

# 2V0-51.23<sup>Q&As</sup>

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**

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

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 applicationswithout 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 SAML1. 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 environment2. 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 agent2. 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 connections3. 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 environment4. 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)4. A vCenter Server is a management platform that provides centralized control and visibility of vSphere hosts and virtual machines in the Horizon environment5. A vCenter Server does not request or issue certificates for users, and it does not integrate with VMware Workspace ONE Access. References: VMware Horizon 8.x Professional by Vmware1 Install and Set Up an Enrollment Server2 Install a Replica Connection Server Instance3 Install a Security Server4 vCenter Server Overview5

# **QUESTION 2**

Which vCenter privileges are required only for instant clones VMs with a Trusted Platform Module (vTPM) device?

- A. Upgrade virtual machine compatibility
- B. Manage KM5
- C. Configure Host USB device
- D. Manage custom attributes
- Correct Answer: B

A Trusted Platform Module (vTPM) is a virtualized version of a physical TPM device that provides enhanced security for virtual machines. A vTPM device can be added to a virtual machine to enable features such as encryption, attestation,



and key management. A vTPM device requires a Key Management Server (KMS) to store and manage the encryption keys.

To create instant clones VMs with a vTPM device, the vCenter Server user must have certain privileges in addition to those required for instant clones without a vTPM device. One of these privileges is Manage KMS, which allows the user to

perform cryptographic operations on the vTPM device, such as cloning, decrypting, encrypting, migrating, and registering. The Manage KMS privilege is part of the Cryptographic operations privilege group on vCenter Server.

The other options are not required only for instant clones VMs with a vTPM device:

Upgrade virtual machine compatibility: This privilege allows the user to upgrade the virtual hardware version of a virtual machine to support new features and capabilities. This privilege is required for instant clones VMs regardless of whether

they have a vTPM device or not.

Configure Host USB device: This privilege allows the user to configure USB devices on an ESXi host and attach them to a virtual machine. This privilege is not related to vTPM devices or instant clones VMs.

Manage custom attributes: This privilege allows the user to create, edit, and delete custom attributes for vCenter Server objects. Custom attributes are user-defined fields that can store additional information about objects. This privilege is not

related to vTPM devices or instant clones VMs.

References: Privileges Required for the vCenter Server User With Instant Clones, vSphere Virtual Machine Administration, and [VMware Horizon 8.x Professional Course]

# **QUESTION 3**

#### DRAG DROP

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:



#### **QUESTION 4**

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: DE

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 5**

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

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.

2V0-51.23 PDF Dumps

2V0-51.23 Exam Questions

2V0-51.23 Braindumps