



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

Shared by *Bates* on *12-12-2023*

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

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

Options:

- 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

Answer:

A

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 2

Question Type: MultipleChoice

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?

Options:

- A- AWCM offloading is not properly 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.

Answer:

B

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 3

Question Type: MultipleChoice

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?

Options:

- 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.

Answer:

D

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

Question Type: MultipleChoice

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 synchronization? (Choose two.)

Options:

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

Answer:

A, C

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 5

Question Type: MultipleChoice

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

Options:

- A- Generate Targeted Log
- B- Upload SMIME Certificate
- C- Sync Device
- D- Launch VMware Assist Session

E- Clear Administrator Passcode

F- Clear Passcode

Answer:

A, B, C

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 6

Question Type: MultipleChoice

Devices were originally configured to move to associated OGs based on their AD group membership. Recently, this process has stopped working, and the organization suspects a configuration was enabled by mistake, and the error is now preventing this process from

executing:

Which console page would confirm a potential configuration change?

Options:

- A- Monitor > Reports & Analytics > Events > Console Events
- B- Groups & Settings > All Settings > Console Security > Session Management
- C- Accounts > Administrators > System Activity
- D- Resources > Device Updates > OEM Updates

Answer:

A

Explanation:

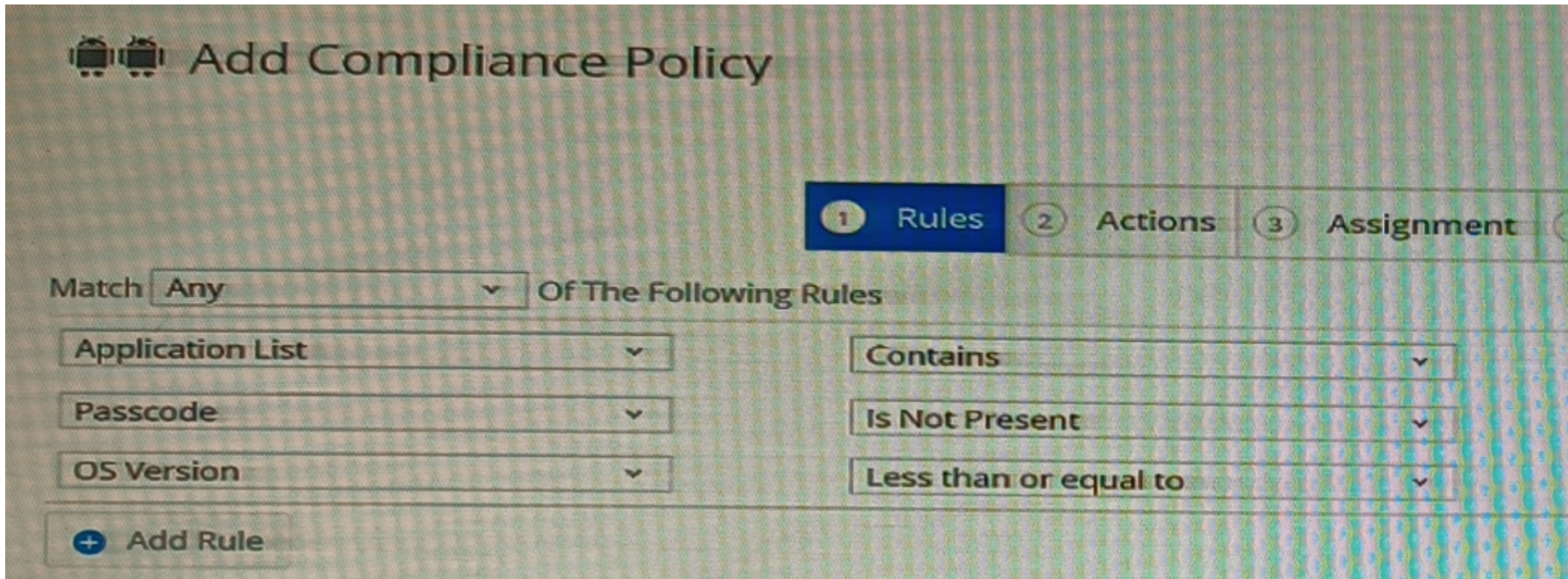
The console page that would confirm a potential configuration change is Monitor > Reports & Analytics > Events > Console Events. This page allows the administrator to view and filter the events that occurred in the Workspace ONE UEM console, such as configuration changes, user actions, system errors, and so on. The administrator can use this page to find out if a configuration was enabled by mistake that caused the error.

Question 7

Question Type: MultipleChoice

Refer to the exhibit.

A company has created a compliance policy with the following rules:



The screenshot shows the 'Add Compliance Policy' interface. At the top, there are two Android icons and the title 'Add Compliance Policy'. Below the title is a progress indicator with three steps: '1 Rules' (highlighted in blue), '2 Actions', and '3 Assignment'. Under the 'Rules' step, there is a 'Match' dropdown menu set to 'Any' and the text 'Of The Following Rules'. Below this, there are two columns of dropdown menus. The left column contains 'Application List', 'Passcode', and 'OS Version'. The right column contains 'Contains', 'Is Not Present', and 'Less than or equal to'. At the bottom left, there is a button with a plus sign and the text 'Add Rule'.

Recently, the Android device was marked as non-compliant. The VMware Workspace ONE UEM 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.)

Options:

- 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.

Answer:

A, B

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 8

Question Type: MultipleChoice

receiving a timeout error when accessing files using the VMware Workspace ONF Content application. The administrator needs to gather log files for troubleshooting these issues with the organization's internal file servers and shared SaaS Workspace ONE- UEM

On which component should the administrator enable verbose logging?

Options:

- A- UAG (Unified Access Gateway) Edge service
- B- Device Services service
- C- ACC (AirWatch Cloud Connector)

D- AWCM (AirWatch Cloud Messaging) service

Answer:

A

Explanation:

The component that the administrator should enable verbose logging on is UAG (Unified Access Gateway) Edge service. UAG is a component that provides secure edge services for Workspace ONE UEM, such as VMware Tunnel, Content Gateway, or Secure Email Gateway². If users are receiving a timeout error when accessing files using the Workspace ONE Content application, it could indicate that there is a problem with UAG configuration, connectivity, or performance. Enabling verbose logging for UAG can help identify and troubleshoot the issue.

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>

