



VMware Workspace ONE 21.X Advanced Integration 5V0-61.22 Practice Questions

Shared by Christensen on 17-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

What is the primary benefit of utilizing Verify (Intelligent Hub) authentication in VMware Workspace ONE Access?

Options:

- A- It allows administrators to integrate with RSA for multi-factor authentication
- B- It provides a second authentication method through Intelligent Hub to access a restricted Hub catalog or restricted applications
- C- It is the primary means of performing direct integration between VMware Workspace ONE Access and VMware Workspace ONE UEM
- D- It integrates with Duo Security for two-factor authentication

Answer:

B

Question 2

Question Type: MultipleChoice

An administrator has enabled and configured Kerberos in the VMware Workspace ONE Access console, but the connection test fails.

What is one reason this connection failed to authenticate?

Options:

- A- The Linux machine on which the Kerberos Auth service is installed was not joined to the domain
- B- The certificate was not enabled on VMware Workspace ONE UEM console
- C- The Kerberos Auth service are incorrectly configured on the AirWatch Cloud Connector
- D- The certificate is unsigned by a trusted SSL or public or internal certificate authority

Answer:

C

Question 3

Question Type: MultipleChoice

Which step is required to configure Digital Employee Experience Management (DEEM)?

Options:

- A- Ensure devices ownership type is set to employee-owned
- B- Enable DEEM Workspace ONE Access
- C- Integrate the productivity app with Workspace ONE SDK
- D- Use Windows and/or macOS managed devices in Workspace ONE UEM

Answer:

B

Question 4

Question Type: MultipleChoice

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

Options:

- 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:

D

Question 5

Question Type: MultipleChoice

Which two actions are valid based on identified risk behaviors in VMware Workspace ONE Intelligence Risk Analytics? (Choose two.)

Options:

- A- Add authentication methods to the user or device with VMware Workspace ONE Access integration
- B- Delete all previous risk scoring for the user
- C- Move the user to the 'very high' risk category
- D- Monitor the device or user
- E- Add authentication methods to the user or device with VMware Workspace ONE UEM integration

Answer:

D, E

Question 6

Question Type: MultipleChoice

A VMware Workspace ONE administrator and the Information Security Officer reported that the Unified Access Gateway (UAG) front-end network is compromised. The compromised device was reconfigured to bypass the UAG.

Why did this action fail in a two-NIC deployment?

Options:

- A- The UAG combines layer 5 firewall rules with layer 7 Unified Access Gateway security
- B- The UAG combines layer 4 firewall rules with layer 7 Unified Access Gateway security
- C- The UAG combines layer 3 firewall rules with layer 7 Unified Access Gateway security
- D- The UAG combines layer 2 firewall rules with layer 7 Unified Access Gateway security

Answer:

B

Question 7

Question Type: MultipleChoice

Which statement accurately describes modern claims-based identity management?

Options:

- A- It supports multiple authentication methods except Single Sign-On
- B- It doesn't support multiple providers
- C- It requires the application to perform the authentication task
- D- It makes account management easier by centralizing authentication

Answer:

D

Question 8

Question Type: MultipleChoice

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

Options:

- 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

Question 9

Question Type: MultipleChoice

An administrator needs to configure OpenID Connect in VMware Workspace ONE Access for third-party identity providers so the users may use their credentials for single sign-on.

Which primary authentication protocol is used?

Options:

- A- LDAP
- B- FTP
- C- IMAP
- D- OAuth2

Answer:

D

Question 10

Question Type: MultipleChoice

A customer has asked for recommendations around a disaster recovery architecture design for VMware Workspace ONE Access. The customer has an extremely aggressive recovery point objective and recovery time objective.

Which HA/DR design should be recommended, given the supported options?

Options:

- A- Multi-datacenter design with two 3-node clusters, One 3-node cluster Datacenter 1 and the other 3-node cluster m Datacenter 2. The two 3-node clusters are setup in an active/passive configuration.
- B- Multi-datacenter design with two 3-node clusters. One 3-node cluster Datacenter 1 and the other 3-node cluster m Datacenter 2. The two 3-node clusters are setup in an active/active configuration.
- C- Multi datacenter design with two 3-node clusters, Both 3-node clusters are spanned across both datacenters, two nodes in one datacenter and one in the other, respectively. The two 3-node clusters are setup in an active/active configuration.
- D- Multi-datacenter design with two 3-node clusters, Both 3-node clusters are spanned across both datacenters, two nodes in one datacenter and one in the other, respectively. The two 3-node clusters are setup in an active/passive configuration.

Answer:

C

Question 11

Question Type: MultipleChoice

Which step is required to configure the AirWatch Provisioning App?

Options:

- A- Configure an identify provider as the SAML Provider
- B- Configure LDAP - Other LDAP at the Container OG level in Workspace ONE UEM
- C- Set up LDAP - Active Directory at the Customer OG level in Workspace ONE UEM
- D- Provision Users at the Container OG level in Workspace ONE UEM

Answer:

C

Question 12

Question Type: MultipleChoice

An organization wants to prevent users from connecting to VMware Horizon desktop or application pools from a Horizon Pod deployed on their internal network unless the user selects the Horizon pool from the Unified Catalog of their Workspace ONE Access shared SaaS tenant.

Which additional setting must the organization administrator configure?

Options:

- A- Enable the Virtual App Service on all Unified Access Gateway systems that allow users to connect to Horizon pools from the Horizon Pod
- B- Configure the Workspace ONE Access tenant as a SAML 2.0 authenticator on all Horizon Connection Servers in the Horizon Pod
- C- Enable the VMware Tunnel on all Unified Access Gateway systems that allow users to connect to Horizon pools from the Horizon Pod
- D- Set "Delegation of authentication to VMware Horizon (SAML 2.0 Authenticator)" to "Allowed" on all Horizon Connection Servers in the Horizon Pod

Answer:

C

Question 13

Question Type: MultipleChoice

Which feature limits the number of changes that can be made to Users and Groups when updating directories in VMware Workspace ONE Access?

Options:

- A- UEM Security PIN
- B- Default Action For Inactive Users
- C- Conditional Group Sync
- D- Directory Sync Safeguard

P2P
exams

Answer:

D

P2P
exams

To Get Premium Files for 5V0-61.22 Visit

<https://www.p2pexams.com/products/5v0-61.22>

For More Free Questions Visit

<https://www.p2pexams.com/vmware/pdf/5v0-61.22>

20%
DISCOUNT

P2P
exams