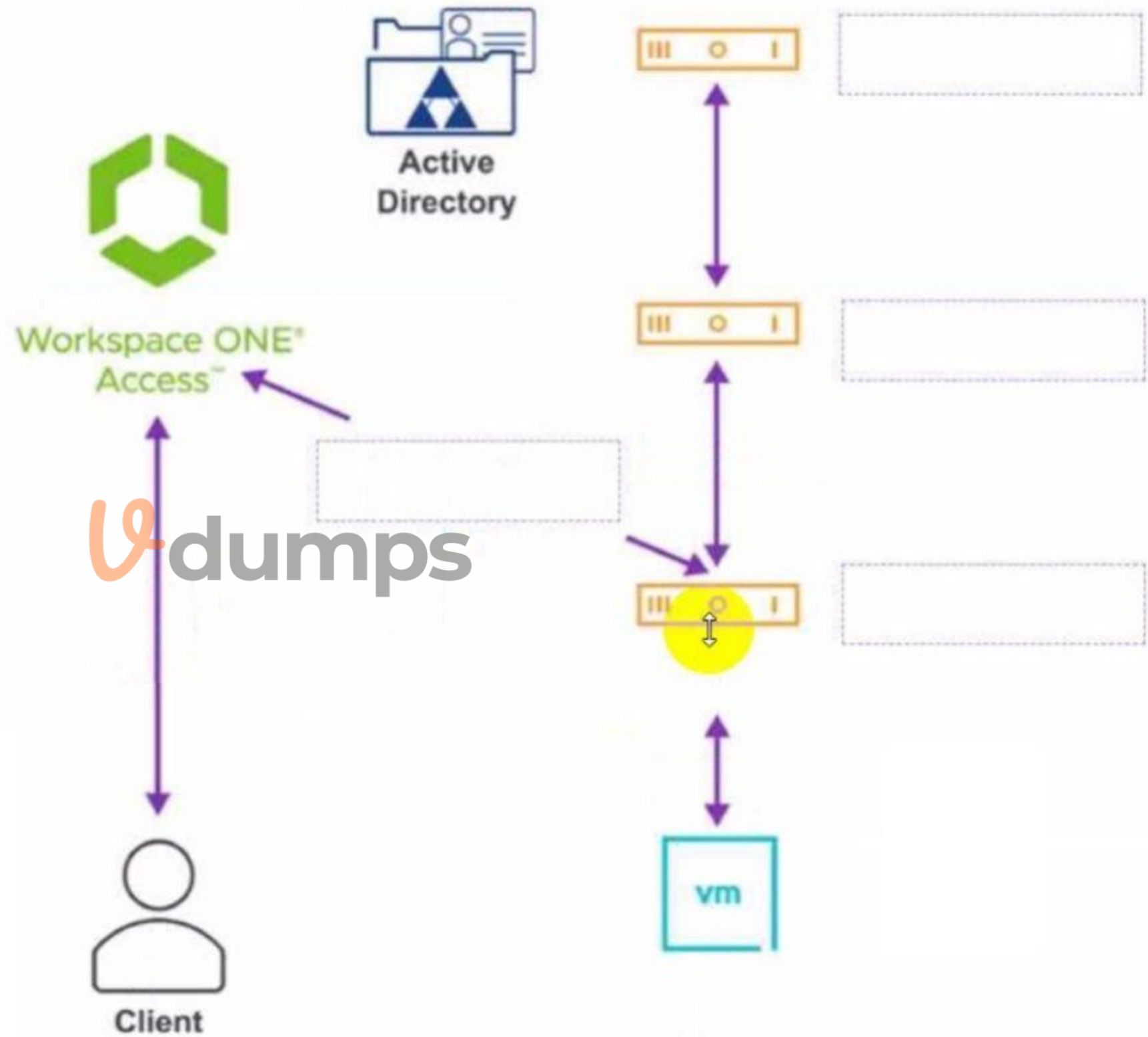
Drag and drop the correct options to build a Simple True 5SO Architecture on the left into the diagram on the right.

**Select and Place:**

Options

- SAML
- Certificate Authority
- Connection Server
- Enrollment Server

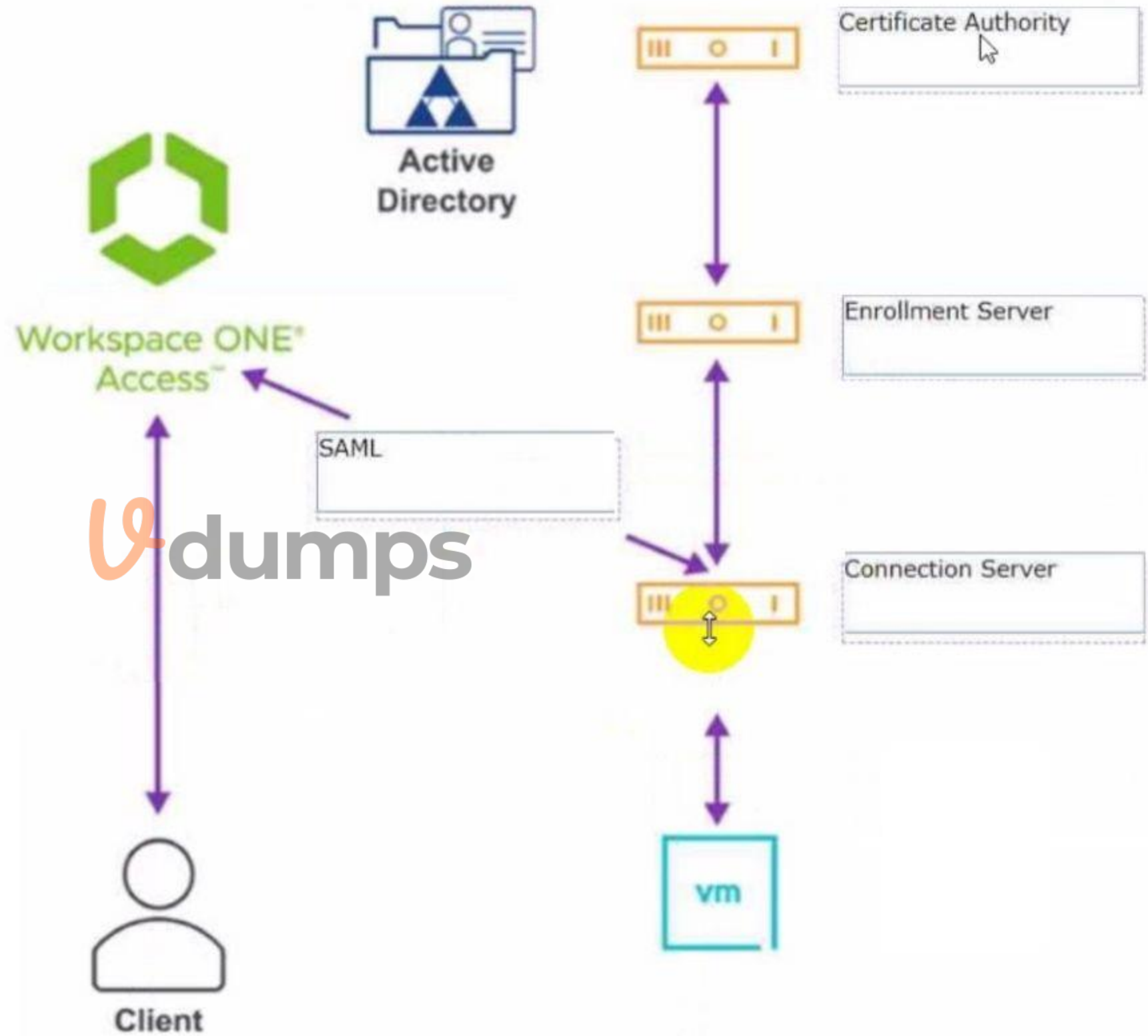
Diagram



Correct Answer:

Options


Diagram



Section:

Explanation:

VMware Horizon 8.x Professional  
Simple True SSO Architecture

### QUESTION 3

A Horizon administrator has been utilizing Application Profiler from Dynamic Environment Manager to create application-specific user defined settings. These files have grown to 2.3GB in size for a particular user and have negatively impacted the user experience.

What can be done to the configuration to improve the user experience?

- A. Configure exclusions to filter out unnecessary folders.
- B. Change the default save path.
- C. Configure exclusions to filter out unnecessary registry entries.
- D. Use Deepest Registry Path.

**Correct Answer: A**

**Section:**

**Explanation:**

To improve the user experience when using Application Profiler from Dynamic Environment Manager to create application-specific user defined settings, the administrator can configure exclusions to filter out unnecessary folders and registry entries. Exclusions are rules that specify which file system or registry locations are not included in the Flex configuration file. Exclusions can reduce the size of the Flex configuration file and the profile archive, and improve the performance of the application profiling and synchronization processes<sup>12</sup>.

