Number: 5V0-62.22
Passing Score: 800
Time Limit: 120
File Version: 4.0

Exam Code: 5V0-62.22

Exam Name: VMware Workspace ONE 21.X UEM Troubleshooting Specialist

Exam A

QUESTION 1
Which three actions can be enabled for users to self-manage devices through the Self-Service Portal? (Choose three.)

A. Generate Targeted Log
B. Upload SMIME Certificate
C. Sync Device
D. Launch VMware Assist Session
E. Clear Administrator Passcode
F. Clear Passcode

Correct Answer: A, B, C
Section:
Explanation:
The three actions that can be enabled for users to self-manage devices through the Self-Service Portal are generate targeted log, upload SMIME certificate, and sync device. The Self-Service Portal is a web-based application that allows users to perform various actions on their enrolled devices, such as lock, unlock, wipe, or unenroll. Users can also generate targeted log to collect device logs for troubleshooting purposes, upload SMIME certificate to enable secure email communication, and sync device to update device information and settings in the Workspace ONE UEM console.

QUESTION 2
An Active Directory administrator added a number of new user accounts to a group that is synced in VMware Workspace ONE UEM, but after several days, the new directory accounts have not synchronized into the VMware Workspace ONE UEM console.
After checking the Directory Services configuration in the VMware Workspace ONE UEM console, the administrator confirmed Auto Sync and Auto Merge are enabled for the group Which two log files would be used to troubleshoot issues related to this Directory synchronizations? (Choose two.)

A. DirectorySyncServiceLogFile.log
B. WebLogFile.log
C. CloudConnector.log
D. AWServices log
E. DeviceServicesLog. log

Correct Answer: A, C
Section:
Explanation:
The two log files that would be used to troubleshoot issues related to this Directory synchronizations are DirectorySyncServiceLogFile.log and CloudConnector.log. DirectorySyncServiceLogFile.log is a log file that records the directory synchronization process between Workspace ONE UEM and Active Directory or LDAP. CloudConnector.log is a log file that records the communication and synchronization between Workspace ONE UEM and ACC (AirWatch Cloud Connector), which is a service that integrates Workspace ONE UEM with internal enterprise systems, such as Active Directory or Certificate Authority. These log files can help identify and troubleshoot any errors or issues related to directory synchronization.

QUESTION 3
An administrator has assigned a purchased application to a new group of EP devices and enabled device-based-licensing. However none of the assigned devices could install the application
Which statement describes the possible cause of this problem?

A. VPP invites are not accepted
B. Devices do not have Workspace ONE Hub installed

C. App Store is hidden.
D. VPP sToken has expired.

Correct Answer: D
Section:
Explanation:
The possible cause of this problem is that VPP sToken has expired. VPP (Volume Purchase Program) sToken is a token that allows Workspace ONE UEM to communicate with Apple's VPP service and manage purchased applications for iOS devices. If the VPP sToken expires or becomes invalid, Workspace ONE UEM will not be able to assign or distribute purchased applications to devices. The administrator should check and renew the VPP sToken if needed.

QUESTION 4
Which option is available for Unified Access Gateway to export a collection of all logs?

A. Use the UAG-log-archive.zip download button within the VMware Workspace ONE Access Admin UI.
B. Export the UAG-log-archive.zip from the VMware Workspace ONE UEM console troubleshooting page.
C. Use the UAG-log-archive zip download button from the Support Settings section in the UAG Admin UI.
D. Export the UAG-log-archive.zip from the logging option in the OVF template

Correct Answer: C
Section:
Explanation:
The option that is available for Unified Access Gateway to export a collection of all logs is using the UAG-log-archive.zip download button from the Support Settings section in the UAG Admin UI.This ZIP file contains all logs from the Unified Access Gateway appliance, such as system information, network configuration, edge service logs, and so on4. This option can help troubleshoot any issues or errors related to Unified Access Gateway deployment and operation.

QUESTION 5
Which VMware Workspace ONE UEM console configuration page would be

A. Groups & Settings > All Settings > Admin > Diagnostics > Logging
B. Groups & Settings > All Settings > Storage > Logging
C. Groups & Settings > All Settings > Troubleshooting > Logging
D. Groups & Settings > All Settings > System > Logging

Correct Answer: A
Section:
Explanation:
The VMware Workspace ONE UEM console configuration page that would be used to enable debug logging for a specific device is Groups & Settings > All Settings > Admin > Diagnostics > Logging5.This page allows administrators to enable debug logging for a specific device or a group of devices based on various criteria, such as platform, model, ownership, and so on5. Debug logging can help collect more detailed information about device events, actions, and errors for troubleshooting purposes.

QUESTION 6
Which feature is included in VMware Workspace ONE Assist in Attended Mode?

A. View and export detailed device information, access activity logs, run commands, and manage files
B. Restrict employees' ability to pause or end a remote session for enhanced privacy.
C. Remotely connect to any unenrolled or enrolled device in seconds, directly from the VMware Workspace ONE console
D. Restrict additional users to a remote session to assist with issues.

