2V0-51.23Q&As

VMware Horizon 8.x Professional

Pass VMware 2V0-51.23 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/2v0-51-23.html

100% Passing Guarantee
100% Money Back Assurance

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

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

QUESTION 1

Refer to the exhibit.

An administrator prepared a golden image based on a Windows Server Operating System.

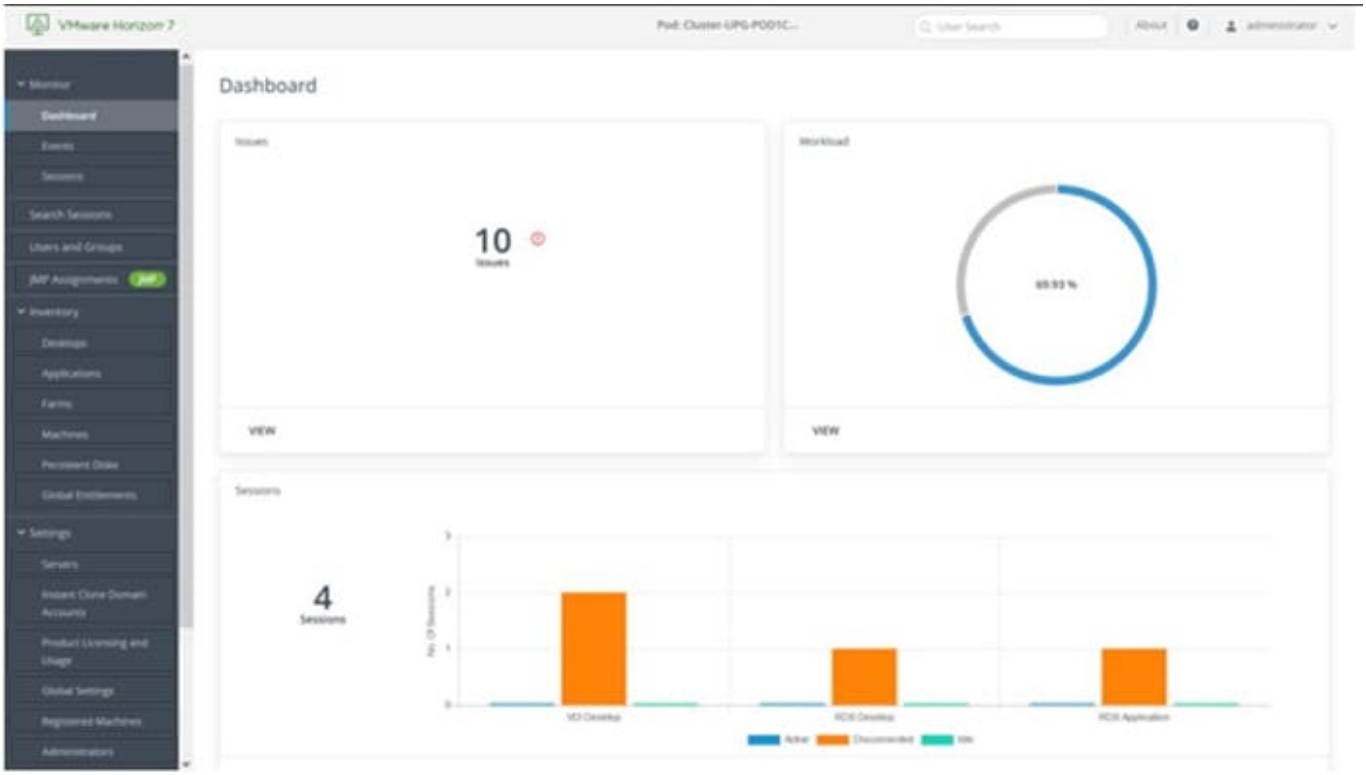
They plan to use this image to create a single-session virtual desktop pool. The installation is completed, the virtual machine is turned off, and the snapshot has been created. When the administrator creates the desktop pool, they are unable

to select the created image and snapshot. They do see other previously created golden images, based on Desktop Operating Systems.

