CERT EMPIRE

Microsoft Fundamentals MS-900 Exam Questions

Total Questions: 400+
Demo Questions: 30
Version: Updated for 2025

Prepared and Verified by Cert Empire – Your Trusted IT Certification Partner

For Access to the full set of Updated Questions – Visit: MS-900 Exam Dumps by Cert Empire

Question: 1

A company plans to migrate to Microsoft 365. You need to advise the company about how Microsoft provides protection in a multitenancy environment. What are three ways that Microsoft provides protection? Each correct answer presents part of the solution.

A: Customer content at restis encrypted on the server by using BitLocker.

B: Microsoft Azure AD provides authorization and role based access control atthe tenantlayer.

C: Customer content at rest is encrypted on the server by using transportlayer security (TLS).

D: Microsoft Azure AD provides authorization and role based access control at the transportlayer.

E: Mailbox databases in Microsoft Exchange Online contain only mailboxes from a single tenant.

F: Mailbox databases in Microsoft Exchange Online contain mailboxesfrom multiple tenants.

Correct Answer:

A, B, F

Explanation:

Microsoft 365's multitenant architecture is secured through a defense-in-depth strategy. At the physical layer, customer data at rest on servers is encrypted using BitLocker volume-level encryption (A). At the identity and logical layer, each customer tenant is isolated within a dedicated Microsoft Azure Active Directory (Azure AD) container, which provides robust authorization and role-based access control (RBAC) to prevent cross-tenant access (B). The architecture itself is fundamentally multitenant, meaning resources such as Exchange Online mailbox databases are shared. These databases contain mailboxes from multiple tenants (F), but are protected by strict logical isolation at the application level, ensuring data from one tenant is inaccessible to another.

Why Incorrect Options are Wrong:

C: Transport Layer Security (TLS) is a protocol used to encrypt data in transit (over a network), not data at rest (stored on a server).

D: Microsoft Azure AD provides access control at the identity and application layer, not the transport layer, which handles data transmission protocols.

E: This describes a single-tenant model. The standard Microsoft 365 service is multitenant, where resources are shared to achieve economies of scale.

References:

1. Microsoft Learn. (2023). Data Encryption in Microsoft 365. "For data at rest, Microsoft 365 uses volume-level and file-level encryption. In Microsoft 365, BitLocker is used for volume-level encryption." This source also clarifies that TLS is used for data in transit, refuting option C.

2. Microsoft Learn. (2023). Isolation and access control in Microsoft 365. "Azure Active Directory (Azure AD) [...] provides the core directory and identity management capabilities for Microsoft 365. Each Microsoft 365 tenant is a unique, isolated container in Azure AD." This supports the role of Azure AD in providing tenant-layer isolation and access control.

3. Microsoft Learn. (2023). Tenant Isolation in Microsoft 365. "Microsoft 365 is a multi-tenant service, meaning that multiple customers' data may be stored on the same physical hardware. Microsoft 365 uses logical isolation to segregate each customer's data from the data of other customers." This confirms the multitenant nature of the service, including shared databases, as described in option F.

Question: 2

You are the Microsoft 365 administratorfor a company. Your company plans to open a new office in the United Kingdom. You need to provide penetration test and security assessmentreports (or the new office. Where can you locate the required reports?

A: Data Governance page of the Security and Compliance portal.

B: Compliance Manager page of the Services Trust portal

C: Data Loss Prevention page of the Security and Compliance portal

D: Regional Compliance page of the Services Trust portal

Correct Answer:

D

Explanation:

The Microsoft Service Trust Portal is the central repository for obtaining documentation related to Microsoft's security, privacy, and compliance. It provides access to a wide range of resources, including independent third-party audit reports (like SOC and ISO), penetration test results, and security assessments. The Regional Compliance section of the portal specifically details how Microsoft cloud services comply with the laws, regulations, and standards of various countries and regions, such as the United Kingdom. This is the precise location to find the necessary reports for a new office in that region.

Why Incorrect Options are Wrong:

A: The Data Governance page is used for managing your organization's data lifecycle and retention policies, not for accessing Microsoft's internal compliance reports.

B: Compliance Manager is a tool to help your organization manage its own compliance activities and assess its compliance score, not a repository for Microsoft's audit documents.

C: The Data Loss Prevention (DLP) page is for configuring policies to prevent sensitive data from leaving your organization; it is unrelated to obtaining security reports.

References:

1. Microsoft Learn. (2024). Describe the Service Trust Portal and privacy at Microsoft. MS-900: Microsoft 365 Fundamentals. "The Service Trust Portal (STP) is a Microsoft public site for publishing audit reports and other compliance-related information... The STP includes... Penetration testing and security assessments... Country/region-specific and industry-specific compliance information."

2. Microsoft Learn. (2023). Get started with Microsoft Service Trust Portal. "The Service Trust Portal provides a variety of content, tools, and other resources about Microsoft security, privacy, and compliance practices... You can access audit reports from independent third parties... and information about how Microsoft's online services can help your organization maintain and track compliance with standards, laws, and regulations, such as... the United Kingdom's G-Cloud."

Question: 3

Your company has a Microsoft Office 365 subscription. As an administrator for this subscription, you have been tasked with recommending a solution that prohibits users from copying corporate information from managed applications installed on unmanaged devices. Which of the following should you recommend?

A: Windows Virtual Desktop.

B: Microsoft Intune.

C: Windows AutoPilot.

D: Azure AD Application Proxy.

Correct Answer:

B

Explanation:

Microsoft Intune is the correct solution as it provides Mobile Application Management (MAM) through App Protection Policies (APP). These policies are specifically designed to protect organizational data within an application, even on unmanaged devices (BYOD). An administrator can create a policy that restricts data transfer actions, such as "cut, copy, and paste," from a managed application (e.g., Microsoft Outlook) to an unmanaged application or the local device storage. This directly fulfills the requirement to prohibit users from copying corporate information from managed apps on unmanaged devices without needing to fully enroll the device.

Why Incorrect Options are Wrong:

A: Windows Virtual Desktop provides a full virtualized desktop experience. It is not a tool for managing applications and data on a user's local, unmanaged device.

C: Windows AutoPilot is a suite of technologies for setting up and pre-configuring new devices. It is not used for ongoing data protection on unmanaged devices.

D: Azure AD Application Proxy is used to publish on-premises web applications for secure remote access, not to control data within applications on client devices.

References:

1. Microsoft Learn. (2024). What is Microsoft Intune? "Microsoft Intune is a cloud-based endpoint management solution. It manages user access to organizational resources and

simplifies app and device management... You can also manage apps on devices not enrolled with Intune."

2. Microsoft Learn. (2024). App protection policies overview. "App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app... For example, you can restrict copy-and-paste and save-as functions." Section: How you can protect app data.

3. Microsoft Learn. (2023). MS-900: Describe modern management and deployment concepts in Microsoft 365. "Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM)." Module 4, Unit 3: Describe endpoint management capabilities with Microsoft Intune.

Question: 4

Your company intends to deploy a number of Microsoft Surface devices that run Windows 10, using Windows AutoPilot. You have been tasked with preparing the devices for the deployment by importing a CSV file via the Microsoft 365 Device Management portal. Which of the following combinations of blades will help you achieve your goal?

A: The Dashboard and Device Configuration blades.

B: The Device Enrollment and Devices blades.

C: The Device Enrollment and Devices Compliance blades.

D: The Device Compliance and Device Configuration blades.

