5V0-62.19.VCEplus.premium.exam.63q

Number: 5V0-62.19
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

5V0-62.19

VMware Workspace ONE Design and Advanced Integration Specialist

Version 1.0

Exam A

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.

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 key use case requires VMware Identity Manager?

A. SSO authentication because they do not want to have to log-in multiple times
B. SSO authentication to SaaS Apps with multiple logins for security
C. SSO-based VPN with SSL-based authentication
D. Active Directory NTLM authentication

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2 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.

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

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3

The latest Configuration Service Provider (CSP) release by Microsoft might not always be visually available in Workspace ONE UEM to configure.

What should be used to create custom settings to distribute through Workspace ONE UEM if that is true?

A. Download the add-on from my.workspaceone.com.
B. Click the Update button in the Custom Settings profile.
C. Use the Device Description Framework.
D. Export them from GPO.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The latest Configuration Service Provider (CSP) release by Microsoft might not always be visually available in Workspace ONE UEM to configure. In this case, an admin can use Device Description Framework (DDF) to create custom settings to distribute through Workspace ONE UEM.

Reference: https://techzone.vmware.com/operational-tutorial-vmware-workspace-one-moving-windows-10-modern-management#897173

QUESTION 4

An administrator configured a Service Provider app to authenticate through SAML to the Service Provider from VMware Identity Manager (vIDM).

Where is the signing certificate?

A. vIDM admin console: Catalog/WebApps/Settings/SaasApps/SAML Metadata
B. vIDM app console: Identity and Access Management/Settings/WebApps//SaasApps/SAML Metadata
C. vIDM app console: Catalog/WebApps/Settings/SaasApps/SAML Metadata
D. vIDM admin console: Identity and Access Management/Settings/WebApps//SaasApps/SAML Metadata

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.okta.com/sites/default/files/Okta-3rd-Party-UEM-Interop_Workspace-ONE.pdf (34)

QUESTION 5
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
Section: (none)
Explanation

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

QUESTION 6
An architect is planning a design for a Workspace ONE deployment that will use Kerberos for integrated windows authentication. A requirement of the solution is that all authentication methods must be highly available.

Which two solution components are necessary to support the design requirement? (Choose two).

A. Connectors deployed behind load-balancer
B. Directory type must be set to Active Directory with IWA
C. IdP Hostname set to load-balancer FQDN
D. Redirect Host Name set to load-balancer FQDN
E. Connectors deployed in Outbound Mode

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 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 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.
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 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

Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Horizon-7/7.9/horizon-administration/GUID-7314E2AF-2DA0-4BD0-939D-F5F352B3EEE0.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
Section: (none)
Explanation

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

QUESTION 9 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
Section: (none)
Explanation

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

QUESTION 10 Which three steps need to be completed to configure Identity Bridging for an SAML application on the VMWare UAG? (Choose three.)

A. An identity provider is configured and the SAML metadata of the identity provider saved.
B. SAML responses from IDP to SP contain SAML assertions which have SAML attribute.
C. Configure a Web Reverse Proxy for Identity Bridging - Certificate to Kerberos.
D. Replace the UAG Certificate with the SAML Certificate.
E. Pin the UAG certificate to the SAML provider.
F. SAML responses are expected from IDP for multiple SAML attributes.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/Unified-Access-Gateway/3.4/com.vmware.uag-34-deploy-config.doc/GUID-B76AE223-2458-40C7-A563-4E544EAEC4F9.html

QUESTION 11 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.

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.

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12 An administrator is adding an SaaS app to authenticate using SAML.

Which file does the administrator need to collect?

A. Config files for adding the SaaS app in Workspace ONE UEM.
B. Within the VMware Identity Manager locate the Service Provider (SP) metadata, save it as sp.xml and import it in the Saas APP where the administrator needs it for the SAML authentication.
C. Within the VMware Identity Manager, locate the Identity Provider (IdP) metadata, save it as idp.xml (sample file name), import it in the Saas APP where the administrator needs it for the SAML authentication.
D. Backup configuration files.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
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.

Correct Answer: AB
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Identity-Manager/services/workspaceone_adfs_integration/GUID-DC3E2A2A-3F29-4B9F-AC73-867EDF5EA6B2.html

QUESTION 15 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.

Correct Answer: B
Section: (none)
Explanation

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

QUESTION 16
An administrator wants to entitle users for Okta applications that are integrated into VMware Workspace ONE Identity Manager. What needs to be configured?