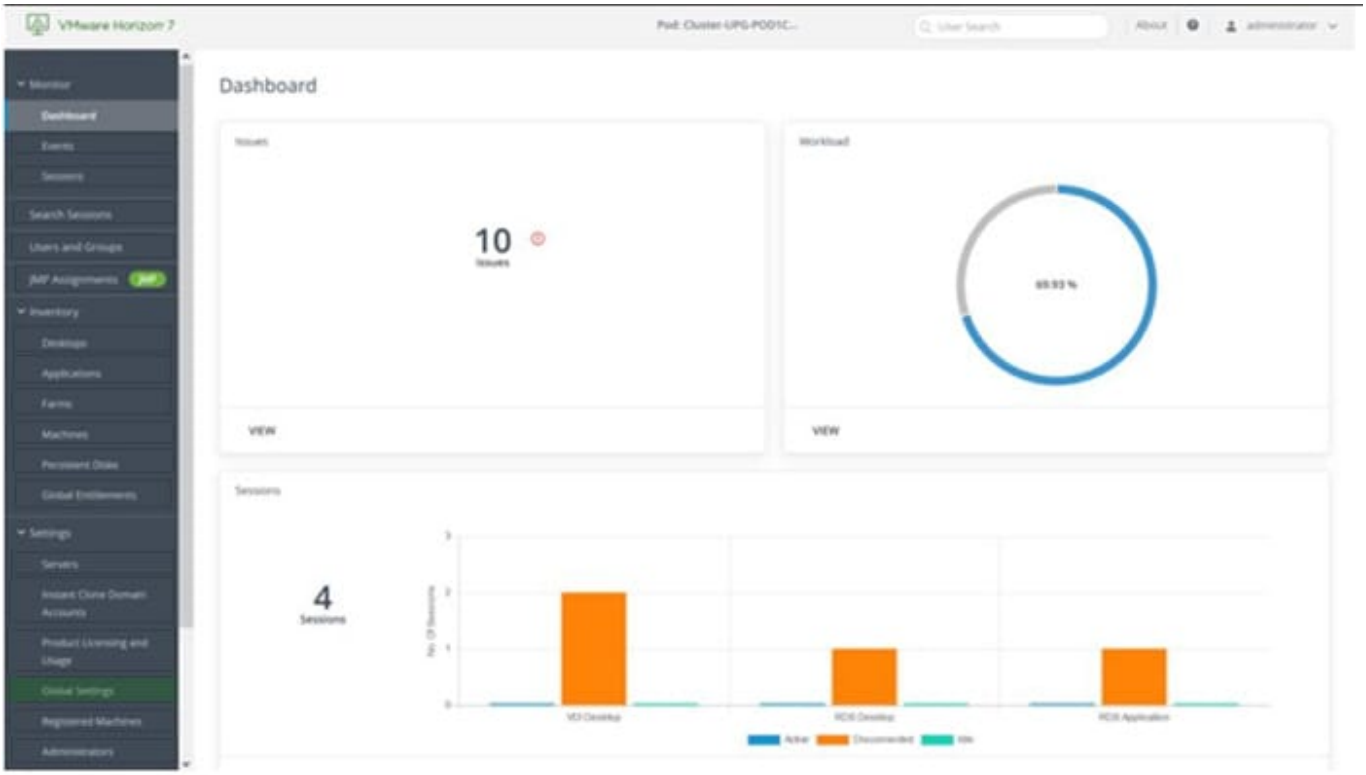
The administrator has opened the Horizon Console.

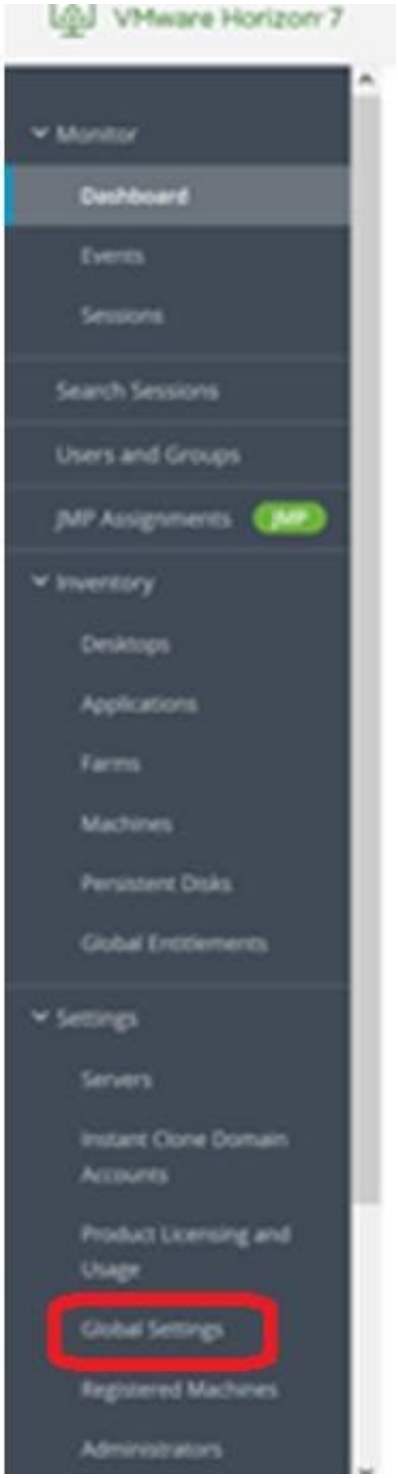
Mark the correct menu option where the administrator can enable Windows Server Operating Systems to be used as single-session desktops by clicking on it.