Correct Answer: A
Section:
Explanation:
The feature that is included in VMware Workspace ONE Assist in Attended Mode is view and export detailed device information, access activity logs, run commands, and manage files. This feature allows the administrator to remotely access the device screen and perform various actions to troubleshoot issues or assist the user. The administrator can also view the device details, such as battery level, network status, memory usage, and so on.The administrator can also access the device logs, run commands such as ping or traceroute, and manage the device files1.

QUESTION 7
The SSL certificates for on-premises VMware Workspace ONE UEM recently expired and were rotated Soon after. Android devices entirely stopped receiving push notifications and many reported AWCM as being disconnected. It was confirmed that the SSL certificates held been rotated on IIS as well as the load balancer.
Which strategy accurately describes the solution for this problem?

A. The SSL certificates were not updated on all device services servers, so updating the remaining servers would resolve the issue.
B. The Device Services service was not restarted after the SSL certificate rotation on IIS. so restarting the service would resolve the issue.
C. The Device Management binding was not updated for SSL handshake compatibility, so selecting the correct binding would resolve the issue.
D. The AWCM keystore was missed for rotation of SSL certificates, so running the keytool import targeting the new certificate would resolve the issue

Correct Answer: D
Section:
Explanation:
The strategy that accurately describes the solution for this problem is running the keytool import targeting the new certificate. The AWCM keystore is a Java keystore file that contains the SSL certificates used by AWCM to establish secure connections with devices and other components. If the SSL certificates are rotated on IIS and the load balancer, but not on the AWCM keystore, then AWCM will not be able to communicate with devices using push notifications.To resolve this issue, the administrator must import the new SSL certificates into the AWCM keystore using the keytool command2.

QUESTION 8
A number of enrolled devices have not checked in with VMware Workspace ONE UEM for several days. When the administrator attempted to push a profile to the devices the devices did not check in to receive the profile.
Which component should be focused on when troubleshooting this device connectivity issue to VMware Workspace ONE UEM?

A. UEM Console
B. UAG
C. API
D. Device Services

Correct Answer: D
Section:
Explanation:
The component that should be focused on when troubleshooting this device connectivity issue to VMware Workspace ONE UEM is Device Services. Device Services is a component of Workspace ONE UEM that handles device enrollment, management, and communication. Device Services also hosts the AWCM service, which is responsible for delivering push notifications to devices.If Device Services is not working properly, devices may not be able to check in with Workspace ONE UEM or receive profiles, commands, or policies3.

QUESTION 9
When an organization administrator attempts to configure a shared SaaS Workspace ONE UEM environment to use their internal Active Directory Certificate Authority, 'Test Connection' fails.
For which service should the organization administrator enable verbose logging to resolve this issued?

A. ACC (AirWatch Cloud Connector) service
B. AWCM (AirWatch Cloud Messaging) service
C. UAG (Unified Access Gateway) Tunnel service
D. Console service

Correct Answer: A
Section:
Explanation:
The service that the organization administrator should enable verbose logging to resolve 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 ''Test Connection'' fails when configuring a shared SaaS Workspace ONE UEM environment to use an internal Active Directory Certificate Authority, 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 issue4.

QUESTION 10
A dozen users just reported various issues with VMware Workspace ONE UFM managed applications on their Android and iOS devices The administrator would like to use VMware Workspace ONE to simultaneously gather detailed troubleshooting information about all these devices with one action
Which form of logging should be used to accomplish this goal?

A. Settings-based targeted logging
B. ACC (AirWatch Cloud Connector) verbose logging
C. Device-based targeted logging
D. AWCM (AirWatch Cloud Messaging) verbose logging

Correct Answer: C
Section:
Explanation:
The form of logging that should be used to accomplish this goal is device-based targeted logging.Device-based targeted logging allows the administrator to enable debug logging for multiple devices at once, based on various criteria, such as platform, model, ownership, and so on1. Device-based targeted logging can help collect more detailed information about device events, actions, and errors for troubleshooting purposes.

QUESTION 11
After introducing an additional AWCM server (for a total of two), enrollments have periodically started to fail. While testing, the administrator notices that when https//awcm.awmdm com;2001/awcm/statistics?awcmsessionid---12345 is accessed, the user is consistently bounced between both AWCM nodes
Which misconfiguration would be causing this behavior?

A. AWCM offloading is not property configured.
B. AWCM Persistence is not correctly configured.
C. WCM secure channel certificate is not installed.
D. AWCM ports are not opened to the new AWCM server.

Correct Answer: B
Section:
Explanation:
The misconfiguration that would be causing this behavior is AWCM Persistence is not correctly configured. AWCM Persistence is a setting that ensures that devices maintain a consistent connection with the same AWCM server in a load-balanced environment. If AWCM Persistence is not correctly configured, devices may be bounced between different AWCM servers and cause enrollment failures or communication errors. The administrator should check and configure AWCM Persistence properly.

QUESTION 12
Where should the logging level for AirWatch Cloud Connector be changed?