Correct Answer:

B

Explanation:

To prepare devices for deployment using Windows Autopilot, an administrator must register the devices by importing a CSV file containing their hardware hashes. This process is initiated within the Microsoft Intune admin center. The administrator navigates to the main Devices blade, and from there, selects the Device Enrollment (or "Enroll devices") blade. Within the Windows enrollment section, the Autopilot devices can be imported. Therefore, the combination of the Device Enrollment and Devices blades is correct for performing this task.

Why Incorrect Options are Wrong:

A: The Dashboard provides an overview, and Device Configuration applies settings to already enrolled devices, not for the initial registration.

C: Device Compliance is used to set and check rules for enrolled devices, which is a post-enrollment activity, not the registration itself.

D: Both Device Compliance and Device Configuration are for managing devices after they are enrolled, not for preparing them for enrollment via Autopilot.

References:

1. Microsoft Learn. (2024). Manually register devices with Windows Autopilot. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/autopilot/add-devices. The procedure explicitly states to navigate to the Microsoft Intune admin center > Devices >

Windows > Windows enrollment > Devices (under Windows Autopilot Deployment Program) > Import. This path directly involves the Devices and Windows enrollment (Device Enrollment) sections.

2. Microsoft Learn. (2023). Windows Autopilot registration overview. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/autopilot/registration-overview. This document describes device registration as the first step in the Autopilot process, which is managed under the enrollment functions within Intune.

3. Microsoft Learn. (2024). What is Microsoft Intune? Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune. This documentation outlines the structure of the Intune admin center, differentiating between device enrollment functions and post-enrollment management tasks like configuration and compliance.

Question: 5

Your company has a Microsoft Office 365 subscription. As an administrator for this subscription, you are educating users on which component to use to register their personal home device with the company. Which of the following is the component that should be used?

A: Microsoft Azure AD Identity Protection

B: Enterprise Mobility + Security

C: Microsoft Teams

D: Microsoft Yammer

Correct Answer:

B

Explanation:

Enterprise Mobility + Security (EMS) is a suite of Microsoft products designed to help organizations manage and secure users, devices, applications, and data. A core component of EMS is Microsoft Intune, which provides mobile device management (MDM) and mobile application management (MAM). Intune is the specific service that enables users to register their personal devices (a "Bring Your Own Device" or BYOD scenario) with the company. This registration process allows administrators to enforce security policies and ensure that personal devices accessing corporate resources meet compliance requirements. Among the given options, EMS is the correct suite that contains the necessary device management capabilities.

Why Incorrect Options are Wrong:

A: Microsoft Azure AD Identity Protection: This service focuses on detecting, investigating, and remediating identity-based risks and vulnerabilities, not on registering or managing devices.

C: Microsoft Teams: This is a collaboration and communication platform for chat, meetings, and file sharing; it does not have device registration or management capabilities.

D: Microsoft Yammer: This is an enterprise social networking service for internal communication and does not include features for device management or registration.

References:

1. Microsoft Enterprise Mobility + Security Documentation. "What is Enterprise Mobility + Security (EMS)?" Microsoft Learn. This document outlines the components of EMS, stating, "Microsoft Intune is a cloud-based service that focuses on mobile device management (MDM) and mobile application management (MAM)." This directly connects the EMS suite to the task of managing devices.

2. Microsoft Intune Documentation. "What is Microsoft Intune?" Microsoft Learn. Section: "Manage devices". This document details how Intune allows organizations to manage devices, including personal devices, to control access to company data. It states, "In Intune, you can manage devices using an MDM approach... Users 'enroll' their devices and receive your rules and settings."

3. Microsoft Azure AD Identity Protection Documentation. "What is Identity Protection?" Microsoft Learn. This source defines Identity Protection as a tool for "automating the detection and remediation of identity-based risks," confirming its focus is on identity security, not device management.

Question: 6

Your company is planning to migrate to Microsoft Azure and Microsoft 365. You are required to identify a cloud service that allows for the deployment of a Linux virtual machine. Which of the following is the model you should choose?

A: Software as a Service (SaaS)

B: Platform as a Service (PaaS)

C: Infrastructure as a Service (IaaS)

D: Container as a Service (CaaS)

Correct Answer:

C

Explanation:

Infrastructure as a Service (IaaS) is the cloud service model that provides virtualized computing resources over the internet. This model offers the highest level of flexibility and management control over IT resources, which is most similar to traditional on-premises IT. IaaS allows you to rent IT infrastructure—servers (virtual machines), storage, and networking—from a cloud provider. The user is responsible for managing the operating system (such as Linux), applications, and data. Therefore, to deploy a Linux virtual machine, the IaaS model is the correct choice.

Why Incorrect Options are Wrong:

A: Software as a Service (SaaS): This model provides access to ready-to-use software applications, not the underlying infrastructure or operating system needed to deploy a custom VM.

B: Platform as a Service (PaaS): This model provides a platform for developing and deploying applications, but the cloud provider manages the operating system, abstracting it from the user.

D: Container as a Service (CaaS): This is a specialized service for deploying and managing containers (e.g., Docker), which are different from the full virtual machines specified in the question.

References:

1. Microsoft Learn. (2024). Describe cloud service types. MS-900: Describe cloud concepts. Microsoft. Retrieved from https://learn.microsoft.com/en-us/training/modules/describe-cloud-concepts/3-describe-cloud-service-types

Reference Details: In the "Infrastructure as a Service (IaaS)" section, it states, "The customer is responsible for everything else: operating system installation, configuration, and maintenance...". This confirms that IaaS is the model for deploying and managing an OS on a VM.

2. Microsoft Azure. (n.d.). What is IaaS? Infrastructure as a Service. Microsoft. Retrieved from https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-iaas/

Reference Details: The article defines IaaS: "Infrastructure as a service (IaaS) is an instant computing infrastructure, provisioned and managed over the internet... IaaS quickly scales up and down with demand, letting you pay only for what you use." It explicitly lists "Virtual machines" as a core component.

3. Microsoft Azure. (n.d.). Virtual Machines (VMs) for Linux and Windows. Microsoft. Retrieved from https://azure.microsoft.com/en-us/products/virtual-machines/

Reference Details: This official product page for Azure Virtual Machines, an IaaS offering, explicitly states, "Provision Windows and Linux virtual machines in seconds." This directly links the deployment of Linux VMs to the IaaS model in Azure.

Question: 7

Your company makes use of Platform as a Service (PaaS) for their Azure solution. Which of the following options are components that Microsoft are responsible for? (Choose all that apply).

A: Storage.

B: Databases.

C: Applications.

D: Operating system.

Correct Answer:

A, B, D

Explanation:

In the Platform as a Service (PaaS) cloud service model, the cloud provider (Microsoft) is responsible for managing the underlying infrastructure. This includes the physical datacenter, network, servers, and storage. Crucially for PaaS, Microsoft also manages the operating systems, middleware, and runtime environments. This allows customers to deploy and manage their applications without the complexity of building and maintaining the infrastructure and platform. Therefore, Microsoft is responsible for the storage infrastructure, the database platform (as a service), and the operating system. The customer remains responsible for their own applications and data.

Why Incorrect Options are Wrong:

C: Applications: In the PaaS model, the customer is responsible for developing, deploying, and managing their own applications and data that run on the platform.

References:

1. Microsoft Learn. "Shared responsibility in the cloud." Microsoft Cloud Adoption Framework for Azure. Accessed May 20, 2024. In the section "Shared responsibility model," the diagram clearly shows that for PaaS, the "Operating system," "Network controls," and underlying physical infrastructure including "Physical hosts" (which contain storage) are managed by the cloud provider.

