



Free Questions for *5V0-62.22* by *certsinside*

Shared by *Spencer* on *15-04-2024*

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A newly-hired administrator has opened a ticket with the Internal IT Helpdesk, stating that they can login but do not have access to the Scheduler settings located at Groups & Settings > All Settings > Admin > Scheduler A colleague performing the same role can see and access this entitlement.

What are two reasons that the newly-hired admin is having this difficulty? (Choose two.)

Options:

- A-** The newly-hired administrator needs to accept the EULA before sensitive configuration settings are visible by this account.
- B-** The newly-hired administrator has the correct roles assigned but has not selected the applicable role in the console access dropdown to view this configuration
- C-** The newly hired administrator did not enter in the restricted action pin to enter the Scheduler settings.
- D-** The newly-hired administrator needs to navigate to Accounts > Administrators > Roles and assign themselves the correct level of access to access the Scheduler setting.
- E-** The newly-hired administrator has the incorrect roles assigned or was not yet provided the correct roles to view this configuration.

Answer:

B, E

Explanation:

The reasons that the newly-hired admin is having this difficulty are that they have the correct roles assigned but have not selected the applicable role in the console access dropdown to view this configuration, and that they have the incorrect roles assigned or were not yet provided the correct roles to view this configuration. The console access dropdown allows the administrator to switch between different roles that they have been assigned in different OGs. If the administrator does not select the correct role for the Scheduler settings, they will not be able to see or access them. Moreover, if the administrator has not been assigned the correct role for the Scheduler settings, they will not be able to see or access them regardless of the console access dropdown selection. The administrator should check and select the appropriate role in the console access dropdown, and also verify and assign themselves the correct role for the Scheduler settings.

Question 2

Question Type: MultipleChoice

Some users report they are unable to enroll their Android and iOS devices using their user account from the organization's Microsoft Active Directory, which is not publicly accessible. The administrator needs to gather the log files for troubleshooting these issues with the organization's shared SaaS VMware Workspace ONE UEM tenant and Active Directory.

Which service does the organization's administrator have direct control over to enable verbose logging to troubleshoot this issue?

Options:

- A- The UAG (Unified Access Gateway) Edge service
- B- The AWCM (AirWatch Cloud Messaging) service
- C- The ACC (AirWatch Cloud Connector) service
- D- The DS (Device Services) service

Answer:

C

Explanation:

The service that the organization administrator has direct control over to enable verbose logging to troubleshoot this issue is ACC (AirWatch Cloud Connector) service. ACC is a service that integrates Workspace ONE UEM with internal enterprise systems, such as Active Directory or Certificate Authority. ACC enables Workspace ONE UEM to use internal resources without exposing them to the Internet. If some users are unable to enroll their devices using their Active Directory accounts, it could indicate that there is a problem with ACC configuration, connectivity, or synchronization. Enabling verbose logging for ACC can help identify and troubleshoot the root cause of the issue.

Question 3

Question Type: MultipleChoice

An organization administrator recently integrated their shared SaaS VMware Workspace ONE UEM and their internal Microsoft Active Directory

Most users report they can enroll their Android and iOS devices using their user account from the organization's internal Microsoft Active Directory, but a few users report they cannot. The organization administrator finds the user accounts of the users unable to enroll failed to synchronize to VMware Workspace ONE UEM.

What is the most likely cause of this issue?

Options:

- A- The organization administrator misconfigured the bind user credentials.
- B- The organization administrator misconfigured the Bind Authentication Type.
- C- The users that failed to synchronize have two or more globally unique identifiers.
- D- The users that failed to synchronize are missing a phone number in Active Directory.

Answer:

C

Explanation:

The most likely cause of this issue is that the users that failed to synchronize have two or more globally unique identifiers. The globally unique identifier (GUID) is a unique value that identifies each user account in Active Directory². If a user account has more than one GUID, it will cause a conflict when synchronizing with Workspace ONE UEM and prevent the user from enrolling their devices³. The administrator should check and resolve any duplicate GUIDs in Active Directory.

