PassQueen
a.k.a dumpsqueen.com

Professional VMware Workspace ONE 21.X

VMware 2V0-62.21

Version Demo

Total Demo Questions: 8

Total Premium Questions: 81

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Architecture and Technologies	12
Topic 2, Products and Solutions	22
Topic 3, Planning and Designing	2
Topic 4, Installing, Configuring, and Setup	30
Topic 5, Troubleshooting and Repairing	4
Topic 6, Administrative and Operational Tasks	11
Total	81

QUESTION NO: 1

For federal clients, FIPS 140-2 and AES 256-bit encryption are applied to which three areas? (Choose three.)

A. data in use

B. data in flying

C. data in pace

D. data in rest

E. data in transit

ANSWER: A D E

Explanation:

For federal client deployments, the applicable protection model covers data throughout its lifecycle: data in use, data in rest, and data in transit. Data in use refers to information being actively processed by the Workspace ONE platform or its managed services. Protecting this state supports the requirement to use validated cryptographic capabilities wherever sensitive federal data is handled. Data in rest covers persisted information, such as records and stored content, and AES 256-bit encryption provides strong encryption for that stored data. Data in transit covers information moving between endpoints, Workspace ONE services, and integrated components; protected transport sessions prevent disclosure or alteration while the data crosses a network.

FIPS 140-2 is a U.S. federal cryptographic-module validation standard, while AES is an approved encryption algorithm used to protect sensitive information. Together, these controls address active processing, storage, and communications rather than limiting encryption solely to a single storage or network layer. VMware's Workspace ONE security material describes encryption and secure communications as core platform protections, and the NIST FIPS standard defines the validation requirements for cryptographic modules used by federal agencies. See NIST FIPS 140-2 and VMware Workspace ONE.

QUESTION NO: 2

An organization has purchased a SaaS Workspace ONE solution and wants to implement these:

▪ integration with back-end resources like Active Directory from Microsoft to sync users and groups ▪ Kerberos authentication

▪ integration with Virtual Desktops and Applications from services (Horizon 7, Horizon Cloud, or Citrix) ▪ third party integration with RSA SecureID, RADIUS for authentication

Which Workspace ONE component is required?

A. VMware AirWatch Cloud Connector

B. VMware Workspace ONE Access Connector

C. VMware Workspace ONE Assist

D. VMware Workspace Unified Access Gateway

ANSWER: B

Explanation:

VMware Workspace ONE Access Connector is required because it provides the on-premises connector services that allow a SaaS Workspace ONE Access tenant to securely use enterprise resources that remain inside the organization's network. Its Directory Sync service connects to Active Directory and synchronizes users and groups into Workspace ONE Access. The connector's authentication-related services support enterprise authentication flows, including Kerberos-based authentication and integration with authentication methods such as RADIUS and RSA SecurID where configured. The Virtual App service is also used to integrate entitled virtual desktops and published applications from supported providers, including Horizon environments and Citrix, so they can be presented through the Workspace ONE catalog. These services use outbound

communication to the SaaS tenant, avoiding a requirement to expose the internal directory, authentication infrastructure, or virtual-app resources directly to the internet. VMware documents that the Access Connector is deployed on-premises for directory synchronization, user authentication, Kerberos authentication, and virtual-app collection functions in Workspace ONE Access SaaS deployments. See the VMware Workspace ONE Access Connector documentation and the Workspace ONE Access architecture guide.

QUESTION NO: 3

Which is required during installation of the Workspace ONE Intelligence Connector service?

