Free Microsoft AZ-800 Practice Questions

Shared by Graves on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

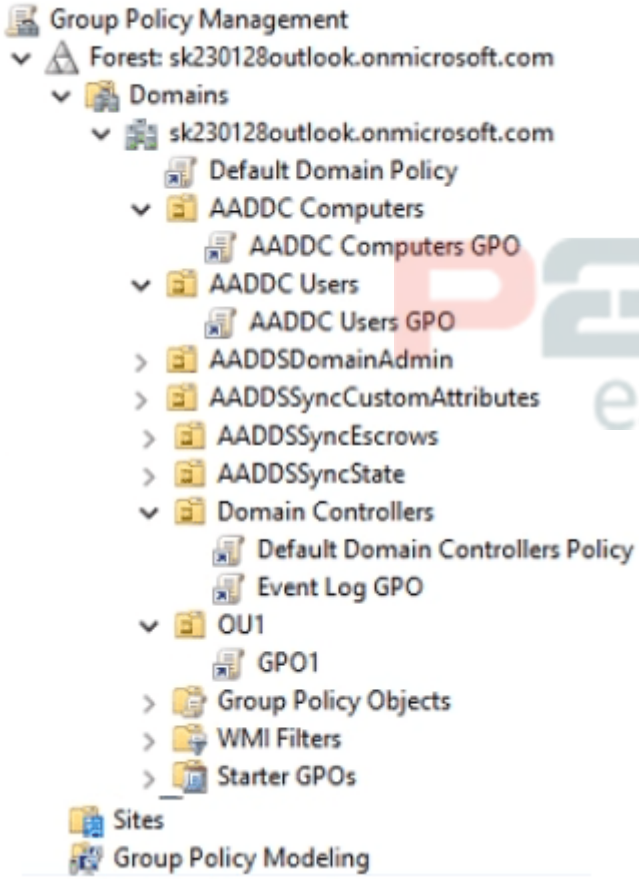
AZ-800 Mix Questions IN THIS CASE STUDY

Your network contains a Microsoft Entra Domain Services domain named sk230128outlook.onmicrosoft.com. The domain contains a server named Server1 that runs Windows Server.

You have the users shown in the following table.

Name	Description
User1	Domain user in the AADDC Users organizational unit (OU)
User2	Local user on Server1
User3	Domain user in an organizational unit (OU) named OU1

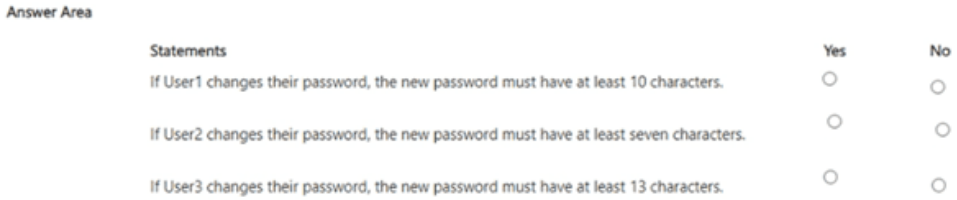
The domain contains the Group Policy Objects (GPOs) shown in the following exhibit.



The minimum password length for each GPO is configured as shown in the following table.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.



Answer:

See the Answer in the Premium Version!

Question 2

Question Type: MultipleChoice

You haw? a server named Host1 that has the Hyper-V server role installed. Host! hosts a virtual machine named VM1.

You have a management server named Server! that runs Windows Server. You remotely manage Host1 from Server1 by using Hyper-V Manager.

You need to ensure that you can access a USB hard drive connected to Server1 when you connect to VM1 by using Virtual Machine Connection.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

Options:

A- From the Hyper-V Settings of Host1, select Allow enhanced session mode
B- From Disk Management on Host1. attach a virtual hard disk.
C- From Virtual Machine Connection, switch to a basic session.
D- From Virtual Machine Connection select Show Options and then select the USB hard drive.
E- From Disk Management on Host1, select Rescan Disks

Answer:

A, D

Explanation:

In Hyper-V, access to local devices such as a USB hard drive connected to the management computer (Server1) from within a VM session (VM1) is provided only when using Enhanced Session Mode through the Virtual Machine Connection (vmconnect) client. The AZ-800/''Administering Windows Server Hybrid Core Infrastructure'' materials emphasize that Enhanced Session Mode ''enables redirection of local resources (audio, clipboard, printers, drives, and supported Plug and Play devices) to a guest when connecting with Virtual Machine Connection.'' To use it, you must first enable it on the host and then select the device in vmconnect before establishing the session.

