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

100% Passing Guarantee
100% Money Back Assurance

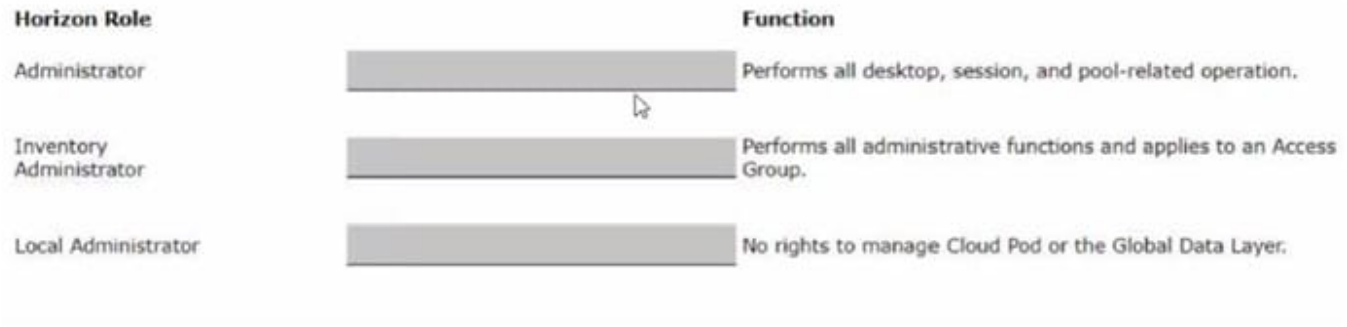
Following Questions and Answers are all new published by VMware Official Exam Center

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

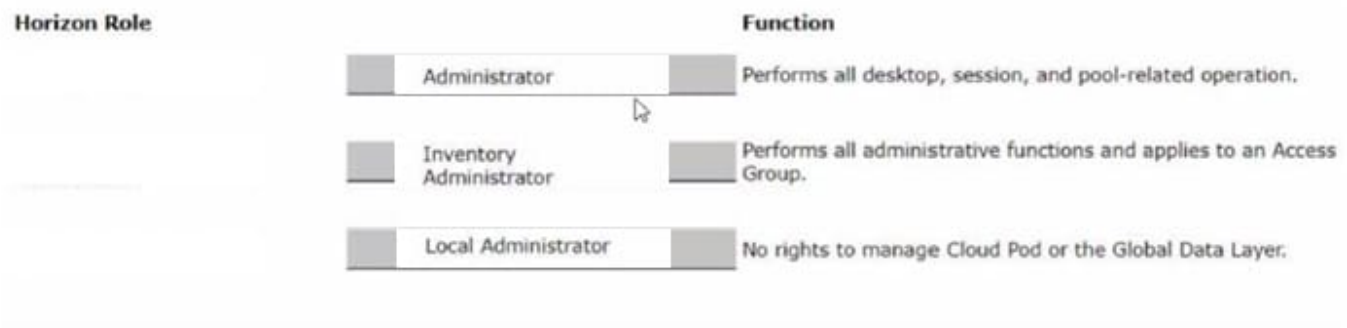
QUESTION 1

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

Select and Place:



Correct Answer:



The following is the correct answer for the drag and drop question:

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.

Predefined Administrator Roles (vmware.com)

The predefined administrator roles in Horizon console are designed to provide different levels of access and control over the Horizon environment. Each role has a set of privileges that grant the ability to perform specific actions or view certain

information. You can assign these roles to users or groups on the root access group, which gives them access to all inventory objects in the system, or on a specific access group or federation access group, which limits their scope to the

objects within that group. You cannot modify the predefined roles, but you can create custom roles by selecting individual privileges.

The Administrator role is the most powerful role in Horizon console. It allows the user to perform all administrative operations, including creating and managing desktop pools, sessions, farms, applications, global settings, and other

administrators. In a Cloud Pod Architecture environment, this role also enables the user to configure and manage a pod federation and manage remote pod sessions. The Administrator role on the root access group is equivalent to a super

user role, as it gives full access to everything in the system. Therefore, you should assign this role to a limited number of users.

The Inventory Administrator role is similar to the Administrator role, but it applies only to an access group. This means that the user can perform all administrative functions on the inventory objects that belong to that access group, such as

desktop pools, farms, applications, and sessions. However, the user cannot manage global settings or other administrators. This role is useful for delegating administration of specific resources to different users or groups.

The Local Administrator role is a restricted version of the Inventory Administrator role. It applies only to an access group and does not grant any rights to manage Cloud Pod Architecture features or the Global Data Layer. This means that the

user can only manage local inventory objects within that access group, such as desktop pools, farms, applications, and sessions. This role is suitable for administrators who do not need to access or modify global settings or cross-pod

resources.

