



Microsoft AZ-802 Dumps

Shared by Fitzgerald on 23-09-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AZ-802 Mix Questions IN THIS CASE STUDY

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains servers that run Windows Server and store BitLocker recovery keys in AD DS. A server named Server1 starts in BitLocker recovery mode. You need to identify the BitLocker recovery key for Server1. Solution: From Active Directory Users and Computers, you use BitLocker Recovery Password Viewer. Does this meet the goal?

Options:

A- Yes

B- No

Answer:

A

Question 2

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AZ-802 Mix Questions IN THIS CASE STUDY

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains servers that run Windows Server and store BitLocker recovery keys in AD DS. A server named Server1 starts in BitLocker recovery mode. You need to identify the BitLocker recovery key for Server1. Solution: You run ntdsutil.exe on a domain controller. Does this meet the goal?

Options:

A- Yes

B- No

Answer:

B

Explanation:

ntdsutil.exe is a command-line management utility for the AD DS database itself, used for tasks such as performing authoritative restores, seizing or transferring FSMO roles, database integrity checks and defragmentation, managing application directory partitions, and Directory Services Restore Mode password resets; it has no built-in command, menu, or capability for browsing individual object attributes such as the ms-FVE-RecoveryPassword value stored on a msFVE-RecoveryInformation child object, and it provides no interface at all for reading or exporting BitLocker recovery data. Retrieving a BitLocker recovery password stored in AD DS requires either the BitLocker Recovery Password Viewer snap-in for Active Directory Users and Computers, which adds a dedicated tab to a computer object's properties specifically to display associated recovery passwords, or direct inspection of the msFVE-RecoveryInformation child objects through a general-purpose LDAP tool such as ADSI Edit or an equivalent PowerShell query against the directory; ntdsutil operates at the database/role-management level and simply has no code path that surfaces this attribute value to an administrator. Because running ntdsutil.exe on a domain controller does not read, display, or export any BitLocker recovery password, and no combination of its available commands can be used to obtain one, this solution does not meet the stated goal of identifying Server1's recovery key.

Question 3

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AZ-802 Mix Questions IN THIS CASE STUDY

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains servers that run Windows Server and store BitLocker recovery keys in AD DS. A server named Server1 starts in BitLocker recovery mode. You need to identify the BitLocker recovery key for Server1. Solution:

You run repair-bde.exe by using a BitLocker key package exported from AD DS. Does this meet the goal?

Options:

A- Yes

B- No

Answer:

B

Explanation:

repair-bde.exe is a disk-repair utility, not a lookup or reporting tool: its purpose is to attempt to decrypt or repair a corrupted BitLocker-protected volume when normal unlock methods have failed, and it accepts either a recovery password or a previously exported BitLocker key package (a file containing the actual encryption keys needed to decrypt sectors directly) as the credential it uses to perform that repair; running it does not display, output, or otherwise identify the volume's 48-digit numerical recovery password value to the administrator at all, and a key package is a different artifact from the recovery password that would actually need to be entered at Server1's BitLocker recovery screen to unlock it through the normal recovery workflow. The stated goal is specifically to identify the recovery key, meaning to determine and retrieve its value, not to repair or decrypt a damaged volume using key material that must already have been exported in advance; even successfully running repair-bde with an exported key package would leave the administrator no closer to knowing what Server1's recovery password actually is, and it does nothing to address a server that is simply sitting at the BitLocker recovery prompt waiting for a password rather than suffering from actual volume corruption. Because this solution does not retrieve or display the recovery key, it does not meet the stated goal.

Question 4

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AZ-802 Mix Questions IN THIS CASE STUDY

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Your network contains

an Active Directory Domain Services (AD DS) domain. The domain contains servers that run Windows Server and store BitLocker recovery keys in AD DS. A server named Server1 starts in BitLocker recovery mode. You need to identify the BitLocker recovery key for Server1. Solution: You use ADSI Edit and view the properties of the Server1 computer object. Does this meet the goal?

Options:

A- Yes

B- No

Answer:

A

Explanation:

When BitLocker recovery information is configured to be backed up to AD DS, each protected volume's recovery data is stored as one or more msFVE-RecoveryInformation objects, which AD DS creates as child objects underneath the corresponding computer object, here Server1's own computer object; each such child object carries the ms-FVE-RecoveryPassword attribute holding the 48-digit numerical recovery password along with an ms-FVE-RecoveryGuid used to match it to the correct BitLocker key protector. ADSI Edit is a low-level LDAP editor capable of navigating directly to any object in the directory, including drilling down into a computer object's child objects, so using ADSI Edit to view Server1's computer object and its msFVE-RecoveryInformation children is one of the two methods Microsoft documents for retrieving an AD DS-stored BitLocker recovery password when the more convenient BitLocker Recovery Password Viewer for Active Directory Users and Computers snap-in is not installed or not preferred; the recovery password read from that child object's attribute is entered at the BitLocker recovery screen to unlock Server1. Because this approach correctly reaches the actual location where the recovery password is stored in AD DS and retrieves the exact value needed, it does meet the stated goal of identifying Server1's BitLocker recovery key.

