

Vendor: Microsoft

Exam Code: AZ-303

Exam Name: Microsoft Azure Architect Technologies

QUESTION 1

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.
- Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- Designate a new user named Admin1 as the service admin for the Azure subscription.
- Admin1 must receive email alerts regarding service outages.
- Ensure that a new user named User3 can create network objects for the Azure subscription.

You need to recommend an identity solution that meets the technical requirements.

What should you recommend?

- A. password hash synchronization and single sign-on (SSO)
- B. federated single sign-on (SSO) and Active Directory Federation Services (AD FS)
- C. Pass-through Authentication and single sign-on (SSO)
- D. cloud-only user accounts

Answer: C

Explanation:

With Pass-through Authentication the on-premises passwords are never stored in the cloud in any form.

Scenario:

Prevent user passwords or hashes of passwords from being stored in Azure.

Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ptc>

QUESTION 2

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.

- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.
- Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- Designate a new user named Admin1 as the service admin for the Azure subscription.
- Admin1 must receive email alerts regarding service outages.
- Ensure that a new user named User3 can create network objects for the Azure subscription.

Hotspot Question

You need to identify the storage requirements for Contoso.

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 Area

Statements	Yes	No
Contoso requires a storage account that supports Blob storage.	<input type="radio"/>	<input type="radio"/>
Contoso requires a storage account that supports Azure Table storage.	<input type="radio"/>	<input type="radio"/>
Contoso requires a storage account that supports Azure File Storage.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Contoso requires a storage account that supports Blob storage.	<input checked="" type="radio"/>	<input type="radio"/>
Contoso requires a storage account that supports Azure Table storage.	<input type="radio"/>	<input checked="" type="radio"/>
Contoso requires a storage account that supports Azure File Storage.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

Scenario: Move the existing product blueprint files to Azure Blob storage.

Scenario: Use unmanaged standard storage for the hard disks of the virtual machines. Page blobs are optimized for writes at random locations within a blob. They also support Unmanaged Disks.

Scenario:

SQL Server Data Files in Microsoft Azure enables native support for SQL Server database files stored as blobs. It allows you to create a database in SQL Server running in on-premises or in a virtual machine in Microsoft Azure with a dedicated storage location for your data in Microsoft Azure Blob storage.

Box 2: No

Box 3: No

Reference:

<https://docs.microsoft.com/en-us/sql/relational-databases/databases/sql-server-data-files-in-microsoft-azure>

QUESTION 3

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.
- Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- Designate a new user named Admin1 as the service admin for the Azure subscription.
- Admin1 must receive email alerts regarding service outages.
- Ensure that a new user named User3 can create network objects for the Azure subscription.

Hotspot Question

You need to recommend a solution for App1. The solution must meet the technical requirements.

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

NOTE: Each correct selection is worth one point.

Answer Area

Number of virtual networks:

	▼
1	
2	
3	

Number of subnets per virtual network:

	▼
1	
2	
3	

Answer:

Answer Area

Number of virtual networks:

	▼
1	
2	
3	

Number of subnets per virtual network:

	▼
1	
2	
3	

Explanation:

Box 1: 3

One virtual network for every tier

Box 2: 1

Only one subnet for each tier, to minimize the number of open ports.

Scenario: You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.

QUESTION 4

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.
- Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- Designate a new user named Admin1 as the service admin for the Azure subscription.
- Admin1 must receive email alerts regarding service outages.
- Ensure that a new user named User3 can create network objects for the Azure subscription.

You need to implement a backup solution for App1 after the application is moved.

What should you create first?

- A. an Azure Backup Server
- B. a Recovery Services vault
- C. a backup policy
- D. a recovery plan

Answer: B

Explanation:

Scenario: Ensure that all the virtual machines for App1 are protected by backups.

You can back up Azure VMs using a couple of methods:

Single Azure VM: You can back up an Azure VM directly from the VM settings.

Multiple Azure VMs: You can set up a Recovery Services vault and configure backup for multiple Azure VMs.

References:

<https://docs.microsoft.com/en-us/azure/backup/backup-azure-vms-first-look-arm>

QUESTION 5

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.
- Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- Designate a new user named Admin1 as the service admin for the Azure subscription.
- Admin1 must receive email alerts regarding service outages.
- Ensure that a new user named User3 can create network objects for the Azure subscription.

You need to move the blueprint files to Azure.

What should you do?

- A. Use the Azure Import/Export service.
- B. Use Azure Storage Explorer to copy the files.
- C. Generate a shared access signature (SAS). Map a drive, and then copy the files by using File Explorer.
- D. Generate an access key. Map a drive, and then copy the files by using File Explorer.

Answer: D

Explanation:

Scenario: Copy the blueprint files to Azure over the Internet.

To mount an Azure file share, you will need the primary (or secondary) storage key. SAS keys are not currently supported for mounting.

Incorrect Answers:

A: Azure Import/Export service is used to securely import large amounts of data to Azure Blob storage and Azure Files by shipping disk drives to an Azure datacenter.

References:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

QUESTION 6

You have an Azure subscription that contains 10 virtual machines on a virtual network.

You need to create a graph visualization to display the traffic flow between the virtual machines.

What should you do from Azure Monitor?

- A. From Activity log, use quick insights.
- B. From Metrics, create a chart.
- C. From Logs, create a new query.
- D. From Workbooks, create a workbook.

Answer: C

Explanation:

Navigate to Azure Monitor and select Logs to begin querying the data

Reference:

<https://azure.microsoft.com/en-us/blog/analysis-of-network-connection-data-with-azure-monitor-for-virtual-machines/>

QUESTION 7

You have an Azure subscription that contains 100 virtual machines.

You have a set of Pester tests in PowerShell that validate the virtual machine environment.

You need to run the tests whenever there is an operating system update on the virtual machines.

The solution must minimize implementation time and recurring costs.

Which three resources should you use to implement the tests? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Azure Automation runbook
- B. an alert rule
- C. an Azure Monitor query
- D. a virtual machine that has network access to the 100 virtual machines
- E. an alert action group

Answer: ABE

Explanation:

AE: You can call Azure Automation runbooks by using action groups or by using classic alerts to automate tasks based on alerts.

B: Alerts are one of the key features of Azure Monitor. They allow us to alert on actions within an Azure subscription

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-create-alert-triggered-runbook>

<https://techsnips.io/snips/how-to-create-and-test-azure-monitor-alerts/?page=13>

QUESTION 8

You have an Azure subscription that contains an Azure Log Analytics workspace.

You have a resource group that contains 100 virtual machines. The virtual machines run Linux.

You need to collect events from the virtual machines to the Log Analytics workspace.

Which type of data source should you configure in the workspace?

- A. Syslog
- B. Linux performance counters
- C. custom fields

Answer: A

Explanation:

Syslog is an event logging protocol that is common to Linux. Applications will send messages that may be stored on the local machine or delivered to a Syslog collector. When the Log Analytics agent for Linux is installed, it configures the local Syslog daemon to forward messages to the agent. The agent then sends the message to Azure Monitor where a corresponding record is created.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-custom-logs>

QUESTION 9

You have a virtual network named VNet1 as shown in the exhibit. (Click the Exhibit tab.)



Refresh



Move



Delete

Resource group ([change](#))
Production

Address space
10.2.0.0/16

Location
West US

DNS servers
Azure provided DNS service

Subscription ([change](#))
Production subscription

Subscription ID
14d26092-8e42-4ea7-b770-9dcef70fb1ea

Tags ([change](#))
[Click here to add tags](#)

Connected devices

Search connected devices

DEVICE	TYPE	IP ADDRESS	SUBNET
No results.			

No devices are connected to VNet1.

You plan to peer VNet1 to another virtual network named VNet2. VNet2 has an address space of 10.2.0.0/16.

You need to create the peering.

What should you do first?

- A. Configure a service endpoint on VNet2.
- B. Add a gateway subnet to VNet1.
- C. Create a subnet on VNet1 and VNet2.
- D. Modify the address space of VNet1.

Answer: D

Explanation:

The virtual networks you peer must have non-overlapping IP address spaces. The exhibit indicates that VNet1 has an address space of 10.2.0.0/16, which is the same as VNet2, and thus overlaps. We need to change the address space for VNet1.

Reference:
<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering#requirements-and-constraints>

QUESTION 10

You have an Azure subscription.

You have 100 Azure virtual machines.

You need to quickly identify underutilized virtual machines that can have their service tier changed to a less expensive offering.

Which blade should you use?

- A. Metrics
- B. Customer sights
- C. Monitor
- D. Advisor

Answer: D

Explanation:

Advisor helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources. You can get cost recommendations from the Cost tab on the Advisor dashboard.

Reference:

<https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations>

QUESTION 11

You have an Azure App Service app.

You need to implement tracing for the app. The tracing information must include the following:

- Usage trends
- AJAX call responses
- Page load speed by browser
- Server and browser exceptions

What should you do?

- A. Configure IIS logging in Azure Log Analytics.
- B. Configure a connection monitor in Azure Network Watcher.
- C. Configure custom logs in Azure Log Analytics.
- D. Enable the Azure Application Insights site extension.

Answer: D

Explanation:

For web pages, Application Insights JavaScript SDK automatically collects AJAX calls as dependencies.

Note: Some of the things you can track or collect are:

What are the most popular webpages in your application, at what time of day and where is that traffic coming from?

Dependency rates or response times and failure rates to find out if there's an external service that's causing performance issues on your app, maybe a user is using a portal to get through to your application and there are response time issues going through there for instance. Exceptions for both server and browser information, as well as page views and load performance from the end users' side.

Reference:

<https://azure.microsoft.com/en-us/blog/ajax-collection-in-application-insights/>

<https://blog.pragmaticworks.com/what-is-application-insights>

QUESTION 12

You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Contains
storagecontoso1	A blob service and a table service
storagecontoso2	A blob service and a file service
storagecontoso3	A queue service
storagecontoso4	A file service and a queue service
storagecontoso5	A table service

You enable Storage Advanced Threat Protection (ATP) for all the storage accounts.

You need to identify which storage accounts will generate Storage ATP alerts.

Which two storage accounts should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. storagecontoso1
- B. storagecontoso2
- C. storagecontoso3
- D. storagecontoso4
- E. storagecontoso5

Answer: AB

Explanation:

Storage Threat Detection is available for the Blob Service.

The screenshot shows the Azure Storage account settings for 'prodsravanthv23'. The 'Advanced Threat Protection (preview)' section is active. A message box states: 'Storage Threat Detection is available for the Blob service. Security alerts are integrated with Azure Security Center and will be sent by email to subscription admins.' Below this, a button labeled 'ON' is selected for 'Advanced Threat Protection (preview)'. The left sidebar lists other settings like Events, Storage Explorer (preview), and Properties.

Reference:

<https://azure.microsoft.com/en-us/blog/advanced-threat-protection-for-azure-storage-now-in-public-preview/>

QUESTION 13

You have an Azure virtual machine named VM1 and an Azure Active Directory (Azure AD) tenant named adatum.com.

VM1 has the following settings:

- IP address: 10.10.0.10
- System-assigned managed identity: On

You need to create a script that will run from within VM1 to retrieve the authentication token of VM1.

Which address should you use in the script?

- A. vm1.adatum.com.onmicrosoft.com
- B. 169.254.169.254
- C. 10.10.0.10
- D. vm1.adatum.com

Answer: B

Explanation:

Your code that's running on the VM can request a token from the Azure Instance Metadata Service identity endpoint, accessible only from within the VM:
<http://169.254.169.254/metadata/identity/oauth2/token>

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

QUESTION 14

You are designing an Azure solution.

The solution must meet the following requirements:

- Distribute traffic to different pools of dedicated virtual machines (VMs) based on rules.
- Provide SSL offloading capabilities.

You need to recommend a solution to distribute network traffic.

Which technology should you recommend?

- A. Azure Application Gateway
- B. Azure Load Balancer
- C. Azure Traffic Manager
- D. server-level firewall rules

Answer: A

Explanation:

If you require "SSL offloading", application layer treatment, or wish to delegate certificate management to Azure, you should use Azure's layer 7 load balancer Application Gateway instead of the Load Balancer.

Incorrect Answers:

D: Because Load Balancer is agnostic to the TCP payload and TLS offload ("SSL") is not provided.

Reference:

<https://docs.microsoft.com/en-us/azure/application-gateway/overview>

QUESTION 15

You are implementing authentication for applications in your company. You plan to implement self-service password reset (SSPR) and multifactor authentication (MFA) in Azure Active Directory (Azure AD).

You need to select authentication mechanisms that can be used for both MFA and SSPR.

Which two authentication methods should you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Authenticator app
- B. Email addresses
- C. App passwords
- D. Short Message Service (SMS) messages
- E. Security questions

Answer: AD

Explanation:

The following authentication mechanisms can be used for both MFA and SSPR:
Short Message Service (SMS) messages

Azure AD passwords
Microsoft Authenticator app
Voice call
Incorrect Answers:
B, E: The following authentication mechanisms are used for SSPR only:
Email addresses
Security questions
E: App passwords authentication mechanisms can be used for MFA only, but only in certain cases.
Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

QUESTION 16

Your company has the groups shown in the following table.

