VMware.5V0-62.22.v2023-11-03.q27

Exam Code:	5V0-62.22
Exam Name:	VMware Workspace ONE 21.X UEM Troubleshooting Specialist
Certification Provider:	VMware
Free Question Number:	27
Version:	v2023-11-03
# of views:	661
# of Questions views:	270
https://www.freepdfdumps.com/VMware.5V0-62.22.v2023-11-03.q27.html	

NEW QUESTION: 1
An administrator working with the VMware Workspace ONE UEM product suite is encountering issues when try.ng to enroll .OS devices us.ng basic users. Wh.ch VMware Workspace ONE UEM service or component logs should be gathered by the administrator to determine a root cause?
A. Console logs
B. AirWatch Cloud Messaging logs
C. AirWatch Cloud Connector logs
D. Device Services logs
Answer: D (LEAVE A REPLY)
Explanation
The VMware Workspace ONE UEM service or component logs that should be gathered by the administrator to determine a root cause are Device Services logs. 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 iOS devices are unable to enroll using basic users, it could indicate that there is a problem with Device Services configuration, connectivity, or synchronization. The administrator should gather and analyze the Device Services logs to identify and troubleshoot the issue.

NEW QUESTION: 2
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
Answer: A (LEAVE A REPLY)

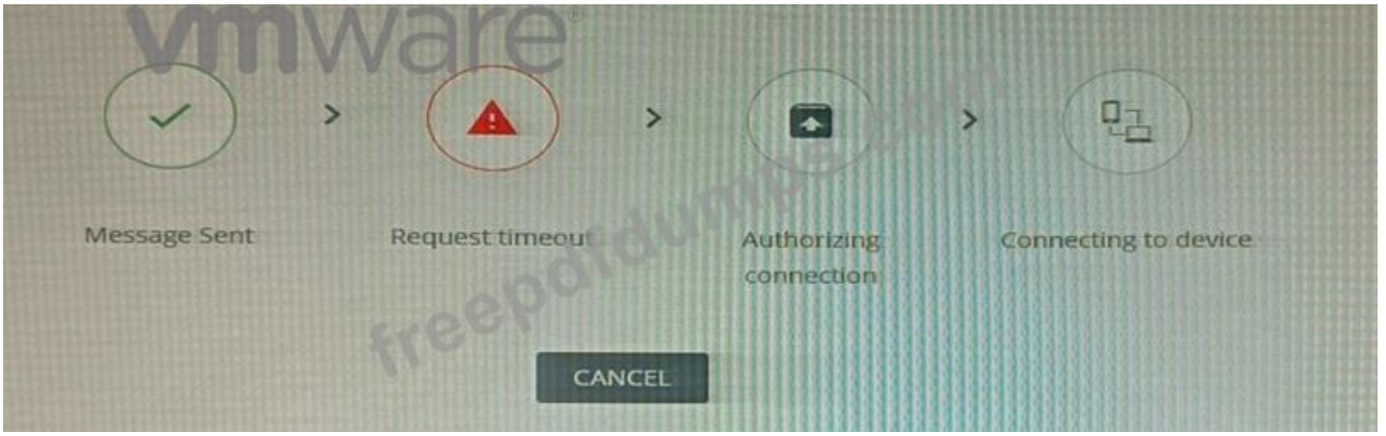
Explanation
The VMware Workspace ONE UEM console configuration page that would be used to enable debug logging for a specific device is Groups & Settings > All Settings > Admin > Diagnostics > Logging5. This page allows administrators to enable debug logging for a specific device or a group of devices 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.

NEW QUESTION: 3
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
Answer: A,C (LEAVE A REPLY)
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.

NEW QUESTION: 4
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
Answer: (SHOW ANSWER)
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.

NEW QUESTION: 5
Refer to the exhibit- An IT administrator tried to start a remote session using Workspace ONE Assist but received this request timeout error:



What might be the root cause of this issue"?
A. Workspace ONE Assist agent failed to connect to the Workspace ONE Assist server
B. Workspace ONE Intelligent Hub failed to connect to the Workspace ONE Assist server
C. The devices were connected remotely using the unattended mode in Workspace ONE Assist agent.
D. The Administrator didn't have proper level of access to Workspace ONE Assist's features.
Answer: A (LEAVE A REPLY)
Explanation
The root cause of this issue is that Workspace ONE Assist agent failed to connect to the Workspace ONE Assist server. The request timeout error indicates that the Workspace ONE Assist agent did not receive a response from the Workspace ONE Assist server within the specified time limit3. This could be due to network issues, firewall settings, or authentication problems. The administrator should check and resolve these issues to enable remote sessions using Workspace ONE Assist.

