AZ-800Q&As

Administering Windows Server Hybrid Core Infrastructure

Pass Microsoft AZ-800 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.passapply.com/az-800.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

HOTSPOT

Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains the VPN servers shown in the following table.

Name	IP address
VPN1	172.16.0.254
VPN2	131.10.15.254
VPN3	10.10.0.254

You have a server named NPS1 that has Network Policy Server (NPS) installed. NPS1 has the following RADIUS clients:

```
Name                          : NPSclient1
Address                       : 172.16.0.254
AuthAttributeRequired         : False
SharedSecret                  : Pa55w.rd
VendorName                    : RADIUS Standard
Enabled                       : False

Name                          : NPSclient2
Address                       : 131.10.15.254
AuthAttributeRequired         : False
SharedSecret                  : Pa55w.rd
VendorName                    : RADIUS Standard
Enabled                       : True

Name                          : NPSclient3
Address                       : 172.16.1.254
AuthAttributeRequired         : False
SharedSecret                  : Pa55w.rd
VendorName                    : RADIUS Standard
Enabled                       : True
```

VPN1, VPN2, and VPN3 use NPS1 for RADIUS authentication. All the users in contoso.com are allowed to establish VPN connections.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Statements	Yes	No
The contoso.com users can authenticate successfully when they establish a VPN connection to VPN1.	○	○
The contoso.com users can authenticate successfully when they establish a VPN connection to VPN2.	○	○
The contoso.com users can authenticate successfully when they establish a VPN connection to VPN3.	○	○

Correct Answer:

Statements	Yes	No
The contoso.com users can authenticate successfully when they establish a VPN connection to VPN1.	○	○
The contoso.com users can authenticate successfully when they establish a VPN connection to VPN2.	○	○
The contoso.com users can authenticate successfully when they establish a VPN connection to VPN3.	○	○

It is important to remember that the client computers that are connecting to the VPNs are not RADIUS clients. The VPN servers are the RADIUS clients. You configure the RADIUS clients on the RADIUS server (NPS1) server to allow the

VPN servers to use NPS1 to authenticate the connections.

Box 1: No

NPSClient1 is not enabled.

Box 2: Yes

NPSClient2 is configured correctly. It is enabled and has the correct IP address of VPN2.

Box 3: No

NPSClient3 has an incorrect IP address configured for VPN3.

QUESTION 2

You should fulfill the security requirements.

How do you configure the remote administration?

A. Use the Azure Bastion host

B. Use Azure AD Privileged Identity Management (PIM)

C. Just in time (JIT) VM access

D. Use the Remote Desktop extension for Azure Cloud Services

Correct Answer: C

QUESTION 3

Please finish the following requirement on Azure Active Directory Domain Services (Azure AD DS) domain named contoso.com.

You need to provide a solution to administrator with the ability to manage Group Policy Objects (GPOs). The principle of least privilege must be fulfilled.

You need to you add the administrator to the group:

A. AAD DC Administrators

B. Enterprise Admins

C. Schema Admins

D. Domain Admins

Correct Answer: B

QUESTION 4

HOTSPOT

You plan to deploy an Azure virtual machine that will run Windows Server.

You need to ensure that an Azure Active Directory (Azure AD) user named user1@contoso.com can connect to the virtual machine by using the Azure Serial Console.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Configure on the Azure virtual machine:
- Boot diagnostics with a custom storage account
- Operating system guest diagnostics
- A system-assigned managed identity

Assign the following role to User1:
- Virtual Machine Contributor
- Virtual Machine Administrator Login
- Virtual Machine User Login

Correct Answer:

Answer Area

Configure on the Azure virtual machine:
- **Boot diagnostics with a custom storage account**
- Operating system guest diagnostics
- A system-assigned managed identity

Assign the following role to User1:
- **Virtual Machine Contributor**
- Virtual Machine Administrator Login
- Virtual Machine User Login

Reference: https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/serial-console-overview

QUESTION 5

Your network contains a single-domain Active Directory Domain Services (AD DS) forest named contoso.com. The forest contains the servers shown in the following exhibit table.

Name	Description
DC1	Domain controller
Server1	Member server

You plan to install a line-of-business (LOB) application on Server1. The application will install a custom Windows service.

A new corporate security policy states that all custom Windows services must run under the context of a group managed service account (gMSA). You deploy a root key.

You need to create, configure, and install the gMSA that will be used by the new application.

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

NOTE: Each correct selection is worth one point

A. On Server1, run the setspncommand.

B. On DC1, run the New-ADServiceAccountcmdlet.

C. On Server1, run the Install-ADServiceAccountcmdlet.

D. On Server1, run the Get-ADServiceAccountcmdlet.

E. On DC1, run the Set-ADComputercmdlet.

F. On DC1, run the Install-ADServiceAccountcmdlet.

Correct Answer: BE

Step 1: Provisioning group Managed Service Accounts

(B) Create a gMSA using the New-ADServiceAccount cmdlet.

Step 2: Configuring service identity application service If using security groups for managing member hosts, add the computer account for the new member host to the security group (that the gMSA\\'s member hosts are a member of). To add member hosts using the Set-ADServiceAccount cmdlet

1.

On the Windows Server 2012 domain controller (DC1, not Server1), run Windows PowerShell from the Taskbar.

2.

At the command prompt for the Windows PowerShell Active Directory module, type the following commands, and then press ENTER:

3.

Get-ADServiceAccount [-Identity] -Properties PrincipalsAllowedToRetrieveManagedPassword

4.

(E) At the command prompt for the Windows PowerShell Active Directory module, type the following commands, and then press ENTER:

5.

Set-ADServiceAccount [-Identity] -PrincipalsAllowedToRetrieveManagedPassword

6.

Etc.

Reference: https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts