

VMware Workspace ONE 21.X Advanced Integration Specialist

Exam Details (Last Updated: 01/09/2022)

The VMware Workspace ONE 21.X Advanced Integration Specialist exam (5V0-61.22) which leads to VMware Specialist - Workspace ONE 21.X Advanced Integration is a 60 item exam, with a passing score of 300 using a scaled method. Exam time is 105 minutes.

Exam Delivery

This is a proctored exam delivered through Pearson VUE. For more information, visit the [Pearson VUE website](#).

Certification Information

For details and a complete list of requirements and recommendations for attainment, please reference the [VMware Education Services – Certification website](#).

Minimally Qualified Candidate

The minimally qualified candidate (MQC) must have earned a VCP-DW certification. It is recommended the MQC have 1 or more years of experience working in an IT role with Windows and Linux servers. The MQC should have 1 or more years of experience configuring and managing UEM and Access. The MQC should have 1 or more years of experience working with mobile and desktop device operating systems. The MQC should have 1 or more years of experience working with network equipment. The MQC should have intermediate knowledge of device data, identity and access management solutions as well as basic knowledge of database technology and caching. The MQC should possess knowledge of the objectives shown in the exam sections in this guide.

Exam Sections

VMware exam blueprint sections are now standardized to the seven sections below, some of which may NOT be included in the final exam blueprint depending on the exam objectives.

- Section 1 – Architecture and Technologies
- Section 2 – Products and Solutions
- Section 3 – Planning and Designing
- Section 4 – Installing, Configuring, and Setup
- Section 5 – Performance-tuning, Optimization, and Upgrades
- Section 6 – Troubleshooting and Repairing
- Section 7 – Administrative and Operational Tasks

If a section does not have testable objectives in this version of the exam, it will be noted below, accordingly. The objective numbering may be referenced in your score report at the end of your testing event for further preparation should a retake of the exam be necessary.

Sections Included in this Exam

Section 1 - Architectures and Technologies

- Objective 1.1 - Outline various authentication methods and workflows that can be implemented to ensure a robust user experience, while meeting your security requirements
- Objective 1.2 - Summarize the integration workflow of Workspace ONE UEM with Workspace ONE Access
- Objective 1.3 - Illustrate an LDAP directory workflow
- Objective 1.4 - Explain how JIT provisioning works in Workspace ONE Access
- Objective 1.5 - Describe the topology of claim-based identity and access management
- Objective 1.6 - Summarize the workflow of OAuth 2.0 authentication for Web Applications
- Objective 1.7 - Summarize the workflow of OpenID Connect
- Objective 1.8 - Summarize the workflow of SAML authentication
- Objective 1.9 - Explain the workflow of the Kerberos authentication method
- Objective 1.10 - Explain the workflow of an access policy and identity provider
- Objective 1.11 - Outline other third-party virtual desktop infrastructures (VDI)
- Objective 1.12 - Describe the differences between Hub Services with or without an integrated Workspace ONE Access
- Objective 1.13 - Define risks and their mitigations - combine with HA DR
- Objective 1.14 - Discuss architecture design decision examples with justifications

Section 2 - VMware Products and Solutions

- Objective 2.1 - Explain the concept of conditional access
- Objective 2.2 - Explain the different use cases and supported features of Workspace ONE Access Connector
- Objective 2.3 - Identify the features and use cases of the AirWatch Provisioning app
- Objective 2.4 - Distinguish authentication methods available in the Workspace ONE Access (Connector, Cloud-based, 3rd party IDP)
- Objective 2.5 - Outline benefits of claims-based identity management
- Objective 2.6 - Describe the workflow of the password (cloud deployment) authentication method
- Objective 2.7 - Explain the workflow of the RADIUS (cloud deployment) authentication method
- Objective 2.8 - Illustrate the workflow of the RSA SecureID (cloud deployment) authentication method
- Objective 2.9 - Explain the authentication workflow of Mobile SSO for iOS
- Objective 2.10 - Explain the authentication of Mobile SSO for Android
- Objective 2.11 - Explain the authentication workflow of certificate cloud deployment
- Objective 2.12 - Describe the workflows of device compliance checking
- Objective 2.13 - Discuss the risk scoring feature with Workspace ONE Intelligence Risk Analytics

Objective 2.14 - Explain features and use cases of Workspace ONE Verify (Intelligent Hub)

Objective 2.15 - Explain how 3rd party integration works to connect and share data with Workspace ONE Intelligence

Objective 2.16 - Describe functionalities of Workspace ONE Intelligence (dashboards, automation, reports, etc.)