Group	Number of members
Managers	10
Sales	100
Development	15

The company has an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com.

An administrator named Admin1 attempts to enable Enterprise State Roaming for all the users in the Managers group.

Admin1 reports that the options for Enterprise State Roaming are unavailable from Azure AD.

You verify that Admin1 is assigned the Global administrator role.

You need to ensure that Admin1 can enable Enterprise State Roaming.

What should you do?

- A. Assign an Azure AD Privileged Identity Management (PIM) role to Admin1.
- B. Purchase an Azure Rights Management (Azure RMS) license for each user in the Managers group.
- C. Enforce Azure Multi-Factor Authentication (MFA) for Admin1.
- D. Purchase an Azure AD Premium P1 license for each user in the Managers group.

Answer: D

Explanation:

Enterprise State Roaming is available to any organization with an Azure AD Premium or Enterprise Mobility + Security (EMS) license.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/devices/enterprise-state-roaming-enable>

QUESTION 17

Your company has an Azure subscription.

You enable multi-factor authentication (MFA) for all users.

The company's help desk reports an increase in calls from users who receive MFA requests while they work from the company's main office.

You need to prevent the users from receiving MFA requests when they sign in from the main office.

What should you do?

- A. From Conditional access in Azure Active Directory (Azure AD), create a named location.
- B. From the MFA service settings, create a trusted IP range.
- C. From Conditional access in Azure Active Directory (Azure AD), create a custom control.
- D. From Azure Active Directory (Azure AD), configure organizational relationships.

Answer: B

Explanation:

The first thing you may want to do, before enabling Multi-Factor Authentication for any users, is to consider configuring some of the available settings. One of the most important features is a trusted IPs list. This will allow you to whitelist a range of IPs for your network. This way, when users are in the office, they will not get prompted with MFA, and when they take their devices elsewhere, they will. Here's how to do it:

Log in to your Azure Portal.

Navigate to Azure AD > Conditional Access > Named locations.

From the top toolbar select Configure MFA trusted IPs.

Reference:

<https://www.kraftkennedy.com/implementing-azure-multi-factor-authentication/>

QUESTION 18

You have an application named App1 that does not support Azure Active Directory (Azure AD) authentication.

You need to ensure that App1 can send messages to an Azure Service Bus queue. The solution must prevent App1 from listening to the queue.

What should you do?

- A. Configure Access control (IAM) for the Service Bus.
- B. Add a shared access policy to the queue.
- C. Modify the locks of the queue.
- D. Configure Access control (IAM) for the queue.

Answer: B

Explanation:

There are two ways to authenticate and authorize access to Azure Service Bus resources: Azure Activity Directory (Azure AD) and Shared Access Signatures (SAS).

Each Service Bus namespace and each Service Bus entity has a Shared Access Authorization policy made up of rules.

Reference:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-authentication-and->

authorization

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-sas>

QUESTION 19

An administrator plans to create a function app in Azure that will have the following settings:

- Runtime stack: .NET Core
- Operating System: Linux
- Plan type: Consumption
- Enable Application Insights: Yes

You need to ensure that you can back up the function app.

Which settings should you recommend changing before creating the function app?

- A. Runtime stack
- B. Enable Application Insights
- C. Operating System
- D. Plan type

Answer: D

Explanation:

The Backup and Restore feature requires the App Service plan to be in the Standard, Premium or Isolated tier.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/manage-backup#requirements-and-restrictions>

QUESTION 20

You have 10 Azure virtual machines on a subnet named Subnet1. Subnet1 is on a virtual network named VNet1.

You plan to deploy a public Azure Standard Load Balancer named LB1 to the same Azure region as the 10 virtual machines.

You need to ensure that traffic from all the virtual machines to the internet flows through LB1. The solution must prevent the virtual machines from being accessible on the internet.

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

NOTE: Each correct selection is worth one point.

- A. Add health probes to LB1.
- B. Add the network interfaces of the virtual machines to the backend pool of LB1.
- C. Add an inbound rule to LB1.
- D. Add an outbound rule to LB1.
- E. Associate a network security group (NSG) to Subnet1.
- F. Associate a user-defined route to Subnet1.

Answer: ABD

Explanation:

A: To allow the Load Balancer to monitor the status of your app, you use a health probe. The

health probe dynamically adds or removes VMs from the Load Balancer rotation based on their response to health checks.

B: To distribute traffic to the VMs, a backend address pool contains the IP addresses of the virtual (NICs) connected to the Load Balancer.

D: A Load Balancer rule is used to define how traffic is distributed to the VMs. Only outbound traffic is allowed.

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/tutorial-load-balancer-standard-manage-portal2>

QUESTION 21

You have SQL Server on an Azure virtual machine named SQL1.

You need to automate the backup of the databases on SQL1 by using Automated Backup v2 for the virtual machines. The backups must meet the following requirements:

- Meet a recovery point objective (RPO) of 15 minutes.
- Retain the backups for 30 days.
- Encrypt the backups at rest.

What should you provision as part of the backup solution?

- A. Elastic Database jobs
- B. Azure Key Vault
- C. an Azure Storage account
- D. a Recovery Services vault

Answer: C

Explanation:

An Azure storage account is used for storing Automated Backup files in blob storage. A container is created at this location to store all backup files. The backup file naming convention includes the date, time, and database GUID.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/virtual-machines/windows/automated-backup>

QUESTION 22

You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

Name	Connected to
VM1	VNET1/Subnet1
VM2	VNET1/Subnet2

KeyVault1 has an access policy that provides several users with Create Key permissions.

You need to ensure that the users can only register secrets in KeyVault1 from VM1.

What should you do?

- A. Create a network security group (NSG) that is linked to Subnet1.
- B. Configure the Firewall and virtual networks settings for KeyVault1.
- C. Modify the access policy for KeyVault1.
- D. Configure KeyVault1 to use a hardware security module (HSM).

Answer: C

Explanation:

You grant data plane access by setting Key Vault access policies for a key vault.

Note 1: Grant our VM's system-assigned managed identity access to the Key Vault.

1. Select Access policies and click Add new.
 2. In Configure from template, select Secret Management.
 3. Choose Select Principal, and in the search field enter the name of the VM you created earlier. Select the VM in the result list and click Select.
 4. Click OK to finishing adding the new access policy, and OK to finish access policy selection.
- Note 2: Access to a key vault is controlled through two interfaces: the management plane and the data plane. The management plane is where you manage Key Vault itself. Operations in this plane include creating and deleting key vaults, retrieving Key Vault properties, and updating access policies. The data plane is where you work with the data stored in a key vault. You can add, delete, and modify keys, secrets, and certificates.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-nonaad>

<https://docs.microsoft.com/en-us/azure/key-vault/general/secure-your-key-vault2>

QUESTION 23

You have resources in three Azure regions. Each region contains two virtual machines. Each virtual machine has a public IP address assigned to its network interface and a locally installed application named App1.

You plan to implement Azure Front Door-based load balancing across all the virtual machines.

You need to ensure that App1 on the virtual machines will only accept traffic routed from Azure Front Door.

What should you implement?

- A. Azure Private Link
- B. service endpoints
- C. network security groups (NSGs) with service tags
- D. network security groups (NSGs) with application security groups

Answer: C

Explanation:

Configure IP ACLing for your backends to accept traffic from Azure Front Door's backend IP address space and Azure's infrastructure services only. Refer the IP details below for ACLing your backend:

Refer AzureFrontDoor.Backend section in Azure IP Ranges and Service Tags for Front Door's IPv4 backend IP address range or you can also use the service tag AzureFrontDoor.Backend in your network security groups.

Reference:

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq>

QUESTION 24

You have an Azure key vault named KV1.

You need to ensure that applications can use KV1 to provision certificates automatically from an external certification authority (CA).

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

NOTE: Each correct selection is worth one point.

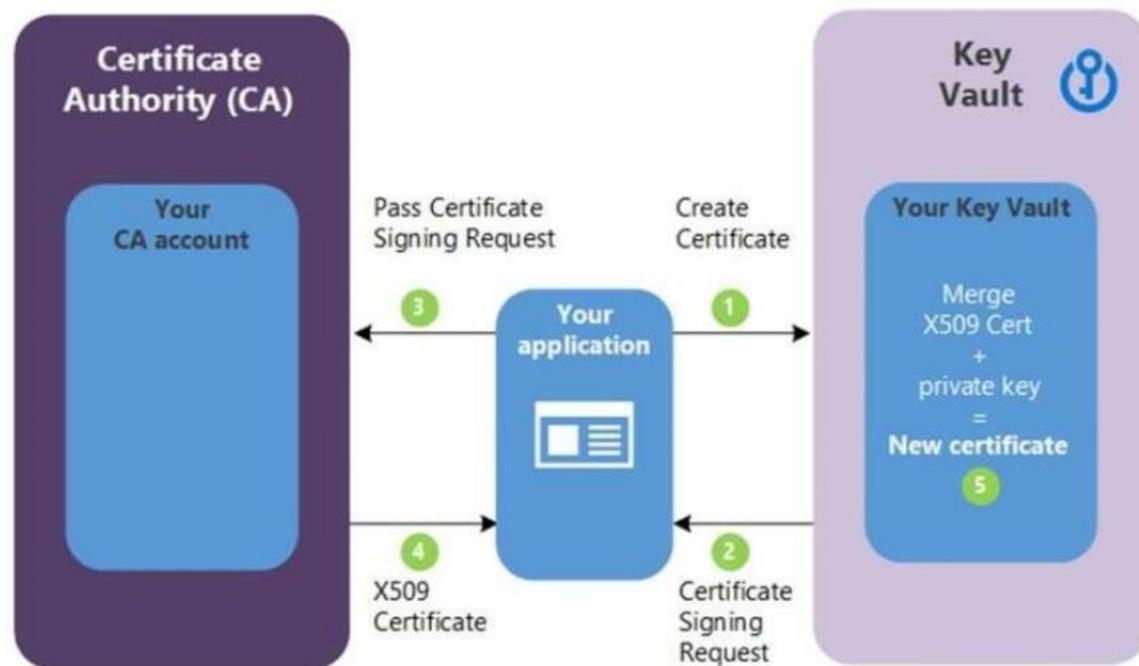
- A. From KV1, create a certificate issuer resource.
- B. Obtain the CA account credentials.
- C. Obtain the root CA certificate.
- D. From KV1, create a certificate signing request (CSR).
- E. From KV1, create a private key,

Answer: CD

Explanation:

C: Obtain the root CA certificate (step 4 in the picture below)

D: From KV1, create a certificate signing request (CSR) (step 2 in the picture below) Note:
Creating a certificate with a CA not partnered with Key Vault This method allows working with other CAs than Key Vault's partnered providers, meaning your organization can work with a CA of its choice.



The following step descriptions correspond to the green lettered steps in the preceding diagram.

1. In the diagram above, your application is creating a certificate, which internally begins by creating a key in your key vault.
2. Key Vault returns to your application a Certificate Signing Request (CSR).
3. Your application passes the CSR to your chosen CA.
4. Your chosen CA responds with an X509 Certificate.
5. Your application completes the new certificate creation with a merger of the X509 Certificate from your CA.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/certificates/certificate-scenarios>

QUESTION 25

You create the following Azure role definition.

```
{  
    "Name": "Role1",  
    "Id": "80808080-8080-8080-8080-808080808080",  
    "IsCustom": false,  
    "Description": "",  
    "Actions": [  
        "Microsoft.Storage/*/read",  
        "Microsoft.Network/*/read",  
        "Microsoft.Compute/virtualMachines/start/action",  
        "Microsoft.Compute/virtualMachines/restart/action",  
        "Microsoft.Authorization/*/read"],  
    "NotActions": [ ],  
    "DataActions": [ ],  
    "NotDataActions": [ ],  
    "AssignableScopes": [ ]  
}
```

You need to create Role1 by using the role definition.

Which two values should you modify before you create Role1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. AssignableScopes
- B. Description
- C. DataActions
- D. IsCustom
- E. Id

Answer: AD

Explanation:

Part of example:

```
"IsCustom": true,  
"AssignableScopes": [  
    "/subscriptions/{subscriptionId1}",  
    "/subscriptions/{subscriptionId2}",  
    "/subscriptions/{subscriptionId3}"
```

The following shows what a custom role looks like as displayed in JSON format. This custom role can be used for monitoring and restarting virtual machines.

```
{  
    "Name": "Virtual Machine Operator",  
    "Id": "88888888-8888-8888-8888-888888888888",  
    "IsCustom": true,  
    "Description": "Can monitor and restart virtual machines.", "Actions": [  
        "Microsoft.Storage/*/read",
```

```
"Microsoft.Network/*/read",
"Microsoft.Compute/*/read",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Authorization/*/read",
"Microsoft.ResourceHealth/availabilityStatuses/read",
"Microsoft.Resources/subscriptions/resourceGroups/read", "Microsoft.Insights/alertRules/*",
"Microsoft.Insights/diagnosticSettings/*",
"Microsoft.Support"
],
"NotActions": [],
"DataActions": [],
"NotDataActions": [],
"AssignableScopes": [
"/subscriptions/{subscriptionId1}",
"/subscriptions/{subscriptionId2}",
"/subscriptions/{subscriptionId3}"
]
}
```

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>

QUESTION 26

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 2019. Server1 is a container host.