The other options are not valid or effective because:

Changing the default save path does not affect the size or content of the Flex configuration file or the profile archive. It only changes where the files are stored on the local machine<sup>3</sup>.

Using Deepest Registry Path does not reduce the size of the Flex configuration file or the profile archive. It only changes how the registry locations are displayed in the Application Profiler interface<sup>4</sup>.

There is no such thing as Cloud Entitlements in Dynamic Environment Manager. The correct term is Global Entitlements, which are used in Cloud Pod Architecture to entitle users to desktops or applications across multiple pods<sup>5</sup>.

### QUESTION 4

HOTSPOT

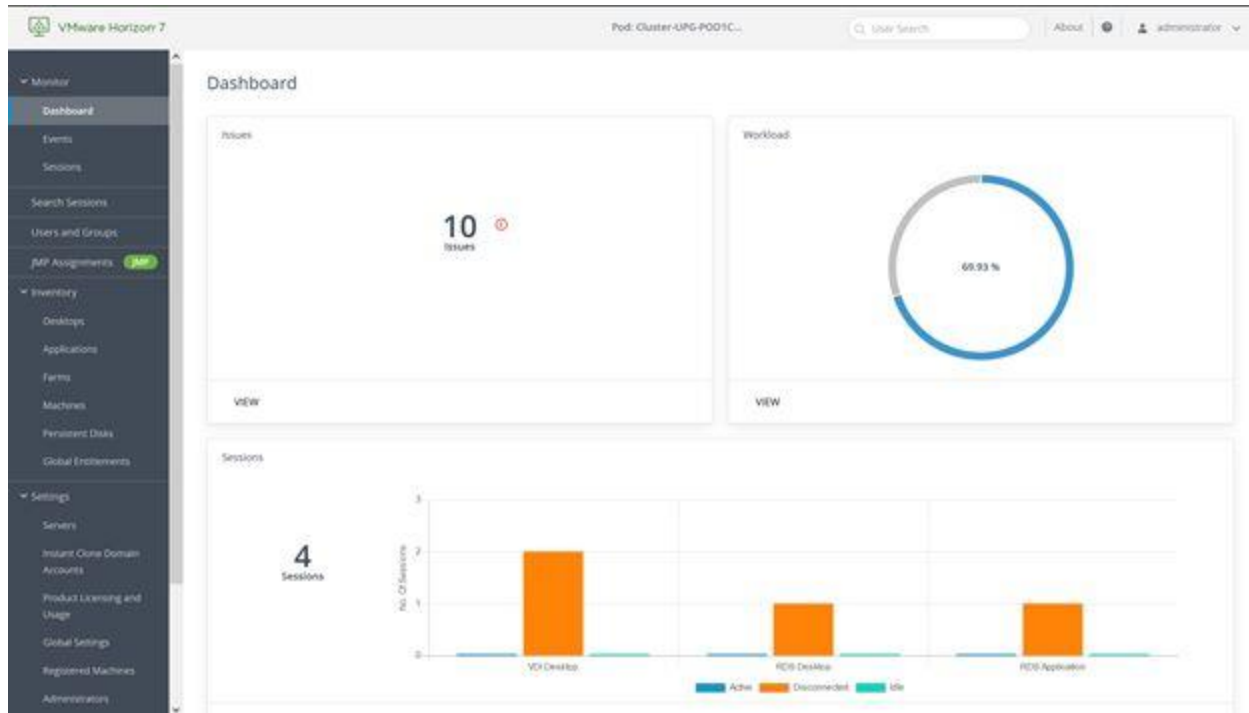
Refer to the exhibit.

An administrator prepared a golden image based on a Windows Server Operating System. They plan to use this image to create a single-session virtual desktop pool. The installation is completed, the virtual machine is turned off, and the snapshot has been created. When the administrator creates the desktop pool, they are unable to select the created image and snapshot. They do see other previously created golden images, based on Desktop Operating Systems.

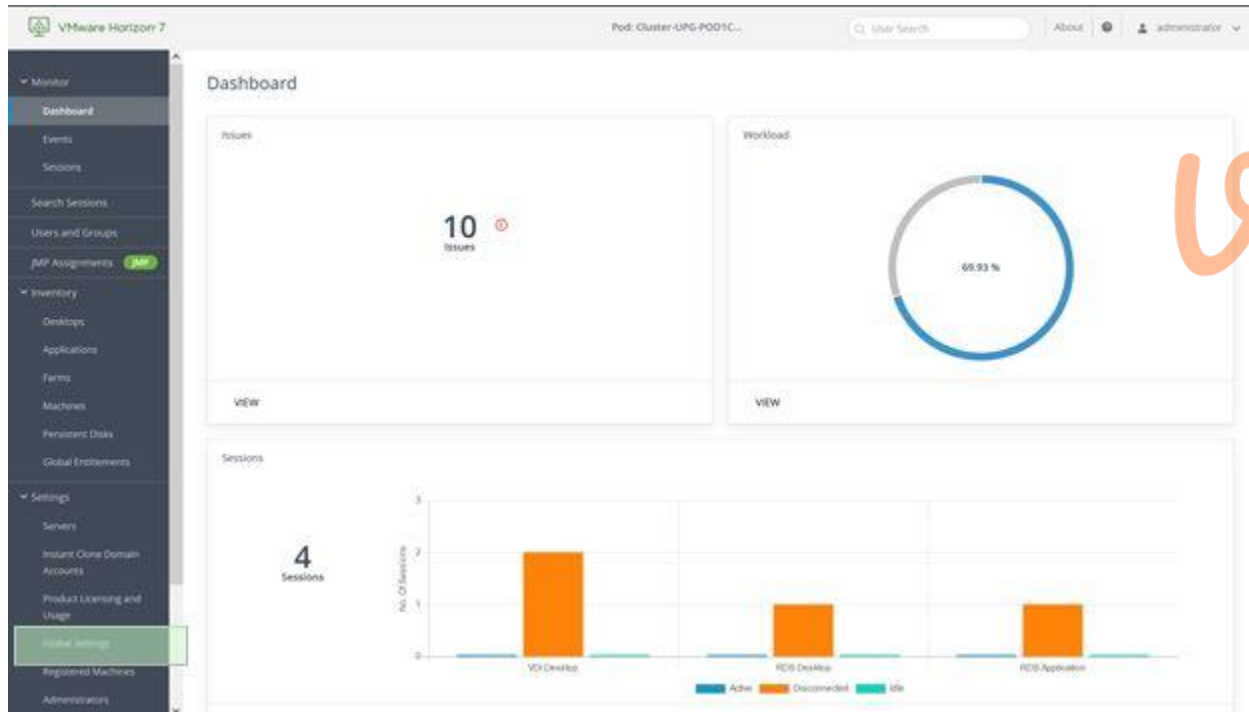
The administrator has opened the Horizon Console.

Mark the correct menu option where the administrator can enable Windows Server Operating Systems to be used as single-session desktops by clicking on it.