A. Workspace ONE Intelligence Connector service must be installed on the AWCM Server.

B. Workspace ONE Intelligence Connector must be installed on the Console Server.

C. Workspace ONE Intelligence Connector service must be installed on the Device Services Server.

D. Workspace ONE Intelligence Connector must be installed on its own server.

ANSWER: D

Explanation:

Workspace ONE Intelligence Connector must be installed on its own server. The connector is an on-premises Workspace ONE UEM component that securely transmits Workspace ONE UEM data to the Workspace ONE Intelligence cloud service for reporting, dashboards, automation, and insights. VMware's documented deployment requirements specify that the Intelligence Connector service is installed on a dedicated server rather than being co-located with core Workspace ONE UEM roles. A dedicated host helps isolate the connector workload, avoids resource contention with UEM services, and supports the intended network and security architecture for outbound communication with Workspace ONE Intelligence. During planning, administrators should also ensure that the dedicated server meets the applicable operating-system, .NET, connectivity, certificate, service-account, and firewall requirements published for the connector release. This installation placement requirement applies specifically to the Intelligence Connector service and is part of preparing a supported on-premises UEM integration with Intelligence. See the VMware Workspace ONE Intelligence Connector requirements documentation at Workspace ONE Intelligence Connector Requirements and the Workspace ONE Intelligence documentation portal at VMware Workspace ONE Intelligence Documentation.

QUESTION NO: 4

Which three device conditions can be evaluated by a Workspace ONE UEM compliance policy? (Choose three.)

A. Compromised status

B. Encryption status

C. Operating system version

D. Monitor refresh rate

E. Processor clock speed

ANSWER: A B C

Explanation:

Workspace ONE UEM compliance policies evaluate reported device conditions and can apply remediation actions when a device does not meet the organization's requirements. **Compromised status** can be evaluated to identify rooted Android devices or jailbroken iOS devices. **Encryption status** can be evaluated to ensure that device storage is protected. **Operating system version** can be evaluated to identify devices that are running an unsupported or outdated OS release.

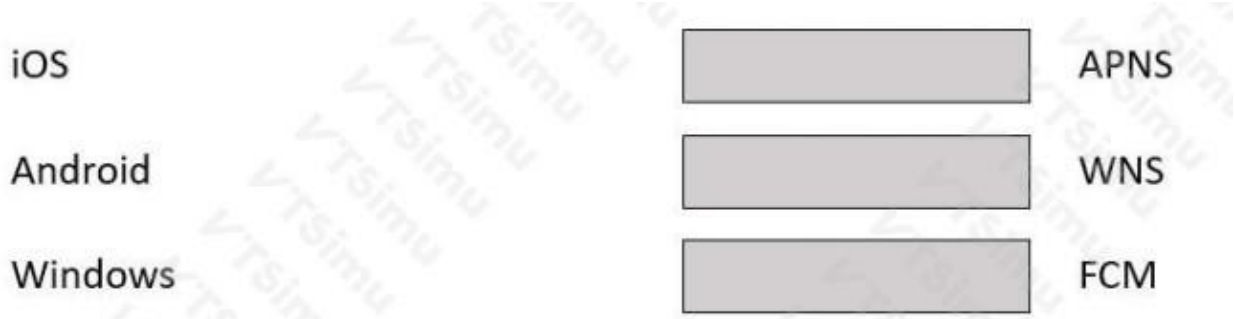
When a device violates a configured compliance rule, Workspace ONE UEM can take actions such as notifying the user, sending an email to an administrator, blocking access, or removing managed enterprise data according to the configured policy.

QUESTION NO: 5 - (DRAG DROP)

DRAG DROP

Drag and drop the device operating system on the left into the box associated with its third party messaging solution.

Select and Place:



ANSWER:



Explanation:

Workspace ONE UEM uses the native push-notification infrastructure provided by each device platform to notify managed devices that they should contact the UEM service and retrieve pending commands or updates. Apple devices use Apple Push Notification service, commonly called APNS. This is the Apple-operated service that enables Workspace ONE UEM to send a lightweight notification to an enrolled iOS device when an administrative action is waiting. VMware's documentation describes APNS configuration as a required part of Apple device management: VMware Workspace ONE UEM APNS overview.