2. Microsoft Learn. "What is Platform as a service (PaaS)?" Azure Fundamentals. Accessed May 20, 2024. This document states, "In a PaaS model, the cloud provider delivers and

manages the hardware and software infrastructure... This infrastructure includes middleware, development tools, business intelligence (BI) services, database management systems, and more." This confirms that databases and the underlying OS/storage are provider-managed.

Question: 8

You need to consider the underlined segment to establish whether it is accurate. All applications will remain in a hybrid environment after migrating to Microsoft Azure. Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A: No adjustment required.

B: Applications that manage sensitive information

C: Applications where access requires a USB-token device

D: All legacy applications

Correct Answer:

D

Explanation:

The original statement, "All applications will remain in a hybrid environment after migrating to Microsoft Azure," is inaccurate because it is an absolute generalization. Many applications can be, and are, fully migrated to the cloud. The most accurate replacement identifies the category of applications that are the most common reason for maintaining a hybrid environment.

Legacy applications are older systems that are often difficult to migrate to the cloud due to dependencies on outdated hardware, specific operating systems, or prohibitive costs and risks associated with modernization. Consequently, organizations often choose to keep these applications on-premises while integrating them with newer cloud services, which is the definition of a hybrid model. While not literally all legacy applications remain hybrid, they represent the primary and most significant category of applications that necessitate a hybrid approach.

Why Incorrect Options are Wrong:

A: No adjustment required. This is incorrect because the original statement is a false generalization. A primary goal of cloud migration is often to move applications entirely to the cloud, not keep them all hybrid.

B: Applications that manage sensitive information. This is incorrect because Microsoft Azure provides extensive compliance certifications and security services specifically designed to host applications with sensitive data, often making a full cloud migration possible and desirable.

C: Applications where access requires a USB-token device. This is incorrect as it describes a specific technical dependency. Such authentication methods can typically be modernized or replaced with cloud-native solutions like Azure AD Multi-Factor Authentication, enabling a full migration.

References:

1. Microsoft Learn, MS-900: Describe cloud concepts, "Describe the benefits and considerations of using cloud services." In the section describing the hybrid cloud model, it states: "A hybrid cloud is a computing environment that combines a public cloud and a private cloud by allowing data and applications to be shared between them... Some organizations may need to run legacy applications that can't be updated, so they run them on-premises." This directly identifies legacy applications as a key driver for the hybrid model.

2. Microsoft Azure Documentation, "What is Hybrid Cloud Computing?". This official document lists common hybrid cloud use cases. One of the primary use cases mentioned is "Legacy application migration," explaining that organizations can "keep the legacy application on-premises while connecting it to a cloud application or service." This reinforces that legacy applications are a principal reason for adopting a hybrid strategy.

Question: 9

You have recently made use of Windows Autopilot to deploy Windows 10 devices in your company's environment. You have been asked to make sure that data that stored in OneDrive for Business is available to users from remote locations. Solution: You enroll the devices in Microsoft Intune. Does the solution meet the goal?

A: Yes

B: No

Correct Answer:

B

Explanation:

The proposed solution does not meet the goal. OneDrive for Business is a cloud-based service that is part of Microsoft 365. By its nature, data stored in OneDrive is inherently accessible from any location with an internet connection, on any supported device with the appropriate credentials. Enrolling a device in Microsoft Intune is a device management action used to apply organizational policies and security settings; it does not enable the fundamental remote accessibility of the OneDrive for Business service itself.

Why Incorrect Options are Wrong:

A: Yes: This is incorrect because the remote availability of OneDrive data is an intrinsic feature of the cloud service, not a feature enabled by enrolling a device in Microsoft Intune.

References:

1. Microsoft Learn. (2024). What is OneDrive in Microsoft 365? Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/microsoft-365/admin/setup/what-is-onedrive-for-work-or-school.

Reference Point: The document states, "OneDrive is the Microsoft 365 files experience for your business. You can access and protect your business files from anywhere." This confirms that remote access is a core feature of the service itself.

2. Microsoft Learn. (2024). What is Microsoft Intune? Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune.

Reference Point: The "What is Intune?" section describes Intune as a cloud-based service focusing on mobile device management (MDM) and mobile application management

(MAM), used to "control how your organization's devices are used" and "manage apps." This shows its purpose is management, not enabling core service functionality like remote access.

Question: 10

Your company makes use of Microsoft 365 in their environment. You have been tasked with making sure that members of the Global Administrators group are protected. The feature you use should achieve this by making use of dynamic risk profiles. Which of the following is a feature you should use?

A: Mobile application protection policy.

B: Device configuration policy.

C: Microsoft Azure AD Privilege Identity Protection.

D: Microsoft Azure AD Conditional Access.

Correct Answer:

C

Explanation:

Azure AD Privileged Identity Protection (PIP) automatically assigns user-risk and sign-in-risk levels—calculated by Microsoft's machine-learning engine—to accounts holding privileged roles (Global Administrator, etc.). PIP lets you create risk-based policies (e.g., require MFA, block access) that are continuously and dynamically evaluated, precisely fulfilling the requirement to "protect members of the Global Administrators group … by making use of dynamic risk profiles."

Why Incorrect Options are Wrong:

Mobile application protection policies secure app data via Intune; they don't evaluate sign-in or user risk or target admin roles.

Device configuration policies manage device settings/compliance, not user risk or privileged-role protection.

Conditional Access can consume risk signals, but dedicated, out-of-the-box risk policies for privileged roles are delivered through PIP, making PIP the more specific solution.

References:

1. Microsoft, "Configure Azure AD Privileged Identity Protection policies," Section "Protected accounts," para 1-2 (docs.microsoft.com) – states Global Administrators are automatically in scope and protected by risk policies.

2. Microsoft, “What is Azure AD Privileged Identity Protection?” para 3-5 – describes dynamic user-risk/sign-in-risk calculation and policy enforcement.

3. Microsoft, “App protection policies overview,” Microsoft Intune docs, para 2 – outlines purpose limited to mobile app data.

4. Microsoft, “Create device configuration profiles,” Intune docs, para 1 – explains focus on device settings, not user risk.

5. Microsoft, “Conditional Access overview,” Section “Signals,” para 4 – shows CA consumes risk but lacks the privileged-account-specific presets provided by PIP.

Question: 11

You need to consider the underlined segment to establish whether it is accurate. You are a Microsoft 365 administrator for a company whose employees are allowed to access corporate information located in the cloud via their personal devices. You have been tasked with making sure that employees are prohibited from copying this information to their personal OneDrive folders. You should make use of Intune App Protection. Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A: No adjustment required

B: Information Rights Management

C: Microsoft Azure AD Privilege Identity Protection

D: Microsoft Azure AD Identity Protection

Correct Answer:

A

Explanation:

Intune App Protection Policies (APP) are the correct tool for this scenario. These policies apply data protection rules at the application level, which is ideal for Bring-Your-Own-Device (BYOD) environments where the organization manages the corporate apps but not the entire device. An administrator can configure an APP to prevent data relocation actions, such as using "Save as" to copy corporate data from a managed application (like a work version of OneDrive or Outlook) to an unmanaged, personal location (like a personal OneDrive folder) on the same device. This directly addresses the requirement to prohibit employees from copying corporate information to their personal folders.

Why Incorrect Options are Wrong:

B: Information Rights Management: IRM protects the data itself through encryption and access rights, but it does not directly prevent the file from being saved to a personal location.

C: Microsoft Azure AD Privilege Identity Protection: This service manages and monitors privileged administrative roles using just-in-time access. It is unrelated to data loss prevention on end-user devices.

D: Microsoft Azure AD Identity Protection: This tool focuses on detecting and remediating risks related to user sign-ins and identity compromise, not on controlling data flow within applications.