A. In the CloudConnector.exe.config file
B. At the Workspace ONE Access Connector settings page
C. In the Cloud ConnectorHub.exe.config file
D. At the UEM console Cloud Connector settings page

Correct Answer: A
Section:
Explanation:
The logging level for AirWatch Cloud Connector should be changed in the CloudConnector.exe.config file. This file contains various settings for ACC (AirWatch Cloud Connector), such as logging level, proxy settings, service URLs, and so on. The administrator can edit this file to change the logging level for ACC from default to verbose or debug, which can provide more detailed information for troubleshooting purposes.

QUESTION 13
Which VMware Tunnel utility can help troubleshooting by gathering all the necessary component log files that may be required during the process?

A. tunnel_snap
B. tunnel_vi
C. tunnela_udrt
D. tunnel_nano

Correct Answer: A
Section:
Explanation:
The tunnel_snap utility can help troubleshooting by gathering all the necessary component log files that may be required during the process.This utility is available on both Linux and Windows versions of VMware Tunnel1.
The tunnel_snap utility collects logs from the following components:
VMware Tunnel service
Per-App Tunnel service
Proxy service
Content Gateway service
VMware Tunnel configuration files
System information
Network information The other options are not valid utilities for VMware Tunnel.

QUESTION 14
An organization has successfully used VMware Workspace ONE UEM to deploy a managed, public application to Android, iOS, and Windows devices in the same OG for the last year.
The Windows and Android users can still install this application The iOS device users, however, report that they can see and install other applications in the VMware Workspace ONE Catalog, but suddenly they are unable to see this application in the VMware Workspace ONE Catalog.
What is the most likely cause of this issue?

A. The application assignment via a smart group was misconfigured.
B. The application assignment via the enrollment type was misconfigured.
C. The organization's Apple Push Notification certificate expired.
D. The organization's Apple sToken expired.

Correct Answer: C
Section:
Explanation:
The most likely cause of this issue is that the organization's Apple Push Notification certificate expired.The Apple Push Notification certificate is required for iOS devices to communicate with Workspace ONE UEM and receive commands, profiles, and applications2. If the certificate expires, the iOS devices will not be able to receive any updates from Workspace ONE UEM, including the application catalog.The organization should renew the certificate as soon as possible to restore the functionality of the iOS devices3. The other options are not likely causes of this issue because:
A misconfigured application assignment via a smart group would affect all devices in the smart group, not just iOS devices.
A misconfigured application assignment via the enrollment type would affect all devices with the same enrollment type, not just iOS devices.
An expired Apple sToken would prevent the organization from purchasing or distributing new applications from Apple Business Manager or Apple School Manager, but it would not affect the existing applications in the Workspace ONE Catalog.

QUESTION 15
An organization wants to use the VMware Tunnel edge service of VMware Workspace ONE UAG (Unified Access Gateway) to allow an application on managed Android, iOS. and Windows devices to access server resources on their internal network.
An organization administrator deployed UAG and configured the VMware Tunnel edge service, but in the UEM console, 'Test Connection' with VMware Tunnel fails What is the most likely cause of this issue'?

A. The Device Traffic Rules are configured incorrectly in the Unified Access Gateway system
B. The Device Traffic Rules are incorrect in UEM.
C. The Unified Access Gateway is unable to communicate with UEM.
D. The VPN payload in a device profile is configured incorrectly in UEM.

Correct Answer: D
Section:
Explanation:
The most likely cause of this issue is that the VPN payload in a device profile is configured incorrectly in UEM. The VPN payload defines how devices connect to the VMware Tunnel edge service and access internal resources. If the VPN payload is incorrect, the devices will not be able to establish a VPN connection with the VMware Tunnel edge service and ''Test Connection'' with VMware Tunnel will fail. The organization should review and correct the VPN payload settings in UEM. The other options are not likely causes of this issue because:
The Device Traffic Rules are configured in UEM, not in Unified Access Gateway. They define which applications or domains are allowed or blocked by the VMware Tunnel edge service.
If the Device Traffic Rules are incorrect in UEM, they would affect all devices that connect to the VMware Tunnel edge service, not just ''Test Connection'' with VMware Tunnel.
If the Unified Access Gateway is unable to communicate with UEM, it would affect all edge services that require UEM integration, such as Content Gateway and Horizon, not just VMware Tunnel.

QUESTION 16
An administrator has started to integrate Workspace ONE UEM with test connection and is unable to move forward.
Which situation could cause this test connection failure?

A. The provided Workspace ONE Access Username is incorrect
B. The provided Workspace ONE UEM API key is incorrect
C. The provided Workspace ONE UEM Username is incorrect.
D. The provided Workspace ONE Access API key is incorrect.

Correct Answer: D
Section:
Explanation:
The most likely cause of this test connection failure is that the provided Workspace ONE Access API key is incorrect. The Workspace ONE Access API key is required to establish a secure connection between Workspace ONE UEM and Workspace ONE Access services. If the API key is incorrect, the test connection will fail and the integration will not work.The administrator should verify and correct the API key in the Workspace ONE UEM console1.