**Hot Area:**



**Answer Area:**



**Udumps**

**Section:**

**Explanation:**

**QUESTION 5**

DRAG DROP

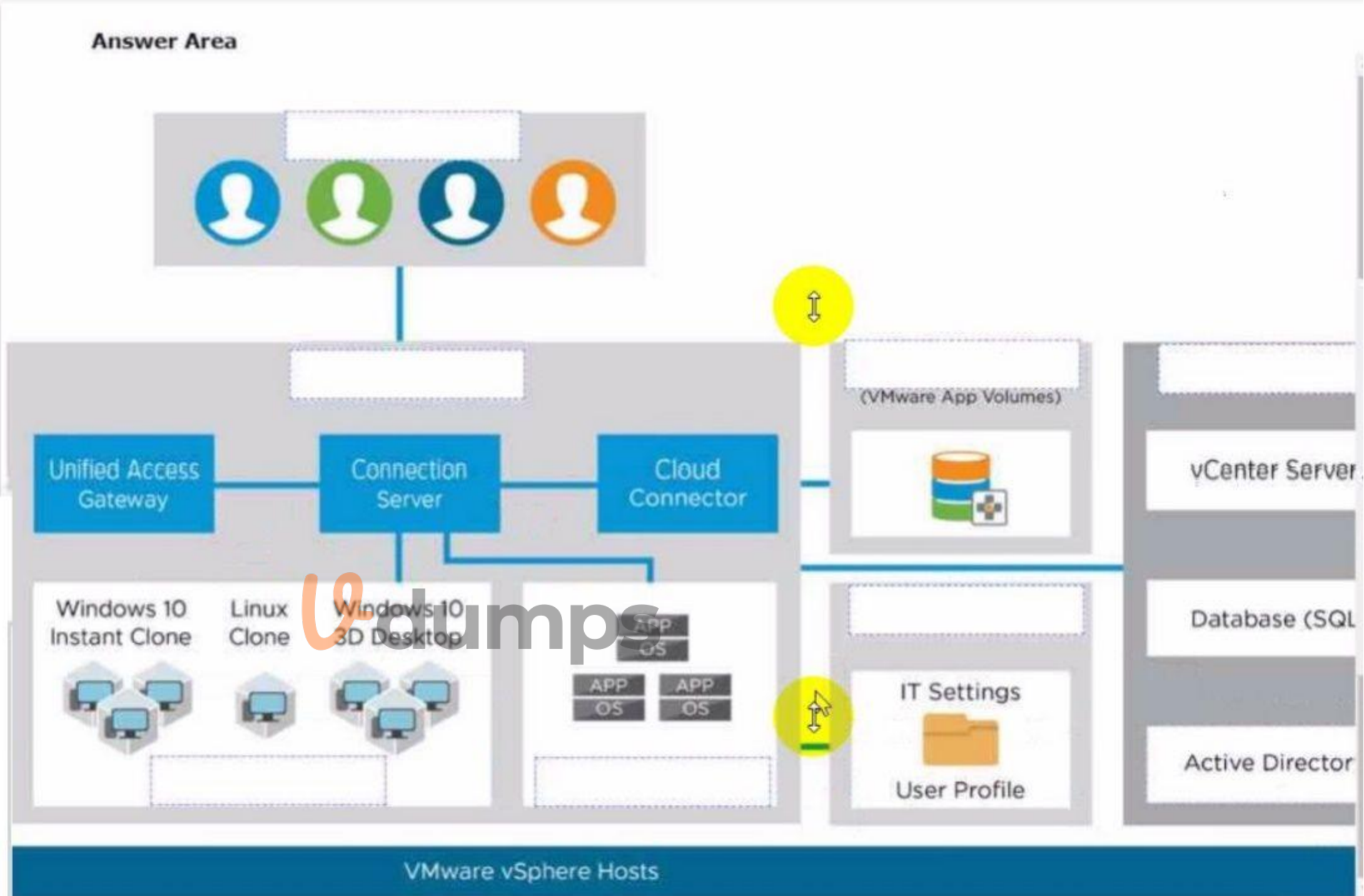
Refer to the exhibit.

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

**Select and Place:**

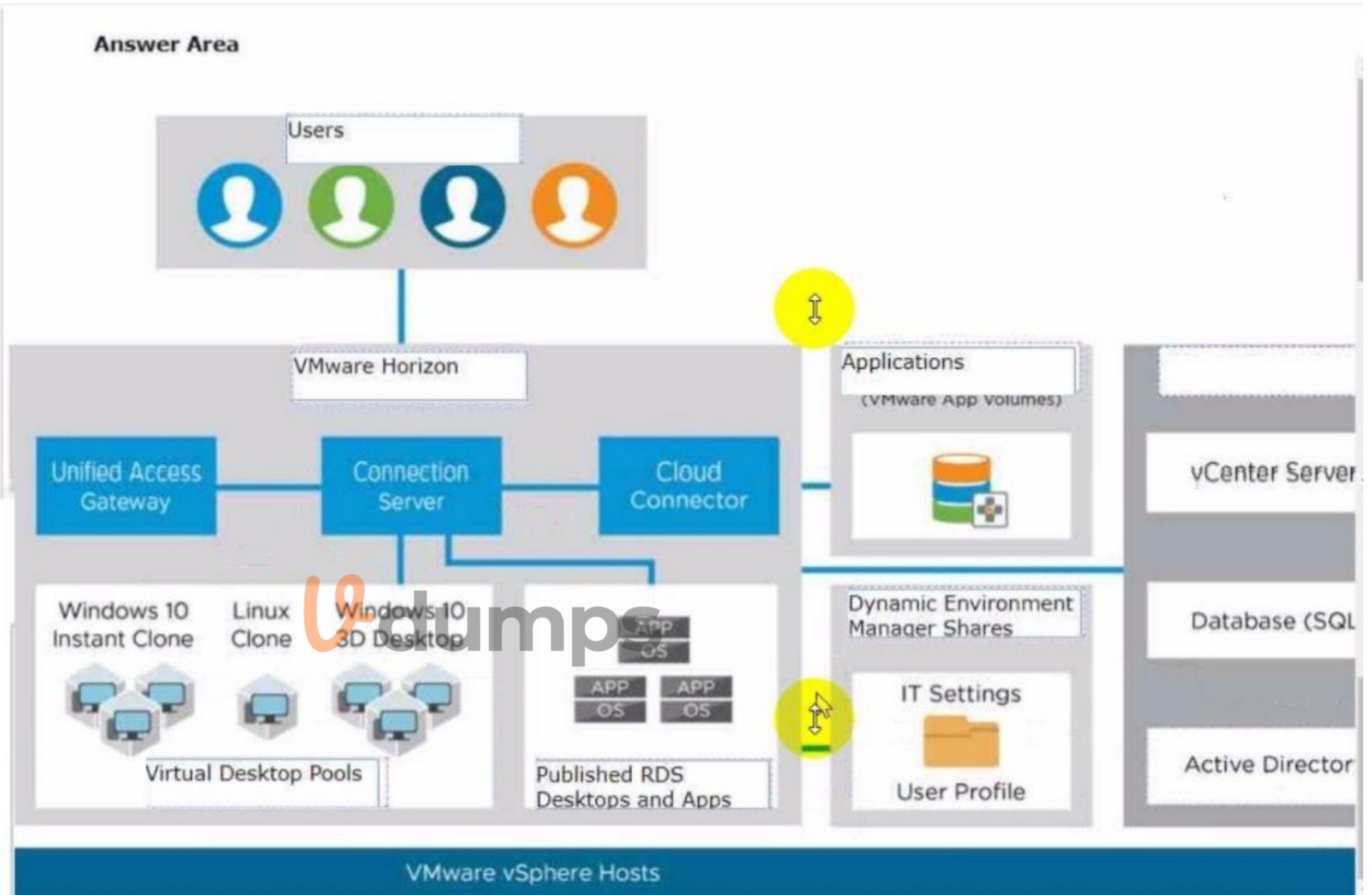
**Labels**

- Users
- VMware Horizon
- Dynamic Environment Manager Shares
- Core Infrastructure
- Virtual Desktop Pools
- Published RDS Desktops and Apps
- Applications



Correct Answer:

## Labels

**Section:**

**Explanation:**

### QUESTION 6

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.



**Correct Answer: D, E**

**Section:**

**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 CPU resources 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. Reference: [Optimizing Your VMware Horizon View 7.x Golden Image] and [VMware Horizon 8.x Professional Course]

#### QUESTION 7

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**

**Section:**

**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. Reference: 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 8

A junior-level Horizon administrator is not able to see all RDS farms.

Where would a high-level administrator need to make changes to correct the issue?

- A. Category Folder
- B. Access Groups
- C. Global Entitlements
- D. Global Policies

**Correct Answer: B**

**Section:**

**Explanation:**

Access groups are a way of organizing and delegating the administration of machines, desktop pools, application pools, and farms in Horizon. By default, all these objects reside in the root access group, which appears as / or Root (/) in Horizon Console. A high-level administrator can create sub-access groups under the root access group and assign different permissions to different administrators for each access group. For example, a high-level administrator can create an access group called RDS Farms and assign the Inventory Administrators role to a junior-level administrator for that access group. This way, the junior-level administrator can see and manage all the RDS farms that are in the RDS Farms access group, but not the ones that are in other access groups or the root access group. Therefore, to correct the issue of a junior-level administrator not being able to see all RDS farms, a high-level administrator needs to make changes to the access groups and the permissions associated with them. Reference: Understanding Permissions and Access Groups and [VMware Horizon 8.x Professional Course]

#### QUESTION 9

A VMware Horizon administrator is tasked with deployment of a desktop pool, which should fulfill these requirements:

- . End-users should always get the same desktop VM.
- . Backups with the existing VMware image-based backup tool should be supported.
- . Desktop VMs will be cloned on a weekly basis per vSphere API.

Which desktop solution can accomplish this requirement?

- A. Automated Desktop Pool, based on Dedicated Full Clone Virtual Machines.
- B. Automated Desktop Pool, based on Floating Full Clone Virtual Machines.
- C. Automated Desktop Pool, based on floating Instant Clones.
- D. Automated Desktop Pool, based on dedicated Instant Clones.