References:

1. Microsoft Learn. "App protection policies overview." Microsoft Intune documentation. "App protection policies (APP) are rules that ensure an organization's data remains safe or contained in a managed app... Data relocation policies include features that control how data can be moved between apps, such as restricting cut, copy, paste, and save-as."

2. Microsoft Learn. "What is Azure Information Protection (AIP)?" Microsoft Purview documentation. This document explains that AIP (which includes IRM) is about classifying and protecting documents and emails by applying labels, which can include encryption and content markings. This is distinct from controlling app behavior.

3. Microsoft Learn. "What is Privileged Identity Management?" Microsoft Entra documentation. "Privileged Identity Management (PIM) is a service in Microsoft Entra ID that enables you to manage, control, and monitor access to important resources in your organization."

4. Microsoft Learn. "What is Identity Protection?" Microsoft Entra documentation. "Identity Protection is a tool that allows organizations to... Automate the detection and remediation of identity-based risks... Investigate risks using data in the portal."

Question: 12

You need to consider the underlined segment to establish whether it is accurate. To ensure that when a new Microsoft Word feature is available for worker to install as soon as it becomes available, you should subscribe to the Targeted release channel. Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A: No adjustment required.

B: Standard release

C: Semi-annual

D: Annual

Correct Answer:

A

Explanation:

The "Targeted release" option is designed for organizations that want to receive the latest Microsoft 365 updates and features as soon as they are available, ahead of the general rollout. By subscribing to the Targeted release, administrators and specified users can preview new functionalities, test them, and prepare the rest of the organization before the features are deployed to everyone in the "Standard release" group. This directly matches the requirement to get a new feature as soon as it becomes available.

Why Incorrect Options are Wrong:

B: Standard release: This is the default, slower option where users receive updates only after they have been made generally available to all customers.

C: Semi-annual: This refers to the Semi-Annual Enterprise Channel for Microsoft 365 Apps, which is a much slower update cadence, releasing features only twice a year.

D: Annual: This is not a valid release cadence or channel name for Microsoft 365 feature updates.

References:

1. Microsoft Learn. (2024). Set up the Standard or Targeted release options in Microsoft 365. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/microsoft-365/admin/manage/release-options-in-office-365. In the "Targeted release" section, it

states, "With Targeted release, your users receive the latest updates and features as soon as they're available."

2. Microsoft Learn. (2024). Overview of update channels for Microsoft 365 Apps. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/deployoffice/updates/overview-update-channels. This document describes the Semi-Annual Enterprise Channel as providing new features "only a few times a year," which is not the fastest option.

Question: 13

Your company plans to acquire a Microsoft 365 subscription. One of the services included in the subscription is described as a cloud service that allows you to do the following: ✑ Store and protect files. ✑ Share files. ✑ Make use of an app or web-browser to access files from anywhere. ✑ Restore files to an earlier date and time. Which of the following is the service being described above?

A: Office 365 Pro Plus.

B: Microsoft Yammer.

C: Microsoft Office Delve.

D: Microsoft OneDrive for Business.

Correct Answer:

D

Explanation:

The service described is Microsoft OneDrive for Business. It is the core Microsoft 365 cloud storage service that allows users to store, protect, and share their files. It provides access to these files from anywhere via a web browser or dedicated applications. A key feature of OneDrive for Business is its robust version history and the "Files Restore" capability, which allows a user to restore their entire library to a previous point in time within the last 30 days, directly matching all the requirements listed in the question.

Why Incorrect Options are Wrong:

A: Office 365 Pro Plus (now Microsoft 365 Apps for enterprise) is the suite of desktop applications (Word, Excel, etc.), not the cloud storage service itself.

B: Microsoft Yammer is an enterprise social networking service for communication and community building, not a primary personal file storage and versioning platform.

C: Microsoft Office Delve is a content discovery tool that surfaces relevant files from other locations like OneDrive and SharePoint; it does not store the files itself.

References:

1. Microsoft Learn. (n.d.). What is OneDrive for work and school? Microsoft Docs. Retrieved from https://support.microsoft.com/en-us/office/what-is-onedrive-for-work-and-school-

187f90af-056f-47c0-9656-cc0ddca7fdc2. (This source states, "OneDrive...is the Microsoft cloud service that connects you to all your files. It lets you store and protect your files, share them with others, and get to them from anywhere on all your devices.")

2. Microsoft Learn. (n.d.). Restore your OneDrive. Microsoft Docs. Retrieved from https://support.microsoft.com/en-us/office/restore-your-onedrive-fa231298-759d-41cf-bcd0-25ac53eb8a15. (This document details the "Files Restore" feature, which allows users to "restore your entire OneDrive to a previous time.")

3. Microsoft Learn. (2023, December 13). Overview of Microsoft 365 Apps for enterprise. Microsoft Docs. Retrieved from https://learn.microsoft.com/en-us/deployoffice/about-microsoft-365-apps. (This source defines Microsoft 365 Apps as the suite of desktop applications.)

4. Microsoft Learn. (n.d.). What is Delve? Microsoft Docs. Retrieved from https://support.microsoft.com/en-us/office/what-is-delve-1315665a-c6af-4409-a28d-49f89168784a. (This source explains that Delve helps you "discover and organize the information that's likely to be most interesting to you...across Microsoft 365.")

Question: 14

Your company has a Microsoft Office 365 subscription. As an administrator for this subscription, you have been tasked with recommending a solution that forces cloud-based applications to use the same credentials as on-premises applications. Which of the following should you recommend?

A: Azure AD Connect.

B: Configuration Manager.

C: Windows AutoPilot.

D: Azure AD Application Proxy.

Correct Answer:

A

Explanation:

Azure AD Connect is the Microsoft tool specifically designed to integrate on-premises directories (Active Directory Domain Services) with Azure Active Directory (Azure AD). Its primary function is to synchronize user identities and password hashes from the on-premises environment to the cloud. This process enables users to use a single set of credentials to access both on-premises resources and cloud-based services like Microsoft 365, fulfilling the requirement for a unified sign-in experience.

Why Incorrect Options are Wrong:

B: Configuration Manager: This tool is part of Microsoft Endpoint Manager and is used for managing on-premises devices, deploying software, and patching, not for identity synchronization.

C: Windows AutoPilot: This is a cloud-based technology used to set up and pre-configure new Windows devices, simplifying deployment. It is unrelated to user credential synchronization.

D: Azure AD Application Proxy: This service provides secure remote access to on-premises web applications. It relies on synchronized identities but is not the tool that performs the synchronization.

References:

1. Microsoft Learn. (2023). What is Azure AD Connect? "Azure AD Connect is the Microsoft tool designed to meet and accomplish your hybrid identity goals. It provides the following features: Password hash synchronization - A sign-in method that synchronizes a hash of a users on-premises AD password with Azure AD."

2. Microsoft Learn. (2023). MS-900: Describe identity and access management solutions. In the section "Describe the concept of hybrid identity," it states, "To achieve hybrid identity, you can use Azure AD Connect to synchronize your on-premises directory with your cloud directory."

3. Microsoft Learn. (2023). What is hybrid identity with Azure Active Directory? "Hybrid identity is creating a common user identity for authentication and authorization to all resources, regardless of location... Azure AD Connect... is used to synchronize your on-premises users, groups, and contacts to your Azure AD tenant."

Question: 15

Your company plans to move their Server environment to the cloud. You have been tasked with identifying a cloud model that allows for the current email environment to be upgraded, while also reducing server and application maintenance. You need to make sure that the requirements are met. Solution: You recommend the Software as a service (SaaS) model. Does the solution meet the goal?

