Free Questions for AZ-801

Shared by Lester on 04-10-2024

For More Free Questions and Preparation Resources

Question 1

You have a failover cluster named FC1 that contains two nodes named Server1 and Server2. FC1 is configured to use a file share witness.

You plan to configure FC1 to use a cloud witness.

You need to configure Azure Storage accounts for the cloud witness.

Which storage account type and authorization method should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Storage account type:

| Premium block blobs |
| Premium file shares |
| Premium page blobs |
| Standard |

Answer:

method:

| Access key |
| Shared access signature (SAS) |
| System-assigned managed identity in Azure Active Directory (Azure AD) |
| User-assigned managed identity in Azure Active Directory (Azure AD) |

Answer:

Explanation:

https://docs.microsoft.com/en-us/windows-server/failover-clustering/deploy-cloud-witness

Question 2

Question Type: MultipleChoice

You have a failover cluster named Cluster1 that has the following configurations:

Number of nodes: 6

Quorum: Dynamic quorum

Witness: File share, Dynamic witness

What is the maximum number of nodes that can fail simultaneously while maintaining quorum?

Options:

A- 1

B- 2

C- 3

D- 4

E- 5

Answer:

C

Explanation:

Note this question is asking about nodes failing 'simultaneously', not nodes failing one after the other.

With six nodes and one witness, there are seven votes. To maintain quorum there needs to be four votes available (four votes is the majority of seven). This means that a minimum of three nodes plus the witness need to remain online for the cluster to function. Therefore, the maximum number of simultaneous failures is three.

https://docs.microsoft.com/en-us/windows-server/storage/storage-spaces/understand-quorum
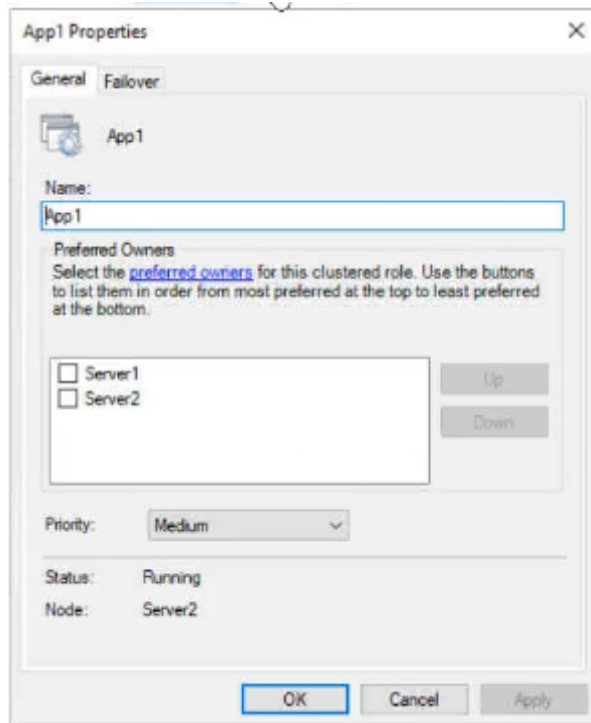
Question 3

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. Some question sets might have more than one correct solution, while others might not have a correct solution.
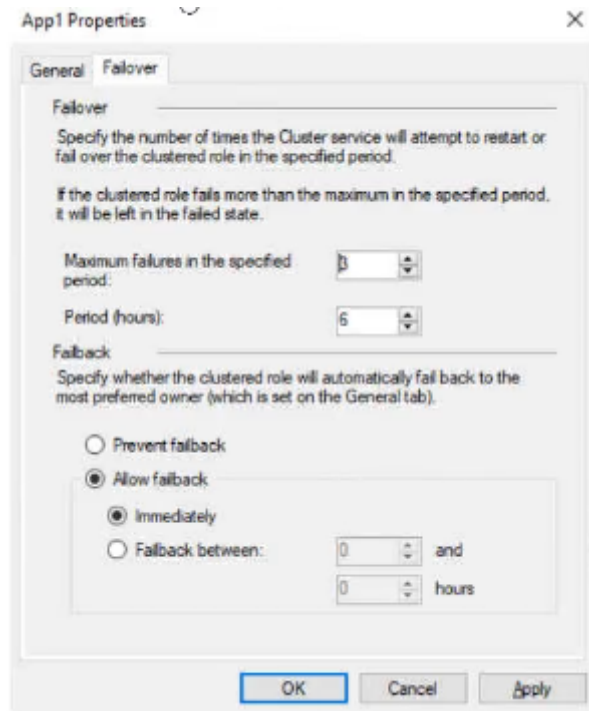
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a failover cluster named Cluster1 that hosts an application named App1.