**Correct Answer: A**

**Section:**

**Explanation:**

An Automated Desktop Pool using Dedicated Full Clone Virtual Machines best meets the requirements because it ensures end-users always receive the same desktop VM, supports backups with VMware's image-based backup tools, and allows for cloning via the vSphere API on a weekly basis. Full clones are standalone VMs that don't depend on a parent VM after being created, making them suitable for image-based backups and consistent user experience.

#### QUESTION 10

An administrator configured a virtual machine to use an NVIDIA card but the virtual machine is not starting up.

What could be the cause of the issue? (Choose two.)

- A. 3D graphics cannot be used with local storage.
- B. The Desktop Pool doesn't support 3D cards.
- C. No suitable host could be found.
- D. Not all memory has been reserved on the VM.
- E. Not all CPU has been reserved on the VM.

**Correct Answer: C, D**

**Section:**

**Explanation:**

When configuring a virtual machine to use an NVIDIA graphics card, issues such as the VM not starting can occur if there is no suitable host available that meets the requirements for 3D graphics, or if not all memory required by the 3D graphics card has been reserved for the VM. Ensuring that the host has the necessary 3D graphics capabilities and that the VM is configured with reserved memory can resolve these issues.

#### QUESTION 11

An administrator has created an application pool for frequently used applications using an RDS Farm. The administrator wants to start these applications immediately after a user has authenticated to the Horizon Connection Server.

Which of the following statements is accurate in this scenario?

- A. Edit the pool and select the Pre-Launch checkbox to start applications immediately after a user has authenticated to the Horizon Connection Server.
- B. Instead of the application pool being of the RDS Farm type, change the Application Pool type to Desktop Pool.

- C. This cannot be done. Published applications cannot start automatically after a user has authenticated to the Horizon Connection Server.
- D. Nothing needs to be done. Published applications start automatically after a user has authenticated to the Horizon Connection Server.

**Correct Answer: A**

**Section:**

**Explanation:**

In VMware Horizon, the Pre-Launch feature allows for the initiation of applications immediately after user authentication, reducing the launch time of frequently used applications. By editing the application pool settings and enabling the Pre-Launch option, administrators can improve user experience by having critical applications ready as soon as the authentication process is completed.

#### QUESTION 12

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**

**Section:**

**Explanation:**

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 13

Which of the following statements are true about Application Profiler?

- A. Application Profiler is installed using VMware Dynamic Environment Manager Enterprise Setup Wizard and explicitly selecting local drive installation.
- B. VMware Dynamic Environment Manager Agent and the Application Profiler cannot be installed on the same machine.
- C. Application Profiler is installed automatically when installing VMware Dynamic Environment Manager FlexEngine.
- D. Application Profiler is installed automatically when installing Dynamic Environment Manager Management Console.

**Correct Answer: A**

**Section:**

**Explanation:**

Application Profiler is a tool that analyzes the registry and file system locations where the settings for a particular application are stored, and creates a Flex configuration file for use with Dynamic Environment Manager. Application Profiler is installed using VMware Dynamic Environment Manager Enterprise Setup Wizard and explicitly selecting local drive installation<sup>1</sup>. This option allows you to install Application Profiler on a separate machine from the Dynamic Environment Manager Agent or Management Console. Alternatively, you can install Application Profiler on the same machine as the Dynamic Environment Manager Agent or Management Console, by selecting network share installation<sup>1</sup>.

VMware Dynamic Environment Manager Agent and the Application Profiler can be installed on the same machine, but it is not recommended. This is because the Dynamic Environment Manager Agent might interfere with the profiling process by applying settings to the application being profiled<sup>1</sup>. Therefore, it is best to use a clean system for profiling applications.

Application Profiler is not installed automatically when installing VMware Dynamic Environment Manager FlexEngine or Management Console. FlexEngine is the component that applies the user environment settings during logon, logoff, and session reconnect or disconnect events<sup>2</sup>. Management Console is the component that allows you to configure and manage the user environment settings<sup>2</sup>. Neither of these components requires Application Profiler to function. Application Profiler is an optional tool that helps you create Flex configuration files for applications that are not included in the predefined settings library<sup>1</sup>. Reference:

VMware Dynamic Environment Manager Overview<sup>2</sup>

Using Application Profiler<sup>1</sup>

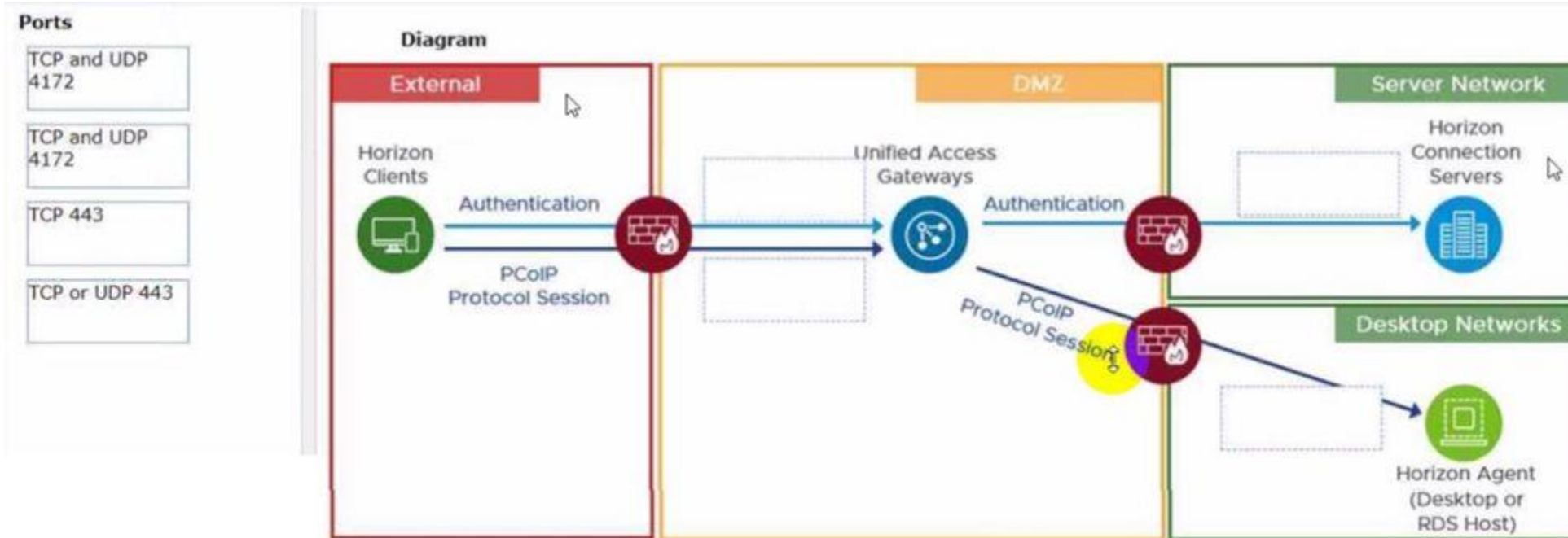
#### QUESTION 14

DRAG DROP

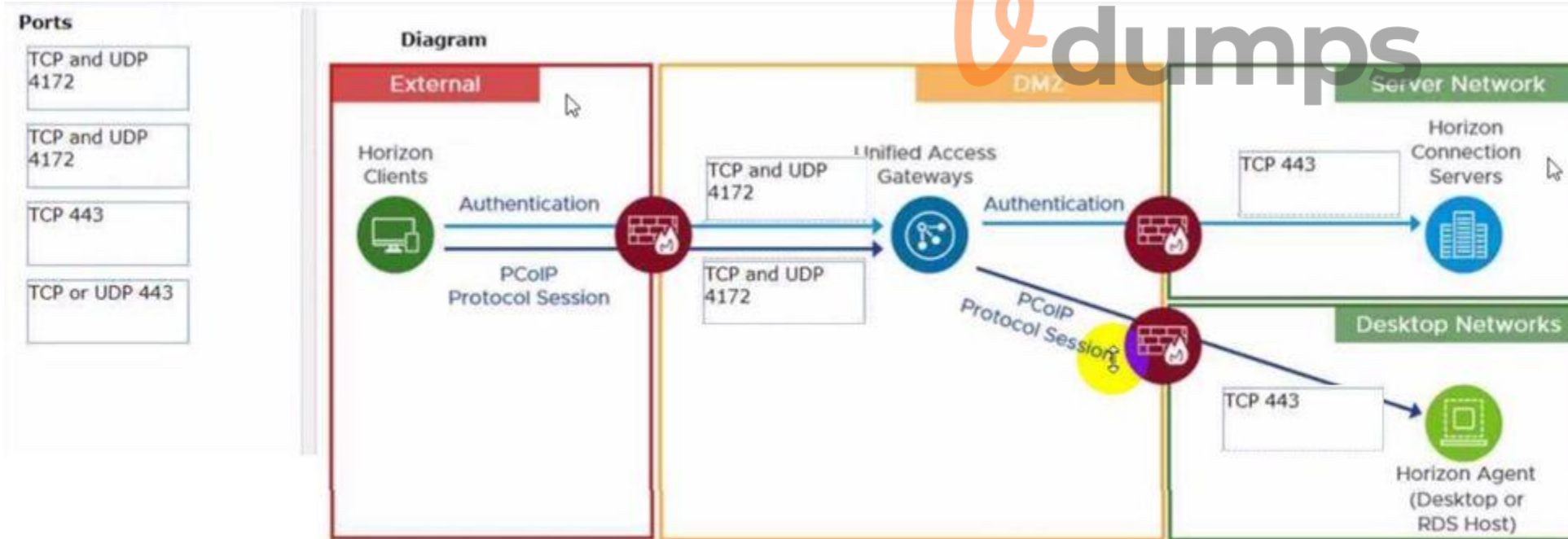
Refer to the exhibit.