A: Yes

B: No

Correct Answer:

A

Explanation:

The Software as a Service (SaaS) model is the correct recommendation. In a SaaS model, the cloud provider is responsible for managing the entire technology stack, including the physical servers, operating systems, and the application software itself. By migrating their email to a SaaS solution like Microsoft Exchange Online, the company effectively outsources all server and application maintenance to Microsoft. This provides them with an upgraded, continuously updated email environment while eliminating the need for in-house management of hardware and software, thereby meeting all the stated requirements.

Why Incorrect Options are Wrong:

B: No: This is incorrect. The SaaS model is specifically designed to abstract away the management of infrastructure and applications from the customer, which directly aligns with the goal of reducing server and application maintenance.

References:

1. Microsoft Learn. (2024). Describe cloud service types. MS-900: Describe cloud concepts. "With SaaS, the cloud provider hosts and manages the software application and underlying infrastructure and handles any maintenance, like software upgrades and security patching. Users connect to the application over the internet, usually with a web browser on their phone, tablet, or PC." Retrieved from https://learn.microsoft.com/en-us/training/modules/describe-cloud-concepts/3-describe-cloud-service-types

2. Microsoft Learn. (2024). Compare cloud services types. MS-900: Describe cloud concepts. The "Shared responsibility model" diagram on this page clearly illustrates that for

SaaS, the cloud provider manages everything from the physical datacenter and network up to the application level, leaving only information, data, devices, accounts, and identities for the customer to manage. Retrieved from https://learn.microsoft.com/en-us/training/modules/describe-cloud-concepts/4-compare-cloud-services-types

Question: 16

Your company is planning to migrate to Microsoft Azure and Microsoft 365. You are required to identify a cloud service that allows for website hosting. Which of the following is the model you should choose?

A: Software as a Service (SaaS)

B: Platform as a Service (PaaS)

C: Infrastructure as a Service (IaaS)

D: Container as a Service (CaaS)

Correct Answer:

B

Explanation:

Platform as a Service (PaaS) is the most appropriate cloud service model for website hosting. PaaS provides a managed platform, including the operating system, development tools, and database management systems, allowing developers to focus on building and deploying their web applications without managing the underlying infrastructure. Microsoft Azure App Service is a primary example of a PaaS offering specifically designed for hosting web applications and APIs. This model abstracts away the complexities of server management, patching, and scaling, which are handled by the cloud provider.

Why Incorrect Options are Wrong:

A: Software as a Service (SaaS): This model delivers ready-to-use software applications (like Microsoft 365) to end-users, not a platform for you to host your own custom website.

C: Infrastructure as a Service (IaaS): While you can host a website on IaaS (e.g., a virtual machine), you are responsible for managing the OS, web server, and runtime, making it less direct than PaaS.

D: Container as a Service (CaaS): This is a specialized service for managing containers. While it can be used for web hosting, PaaS is the broader and more fundamental model for application hosting.

References:

1. Microsoft Learn. (2023). Describe cloud service types. MS-900: Microsoft 365 Fundamentals. "Platform as a service (PaaS) is a complete development and deployment

environment in the cloud... PaaS is designed to support the complete web application lifecycle: building, testing, deploying, managing, and updating."

2. Microsoft Azure Documentation. (n.d.). What is Platform as a service (PaaS)?. "PaaS provides a framework that developers can build upon to develop or customize cloud-based applications... This makes it easier for developers to quickly create web or mobile apps."

3. Microsoft Azure Documentation. (n.d.). What is IaaS?. "In an IaaS model, a cloud provider hosts the infrastructure components traditionally present in an on-premises data center... You’re responsible for managing the operating systems, data, and applications." (This highlights the additional management overhead compared to PaaS for the same goal).

Question: 17

You have been tasked with deploying Microsoft 365 for your company in a hybrid configuration. You want to make sure that a smart card can be used by staff for authentication purposes. Solution: You configure the use of pass-through authentication and single sign-on as the hybrid identity solution. Does the solution meet the goal?

A: Yes

B: No

Correct Answer:

B

Explanation:

The proposed solution does not meet the goal. Pass-through Authentication (PTA) is a sign-in method that allows users to sign in to both on-premises and cloud-based applications using the same passwords. The validation of these passwords happens directly against the on-premises Active Directory. However, PTA is fundamentally designed for password-based authentication and does not support certificate-based authentication methods, which are required for smart cards. The correct hybrid identity solution to enable smart card authentication is Active Directory Federation Services (AD FS), which can be configured to handle various advanced authentication scenarios, including certificate-based and smart card sign-ins.

Why Incorrect Options are Wrong:

A: This is incorrect because Pass-through Authentication validates user passwords, not the certificates used by smart cards. It lacks the necessary mechanism to process this form of authentication.

References:

1. Microsoft Learn. (2024). Choose the right authentication method for your Microsoft Entra hybrid identity solution. In the feature comparison table under the "Authentication" section, it explicitly states that "Third-party and smartcard authentication" is supported by Federation (AD FS) but not by Pass-through Authentication.

2. Microsoft Learn. (2023). User sign-in with Microsoft Entra Pass-through Authentication. This document details the workflow for PTA, which involves an agent validating a user's

password against the on-premises Active Directory. The process described is exclusively for password credentials.

3. Microsoft Learn. (2023). What is federation with Microsoft Entra ID?. This document explains that with federation, "You can implement more advanced authentication requirements. For example, smartcard-based authentication or third-party multifactor authentication." This confirms AD FS is the appropriate choice for the scenario.

Question: 18

Your company makes use of Microsoft 365 in their environment. You have been tasked with making sure that admin roles are protected. The feature you use should achieve this by requiring approvals. Which of the following is a feature you should use?

A: Mobile application protection policy.

B: Microsoft Azure AD Identity Protection.

C: Microsoft Azure AD Privilege Identity Protection.

D: Microsoft Azure AD Conditional Access.

Correct Answer:

C

Explanation:

Microsoft Azure AD Privileged Identity Management (PIM) is the service designed specifically to manage, control, and monitor access to privileged roles. A core capability of PIM is providing just-in-time (JIT) access, where users are made "eligible" for a role. To use the role, they must activate it for a limited time. This activation process can be configured to require justification and, crucially, approval from a designated approver. This directly addresses the question's requirement to protect admin roles by requiring approvals before privileges are granted.

Why Incorrect Options are Wrong:

A: Mobile application protection policies are part of Microsoft Intune and are used to protect organizational data within apps on mobile devices, not manage administrative role activation.

B: Microsoft Azure AD Identity Protection focuses on detecting and remediating identity-based risks, such as suspicious sign-ins, but it does not include an approval workflow for activating roles.

D: Microsoft Azure AD Conditional Access enforces access policies at the point of sign-in based on signals like user location or device health, but it does not manage role eligibility or activation approvals.

References:

1. Microsoft Learn. "What is Privileged Identity Management?". Microsoft Entra documentation. This document states, "Privileged Identity Management (PIM) is a service in Microsoft Entra ID that enables you to manage, control, and monitor access to important resources in your organization... You can also enforce policy options like requiring approval to activate privileged roles."

2. Microsoft Learn. "Approve or deny requests for Azure AD roles in Privileged Identity Management". Microsoft Entra documentation. This guide details the specific process for approvers, stating, "As a delegated approver, you receive an email notification from Microsoft Azure when a request for an Azure AD role is pending your approval."

3. Microsoft Learn. "What is Identity Protection?". Microsoft Entra documentation. This source describes Identity Protection's function as automating the detection and remediation of identity-based risks, with no mention of approval workflows for role activation.