Accordingly, you should:

Enable Enhanced Session on the host: In Hyper-V Manager Host1 Hyper-V Settings Enhanced Session Mode Policy, select Allow enhanced session mode (and optionally Use enhanced session mode under User settings). This satisfies option A.

Choose the USB drive in the vmconnect UI: When launching the connection to VM1, click Show Options Local Resources More..., and select Drives or the specific USB device so it is redirected into the guest. This matches option D.

Options B and E relate to host Disk Management operations and do not provide guest redirection of a USB attached to Server1. Option C (''switch to a basic session'') explicitly disables the RDP-based redirection channel that Enhanced Session Mode relies upon, preventing USB/drive passthrough. Therefore, the correct pair is A and D.

Question 3

Question Type: MultipleChoice

You plan to deploy a containerized application that requires .NET Core.

You need to create a container image for the application. The image must be as small as possible.

Which base image should you use?

Options:

A- Nano Server

B- Server Cote
C- Windows Server
D- Windows

Answer:

A

Explanation:

When building Windows container images, the base image determines both compatibility and image size. The hybrid core curriculum emphasizes that Nano Server is the smallest Windows base image, intended for headless, app-only workloads such as .NET (/.NET Core) applications. .NET Core's modular, self-contained approach enables it to run on Nano Server images designed for Windows containers, yielding significantly smaller images and faster pull/start times than Server Core or Windows Server (Full) bases. Server Core includes additional components (GUI-less but still broad OS surface) and is used when you need APIs or frameworks not present in Nano. ''Windows'' or ''Windows Server (Full)'' are not container base images for modern Windows containers and would produce unnecessarily large layers. To meet the requirement ''the image must be as small as possible'' for a .NET Core app, the guidance is to select Nano Server as the base (for matching architecture and Windows version), then layer the .NET runtime or self-contained app on top. This choice aligns with best practices for minimizing footprint, improving density, and reducing network transfer during CI/CD.

Question 4

Question Type: MultipleChoice

You have an on premises Active Directory Domain Services (AD DS) domain that syncs with an Azure Active Directory (Azure AD) tenant.

You plan to implement self-service password reset (SSPR) in Azure AD.

You need to ensure that users that reset their passwords by using SSPR can use the new password resources in the AD DS domain.

What should you do?

Options:

A- Deploy the Azure AD Password Protection proxy service to the on premises network.
B- Run the Microsoft Azure Active Directory Connect wizard and select Password writeback.
C- Grant the Change password permission for the domain to the Azure AD Connect service

account.
D- Grant the impersonate a client after authentication user right to the Azure AD Connect service account.

Answer:

B

Explanation:

In the Administering Windows Server Hybrid Core Infrastructure content for identity synchronization and password management, Microsoft specifies that self-service password reset (SSPR) for hybrid users requires password writeback through Azure AD Connect. The materials state: ''Password writeback enables Azure AD to write password changes made in the cloud back to your on-premises Active Directory. This feature is required to allow users who reset their passwords using SSPR to use those new passwords when authenticating to on-premises resources.'' The configuration steps emphasize: ''Run the Azure AD Connect wizard and enable Password writeback.'' By contrast, the Azure AD Password Protection proxy pertains to banned password enforcement and does not perform writeback, and granting extra rights to the sync account does not replace enabling the writeback capability in the connector. Therefore, enabling Password writeback in Azure AD Connect is the correct and required action to ensure SSPR changes are reflected in the on-premises AD DS domain.

Question 5

Question Type: MultipleChoice

SIMULATION

Task 10

You use a Group Policy preference to map \\dd.contoso.com\instal1 as drive H for all users. If a user already has an existing drive mapping for H. the new drive mapping must take precedence.

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

To map\\dd.contoso.com\instal1as drive H for all users using Group Policy Preferences and ensure that the new drive mapping takes precedence over any existing mappings, follow these steps:

Step 1: Open Group Policy Management ConsoleOpen the Group Policy Management Console (GPMC) on a machine that has administrative privileges over the domain.

Step 2: Create or Edit a GPOCreate a new Group Policy Object (GPO) or edit an existing one that applies to the users who need the drive mapping.

Step 3: Navigate to Drive MappingsIn the GPO Editor, navigate to:

User Configuration -> Preferences -> Windows Settings -> Drive Maps

Step 4: New Drive MappingRight-click on Drive Maps and selectNew->Mapped Drive.

Step 5: Configure Drive MappingIn the New Drive Properties window, configure the following settings:

Action: SelectReplace. This action will overwrite any existing mappings with the same drive letter.

Location: Enter the UNC path\\dd.contoso.com\instal1.

Drive Letter: ChooseH:from the drop-down menu.

Reconnect: Check this option if you want the drive mapping to persist across logon sessions.