Drag and drop the ports on the left to allow an external PCoIP connection through Unified Access Gateway (UAG) into the diagram on the right.

Select and Place:



Correct Answer:



Section:

Explanation:

QUESTION 15

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: A, C**

**Section:**

**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 and up 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.

#### QUESTION 16

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**

**Section:**

**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 sessions.<sup>12</sup>Reference:

Configuring Horizon Connection Server<sup>1</sup>

Understanding VMware Horizon Services<sup>2</sup>

#### QUESTION 17

An administrator has been tasked with determining the type of VMware Horizon deployment for their organization.

These requirements have been provided to the administrator:

\* It must support Windows 10 Enterprise multi-session desktops.

- \* It must support App Volumes.
- \* It must support centralized brokering.
- \* It must automatically route end-users to the most appropriate virtual workspace.

Which deployment solution meets the requirements?

- A. VMware vSphere Desktop Edition
- B. VMware Workspace ONE Unified Endpoint Management
- C. VMware Horizon On-Premises
- D. VMware Horizon Cloud on Microsoft Azure

**Correct Answer: D**

**Section:**

**Explanation:**

VMware Horizon Cloud on Microsoft Azure is the only deployment solution that meets all the requirements. VMware Horizon Cloud on Microsoft Azure supports Windows 10 Enterprise multi-session desktops, which are a new Remote Desktop Session Host exclusive to Azure Virtual Desktop on Azure<sup>1</sup>. It also supports App Volumes, which is a real-time application delivery system that enables IT to instantly provision applications to users or desktops. VMware Horizon Cloud on Microsoft Azure supports centralized brokering, which means that the Horizon Cloud Service acts as a single point of entry for end users to access their virtual desktops and applications. VMware Horizon Cloud on Microsoft Azure also supports automatic routing of end-users to the most appropriate virtual workspace, using the Universal Broker feature. Universal Broker is a cloud-based brokering service that provides a unified user experience across multiple Horizon pods and clouds.

VMware vSphere Desktop Edition does not support Windows 10 Enterprise multi-session desktops, as they are only available on Azure Virtual Desktop<sup>1</sup>. VMware Workspace ONE Unified Endpoint Management does not support App Volumes, as it is a different solution for managing devices and applications. VMware Horizon On-Premises does not support automatic routing of end-users to the most appropriate virtual workspace, as it requires manual configuration of load balancing and global entitlements. Reference:

Profile production applications in Azure with Application Insights Profiler<sup>1</sup>

Using Application Profiler - VMware Docs<sup>2</sup>

First look at profiling tools - Visual Studio (Windows)<sup>3</sup>

App Volumes Overview

Horizon Cloud Service on Microsoft Azure Architecture

Universal Broker Overview

Workspace ONE UEM Overview

Load Balancing Across Pods and Sites in a Cloud Pod Architecture Environment



#### QUESTION 18

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**

**Section:**

**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 applications without 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 SAML<sup>1</sup>. 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 environment<sup>2</sup>. 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 agent<sup>2</sup>.

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 connections<sup>3</sup>. 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 environment<sup>4</sup>. 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)<sup>4</sup>.

A vCenter Server is a management platform that provides centralized control and visibility of vSphere hosts and virtual machines in the Horizon environment<sup>5</sup>. A vCenter Server does not request or issue certificates for users, and it does not integrate with VMware Workspace ONE Access.

VMware Horizon 8.x Professional by VMware<sup>1</sup>

Install and Set Up an Enrollment Server<sup>2</sup>

Install a Replica Connection Server Instance<sup>3</sup>

Install a Security Server<sup>4</sup>

vCenter Server Overview<sup>5</sup>

### QUESTION 19

DRAG DROP

An organization with an existing Windows 2012 R2 Server RDSH farm decided to move to Windows Server 2019 as their new standard. Order the steps that need to be taken by the administrator to deploy a RDS desktop pool with this new standard.

Select and Place:

**Steps**

- Add a RDS desktop pool.
- Launch Horizon Client and verify access to RDS desktop.
- Entitle AD users and/or groups.
- Prepare the Windows Server 2019 golden image.
- Add an Automated Farm.

**Sequential Order**

Correct Answer:

## Steps


## Sequential Order

	Prepare the Windows Server 2019 golden image.	
	Add an Automated Farm.	
	Add a RDS desktop pool.	
	Entitle AD users and/or groups.	
	Launch Horizon Client and verify access to RDS desktop.	

### Section:

### Explanation:

Prepare the Windows Server 2019 golden image.

Add an Automated Farm.

Add a RDS desktop pool.

Entitle AD users and/or groups.

Launch Horizon Client and verify access to RDS desktop.

### QUESTION 20

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

### Section:

### Explanation:

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 availability<sup>1</sup>.

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 desktops<sup>2</sup>.

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 Extreme<sup>3</sup>.

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 directly<sup>4</sup>.

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 sessions 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.

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 21

An administrator needs to enable Session Collaboration in the VMware Horizon environment. What will be used as a requirement to enable Session Collaboration?

- A. floating Instant Clone pool
- B. dedicated Instant Clone pool
- C. PCoIP protocol
- D. BLAST protocol

**Correct Answer: D**

**Section:**

**Explanation:**

Collaboration is a feature that allows users to invite other users to join an existing Windows or Linux remote desktop session with both screen sharing and audio out features enabled. A remote desktop session that is shared in this way is called a collaborative session. The user that shares a session with another user is called the session owner, and the user that joins a shared session is called a session collaborator. A Horizon administrator must enable the Session Collaboration feature for the desktop pool or farm that contains the remote desktops that support collaboration.

One of the requirements to enable Session Collaboration is to use the VMware Blast display protocol for the remote desktops. VMware Blast is a protocol that provides high-performance, high-quality graphics and multimedia delivery over LAN or WAN networks. VMware Blast supports Session Collaboration by allowing multiple users to view and interact with the same remote desktop session simultaneously. Other display protocols, such as PCoIP or RDP, do not support Session Collaboration and will not allow users to share or join collaborative sessions.

Therefore, to enable Session Collaboration in the VMware Horizon environment, the administrator needs to use the BLAST protocol as a requirement. Reference: Configuring Session Collaboration, Sharing Remote Desktop Sessions, and [VMware Horizon 8.x Professional Course]

#### QUESTION 22

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.

**Correct Answer: A, D**



**Section:****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. Reference: Configuring URL Content Redirection and [VMware Horizon 8.x Professional Course]

**QUESTION 23**

An administrator needs to deploy an application to specific users in their instant-clone desktop environment with the following characteristics:

- \* The application needs to be updated very frequently.
- \* The application needs to be installed as soon as possible.
- \* The application is not multi-user aware.

Which solution would meet the requirements?

- A. VMware Horizon Published Application
- B. VMware Dynamic Environment Manager
- C. VMware ThinApp
- D. VMware App Volumes

**Correct Answer: D**

**Section:****Explanation:**

VMware 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.

App Volumes is a suitable solution for deploying an application to specific users in an instant-clone desktop environment with the following characteristics:

The application needs to be updated very frequently: App Volumes allows administrators to update applications in real time by using the update or push-image operations. These operations replace the existing packages with new ones that have the latest updates applied, without affecting the user data or settings. The updated packages are delivered to the users at the next login or refresh.

The application needs to be installed as soon as possible: App Volumes allows administrators to install applications quickly and easily by using a clean packaging system and capturing the application installation process. The resulting package can be assigned to users or groups immediately, without requiring any recomposing or rebooting of the desktops.