You are creating a Dockerfile to build a container image.

You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.

Solution: You add the following line to the Dockerfile.

```
COPY File1.txt /Folder1/
```

You then build the container image.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Copy is the correct command to copy a file to the container image.

Reference:

https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy

<https://docs.docker.com/engine/reference/builder/>

QUESTION 27

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 2019. Server1 is a container host.

You are creating a Dockerfile to build a container image.

You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.

Solution: You add the following line to the Dockerfile.

```
XCOPY File1.txt C:\Folder1\
```

You then build the container image.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Copy is the correct command to copy a file to the container image. Furthermore, the root directory is specified as '/' and not as 'C:/'.

Reference:

https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy

<https://docs.docker.com/engine/reference/builder/>

QUESTION 28

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 2019. Server1 is a container host.

You are creating a Dockerfile to build a container image.

You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.

Solution: You add the following line to the Dockerfile.

```
ADD File1.txt C:/Folder1/
```

You then build the container image.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Copy is the correct command to copy a file to the container image. The ADD command can also be used.

However, the root directory is specified as '/' and not as 'C:/'.

Reference:

https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy

<https://docs.docker.com/engine/reference/builder/>

QUESTION 29

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 an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other identity Governance settings are available.

Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.

You need to ensure that Admin1 can create access reviews in contoso.com.

Solution: You create an access package.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You do not use access packages for Identity Governance. Instead use Azure AD Privileged Identity Management.

Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:

Conduct access reviews to ensure users still need roles

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure> <https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview>

QUESTION 30

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 an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other identity Governance settings are available.

Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.

You need to ensure that Admin1 can create access reviews in contoso.com.

Solution: You purchase an Azure Directory Premium P2 license for contoso.com.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead use Azure AD Privileged Identity Management.

Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:

Conduct access reviews to ensure users still need roles

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

QUESTION 31

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 an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other identity Governance settings are available.

Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.

You need to ensure that Admin1 can create access reviews in contoso.com.

Solution: You assign the Global administrator role to Admin1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead use Azure AD Privileged Identity Management.

Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:

Conduct access reviews to ensure users still need roles

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

QUESTION 32

Your network contains an on-premises Active Directory domain named contoso.com that contains a member server named Server1.

You have the accounts shown in the following table.

Name	Member of
CONTOSO\User1	Domain Admins
CONTOSO\User2	Domain Users
CONTOSO\User3	Enterprise Admin
SERVER1\User4	Users

You are installing Azure AD Connect on Server1.

You need to specify the account for Azure AD Connect synchronization. The solution must use the principle of least privilege.

Which account should you specify?

- A. CONTOSO\User2
- B. SERVER1\User4

- C. CONTOSO\User1
- D. CONTOSO\User3

Answer: A

Explanation:

The default Domain User permissions are sufficient

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions>

QUESTION 33

You have an Azure subscription that contains the web apps shown in the following table.

Name	Runtime stack
WebApp1	Java SE
WebApp2	Ruby 2.6
WebApp3	Python 3.7
WebApp4	ASP.NET V4.7

For which web app can you configure a WebJob?

- A. WebApp1
- B. WebApp4
- C. WebApp2
- D. WebApp3

Answer: B

Explanation:

Publishing a .NET Core WebJob to App Service from Visual Studio uses the same tooling as publishing an ASP.NET Core app.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/webjobs-dotnet-deploy-vs>

QUESTION 34

The developers at your company request that you create databases in Azure Cosmos DB as shown in the following table.

Name	Requirement
CosmosDB1	<ul style="list-style-type: none"> Provides a throughput of 1,200 RU/s Has multiple write regions Uses the Core (SQL) API
CosmosDB2	<ul style="list-style-type: none"> Provides a throughput of 800 RU/s Uses the MongoDB API
CosmosDB3	<ul style="list-style-type: none"> Provides a throughput of 1,200 RU/s Has only one write region Uses the Core (SQL) API
CosmosDB4	<ul style="list-style-type: none"> Provides a throughput of 2,000 RU/s Uses the MongoDB API

You need to create the Azure Cosmos DB databases to meet the developer request. The solution must minimize costs.

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

NOTE: Each correct selection is worth one point.

- Create three Azure Cosmos DB accounts, one for the databases that use the Core (SQL) API, one for CosmosDB2, and one for CosmosDB4.
- Create two Azure Cosmos DB accounts, one for CosmosDB2 and CosmosDB4 and one for CosmosDB1 and CosmosDB3.
- Create one Azure Cosmos DB account for each database.
- Create three Azure Cosmos DB accounts, one for the databases that use the MongoDB API, one for CosmosDB1, and one for CosmosDB3.

Answer: BD

Explanation:

Note:

Microsoft recommends using the same API for all access to the data in a given account. One throughput provisioned container per subscription for SQL, Gremlin API, and Table accounts.

Up to three throughput provisioned collections per subscription for MongoDB accounts.

The throughput provisioned on an Azure Cosmos container is exclusively reserved for that container. The container receives the provisioned throughput all the time.

Incorrect Answers:

A: DB2 and DB4 can use the same account.

C: The most costly alternative.

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/set-throughput#set-throughput-on-a-container>

QUESTION 35

You have three Azure SQL Database servers shown in the following table.

Name	Resource group	Location
sqlserver1	RG1	West US
sqlserver2	RG1	West US
sqlserver3	RG2	West US
sqlserver4	RG1	West Europe
sqlserver5	RG2	West Europe

You plan to specify sqlserver1 as the primary server in a failover group.

Which servers can be used as a secondary server?

- A. sqlserver4 and sqlserver5 only
- B. sqlserver2 and sqlserver3 only
- C. sqlserver1 and sqlserver3 only
- D. sqlserver2 and sqlserver4 only

Answer: A

Explanation:

You can use different resource groups using Power Shell ou CLI.

The secondary must be in a different region.

<https://docs.microsoft.com/en-us/azure/azure-sql/database/auto-failover-group-overview?tabs=azure-powershell>

QUESTION 36

You have two Azure SQL Database managed instances in different Azure regions.

You plan to configure the managed instances in an instance failover group.

What should you configure before you can add the managed instances to the instance failover group?

- A. an internal Azure Load Balancer instance that has managed instance endpoints in a backend pool
- B. Azure Private Link that has endpoints on two virtual networks
- C. an Azure Application Gateway that has managed instance endpoints in a backend pool
- D. a Site-to-Site VPN between the virtual networks that contain the instances

Answer: D

Explanation:

For two managed instances to participate in a failover group, there must be either ExpressRoute or a gateway configured between the virtual networks of the two managed instances to allow network communication.

You create the two VPN gateways and connect them.

1. Create the gateway for the virtual network of your primary managed instance using the Azure portal.
2. Create the gateway for the virtual network of your secondary managed instance using the Azure portal.
3. Create a bidirectional connection between the two gateways of the two virtual networks.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/failover-group-add-instance-tutorial?tabs=azure-portal#4---create-a-primary-gateway>

QUESTION 37

Hotspot Question

You plan to create an Azure Storage account in the Azure region of East US 2.

You need to create a storage account that meets the following requirements:

- Replicates synchronously
- Remains available if a single data center in the region fails

How should you configure the storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Replication:

Geo-redundant storage (GRS)
Locally-redundant storage (LRS)
Read-access geo-redundant storage (RA GRS)
Zone-redundant storage (ZRS)

Account type:

Blob storage
Storage (general purpose v1)
StorageV2 (general purpose v2)

Answer:

Answer Area

Replication:

Geo-redundant storage (GRS)
Locally-redundant storage (LRS)
Read-access geo-redundant storage (RA GRS)
Zone-redundant storage (ZRS)

Account type:

Blob storage
Storage (general purpose v1)
StorageV2 (general purpose v2)

Explanation:

Box 1: Zone-redundant storage (ZRS)

Zone-redundant storage (ZRS) replicates your data synchronously across three storage clusters in a single region.

LRS would not remain available if a data center in the region fails GRS and RA GRS use asynchronous replication.

Box 2: StorageV2 (general purpose V2)

ZRS only support GPv2.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-zrs>

QUESTION 38

Hotspot Question

You plan to deploy an Azure virtual machine named VM1 by using an Azure Resource Manager template.

You need to complete the template.

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

NOTE: Each correct selection is worth one point.

Answer Area

```
{  
    "type": "Microsoft.Compute/virtualMachines",  
    "apiVersion": "2018-10-01",  
    "name": "VM1",  
    "location": "[parameters('location')]",  
    "dependsOn": [  
        "[resourceId('Microsoft.Storage/storageAccounts/', variables('Name3'))]",  
        "[resourceId(  
            'Microsoft.Network/publicIPAddresses/'  
            'Microsoft.Network/virtualNetworks/'  
            'Microsoft.Network/networkInterfaces/'  
            'Microsoft.Network/virtualNetworks/subnets'  
            'Microsoft.Storage/storageAccounts/'  
        ]]  
    ],  
    {  
        "type": "Microsoft.Network/networkInterfaces",  
        "apiVersion": "2018-11-01",  
        "name": "NIC1",  
        "location": "[parameters('location')]",  
        "dependsOn": [  
            "[resourceId('Microsoft.Network/publicIPAddresses/', variables('Name1'))]",  
            "[resourceId(  
                'Microsoft.Network/publicIPAddresses/'  
                'Microsoft.Network/virtualNetworks/'  
                'Microsoft.Network/networkInterfaces/'  
                'Microsoft.Network/virtualNetworks/subnets'  
                'Microsoft.Storage/storageAccounts/'  
            ]]  
        ],  
    },  
}
```

Answer:

Answer Area

```
{  
    "type": "Microsoft.Compute/virtualMachines",  
    "apiVersion": "2018-10-01",  
    "name": "VM1",  
    "location": "[parameters('location')]",  
    "dependsOn": [  
        "[resourceId('Microsoft.Storage/storageAccounts/', variables('Name3'))]",  
        "[resourceId('Microsoft.Network/publicIPAddresses/', variables('Name4'))]"  
        'Microsoft.Network/publicIPAddresses/'  
        'Microsoft.Network/virtualNetworks/'  
        'Microsoft.Network/networkInterfaces/'  
        'Microsoft.Network/virtualNetworks/subnets'  
        'Microsoft.Storage/storageAccounts/'  
    ],  
    {  
        "type": "Microsoft.Network/networkInterfaces",  
        "apiVersion": "2018-11-01",  
        "name": "NIC1",  
        "location": "[parameters('location')]",  
        "dependsOn": [  
            "[resourceId('Microsoft.Network/publicIPAddresses/', variables('Name1'))]",  
            "[resourceId('Microsoft.Network/publicIPAddresses/', variables('Name2'))]"  
            'Microsoft.Network/publicIPAddresses/'  
            'Microsoft.Network/virtualNetworks/'  
            'Microsoft.Network/networkInterfaces/'  
            'Microsoft.Network/virtualNetworks/subnets'  
            'Microsoft.Storage/storageAccounts/'  
        ],  
    },  
}
```

Explanation:

Within your template, the dependsOn element enables you to define one resource as a dependent on one or more resources. Its value can be a comma-separated list of resource names.

Box 1: 'Microsoft.Network/networkInterfaces'

This resource is a virtual machine. It depends on two other resources:

Microsoft.Storage/storageAccounts
Microsoft.Network/networkInterfaces

Box 2: 'Microsoft.Network/virtualNetworks/'

The dependsOn element enables you to define one resource as a dependent on one or more resources.

The resource depends on two other resources:

Microsoft.Network/publicIPAddresses
Microsoft.Network/virtualNetworks

```

"resources": [
  {
    ...
  },
  {
    ...
  },
  {
    ...
  },
  {
    ...
  },
  {
    "type": "Microsoft.Network/networkInterfaces",
    "name": "[variables('nicName')]",
    "location": "[parameters('location')]",
    "apiVersion": "2018-08-01",
    "dependsOn": [
      "[resourceId('Microsoft.Network/publicIPAddresses', variables('publicIPAddressName'))]",
      "[resourceId('Microsoft.Network/virtualNetworks', variables('virtualNetworkName'))]"
    ],
    "properties": {
      "ipConfigurations": [
        {
          "name": "ipconfig1",
          "properties": {
            "privateIPAllocationMethod": "Dynamic",
            "publicIPAddress": {
              "id": "[resourceId('Microsoft.Network/publicIPAddresses', variables('publicIPAddressName'))]"
            },
            "subnet": {
              "id": "[variables('subnetRef')]"
            }
          }
        }
      ]
    }
  }
]

```

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-tutorial-create-templates-with-dependent-resources>

QUESTION 39

Hotspot Question

Your network contains an Active Directory domain named adatum.com and an Azure Active Directory (Azure AD) tenant named adatum.onmicrosoft.com.

