DUMPSARENA

# Workspace ONE Design and Advanced Integration Specialist

## VMware 5V0-62.19

**Version Demo**

**Total Demo Questions: 10**

**Total Premium Questions: 63**

**Buy Premium PDF**

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

## QUESTION NO: 1

What are three requirements for a device that is already joined to Azure AD to enroll into Workspace ONE UEM? (Choose three.)

**A.** No Azure AD account configured on the device.

**B.** Windows 10 OS build 14393.82 and above.

**C.** KB update KB3176934 installed.

**D.** No MDM managed.

**E.** User must be a member of the Console Admin Group.

**F.** Windows Update services not started.

## ANSWER: B C D

**Explanation:**

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1811/Workspace-ONE-UEM-Windows-Desktop-Device-Management/GUID-AWT-ENROLL-AADMANAGED.html

## QUESTION NO: 2

An administrator wants to integrate VMware Identity Manager as a Federated Identity Provider for AD FS.

Which two steps need to be completed? (Choose two.)

**A.** Configure VMware Identity Manager as a Service Provider for AD FS.

**B.** Create a VMware Identity Manager claims Provider Trust in AD FS.

**C.** Exchange the certificates between Workspace ONE IDM and the domain controllers.

**D.** Integrate Workspace ONE federated applications with AD FS.

**E.** Redirect mobile users to VMware Identity Manager for authentication.

## ANSWER: A B

**Explanation:**

Reference: https://docs.vmware.com/en/VMware-Identity-Manager/services/ workspaceone_adfs_integration/GUID-DC3E2A2A-3F29-4B9F-AC73-867EDF5EA6B2.html

## QUESTION NO: 3

An administrator wants to migrate a System Center Configuration Manager (SCCM) collection into a co-managed stage in Workspace One UEM. Workspace ONE AirLift does not display the collection as mapped.

What is most likely the issue?

**A.** The collection is mapped to the wrong API.

**B.** The collection mapping is removed or the migration is completed and the ConfigMgr collection is no longer used.

**C.** The collection mapping is busy or the migration is failed.

**D.** The collection has at least one Windows 10 device.

## ANSWER: B

**Explanation:**

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1909/ WS1_AirLift_Configuration.pdf (14)

## QUESTION NO: 4

What is the goal of Mobile SSO?

**A.** Log into services and apps, without a corporate VPN connection and without entering credentials.

**B.** Log into services and apps, without a corporate VPN connection and with entering appspecific credentials.

**C.** Log into services and apps, with a corporate VPN connection and without entering credentials.

**D.** Log into services and apps, with a corporate VPN connection and without entering appspecific credentials.

## ANSWER: D

**Explanation:**

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1908/iOS_Platform/ GUID-AWT-PROFILESSO.html

## QUESTION NO: 5

Which three enrollment options are supported with Workspace ONE and Azure AD? (Choose three.)

**A.** Only supported on Dell EMC devices.

**B.** Enroll through On-Premise Exchange.

**C.** Enroll through Out of Box Experience.

**D.** Enroll through Office 365 apps.

**E.** Enroll an Azure AD managed device into Workspace ONE UEM.

**F.** Enroll in the local AD and then sync to Azure AD.

**ANSWER: C D E**

**Explanation:**

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1810/Workspace-ONE-UEM-Windows-Desktop-Device-Management/GUID-AWT-ENROLL-CLOUD.html

## QUESTION NO: 6

Which settings need to be prepared when planning a Workspace ONE AirLift installation?

**A.** Identity Manager Tenant URL

**B.** IDP.XML

**C.** SSO Domain

**D.** System Center Configuration Manager (SCCM) Site Code

**ANSWER: D**

**Explanation:**

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1909/ WS1_AirLift_Configuration.pdf

## QUESTION NO: 7

Refer to the ACME Financials design use case.

ACME Financials Design Use Case

1. Introduction

1.1 Business Overview

ACME Financials is an investment firm that has established itself as a leader in USA's fast-moving financial asset management market and has around 1000 employees.

ACME plans to transform its end-user computing resources to the digital workspace. ACME wants a secure platform that is available from any device and from anywhere, as well as a solution that reduces operating costs.

ACME's major business driver for the digital workplace is to enable employees to work remotely, and to enable the secure access to all of its resources from anywhere and any device while enhancing security with multi-factor authentication. The solution should support its BYOD strategy and let remote employees use their own laptop, desktop, or mobile device to access the resources from any location.

ACME also wants to remove the need to supply and manage desktop hardware to external contractors. Because financial data is highly sensitive, the firm needs a technology that would protect customer and other critical information - even when accessed on a mobile device. ACME is looking to improve the security of the desktop and application platforms across the enterprise. In addition to using endpoint security tools and multi-factor authentication, ACME insists on using additional security and controls to provide the highest level of security and protection to services and applications.

ACME currently uses a VPN-based remote access solution. ACME would like to remove additional components that add support or management complexity, and device dependence for remote access users. ACME is looking to achieve the same access to virtual desktops and Windows 10 or mobile applications, both inside and outside of the ACME enterprise network.