The application is not multi-user aware: App Volumes allows administrators to deliver applications that are not multi-user aware by using writable volumes. Writable volumes are user-specific virtual disks that store user-installed applications, data, and settings. Writable volumes can be attached to desktops along with application packages, and they can isolate the user-installed applications from the system-installed applications.

The other options are not suitable for meeting the requirements:

VMware Horizon Published Application: This option allows administrators to publish applications from RDS hosts to users in Horizon. However, this option requires a separate RDS infrastructure and licensing, and it does not support instant updates or writable volumes for user-installed applications.

VMware Dynamic Environment Manager: This option allows administrators to manage user profiles and policies in Horizon. However, this option does not deliver or update applications, and it does not support writable volumes for user-installed applications.

VMware ThinApp: This option allows administrators to package applications into portable executables that can run on any Windows system without installation. However, this option requires a separate packaging process and licensing, and it does not support instant updates or writable volumes for user-installed applications.

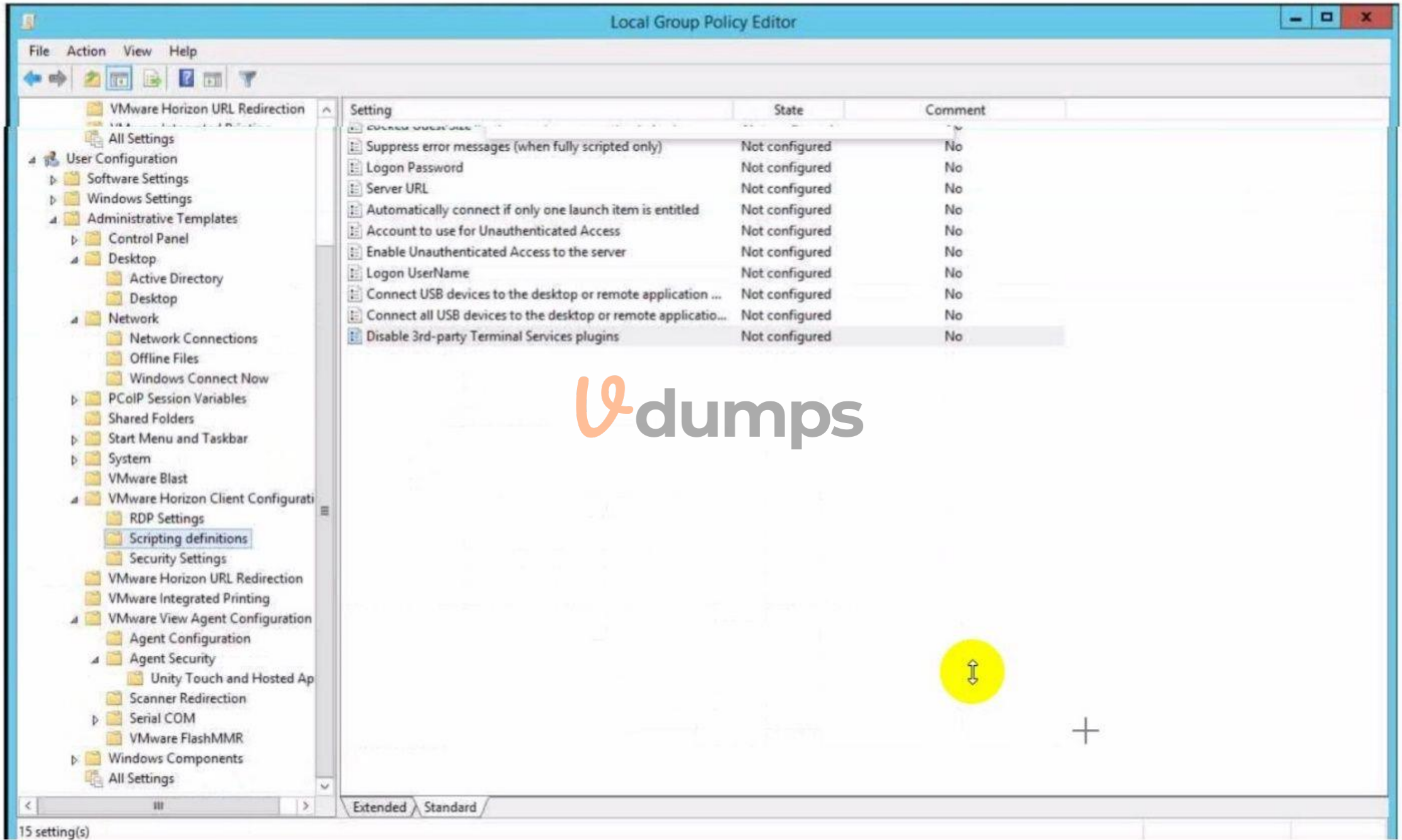
**QUESTION 24****HOTSPOT**

Refer to the exhibit.

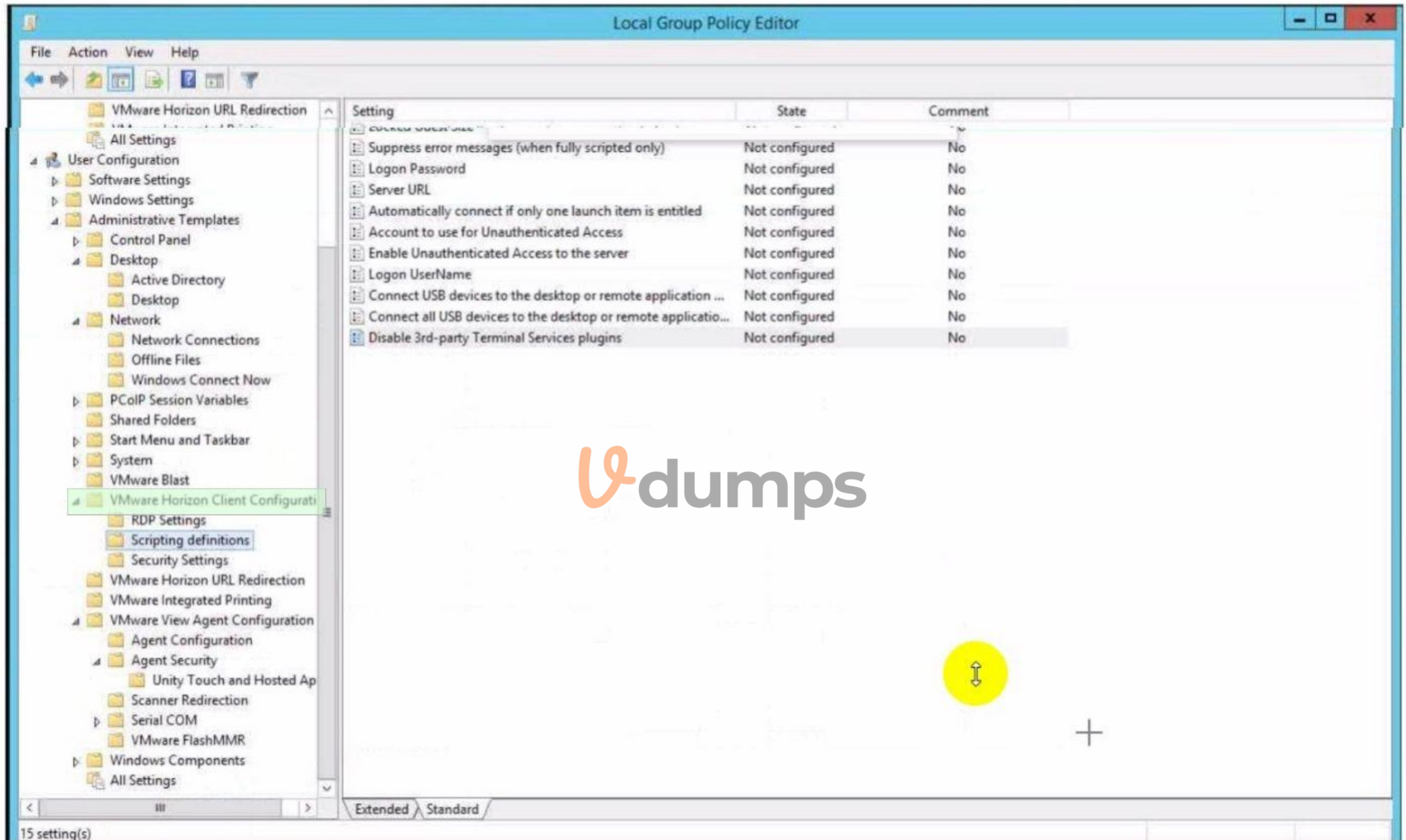


An administrator wants to set the initial login into a VDI desktop to be full screen.  
In the Group Policy Management Editor Window, mark the setting that needs to be configured by clicking on it.