Adatum.com contains the user accounts in the following table.

Name	Member of
User1	Domain Admins
User2	Schema Admins
User3	Incoming Forest Trust Builders
User4	Replicator
User5	Enterprise Admins

Adatum.onmicrosoft.com contains the user accounts in the following table.

Name	Role
UserA	Global administrator
UserB	User administrator
UserC	Security administrator
UserD	Service administrator

You need to implement Azure AD Connect. The solution must follow the principle of least privilege.

Which user accounts should you use in Adatum.com and Adatum.onmicrosoft.com to implement Azure AD Connect? To answer select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Adatum.com:

	▼
User1	
User2	
User3	
User4	
User5	

Adatum.onmicrosoft.com:

	▼
UserA	
UserB	
UserC	
UserD	

Answer:

Answer Area

Adatum.com:

	▼
User1	
User2	
User3	
User4	
User5	

Adatum.onmicrosoft.com:

	▼
UserA	
UserB	
UserC	
UserD	

Explanation:

Box 1: User5

In Express settings, the installation wizard asks for the following:

AD DS Enterprise Administrator credentials

Azure AD Global Administrator credentials

The AD DS Enterprise Admin account is used to configure your on-premises Active Directory.

These credentials are only used during the installation and are not used after the installation has completed. The Enterprise Admin, not the Domain Admin should make sure the permissions in Active Directory can be set in all domains.

Box 2: UserA

Azure AD Global Admin credentials are only used during the installation and are not used after the installation has completed. It is used to create the Azure AD Connector account used for synchronizing changes to Azure AD. The account also enables sync as a feature in Azure AD.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-accounts-permissions>

QUESTION 40

Hotspot Question

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Location
RG1	West US
RG2	East US

You create an Azure Resource Manager template named Template1 as shown in the following exhibit.

```
{
    "$schema": "http://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "name": {
            "type": "String"
        },
        "location": {
            "defaultValue": "westus",
            "type": "String"
        }
    },
    "variables": {
        "location": "[resourceGroup().location]"
    },
    "resources": [
        {
            "type": "Microsoft.Network/publicIPAddresses",
            "apiVersion": "2019-11-01",
            "name": "[parameters('name')]",
            "location": "[variables('location')]",
            "sku": {
                "name": "Basic"
            },
            "properties": {
                "publicIPAddressVersion": "IPv4",
                "publicIPAllocationMethod": "Dynamic",
                "idleTimeoutInMinutes": 4,
                "ipTags": []
            }
        }
    ]
}
```

From the Azure portal, you deploy Template1 four times by using the settings shown in the following table.

Resource group	Name	Location
RG1	IP1	westus
RG1	IP2	westus
RG2	IP1	westus
RG2	IP3	westus

What is the result of the deployment? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Number of public IP addresses in West US:

	▼
1	
2	
3	
4	

Total number of public IP addresses created:

	▼
1	
2	
3	
4	

Answer:

Answer Area

Number of public IP addresses in West US:

	▼
1	
2	
3	
4	

Total number of public IP addresses created:

	▼
1	
2	
3	
4	

QUESTION 41

Hotspot Question

You have an Azure subscription that contains multiple resource groups.

You create an availability set as shown in the following exhibit.

Create availability set

Basics Advanced Tags Review + create

An Availability Set is a logical grouping capability for isolating VM resources from each other when they're deployed. Azure makes sure that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or software failure happens, only a subset of your VMs are impacted and your overall solution stays operational. Availability Sets are essential for building reliable cloud solutions.

[Learn more about the availability sets.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Azure Pass - Sponsorship

Resource group * ⓘ

RG1

[Create new](#)

Instance details

Name * ⓘ

AS1



Region * ⓘ

(Europe) West Europe



Fault domains ⓘ

—○— 2

2

Update domains ⓘ

—○— 3

3

Use managed disks ⓘ

No (Classic) Yes (Aligned)

Yes (Aligned)

You deploy 10 virtual machines to AS1.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

During planned maintenance, at least [answer choice] virtual machines will be available.

	▼
4	
5	
6	
8	

To add another virtual machine to AS1, the virtual machine must be added to [answer choice].

	▼
any region and the RG1 resource group	
the West Europe region and any resource group	
the West Europe region and the RG1 resource group	

Answer:

Answer Area

During planned maintenance, at least [answer choice] virtual machines will be available.

	▼
4	
5	
6	
8	

To add another virtual machine to AS1, the virtual machine must be added to [answer choice].

	▼
any region and the RG1 resource group	
the West Europe region and any resource group	
the West Europe region and the RG1 resource group	

Explanation:

Box 1: 6

Two out of three update domains would be available, each with at least 3 VMs. An update domain is a group of VMs and underlying physical hardware that can be rebooted at the same time.

As you create VMs within an availability set, the Azure platform automatically distributes your VMs across these update domains. This approach ensures that at least one instance of your application always remains running as the Azure platform undergoes periodic maintenance.

Box 2: the West Europe region and the RG1 resource group

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/regions>

QUESTION 42

Hotspot Question

You have an Azure Resource Manager template for a virtual machine named Template1. Template1 has the following parameters section.

```
"parameters": {  
    "adminUsername": {  
        "type": "string"  
    },  
    "adminPassword": {  
        "type": "securestring"  
    },  
    "dnsLabelPrefix": {  
        "type": "string"  
    },  
    "windowsOSVersion": {  
        "type": "string",  
        "defaultValue": "2016-Datacenter",  
        "allowedValues": [  
            "2016-Datacenter",  
            "2019-Datacenter",  
        ]  
    },  
    "location": {  
        "type": "String",  
        "allowedValues": [  
            "eastus",  
            "centralus",  
            "westus" ]  
    }  
},
```

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 Area

Statements	Yes	No
When you deploy Template1, you are prompted for a resource group.	<input type="radio"/>	<input type="radio"/>
When you deploy Template1, you are prompted for the Windows operating system version.	<input type="radio"/>	<input type="radio"/>
When you deploy Template1, you are prompted for a location.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
When you deploy Template1, you are prompted for a resource group.	<input checked="" type="radio"/>	<input type="radio"/>
When you deploy Template1, you are prompted for the Windows operating system version.	<input type="radio"/>	<input checked="" type="radio"/>
When you deploy Template1, you are prompted for a location.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: Yes

The Resource group is not specified.

Box 2: No

The default value for the operating system is Windows 2016 Datacenter.

Box 3: Yes

Location is no default value.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/virtual-machines/windows/ps-template>

QUESTION 43

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

The tenant contains computers that run Windows 10. The computers are configured as shown in the following table.

Name	Member of
Computer1	GroupA
Computer2	GroupA
Computer3	GroupB

You enable Enterprise State Roaming in contoso.com for Group1 and GroupA.

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 Area

Statements	Yes	No
If User1 modifies the desktop background of Computer1, User1 will see the changed background when signing in to Computer3.	<input type="radio"/>	<input type="radio"/>
If User2 modifies the desktop background of Computer1, User2 will see the changed background when signing in to Computer2.	<input type="radio"/>	<input type="radio"/>
If User1 modifies the desktop background of Computer3, User1 will see the changed background when signing in to Computer2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If User1 modifies the desktop background of Computer1, User1 will see the changed background when signing in to Computer3.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 modifies the desktop background of Computer1, User2 will see the changed background when signing in to Computer2.	<input type="radio"/>	<input checked="" type="radio"/>
If User1 modifies the desktop background of Computer3, User1 will see the changed background when signing in to Computer2.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.

Box 1: Yes

Box 2: No

Box 3: Yes

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-overview>

QUESTION 44

Hotspot Question

You have an Azure Resource Manager template named Template1 in the library as shown in the following exhibit.