The General tab in App1 Properties is shown in the General exhibit. (Click the General tab.)

The Failover tab in App1 Properties is shown in the Failover exhibit. (Click the Failover tab.)

App1 Properties

General Failover

Failover

Specify the number of times the Cluster service will attempt to restart or fail over the clustered role in the specified period.

If the clustered role fails more than the maximum in the specified period, it will be left in the failed state.

Maximum failures in the specified period: 3

Period (hours): 6

Fallback

Specify whether the clustered role will automatically fail back to the most preferred owner (which is set on the General tab).

○ Prevent failback
◉ Allow failback
  ◉ Immediately
  ○ Failback between: 0 and
                       0 hours

OK   Cancel   Apply

Server1 shuts down unexpectedly.

You need to ensure that when you start Server1, App1 continues to run on Server2.

Solution: From the General settings, you move Server2 up.

Does this meet the goal?

Options:

A- Yes

B- No

Answer:

B

Explanation:

Server1 and Server2 are both unticked so the order they are listed in has no effect on whether the cluster will fail back.
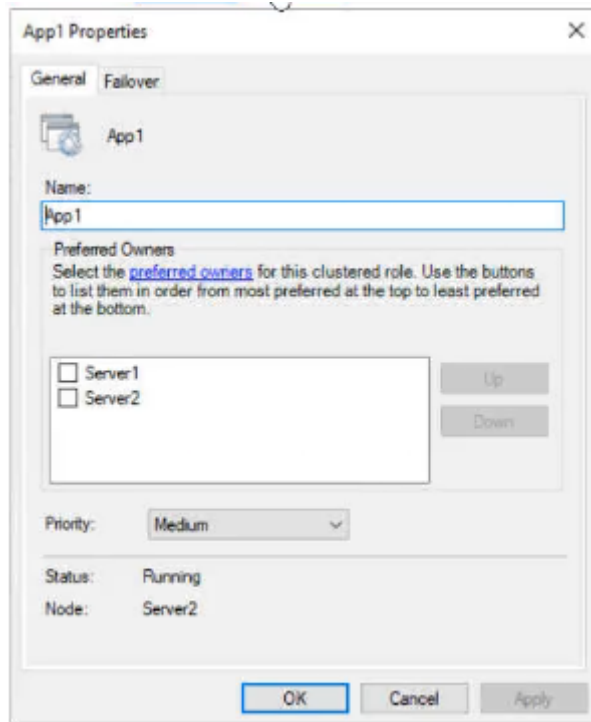
Question 4

Question Type: **MultipleChoice**

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. Some question sets might have more than one correct solution, while others might not have a correct solution.
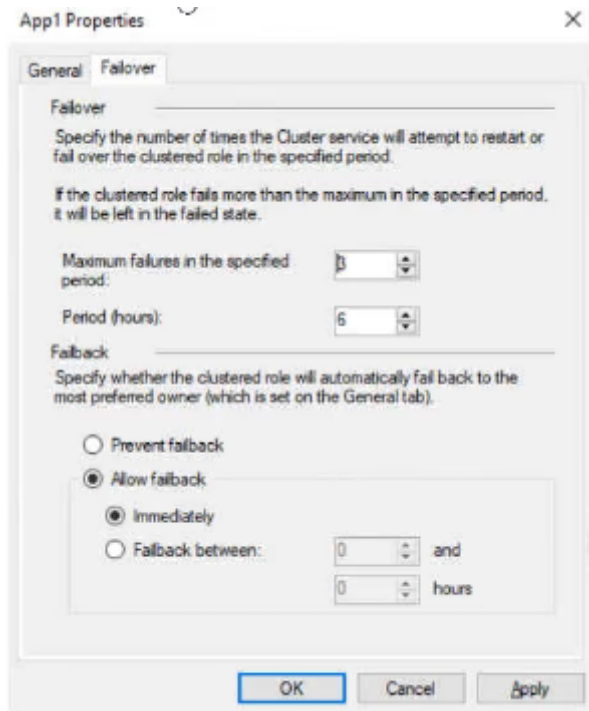
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a failover cluster named Cluster1 that hosts an application named App1.