QUESTION 17
The following error is seen on the AirWatch Cloud Connector (ACC) logging:

```
ErrorSystem.Type.TestConnectionDirectory call failed. System.DirectoryServices.Protocols.LdapException: Error code:81 User
Name:CustomerAdministrator Error Details:Server is not reachable*** EXCEPTION ***
System.DirectoryServices.Protocols.LdapException: The LDAP server is unavailable.
```

Which connectivity should be investigated to restore ACC functionality?

A. From ACC to AWCM
B. From the Active Directory Server to the ACC
C. From AWCM to the Active Directory Server
D. From the ACC to the Active Directory server

Correct Answer: D

Section:
Explanation:
The connectivity that should be investigated to restore ACC functionality is from the ACC to the Active Directory server. The error message in the ACC logging indicates that the ACC cannot connect to the Active Directory server due to a network error. This could be caused by firewall settings, proxy settings, network configuration, or other factors that prevent the ACC from communicating with the Active Directory server.The administrator should check and resolve these issues to restore the ACC functionality2.

QUESTION 18
An administrator is unable to enroll Android devices with directory accounts but successfully enrolled the device with a basic working previously.
Which logs should the administrator review to begin troubleshooting the Android directory account enrollment issue?

A. VMware Tunnel
B. VMware Workspace ONE Intelligent Android Hub
C. AirWatch Cloud Connector
D. Unified Access Gateway

Correct Answer: C
Section:
Explanation:
According to the Device enrollment issues with Workspace ONE article3, one of the possible causes of enrollment failure is that the ACC service is not working properly or cannot communicate with the directory service. The administrator can review the ACC logs and test the connection to verify if there are any errors or issues with the ACC service or configuration.
The logs that the administrator should review to begin troubleshooting the Android directory account enrollment issue are AirWatch Cloud Connector (ACC) logs. The ACC is responsible for integrating Workspace ONE UEM with directory services such as Active Directory or LDAP. If the administrator is unable to enroll Android devices with directory accounts, it could indicate that there is a problem with the ACC configuration, connectivity, or synchronization.The administrator should review the ACC logs to identify and troubleshoot the root cause of the issue3.

QUESTION 19
A company uses Secure Email Gateway to provide email access to its mobile devices and uses Exchange 20VT6 as its email infrastructure.
Today the VMware Workspace ONE UEM administrator received a report that all newly enrolled devices (iOS and Android) were unable to receive email After speaking with some end users, the administrator found previously enrolled devices were still able to receive email on their mobile devices. The users who reported this issue are able to access their email through Outlook Web Access (OWA) on their computers.
Which statement describes the possible root cause of this issue?

A. The Secure Email Gateway server is unable to connect to the Exchange server.
B. The Exchange 2016 client access server cluster sporadically refuses to connect (HTTP 500)
C. There is an email compliance policy restricting email access to only Android devices.
D. The Secure Email Gateway is unable to update policy with VMware Workspace ONE UEM API

Correct Answer: A
Section:
Explanation:
The possible root cause of this issue is that the Secure Email Gateway server is unable to connect to the Exchange server. This could be due to network issues, firewall settings, or authentication problems. If the Secure Email Gateway server cannot communicate with the Exchange server, it will not be able to deliver email to the newly enrolled devices. The previously enrolled devices may still be able to receive email because they have cached credentials or sessions with the Exchange server. The users who reported this issue are able to access their email through OWA on their computers because OWA does not rely on the Secure Email Gateway server.

QUESTION 20
An organization has introduced a complex password requirement on enrolled mobile devices. This has also caused a significant increase in the help desk's ticket load around password resets for mobile devices. The organization needs to curb these requests and allow users, once authenticated, to resolve their own device passcode issues
Which service can help meet this goal?

A. Device Management Console

B. Self-Service Portal
C. SQLCMD
D. AWCM

Correct Answer: B
Section:
Explanation:
The service that can help meet this goal is the Self-Service Portal.The Self-Service Portal is a web-based application that allows users to perform various actions on their enrolled devices, such as lock, unlock, wipe, or unenroll1.Users can also reset their device passcode through the Self-Service Portal, which can reduce the number of help desk tickets and improve user satisfaction2.

QUESTION 21
A VMware Workspace ONE administrator is managing a fleet of console
Which step would assist in troubleshooting this problem?

A. Network traffic tools to capture Android traffic
B. xCode to extract the device debug log
C. Android SDK and do a tcpdump
D. Workspace ONE UEM Console Request Debug Log

Correct Answer: A
Section:
Explanation:
The step that would assist in troubleshooting this problem is using network traffic tools to capture Android traffic.Network traffic tools, such as Wireshark or Fiddler, can capture and analyze the network packets sent and received by the Android devices3. This can help identify any errors, delays, or anomalies in the communication between the devices and the console. Network traffic tools can also show the HTTP headers and body of the requests and responses, which can provide more information about the device status and configuration.

QUESTION 22
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?

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.

Correct Answer: D
Section:
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 app3. 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 23
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?

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.

Correct Answer: D
Section:
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 24
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'-'

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.

