5V0-62.19^{Q&As}

VMware Workspace ONE Design and Advanced Integration Specialist

Pass VMware 5V0-62.19 Exam with 100% Guarantee

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

https://www.certbus.com/5v0-62-19.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

Which two are requirements for managing Microsoft Windows endpoints with Microsoft System Center Configuration Manager (SCCM) and Workspace ONE UEM? (Choose two.)

A. VMware Workspace ONE SCCM Integration client

B. Identity connector directly installed on the SCCM server

C. AirWatch 8.2 and higher

D. Directory Synchronization Server for SCCM

E. Windows 7 devices and newer

Correct Answer: AB

QUESTION 2

An administrator has created a new VMware Horizon desktop pool and added the entitlement within the Horizon Administrator. The Horizon environment is properly connected to VMware Identity Manager.

What are the next steps in the VMware Identity Manager admin console to make the desktop pool available to users?

A. There are no additional steps needed.

B. Create a new entitlement in the VMware Identity Manager.

C. Create a new assignment in the VMware Identity Manager.

D. Create a new entitlement in the VMware Workspace ONE UEM.

Correct Answer: C

Reference: https://docs.vmware.com/en/VMware-Horizon-7/7.9/horizon-console-administration.pdf

QUESTION 3

Which two authentication methods are for built-in identity providers? (Choose two.)

A. Device Compliance with Workspace ONE UEM

B. One Time Password (Local Directory)

C. Workspace ONE UEM External Access Token

D. Password using the Microsoft AD FS Connector

E. VMware Horizon for two-factor authentication

Correct Answer: AC

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-IDM-deploymentguide/ GUID-AD9A5715-C21B-4D54-A413-28980A70A4B4.html

QUESTION 4

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 app-stores, 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 ACME\\'s 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 off-premises.

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.

The design must use the F5 Loadbalancer and should be as redundant as possible.

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

outsource basic IT-tasks.

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.

What could be a business driver for ACME Financials to use Workspace ONE UEM?

A. Standardization of app and device controls.

B. Utilization of already owned apps and hardware.

C. Always use MFA for high-security apps.

D. Utilization of high-end workstations for administrators and developers.

Correct Answer: A

QUESTION 5

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 app-stores, 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 off-premises.

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.

The design must use the F5 Loadbalancer and should be as redundant as possible.

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

outsource basic IT-tasks.

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

Correct Answer: BCD

QUESTION 6

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.

Correct Answer: D

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

QUESTION 7

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

Correct Answer: ACD

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1907/AirLift_Configuration/GUIDAWT-REQUIREMENTS-AIRLIFT.html

QUESTION 8

Which authentication method needs to be configured when configuring Mobile SSO for Apple devices?

A. Mobile SSO (Android and IOS)

B. Mobile SSO (for IOS)

C. Mobile SSO

D. Mobile SSO (IOS and IPadOS)

Correct Answer: B

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-IDM-deploymentguide/GUID-3EC86F69-6F6E-4C48-A5D9-F319562B6B9C.html

QUESTION 9

What are two prerequisites for using Workspace ONE and Azure AD? (Choose two.)

A. Azure AD will not work as an identity source.

B. Azure AD integration with Workspace ONE UEM must be configured at the tenant where Active Directory is configured.

C. The administrator must have a Premium Azure AD P1 or P2 subscription.

D. The administrator must have a Basic Azure AD subscription.

E. An Azure AD trusted certificate is needed.

Correct Answer: BC

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/9.4/vmware-airwatch-guides-94/ GUID-AW94-Enroll_ConfigAADServices.html

---

QUESTION 10

An administrator wants to add Okta as a new Identity Provider.

Which two pieces of information are needed to enter in the New Identity Provider page? (Choose two.)

A. SAML AuthN Request Binding

B. Binding Certificate

C. Connector association

D. Connector Metadata

E. Authentication Methods

Correct Answer: DE

QUESTION 11

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.

Correct Answer: C

Reference: https://help.okta.com/en/prod/Content/Topics/device-trust/SAML/Mobile/configure-okta-idpvidm.htm

---

QUESTION 12

An administrator receives the following error message:

"404.idp.not.found"

Which authentication method change needs to be completed?

A. Navigate to the access policy rule settings, then select an authentication method that is passive.

B. Okta has to be configured as a third-party IDP.

C. Navigate to the access policy rule setting, then select an authentication method that is active and current.

D. AD FS has to be configured as a third-party IDP.

Correct Answer: C

Reference: https://docs.vmware.com/en/VMware-Identity-Manager/services/
workspaceone_adfs_integration/GUID-1B280F57-A89E-483F-A5B8-FCC39C7EBD7F.html

QUESTION 13

Which two options are available as SSO configuration for a third-party identity provider? (Choose two.)

A. Users get redirected to a customized endpoint URL.

B. If the third-party identity provider supports SAML-based single logout protocol (SLO), users are logged out of both sessions.

C. The user needs to close the browser session.

D. Users get logged out of their Workspace ONE portal and redirected to a customized endpoint URL.

E. If the third-party identity provider does not support logout, the provider is not supported by Workspace ONE.

Correct Answer: BD

Reference: https://docs.vmware.com/en/VMware-Identity-Manager/services/
IDM_service_administration_cloud/GUID-0C459D5A-A0FF-4893-87A0-10ADDC4E1B8D.html

QUESTION 14

What statement is true about OAuth2?

A. It is lighter than SAML, it is XML-based rather than JSON.

B. It is heavier than SAML, it is JSON-based rather than XML.

C. It is lighter than SAML, it is JSON-based rather than XML.

D. It is heavier than SAML, it is XML-based rather than JSON.

Correct Answer: C

QUESTION 15

What are two prerequisites for VMware Identity Manager as the Default Claims Provider for an application that is joined using AD FS? (Choose two.)

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

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

C. Exchange the HTTPS certificate between AD FS and Identity Manager.

D. Create a AD FS Claims Provider Trust in VMware Identity Manager.

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

Correct Answer: BE

Reference: https://docs.vmware.com/en/VMware-Identity-Manager/services/
workspaceone_adfs_integration/GUID-6E9EC5E1-3AD3-429B-86F6-DCB776A87655.html

5V0-62.19 Practice Test   5V0-62.19 Study Guide   5V0-62.19 Exam Questions