The General tab in App1 Properties is shown in the General exhibit. (Click the General tab.)

The Failover tab in App1 Properties is shown in the Failover exhibit. (Click the Failover tab.)

App1 Properties

General | Failover

Failover

Specify the number of times the Cluster service will attempt to restart or fail over the clustered role in the specified period.

If the clustered role fails more than the maximum in the specified period, it will be left in the failed state.

Maximum failures in the specified period: 3

Period (hours): 6

Failback

Specify whether the clustered role will automatically fail back to the most preferred owner (which is set on the General tab).

○ Prevent failback
◉ Allow failback
  ◉ Immediately
  ○ Failback between: 0 and
    0 hours

OK | Cancel | Apply

Server1 shuts down unexpectedly.

You need to ensure that when you start Server1, App1 continues to run on Server2.

Solution: You increase Maximum failures in the specified period for the App1 cluster role.

Does this meet the goal?

Options:

A- Yes

B- No

Answer:

B

Explanation:

The Maximum failures setting is used to determine when the cluster determines that a node is offline. It does not affect whether a cluster will fail back when a node comes online.
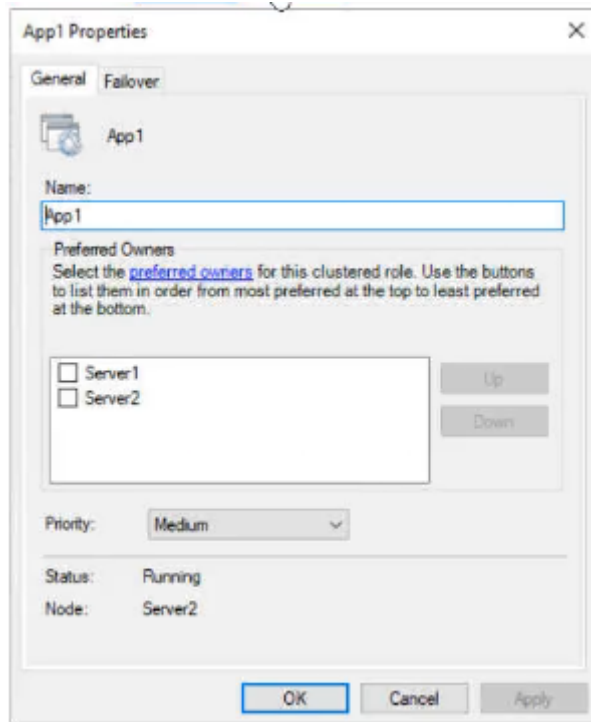
Question 5

Question Type: **MultipleChoice**

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. Some question sets might have more than one correct solution, while others might not have a correct solution.
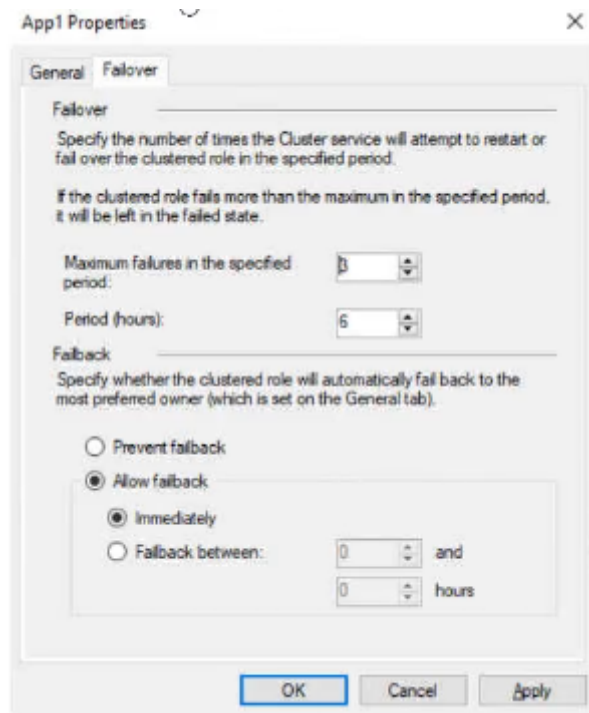
After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a failover cluster named Cluster1 that hosts an application named App1.