Correct Answer: A
Section:
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 25
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 find 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?

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

Correct Answer: C
Section:
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 26
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?

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

Correct Answer: C
Section:
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 27
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.)

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.

Correct Answer: B, E
Section:
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 28
An organization administrator configures VMware Workspace ONE UEM to deploy a new internal Win32 application to Windows devices, which are all located in the same OG (organization group). Users of newer Windows devices with increased hardware capacities can install this application, but older Windows devices with lower capacities are unable to complete the installation.
What is the most likely cause of this issue?

A. The VMware Workspace ONE administrator set 'RAM Required' for the application in the 'Details' tab options.
B. The organization's Windows Azure AD credentials in their Microsoft Store for Business expired.
C. The assignment of the internal application via the common OG (organization group) is misconfigured
D. The VMware Workspace ONE administrator set 'Admin Privileges' for the application in the 'Details' tab options

Correct Answer: A
Section:
Explanation:

The most likely cause of this issue is that the VMware Workspace ONE administrator set ''RAM Required'' for the application in the ''Details'' tab options. The ''RAM Required'' option specifies the minimum amount of RAM needed for the application to run on Windows devices. If some devices do not meet this requirement, they will not be able to complete the installation of the application. The administrator should check and adjust the ''RAM Required'' option for the application according to the device capabilities.

QUESTION 29
An administrator has mistakenly selected the prevent re-enrollment option when enterprise wiping a device that was intended to be re-enrolled. The administrator needs to remove this block and ensure that users are successful when they re-attempt enrollment
Which console page should be used to meet these goals?

A. Devices > Lifecycle > Enrollment Status
B. Monitor > Events > Device Events
C. Devices > Wipe Log
D. Resources > Device Updates

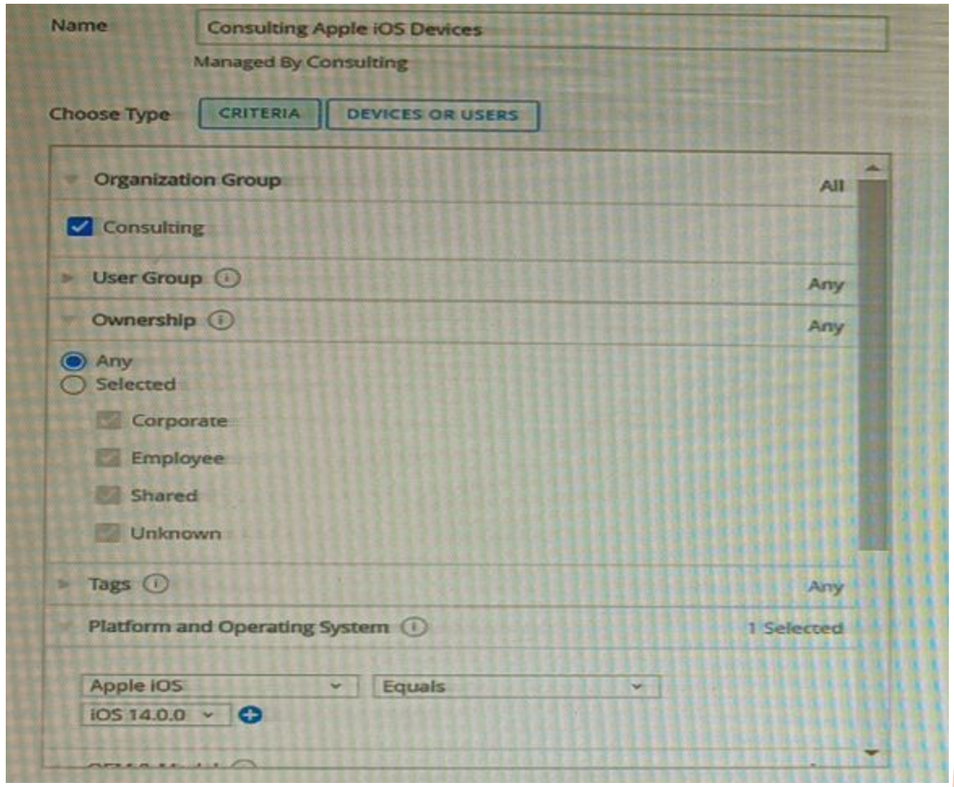
Correct Answer: A
Section:
Explanation:
The console page that should be used to meet these goals is Devices > Lifecycle > Enrollment Status.This page allows the administrator to view and manage the enrollment status of devices, such as blocked, unenrolled, or pending1. The administrator can also remove the block on a device that was enterprise wiped with the prevent re-enrollment option, and allow the user to re-enroll the device.

QUESTION 30
An organization wants to use the VMware Tunnel edge service of VMware Workspace ONF UAG (Unified Access Gateway) to allow an application on managed Android iOS and Windows devices to access server resources on their internal network.
An organization administrator configured the VMware Tunnel edge service on UAG and successfully completed the 'Test Connection' in the UEM console. Windows and iOS device users can access server resources on the organization's internal network, but Android device users report that they are getting a 'connection failed' error in the application.
What is the most likely cause of this issue?

