Vendor: Microsoft

Exam Code: AZ-801

Exam Name: Configuring Windows Server Hybrid Advanced Services

Version: DEMO

QUESTION 1
Case Study 1 - Fabrikam inc
Overview
Fabrikam, Inc. is a manufacturing company that has a main office in Chicago and a branch office in Paris.

Existing Environment
Identity Infrastructure
Fabrikam has an Active Directory Domain Services (AD DS) forest that syncs with an Azure Active Directory (Azure AD) tenant. The AD DS forest contains two domains named corp.fabrikam.com and europe.fabrikam.com.

Chicago Office On-Premises Servers
The office in Chicago contains on-premises servers that run Windows Server 2016 as shown in the following table.

Name	Type	Configuration
HV1	Physical	Hyper-V host
HV2	Physical	Hyper-V host
APP1	Virtual machine	Application server
APP2	Virtual machine	Application server
APP3	Virtual machine	Application server
APP4	Virtual machine	Application server
DC1	Virtual machine	Domain controller
Archive1	Physical	File server
DHCP1	Virtual machine	DHCP server
Fileserver1	Virtual machine	File server
WEB1	Virtual machine	Web server
WEB2	Virtual machine	Web server
AADC1	Virtual machine	Azure AD Connect

You are remediating the firewall security risks to meet the security requirements.

What should you configure to reduce the risks?

A. a Group Policy Object (GPO)
B. adaptive network hardening in Microsoft Defender for Cloud
C. a network security group (NSG) in Sub1
D. an Azure Firewall policy

Answer: A
Explanation:
Firewall rules configured in a Group Policy Object cannot be modified by local server administrators.
Reference:

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

QUESTION 2
Case Study 2 - Contoso, Ltd
Overview

Contoso, Ltd. is a manufacturing company that has a main office in Seattle and branch offices in Los Angeles and Montreal.

Existing Environment
Active Directory Environment

Contoso has an on-premises Active Directory Domain Services (AD DS) domain named contoso.com that syncs with an Azure Active Directory (Azure AD) tenant. The AD DS domain contains the domain controllers shown in the following table.

Name	Operating system	Operation master role
DC1	Windows Server 2012 R2	RID master, schema master
DC2	Windows Server 2016	PDC emulator, infrastructure master
DC3	Windows Server 2016	Domain naming master

Contoso recently purchased an Azure subscription.

The functional level of the forest is Windows Server 2012 R2. The functional level of the domain is Windows Server 2012. The forest has the Active Directory Recycle Bin enabled.

You need to meet the technical requirements for Cluster3.

What should you include in the solution?

A. Enable integration services on all the virtual machines.
B. Add a Windows Server server role.
C. Configure a fault domain doe the cluster.
D. Add a failover cluster role.

Answer: D
Explanation:
The Hyper-V replica broker role is required on the cluster.
Reference:
https://docs.microsoft.com/en-us/virtualization/community/team-blog/2012/20120327-why-is-the-hyper-v-replica-broker-required

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 server named Server1 that runs Windows Server.

You need to ensure that only specific applications can modify the data in protected folders on Server1.

Solution: From Virus & threat protection, you configure Tamper Protection

Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Tamper Protection in Windows Security helps prevent malicious apps from changing important Microsoft Defender Antivirus settings, including real-time protection and cloud-delivered protection.
https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/customize-controlled-folders?view=o365-worldwide

QUESTION 4
You have 100 Azure virtual machines that run Windows Server. The virtual machines are onboarded to Microsoft Defender for Cloud.

You need to shut down a virtual machine automatically if Microsoft Defender for Cloud generates the "Antimalware disabled in the virtual machine" alert for the virtual machine.

What should you use in Microsoft Defender for Cloud?

A. a logic app
B. a workbook
C. a security policy
D. adaptive network hardening

Answer: A
Explanation:
Trigger automated response - provides the option to trigger a logic app as a response to this security alert.
https://docs.microsoft.com/en-us/azure/defender-for-cloud/managing-and-responding-alerts

QUESTION 5
You have a Microsoft Sentinel deployment and 100 Azure Arc-enabled on-premises servers. All the Azure Arc-enabled resources are in the same resource group.

You need to onboard the servers to Microsoft Sentinel. The solution must minimize administrative effort.

What should you use to onboard the servers to Microsoft Sentinel?

A. Azure Automation

B. Azure Policy
C. Azure virtual machine extensions
D. Microsoft Defender for Cloud

Answer: B
Explanation:
You can use Azure Policy to audit settings in the operating system of an Azure Arc-enabled server, if a setting is not compliant you can also trigger a remediation task (deployIfNotExists).
https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/manage/hybrid/server/best-practices/arc-policies-mma

QUESTION 6
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?

A. NTLMv2
B. pre-shared key
C. KerberosV5
D. computer certificate

Answer: D
Explanation:
Certificate form part of PKI (public key infrastructure), and are used for authentication and encryption purposes. Also, since they are workgroup based servers, NTLM and Kerberos cannot be suitable answers because these protocols are domain-based. Lastly, a pre-shared key is used to authenticate 2 VPN Gateways.
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/create-an-authentication-request-rule

QUESTION 7
Hotspot Question

Your network contains an on-premises Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains the accounts shown in the following table.

Name	Account type	In organizational unit (OU)
Admin1	User	OU1
Admin2	User	OU2
Server1	Computer	OU3
Server2	Computer	OU4

The domain is configured to store BitLocker recovery keys in Active Directory.
Admin1 and Admin2 perform the following configurations:
1. Admin1 turns on BitLocker Drive Encryption (BitLocker) for volume C on Server1.

2. Admin1 moves Server1 to OU1.
3. Admin2 turns on BitLocker for removable volume E on Server2.
4. Admin2 moves removable volume E from Server2 to Server1 and unlocks the volume.

On which Active Directory object can you view each BitLocker recovery key? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

The BitLocker recovery key for volume C:	Admin1 contoso.com OU1 OU3 Server1 TPM devices
The BitLocker recovery for key volume E:	Admin2 contoso.com OU4 Server1 Server2 TPM devices

Answer:

Answer Area

The BitLocker recovery key for volume C:	Admin1 contoso.com OU1 OU3 **Server1** TPM devices
The BitLocker recovery for key volume E:	Admin2 contoso.com OU4 Server1 **Server2** TPM devices

Explanation:
Box 1: Server1

You can configure Group Policies in your domain so that when encrypting any drive with BitLocker, the computer will save the recovery key in its computer object account in AD (like storing a local computer administrator password generated using LAPS).

Box 2: Server2

Reference:
http://woshub.com/store-bitlocker-recovery-keys-active-directory/

QUESTION 8
Your network contains an Active Directory Domain Services (AD DS) domain named contoso.com. The domain contains three domain controllers named DC1, DC2, and DC3.

You connect a Microsoft Defender for Identity instance to the domain.

You need to onboard all the domain controllers to Defender for Identity.

What should you run on the domain controllers?

A. AzureConnectedMachineAgent.msi
B. MARAgentInstaller,exe
C. Azure ATP Sensor setup,exe
D. MMASetup-AMD64.exe

Answer: C
Explanation:
Azure ATP uses data from sensors, known as Azure ATP Sensors, that are installed on your domain controllers. The ATP sensors monitor the domain controller network traffic for signs of malicious activity, as well as other security risks such as connections made with weak or insecure protocols.

QUESTION 9
You have a three-node failover cluster.

You need to run pre-scripts and post-scripts when Cluster-Aware Updating (CAU) runs. The solution must minimize administrative effort.

What should you use?

A. Scheduled tasks
B. Run profiles
C. Azure Functions
D. Windows Server Update Serveries (WSUS)

Answer: B
Explanation:
Cluster-Aware Updating advanced options and updating run profiles.
You can set the PreUpdateScript or PostUpdateScript the option.
Reference:
https://docs.microsoft.com/en-us/windows-server/failover-clustering/cluster-aware-updating-options

QUESTION 10
Your network contains an Active Directory Domain Services (AD DS> domain. The domain contains 20 Active Directory sites. All user management is performed from a central site.

You add users to a group.

You discover that group changes do NOT appear on a domain controller in a remote site.

You need to identify whether the group changes appear on other domain controllers.

What should you use?

A. Microsoft Support and Recovery Assistant
B. File Replication Service (FRS) Status Viewer
C. Active Directory Replication Status Tool
D. Active Directory Sites and Services

Answer: C
Explanation:
The Active Directory Replication Status Tool (ADREPLSTATUS) analyzes the replication status for domain controllers in an Active Directory domain or forest.
The Active Directory Replication Status Tool (ADREPLSTATUS) analyzes the replication status for domain controllers in an Active Directory domain or forest.
ADREPLSTATUS displays data in a format that is similar to REPADMIN /SHOWREPL * /CSV imported into Excel but with significant enhancements.
Specific capabilities for this tool include:
- Expose Active Directory replication errors occurring in a domain or forest
- Prioritize errors that need to be resolved in order to avoid the creation of lingering objects in Active Directory forests
- Help administrators and support professionals resolve replication errors by linking to Active Directory replication troubleshooting content on Microsoft TechNet
- Allow replication data to be exported to source or destination domain administrators or support professionals for offline analysis
Reference:
https://www.microsoft.com/en-us/download/details.aspx

QUESTION 11
You have an Azure virtual machine named VM1 that runs Windows Server.