Objective 2.17 - Describe what Workspace ONE Intelligence Trust Network is and what third-party solutions are in the ecosystem

Objective 2.18 - Explain the steps to write a Workspace ONE Access API call

Objective 2.19 - Explain the required services for service integration (ENS, SEGV2, UAG, etc.)

Section 3 - Planning and Designing

Objective 3.1 - Outline Workspace ONE design methodology and how it can apply to your organization

Objective 3.2 - Identify benefits of integrating Workspace ONE Access with other Workspace ONE products

Objective 3.3 - Describe the relationship of Hub Services, Workspace ONE Intelligent Hub, Workspace ONE UEM and Workspace ONE Access

Objective 3.4 - Explain how to deploy Workspace ONE experience workflows according to a use case

Objective 3.5 - Discuss all third-party components that are required for infrastructure design

Section 4 - Installing, Configuring, and Setup

Objective 4.1 - Differentiate common authentication methods in Workspace ONE Access and select the most suitable method to fit your business needs

Objective 4.2 - Outline the workflow of integrating Workspace ONE Access with VMware Horizon

Objective 4.3 - Explain AD synchronization from Workspace ONE UEM and from the Workspace ONE Access connector

Objective 4.4 - Explain how to configure SCIM provisioning

Objective 4.5 - Distinguish the types of resources and how to configure them in the Workspace ONE Access catalog

Objective 4.6 - Describe the integration steps of a Virtual apps integration with Workspace ONE Access (Horizon, Citrix, etc.)

Objective 4.7 - Describe integration steps for Hub Services Features (Passport, Templates, Watson, etc.)

Objective 4.8 - Describe use-cases and steps to implement DEEM.

Objective 4.9 - Outline the steps of integrating a third-party solution with Workspace ONE Intelligence for data or automation

Objective 4.10 - Describe steps to create a remote app access client using Workspace ONE Access

Section 5 – Not Applicable Section 6 - There are no testable objectives for this section.

Section 7 - Administrative and Operational Tasks

Objective 7.1 - Discuss the usage of directory sync safeguards

Objective 7.2 - Explain how to perform general Workspace ONE UEM administration and maintenance through the API

Objective 7.3 - Explain how to perform general Workspace ONE Access administration and maintenance through the API

Recommended Courses

VMware Workspace ONE: Advanced Integration [21.X]

References

In addition to the recommended courses, item writers used the following references for information when writing exam questions. It is recommended that you study the reference content as you prepare to take the exam, in addition to the recommended training.

Name	Products
http://kb.vmware.com	VMware Workspace ONE 21.X
http://www.vmware.com	VMware Workspace ONE 21.X
https://blogs.vmware.com	VMware Workspace ONE 21.X
https://docs.vmware.com	VMware Workspace ONE 21.X
https://www.vmware.com/support/pubs	VMware Workspace ONE 21.X
https://www.vmware.com/techpapers.html	VMware Workspace ONE 21.X
http://pubs.vmware.com	VMware Workspace ONE 21.X

Exam Content Contributors

Ashley Frame
Benjamin Jacoby
Cameron Megaw
Jason Huang
Jiquing Xu
Mark Miller
Roy McCord



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com © 2022 VMware, Inc. All rights reserved. The product or workshop materials is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/download/patents.html>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware warrants that it will perform these workshop services in a reasonable manner using generally accepted industry standards and practices. THE EXPRESS WARRANTY SET FORTH IS IN LIEU OF ALL OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE INCLUDING IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE SERVICES AND DELIVERABLES PROVIDED BY VMWARE, OR AS TO THE RESULTS WHICH MAY BE OBTAINED THEREFROM. VMWARE WILL NOT BE LIABLE FOR ANY THIRD-PARTY SERVICES OR PRODUCTS IDENTIFIED OR REFERRED TO CUSTOMER. All materials provided in this workshop are copyrighted by VMware ("Workshop Materials"). VMware grants the customer of this workshop a license to use and make reasonable copies of any Workshop Materials strictly for the purpose of facilitating such company's internal understanding, utilization and operation of its licensed VMware product(s). Except as set forth expressly in the sentence above, there is no transfer of any intellectual property rights or any other license granted under the terms of this workshop. If you are located in the United States, the VMware contracting entity for the service will be VMware, Inc., and if outside of the United States, the VMware contracting entity will be VMware International Limited.