NEW QUESTION: 6

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

Answer: D (LEAVE A REPLY)

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.

NEW QUESTION: 7

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

Answer: A,B,C (LEAVE A REPLY)

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.

NEW QUESTION: 8

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
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 9
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
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 10
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

Answer: B (LEAVE A REPLY)

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.

NEW QUESTION: 11

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.

Answer: C (LEAVE A REPLY)

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.

NEW QUESTION: 12

A few devices have stopped updating their last seen time within the console After testing with a device, the administrator notices the Intelligent Hub states AWCM is connected. The administrator decides to review the connection flow to determine the cause of the failure?

Which connection flow should be examined to gain this insight?

A. Device Services connection to DB

B. Device connection to Device Services

C. Device Connection to Console Server
D. AWCM connection to Device Services
Answer: (SHOW ANSWER)
Explanation
The connection flow that should be examined to gain this insight is device connection to 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 devices have stopped updating their last seen time within the console, it could indicate that there is a problem with device connection to Device Services. The administrator should check and resolve any issues with device connection to Device Services.

NEW QUESTION: 13
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
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 14
Refer to the exhibit.

A VMware Workspace ONE administrator made changes to the Secure Email Gateway in the VMware Workspace ONE UEM console When validating the new settings, the test connection fails Which statement describes the root cause of this issue?

A. The outbound proxy host, port, username, and password values are missing.

B. The protocol https: // is missing in the Secure Email Gateway hostname value

C. The Secure Email Gateway configuration does not have a valid SSL certificate.

D. The protocol https: // is missing in the API server URL value.

Answer: B (LEAVE A REPLY)

Explanation

The statement that describes the root cause of this issue is that the protocol https:// is missing in the Secure Email Gateway hostname value. The Secure Email Gateway hostname value is the URL that Workspace ONE UEM uses to connect to the Secure Email Gateway edge service on UAG and perform email management tasks, such as quarantine, wipe, or block. The protocol https:// is required to indicate that the connection is secure and encrypted. If the protocol https:// is missing, Workspace ONE UEM will not be able to connect to the Secure Email Gateway edge service, and the test connection will fail. The administrator should add the protocol https:// to the Secure Email Gateway hostname value.

NEW QUESTION: 15

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
Answer: D (LEAVE A REPLY)
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.

NEW QUESTION: 16
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
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 17
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
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 18
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
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 19
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?
A. UAG (Unified Access Gateway) Edge service
B. Device Services service
C. ACC (AirWatch Cloud Connector)
D. AWCM (AirWatch Cloud Messaging) service
Answer: A (LEAVE A REPLY)
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.

NEW QUESTION: 20
A VMware Workspace ONE 3dministrator is troubleshooting an information in the CloudConnector.log.
Which logging level should the administrator use?
A. Verbose
B. Debug
C. Error
D. Information
Answer: A (LEAVE A REPLY)
Explanation
The logging level that the administrator should use is verbose. Verbose logging provides the most detailed information about the ACC (AirWatch Cloud Connector) service, such as configuration, connectivity, synchronization, and errors2. Verbose logging can help identify and troubleshoot the root cause of the issue with the CloudConnector.log.

NEW QUESTION: 21
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.

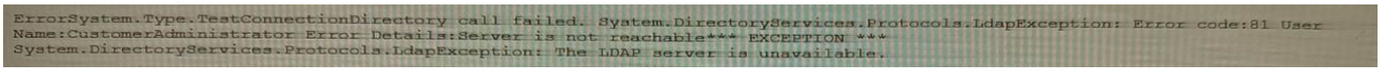
Answer: D (LEAVE A REPLY)

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.

NEW QUESTION: 22

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



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

Answer: D (LEAVE A REPLY)

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.

NEW QUESTION: 23

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?

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 (LEAVE A REPLY)

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.

NEW QUESTION: 24

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).

Answer: (SHOW ANSWER)

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.

NEW QUESTION: 25

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

Answer: A (LEAVE A REPLY)

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.

NEW QUESTION: 26
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
Answer: C (LEAVE A REPLY)
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.

NEW QUESTION: 27
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.
Answer: D (LEAVE A REPLY)
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.