Question 5

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AZ-802 Mix Questions IN THIS CASE STUDY

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains a domain controller named DC1 and a member server named Server1. Users cannot sign in to Server1 by using domain credentials and receive the following error message: The trust relationship between this workstation and the primary domain failed. You need to restore domain authentication on Server1 without removing Server1 from the domain. Solution: From Server1, you run `Add-Computer -DomainName contoso.com -Server DC1`. Does this meet the goal?

Options:

A- Yes

B- No

Answer:

A

Explanation:

Running `Add-Computer -DomainName contoso.com -Server DC1` against domain administrator credentials from a computer that is already a member of contoso.com re-establishes Server1's domain membership against the specified domain controller: rather than requiring an explicit prior removal from the domain, the join operation detects the existing computer account for Server1 in AD DS, and with appropriate rights re-associates Server1 with that account, resetting and resynchronizing the computer account's password on both Server1 and DC1 as part of completing the join, which repairs the same underlying password mismatch responsible for the trust relationship failed error. Because the account itself is reused (not deleted and recreated) and Server1 remains continuously a member computer object of contoso.com throughout the operation, this satisfies the requirement to restore authentication without removing Server1 from the domain, even though the mechanism is a rejoin-style operation rather than a dedicated secure-channel-repair cmdlet. In practice, this is a commonly documented alternate remediation for a broken secure channel when `Test-ComputerSecureChannel -Repair` or `Reset-ComputerMachinePassword` are unavailable or insufficient, since the join process inherently resets the shared password consistently on both sides, restoring the secure channel and domain authentication on Server1 without any domain-wide or server-wide configuration changes and without an explicit disjoin step.

Question 6

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AZ-802 Mix Questions IN THIS CASE STUDY

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains a domain controller named DC1 and a member server named Server1. Users cannot sign in to Server1 by using domain credentials and receive the following error message: The trust relationship between this workstation and the primary domain failed. You need to restore domain authentication on Server1 without removing Server1 from the domain. Solution: From Server1, you run `Reset-ComputerMachinePassword -Server DC1`. Does this meet the goal?

Options:

A- Yes

B- No

Answer:

A

Explanation:

`Reset-ComputerMachinePassword` is a PowerShell cmdlet designed specifically to reset a computer's domain account password directly against a specified domain controller, and when run locally on the affected computer itself, here Server1, targeting DC1 with `-Server`, it resets and resynchronizes the computer account's password on both sides of the secure channel: it generates a new password, writes it to the Server1\$ computer account object on DC1, and simultaneously updates Server1's own local machine-account secret to match, in a single coordinated operation. Because both the AD DS side and the local Server1 side of the shared secret end up holding the same new password value, the secure channel between Server1 and the domain is fully restored, resolving the trust relationship failed error. This is done without removing Server1 from the domain at any point, satisfying the stated constraint, and without changing any domain-wide or server-wide authentication policy setting. This cmdlet, along with `Test-ComputerSecureChannel -Repair`, is one of Microsoft's two documented, non-disruptive remediation methods for a broken computer secure channel, both of which succeed precisely because they update the password consistently on both the local computer and the domain

controller rather than on only one side, unlike a solution that touches only the AD DS-stored value.

Question 7

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AZ-802 Mix Questions IN THIS CASE STUDY

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains a domain controller named DC1 and a member server named Server1. Users cannot sign in to Server1 by using domain credentials and receive the following error message: The trust relationship between this workstation and the primary domain failed. You need to restore domain authentication on Server1 without removing Server1 from the domain. Solution: From Server1, you run Set-ADAccountPassword -Identity "Server1\$" -Reset. Does this meet the goal?

Options:

- A- Yes
- B- No

Answer:

B

Explanation:

A broken trust relationship exists because the computer account password Server1 has stored locally no longer matches the password value AD DS holds for the Server1\$ computer account, and repairing the secure channel requires both sides of that shared secret to be resynchronized to the same value. Set-ADAccountPassword -Identity 'Server1\$' -Reset changes only the AD DS side of that shared secret: it sets a new password value on the computer account object as stored in the directory, but it has no mechanism to also update the local secret Server1 itself has cached, since Set-ADAccountPassword is an Active Directory module cmdlet that operates purely against the directory over LDAP/Kerberos and never touches a computer's local machine-account secret store. After running this cmdlet, the two sides of the secure channel are now mismatched

in the opposite direction from before (AD DS has the new password, Server1 still has the old one), which does not restore the trust relationship at all and can, in practice, leave the account in exactly the same broken state or worse. Restoring the secure channel properly requires a cmdlet or tool that updates both sides together, such as Test-ComputerSecureChannel -Repair or Reset-ComputerMachinePassword run from Server1 itself, neither of which this solution uses, so this solution does not meet the goal.