Windows devices use Windows Notification Service, abbreviated WNS. This Microsoft service is the platform notification channel used to wake or notify supported Windows devices, enabling them to receive and process management activity from Workspace ONE UEM. Android devices use Firebase Cloud Messaging, abbreviated FCM, which is Google's messaging service for delivering notifications to Android applications and devices. Google documents FCM as its cross-platform messaging solution at Firebase Cloud Messaging documentation. Thus, the correct completed relationship is iOS with APNS, Windows with WNS, and Android with FCM. The placements shown in the answered image match these platform-specific third-party messaging services exactly.

QUESTION NO: 6

Which three are features of the Workspace ONE Content Gateway service? (Choose three.)

A. Encrypted communications using SSL/TLS.

B. Secure access to internal repositories.

C. Provides health status on external repositories.

D. Support for most corporate file servers.

E. Provides email notification for Exchange mail.

ANSWER: B C D

Explanation:

Workspace ONE Content Gateway is an edge service that securely brokers managed-device access to enterprise content repositories without exposing those repositories directly to the internet. **Secure access to internal repositories.** is a core purpose of the service: requests from authorized Workspace ONE users and devices are proxied to content sources located on the corporate network. **Support for most corporate file servers.** is also a key capability because Content Gateway integrates Workspace ONE Content with common enterprise repository types, allowing organizations to make existing corporate content available through a controlled mobile-access path. **Provides health status on external repositories.** is correct because the service and its repository connections can be monitored, enabling administrators to identify the operational state of configured repository access and maintain service availability. These capabilities make Content Gateway suitable for publishing internal corporate content securely while retaining centralized management and visibility in the Workspace ONE environment. VMware's Unified Access Gateway operational guidance describes Content Gateway as an edge service used to provide secure access to internal content resources; see VMware Tech Zone: Configuring Edge Services. Additional architectural and deployment guidance is available in the Workspace ONE Unified Access Gateway Architecture.

QUESTION NO: 7

An administrator is preparing to setup email management for Office 365 in UEM.

Which is VMware's recommended email deployment model for this scenario?

A. VPN

B. Proxy

C. Indirect

D. Direct

ANSWER: D

Explanation:

Direct is VMware's recommended email deployment model for an Office 365 scenario because Office 365 is a cloud-hosted service that mobile devices can reach directly over the internet. In the direct model, Workspace ONE UEM deploys the appropriate email configuration to enrolled devices, and the mail client establishes its connection directly with the organization's Office 365 or Exchange Online tenant. This design is well suited to cloud email because it avoids placing an on-premises email gateway in the mail-flow path solely to reach a service that is already internet-accessible. Administrators can use Workspace ONE UEM profiles and application configuration to consistently provide account, server, authentication, and security settings to managed devices while Microsoft 365 handles the hosted email service. The approach also reduces infrastructure complexity and aligns with the operational model of Exchange Online. VMware's Workspace ONE UEM documentation describes the available email deployment approaches and their use with cloud-hosted email, while Microsoft documents Exchange Online as part of its Microsoft 365 cloud service. See the Workspace ONE UEM Email Management documentation and Microsoft Exchange Online documentation.

QUESTION NO: 8

An administrator needs to deploy a sequence of applications, profiles, and scripts to Windows devices. The deployment must continue only after each preceding resource has successfully installed.

Which Workspace ONE feature should the administrator use?

A. Freestyle Orchestrator

B. Workspace ONE Intelligence Dashboards

C. Organization Group Assignment Rules

D. Report Subscriptions

ANSWER: A

Explanation:

Freestyle Orchestrator is the correct feature because it allows administrators to create resource workflows with ordered deployment steps and defined installation dependencies. A workflow can contain applications, profiles, scripts, sensors, and other supported Workspace ONE UEM resources.

Freestyle Orchestrator evaluates the status of each resource before processing the next item in the workflow. This enables administrators to create a controlled deployment sequence, such as installing a prerequisite application before deploying a dependent application or applying a configuration profile after a required application is present. Standard independent assignments do not provide the same workflow-based sequencing capability.

For more information, see the Freestyle Orchestrator for Workspace ONE UEM resource.