ARM Template

template1

```
1  {
2      "$schema": "https://schema.management.azure.com/
schemas/2015-01-01/deploymentTemplate.json#",
3      "contentVersion": "1.0.0.0",
4      "parameters": {},
5      "resources": [
6          {
7              "apiVersion": "2016-01-01",
8              "type": "Microsoft.Storage/storageAccounts",
9              "name": "[concat(copyIndex(), 'storage',
uniqueString(resourceGroup().id))]",
10             "location": "[resourceGroup().location]",
11             "sku": {
12                 "name": "Premium_LRS"
13             },
14             "kind": "Storage",
15             "properties": {},
16             "copy": {
17                 "name": "storagecopy",
18                 "count": 3,
19                 "mode": "Serial",
20                 "batchSize": 1
21             }
22         }
23     ]
24 }
25 }
26 }
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

During the deployment of Template1, you can specify [answer choice].

the number of resources to deploy
the name of the resources to deploy
the resource group to which to deploy the resources
the permissions for the resources that will be deployed

Template1 deploys [answer choice].

a single storage account in one resource group
three storage accounts in one resource group
three resource groups that each has one storage account
three resource groups that each has three storage accounts

Answer:

Answer Area

During the deployment of Template1, you can specify [answer choice].

the number of resources to deploy
the name of the resources to deploy
the resource group to which to deploy the resources
the permissions for the resources that will be deployed

Template1 deploys [answer choice].

a single storage account in one resource group
three storage accounts in one resource group
three resource groups that each has one storage account
three resource groups that each has three storage accounts

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-syntax>

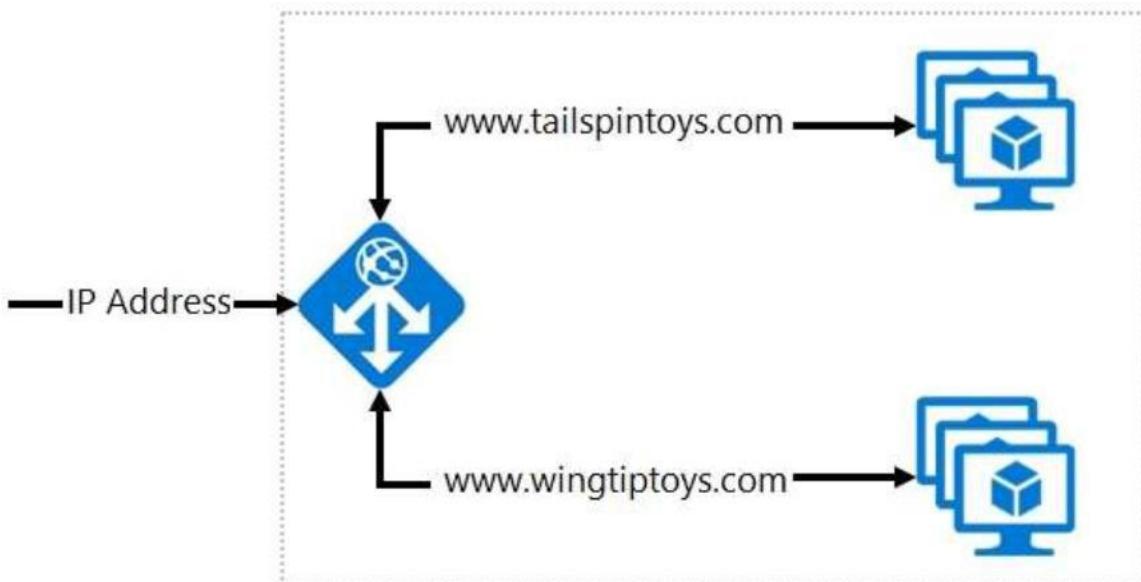
QUESTION 45

Hotspot Question

Your company hosts multiple websites by using Azure virtual machine scale sets (VMSS) that run Internet Information Server (IIS).

All network communications must be secured by using end to end Secure Socket Layer (SSL) encryption. User sessions must be routed to the same server by using cookie-based session affinity.

The image shown depicts the network traffic flow for the websites to the VMSS.



Use the drop-down menus to select the answer choice that answers each question.

NOTE: Each correct selection is worth one point.

Answer Area

Which Azure solution should you create to route the web application traffic to the VMSS?

Azure VPN Gateway
Azure Application Gateway
Azure ExpressRoute
Azure Network Watcher

What should you configure to make sure web traffic arrives at the appropriate server in the VMSS?

Routing rules and backend listeners
CNAME and A records
Routing method and DNS time to live (TTL)
Path-based redirection and WebSockets

Answer:

Answer Area

Which Azure solution should you create to route the web application traffic to the VMSS?

Azure VPN Gateway
Azure Application Gateway
Azure ExpressRoute
Azure Network Watcher

What should you configure to make sure web traffic arrives at the appropriate server in the VMSS?

Routing rules and backend listeners
CNAME and A records
Routing method and DNS time to live (TTL)
Path-based redirection and WebSockets

Explanation:

Box 1: Azure Application Gateway

You can create an application gateway with URL path-based redirection using Azure PowerShell.

Box 2: Path-based redirection and Websockets

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure//application-gateway/tutorial-url-redirect-powershell>

QUESTION 46

Drag and Drop Question

You have an Azure subscription that contains two virtual networks named VNet1 and VNet2. Virtual machines connect to the virtual networks.

The virtual networks have the address spaces and the subnets configured as shown in the following table.

Virtual network	Address space	Subnet	Peering
VNet1	10.1.0.0/16	10.1.0.0/24 10.1.1.0/26	VNet2
VNet2	10.2.0.0/26	10.2.0.0/24	VNet1

You need to add the address space of 10.33.0.0/16 to VNet1. The solution must ensure that the hosts on VNet1 and VNet2 can communicate.

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.

Actions	Answer Area
On the peering connection in VNet2, allow gateway transit.	
Recreate peering between VNet1 and VNet2.	
Remove VNet1.	
Create a new virtual network named VNet1.	
On the peering connection in VNet1, allow gateway transit.	
Add the 10.33.0.0/16 address space to VNet1.	
Remove peering between VNet1 and VNet2.	

Answer:

Actions	Answer Area
On the peering connection in VNet2, allow gateway transit.	Remove peering between VNet1 and VNet2.
Remove VNet1.	Add the 10.33.0.0/16 address space to VNet1.
Create a new virtual network named VNet1.	Recreate peering between VNet1 and VNet2.
On the peering connection in VNet1, allow gateway transit.	

Explanation:

Step 1: Remove peering between VNet1 and VNet2.

You can't add address ranges to, or delete address ranges from a virtual network's address space once a virtual network is peered with another virtual network. To add or remove address ranges, delete the peering, add or remove the address ranges, then re-create the peering.

Step 2: Add the 10.44.0.0/16 address space to VNet1.

Step 3: Recreate peering between VNet1 and VNet2

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering>

QUESTION 47

Hotspot Question

You have an Azure subscription named Subscription1. Subscription1 contains the resources in the following table.

Name	Type
RG1	Resource group
RG2	Resource group
VNet1	Virtual network
VNet2	Virtual network

VNet1 is in RG1. VNet2 is in RG2. There is no connectivity between VNet1 and VNet2.

An administrator named Admin1 creates an Azure virtual machine named VM1 in RG1. VM1 uses a disk named Disk1 and connects to VNet1. Admin1 then installs a custom application in VM1.

You need to move the custom application to VNet2. The solution must minimize administrative effort.

Which two actions should you perform? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

First action:	<p>▼</p> <p>Create a network interface in RG2.</p> <p>Detach a network interface.</p> <p>Delete VM1.</p> <p>Move a network interface to RG2.</p>
Second action:	<p>▼</p> <p>Attach a network interface.</p> <p>Create a network interface in RG2.</p> <p>Create a new virtual machine.</p> <p>Move VM1 to RG2.</p>

Answer:

Answer Area

First action:	<p>▼</p> <p>Create a network interface in RG2.</p> <p>Detach a network interface.</p> <p>Delete VM1.</p> <p>Move a network interface to RG2.</p>
Second action:	<p>▼</p> <p>Attach a network interface.</p> <p>Create a network interface in RG2.</p> <p>Create a new virtual machine.</p> <p>Move VM1 to RG2.</p>

Explanation:

We cannot just move a virtual machine between networks. What we need to do is identify the disk used by the VM, delete the VM itself while retaining the disk, and recreate the VM in the target virtual network and then attach the original disk to it.

Reference:

<https://blogs.technet.microsoft.com/canitpro/2014/06/16/step-by-step-move-a-vm-to-a-different-vnet-on-azure/>

<https://4sysops.com/archives/move-an-azure-vm-to-another-virtual-network-vnet/#migrate-an-azure-vm-between-vnets>

QUESTION 48

Hotspot Question

You company has an Azure Container Registry named Registry1.

You have an Azure virtual machine named Server1 that runs Windows Server 2019.

From Server1, you create a container image named image1.

You need to add image1 to Registry1.

Which command should you run on Server1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

<input type="checkbox"/>	push	<input type="checkbox"/>
<input type="checkbox"/>		registry1.azurecr.io
<input type="checkbox"/>		registry1.onmicrosoft.com
<input type="checkbox"/>		https://registry1.onmicrosoft.com
<input type="checkbox"/>		\\\\registry1.blob.core.windows.net

Answer:

Answer Area

<input checked="" type="checkbox"/>	push	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>		registry1.azurecr.io
<input checked="" type="checkbox"/>		registry1.onmicrosoft.com
<input checked="" type="checkbox"/>		https://registry1.onmicrosoft.com
<input checked="" type="checkbox"/>		\\\\registry1.blob.core.windows.net

Explanation:

An Azure container registry stores and manages private Docker container images, similar to the way Docker Hub stores public Docker images. You can use the Docker command-line interface (Docker CLI) for login, push, pull, and other operations on your container registry.

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-get-started-docker-cli>

<https://docs.docker.com/engine/reference/commandline/push/>

QUESTION 49

Hotspot Question

You are developing an Azure Web App. You configure TLS mutual authentication for the web app.

You need to validate the client certificate in the web app. To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Property	Value
Client certificate location	<input type="checkbox"/> HTTP request header <input type="checkbox"/> Client cookie <input type="checkbox"/> HTTP message body <input type="checkbox"/> URL query string
Encoding type	<input type="checkbox"/> HTML <input type="checkbox"/> URL <input type="checkbox"/> Unicode <input type="checkbox"/> Base64

Answer:

Answer Area

Property	Value
Client certificate location	<div style="border: 1px solid black; padding: 5px;"><div style="background-color: #e0f2e0; height: 15px;"></div><div style="background-color: #d9ead3; height: 15px;"></div><div style="background-color: #d9ead3; height: 15px;"></div><div style="background-color: #d9ead3; height: 15px;"></div><div style="background-color: #d9ead3; height: 15px;"></div></div>
Encoding type	<div style="border: 1px solid black; padding: 5px;"><div style="background-color: #e0f2e0; height: 15px;"></div><div style="background-color: #d9ead3; height: 15px;"></div><div style="background-color: #d9ead3; height: 15px;"></div><div style="background-color: #d9ead3; height: 15px;"></div><div style="background-color: #d9ead3; height: 15px;"></div></div>

QUESTION 50

Drag and Drop Question

You are designing a solution to secure a company's Azure resources. The environment hosts 10 teams. Each team manages a project and has a project manager, a virtual machine (VM) operator, developers, and contractors.

Project managers must be able to manage everything except access and authentication for users. VM operators must be able to manage VMs, but not the virtual network or storage account to which they are connected. Developers and contractors must be able to manage storage accounts.

You need to recommend roles for each member.

What should you recommend? To answer, drag the appropriate roles to the correct employee types. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles	Answer Area	
	Employee type	Role
Owner	Project manager	Role
Contributor	VM operators	Role
Reader	Developers	Role
Virtual Machine Contributor	Contractors	Role
Storage Account Contributor		

Answer:

Roles	Answer Area	
	Employee type	Role
Owner	Project manager	Contributor
Contributor	VM operators	Virtual Machine Contributor
Reader	Developers	Storage Account Contributor
Virtual Machine Contributor	Contractors	Storage Account Contributor
Storage Account Contributor		

QUESTION 51

Hotspot Question

Your company has a virtualization environment that contains the virtualization hosts shown in the following table.

Name	Hypervisor	Guest
Server1	VMware	VM1, VM2, VM3
Server2	Hyper-V	VMA, VMB, VMC

The virtual machines are configured as shown in the following table.

Name	Generation	Memory	Operating system (OS)	OS disk	Data disk
VM1	<i>Not applicable</i>	4 GB	Windows Server 2016	200 GB	800 GB
VM2	<i>Not applicable</i>	12 GB	Red Hat Enterprise Linux 7.2	3 TB	200 GB
VM3	<i>Not applicable</i>	32 GB	Windows Server 2012 R2	200 GB	1 TB
VMA	1	8 GB	Windows Server 2012	100 GB	2 TB
VMB	1	16 GB	Red Hat Enterprise Linux 7.2	150 GB	3 TB
VMC	2	24 GB	Windows Server 2016	500 GB	6 TB

All the virtual machines use basic disks. VM1 is protected by using BitLocker Drive Encryption (BitLocker).

You plan to migrate the virtual machines to Azure by using Azure Site Recovery.

You need to identify which virtual machines can be migrated.

Which virtual machines should you identify for each server? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

The virtual machines that can be migrated from Server1:

VM1 only
VM2 only
VM3 only
VM1 and VM2 only
VM1 and VM3 only
VM1, VM2, and VM3

The virtual machines that can be migrated from Server2:

VMA only
VMB only
VMC only
VMA and VMB only
VMA and VMC only
VMA, VMB, and VMC

Answer:

Answer Area

The virtual machines that can be migrated from Server1:

VM1 only
VM2 only
VM3 only
VM1 and VM2 only
VM1 and VM3 only
VM1, VM2, and VM3

The virtual machines that can be migrated from Server2:

VMA only
VMB only
VMC only
VMA and VMB only
VMA and VMC only
VMA, VMB, and VMC

Explanation:

Incorrect Answers:

VM1 cannot be migrates as it has BitLocker enabled.

VM2 cannot be migrates as the OS disk on VM2 is larger than 2TB. VMC cannot be migrates as the Data disk on VMC is larger than 4TB.

Reference:

<https://docs.microsoft.com/en-us/azure/site-recovery/hyper-v-azure-support-matrix#azure-vm-requirements>

QUESTION 52

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant.

You need to create a conditional access policy that requires all users to use multi-factor authentication when they access the Azure portal.

Which three settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

* Name

Policy1



Assignments

Users and groups i

0 users and groups selected



Cloud apps i

0 cloud apps selected



Conditions i

0 conditions selected



Access controls

Grant i

0 controls selected



Session i

0 controls selected



Enable policy

On

Off

Answer:

* Name
Policy1 

Assignments

Users and groups  >
0 users and groups selected

Cloud apps  >
0 cloud apps selected

Conditions  >
0 conditions selected

Access controls

Grant  >
0 controls selected

Session  >
0 controls selected

Enable policy

Explanation:

You will use the Users and Groups section to choose the group. You would then choose the Cloud Apps or actions section to ensure that the setting is enforced during the use of accessing the Azure Portal. And then you would use the Grant section to enforce Multi-Factor Authentication.

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa>

QUESTION 53

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant that contains the user groups shown in the following table.

Name	Role	Member of
User1	Global administrator	<i>None</i>
User2	User administrator	Group1
User3	Password administrator	Group1
User4	<i>None</i>	Group1

You enable self-service password reset (SSPR) for Group1.

You configure the Notifications settings as shown in the following exhibit.

Save Discard

Notify users on password resets?

Yes No

Notify all admins when other admins reset their password?

Yes No

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 Area

Statements	Yes	No
User1 gets a notification when User3 resets her password by using SSPR.	<input type="radio"/>	<input type="radio"/>
User3 gets a notification when User3 resets her password by using SSPR.	<input type="radio"/>	<input type="radio"/>
User1 gets a notification when User2 resets the password of User4.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 gets a notification when User3 resets her password by using SSPR.	<input checked="" type="radio"/>	<input type="radio"/>
User3 gets a notification when User3 resets her password by using SSPR.	<input type="radio"/>	<input checked="" type="radio"/>
User1 gets a notification when User2 resets the password of User4.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

Notify all admins when other admins reset their passwords: Yes.

Box 2: No

Notify users on password resets: No.

Box 3: No

Notify users on password resets

If this option is set to Yes, then users resetting their password receive an email notifying them that their password has been changed. The email is sent via the SSPR portal to their primary and alternate email addresses that are on file in Azure AD. No one else is notified of the reset event.

Notify all admins when other admins reset their passwords

If this option is set to Yes, then all administrators receive an email to their primary email address on file in Azure AD. The email notifies them that another administrator has changed their password by using SSPR.

Example: There are four administrators in an environment. Administrator A resets their password by using SSPR. Administrators B, C, and D receive an email alerting them of the password reset.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-howitworks>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr>

QUESTION 54

Hotspot Question

You have an Azure logic app named App1 and an Azure Service Bus queue named Queue1.

You need to ensure that App1 can read messages from Queue1. App1 must authenticate by using Azure Active Directory (Azure AD).

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

NOTE: Each correct selection is worth one point.

Answer Area

On App1:

- | |
|--------------------------------|
| Add a logic app step |
| Configure Access control (IAM) |
| Regenerate the access key |
| Turn on the managed identity |

On Queue1:

- | |
|--------------------------------|
| Add a read-only lock |
| Add a shared access policy |
| Configure Access control (IAM) |
| Modify the properties |

Answer:

Answer Area