Question 4

Question Type: MultipleChoice

An administrator could not locate Hub Services settings page under an organization group and has asked why this problem is occurring. Which statement describes the root cause of this problem?'

Options:

- A-** This organization group is not a Customer type OG.
- B-** Unified Access Gateway has not been deployed for this OG.

C- AirWatch Cloud Connector has not been installed for this OG.

D- VMware Tunnel has not been configured under this OG.

Answer:

A

Explanation:

The root cause of this problem is that this organization group is not a Customer type OG. The Hub Services settings page is only available for Customer type OGs, which are the top-level OGs in the hierarchy¹. The Hub Services settings page allows the administrator to configure various features and services for the Intelligent Hub app, such as notifications, people, home, and catalog¹. The administrator should navigate to the Customer type OG to access the Hub Services settings page.

Question 5

Question Type: MultipleChoice

An administrator has been troubleshooting an issue where a single device is unable to check in to VMware Workspace ONE UEM and receive commands. All services are functioning, and this issue appears to be isolated to this specific device. Service logs have also been reviewed and do not show any instances of communication with the device in question.

Which troubleshooting step should be taken next to find the root cause, while not causing any data loss to the end user's device?

Options:

- A- Manually update the device record in the DB.
- B- Renew the Device Root Certificate.
- C- Use Device Wipe, and then re-enroll the device.
- D- Gather Device Side Logging.

Answer:

D

Explanation:

The troubleshooting step that should be taken next to find the root cause, while not causing any data loss to the end user's device, is to gather device side logging. Device side logging can help collect more detailed information about device events, actions, and errors for troubleshooting purposes. Device side logging can be enabled from the Workspace ONE UEM console or from the device itself. Device side logging does not affect the user's data or settings on the device.

Question 6

Question Type: MultipleChoice

An organization has successfully deployed native applications to VMware Workspace ONE managed Android, iOS, and Windows devices in the same OG.

The organization administrator just configured VMware Workspace ONE to provide all those same devices access to a SaaS application that was previously successfully integrated with the organization's VMware Workspace ONE Access tenant. Windows and Android users can access this SaaS application, but iOS device users report that they are unable to see this application in the VMware Workspace ONE Catalog.

What is the most likely cause of this issue?

Options:

- A- The Intelligent Hub Catalog integration was not completed for the OG.
- B- The application assignment via the OG was misconfigured.
- C- The organization's Apple sToken expired.
- D- The Intelligent Hub Catalog (iOS) setting was not enabled.

Answer:

D

Explanation:

The most likely cause of this issue is that the Intelligent Hub Catalog (iOS) setting was not enabled. This setting allows iOS devices to access SaaS applications from the Intelligent Hub app. If this setting is disabled, iOS devices will not be able to see or launch SaaS applications from the Intelligent Hub Catalog. The administrator should enable this setting in the Workspace ONE UEM console.

Question 7

Question Type: MultipleChoice

After deploying an iOS profile, there are several devices that are not showing successful installation. Upon reviewing the troubleshooting logs, the administrator notices that the device has responded with NotNow.

Which action should the administrator take to resolve this status?

Options:

A- Check the AWCM server logs to ensure that the device is connected to Cloud Messaging.

- B-** Send several push notifications to the device in order to allow processing of profiles
- C-** Contact the user, and ensure the iOS device is unlocked and powered on.
- D-** Re-push the profile to the device since the hang up is on the Workspace ONE UEM side

Answer:

C

Explanation:

The action that the administrator should take to resolve this status is to contact the user and ensure the iOS device is unlocked and powered on. The NotNow status means that the device has received the profile but has not installed it yet. This could be because the device is locked, powered off, or has a pending user action. The administrator should ask the user to unlock the device, power it on, and accept any prompts or notifications related to the profile installation.