Label As: Optionally, provide a label for the drive mapping.

Hide/Show this drive: Set according to your preference.

Hide/Show all drives: Set according to your preference.

Step 6: Common TabGo to theCommontab and configure the following:

Run in logged-on user's security context (user policy option): Check this option.

Item-level targeting: Click onTargetingand set up any specific criteria if needed.

Step 7: Apply the GPOClickApplyand thenOKto save the drive mapping configuration.

Step 8: Link the GPOLink the GPO to an Organizational Unit (OU) or domain that contains the users who should receive the drive mapping.

Step 9: Update Group PolicyInstruct users to log off and log back on, or use thegpupdate /forcecommand to refresh Group Policy on their computers.

Question 6

Question Type: MultipleChoice

SIMULATION

Task 8

You plan to delegate the management of a ONS zone named fabnkam.com located on DO to the BranchAdmins group. You need to ensure that you can grant permissions to the fabikam.com zone.

Options:

A- See the solution of this Task below

Answer:

A

Explanation:

Objective:

Grant permissions to the BranchAdmins group to manage the fabikam.com DNS zone on DC1.

Step-by-Step Guide

Step 1: Log in to the DNS Server

Log in to DC1 (which hosts the DNS zone fabikam.com) using an account with Domain Admin or Enterprise Admin rights.

Step 2: Open the DNS Manager

Open DNS Manager:

Press Windows + R, type dnsmgmt.msc, and hit Enter.

Step 3: Locate the Zone

In the DNS Manager, expand the Forward Lookup Zones.

Locate and right-click on the zone fabikam.com.

Step 4: Open Zone Properties

Right-click on fabikam.com and select Properties.

In the Properties window, go to the Security tab.

Step 5: Grant Permissions

In the Security tab, click Add.

Enter the name of the group:

nginx

Copy

BranchAdmins

Click Check Names to resolve the group.

Click OK.

Step 6: Assign the Appropriate Permissions

In the Permissions window, select the BranchAdmins group.

Assign the following permissions:

Read

Write

Create All Child Objects

Delete All Child Objects

Optionally, click Advanced for more granular control if needed.

Step 7: Apply and Close

Click Apply and OK to save the changes.

Question 7

Question Type: MultipleChoice

You have an on-premises server named Server 1 that runs Windows Server. You have an Azure subscription that contains a virtual network named VNetl. You need to connect Server1 to VNetl by using Azure Network Adapter. What should you use?

Options:

A- the Azure portal
B- Azure AD Connect
C- Device Manager
D- Windows Admin Center

Answer:

D

Explanation:

The hybrid networking module in AZ-800 details Azure Network Adapter (ANA) as a Windows Admin Center (WAC) workflow that creates a point-to-site (P2S) VPN from an on-premises Windows Server to an Azure virtual network. The documentation states that ANA is initiated directly from Windows Admin Center, which automates provisioning of the necessary Azure resources (e.g., VPN gateway configuration and certificates) and installs/configures the VPN client on the server, establishing secure connectivity to the target VNet. The Azure portal does not install or configure the on-premises VPN client for a standalone server; Azure AD Connect is used for identity synchronization and is unrelated to network tunneling; and Device Manager is not used for configuring VPN or Azure connectivity. In practice, you add the server to WAC, open the Network tool, and select Add Azure Network Adapter, sign in to Azure, choose VNet1, and complete the wizard. This is the prescribed, streamlined method for connecting Server1 to VNet1 using Azure Network Adapter, validating Windows Admin Center as the correct choice.

Question 8

Question Type: MultipleChoice

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains three servers that run Windows Server and have the Hyper-V server role installed. Each server has a Switch Embedded Teaming (SET) team.

You need to verify that Remote Direct Memory Access (RDMA) and required Windows Server settings are configured properly on each server to support a failover cluster.

What should you use?

Options:

A- the validate-DCB cmdlet
B- Server Manager
C- the Get-NetAdapter cmdlet
D- Failover Cluster Manager

Answer:

A

Explanation:

In Windows Server environments that use Switch Embedded Teaming (SET) with RDMA/SMB Direct, Microsoft's hybrid server administration guidance specifies validating Data Center Bridging (DCB) and RDMA prerequisites before you place the hosts into a cluster. The Validate-DCB PowerShell cmdlet (from the DataCenterBridging module) is the purpose-built tool to confirm that Priority-based Flow Control (PFC), ETS/QoS policies, and SMB Direct priorities are consistently configured and operational across adapters and vSwitch/SET configurations. The study content emphasizes that resilient RDMA requires correct DCB on every host NIC participating in SMB Direct, and that Validate-DCB ''verifies RDMA readiness and flags misconfiguration,'' including priority mappings and host settings needed for failover clustering. By contrast, Server Manager and Failover Cluster Manager do not test DCB/RDMA health at the NIC policy level, and Get-NetAdapter only reports adapter state (for example, RDMA enabled/disabled) without end-to-end policy validation. Therefore, when you must ''verify that RDMA and required Windows Server settings are configured properly on each server'' prior to building the cluster, the documented and supported method is to run Validate-DCB on each Hyper-V host with SET. This aligns with the exam objectives for validating network offloads and SMB Direct for cluster deployments in hybrid infrastructures.