A. The Android application assignment is incorrectly set to 'Managed' in UEM.
B. The time is incorrect on the organization's Unified Access Gateway systems
C. The VPN payload in the Android device profile is configured incorrectly in UEM
D. The certificate expired on the organization's Unified Access Gateway systems

Correct Answer: C
Section:
Explanation:
The most likely cause of this issue is that the VPN payload in the Android device profile is configured incorrectly in UEM. The VPN payload defines how devices connect to the VMware Tunnel edge service and access internal resources. If the VPN payload is incorrect, the devices will not be able to establish a VPN connection with the VMware Tunnel edge service and access server resources on the organization's internal network. The administrator should review and correct the VPN payload settings in UEM.

QUESTION 31
Refer to the exhibit. Consider this assignment group:



A company created a new assignment group tor its Consulting department and deployed Salesforce application to that group. After two days, only a small number of consultants have confirmed that they have received the application. Under the Consulting organization group, the VMware Workspace ONE UEM administrator can see 109 enrolled iOS devices, but under the Salesforce application installation status, it shows the application is only assigned to nine devices. Which statement describes the 100 iOS devices that are unable to see the application assignment?

A. They are not enrolled.
B. They are not corporate-owned devices.
C. They are not on iOS 14.0.0.
D. They are on iOS 14.0 0.

Correct Answer: C
Section:
Explanation:
The 100 iOS devices that are unable to see the application assignment are not on iOS 14.0.0.The assignment group is filtered by platform and operating system, and only includes devices that are on Apple iOS and iOS 14.0.02. If some devices are on a different iOS version, they will not be included in the assignment group and will not receive the application.

QUESTION 32
An VMware Workspace ONE administrator is using device-based commands to manage Android mobile devices, but the devices stopped receiving the UEM Commands from the Workspace ONE UEM Console (e.g. 'Lock Device')
Why is this problem occurring?

A. The VMware AirWatch Cloud Connector (ACC) stopped communicating with Workspace ONE UAG.
B. The Workspace ONE UEM Console stopped communicating with Workspace ONE Access.
C. The Workspace ONE UEM Console stopped communicating with VMware AirWatch Cloud Messaging (AWCM)
D. The VMware AirWatch Cloud Connector (ACC) stopped communicating with VMware AirWatch Cloud Messaging (AWCM).

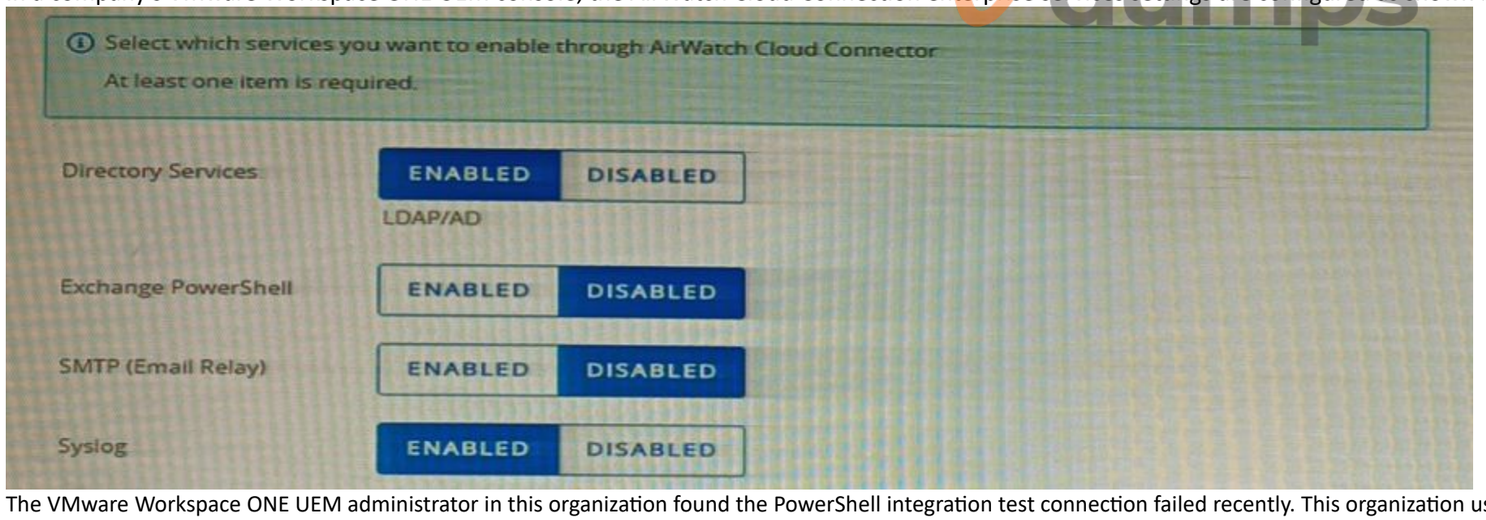
Correct Answer: C
Section:
Explanation:
The reason that this problem is occurring is that the Workspace ONE UEM Console stopped communicating with VMware AirWatch Cloud Messaging (AWCM).AWCM is a service that delivers push notifications to devices and enables device-based commands from the Workspace ONE UEM Console3. If the Workspace ONE UEM Console cannot communicate with AWCM, it will not be able to send commands to devices, such as ''Lock Device''. The administrator should check and resolve any issues with AWCM connectivity.