Hot Area:



Correct Answer:


Dashboard
10
VIEW
VIEW
4
Sessions



QUESTION 2

Which two capabilities are supported by VMware Dynamic Environment Manager Application Profiler? (Choose two.)

A. It allows individual user personalization of applications.

B. It allows creation of application-specific predefined settings.

C. It allows third-party user personalization of applications.

D. It analyzes registry and file system location settings for an application.

E. It allows creation of computer templates.

Correct Answer: BD

Explanation: VMware Dynamic Environment Manager Application Profiler is a standalone application that simplifies the creation of Flex configuration files and predefined settings for use with VMware Dynamic Environment Manager.

Application Profiler analyzes where an application stores its file and registry configuration. The analysis results in an optimized Flex configuration file, which you can edit in the Application Profiler or use directly in the VMware Dynamic

Environment Manager environment. With Application Profiler, you can also create application-specific predefined settings, with which you can set the initial configuration state of applications. Save the Flex configuration file with predefined

settings to export the current application configuration state1. Therefore, the two capabilities that are supported by VMware Dynamic Environment Manager Application Profiler are:

It allows creation of application-specific predefined settings. This means that you can configure the default settings for an application that will be applied when a user launches it for the first time. For example, you can set the language, theme,

or preferences of an application using Application Profiler2. It analyzes registry and file system location settings for an application. This means that it monitors the changes that an application makes to the registry and file system when it is

running, and generates a Flex configuration file that captures those changes. This allows VMware Dynamic Environment Manager to manage the user personalization of those settings across different devices and sessions3. The other

options are not supported by VMware Dynamic Environment Manager Application Profiler:

It allows individual user personalization of applications. This is not a capability of Application Profiler, but rather of VMware Dynamic Environment Manager itself. Application Profiler only helps to create the Flex configuration files that enable

user personalization, but it does not apply them to individual users4. It allows third-party user personalization of applications. This is also not a capability of Application Profiler, but rather of VMware Dynamic Environment Manager itself.

Application Profiler only works with applications that store their settings in the registry or file system, and does not support third-party user personalization solutions such as AppSense or RES. It allows creation of computer templates. This is

not a capability of Application Profiler at all. Computer templates are used to create virtual machines or physical computers with a predefined configuration, and are not related to application management or user personalization.

References:

Introduction to VMware Dynamic Environment Manager Application Profiler Editing a Profile Archive

Profile an Application

Introduction to VMware Dynamic Environment Manager [VMware Dynamic Environment Manager FAQ]

[Create a Computer Template]

QUESTION 3

Where are exclusions specified for Writable Volumes to prevent App Volumes from persisting specific data between sessions?

A. snapvol.cfg

B. config.ini

C. svservice.log

D. json.cfg

Correct Answer: A

Explanation: Writable Volumes are user-specific virtual disks that store user-installed applications, data, and settings. App Volumes is a real-time application delivery system that uses Writable Volumes to deliver applications that are not multiuser aware. However, sometimes it might be necessary to prevent App Volumes from persisting specific databetween sessions, such as temporary files, application updates, or registry keys. To do this, administrators can specify exclusions

for Writable Volumes in a policy file called snapvol.cfg.

The snapvol.cfg file is a text file that contains policy settings for App Volumes. These settings determine which files and registry keys are captured or excluded by App Volumes. The snapvol.cfg file can be customized by administrators to suit

different needs and scenarios. The snapvol.cfg file can be applied to both application packages and Writable Volumes.