Question 8

Question Type: MultipleChoice

Refer to the exhibit. The VMBeans company has created the following organization group (OG) structure:

VMBeans

Logistics

Midwest Warehouse

Sales

The senior VMware Workspace ONE UEM administrator has created these smart groups at different OG levels for lower level admin

Groups & Settings > Groups

Assignment Groups

Filters >>

[+ ADD SMART GROUP](#)

<input type="checkbox"/>	Groups	Managed By	Group Type
<input type="checkbox"/>	Logistics Team Central Office	Logistics	Smart Group
<input type="checkbox"/>	Midwest Rugged	Midwest Warehouse	Smart Group
<input type="checkbox"/>	Sales Android Device	Sales	Smart Group
<input type="checkbox"/>	Sales Laptop	Sales	Smart Group
<input type="checkbox"/>	VMBeans (VMBeans)	VMBeans	Organization Group
<input type="checkbox"/>	Logistics (VMBeans / Logistics)	Logistics	Organization Group
<input type="checkbox"/>	Midwest Warehouse (VMBeans / Log	Midwest Warehouse	Organization Group
<input type="checkbox"/>	Sales (VMBeans / Sales)	Sales	Organization Group

The administrator at the Logistics OG has the Console Administrator role. Which two smart groups could this administrator manage? (Choose two.)

Options:

- A- VMBeans (VMBeans)
- B- Logistics Team Central Office
- C- Midwest Rugged
- D- Sales Android Device
- E- Sales Laptop

Answer:

B, C

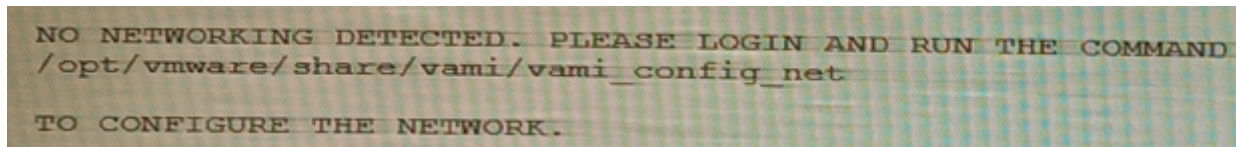
Explanation:

The administrator at the Logistics OG has the Console Administrator role, which means they can manage all the smart groups that are created in their own OG or below¹. Therefore, they can manage the Logistics Team Central Office and Midwest Rugged smart groups, which are both created in the Logistics OG. They cannot manage the VMBeans (VMBeans), Sales Android Device, and Sales Laptop smart groups, which are created in higher OGs.

