PassQueen
a.k.a dumpsqueen.com

VMware Workspace ONE 21.X Advanced Integration Specialist

VMware 5V0-61.22

Version Demo

Total Demo Questions: 8

Total Premium Questions: 80

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Architectures and Technologies	12
Topic 2, VMware Products and Solutions	25
Topic 3, Planning and Designing	3
Topic 4, Installing, Configuring, and Setup	29
Topic 5, Troubleshooting and Repairing	2
Topic 6, Administrative and Operational Tasks	9
Total	80

QUESTION NO: 1

Which two items must be supplied to a third-party SAML identity provider when configuring Workspace ONE Access as a SAML service provider? (Choose two.)

A. Service provider entity ID

B. Assertion consumer service URL

C. RADIUS shared secret

D. Active Directory bind password

E. Apple Push Notification service certificate

ANSWER: A B

Explanation:

Service provider entity ID and **assertion consumer service URL** are required SAML service-provider values. The entity ID uniquely identifies Workspace ONE Access to the external identity provider. The assertion consumer service URL identifies the Workspace ONE Access endpoint to which the identity provider sends the SAML response after the user is authenticated.

These settings are commonly supplied through Workspace ONE Access service-provider metadata. The identity provider uses the metadata to establish the trust configuration, including the service-provider identifier, response destination, and signing certificate information. See the OASIS SAML 2.0 Core specification and the Omnissa documentation portal.

QUESTION NO: 2

Which two solutions needs to be integrated for an administrator to have conditional access with User Risk Score? (Choose two.)

A. Workspace ONE Hub Services

B. Workspace ONE SASE

C. Workspace ONE Assist

D. Workspace ONE Access

E. Workspace ONE Intelligence

ANSWER: D E

Explanation:

Workspace ONE Access and **Workspace ONE Intelligence** must be integrated to implement conditional access based on User Risk Score. Workspace ONE Intelligence analyzes the available Workspace ONE UEM, application, device, and user-context data to calculate risk scores. Its risk-scoring capability provides the user risk assessment that can identify circumstances requiring a response, such as elevated risk associated with a user's activity or environment.

Workspace ONE Access provides the identity and access-management policy enforcement point. After it receives the user-risk information from Workspace ONE Intelligence, an administrator can use that risk context in access policies to control authentication and application access. The resulting policy can require stronger authentication or deny access when the user's assessed risk reaches the configured threshold. This integration therefore combines Intelligence's risk evaluation with Access's conditional-access decision and enforcement capabilities.

For implementation context, see the Omnissa Tech Zone guidance on Workspace ONE Intelligence risk scores and the Workspace ONE Access conditional-access overview.

QUESTION NO: 3

Which VMware Workspace ONE Access prerequisites must be completed to successfully deploy a Virtual Apps Collection?

A. Workspace ONE Access Connector Enrollment Server, App Volumes Manager

B. SAML Authenticator, Enrollment Server, Horizon Pod

C. SAML Authenticator, Workspace ONE Access Connector, Horizon Pod

D. Workspace ONE Access Connector, Horizon Connection Server, App Volumes Manager

ANSWER: C

Explanation:

SAML Authenticator, Workspace ONE Access Connector, Horizon Pod is correct because a Horizon virtual-apps collection relies on these components being prepared before Workspace ONE Access can enumerate and publish Horizon-hosted resources. The Workspace ONE Access Connector provides the on-premises Virtual Apps service connection used to communicate securely with Horizon infrastructure and synchronize entitled applications and desktops into the Workspace ONE Access catalog. A configured Horizon pod supplies the Connection Server environment from which those resources, assignments, and metadata are collected. Finally, configuring the SAML authenticator establishes the trust required for Workspace ONE Access to authenticate users to Horizon through SAML when they launch the published resources. Together, these prerequisites enable both resource synchronization and the end-user launch flow, which are the essential functions of a Horizon virtual-apps collection. VMware's Workspace ONE Access documentation describes the connector-based integration and Horizon resource setup in its Workspace ONE Access documentation. The Horizon-side SAML and pod configuration requirements are covered in the official VMware Horizon documentation.

QUESTION NO: 4

A VMware Workspace ONE environment has been setup with Roles Based Access Control (RBAC), and the directory-based administrators who managed in Workspace ONE UEM have limited permissions to access the console.

The administrator has enabled VMware Workspace ONE Intelligence in the environment and must now enable the correct configuration setting that will allow administrators to access VMware Workspace ONE Intelligence from VMware Workspace ONE UEM.

Which configuration setting must be enabled?

A. Create a new admin role in the Intelligence Console, and then give the rote Read and Edit permissions to Intelligence

B. Create a new user role, and then give the role Read and Edit permissions to Intelligence in Categories > Monitor

C. Create a new admin role, and then give the role Read and Edit permissions to Intelligence in Categories > Monitor

D. Create a new user role in the Intelligence Console, and then give the role Read and Edit permissions to Intelligence

ANSWER: C

Explanation:

Create a new admin role, and then give the role Read and Edit permissions to Intelligence in Categories > Monitor is correct because Workspace ONE UEM controls administrator access to the Workspace ONE Intelligence launch point through its administrator-role permissions. In a role-based access-control deployment, directory-based administrators do not automatically receive Intelligence access simply because the Intelligence service has been enabled for the organization. An appropriate UEM administrator role must explicitly include the Intelligence permission.

To configure this, an administrator creates or edits an admin role in the UEM console and navigates to the Monitor category. Granting both Read and Edit for Intelligence makes the Intelligence entry available to members assigned that admin role and authorizes the role to access the integrated Intelligence experience. The role can then be assigned to the relevant directory-based administrator accounts, maintaining least-privilege administration while allowing the intended personnel to use Intelligence from UEM.

