



5V0-61.22^{Q&As}

VMware Workspace ONE 21.X Advanced Integration Specialist

Pass VMware 5V0-61.22 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/5v0-61-22.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by VMware
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





QUESTION 1

An organization wants to allow users to connect to VMware Horizon desktop or application pools from a Horizon Pod deployed on their internal network by selecting the Horizon resources from the Unified Catalog of their Workspace ONE Access shared SaaS tenant.

Which setting must an organization administrator make to achieve this goal?

- A. Set authentication method in VMware Horizon to ADFS Authenticator = Allowed on all Horizon Connection Servers in the Horizon Pod
- B. Enable the Virtual App Service on all Unified Access Gateway systems that allow users to connect to Horizon pools from 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

Correct Answer: D

Reference: <https://techzone.vmware.com/resource/workspace-one-access-architecture>

QUESTION 2

An administrator of iOS supervised devices has noticed that devices are checking in regularly but are failing the Last Compromised Scan compliance policy. The administrator is fine with having slight disruptions to users but does not want

any interaction from the user to be required.

The administrator decides to use an action in the Last Compromised Scan compliance policy that would force the device to report back the compromised status without requiring user input.

Which action in the Last Compromised Scan compliance policy should be used?

- A. Assign a sensor to the device to request the compromised status
- B. Assign the command to Request Device Check-In
- C. Assign a push notification to the device to request the compromised status
- D. Assign a compliance profile containing a single app payload for the Hub application

Correct Answer: C

QUESTION 3

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

Correct Answer: AD

QUESTION 4

Which combination of authentication challenges does an integration of RSA SecurID in Workspace ONE Access provide to protect resources?

- A. Password and PIN
- B. Password, PIN, and biometrics
- C. Password and biometrics
- D. Password, email, and biometrics

Correct Answer: B

Reference: <https://blogs.vmware.com/euc/2018/12/digital-workspace-rsa-securid.html>

QUESTION 5

What is the primary purpose of VMware Workspace ONE Trust Network in VMware Workspace ONE Intelligence?

- A. Delivering VPN profiles to devices
- B. Assisting with integration of the Multi-Domain directory services across a trusted network
- C. Integrating threat data from security solutions, including endpoint detection and response (EDR) solutions
- D. Providing applications to end users

Correct Answer: C

Reference: <https://www.vmware.com/products/workspace-one/intelligence.html#:~:text=Workspace%20ONE%20Trust%20Network%20is,security%20posture%20in%20the%20organization>