ACME is very keen on enforcing standardization to keep the IT infrastructure as consistent as possible. IT wants to use standardized versions of Windows (Windows 10), consistent configurations, and application delivery from a central source. All while maintaining the compliance of every device that requires encryption, password and PIN protection, as well as update -and anti-virus control.

To simplify and standardize desktop and application delivery, ACME wants to offer a service catalog based approach based on ACME IT standards. This will allow ACME to effectively deliver and manage resources, allowing IT to deliver device and application services that meet business and technical needs, while maximizing the use of shared IT computing resources.

Additional Facts

- Speaking to the developers revealed that most apps are standardized apps from public appstores, but ACME uses some their in-house developed, critical mobile apps, where some of the developers have already left the company, so that they cannot be rewritten in a short amount of time.

- To reduce operating costs, ACME has already moved to Office 365 and is currently running a few migrations from on-premises to the cloud for other applications.

- ACME's IT says that it is a Microsoft Windows only shop, but the assessment shows that currently most of the managers are using Apple devices.

- ACME currently uses directory services and two-factor authentication mechanisms (Radius) for internal and external access. ACME requires to support Single Sign-On (SSO) integration with their current authentication solutions. They also require to use SSO whenever possible, as they do not believe in having multiple user accounts and passwords for their end users. - ACME wants the solution to provide mechanisms to provide a secure e-mail solution to any device that complies to global security standards even for BYO devices.

1.2 High Level User Classification

- 680 Office workers (call center, corporate and office administrators) use standardized PCs or Thin-Clients to access ACMEs core apps and tools.

- 240 Remote-office workers use the company's CYOD initiative and use these devices (Notebooks, Convertibles, Tablets, Android phones) to access their apps and tools from remote.

- 30 Executives use Apple Mac Books as well as iPhones and iPads to work on- and offpremises.

- 80 IT -admins and software developers are using high-end workstations with administrative access.

1.3 High Level Application Assessment

- ACME currently has 261 applications, of which 186 are based on Microsoft Windows.

- Today, users are allocated applications via AD group membership.

- 75 applications are either web-based or SaaS-based, including Office 365.

- A major incident recently meant sales workers were disappearing suddenly along with their data and laptops on some new colonies.

- Any external access should require multi-factor authentication. Access from the internal network should work seamlessly with SSO for the core applications. High-security applications also require MFA from internal access.

- The address ranges of the HQ datacenter are as follows:

◦ 172.16.0.0/16 internal

◦ 80.34.57.20/21 external

2. Initial Stakeholder Interview Findings

In addition to the goals summarized in the previous section, the following are findings from initial interviews with the key stakeholders and an analysis of their service level agreements. 1. The design must use the F5 Loadbalancer and should be as redundant as possible.

2. Qualified IT personal is hard to find these days. If possible, reduce operational costs and try to automate or outsource basic IT-tasks.

3. ACME is very particular about meeting the go-live date. If there are unforeseen delays, the project may not be delivered for the required go-live date.

Which three are physical design requirements in the Workspace ONE UEM design for ACME

(Choose three.)

**A.** SAAS apps

**B.** Devices

**C.** Microsoft Storage Spaces

**D.** Switches and router

**E.** vSphere ESXi hosts

**F.** WEB apps

**ANSWER: B C D**

## QUESTION NO: 8

What are three prerequisites for Workspace ONE Airlift? (Choose three.)

**A.** PowerShell with Admin rights

**B.** RPC server access

**C.** Workspace ONE UEM v9.5 or later

**D.** System Center Configuration Manager (SCCM) 2012 R2

**E.** System Center Configuration Manager (SCCM) 2007 R2

**F.** Workspace ONE IDM 3.1 or later

**ANSWER: A C D**

**Explanation:**

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1907/

AirLift_Configuration/GUID-AWT-REQUIREMENTS-AIRLIFT.html

**QUESTION NO: 9**

An administrator configured Okta as an identity provider for Workspace ONE. Users complain that they still cannot authenticate via Okta.

What is most likely the issue?

**A.** The connector is down.

**B.** The Active Directory sync has failed.

**C.** The Okta IDP authentication method has not been selected in the access policies.

**D.** Okta authentication method for built-in identity providers is disabled.

**ANSWER: C**

**Explanation:**

Reference: https://help.okta.com/en/prod/Content/Topics/device-trust/SAML/Mobile/configureokta-idp-vidm.htm

**QUESTION NO: 10**

What are the requirements to configure Kerberos for VMware Identity Manager?

**A.** Add the authentication method in Workspace ONE UEM.

**B.** Assign the user to the Active Directory group for Kerberos.

**C.** Enter the account attribute that contains the SID of the user.

**D.** Enable Windows Authentication.

**ANSWER: D**

**Explanation:**

Reference: https://docs.vmware.com/en/VMware-Identity-Manager/3.3/com.vmware.vidm-dmzdeployment/GUID-28F5A610-FD08-404D-AC4B-F2F8B0DD60E4.html