Hot Area:



Answer Area:



Section:

Explanation:

**QUESTION 25**

An administrator is preparing to upgrade Horizon Connection Servers in parallel.

What action must first be performed to ensure that there are no issues with Horizon LDAP replication within the Pod?

- A. Execute repadmin.exe/showrepl localhost:389.
- B. Execute ViewDBChk.cmd --scanMachines.
- C. Execute vdmexport.exe -f Myexport.IDF.
- D. Execute vdmadmin.exe -S.

**Correct Answer: A**

**Section:**

**Explanation:**

The action that must first be performed to ensure that there are no issues with Horizon LDAP replication within the Pod is to execute repadmin.exe/showrepl localhost:389. This command will display the replication status of the local Connection Server instance and show any errors or warnings that might affect the replication process<sup>1</sup>. The administrator should run this command on each Connection Server instance in the Pod before upgrading them in parallel, and resolve any issues that are reported.

The other options are not valid or feasible because:

Executing ViewDBChk.cmd --scanMachines will not check the Horizon LDAP replication status, but rather scan the vCenter Server inventory for virtual machines that are managed by Horizon and report any inconsistencies or errors<sup>2</sup>. This command is useful for troubleshooting virtual machine issues, but not for verifying LDAP replication.

Executing vdmexport.exe -f Myexport.IDF will not check the Horizon LDAP replication status, but rather export the Horizon LDAP configuration data to a file named Myexport.IDF<sup>3</sup>. This command is useful for backing up or restoring the Horizon LDAP data, but not for verifying LDAP replication.

Executing vdmadmin.exe -S will not check the Horizon LDAP replication status, but rather display the health status of the Connection Server instances in the Pod<sup>4</sup>. This command is useful for monitoring the Connection Server performance and availability, but not for verifying LDAP replication.

Repadmin Examples<sup>1</sup>

ViewDBChk Tool<sup>2</sup>

Back Up Horizon Configuration Data<sup>3</sup>

Display Health Status Information<sup>4</sup>



**QUESTION 26**

DRAG DROP

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

**Select and Place:**

**Horizon Role**

**Function**

Administrator



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

Inventory Administrator



Performs all administrative functions and applies to an Access Group.

Local Administrator

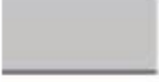




No rights to manage Cloud Pod or the Global Data Layer.

**Correct Answer:**

## Horizon Role

## Function

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.

### Section:

### Explanation:

Some possible references are:  
Predefined Administrator Roles  
Assigning Administrator Roles  
Understanding Roles and Privileges

### QUESTION 27

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: B, C, E**

### Section:

### 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.

Virtual Machines Overview

Creating and Provisioning Virtual Machines

Migrating Virtual Machines

### QUESTION 28

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: A, B, C**

**Section:**

**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 resources<sup>12</sup>. Reference:=1: VMware Horizon Architecture Planning:Unified Access Gateway2: VMware Unified Access Gateway Administration Guide:Introduction to Unified Access Gateway

#### QUESTION 29

Which two of the following are features of VMware Horizon Agent for Linux? (Choose two.)

- A. USB redirection
- B. location based printing
- C. display protocol PCoIP
- D. installation registration requirement
- E. session collaboration

**Correct Answer: A, C**

**Section:**

**Explanation:**

VMware Horizon Agent for Linux is a software component that enables Linux machines to be used as remote desktops or published applications in a Horizon environment. Horizon Agent for Linux supports several features that enhance the user experience and manageability of Linux desktops and applications, such as USB redirection, display protocol PCoIP, multiple-session mode, single sign-on, smart card authentication, and 3D graphics<sup>34</sup>. However, Horizon Agent for Linux does not support location based printing or session collaboration features that are available for Windows machines<sup>5</sup>. Also, Horizon Agent for Linux does not require installation registration as it automatically registers with the Connection Server when the viewagent service is started<sup>6</sup>. Reference:=3: VMware Horizon 8 Documentation:Horizon Agent for Linux4: VMware Horizon 8 Documentation:Features Supported by Horizon Agent for Linux5: VMware Horizon 8 Documentation:Features Not Supported by Horizon Agent for Linux6: VMware Horizon 8 Documentation:Install Horizon Agent on a Linux Machine

#### QUESTION 30

HOTSPOT

Refer to the exhibit.

An administrator wants the current site to be designated as the Home Site for a user.

Mark the menu option on the left that will allow the administrator to assign home sites by clicking on it.

**Hot Area:**



Refer to the exhibit.

An administrator wants the current site to be designated as the Home Site for a user.

Mark the menu option on the left that will allow the administrator to assign home sites by clicking on it.

The screenshot shows the VMware Horizon administrator interface. The top navigation bar includes the VMware logo, the text 'VMware Horizon\*', the pod cluster name 'Pod Cluster-HORIZON-0...', a search bar labeled 'User Search', and user information 'administrator'. The left sidebar menu is expanded to 'Sites', which is highlighted in grey. The main content area is titled 'Sites' and contains three buttons: 'Add', 'Edit', and 'Delete'. Below these buttons is a table with the following data:

Name	Description	Number of Pods
<input type="radio"/> Default First Site		2

At the bottom right of this table, it says '1 - 1 of 1 row(s)'. Below the table is an 'Edit' button. Underneath the 'Edit' button is another table with the following data:

Pod	Description	Global Entitlement
No records available.		

At the bottom right of this table, it says '0 rows'. A large 'Vdumps' watermark is overlaid on the center of the screenshot.

Answer Area:



Refer to the exhibit.

An administrator wants the current site to be designated as the Home Site for a user.

Mark the menu option on the left that will allow the administrator to assign home sites by clicking on it.

The screenshot shows the VMware Horizon administrator interface. The left-hand navigation pane is expanded to show 'Cloud Pod Architecture' highlighted. The main content area is titled 'Sites' and contains a table with the following data:

Name	Description	Number of Pods
<input type="radio"/> Default First Site		2

Below the 'Sites' table is an 'Edit' button and another table with the following data:

Pod	Description	Global Entitlement
No records available.		

**Section:**

**Explanation:**

**QUESTION 31**

An administrator recently deployed a Horizon pod with external access using Unified Access Gateway (UAG). While trying to launch VDI from an External network, VDI launches with a black screen and then disconnects. The administrator has validated the port requirement and all other required ports are open. Users are able to connect internally using the connection server URL. While reviewing the UAG logs, the administrator found that the Blast connection is hitting the Connection Server instead of VDI IP.

What should the administrator do to resolve the issue?

- A. Update the Blast External URL in UAG with port number.
- B. Upload the Blast Proxy Certificate in Horizon Edge Settings.
- C. Enable Tunnel in UAG.
- D. Disable the Tunnel and Gateways in Horizon Connection Server.

**Correct Answer: D**

**Section:**

**Explanation:**

The issue described indicates that the Horizon Connection Server is incorrectly handling traffic that should be directed to the Unified Access Gateway (UAG) and then to the VDI desktops. Disabling the Tunnel and Gateways settings on the Horizon Connection Server forces the UAG to handle the Blast traffic directly, ensuring that the connections are made to the VDI desktops' IP addresses, thus resolving the black screen and disconnection issue.

#### QUESTION 32

An administrator needs to upgrade a Unified Access Gateway (UAG) appliance. The UAG is connected to a load balancer with other UAGs and has existing sessions. Which option provided allows minimal downtime for maintenance?

- A. Enable Quiesce Mode in the UAG Admin UI.
- B. Remove the Horizon Connection Server thumbprint in the UAG Admin UI.
- C. Suspend the UAG appliance.
- D. Power off the UAG appliance.

**Correct Answer: A**

**Section:**

**Explanation:**

Enabling Quiesce Mode in the Unified Access Gateway (UAG) Admin UI is the recommended approach for minimizing downtime during maintenance or upgrades when the UAG is part of a load-balanced cluster. Quiesce Mode allows the UAG to stop accepting new connections while allowing existing sessions to continue until they naturally end. This ensures minimal disruption to users and allows for a controlled upgrade process.

#### QUESTION 33

An administrator needs to configure BLAST Bandwidth Profiles to define the quality, maximum session bandwidth, and frame rate. Which are the two possible ways an administrator can accomplish this goal? (Choose two.)

- A. Create a login script which will set all required settings in the desktop.
- B. Use post-synchronization scripts during pool creation to define these settings.
- C. Configure these BLAST settings in the desktop pool configuration.
- D. Use Horizon Smart Policies of Dynamic Environment Manager.
- E. Set all required settings from a profile manually through GPO policies.