4. Microsoft Learn. "What is Conditional Access?". Microsoft Entra documentation. This document explains that Conditional Access is a tool to "bring signals together, to make decisions, and enforce organizational policies" during sign-in, which is distinct from managing role activation.

Question: 19

You have recently made use of Windows Autopilot to deploy Windows 10 devices in your company's environment. You have been asked to make sure that data that stored in OneDrive for Business is available to users from remote locations. Solution: You enable Microsoft Azure AD multi-factor authentication for the users. Does the solution meet the goal?

A: Yes

B: No

Correct Answer:

B

Explanation:

The goal is to ensure data in OneDrive for Business is available from remote locations. OneDrive for Business is an internet-based cloud storage service, meaning its data is inherently designed to be accessible from any location with an internet connection, provided the user can authenticate. The proposed solution, enabling Microsoft Azure AD Multi-Factor Authentication (MFA), is a security measure. MFA adds a second layer of verification to the sign-in process to protect user accounts and data. While it secures remote access, it does not enable it; the remote access capability is a fundamental feature of the OneDrive for Business service itself.

Why Incorrect Options are Wrong:

A: Yes: This is incorrect because MFA is a security feature that safeguards access, not a feature that provides the core functionality of remote availability. The availability is inherent to the OneDrive cloud service.

References:

1. Microsoft Learn. (2024). What is OneDrive? "OneDrive is the Microsoft cloud service that connects you to all your files. It lets you store and protect your files, share them with others, and get to them from anywhere on all your devices." This source confirms that remote access ("from anywhere") is an intrinsic feature of OneDrive.

2. Microsoft Learn. (2023). How it works: Azure AD Multi-Factor Authentication. "Azure AD Multi-Factor Authentication helps safeguard access to data and applications, providing

another layer of security by using a second form of authentication." This source defines MFA as a security mechanism, not an availability feature.

3. Microsoft Learn. (2024). Describe identity and access management capabilities of Microsoft 365. MS-900 Study Guide. This module clarifies that features like MFA are part of identity and access management, which focuses on ensuring that only authorized users can access resources, rather than enabling the availability of those resources.

Question: 20

Your company makes use of Platform as a Service (PaaS) for their Azure solution. Which of the following options are components that your IT employees are responsible for?

A: Networks.

B: Databases.

C: Applications.

D: Servers.

Correct Answer:

B, C

Explanation:

In the Platform as a Service (PaaS) cloud service model, the cloud provider (Microsoft) is responsible for managing the underlying infrastructure, which includes physical servers, networking, storage, and the operating system. The customer retains responsibility for the components they build on top of this platform. This includes the applications they deploy and the data they manage, which encompasses the data, schema, and access controls for their databases. Therefore, the company's IT employees are responsible for both their applications and databases.

Why Incorrect Options are Wrong:

A: Networks: The underlying physical network infrastructure and its controls are managed by the cloud provider in the PaaS model.

D: Servers: The physical hosts and virtual servers that run the platform are the responsibility of the cloud provider, which is a key benefit of PaaS.

References:

1. Microsoft Learn. "Shared responsibility in the cloud." Microsoft Azure Documentation. Accessed May 20, 2024. In the diagram illustrating the division of responsibility, the "PaaS" column clearly shows that "Application" and "Information & data" (which includes databases) are customer responsibilities, while "Physical hosts" (Servers) and "Physical network" are Microsoft's responsibilities.

2. Microsoft Learn. "Describe cloud service types - MS-900." Microsoft 365 Fundamentals. Accessed May 20, 2024. This module explains that with PaaS, "The cloud provider

maintains the infrastructure... The customer is responsible for their own applications and data." This directly supports that applications and the data within databases are customer-managed components.

Question: 21

Your company plans to move their Server environment to the cloud. You have been tasked with identifying a cloud model that allows for the current email environment to be upgraded, while also reducing server and application maintenance. You need to make sure that the requirements are met. Solution: You recommend the Infrastructure as a service (IaaS) model. Does the solution meet the goal?

A: Yes

B: No

Correct Answer:

B

Explanation:

The proposed solution, Infrastructure as a Service (IaaS), does not fully meet the stated goals. While IaaS eliminates the need for the company to manage physical servers, it still requires the company to manage the operating systems, middleware, and the email application itself. This contradicts the key requirement to reduce application maintenance. A Software as a Service (SaaS) model, such as Microsoft 365 with Exchange Online, would be the appropriate solution. In a SaaS model, the cloud provider manages the entire infrastructure and the application, thereby reducing both server and application maintenance for the customer.

Why Incorrect Options are Wrong:

References:

1. Microsoft Learn. "Describe cloud service types." MS-900: Microsoft 365 Fundamentals. This module explains the shared responsibility model. For IaaS, it states, "You're responsible for the operating system and software... you're responsible for all software installation, configuration, and maintenance." This directly contradicts the requirement to reduce application maintenance.

2. Microsoft Learn. "Shared responsibility in the cloud." Microsoft Cloud Adoption Framework for Azure. The responsibility chart in this document clearly shows that for IaaS, the customer is responsible for the "Operating system," "Middleware," "Runtime," and "Applications." In contrast, for SaaS, these are all managed by the cloud provider, which aligns with the user's goal.

Question: 22

Your company plans to move their Server environment to the cloud. You have been tasked with identifying a cloud model that allows for the current email environment to be upgraded, while also reducing server and application maintenance. You need to make sure that the requirements are met. Solution: You recommend the Platform as a service (PaaS) model. Does the solution meet the goal?

A: Yes

B: No

Correct Answer:

B

Explanation:

The proposed solution, Platform as a Service (PaaS), does not meet the goal because it fails to reduce application maintenance. In a PaaS model, the cloud provider manages the underlying infrastructure, including servers, storage, and operating systems, which meets the server maintenance reduction requirement. However, the customer remains responsible for deploying, managing, and maintaining the applications and data running on the platform. To upgrade an email environment while also reducing application maintenance, a Software as a Service (SaaS) model, such as Microsoft Exchange Online, would be the appropriate choice, as the vendor manages the entire stack, including the application itself.

Why Incorrect Options are Wrong:

A: This is incorrect because the PaaS model does not fulfill the requirement to reduce application maintenance; this responsibility remains with the customer.

References:

1. Microsoft Learn. (n.d.). Describe cloud service types. MS-900: Microsoft 365 Fundamentals. In this module, PaaS is described as a service where the cloud provider maintains the platform, but the customer is responsible for the applications they deploy. It states, "For PaaS, the cloud provider maintains the platform... You don't have to worry about the licensing or patching for operating systems and databases. You are responsible for the applications you deploy onto the platform."

2. Microsoft Learn. (n.d.). Describe the shared responsibility model. MS-900: Microsoft 365 Fundamentals. The shared responsibility model diagram clearly illustrates that in a PaaS

environment, the "Application" layer is a customer responsibility. In contrast, for SaaS, the application is managed by the cloud provider, which aligns with the scenario's requirements.

Question: 23

Your company plans to acquire a Microsoft 365 subscription. One of the services included in the subscription is described as a private social network that can be used to effectively sort out support problems. It can also be used to collect feedback on projects and documents. Which of the following is the service being described above?

A: Microsoft Teams.

B: Microsoft Yammer.

C: Microsoft Office Delve.

D: Microsoft SharePoint Online.

Correct Answer:

B

Explanation:

Microsoft Yammer is an enterprise social network service that is part of the Microsoft 365 suite. It is designed to facilitate open communication and collaboration across an entire organization, functioning as a private social network. Its community-based structure is ideal for creating groups dedicated to specific topics, such as technical support, where employees can ask questions and receive crowd-sourced answers. It is also widely used for gathering feedback on projects, documents, and company-wide initiatives, perfectly matching the service described in the question.