On App1:

- | |
|--------------------------------|
| Add a logic app step |
| Configure Access control (IAM) |
| Regenerate the access key |
| Turn on the managed identity |

On Queue1:

- | |
|--------------------------------|
| Add a read-only lock |
| Add a shared access policy |
| Configure Access control (IAM) |
| Modify the properties |

Explanation:

On App1: Turn on the managed identity

To use Service Bus with managed identities, you need to assign the identity the role and the appropriate scope. The procedure in this section uses a simple application that runs under a managed identity and accesses Service Bus resources.

Once the application is created, follow these steps:

1. Go to Settings and select Identity.
2. Select the Status to be On.
3. Select Save to save the setting.

On Queue1: Configure Access Control (IAM)

Azure Active Directory (Azure AD) authorizes access rights to secured resources through role-based access control (RBAC). Azure Service Bus defines a set of built-in RBAC roles that encompass common sets of permissions used to access Service Bus entities and you can also define custom roles for accessing the data.

Assign RBAC roles using the Azure portal

In the Azure portal, navigate to your Service Bus namespace. Select Access Control (IAM) on the left menu to display access control settings for the namespace. If you need to create a Service Bus namespace.

Select the Role assignments tab to see the list of role assignments. Select the Add button on the toolbar and then select Add role assignment.

Reference:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/authenticate-application>

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-managed-service-identity>

QUESTION 55

Hotspot Question

You have an Azure subscription.

You plan to deploy an app that has a web front end and an application tier.

You need to recommend a load balancing solution that meets the following requirements:

Internet to web tier:

- Provides URL-based routing
- Supports connection draining
- Prevents SQL injection attacks

Web tier to application tier:

- Provides port forwarding
- Supports HTTPS health probes
- Supports an availability set as a backend pool

Which load balancing solution should you recommend for each tier? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Internet to web tier:

An Azure Application Gateway that has a web application firewall (WAF)
An internal Azure Standard Load Balancer
A public Azure Basic Load Balancer

Web tier to application tier:

An Azure Application Gateway that has a web application firewall (WAF)
An internal Azure Standard Load Balancer
A public Azure Basic Load Balancer

Answer:

Answer Area

Internet to web tier:

An Azure Application Gateway that has a web application firewall (WAF)
An internal Azure Standard Load Balancer
A public Azure Basic Load Balancer

Web tier to application tier:

An Azure Application Gateway that has a web application firewall (WAF)
An internal Azure Standard Load Balancer
A public Azure Basic Load Balancer

Explanation:

Box 1: An Azure Application Gateway that has a web application firewall (WAF) Azure Application Gateway offers a web application firewall (WAF) that provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

Application Gateway operates as an application delivery controller (ADC). It offers Secure Sockets Layer (SSL) termination, cookie-based session affinity, round-robin load distribution, content-based routing, ability to host multiple websites, and security enhancements.

Box 2: An internal Azure Standard Load Balancer

The internet to web tier is the public interface, while the web tier to application tier should be internal.

Note: When using load-balancing rules with Azure Load Balancer, you need to specify a health probes to allow Load Balancer to detect the backend endpoint status.

Health probes support the TCP, HTTP, HTTPS protocols.

Reference:

<https://docs.microsoft.com/en-us/azure/application-gateway/waf-overview>

<https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview>

QUESTION 56

Hotspot Question

You have an Azure subscription named Subscription1 that contains a virtual network named VNet1.

You add the users in the following table.

User	Role
User1	Owner
User2	Security Admin
User3	Network Contributor

Which user can perform each configuration? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Add a subnet to VNet1:

User1 only
User3 only
User1 and User3 only
User2 and User3 only
User1, User2, and User3

Assign a user the Reader role to VNet1:

User1 only
User2 only
User3 only
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Answer:

Answer Area

Add a subnet to VNet1:

User1 only
User3 only
User1 and User3 only
User2 and User3 only
User1, User2, and User3

Assign a user the Reader role to VNet1:

User1 only
User2 only
User3 only
User1 and User2 only
User2 and User3 only
User1, User2, and User3

Explanation:

Box 1: User1 and User3 only

Owner have all privileges and Network Contributor can create and manage resources but not access so creation is possible

Box 2: User1 only

Security admin an view and update permission, not create

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

QUESTION 57

Hotspot Question

A company runs multiple Windows virtual machines (VMs) in Azure.

The IT operations department wants to apply the same policies as they have for on-premises VMs to the VMs running in Azure, including domain administrator permissions and schema

extensions.

You need to recommend a solution for the hybrid scenario that minimizes the amount of maintenance required.

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

NOTE: Each correct selection is worth one point.

Answer Area

Component	Action
Domain	<ul style="list-style-type: none">Join the VMs to the existing on-premises domain.Join the VMs to a new domain controller VM in Azure.Join the VMs to Azure Active Directory Domain Services (AD DS).
Connectivity	<ul style="list-style-type: none">Set up VPN connectivity.Set up HTTPS connectivity.Set up Azure Relay Service.

Answer:

Answer Area

Component	Action
Domain	<ul style="list-style-type: none">Join the VMs to the existing on-premises domain.Join the VMs to a new domain controller VM in Azure.Join the VMs to Azure Active Directory Domain Services (AD DS).
Connectivity	<ul style="list-style-type: none">Set up VPN connectivity.Set up HTTPS connectivity.Set up Azure Relay Service.

Explanation:

Box 1: Join the VMs to a new domain controller VM in Azure Azure provides two solutions for implementing directory and identity services in Azure:

(Used in this scenario) Extend your existing on-premises Active Directory infrastructure to Azure, by deploying a VM in Azure that runs AD DS as a Domain Controller. This architecture is more common when the on-premises network and the Azure virtual network (VNet) are connected by a VPN or ExpressRoute connection.

Use Azure AD to create an Active Directory domain in the cloud and connect it to your on-premises Active Directory domain. Azure AD Connect integrates your on-premises directories with Azure AD.

Box 2: Set up VPN connectivity.

This architecture is more common when the on-premises network and the Azure virtual network (VNet) are connected by a VPN or ExpressRoute connection.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/identity/>

QUESTION 58

You have an Azure Kubernetes Service (AKS) cluster named Clus1 in a resource group named RG1.

An administrator plans to manage Clus1 from an Azure AD-joined device.

You need to ensure that the administrator can deploy the YAML application manifest file for a container application.

You install the Azure CLI on the device.

Which command should you run next?

- A. kubectl get nodes
- B. az aks install-cli
- C. kubectl apply -f appl.yaml
- D. az aks get-credentials --resource-group RG1 --name Clus1

Answer: B

Explanation:

To manage a Kubernetes cluster, you use kubectl, the Kubernetes command-line client. If you use Azure Cloud Shell, kubectl is already installed. To install kubectl locally, use the az aks install-cli command.

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-walkthrough>

QUESTION 59

Note: This question is part of 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.

Your network contains an Active Directory forest named fabrikam.com. The forest contains two child domains named corp.fabrikam.com and research.fabrikam.com.

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com.

You install Azure AD Connect and sync all the on-premises user accounts to the Azure AD tenant. You implement seamless single sign-on (SSO).

You plan to change the source of authority for all the user accounts in research.fabrikam.com to Azure AD.

You need to prevent research.fabrikam.com from resyncing to Azure AD.

Solution: You use Active Directory Domains and Trusts from a computer joined to fabrikam.com.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead you should customize the default synchronization rule.

Note:

To delete a custom domain name, you must first ensure that no resources in your directory rely on the domain name. You can't delete a domain name from your directory if:

Any user has a user name, email address, or proxy address that includes the domain name.

Any group has an email address or proxy address that includes the domain name.

Any application in your Azure AD has an app ID URI that includes the domain name.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-create-custom-sync-rule>

QUESTION 60

You have an Azure subscription named Subscription1.

You create several Azure virtual machines in Subscription1. All of the virtual machines belong to the same virtual network.

You have an on-premises Hyper-V server named Server1. Server1 hosts a virtual machine named VM1.

You plan to replicate VM1 to Azure.

You need to create additional objects in Subscription1 to support the planned deployment.

Which three objects should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Hyper-V site
- B. Azure Recovery Services Vault
- C. storage account
- D. replication policy
- E. Azure Traffic Manager instance
- F. endpoint

Answer: ABD

QUESTION 61

Hotspot Question

You have an Azure Service Bus and a queue named Queue1. Queue1 is configured as shown in the following exhibit.

* Name i

Queue1



Max queue size

1 GB



Message time to live i

Days

Hours

Minutes

Seconds

0

2

0

0

Lock duration i

Days

Hours

Minutes

Seconds

0

0

5

0

Enable duplicate detection i

Enable dead lettering on message expiration i

Enable sessions i

Enable partitioning i

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

If a message is written to Queue1 and is never read, the message will be

- ▼ deleted after 24 hours
- deleted after two hours and five minutes
- deleted after two hours
- retained until it is deleted manually

If a message is written to Queue1, and then read after one hour, the message will be

- ▼ deleted immediately
- deleted after five minutes
- deleted after one hour
- retained until it is deleted manually

Answer:

Answer Area

If a message is written to Queue1 and is never read, the message will be

- ▼ deleted after 24 hours
- deleted after two hours and five minutes
- deleted after two hours
- retained until it is deleted manually

If a message is written to Queue1, and then read after one hour, the message will be

- ▼ deleted immediately
- deleted after five minutes
- deleted after one hour
- retained until it is deleted manually

QUESTION 62

Hotspot Question

Your organization has developed and deployed several Azure App Service Web and API applications. The applications use Azure SQL Database to store and retrieve data. Several departments have the following requests to support the applications:

Department	Request
Database	Store an asymmetric key to allow real-time I/O encryption and decryption of the Azure SQL Database data and log files.
Development	Enable the applications to retrieve x.509 certificates, stored in an Azure AD-protected resource, by using an access token.
Security	Protect Azure SQL Database connection strings and only allow access to the connection strings during the application runtime.

You need to recommend the appropriate Azure service for each department request.

What should you recommend? To answer, configure the appropriate options in the dialog box in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Department	Azure Service
Database	<ul style="list-style-type: none">Azure AD Privileged Identity ManagementAzure AD Managed Service IdentityAzure Key VaultAzure Security Center
Development	<ul style="list-style-type: none">Azure AD Privileged Identity ManagementAzure AD Managed Service IdentityAzure Key VaultAzure Security Center
Security	<ul style="list-style-type: none">Azure AD Privileged Identity ManagementAzure AD Managed Service IdentityAzure Key VaultAzure Security Center

Answer:

Answer Area

Department	Azure Service
Database	Azure AD Privileged Identity Management Azure AD Managed Service Identity Azure Key Vault Azure Security Center
Development	Azure AD Privileged Identity Management Azure AD Managed Service Identity Azure Key Vault Azure Security Center
Security	Azure AD Privileged Identity Management Azure AD Managed Service Identity Azure Key Vault Azure Security Center

Explanation:

<https://docs.microsoft.com/en-us/azure/sql-database/transparent-data-encryption-azure-sql>

QUESTION 63

Note: This question is part of 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 are planning to create a virtual network that has a scale set that contains six virtual machines (VMs).

A monitoring solution on a different network will need access to the VMs inside the scale set.

You need to define public access to the VMs.

Solution: Use Remote Desktop Protocol (RDP) to connect to the VM in the scale set.

Does the solution meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead, deploy a standalone VM that has a public IP address to the virtual network.

QUESTION 64

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Address space	Location	Number of Azure virtual machines
VNET1	10.1.0.0/16	West US	100
VNET2	172.16.0.0/16	East US	400

You need to recommend a connectivity solution that will enable the virtual machines on VNET1 and VNET2 to communicate through the Microsoft backbone infrastructure.

What should you include in the recommendation?

- A. Azure ExpressRoute
- B. peering
- C. a site-to-site VPN
- D. a point-to-site VPN

Answer: B

Explanation:

Virtual network peering enables you to seamlessly connect Azure virtual networks. Once peered, the virtual networks appear as one, for connectivity purposes. The traffic between virtual machines in the peered virtual networks is routed through the Microsoft backbone infrastructure, much like traffic is routed between virtual machines in the same virtual network, through private IP addresses only. Azure supports:

VNet peering - connecting VNets within the same Azure region

Global VNet peering - connecting VNets across Azure regions

References:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview>

QUESTION 65

You create an Azure virtual machine named VM1 in a resource group named RG1.

You discover that VM1 performs slower than expected.

You need to capture a network trace on VM1.

What should you do?

- A. From Diagnostic settings for VM1, configure the performance counters to include network counters.
- B. From the VM1 blade, configure Connection troubleshoot.
- C. From the VM1 blade, install performance diagnostics and run advanced performance analysis
- D. From Diagnostic settings for VM1, configure the log level of the diagnostic agent.

Answer: C

Explanation:

The performance diagnostics tool helps you troubleshoot performance issues that can affect a Windows or Linux virtual machine (VM). Supported troubleshooting scenarios include quick checks on known issues and best practices, and complex problems that involve slow VM performance or high usage of CPU, disk space, or memory.

Advanced performance analysis, included in the performance diagnostics tool, includes all checks in the performance analysis, and collects one or more of the traces, as listed in the following sections. Use this scenario to troubleshoot complex issues that require additional traces. Running this scenario for longer periods will increase the overall size of diagnostics output, depending on the size of the VM and the trace options that are selected.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/troubleshooting/performance-diagnostics>

QUESTION 66

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Region
RG1	East US
RG2	West US

The subscription contains the storage accounts shown in the following table.

Name	Resource group	Location	Account kind
Storage1	RG1	West US	BlobStorage
Storage2	RG2	West US	Storage (general purpose v1)
Storage3	RG1	East US	Storage V2 (general purpose v2)

You create a Recovery Services vault named Vault1 in RG1 in the West US location.

You need to identify which storage accounts can be used to archive the diagnostics logs of Vault1.

Which storage accounts should you identify?

- A. Storage1 only
- B. Storage2 only
- C. Storage3 only
- D. Storage1 or Storage2 only
- E. Storage1 or Storage3 only

Answer: D

Explanation:

Vault must be in the same region as the logs to be archived from the storage account. Hence, only storage accounts within West US can be used → Answer D

QUESTION 67

You have an Azure subscription.

You create a custom role in Azure by using the following Azure Resource Manager template.