**Correct Answer: D, E**

**Section:**

**Explanation:**

Configuring BLAST Bandwidth Profiles involves setting quality, maximum session bandwidth, and frame rate controls. This can be effectively managed using Horizon Smart Policies within VMware's Dynamic Environment Manager (DEM), which allows administrators to create contextual policies that dynamically adapt to the end-user's environment. Alternatively, Group Policy Objects (GPOs) can be used to manually set these configurations across the desktop environment, providing a more static approach to enforcing these settings.

#### QUESTION 34

Which two steps must be completed in order to expand a Writable Volume? (Choose two.)

- A. Select Volumes > Writables > Select Volume > Update Writable.

- B. Specify a size which is at least 1MB larger than the current size of the volume.
- C. Select Volumes > Writables > Select Volume > Expand.
- D. Specify a size which is at least 1GB larger than the current size of the volume.
- E. Modify the snapvol.cfg to reflect the new size.

**Correct Answer: A, D**

**Section:**

**Explanation:**

To expand a Writable Volume in VMware Horizon, the administrator needs to navigate to the Volumes > Writables section in the Horizon Console, select the specific volume, and choose the option to update or expand the writable volume. The new size specified must be at least 1GB larger than the current size to ensure there is enough space for the expansion process and to accommodate the growth of user data.

#### QUESTION 35

A senior Horizon administrator is tasked with enabling two-factor authentication for other Horizon administrators to login to the Horizon Console. Which option will the administrator use that supports two-factor authentication?

- A. Smart Card Authentication
- B. RSA SecureID
- C. SAML
- D. RADIUS

**Correct Answer: D**

**Section:**

**Explanation:**

RADIUS (Remote Authentication Dial-In User Service) supports two-factor authentication and can be integrated with VMware Horizon to secure administrative access to the Horizon Console. RADIUS servers authenticate users based on a combination of something they know (a password) and something they have (a token or mobile app-generated code), providing an added layer of security for administrative logins.

#### QUESTION 36

Which storage product allows the pooling of resources to create datastores in a software defined datacenter?

- A. VMware VMFS
- B. VMware Storage I/O Control
- C. VMware HCI Mesh
- D. VMware vSAN

**Correct Answer: D**

**Section:**

**Explanation:**

VMware vSAN is a storage product that allows the pooling of resources to create datastores in a software defined datacenter. VMware vSAN is a hyper-converged infrastructure solution that integrates compute, storage, and networking resources on industry-standard x86 servers. VMware vSAN aggregates local or direct-attached data storage devices to create a single storage pool shared across all hosts in the vSAN cluster. VMware vSAN enables you to provision and manage storage from the VMware vSphere Web Client or the VMware vCenter Server Appliance Shell. VMware vSAN provides several benefits, such as lower total cost of ownership, simplified management, high performance, scalability, and availability.<sup>12</sup> Reference:=1: VMware Horizon 8 Documentation:VMware vSAN Overview2: VMware Horizon 8 Documentation:Benefits of Using VMware vSAN with Horizon 8

#### QUESTION 37

DRAG DROP

Drag and drop the codecs supported by Blast on the left to the appropriate use case on the right.

**Select and Place:**

Codec	Use Case
JPEG / PNG	low-motion graphics, high-quality graphics such as Photoshop, and AutoCAD
H.264	rapidly moving content and motion graphics such as streaming video
HEVC	rapidly moving content and motion graphics such as streaming video on a low bandwidth resource
Blast Codec	still images such as spreadsheets and documents

Correct Answer:

Codec	Use Case
Blast Codec	low-motion graphics, high-quality graphics such as Photoshop, and AutoCAD
H.264	rapidly moving content and motion graphics such as streaming video
HEVC	rapidly moving content and motion graphics such as streaming video on a low bandwidth resource
JPEG / PNG	still images such as spreadsheets and documents

Section:

Explanation:

**QUESTION 38**

Which three steps are required to entitle user and groups to pools? (Choose three.)

- A. Run the Active Directory entitlement script in the golden master, when preparing if for the pool.
- B. During pool creation in the entitlement pane, click on add, search for users and groups in the Active Directory, continue and finish the pool creation.
- C. During the Pool creation the desired Active Directory OU for the VMs will be specified. This will automatically add the preconfigured associated user group to the Horizon entitlements.
- D. Navigate to Inventory > Desktops > check mark a pool > click on Add Entitlement.

E. Navigate to Users and Groups > Entitlements > click on Entitlements > click on Add Entitlements, search for users and groups in the Users pane and add the desired desktop pool in the next pane Desktop Pools.

**Correct Answer: B, D, E**

**Section:**

**Explanation:**

To entitle users and groups to pools, you need to perform the following steps:

During pool creation in the entitlement pane, click on add, search for users and groups in the Active Directory, continue and finish the pool creation. This option allows you to entitle users and groups to a desktop or application pool at the same time as you create the pool<sup>3</sup>.

Navigate to Inventory > Desktops > check mark a pool > click on Add Entitlement. This option allows you to add entitlements to an existing desktop or application pool after you create the pool<sup>4</sup>.

Navigate to Users and Groups > Entitlements > click on Entitlements > click on Add Entitlements, search for users and groups in the Users pane and add the desired desktop pool in the next pane Desktop Pools. This option allows you to review and manage the entitlements for users and groups from a single location<sup>5</sup>.

The other options are not required or valid for entitling users and groups to pools. Running the Active Directory entitlement script in the golden master is not necessary as Horizon 8 automatically synchronizes with Active Directory domains that are configured in Horizon Console<sup>6</sup>. Specifying the desired Active Directory OU for the VMs during pool creation does not automatically add the preconfigured associated user group to the Horizon entitlements as you still need to select the users or groups from the search results<sup>7</sup>. Reference: <sup>3</sup> VMware Horizon 8 Documentation: Add Entitlements During Pool Creation <sup>4</sup> VMware Horizon 8 Documentation: Add Entitlements After Pool Creation <sup>5</sup> VMware Horizon 8 Documentation: Review and Manage Entitlements <sup>6</sup> VMware Horizon 8 Documentation: Active Directory Requirements for Horizon Connection Server <sup>7</sup> VMware Horizon 8 Documentation: Create an Automated Desktop Pool

### QUESTION 39

An administrator is creating an instant clone desktop pool and needs to enable NVIDIA Grid 3D Rendering. NVIDIA GRID vGPU and drivers are installed on the physical ESXi hosts.

In Horizon Console, when creating an instant-clone pool, the NVIDIA GRID vGPU option is not available in the 3D Render field.

Which two of the following could be the reason for the issue? (Choose two.)

- A. Horizon 8 does not have an explicit 3D renderer option for instant clone. Select Manage Using vSphere Client in the 3D Render field. Instant-clones inherit the settings configured in the vSphere Client for the golden image.
- B. In Horizon Console, when an instant-clone pool is created, the golden image and snapshot that the administrator selected has not been configured for NVIDIA GRID vGPU.
- C. The administrator has selected Shared when editing the Host Graphics Settings for the ESXi host in the vCenter Server.
- D. Instant-clone pools do not support NVIDIA GRID vGPU.
- E. The administrator has selected Shared Direct when editing the Host Graphics Settings for the ESXi host in the vCenter Server.

**Correct Answer: A, B**

**Section:**

**Explanation:**

To enable an instant-clone pool to use NVIDIA GRID vGPU, the administrator needs to do the following:

Install NVIDIA GRID vGPU in the physical ESXi hosts and select Shared Direct in the Host Graphics Settings<sup>12</sup>.

Prepare a golden image with NVIDIA GRID vGPU configured, including selecting the vGPU profile to use<sup>12</sup>.

Take a snapshot of the golden image<sup>12</sup>.

In Horizon Console, when creating an instant-clone pool, select Manage Using vSphere Client in the 3D Render field. Instant-clones inherit the settings configured in the vSphere Client for the golden image<sup>12</sup>.

Therefore, the possible reasons for the issue are:

The administrator has selected Shared instead of Shared Direct when editing the Host Graphics Settings for the ESXi host in the vCenter Server. This option is for vSGA, not vGPU<sup>3</sup>.

The golden image and snapshot that the administrator selected has not been configured for NVIDIA GRID vGPU. The administrator needs to verify that the correct vGPU profile is selected and that the NVIDIA drivers are installed in the golden image<sup>4</sup>.

The other options are not valid because:

Horizon 8 does have an explicit 3D renderer option for instant clone, but it is Manage Using vSphere Client, not NVIDIA GRID vGPU<sup>12</sup>.

Instant-clone pools do support NVIDIA GRID vGPU as long as the ESXi hosts and the golden image are properly configured<sup>12</sup>.