Why Incorrect Options are Wrong:

A: Microsoft Teams: This is a collaboration hub for focused teamwork within specific groups, centered on chat, meetings, and file sharing, not a company-wide social network.

C: Microsoft Office Delve: This is a content discovery tool that surfaces relevant documents based on user activity and connections, not a platform for social interaction or support.

D: Microsoft SharePoint Online: This is primarily a platform for creating websites and managing content, documents, and knowledge, not an enterprise social network itself.

References:

1. Microsoft Learn. (2023). Describe the capabilities of Microsoft 365 - Describe collaboration solutions of Microsoft 365. MS-900: Microsoft 365 Fundamentals. "Yammer is

an enterprise social network that helps you and your team collaborate openly and stay connected across your organization."

2. Microsoft Learn. (2023). Describe the capabilities of Microsoft 365 - Describe collaboration solutions of Microsoft 365. MS-900: Microsoft 365 Fundamentals. "Microsoft Teams is the hub for teamwork in Microsoft 365."

3. Microsoft Learn. (2023). Describe the capabilities of Microsoft 365 - Describe endpoint management capabilities of Microsoft 365. MS-900: Microsoft 365 Fundamentals. "SharePoint Online helps organizations share and manage content, knowledge, and applications to empower teamwork."

4. Microsoft Support. (n.d.). What is Delve?. "Delve helps you discover the information that's likely to be most interesting to you right now - across Microsoft 365."

Question: 24

Your company has a Microsoft Office 365 subscription. As an administrator for this subscription, you are educating new users on which component to use for audio and visual communications with colleagues. Which of the following is the component that should be used?

A: Microsoft Exchange Online

B: Enterprise Mobility + Security

C: Microsoft Teams

D: Microsoft SharePoint Online

Correct Answer:

C

Explanation:

Microsoft Teams is the central hub for teamwork and communication within Microsoft 365. It is specifically designed to facilitate real-time collaboration through features such as instant messaging, online meetings, and calling. Its core functionality includes high-definition audio and video conferencing, making it the designated component for the audio and visual communication needs described in the question. Teams integrates chat, meetings, calling, and file sharing into a single application, providing a comprehensive communication solution for colleagues.

Why Incorrect Options are Wrong:

A: Microsoft Exchange Online: This service provides hosted email, calendar, and contact management. It is not the primary tool for real-time audio or visual communication.

B: Enterprise Mobility + Security: This is a suite of security and management services for protecting corporate data and managing devices, not a user-facing communication application.

D: Microsoft SharePoint Online: This is a platform for creating websites and serves as a secure place to store, organize, and share information, primarily for document management.

References:

1. Microsoft Learn. (2024). Describe collaboration solutions in Microsoft 365. MS-900: Microsoft 365 Fundamentals. "Microsoft Teams is a collaboration app that helps your team stay organized and have conversations—all in one place... Key features include... Meetings - Host audio, video, and web conferences."

2. Microsoft Learn. (2024). What is Microsoft Teams?. "Microsoft Teams is the hub for teamwork in Microsoft 365 that integrates the people, content, and tools your team needs to be more engaged and effective."

3. Microsoft Learn. (2024). Describe endpoint management capabilities in Microsoft 365. MS-900: Microsoft 365 Fundamentals. "Microsoft Enterprise Mobility + Security (EMS) is an intelligent mobility management and security platform."

4. Microsoft Learn. (2024). Describe business management solutions in Microsoft 365. MS-900: Microsoft 365 Fundamentals. "SharePoint Online is a service that helps organizations share and manage content, knowledge, and applications... It's a central place to store information."

Question: 25

Your company has a Microsoft Office 365 subscription. As an administrator for this subscription, you have been tasked with recommending a solution that will allow users to make use of unsuited applications on their Windows 10 devices. Which of the following should you recommend?

A: Azure AD Connect.

B: Configuration Manager.

C: Windows AutoPilot.

D: Windows Virtual Desktop.

Correct Answer:

D

Explanation:

Windows Virtual Desktop (now known as Azure Virtual Desktop) is a cloud-based desktop and application virtualization service. It enables organizations to deliver virtual desktops and applications to users on any device. This service is the ideal solution for running "unsuited" applications, such as legacy software or applications that are incompatible with the standard Windows 10 operating system, by hosting them in an Azure virtual machine and streaming them to the user's local device. This approach ensures application compatibility and centralizes management without altering the user's local machine configuration.

Why Incorrect Options are Wrong:

A: Azure AD Connect: This is a service for synchronizing on-premises identity directories (Active Directory) with Azure Active Directory. It does not deliver or manage applications.

B: Configuration Manager: This tool is used for managing and deploying software, updates, and policies to on-premises devices. It does not virtualize or stream incompatible applications.

C: Windows AutoPilot: This is a suite of technologies used to set up and pre-configure new Windows 10 devices for enterprise use. It is for device provisioning, not application virtualization.

References:

1. Microsoft Learn. "What is Azure Virtual Desktop?" Azure Documentation. "Azure Virtual Desktop is a desktop and app virtualization service that runs on the cloud... You can use Azure Virtual Desktop to... Deliver legacy applications to any computer."

2. Microsoft Learn. "What is Windows Autopilot?" Microsoft Intune Documentation. "Windows Autopilot is a collection of technologies used to set up and pre-configure new devices, getting them ready for productive use."

3. Microsoft Learn. "What is Azure AD Connect?" Microsoft Entra Documentation. "Azure AD Connect is an on-premises Microsoft application that is designed to meet and accomplish your hybrid identity goals."

4. Microsoft Learn. "What is Configuration Manager?" Microsoft Configuration Manager Documentation. "Configuration Manager is an on-premises management solution to manage desktops, servers, and laptops that are on your network or internet-based."

Question: 26

You have recently made use of Windows Autopilot to deploy Windows 10 devices in your company's environment. You have been asked to make sure that data that stored in OneDrive for Business is available to users from remote locations. Solution: You inform users that they should use their Microsoft Azure AD credentials to sign in to their devices. Does the solution meet the goal?

A: Yes

B: No

Correct Answer:

B

Explanation:

Using Azure AD credentials to sign-in only authenticates the user to Windows and provides single-sign-on tokens. It does not configure, enable, or sync the OneDrive for Business client, nor does it set Files-On-Demand or Known-Folder-Move. Without these settings, OneDrive data is not automatically available when the user works remotely. Therefore, the goal is not met by the proposed solution.

Why Incorrect Options are Wrong:

A: Signing in with Azure AD credentials alone neither installs nor configures OneDrive; availability of OneDrive data from remote locations still requires the OneDrive sync client and its policies.

References:

1. Microsoft Docs – “Deploy and configure the OneDrive sync app for Windows” → Prerequisites & Step 3 “Silently configure OneDrive” (Sections: Prerequisites; Silently configure OneDrive) https://learn.microsoft.com/sharepoint/deploy-on-windows

2. Microsoft Docs – “Use OneDrive Files On-Demand” → “Pre-requisites” & “Turn on Files On-Demand” (Sections: Requirements; Enable Files On-Demand) https://learn.microsoft.com/onedrive/files-on-demand

3. Microsoft Docs – “Windows Autopilot overview” (Section: Azure AD-joined devices) https://learn.microsoft.com/mem/autopilot/windows-autopilot

Question: 27

You have been tasked with deploying Microsoft 365 for your company in a hybrid configuration. You want to make sure that a smart card can be used by staff for authentication purposes. Solution: You configure the use of password hash synchronization with single-on as the hybrid identity solution. Does the solution meet the goal?