To specify exclusions for Writable Volumes, administrators can use the following keywords in the snapvol.cfg file:

exclude_uwv_file: This keyword excludes a file or folder path from being persisted on a Writable Volume. For example, exclude_uwv_file=\Program Files (x86)\Notepad++ excludes the folder location of Notepad++ from being overwritten

during an update.

exclude_uwv_reg: This keyword excludes a registry key or value from being persisted on a Writable Volume. For example,

exclude_uwv_reg=\REGISTRY\MACHINE\SOFTWARE\Notepad++ excludes the registry location of Notepad++ from being overwritten during an update. The snapvol.cfg file must be uploaded to the Writable Volume by using the Update

Writable Volumes feature in App Volumes Manager. The exclusions will take effect after the user logs off and logs back in to the desktop.

The other options are not valid files for specifying exclusions for Writable Volumes:

config.ini: This file is used to configure the App Volumes agent settings, such as the App Volumes Manager address, the logging level, and the SSL certificate validation.

svservice.log: This file is used to record the App Volumes agent log messages, such as the agent status, the package attachment, and the error messages. json.cfg: This file does not exist in App Volumes. References: Writable Volume

Exclusions, Policy Files (snapvol.cfg) in App Volumes, and [VMware Horizon 8.x Professional Course]

QUESTION 4

While creating a new Instant Clone Desktop Pool, an administrator does not see a particular Windows 10 VM available or listed as an option for use as the golden image. Which step must the administrator perform, prior to creating this new desktop pool?

A. Validate the Golden Image with VMware Skyline Health.

B. Install VMware Dynamic Environment Manager Agent.

C. Take a Snapshot of the VM that is the golden image.

D. Configure Advanced parameters of VMware Tools for Horizon of this VM.

Correct Answer: C

Explanation: To create an instant-clone desktop pool, you must first create a golden image virtual machine and take a snapshot of it in a powered-down state. This snapshot provides the base image for the clones. You cannot create an instant-clone desktop pool from a VM template or a powered-on VM. Therefore, the administrator must take a snapshot of the VM that is the golden image before creating the new desktop pool. References: Create an Instant-Clone Desktop Pool and Instant Clone Desktop Pools

QUESTION 5

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

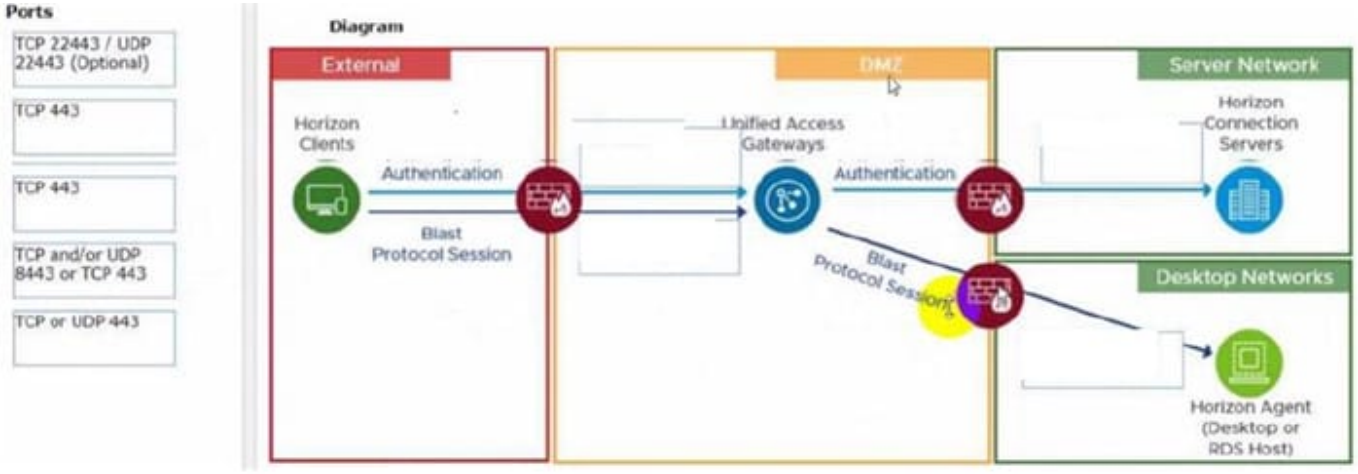
Explanation: The default URL used to access the Horizon Console is https:///admin, where is the fully qualified domain name of the Connection Server instance. This URL allows you to log in to Horizon Console by using a secure (TLS) connection. You can also use the IP address of the Connection Server 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 6