When you attempt to install the Azure Performance Diagnostics extension on VM I, the installation fails.

You need to identify the cause of the installation failure.

What are two possible ways to achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Sign in to VM1 and verify the WaAppAgent.log file.
B. From the Azure portal, view the alerts for VM1.
C. From the Azure portal, view the activity log for VM1.
D. Sign in to VM1 and verify the MonitoringAgent.log file.

Answer: AC
Explanation:
Windows Azure Guest Agent Service: This service is the service that is responsible for all the logging in WAppAgent.log. This service is responsible for configuring various extensions and communication from Guest to Host.
Activity log: See activity log entries filtered for the current virtual machine. Use this log to view the recent activity of the machine, such as any configuration changes and when it was stopped and started.
Reference:
https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/performance-diagnostics-vm-extension
https://docs.microsoft.com/en-us/azure/azure-monitor/vm/monitor-virtual-machine-analyze

QUESTION 12
Your on-premises network has a 200-Mbps connection to Azure and contains a server named Server1 that stores 70 TB of data files.

You have an Azure Storage account named storage 1.

You plan to migrate the data files from Server1 to a blob storage container in storage!. Testing shows that copying the data files by using azcopy will take approximately 35 days.

You need to minimize how long it will take to migrate the data to Azure.

What should you use?

A. Storage Migration Service
B. Azure Storage Explorer
C. Azure Data Box
D. Azure File Sync

Answer: C
Explanation:
The Microsoft Azure Data Box cloud solution lets you send terabytes of data into and out of Azure in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device. Each storage device has a maximum usable storage capacity of 80 TB and is transported to your datacenter through a regional carrier. The device has a rugged casing to protect and secure data during the transit.
Reference:
https://docs.microsoft.com/en-us/azure/databox/data-box-overview

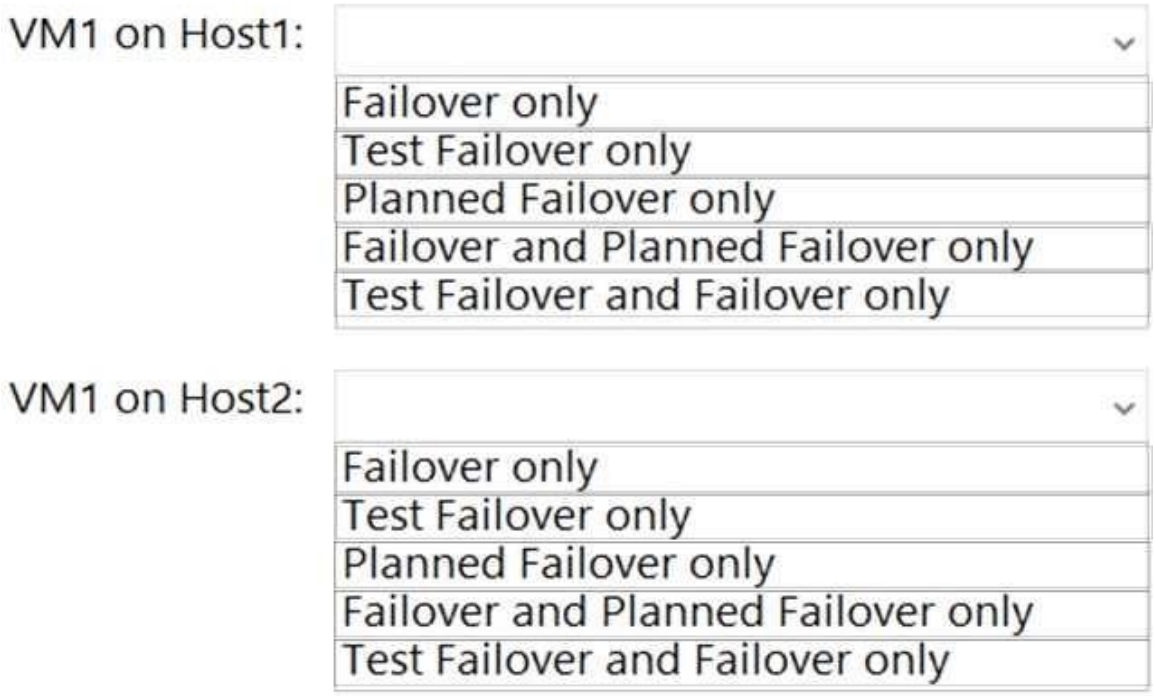
QUESTION 13
Hotspot Question

You have three servers named Host1, Host2, and VM1 that run Windows Server. Host1 and Host2 have the Hyper-V server role installed. VM1 is a virtual machine hosted on Host1.

