5V0-62.19Q&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.pass4itsure.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

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.

ACME requires multi-factor authentication for application access from external networks. This has been

established with a default access policy that incorporates multi-factor authentication. However, some users complain that they do not want to enter the multi-factor authentication when accessing the applications from within the company network.

How can the user experience be improved?

A. Create an access policy that excludes internal users.

B. Create an access policy that does not require multi-factor authentication when accessing from LAN.

C. Create an access policy with a network range of 80.34.57.20/21 that does not require multi-factor authentication.

D. Create an access policy with a network range of 172.16.0.0/16 that does not require multi-factor authentication.

Correct Answer: A

QUESTION 2

An architect is planning for a cloud-hosted implementation of VMware Identity Manager to integrate with an existing implementation of Workspace ONE UEM. The solution will include the following authentication methods:

Username/Password (Cloud Deployment)

VMware Verify

RADIUS (Cloud Deployment)

Device Compliance

Workspace ONE UEM is also cloud hosted, however, the Active Directory and RADIUS servers are deployed on-premises.

Which two design elements are required to ensure all authentication methods are highly available? (Choose two.)

A. IdP Hostname set to load-balancer FQDN

B. Connectors configured for Legacy Mode

C. Enable Redirect configured on each Connector

D. Associate connectors with Build-In IdP

E. Enable authentication methods on all connectors

Correct Answer: CD

Reference: https://docs.vmware.com/en/VMware-Identity-Manager/services/vidm_cloud_deployment.pdf

QUESTION 3

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 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.

An administrator is tasked with the creation of the logical design for the e-mail flow.

Which two components are needed in the design? (Choose two.)

A. Microsoft Powershell Host

B. VMware SEG

C. Microsoft Cloud Connector Server

D. Active Directory Sync Host

E. Microsoft Certificate Authority

Correct Answer: BE

QUESTION 5

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 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.

ACME continues to use directory services for authentication.

Which two ports are needed to be accessed from the Cloud Connector to the Workspace ONE UEM

console server? (Choose two.)

A. TCP 2195

B. UDP 443

C. TCP 80

D. UDP 22

E. TCP 443

Correct Answer: CE

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1902/UEM_-Recommended_Architecture/GUID-AWT-NETWORKREQS.html

QUESTION 7

An administrator wants to add the Workspace ONE Identity Manager as an Identify Provider in Okla. What is the correct entityID (Issuer URI)?

A. https://tenant.vmwareidentity.com/SAAS/API/1.0/GET/metadata/idp.xml

B. https://tenant.vmwareidentity.com/API/1.0/GET/metadata/sp.xml

C. https://tenant.vmwareidentity.com/SAAS/API/1.0/GET/metadata/sp.xml

D. https://tenant.vmwareidentity.com/API/l.0/GET/metadata/idp.xml

Correct Answer: C

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/ workspaceone_okta_integration/GUID-BC206856-8BF4-4CE7-BBA2-9650971ABA23.html

QUESTION 8

What is required to configure VMware Horizon View to connect to VMware Identity Manager?

A. Add a SAML connector.

B. Add a OAUTH2 connector.

C. Add a SAML authenticator.

D. Add a OAUTH2 authenticator.

Correct Answer: C

Reference: https://docs.vmware.com/en/VMware-Identity-Manager/services/workspace-air-resource.pdf

QUESTION 9

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 10

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 11

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 12

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.

After the successful deployment of Workspace ONE, ACME plans to move their virtual desktop infrastructure to Horizon on AWS. But there are still Web apps and file services which will run in the on-premises datacenter.

Which two components are still needed in the on-premises datacenter? (Choose two.)

A. Content gateway

B. PowerShell host for e-mail

C. Layer 2 connection between Horizon on AWS on the ACME datacenter

D. AWS Storage

E. Identity bridging

Correct Answer: CE

QUESTION 13

Which two components can be shared across Workspace ONE, Workspace ONE UEM and VMware Horizon? (Choose two.)

A. Horizon True SSO Server

B. Universal Access Gateway (UAG)

C. Workspace ONE Identity Manager Connector

D. Microsoft Sharepoint Services

E. Microsoft Remote Desktop License Server

Correct Answer: BC

QUESTION 14

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 15

Which tasks need to be completed before a third-party identity provider instance can be added in Workspace ONE?

A. Configure the Metadata on the third-party side to match Workspace ONE.

B. Verify that the third-party instances is SAML 1.0 compliant.

C. VMware Identity Manager service must reach the third-party instance.

D. Verify that the third-party instances is REST compliant.

Correct Answer: C

Reference: https://docs.vmware.com/en/VMware-Identity-Manager/services/ IDM_service_administration_cloud/GUID-C04AED8C-0D84-4DA6-A6DA-8DCBC8341E6E.html