A. Okta as an Built-in Service Provider
B. AD FS in VMware Identity Manager
C. Workspace ONE UEM integration in VMware Identity Manager
D. Okta application source in VMware Identity Manager

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/workspaceone_okta_integration/GUID-BBB3679E-13E2-46F3-8DB1-D0988A4E236E.html

QUESTION 17 The certproxy will be managed on which server when using
it on-premises?

A. The cert proxy settings must be configured on the Workspace ONE UEM Admin console to manage the Android Mobile SSO requests.
B. The cert proxy settings must be configured on the VMware Identity Manager in the appliance settings to manage the Android Mobile SSO requests.
C. The cert proxy settings must be configured on the Workspace ONE UEM Self Service portal to manage the Android Mobile SSO requests.
D. The cert proxy settings must be configured on the VMware UAG admin console to manage the Android Mobile SSO requests.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1_android_sso_config/GUID-1E5128A5-1394-4A50-8098-947780E38166.html

QUESTION 18
Which Workspace ONE Android app is needed for Mobile SSO for Android?

A. VMware Tunnel configured with the Cloud Tunnel component installed.
B. VMware Tunnel configured with the Device Tunnel component installed.
C. VMware Tunnel configured with the User Tunnel component installed.
D. VMware Tunnel configured with the Per-App Tunnel component installed.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1_android_sso_config.pdf (p.9)

QUESTION 19 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.

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.

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
Section: (none)
Explanation

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

QUESTION 20 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21 What is used by the Mobile SSO for Android?

A. Cloud KDC
B. HTTPS proxy
C. IPSec
D. ServiceProvider Idp certificate

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23 Which two steps must be fulfilled to enable Kerberos Constrained Delegation on the SEGv2? (Choose two.)

A. Upload the Offline Root CA Certificate to the SEG v2.
B. Verify that the SEG Server is able to connect to the domain controller through Port 80.
C. Join the SEGv2 to the Active Directory.
D. Enable Require Client Certificate.
E. Enter Target SPN in HTTP/{exchangeName} format.

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/9.7/kerberos-constrained-delegation-authentication-for-seg-v2.pdf

QUESTION 24 What will the collection in System Center Configuration Manager (SCCM) be mapped to in Workspace ONE UEM?

A. Tenant
B. User Group
C. API user
D. Smart Group

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 25 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
Section: (none)
Explanation
Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Identity-Manager/3.2/com.vmware.wsp-resource/GUID-8B97BC55-7A6C-4F52-9F68-EC486A4241B7.html

QUESTION 26
What are three system requirements before beginning the Workspace ONE and Active Directory Federation Services integration? (Choose three.)

A. Active Directory Integration
B. Enterprise Integration Service
C. Microsoft Active Directory Federation Services administrator role
D. VMware Identity Manager using VMware Identity Manager connector
E. Ensure the same users is synced only to Active Directory Federation Services
F. A VMware Identity Manager tenant with user role

Correct Answer: CDF
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Identity-Manager/services/workspaceone_adfs_integration/GUID-8A111967-D3AB-49F7-8139-27EAC5C28A4A.html

QUESTION 27 Which two steps must be fulfilled to enable Kerberos Constrained Delegation on the SEGv2? (Choose two.)

Given the following list of features and functions:

1: Synchronizes System Center Configuration Manager (SCCM) and Workspace ONE
2: Enables mapping between SCCM device collections and Workspace ONE UEM smart groups
3: Provides detailed logs
4: Creates SCCM deployments to enable Workspace ONE device enrollment

What is a complete list that Workspace ONE AirLift provides?

A. 1, 2, 4
B. 1, 2
C. 1, 2, 3, 4
D. 2, 4

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Reference: https://techzone.vmware.com/sites/default/files/resource/modernizing_windows_10_management_vmware_workspace_one_operational_tutorial.pdf (15)

QUESTION 28

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
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Identity-Manager/services/IDM_service_administration_cloud/GUID-0C459D5A-A0FF-4893-87A0-10ADDC4E1B8D.html **QUESTION 29** 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which two application permissions are required to be set in Azure AD to integrate Identity Services in Workspace ONE UEM? (Choose two.)

A. Request certificates on behalf of the user
B. Read and write directory data
C. Register devices
D. Issue Certificates
E. Read and write devices

Correct Answer: BE
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1908/Application_Management_Windows/GUID-AWT-ENROLL-CONFIGAADSERVICES.html

QUESTION 31 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 app-specific 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 app-specific credentials.

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 32 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.

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.

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33 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.

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 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34 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
Section: (none)
Explanation

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

QUESTION 35
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
Section: (none)
Explanation

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

QUESTION 36
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
Section: (none)
Explanation

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

QUESTION 37 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
Section: (none)
Explanation

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

QUESTION 38 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39 What are three requirements before beginning work on a VMware Workspace ONE and Okta Integration? (Choose three.)