The General tab in App1 Properties is shown in the General exhibit. (Click the General tab.)

The Failover tab in App1 Properties is shown in the Failover exhibit. (Click the Failover tab.)

App1 Properties   ✕

General Failover

Failover

Specify the number of times the Cluster service will attempt to restart or fail over the clustered role in the specified period.

If the clustered role fails more than the maximum in the specified period, it will be left in the failed state.

Maximum failures in the specified period: 3 ⬍

Period (hours):   6 ⬍

Failback

Specify whether the clustered role will automatically fail back to the most preferred owner (which is set on the General tab).

◯ Prevent failback
◉ Allow failback
  ◉ Immediately
  ◯ Failback between: 0 ⬍ and
                        0 ⬍ hours

OK   Cancel   Apply

Server1 shuts down unexpectedly.

You need to ensure that when you start Server1, App1 continues to run on Server2.

Solution: From the Failover settings, you select Prevent failback.

Does this meet the goal?

Options:

A- Yes

B- No

Answer:

A

Explanation:

The Prevent failback setting will prevent the cluster failing back to Server1.

Question 6

Question Type: MultipleChoice

You have an Azure virtual machine named VM1.

You enable Microsoft Defender SmartScreen on VM1.

You need to ensure that the SmartScreen messages displayed to users are logged.

What should you do?

Options:

A- From a command prompt, run WinRM quickconfig.

B- From the local Group Policy, modify the Advanced Audit Policy Configuration settings.

C- From Event Viewer, enable the Debug log.

D- From the Windows Security app. configure the Virus & threat protection settings.

Answer:

C

Explanation:

https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-smartscreen/microsoft-defender-smartscreen-overview

Question 7

Question Type: MultipleChoice

You have a server that runs Windows Server. The server is configured to encrypt all incoming traffic by using a connection security rule.

You need to ensure that Server1 can respond to the unencrypted tracert commands initiated from computers on the same network.

What should you do from Windows Defender Firewall with Advanced Security?

Options:

A- From the IPsec Settings, configure IPsec defaults.

B- Create a new custom outbound rule that allows ICMPv4 protocol connections for all profiles.

C- Change the Firewall state of the Private profile to Off.

D- From the IPsec Settings, configure IPsec exemptions.

Answer:

D

Question 8

Question Type: MultipleChoice

Your network contains an Active Directory Domain Services (AD DS) domain. The domain contains two servers named Server1 and Server2 that run Windows Server.

You need to ensure that you can use the Computer Management console to manage Server2. The solution must use the principle of least privilege.

Which two Windows Defender Firewall with Advanced Security rules should you enable on Server2? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

Options:

A- the COM+ Network Access (DCOM-In) rule

B- all the rules in the Remote Event Log Management group

C- the Windows Management Instrumentation (WMI-In) rule

D- the COM+ Remote Administration (DCOM-In) rule

E- the Windows Management Instrumentation (DCOM-In) rule

Answer:

A, B

Explanation:

Question 9

Question Type: **MultipleChoice**

You have an Azure virtual machine named VM1 that runs Windows Server.

You need to encrypt the contents of the disks on VM1 by using Azure Disk Encryption.

What is a prerequisite for implementing Azure Disk Encryption?

Options:

A- Customer Lockbox for Microsoft Azure

B- an Azure key vault

C- a BitLocker recovery key

D- data-link layer encryption in Azure

Answer:

B

Explanation:

https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-overview

Question 10

Question Type: **MultipleChoice**

You have 10 servers that run Windows Server in a workgroup.

You need to configure the servers to encrypt all the network traffic between the servers. The solution must be as secure as possible.

Which authentication method should you configure in a connection security rule?

Options:

A- NTLMv2

B- pre-shared key

C- KerberosV5

D- computer certificate

Answer:

D

Explanation:

https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-authentication-request-rule