QUESTION 33
A VMware Workspace ONE UEM administrator is troubleshooting an internal application installation that affects one Android device. Which two pieces of information will help the administrator with this task? (Choose two)

A. Internal application APK file
B. Android OS version
C. Verbosed Web Console log
D. Workspace ONE Intelligent Hub log
E. Console server IIS log

Correct Answer: A, B
Section:
Explanation:
The two pieces of information that will help the administrator with this task are internal application APK file and Android OS version. The internal application APK file is the installation file for Android applications. The administrator can check if the file is corrupted, compatible, or configured correctly for the device. The Android OS version is the operating system version of the device. The administrator can check if the device meets the minimum requirements for the application or if there are any known issues or bugs with the OS version.

QUESTION 34
In a company's VMware Workspace ONE UEM console, the AirWatch Cloud Connection enterprise services settings are configured as shown below Refer to the exhibit.



The VMware Workspace ONE UEM administrator in this organization found the PowerShell integration test connection failed recently. This organization uses Office 365 as their email infrastructure.
Which statement accurately describes this situation?

A. The PowerShell integration test connection failure is related to the PowerShell request originating from the AirWatch Cloud Connector
B. The PowerShell integration test connection failure is related to the PowerShell request originating from the Console Server.
C. Only one enterprise services can be enabled to pass through AirWatch Cloud Connector.
D. PowerShell integration test connection failure is caused by SMTP (Email Relay) disabled status.

Correct Answer: B
Section:
Explanation:
The PowerShell integration test connection failure is related to the PowerShell request originating from the Console Server.The Console Server is the component of Workspace ONE UEM that communicates with the Exchange server via PowerShell to perform email management tasks, such as quarantine, wipe, or block1. If the Console Server cannot connect to the Exchange server, the PowerShell integration test connection will fail. The administrator should check and resolve any issues with the Console Server connectivity.

QUESTION 35
New information security requirements were put in place where remote access of any device must have a user present, and the user must consent to many of the remote actions Which VMware Workspace ONE Assist Agent mode will meet this requirement?

A. Unattended
B. COPE
C. User Secure
D. Attended

Correct Answer: D
Section:
Explanation:
The VMware Workspace ONE Assist Agent mode that will meet this requirement is Attended Mode. Attended Mode is a mode that requires user consent and presence for remote sessions.The user can see and control the remote session, and can also pause or end it at any time for enhanced privacy2.Attended Mode also allows the user to approve or deny many of the remote actions, such as file transfer, command execution, or device information access2.

QUESTION 36
After adding additional server traffic rules for runnel to proxy certain URLs, the sites/apps are still being proxied incorrectly. After a few hours, the configuration finally updates to the correct configuration. The administrator decides to review the communication path to ensure that UAGs can receive the most recent configuration updates.
Which communication path should be reviewed?

A. Apl outbound to UAG
B. UAG outbound to AWCM
C. AWCM outbound to UAG
D. UAG outbound to AP

Correct Answer: C
Section:
Explanation:
The communication path that should be reviewed is AWCM outbound to UAG.AWCM (AirWatch Cloud Messaging) is a service that delivers push notifications to devices and enables device-based commands from the Workspace ONE UEM Console3. AWCM also communicates with UAG (Unified Access Gateway) to send server traffic rules for tunnel to proxy certain URLs. If AWCM cannot communicate with UAG, the server traffic rules will not be updated on UAG and the sites/apps will be proxied incorrectly. The administrator should check and resolve any issues with AWCM outbound to UAG communication.

QUESTION 37
An administrator is getting reports that the profile status on multiple devices is not updating and need view the log which provides information about profile samples from the device. Which log should be viewed?

A. On the Console Server. \Logs\Services\Devicequeue.log
B. On the Console Server \Logs\Services\QueuingService.log
C. On the Device Services Server \Logs\Services\InterrogatorQueueService log
D. On the Device Services Server \Logs\Services\Queuemanager_log