A. An Okta tenant: Role required: System or Console Administrator
B. A Workspace ONE UEM tenant: Role required: Console Administrator
C. A VMware Identity Manager tenant: Role required: System Administrator
D. A VMware Identity Manager tenant: Role required: Console Administrator

E. An Okta tenant: Role required: Super or Org Administrator
F. A Workspace ONE UEM tenant: Role required: System Administrator

Correct Answer: CEF
Section: (none)
Explanation

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

QUESTION 40 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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
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
Section: (none)
Explanation

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

QUESTION 42 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
Section: (none)
Explanation

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

QUESTION 43 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
Section: (none)
Explanation

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

QUESTION 44
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
Section: (none)
Explanation

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

QUESTION 45 What are two prerequisites to integrate Ping into VMware Workspace ONE? (Choose two.)

A. PingFederate must have Service Provider role enabled.
B. PingFederate must have remote authentication enabled.
C. PingFederate must be enabled as remote IdP.D. PingFederate must be enabled as Built-in IdP.
E. PingFederate must have Identity Provider role enabled.

Correct Answer: AE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46 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.

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.

There is a requirement of having F5 as a primary load balancer.

Which two components are part of the logical design behind the load balancer? (Choose two.)

A. Secure E-Mail Gateway (SEG)
B. Workspace ONE UEM Device Servers
C. VMware Universal Access Gateway (UAG)
D. Active Directory Domain Controllers
E. VMware NSX Manager

Correct Answer: DE
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
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
Section: (none)
Explanation

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

QUESTION 48 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
Section: (none)
Explanation

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

QUESTION 49 Which certificate is needed during profile configuration when configuring an iOS Mobile SSO profile within Workspace ONE UEM?

A. The Workspace ONE UEM Device root certificate
B. KDC certificate
C. Valid Webserver certificate from a Devices Server
D. APNS certificate

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

Reference: https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-IDM-deploymentguide/GUID-61B2CB4F-EA72-4D9C-BF1C-5A80A73263D0.html

QUESTION 50
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

Correct Answer: D
Section: (none)
Explanation

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

QUESTION 51
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.

Correct Answer: BCD
Section: (none)
Explanation

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

QUESTION 52 What is the purpose of network ranges in conditional access policies?

A. Network ranges are a fallback authentication method for an application.
B. Network ranges limit access to an application depending of the source IP address.
C. All applications are using the new network range by default.
D. Network ranges limit access to an application depending of the destination IP address.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1810/VMware-Workspace-ONE-UEM-Mobile-Application-Management/GUID-AWT-AP-ADD-NETWORKRANGE.html

QUESTION 53 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.
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.

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
Section: (none)
Explanation
Explanation/Reference:

QUESTION 54
What needs to be configured in VMware Identity Manager to access the applications or desktop externally when implementing Horizon in Workspace ONE?

A. Client Access URLs
B. Entitlement
C. Pod Federation
D. Catalog Item

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference: https://docs.vmware.com/en/VMware-Horizon-7/7.9/horizon-console-administration/GUID-71DC2C64-176C-4A2B-A681-93FE6B41DDCC.html

QUESTION 55
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56 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.

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.

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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
What are two prerequisites for the integration of Office 365 in VMware Workspace ONE? (Choose two.)

A. Attributes sAMAccountName and object GUID or sourceAnchor enabled
B. Attributes userPrincipalName and object GUID or sourceAnchor enabled

C. Microsoft Office 365 Business Premium account
D. Certificate from Microsoft Office 365
E. PowerShell 1.0 installed on the Windows server

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:
Reference: https://www.vmware.com/pdf/vidm-office365-saml.pdf (12)

QUESTION 58 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.

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.

What are three required components in the logical design? (Choose three.)

A. VMware Universal Access Gateways (UAG)
B. Airwatch Cloud Connector
C. Secure e-mail gateway
D. Microsoft Exchange Server
E. Microsoft System Center Virtual Machine Manager

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59 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
Section: (none)
Explanation

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

QUESTION 60 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.

Correct Answer: CDE
Section: (none)
Explanation

Explanation/Reference:

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

QUESTION 61
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
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62 An administrator wants to configure Okta as the Service Provider for Workspace ONE. Which metadata needs to be provided?
(Choose two.)

A. Service Provider (SP) metadata B.
Network Range
C. Identity Provider (IdP) metadata
D. Signing Certificate
E. Authentication Type

Correct Answer: AD
Section: (none)
Explanation

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

QUESTION 63 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
Section: (none)
Explanation

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