Question 8

Question Type: MultipleChoice

Case Study: Mix Questions

Mix Questions

AZ-802 Mix Questions IN THIS CASE STUDY

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains a domain controller named DC1 and a member server named Server1. Users cannot sign in to Server1 by using domain credentials and receive the following error message: The trust relationship between this workstation and the primary domain failed. You need to restore domain authentication on Server1 without removing Server1 from the domain. Solution: From Server1, you run Test-ComputerSecureChannel -Repair. Does this meet the goal?

Options:

- A- Yes
- B- No

Answer:

A

Explanation:

The trust relationship between this workstation and the primary domain failed error means the shared secret (the computer account's password) that Server1 stores locally no longer matches the password value stored for Server1's computer account in AD DS, breaking the secure channel Server1 needs to authenticate domain sign-ins. Test-ComputerSecureChannel is the PowerShell cmdlet specifically built to test, and with the -Repair switch, restore, that secure channel: when

run with -Repair (optionally supplying domain administrator credentials via -Credential if the caller's own cached credentials are insufficient), it resynchronizes Server1's local computer account password with the value AD DS expects, using the same underlying mechanism as Netlogon's channel-repair logic, without requiring Server1 to be removed from and rejoined to the domain and without requiring any domain-wide or server-wide configuration change. Because this directly restores password synchronization on both sides of the secure channel in a single, targeted operation scoped to Server1 alone, it fully satisfies the stated goal of restoring domain authentication without removing Server1 from the domain. This is, in fact, Microsoft's documented first-line remediation for this exact error message, ahead of more disruptive options such as Reset-ComputerMachinePassword or a full disjoin/rejoin, both of which are typically reserved for cases where Test-ComputerSecureChannel -Repair itself fails to resolve the broken channel.



Question 9

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

AZ-802 Mix Questions IN THIS CASE STUDY

You have a Hyper-V host named HV1 that contains a virtual machine named VM1.

VM1 has Dynamic Memory enabled. HV1 contains a PCIe NVMe storage device named Device1 that supports Discrete Device Assignment (DDA) and is disabled on HV1.

You need to ensure that Device1 can be assigned directly to VM1 by using DD

What should you do? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.



Answer Area

Preparation:

- Save VM1.
- Pause VM1.
- Shut down HV1.
- Shut down VM1

Memory configuration on VM1:

- Disable Dynamic Memory
- Set Memory weight to High.
- Increase the memory buffer.

PCIe NVMe configuration on HV1:

- Enable Device1.
- Remove Device1.
- Dismount Device1

P2P exams

Answer:

See the Answer in the Premium Version!

Question 10

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

AZ-802 Mix Questions IN THIS CASE STUDY

You have a Hyper-V host named HV1 that contains a virtual machine named VM1. HV1 supports nested visualization. VM1 is connected to an external virtual switch.

You plan to install the Hyper-V server role on VM1.

You need to prepare VM1 to host nested virtual machines. The solution must meet the following requirements:

- * Enable VM1 to run Hyper-V.
- * Enable nested virtual machines to communicate on the physical LAN.

How should you configure VM1? To answer, select the appropriate options in the answer are

a. NOTE: Each correct selection is worth one point.

Answer Area

Processor configuration:

- Select Use Hardware Topology.
- Expose virtualization extensions.
- Enable processor compatibility mode.
- Increase the number of virtual processors.

Network configuration:

- Enable NIC Teaming.
- Enable Router Guard.
- Configure port mirroring.
- Enable MAC Address spoofing

Answer:

See the Answer in the Premium Version!

Question 11

Question Type: Hotspot

Case Study: Mix Questions

Mix Questions

AZ-802 Mix Questions IN THIS CASE STUDY

You have an Azure virtual machine scale set named vmssWeb

vmssWeb hosts identical virtual machines that run Windows Server and have the Web Server (IIS) server role installed. vmssWeb has a fixed capacity of 10 virtual machine instances.

Monitoring shows the following patterns:

- * On Saturdays and Sundays, vmssWeb requires only two virtual machine instances by 7:00 AM.
- * During business days, launches by your company's marketing department can cause unpredictable processor demand.

You need to configure capacity management for vmssWeb. The solution must meet the following requirements:

- * Automatically set weekend capacity to two virtual machine instances
- * Increase capacity during business-day demand spikes.
- * Minimize manual intervention.

What should you configure for each requirement? To answer, select the appropriate options in

the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Weekend capacity: 

Configure manual scaling.

Resize the virtual machine instances.

Configure a recurring autoscale profile

Configure a fixed-date autoscale profile.

Business-day demand spikes:

Configure a manual scale increase.

Configure a metric scale-out rule

Resize the virtual machine instances.

Configure a scheduled scale-out profile.

P2P
exams

Answer:

See the Answer in the Premium Version!

P2P
exams

To Get Premium Files for AZ-802 Visit

<https://www.p2pexams.com/products/az-802>

For More Free Questions Visit

<https://www.p2pexams.com/microsoft/pdf/az-802>

20%
DISCOUNT

P2P
exams