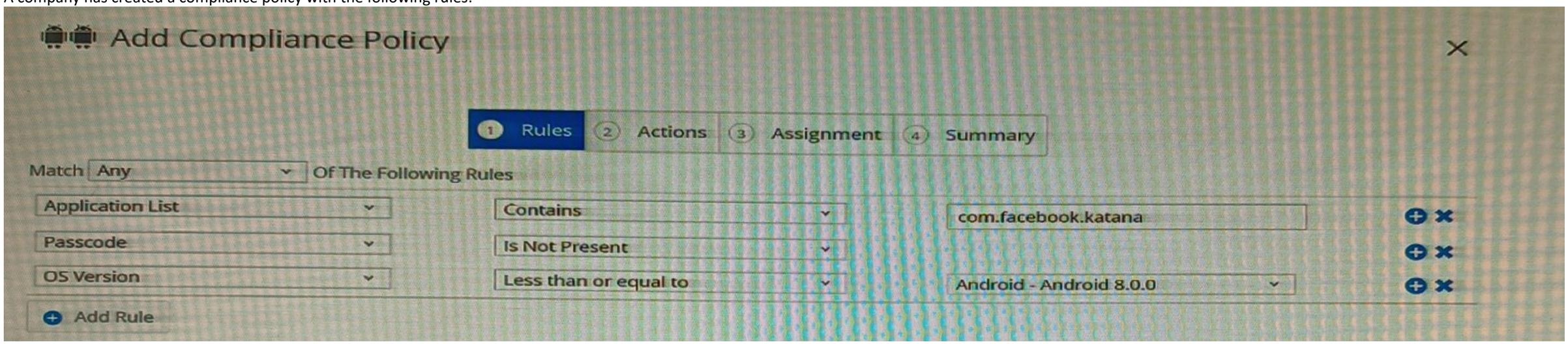
Correct Answer: C
Section:
Explanation:
The log file that should be viewed is On the Device Services Server \Logs\Services\InterrogatorQueueService.log. InterrogatorQueueService.log is a log file that records the profile samples from devices and updates them in the Workspace ONE UEM console. Profile samples are data that show the status and details of profiles installed on devices. If profile status on multiple devices is not updating, it could indicate that there is a problem with InterrogatorQueueService configuration, connectivity, or performance. The administrator should view and analyze the InterrogatorQueueService.log file to identify and troubleshoot the issue.

QUESTION 38
The VMware Workspace ONE UEM administrator in an organization found that the Certificate Authority integration test connection failed recently I his organization uses on-premises Microsoft ADCS CA as their certificate authority, which resides on an internal-only Windows server. The VMware Workspace ONE UEM console resides in the cloud.
Why did this certificate authority integration test connection fail?

A. Entrust PKI is disabled under the Certificate Authorities settings.
B. Symantec MPKI is disabled under the Certificate Authorities settings.
C. Fetching the root certificate from CA failed.
D. Credential in UEM is incorrect.

Correct Answer: C
Section:
Explanation:
The reason that this certificate authority integration test connection failed is that fetching the root certificate from CA failed. The root certificate from CA is a certificate that validates the identity and trustworthiness of the certificate authority (CA) that issues certificates for devices. Workspace ONE UEM needs to fetch the root certificate from CA to verify and manage certificates for devices. If fetching the root certificate from CA failed, it could indicate that there is a problem with CA configuration, connectivity, or availability. Workspace ONE UEM will not be able to connect to CA or issue certificates for devices, and the certificate authority integration test connection will fail.

QUESTION 39
Refer to the exhibit.
A company has created a compliance policy with the following rules:



Recently, the Android device was marked as non-compliant. The VMware Workspace ONE UGM administrator found that the Facebook application was installed on the device and that a passcode was not present. However, after the user removed the Facebook app and created a device passcode, the Android device still shows as non-compliant in the VMware Workspace ONE UEM console. Other devices within this organization all show as compliant.
Which two root causes could possibly cause this problem? (Choose two.)

A. The device has not checked in with the Workspace ONE UEM tenant.

B. The Policy Engine Service is not running
C. The Interrogator Queue Service is not running.
D. The Android device operating system version is lower than 8.0.0
E. The device is not enrolled into Workspace ONE UEM.

Correct Answer: A, B
Section:
Explanation:
The two root causes that could possibly cause this problem are that the device has not checked in with the Workspace ONE UEM tenant, and that the Policy Engine Service is not running.The device check-in is a process that updates the device status and information in the Workspace ONE UEM console3. If the device has not checked in with the Workspace ONE UEM tenant, it will not receive the latest compliance policy or report its compliance status. The Policy Engine Service is a service that evaluates and enforces compliance policies on devices. If the Policy Engine Service is not running, it will not be able to detect or remediate non-compliant devices. The administrator should check and resolve any issues with device check-in and Policy Engine Service.

QUESTION 40
An organization administrator started utilizing VMware Workspace ONE UEM to configure emails clients on managed Android, OS, and Windows devices. Windows and Android users can access their email inboxes. iOS device users are able to check in, but their email inbox fails to load:
What is the most likely cause of this issue?

A. The organization's Apple sToken expired.
B. The profile that configures the email client is misconfigured.
C. The organization group that assigns the email client is misconfigured.
D. The organization's Apple Push Notification certificate expired.

Correct Answer: D
Section:
Explanation:
The organization's Apple Push Notification certificate expired. The Apple Push Notification certificate is a certificate that allows Workspace ONE UEM to communicate with iOS devices using push notifications. Push notifications are required for iOS devices to check in and receive email configuration profiles from Workspace ONE UEM. If the Apple Push Notification certificate expires or becomes invalid, iOS devices will not be able to check in or receive email configuration profiles, and their email inbox will fail to load. The administrator should check and renew the Apple Push Notification certificate if needed.