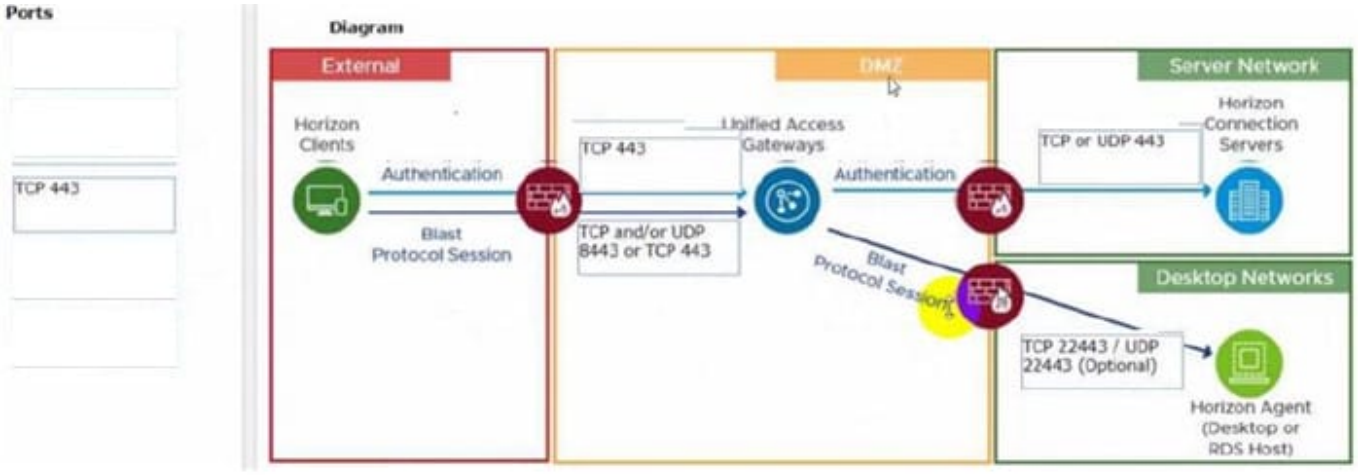
Refer to the exhibit.

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

Select and Place:



Correct Answer:



C:\Users\Waqas Shahid\Desktop\Mudassir\Untitled.jpg

QUESTION 7

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

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 installation1. 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 installation1. 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 profiled1. 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 events2. Management Console is the component that allows you to configure and manage the user environment settings2. 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 library1. References: VMware Dynamic Environment Manager Overview2 Using Application Profiler1

QUESTION 8

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

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 availability1. 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 desktops2. 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 Extreme3. 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 directly4. 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 session 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. References: 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 9

End-users are complaining that they are frequently being asked for credentials when opening additional apps. Which step should the administrator take to resolve the issue?

A. Configure SSO Timeout by modifying the Global Settings in Horizon Administrator.

B. Configure a time limit by modifying the Horizon GPO.

C. Configure Desktop Timeout by modifying the Pool Settings in Horizon Administrator.

D. Configure Session Timeout by modifying the Client Settings in Horizon Client.

Correct Answer: A

Explanation: Single sign-on (SSO) is a feature that allows users to log in to Horizon Client once and launch remote desktops and applications without being prompted for credentials again. SSO is enabled by default and can be configured in the Global Settings of Horizon Administrator. One of the settings is SSO Timeout, which determines how long the user\\'s credentials are cached before they expire. If the SSO Timeout is too short, users might be frequently asked for credentials when opening additional apps. To resolve this issue, the administrator can increase the SSO Timeout value or set it to -1, which means that no SSO timeout limit is set. References: Global Settings for Client Sessions in Horizon Console and [VMware Horizon 8.x Professional Course] https://docs.vmware.com/en/VMware-Horizon-7/7.13/horizon-console-administration/GUID- E2A7CA32-193D-43D9-B08E-DD20CAE9CA28.html

QUESTION 10

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

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. References: Understanding Permissions and Access Groups and [VMware Horizon 8.x Professional Course]