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.leads4pass.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

SATISFACTION GUARANTEED 100% SATISFACTION GUARANTEED

QUESTION 1

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

QUESTION 2

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 3

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 4

Which parameters are needed to enter an OpenID Connect/OAuth 2.0 Connect Application?

A. Target URL, provider URL, client ID, and client secret

B. Target URL, redirect URL, client ID, and client secret

C. Server URL, redirect URL, provider ID, and client secret

D. Server URL, redirect URL, client ID, and client secret

Correct Answer: B

Reference: https://docs.vmware.com/en/VMware-Identity-Manager/3.2/com.vmware.wsp-resource/GUID8B97BC55-7A6C-4F52-9F68-EC486A4241B7.html

QUESTION 5

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 6

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.

Which component needs to be implemented if ACME wants to a seamlessly login into the Horizon View Desktop when accessing it externally with a certificate-based authentication?

A. True SSO

B. Security Server

C. Provisioning Server

D. Integration Broker

Correct Answer: A

Reference: https://docs.vmware.com/en/VMware-Horizon-7/7.9/horizon-administration/GUID-7314E2AF2DA0-4BD0-939D-F5F352B3EEE0.html

QUESTION 7

Which two are possible authentication methods for a third-party integrated Identity Provider (iDP)? (Choose two.)

A. Device-based certificate

B. Windows authentication

C. PIN code

D. SAML password

E. SAML-based certificate

Correct Answer: BD

Reference: https://techzone.vmware.com/configuring-ad-fs-third-party-idp-vmware-identity-managervmware-workspace-one-operational-tutorial#266138

QUESTION 8

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.

Which two processes or actions can be used to test the correct functionality of the ACME infrastructure? (Choose two.)

A. Start an app where SSO should work and the user will be logged in.

B. Enroll an IOS device in the ACME environment.

C. Start the already deployed VPN client and access an internal website.

D. For security reason, the administrator has a user enter their credential multiple times.

E. Start any corporate app on any mobile phone.

Correct Answer: AB

QUESTION 9

Whet are two supported configurations for Windows Auto Discovery Service? (Choose two.)

A. Requiring installation on an on-premises and cloud deployment.

B. Enabling Workplace Web Enrollment for Windows Phone 8.

C. Windows Phone and Windows Desktop Simplified Enrollment.

D. Leveraging Server Name Indication (SNI) to support multiple domains.

E. Using Workspace ONE UEM Auto-Discovery to return User ID.

Correct Answer: DE

QUESTION 10

What is required in a multi-Office 365 domain environment?

A. The domains must not have been federated.

B. It is not supported.

C. Enter the domain ID for the specific domains in ActiveLogOnUri.

D. Open a support ticket with Microsoft to have the setting enabled.

Correct Answer: B

QUESTION 11

An administrator plans to create a staged enrollment of devices in Workspace ONE UEM.

What is a possible solution that enables the administrator to onboard devices one department after another?

A. Device Restriction Policy

B. Restrict enrollment to Configured Groups

C. Restrict enrollment to Assignment Groups

D. Access Policy

Correct Answer: B

QUESTION 12

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 13

Which list of Okta apps that are supported for an Okta integration into VMware Workspace ONE Identity Manager is the most complete?

A. SAML 2.0, WS-Federation, OpenID Connect, Bookmark

B. SAML 1.x, SAML 2.0, WS-Federation, OpenID Connect, Bookmark

C. SAML 1.x, SAML 2.0, WS-Federation, OpenID Connect

D. SAML 2.0, WS-Federation, OpenID Connect

Correct Answer: A

QUESTION 14

An administrator is tasked to configure Okta as an Identity Provider for Workspace ONE.

What is the correct order of implementation?

A. Add a Connector, create a third-party IDM in Workspace ONE, and create SAML app in Okta.

B. Create SAML App in Okta, configure Routing Rules, and create a third-party IDP in Workspace ONE.

C. Gather Service Provider Metadata from Identity Manager, create SAML App in Okta, and create a third-party IDP in Workspace ONE.

D. Create a third-party IDP in Workspace ONE, gather Service Provider Metadata from Identity Manager, and create SAML App in Okta.

Correct Answer: B

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/ workspaceone_okta_integration.pdf

QUESTION 15

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 3176934 installed.

D. No MDM managed.

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

F. Windows Update services not started.

Correct Answer: BCD

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

5V0-62.19 Practice Test 5V0-62.19 Exam Questions 5V0-62.19 Braindumps