Question 9

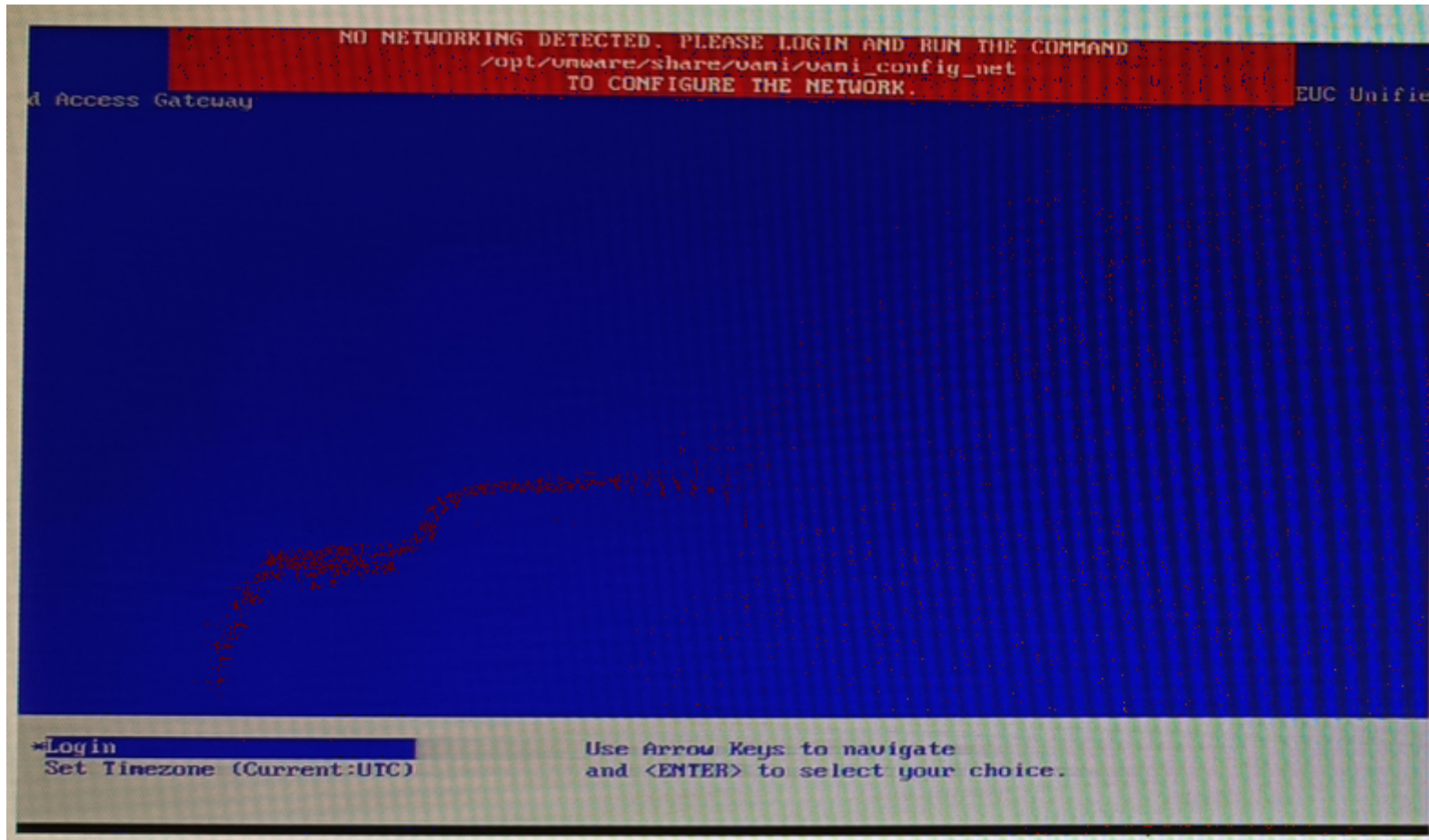
Question Type: MultipleChoice

Upon deploying a fresh Unified Access Gateway via the OVF template, the administrator sees the following:



```
NO NETWORKING DETECTED. PLEASE LOGIN AND RUN THE COMMAND  
/opt/vmware/share/vami/vami_config_net  
TO CONFIGURE THE NETWORK.
```

Refer to the exhibit.



The administrator would like to avoid running the VAMI command and reconfiguring the network. Which other option to remediate this error message is possible?

Options:

- A- Reboot the UAG, press F10, and in the setparams, enter `rw init=/bin/bash`.
- B- Login to the UAG with the root account, and manually modify the `l3config`.
- C- Redeploy the UAG to ensure that all of the guest property configurations have been configured correctly
- D- Power off the UAG, and reconfigure the quest properties to ensure that the information is correct.

Answer:

C

Explanation:

The other option to remediate this error message is to redeploy the UAG to ensure that all of the guest property configurations have been configured correctly. The error message indicates that there is a problem with the guest property settings of the UAG appliance, such as network configuration, edge service settings, or certificate settings⁵. Redeploying the UAG can help fix any errors or inconsistencies in the guest property settings.

To Get Premium Files for 5V0-62.22 Visit

<https://www.p2pexams.com/products/5v0-62.22>

For More Free Questions Visit

<https://www.p2pexams.com/vmware/pdf/5v0-62.22>