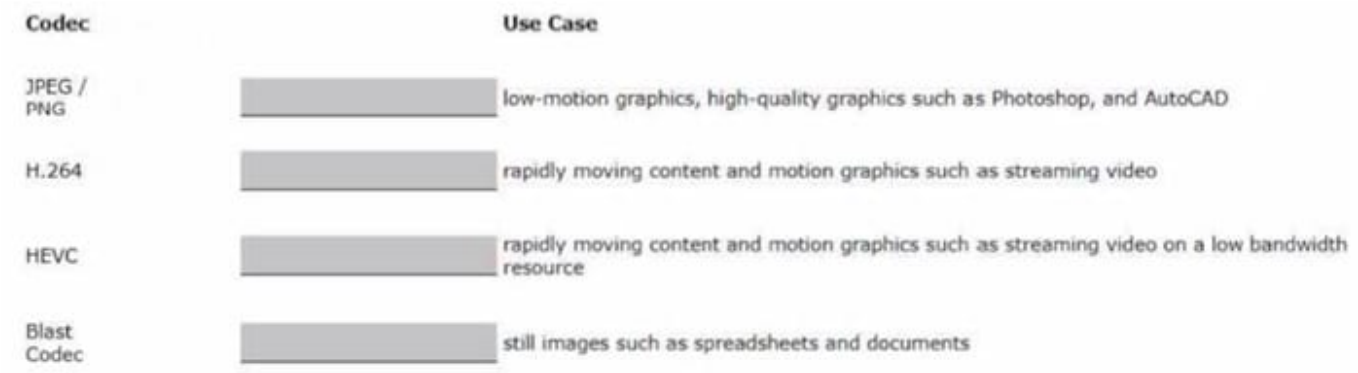
The Help Desk Administrator role is a specialized role that allows the user to perform desktop and application actions for troubleshooting and support purposes. These actions include shutting down, resetting, restarting, logging off,

disconnecting, and sending messages to users

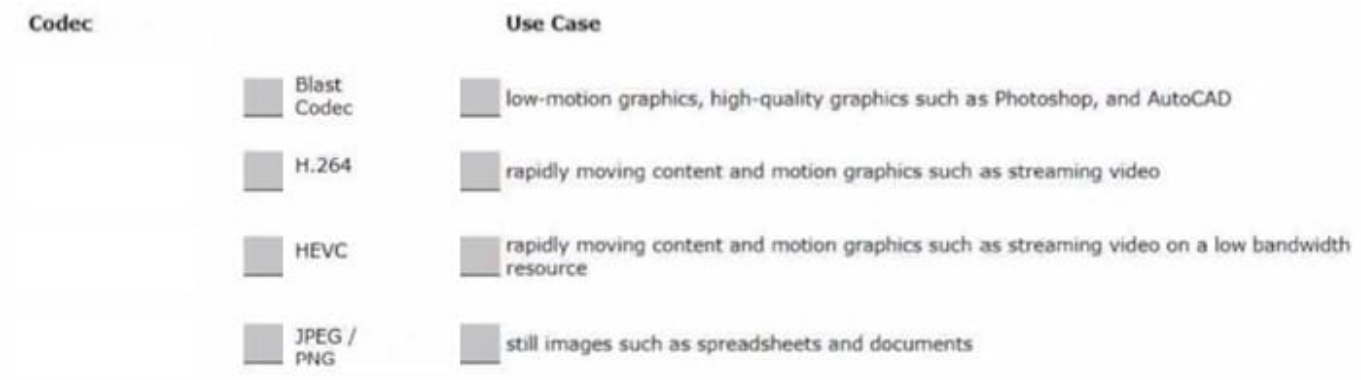
QUESTION 2

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

Select and Place:



Correct Answer:



JPEG/PNG - Still images.

H.264: Rapidly moving content and motion graphics such as streaming video, video editing, and gaming.

HEVC: Rapidly moving content on a low bandwidth resource.

Proprietary Blast codec: Low-motion graphics, high-quality graphics such as Photoshop, and AutoCAD.

QUESTION 3

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: AC

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 andup 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.

References: Cloud Pod Architecture Limitations in Horizon 8 and [VMware Horizon 8.x Professional Course]

QUESTION 4

What is the default URL used to access the Horizon Console?

A. https:///admin

B. https:///default

C. https:///administrator

D. https:///login

Correct Answer: A

Explanation: The default URL used to access the Horizon Console is https:///admin, where is the fully qualified domain name of the Connection Server instance. This URL allows you to log in to Horizon Console by using a secure (TLS) connection. You can also use the IP address of the Connection Server instance instead of the FQDN, but this might result in blocked access or reduced security due to certificate mismatch. You cannot use https://localhost to connect fromthe Connection Server host, but you can use https://127.0.0.1 instead. The other options are not valid URLs for Horizon Console. References: Log In to Horizon Console

QUESTION 5

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: AD

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 establishedbetween 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]