Question: 1

Refer to the ACME Financials design use case.
ACME Financials Design Use Case
1. Introduction
1.1 Business Overview
ACME Financials is an investment firm that has established itself as a leader in USA's fast-moving financial asset management market and has around 1000 employees.
ACME plans to transform its end-user computing resources to the digital workspace. ACME wants a secure platform that is available from any device and from anywhere, as well as a solution that reduces operating costs.
ACME's major business driver for the digital workplace is to enable employees to work remotely, and to enable the secure access to all of its resources from anywhere and any device while enhancing security with multi-factor authentication. The solution should support its BYOD strategy and let remote employees use their own laptop, desktop, or mobile device to access the resources from any location.
ACME also wants to remove the need to supply and manage desktop hardware to external contractors. Because financial data is highly sensitive, the firm needs a technology that would protect customer and other critical information - even when accessed on a mobile device. ACME is looking to improve the security of the desktop and application platforms across the enterprise. In addition to using endpoint security tools and multi-factor authentication, ACME insists on using additional security and controls to provide the highest level of security and protection to services and applications.
ACME currently uses a VPN-based remote access solution. ACME would like to remove additional components that add support or management complexity, and device dependence for remote access users. ACME is looking to achieve the same access to virtual desktops and Windows 10 or mobile applications, both inside and outside of the ACME enterprise network.
ACME is very keen on enforcing standardization to keep the IT infrastructure as consistent as possible. IT wants to use standardized versions of Windows (Windows 10), consistent configurations, and application delivery from a central source. All while maintaining the compliance of every device that requires encryption, password and PIN protection, as well as update -and anti-virus control.
To simplify and standardize desktop and application delivery, ACME wants to offer a service catalog based approach based on ACME IT standards. This will allow ACME to effectively deliver and manage resources, allowing IT to deliver device and application services that meet business and technical needs, while maximizing the use of shared IT computing resources.
Additional Facts
• Speaking to the developers revealed that most apps are standardized apps from public app-stores, but ACME uses some their in-house developed, critical mobile apps, where some of the developers have already left the company, so that they cannot be rewritten in a short amount of time.

• To reduce operating costs, ACME has already moved to Office 365 and is currently running a few migrations from on-premises to the cloud for other applications.
• ACME's IT says that it is a Microsoft Windows only shop, but the assessment shows that currently most of the managers are using Apple devices.
• ACME currently uses directory services and two-factor authentication mechanisms (Radius) for internal and external access. ACME requires to support Single Sign-On (SSO) integration with their

current authentication solutions. They also require to use SSO whenever possible, as they do not believe in having multiple user accounts and passwords for their end users.
• ACME wants the solution to provide mechanisms to provide a secure e-mail solution to any device that complies to global security standards even for BYO devices.

1.2 High Level User Classification

• 680 Office workers (call center, corporate and office administrators) use standardized PCs or Thin-Clients to access ACME's core apps and tools.
• 240 Remote-office workers use the company's CYOD initiative and use these devices (Notebooks, Convertibles, Tablets, Android phones) to access their apps and tools from remote.
• 30 Executives use Apple Mac Books as well as iPhones and iPads to work on- and off-premises.
• 80 IT -admins and software developers are using high-end workstations with administrative access.

1.3 High Level Application Assessment

• ACME currently has 261 applications, of which 186 are based on Microsoft Windows.
• Today, users are allocated applications via AD group membership.
• 75 applications are either web-based or SaaS-based, including Office 365.
• A major incident recently meant sales workers were disappearing suddenly along with their data and laptops on some new colonies.
• Any external access should require multi-factor authentication. Access from the internal network should work seamlessly with SSO for the core applications. High-security applications also require MFA from internal access.

The address ranges of the HQ datacenter are as follows:
◦ 172.16.0.0/16 internal
◦ 80.34.57.20/21 external

2. Initial Stakeholder Interview Findings

In addition to the goals summarized in the previous section, the following are findings from initial interviews with the key stakeholders and an analysis of their service level agreements.
• The design must use the F5 Loadbalancer and should be as redundant as possible.
• Qualified IT personal is hard to find these days. If possible, reduce operational costs and try to automate or outsource basic IT-tasks.
• ACME is very particular about meeting the go-live date. If there are unforeseen delays, the project may not be delivered for the required go-live date.

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

Answer: A

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 ACME's core apps and tools.
• 240 Remote-office workers use the company's CYOD initiative and use these devices (Notebooks,

Convertibles, Tablets, Android phones) to access their apps and tools from remote.
• 30 Executives use Apple Mac Books as well as iPhones and iPads to work on- and off-premises.
• 80 IT -admins and software developers are using high-end workstations with administrative access.

1.3 High Level Application Assessment

• ACME currently has 261 applications, of which 186 are based on Microsoft Windows.
• Today, users are allocated applications via AD group membership.
• 75 applications are either web-based or SaaS-based, including Office 365.
• A major incident recently meant sales workers were disappearing suddenly along with their data and laptops on some new colonies.
• Any external access should require multi-factor authentication. Access from the internal network should work seamlessly with SSO for the core applications. High-security applications also require MFA from internal access.

The address ranges of the HQ datacenter are as follows:
◦ 172.16.0.0/16 internal
◦ 80.34.57.20/21 external

2. Initial Stakeholder Interview Findings

In addition to the goals summarized in the previous section, the following are findings from initial interviews with the key stakeholders and an analysis of their service level agreements.
• The design must use the F5 Loadbalancer and should be as redundant as possible.
• Qualified IT personal is hard to find these days. If possible, reduce operational costs and try to automate or outsource basic IT-tasks.
• ACME is very particular about meeting the go-live date. If there are unforeseen delays, the project may not be delivered for the required go-live date.

Which three are physical design requirements in the Workspace ONE UEM design for ACME (Choose three.)

A. SAAS apps
B. Devices
C. Microsoft Storage Spaces
D. Switches and router
E. vSphere ESXi hosts
F. WEB apps

Answer: B,C,D

Question: 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.
.certicationsbuzz.com
B. Click the Update button in the Custom Settings profile.
C. Use the Device Description Framework.

D. Export them from GPO.

Answer: C

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.

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

Answer: C

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.

Answer: C