```
{  
    "Name": "Role1",  
    "Id": "88888888-8888-8888-888888888888",  
    "IsCustom" : true,  
    "Description" : "Role1 Description",  
    "Actions" : [  
        "Microsoft.Storage/*/read",  
        "Microsoft.Network/*/read",  
        "Microsoft.Compute/*/read",  
        "Microsoft.Compute/virtualMachines/start/action",  
        "Microsoft.Compute/virtualMachines/restart/action",  
        "Microsoft.Authorization/*/read",  
        "Microsoft.ResourceHealth/availabilityStatuses/read",  
        "Microsoft.Resources/subscriptions/resourceGroups/read",  
        "Microsoft.Insights/alertRules/*",  
        "Microsoft.Insights/diagnosticSettings/*",  
        "Microsoft.Support/*"  
    ],  
    "NotActions": [],  
    "DataActions": [],  
    "NotDataActions" : [],  
    "AssignableScopes" : [  
        "/subscriptions/981dd4bc-8cf4-46fc-9513-0c599648b44b  
    ]  
}
```

You assign the role to a user named User1.

Which action can User1 perform?

- A. Delete virtual machines.
- B. Create resource groups.
- C. Create virtual machines.
- D. Create support requests.

Answer: D

Explanation:

The "Microsoft.Support/*" operation will allow the user to create support tickets.

References:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/tutorial-custom-role-powershell>

QUESTION 68

A company plans to use third-party application software to perform complex data analysis processes. The software will use up to 500 identical virtual machines (VMs) based on an Azure Marketplace VM image.

You need to design the infrastructure for the third-party application server. The solution must meet the following requirements:

- The number of VMs that are running at any given point in time must change when the user workload changes.
- When a new version of the application is available in Azure Marketplace it must be deployed without causing application downtime.
- Use VM scale sets.
- Minimize the need for ongoing maintenance.

Which two technologies should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. single storage account
- B. autoscale
- C. single placement group
- D. managed disks

Answer: BD

QUESTION 69

You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Account kind	Size
contosostorage1	General Purpose v1	15 TB
contosostorage2	General Purpose v1	1 TB
contosostorage3	General Purpose v2	15 TB
contosostorage4	General Purpose v2	1 TB
contosostorage5	blobstorage	5 TB

All storage accounts contain blobs only.

You need to implement several lifecycle management rules for all storage accounts.

What should you do first?

- A. Upgrade contosostorage1 and contosostorage2 to General Purpose V2 accounts.
- B. Move 5 TB of blob data from contosostorage3 to contosostorage4.
- C. Move 5 TB of blob data from contosostorage1 to contosostorage2.
- D. Recreate contosostorage5 as General Purpose V2 account.

Answer: A

Explanation:

Microsoft recommends that you use a general-purpose v2 storage account for most scenarios. You can easily upgrade a general-purpose v1 or an Azure Blob storage account to a general-purpose v2 account with no downtime and without the need to copy data.

References:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-scalability-targets>

QUESTION 70

Note: This question is part of 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 an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other Identity Governance settings are available.

Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.

You need to ensure that the Admin1 can create access reviews in contoso.com.

Solution: You consent to Azure AD Privileged Identity Management (PIM).

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:

Conduct access reviews to ensure users still need roles

Note: Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization. This includes access to resources in Azure AD, Azure resources, and other Microsoft Online Services like Office 365 or Microsoft Intune.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

QUESTION 71

Note: This question is part of 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 an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other Identity Governance settings are available.

Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.

You need to ensure that the Admin1 can create access reviews in contoso.com.

Solution: You assign the Global administrator role to Admin1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead use Azure AD Privileged Identity Management.

Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:

Conduct access reviews to ensure users still need roles

References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

QUESTION 72

Note: This question is part of 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 an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other Identity Governance settings are available.

Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.

You need to ensure that the Admin1 can create access reviews in contoso.com.

Solution: You purchase an Azure Directory Premium P2 license for contoso.com.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead use Azure AD Privileged Identity Management.

Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:

Conduct access reviews to ensure users still need roles

References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

QUESTION 73

You have a resource group named RG1 that contains the following:

- A virtual network that contains two subnets named Subnet1 and Subnet2
- An Azure Storage account named contososa1
- An Azure firewall deployed to Subnet2

You need to ensure that contososa1 is accessible from Subnet1 over the Azure backbone network.

What should you do?

- A. Deploy an Azure firewall to Subnet1.
- B. Remove the Azure firewall.
- C. Implement a virtual network service endpoint.
- D. Create a stored access policy for contososa1.

Answer: C

Explanation:

Virtual Network (VNet) service endpoints extend your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Traffic from your VNet to the Azure service always remains on the Microsoft Azure backbone network.

References:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-service-endpoints-overview>

QUESTION 74

Your company has the groups shown in the following table.

Group	Number of members
Managers	10
Sales	100
Development	15

The company has an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com.

An administrator named Admin1 attempts to enable Enterprise State Roaming for all the users in the Managers group.

Admin1 reports that the options for Enterprise State Roaming are unavailable from Azure AD.

You verify that Admin1 is assigned the Global administrator role.

You need to ensure that Admin1 can enable Enterprise State Roaming.

What should you do?

- A. Enforce Azure Multi-Factor Authentication (MFA) for Admin1.
- B. Purchase an Azure AD Premium P1 license for each user in the Managers group.
- C. Assign an Azure AD Privileged Identity Management (PIM) role to Admin1.
- D. Purchase an Azure Rights Management (Azure RMS) license for each user in the Managers group.

Answer: B

Explanation:

Enterprise State Roaming is available to any organization with an Azure AD Premium or Enterprise Mobility + Security (EMS) license.

References:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/devices/enterprise-state-roaming-enable>

QUESTION 75

You create a new Azure subscription. You create a resource group named RG1. In RG1, you create the resources shown in the following table.

Name	Type
VNET1	Virtual network
VM1	Virtual machine
GWSN1	Gateway subnet
VPNGW1	Virtual network gateway

You need to configure an encrypted tunnel between your on-premises network and VNET1.

Which two additional resources should you create in Azure? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a site-to-site connection
- B. a VPN gateway
- C. a VNet-to VNet connection
- D. a local network gateway
- E. a point-to-site configuration

Answer: BD

Explanation:

A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires

a VPN device, a local network gateway, located on-premises that has an externally facing public IP address assigned to it.

Finally, create a Site-to-Site VPN connection between your virtual network gateway and your on-premises VPN device.

References:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

QUESTION 76

Note: This question is part of 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 an Azure subscription.

You have an on-premises file server named Server1 that runs Windows Server 2019.

You manage Server1 by using Windows Admin Center.

You need to ensure that if Server1 fails, you can recover the data from Azure.

Solution: From the Azure portal, you create a Recovery Services vault. On VM1, you install the Azure Backup agent and you schedule a backup.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead use Azure Storage Sync service and configure Azure File.

Use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share.

References:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction>

QUESTION 77

Note: This question is part of 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 an Azure subscription.

You have an on-premises file server named Server1 that runs Windows Server 2019.

You manage Server1 by using Windows Admin Center.

You need to ensure that if Server1 fails, you can recover the data from Azure.

Solution: You create a Recovery Services vault and configure a backup by using Windows Server Backup.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead use Azure Storage Sync service and configure Azure File.

Use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share.

References:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction>

QUESTION 78

Note: This question is part of 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 an Azure subscription.

You have an on-premises file server named Server1 that runs Windows Server 2019.

You manage Server1 by using Windows Admin Center.

You need to ensure that if Server1 fails, you can recover the data from Azure.

Solution: You create an Azure Storage account and an Azure Storage Sync service. You configure Azure File Sync for Server1.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share.

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol. Azure file shares can be mounted concurrently

by cloud or on-premises deployments of Windows, Linux, and macOS. Additionally, Azure file shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.

Azure file shares can be used to:

Replace or supplement on-premises file servers:

Azure Files can be used to completely replace or supplement traditional on-premises file servers or NAS devices. Popular operating systems such as Windows, macOS, and Linux can directly mount Azure file shares wherever they are in the world. Azure file shares can also be replicated with Azure File Sync to Windows Servers, either on-premises or in the cloud, for performance and distributed caching of the data where it's being used.

References:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-introduction>

<https://docs.microsoft.com/en-us/azure/storage/files/storage-sync-files-deployment-guide?tabs=azure-portal>

QUESTION 79

You have an Azure subscription that contains the Azure virtual machines shown in the following table.

Name	Operating system	Location
VM1	Windows Server 2012 R2	East US
VM2	Windows Server 2016	East US
VM3	Windows Server 2019	West US
VM4	Ubuntu Server 18.04	East US

You create an Azure key vault named Vault1 in the East US location.

You need to identify which virtual machines can enable Azure Disk Encryption by using Vault1. Which virtual machines should you identify?

- A. VM2 and VM3 only
- B. VM1, VM2, and VM4 only
- C. VM1, VM2, and VM3 only
- D. VM3 only

Answer: B

Explanation:

Your key vault and VMs must reside in the same Azure region and subscription.

References:

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

QUESTION 80

A company is migrating an existing on-premises third-party website to Azure. The website is stateless.

The company does not have access to the source code for the website. They have the original installer.

The number of visitors at the website varies throughout the year. The on-premises infrastructure was resized to accommodate peaks but the extra capacity was not used.

You need to implement a virtual machine scale set instance.

What should you do

- A. Use a webhook to log autoscale failures.
- B. Use an autoscale setting to scale instances vertically.
- C. Use only default diagnostics metrics to trigger autoscaling
- D. Use an autoscale setting to define more profiles that have one or more autoscale rules.

Answer: C

Explanation:

In-guest VM metrics with the Azure diagnostics extension The Azure diagnostics extension is an agent that runs inside a VM instance. The agent monitors and saves performance metrics to Azure storage. These performance metrics contain more detailed information about the status of the VM, such as AverageReadTime for disks or PercentIdleTime for CPU. You can create autoscale rules based on a more detailed awareness of the VM performance, not just the percentage of CPU usage or memory consumption.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-autoscale-overview>

QUESTION 81

Note: This question is part of 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 an Azure Cosmos DB database that contains a container named Container1. The partition key for Container1 is set to /day. Container1 contains the items shown in the following table.

Name	Content
Item1	{ "id": "1", "day": "Mon", "value" : "10" }
Item2	{ "id": "2", "day": "Mon", "value" : "15" }
Item3	{ "id": "3", "day": "True", "value" : "10" }
Item4	{ "id": "4", "day": "Wed", "value" : "15" }

You need to programmatically query Azure Cosmos DB and retrieve item1 and item2 only.

Solution: You run the following query.