A: Yes

B: No

Correct Answer:

B

Explanation:

The proposed solution does not meet the goal. Password hash synchronization (PHS) is an authentication method that synchronizes a hash of the user's on-premises Active Directory password to Microsoft Entra IAuthentication occurs by validating this password hash in the cloud. This method is fundamentally password-based and does not support non-password credentials like smart cards (which use certificate-based authentication). To enable smart card authentication in a hybrid environment, you must use a different identity solution, such as federation with Active Directory Federation Services (AD FS) or Pass-through Authentication (PTA), which can leverage the on-premises infrastructure to process smart card sign-ins.

Why Incorrect Options are Wrong:

A: This is incorrect because password hash synchronization is exclusively a password-based authentication method and lacks the capability to process certificate-based authentication from smart cards.

References:

1. Microsoft Entra Documentation. (2023). Choose the right authentication method for your Microsoft Entra hybrid identity solution. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn.

Reference Specifics: In the table under the "Compare methods" section, the row for "Smartcard" explicitly states "No" for "Password Hash Sync" and "Yes" for both "Pass-through Authentication" and "Federation."

2. Microsoft Entra Documentation. (2023). What is password hash synchronization with Microsoft Entra ID?. Microsoft Learn. Retrieved from https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/whatis-phs.

Reference Specifics: The "How password hash synchronization works" section describes a process based entirely on password hashes, with no mention or mechanism for certificate-based credentials like smart cards.

Question: 28

You have been tasked with deploying Microsoft 365 for your company in a hybrid configuration. You want to make sure that a smart card can be used by staff for authentication purposes. Solution: You configure the use of Active Directory Federation Services (AD FS) as the hybrid identity solution. Does the solution meet the goal?

A: Yes

B: No

Correct Answer:

A

Explanation:

The solution meets the goal. Active Directory Federation Services (AD FS) is a federated identity solution that redirects authentication requests from Microsoft 365 to on-premises AD FS servers. This architecture allows an organization to use its on-premises authentication infrastructure and policies. Since smart card authentication is a form of on-premises, certificate-based authentication, AD FS can be configured to handle these requests, enabling staff to use their smart cards to sign in to Microsoft 365 services.

Why Incorrect Options are Wrong:

B: This option is incorrect because AD FS is the primary Microsoft hybrid identity solution designed to enable advanced, on-premises authentication methods like smart cards for cloud resources.

References:

1. Microsoft Learn. (2024). Choose the right authentication method for your Microsoft Entra hybrid identity solution. "Federation" section. Retrieved from https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/choose-ad-authn#federation. The documentation states, "With federation, you can... implement more advanced authentication scenarios, such as smartcard-based authentication".

2. Microsoft Learn. (2024). Overview of Microsoft Entra certificate-based authentication. "How does CBA work?" section. Retrieved from https://learn.microsoft.com/en-us/entra/identity/authentication/concept-certificate-based-authentication. This document explains that for federated tenants, authentication can be done using AD FS, which handles the certificate validation.

Question: 29

You are employed as a Microsoft 365 administrator. Your company plans to make use of MyAnalytics. You need to identify the different features of MyAnalytics and Workspace Analytics. Which of the following are features of MyAnalytics? (Choose all that apply.)

A: It can only be acquired as an added reference-on license.

B: It provides team work and collaboration metrics.

C: It is included in the Office 365 ProPlus license.

D: It provides employee work and collaboration metrics

Correct Answer:

D

Explanation:

MyAnalytics, now known as personal insights within Microsoft Viva Insights, is designed to help individual employees understand their work patterns and improve personal productivity and well-being. It provides private, personalized metrics and insights based on an individual's Microsoft 365 data, such as time spent in meetings, email habits, focus hours, and after-hours work. The core function is to deliver insights to the individual employee about their own work and collaboration activities.

Why Incorrect Options are Wrong:

A: This is incorrect because MyAnalytics is included by default in many Microsoft 365 and Office 365 enterprise and business suites, not sold only as an add-on license.

B: This describes the functionality of advanced insights in Viva Insights (formerly Workspace Analytics), which provides aggregated, de-identified data for team and organizational-level analysis, not MyAnalytics.

C: MyAnalytics is not included with the standalone Office 365 ProPlus (now Microsoft 365 Apps for enterprise) license. It requires a service plan included in suites like Microsoft 365 E3/E5.

References:

1. Microsoft Documentation - Viva Insights, "Personal insights in Microsoft Viva Insights." This document describes the function of MyAnalytics (personal insights), stating, "Personal insights are your own, for you to explore your work patterns... Viva Insights provides

personal insights about... Focus, Wellbeing, Network, [and] Collaboration." This supports that it provides individual employee work and collaboration metrics (Answer D).

2. Microsoft Documentation - Viva Insights, "Plans and environments for Viva Insights." This official licensing guide lists the specific Microsoft 365 and Office 365 plans that include personal insights (MyAnalytics). It confirms that the feature is bundled with suites like Microsoft 365 E3/E5 and Office 365 E1/E3/E5, invalidating the claims that it is "only" an add-on (Answer A) or included with Office 365 ProPlus standalone (Answer C).

3. Microsoft Documentation - Viva Insights, "Advanced insights in Microsoft Viva Insights." This source clarifies the distinction between personal and advanced insights. It states, "Advanced insights help business leaders address critical questions about organizational resiliency and culture," confirming that team and organizational metrics are part of a different offering (invalidating Answer B for MyAnalytics).

Question: 30

You need to consider the underlined segment to establish whether it is accurate. To retrieve data for employees who request personal data under General Data Protection Regulation (GDPR) guidelines, you have to create a GDPR assessment. Select `No adjustment required` if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option. What should you do?

A: No adjustment required

B: mobile application protection policy

C: device configuration policy

D: data subject request case

Correct Answer:

D

Explanation:

The General Data Protection Regulation (GDPR) grants individuals, referred to as data subjects, the right to access, modify, or delete their personal data held by an organization. When an employee makes such a request, it is formally known as a Data Subject Request (DSR). Within the Microsoft Purview compliance portal, the specific tool designed to manage these requests is the DSR case tool. Creating a data subject request case is the correct procedure to find, review, and export the relevant personal data from across Microsoft 365 services to fulfill the employee's request. A "GDPR assessment" evaluates an organization's overall compliance posture, which is a different function.

Why Incorrect Options are Wrong:

A: A GDPR assessment is a tool in Compliance Manager to evaluate an organization's overall compliance, not to process an individual's data request.

B: A mobile application protection policy is an Intune feature that secures organizational data within apps on mobile devices, unrelated to GDPR data retrieval.

C: A device configuration policy is an Intune feature used to manage settings on enrolled devices, not for fulfilling data subject requests.

References:

1. Microsoft Learn. (2024). Data Subject Requests for the GDPR and CCPIn "Describe the compliance management capabilities in Microsoft Purview". "The GDPR gives individuals... the right to... Get copies of their personal data... These requests are called Data Subject Requests or DSRs. To find and act on DSRs for data in Microsoft 365, you can use the DSR case tool in the Microsoft Purview compliance portal."

2. Microsoft Learn. (2024). Manage Data Subject Requests in the Microsoft Purview compliance portal. "You can use the DSR case tool in the Microsoft Purview compliance portal to manage investigations that are created in response to a DSR... The first step is to create a DSR case."

3. Microsoft Learn. (2024). Microsoft Purview Compliance Manager. "Compliance Manager helps you manage your organization’s compliance requirements... It provides... pre-built assessments for common industry and regional standards and regulations". This reference distinguishes the function of an assessment from a DSR case.