Question 9

Question Type: MultipleChoice

You have an Active Directory Domain Services (AD DS) domain. The domain contains a member server named Server1 that runs Windows Server.

You need to ensure that you can manage password policies for the domain from Serve1.

Which command should you run first on Server1?

Options:

A- Install-Windows Feature RSAT-AO-PowerShell
B- Install-Windows Feature 6PHC
C- Install-Windows Feature RSAT-AD-Tool$
D- Install-windows Feature RSAT-AWIMS

Answer:

C

Explanation:

In Windows Server hybrid environments, domain password policy and fine-grained password policy (PSO) administration is performed with the Active Directory administration tools. The AZ-800 study domain states that to ''manage AD DS, including users, groups, OUs, Group Policy, and fine-grained password policies from a member server, you must first install the Remote Server Administration Tools (RSAT) for Active Directory.'' The RSAT AD DS package (RSAT-AD-Tools) installs Active Directory Users and Computers (ADUC), Active Directory Administrative Center (ADAC) (which includes the Password Settings container UI), and Windows PowerShell for Active Directory (the ActiveDirectory module). The guidance further clarifies: ''ADAC exposes Password Settings Objects (PSOs) and lets administrators create, link, and manage fine-grained password and lockout policies without signing in to a domain controller.'' Therefore, on Server1 the first required command is: Install-WindowsFeature RSAT-AD-Tools. Options for only PowerShell, DHCP, or WINS features do not provide ADAC/ADUC and cannot manage PSOs or domain password policies from a member server.

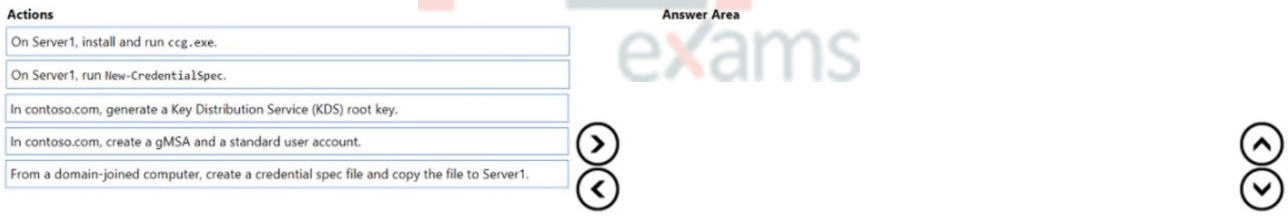
Question 10

Question Type: OrderList

Your network contains an Active Directory domain named contoso.com. The domain contains group managed service accounts (gMSAs). You have a server named Server1 that runs Windows Server and is in a workgroup. Server! hosts Windows containers.

You need to ensure that the Windows containers can authenticate to contoso.com.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

In contoso.com, generate a Key Distribution Service (KDS) root key.In contoso.com, create a gMSA and a standard user account.From a domain-joined computer, create a credential spec file and copy the file to Server1.

Question 11

Question Type: MultipleChoice

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com.

You need to identify which server is the PDC emulator for the domain.

Solution: From Active Directory Sites and Services, you right-click Default-First-Site-Name in the console tree, and then select Properties.

Does this meet the goal?

Options:

A- Yes
B- No

Answer:

B

Explanation:

The course content distinguishes site management from FSMO role administration. Active Directory Sites and Services is used to manage sites, subnets, site links, replication topology, and server objects (NTDS Settings), not domain or forest operations master roles. The documentation explains that FSMO roles are either forest-wide (Schema, Domain Naming) or domain-wide (RID, PDC, Infrastructure) and are exposed via ADUC (domain roles), Active Directory Domains and Trusts (Domain Naming), and Active Directory Schema (Schema), or by command-line tools like NETDOM and NTDSUTIL. Right-clicking Default-First-Site-Name and opening Properties shows site-level configuration (e.g., inter-site transports, licensing, location metadata) but does not display FSMO role holders. Consequently, the proposed action does not meet the goal of identifying the PDC Emulator. To meet the goal, use ADUC Operations Masters, netdom query fsmo, or ntdsutil roles as laid out in the administration guide.