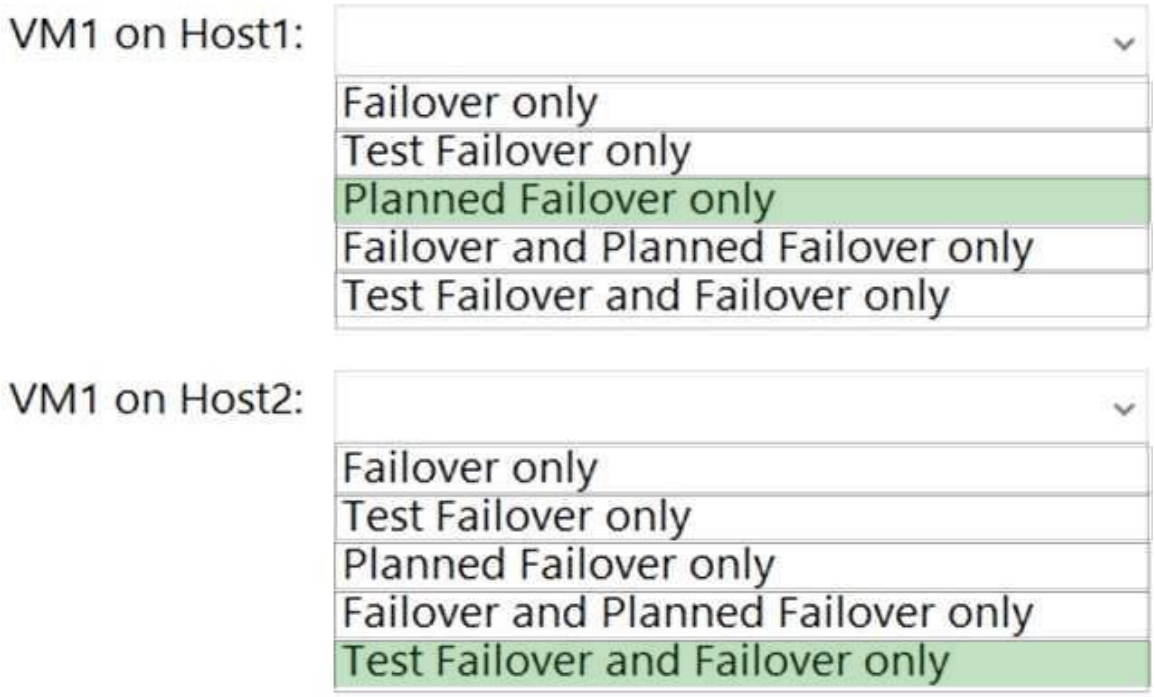
You configure VM1 to replicate to Host2 by using Hyper-V Replica.

Which types of failovers can you perform on VM1 on each host? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.



Answer:



Explanation:
Planned failover performs prerequisites checks to ensure zero data loss. It checks that the primary virtual machine is shut down before beginning the failover. After the virtual machine is failed over, it starts replicating the changes back to the primary site when it's available.

Failover. Pick the latest or other recovery point if configured. A new test virtual machine will be created and started on the secondary site.
Unplanned Failover from Hyper-V Manager or Failover Clustering Manager. You can recover from the latest recovery point or from
previous recovery points if this option is enabled.
https://learn.microsoft.com/en-us/windows-server/virtualization/hyper-v/manage/set-up-hyper-v-replica

QUESTION 14
You have an Azure virtual machine named VM1.
You install an application on VM1, and then restart the virtual machine.
After the restart, you get the following error message: "Boot failure. Reboot and Select proper Boot Device or Insert Boot Media in selected Boot Device."
You need to mount the operating system disk offline from VM1 to a temporary virtual machine to troubleshoot the issue.
Which command should you run in Azure CLI?

A. az vm repair create
B. az vm boot-diagnostics enable
C. az vm capture
D. az vm disk attach

Answer: A
Explanation:
Create a new repair VM and attach the source VM's copied OS disk as a data disk.
https://docs.microsoft.com/en-us/cli/azure/vm/repair?view=azure-cli-latest

QUESTION 15
You have an Azure virtual machine named VM1 that has the Web Server (IIS) server role installed.
VM1 hosts a critical line-of-business (LOB) application.
After the security team at your company deploys a new security baseline to VM1, users begin reporting that the application is unresponsive.
You suspect that the security baseline has caused networking issues.
You need to perform a network trace on VM1.
What should you do?

A. From VM1, run necscac.
B. From Performance Monitor on VM1. create a Data Collector Set.
C. From the Azure portal, configure the Diagnostics settings for VM1.
D. From the Azure portal, configure the Performance diagnostics settings for VM1.

Answer: D
Explanation:
Azure Files analysis
Includes all checks in the performance analysis, and captures a network trace and SMB counters.
https://docs.microsoft.com/en-us/troubleshoot/azure/virtual-machines/performance-diagnostics

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: **ASTR14**