This approach follows the Workspace ONE UEM administration model, in which console capabilities are granted through admin roles and category permissions. See the Workspace ONE UEM Administration Guide and the Workspace ONE Intelligence resource page for product administration guidance.

QUESTION NO: 5

Hub Services is being integrated with VMware Workspace ONE Access to provide additional features.

Which three additional features become available? (Choose three.)

A. Templates

B. Customize Branding

C. Digital Badge

D. People Search

E. Hub Virtual Assistant

F. Employee Self-Service Support

ANSWER: B C D

Explanation:

Integrating Hub Services with Workspace ONE Access makes the Intelligent Hub experience more personalized and employee-centric. **Customize Branding** is available because Hub Services provides controls for configuring the Hub portal's appearance, including organizational branding elements, so that the employee experience aligns with company identity. **Digital Badge** is also a Hub Services capability: it enables an organization to issue and present digital employee credentials through Intelligent Hub, helping users access supported workplace services using a mobile badge. **People Search** becomes available through the Hub directory experience, allowing employees to find colleagues and view relevant directory details from Intelligent Hub. Together, these services extend Workspace ONE Access beyond application access into a unified employee experience that includes branded communications, identity-oriented workplace services, and organizational discovery. VMware's Workspace ONE documentation describes Hub Services configuration and its employee-experience features, while the Intelligent Hub documentation covers the user-facing services available after Hub Services is enabled. See the VMware Hub Services documentation and the Intelligent Hub services documentation.

QUESTION NO: 6

An administrator is setting up a new integration between VMware Workspace ONE UEM and VMware Workspace ONE Access.

Which settings need to be configured in the VMware Workspace ONE UEM console?

A. Kerberos admin key, import the Kerberos Admin account, and the admin auth certificate for VMware Workspace ONE Access

B. REST API admin key, import the API Admin account, and the admin auth certificate for VMware Workspace ONE Access

C. SOAP API admin key, import the API Admin account, and the admin auth certificate for VMware Workspace ONE Access

D. Certificate API admin key, import the API Admin account, and the admin auth certificate for VMware Workspace ONE Access

ANSWER: B

Explanation:

REST API admin key, import the API Admin account, and the admin auth certificate for VMware Workspace ONE Access is correct because Workspace ONE UEM uses its REST API integration framework to establish trusted, authenticated

communication with Workspace ONE Access. The REST API key identifies and authorizes the Workspace ONE Access service when it makes API requests to UEM. An imported API administrator account supplies the UEM administrative identity and permissions required for the integration to query device and user information and to support unified catalog and access workflows. The Workspace ONE Access administrator authentication certificate must also be imported into UEM so that UEM can validate the certificate-based authentication used by the Access service. These items are configured as part of the Workspace ONE Access integration settings in the UEM Console and collectively provide API authorization, an authorized service account, and certificate trust. This integration enables Workspace ONE Access to consume UEM-managed device compliance and application-management information in a secure manner. See the Omnissa Workspace ONE documentation portal at Omnissa Docs and the Workspace ONE technical resource library at Omnissa Tech Zone for Workspace ONE Access and UEM integration guidance.

QUESTION NO: 7

Which two methods may administrators use to provision users from Okta to VMware Workspace ONE Access? (Choose two.)

A. System for Cross-domain Identity Management (SCIM) API

B. Workspace ONE UEM REST API

C. Active Directory Sync

D. Just-in-time (JIT) Provisioning

E. AirWatch Cloud Connector

ANSWER: A D

Explanation:

System for Cross-domain Identity Management (SCIM) API is correct because Okta can use its lifecycle-management provisioning service with a SCIM endpoint exposed by VMware Workspace ONE Access. SCIM supports automated account lifecycle operations, including creating and updating users and, where configured, managing deactivation. This provides a standards-based way to synchronize user identity data from Okta into the Workspace ONE Access directory.

Just-in-time (JIT) Provisioning is also correct. With federated SAML authentication, Workspace ONE Access can be configured to create a user account when an authenticated user first signs in from the external identity provider. JIT provisioning is useful when administrators want accounts to be created on first successful access rather than pre-populating all users through a synchronization process. The identity-provider assertion supplies the required user attributes used to establish the Workspace ONE Access user record.

These approaches support distinct operational models: SCIM is appropriate for proactive lifecycle synchronization, while JIT creates users at authentication time. Okta describes SCIM-based lifecycle provisioning in its Lifecycle Management documentation, and its VMware Workspace ONE integration listing identifies the integration's supported identity and provisioning capabilities.

QUESTION NO: 8

Which category setting of Citrix-published resources is supported in VMware Workspace ONE Access?

A. Syncing

B. Nested categories

C. StoreFront Filtering

D. Tagging

ANSWER: C

Explanation:

StoreFront Filtering is supported for Citrix-published resources integrated with VMware Workspace ONE Access. When Workspace ONE Access is configured to use a Citrix StoreFront deployment, StoreFront can control which published applications and desktops are presented to users. This enables administrators to apply StoreFront filtering rules and then synchronize only the resources that are available through the configured StoreFront view into the Workspace ONE Access catalog. The Workspace ONE Access Citrix integration relies on StoreFront to enumerate entitled resources, making StoreFront-based filtering a supported method for managing the published-resource catalog exposed through the Workspace ONE Intelligent Hub or web portal. Administrators should configure the Citrix integration and resource synchronization according to the documented connector and StoreFront requirements so that the filtered resource set is consistently reflected for entitled users. VMware's Workspace ONE Access documentation covers configuring Citrix-published resources and synchronizing them through the connector: VMware Workspace ONE Access Documentation. Additional product documentation and integration guidance is available from the official Broadcom TechDocs portal: VMware Identity Manager / Workspace ONE Access TechDocs.