```
SELECT day
  WHERE value = "10"
```

You set the EnableCrossPartitionQuery property to False.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

QUESTION 82

Note: This question is part of 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 an Azure Cosmos DB database that contains a container named Container1. The partition key for Container1 is set to /day. Container1 contains the items shown in the following table.

Name	Content
Item1	{ "id": "1", "day": "Mon", "value" : "10" }
Item2	{ "id": "2", "day": "Mon", "value" : "15" }
Item3	{ "id": "3", "day": "True", "value" : "10" }
Item4	{ "id": "4", "day": "Wed", "value" : "15" }

You need to programmatically query Azure Cosmos DB and retrieve item1 and item2 only.

Solution: You run the following query.

```
SELECT day FROM c
WHERE c.value = "10" OR c.value = "15"
```

You set the EnableCrossPartitionQuery property to True.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The screenshot shows the Azure Cosmos DB SQL API interface. On the left, the navigation pane includes sections for __Cosmos, __Query, Items, Scale & Settings, Stored Procedures, User Defined Functions, and Triggers. Under __Query, there is a 'Query' section. The main area displays a query editor with the following content:

```
Items | Bring all values | Query 2 |
```

```
1 SELECT day FROM c
2 where c.value = "10" OR c.value = "15"
```

Below the query editor, an 'Errors' section shows a message: "Gateway Failed to Retrieve Query Plan: Message: [\"errors\":[{\"severity\":\"Error\",\"location\":{\"start\":27,\"end\":32},\"code\":\"SC1001\",\"message\":\"Syntax error, incorrect syntax near 'value'.\"]}]".

At the bottom, a notifications panel shows two failed activity logs from 12:44 AM:

- Failed to query item for container container1: Gateway Failed to Retrieve Query Plan: Message: [\"errors\":[{\"severity\":\"Error\",\"location\":{\"start\":27,\"end\":32},\"code\":\"SC1001\",\"message\":\"Syntax error, incorrect syntax near 'value'.\"]}]] ActivityId: da9bd97a-7890-4891-adfa-d469a6c87e63, Microsoft.Azure.Documents.Common/2.11.0, Microsoft.Azure.Documents.Common/2.11.0
- Failed to query item for container container1: Gateway Failed to Retrieve Query Plan: Message: [\"errors\":[{\"severity\":\"Error\",\"location\":{\"start\":27,\"end\":32},\"code\":\"SC1001\",\"message\":\"Syntax error, incorrect syntax near 'value'.\"]}]] ActivityId: 07c716af-bd42-4709-aeca-3e3fd9bcfc32, Microsoft.Azure.Documents.Common/2.11.0, Microsoft.Azure.Documents.Common/2.11.0

QUESTION 83

Note: This question is part of 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 an Azure Cosmos DB database that contains a container named Container1. The partition key for Container1 is set to /day. Container1 contains the items shown in the following table.

Name	Content
Item1	{ "id": "1", "day": "Mon", "value" : "10" }
Item2	{ "id": "2", "day": "Mon", "value" : "15" }
Item3	{ "id": "3", "day": "True", "value" : "10" }
Item4	{ "id": "4", "day": "Wed", "value" : "15" }

You need to programmatically query Azure Cosmos DB and retrieve item1 and item2 only.

Solution: You run the following query.

```
SELECT id FROM c  
WHERE c.day = "Mon"
```

You set the EnableCrossPartitionQuery property to True.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

The screenshot shows the Azure portal interface. On the left, there is a table with columns 'id' and '/day'. The table contains four rows: 1 (id: 1, day: Mon), 2 (id: 2, day: Mon), 3 (id: 3, day: Tue), and 4 (id: 4, day: Wed). A cursor is hovering over the second row. To the right of the table, a large JSON object representing item 1 is displayed, showing its properties like id, day, value, etc. Below the table, there is a 'Load more' button. At the bottom of the screen, there is a 'Query 1' section containing the SQL query: 'SELECT id FROM c WHERE c.day = "Mon"'. Below this, there is an 'Errors' section with a message: 'Gateway Failed to Retrieve Query Plan: Message: {"errors": [{"severity": "Error", "location": {"start": 7, "end": 9}, "code": "..."}]} More details'.

```
1  "id": "1",  
2  "day": "Mon",  
3  "value": "10",  
4  "_rid": "dRlYAP1byEYBAAAAAAAA==",  
5  "_self": " dbs/dRlYAA==/colls/dRlYAP1byEY=/docs/dRlYAP1byEYBAAAAAAAA==/",  
6  "_etag": "\\"05005928-0000-0d00-0000-6005fe080000\\\"",  
7  "_attachments": "attachments/",  
8  "_ts": 1611005448
```

id	/day
1	Mon
2	Mon
3	Tue
4	Wed

Load more

```
1  SELECT id FROM c  
2  where c.day = "Mon"
```

Items ! Query 1 ×

Errors

Gateway Failed to Retrieve Query Plan: Message: {"errors": [{"severity": "Error", "location": {"start": 7, "end": 9}, "code": "..."}]} More details

For you to be able to retrieve Item1 and Item2 the correct query should be:

Items Query 1 x

```
1  SELECT c.id FROM c
2  where c.day = "Mon"
```

Results Query Stats

1 - 2

```
[{"id": "1"}, {"id": "2"}]
```

QUESTION 84

Your company is developing an e-commerce Azure App Service Web App to support hundreds of restaurant locations around the world.

You are designing the messaging solution architecture to support the e-commerce transactions and messages. The e-commerce application has the following features and requirements:

Feature	Requirement
Shopping Cart	<ul style="list-style-type: none"> Items in a shopping cart must be processed by an Azure Function within a specified number of minutes. Failure to process should move the items to a failed state for processing by a separate Azure Function Shopping cart transactions must not be lost and fault conditions must be processed separately Shopping cart transactions must be read by the inventory and sales systems for further processing
Inventory Distribution	<ul style="list-style-type: none"> Items sent to the inventory system must run a separate workflow for each item that includes warehouse, shipping, and order processing updates Inventory uses Azure Blob storage to store inventory items and related information Inventory is processed by using an Azure Logic App
Restaurant Telemetry	<ul style="list-style-type: none"> Restaurants stream millions of daily events from all locations Restaurant data should be captured in Azure Blob storage for conditional processing Restaurant event data should expire after 24 hours

You need to choose the Azure messaging solution to support the Shopping Cart feature.

Which Azure service should you use?

- Azure Service Bus
- Azure Relay
- Azure Event Grid
- Azure Event Hub

Answer: A

Explanation:

Microsoft Azure Service Bus is a fully managed enterprise integration message broker. Service Bus is most commonly used to decouple applications and services from each other, and is a reliable and secure platform for asynchronous data and state transfer.

One common messaging scenario is Messaging: transfer business data, such as sales or purchase orders, journals, or inventory movements.

Incorrect Answers:

B: The Azure Relay service enables you to securely expose services that run in your corporate network to the public cloud.

References:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messaging-overview>

QUESTION 85

Your company is developing an e-commerce Azure App Service Web App to support hundreds of restaurant locations around the world.

You are designing the messaging solution architecture to support the e-commerce transactions and messages. The e-commerce application has the following features and requirements:

Feature	Requirement
Shopping Cart	<ul style="list-style-type: none"> Items in a shopping cart must be processed by an Azure Function within a specified number of minutes. Failure to process should move the items to a failed state for processing by a separate Azure Function Shopping cart transactions must not be lost and fault conditions must be processed separately Shopping cart transactions must be read by the inventory and sales systems for further processing
Inventory Distribution	<ul style="list-style-type: none"> Items sent to the inventory system must run a separate workflow for each item that includes warehouse, shipping, and order processing updates Inventory uses Azure Blob storage to store inventory items and related information Inventory is processed by using an Azure Logic App
Restaurant Telemetry	<ul style="list-style-type: none"> Restaurants stream millions of daily events from all locations Restaurant data should be captured in Azure Blob storage for conditional processing Restaurant event data should expire after 24 hours

You need to choose the Azure messaging solution to support the Restaurant Telemetry feature.

Which Azure service should you use?

- A. Azure Relay
- B. Azure Event Grid
- C. Azure Event Hub
- D. Azure Service Bus

Answer: C

Explanation:

Azure Event Hubs is a big data pipeline. It facilitates the capture, retention, and replay of telemetry and event stream data. The data can come from many concurrent sources. Event Hubs allows telemetry and event data to be made available to a variety of stream-processing infrastructures and analytics services. It is available either as data streams or bundled event batches. This service provides a single solution that enables rapid data retrieval for real-time processing as well as repeated replay of stored raw data. It can capture the streaming data into a file for processing and analysis.

It has the following characteristics:

low latency

capable of receiving and processing millions of events per second
at least once delivery

Note: Comparison of services

Service	Purpose	Type	When to use
Event Grid	Reactive programming	Event distribution (discrete)	React to status changes
Event Hubs	Big data pipeline	Event streaming (series)	Telemetry and distributed data streaming
Service Bus	High-value enterprise messaging	Message	Order processing and financial transactions

References:

<https://docs.microsoft.com/en-us/azure/event-grid/compare-messaging-services>

QUESTION 86

Hotspot Question

You have an Azure subscription.

You plan to deploy two Azure web apps that have the requirements shown in the following table.

Name	Requirement
App1	<ul style="list-style-type: none"> Accessible by using a URL of https://app1.contoso.com Scalable to two instances during busy periods Supports two deployment slots
App2	<ul style="list-style-type: none"> Accessible by using a URL of https://app2.contoso.com Scalable to 15 instances during busy periods Supports three deployment slots

You need to select the App Service plans for the web apps. The solution must minimize costs.

Which App Service plan should you select for each web app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

App1:

B1 Basic
D1 Shared
P1v2 PremiumV2
S1 Standard

App2:

B1 Basic
D1 Shared
P1v2 PremiumV2
S1 Standard

Answer:

Answer Area

App1:

B1 Basic
D1 Shared
P1v2 PremiumV2
S1 Standard

App2:

B1 Basic
D1 Shared
P1v2 PremiumV2
S1 Standard

Explanation:

	FREE	SHARED	BASIC	STANDARD	PREMIUM	ISOLATED*	APP SERVICE LINUX	CONSUMPTION PLAN (FUNCTIONS)
- Limits**								
Apps	10	100	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	500
Disk space	1 GB	1 GB	10 GB	50 GB	250 GB	1 TB		
Max instances			Up to 3	Up to 10	Up to 20	Up to 100		
SLA			99.95%	99.95%	99.95%	99.95%		
Functions on App Service Plans*			✓	✓	✓	✓		
- App Deployment								
Continuous Deployment*	✓	✓	✓	✓	✓	✓ ³	✓	✓
Deployment Slots			✓	✓	✓	✓	✓	

Reference:

<https://azure.microsoft.com/en-us/pricing/details/app-service/plans/>

QUESTION 87

Hotspot Question

You have an Azure subscription that contains the storage account shown in the following table.

Name	Kind	Performance tier	Replication	Location
storage1	StorageV2	Premium	Locally-redundant storage (LRS)	East US
storage2	Storage	Standard	Geo-redundant storage (GRS)	UK West
storage3	BlobStorage	Standard	Locally-redundant storage (LRS)	North Europe

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 Area

Statements	Yes	No
storage1 can host Azure file shares.	<input type="radio"/>	<input type="radio"/>
There are six copies of the data in storage2.	<input type="radio"/>	<input type="radio"/>
storage3 can be converted to a GRS account.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
storage1 can host Azure file shares.	<input type="radio"/>	<input checked="" type="radio"/>
There are six copies of the data in storage2.	<input checked="" type="radio"/>	<input type="radio"/>
storage3 can be converted to a GRS account.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No

Azure Files supports two storage tiers: premium and standard. Standard file shares are created in general purpose (GPv1 or GPv2) storage accounts and premium file shares are created in FileStorage storage accounts.

You cannot create Azure file shares from Blob storage accounts or premium general purpose (GPv1 or GPv2) storage accounts. Standard Azure file shares must be created in standard general purpose accounts only and premium Azure file shares must be created in FileStorage storage accounts only. Premium general purpose (GPv1 and GPv2) storage accounts are for premium page blobs only.

Box 2: Yes

Geo-redundant storage (GRS) brings additional redundancy to the data storage over both LRS or ZRS. Along with the three copies of your data stored within a single region, a further three copies are stored in the twinned Azure region. So using GRS means you get all the features of the LRS storage within your primary zone, but you also get a second LRS data storage in a neighbouring Azure region. This data is updated asynchronously, so there is a small lag between the 2 data sets, but for most cases this is acceptable.

Box 3: Yes

Blob Storage Standard can be used both LRS and GRS.

References:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-faq>

<https://www.skylinесacademy.com/blog/2019/7/31/azure-storage-replication>

<https://docs.microsoft.com/en-us/azure/storage/common/storage-introduction>

QUESTION 88

Hotspot Question

You create and save an Azure Resource Manager template named Template1 that includes the following four sections.

Section1.

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.0",
  "parameters": {
    "windowsOSVersion": {
      "defaultValue": "2019-Datacenter",
      "allowedValues": [
        "2012-Datacenter",
        "2012-R2-Datacenter",
        "2016-Datacenter",
        "2019-Datacenter"
      ],
      "type": "string"
    }
  },
}
```

Section2.

```
"variables": {
  "windowsOSVersion": "2012-Datacenter",
```

Section3.

```
},
"resources": [
  {
    "type": "Microsoft.Compute/virtualMachines",
```

Section4.

```
"storageProfile": {
    "imageReference": {
        "publisher": "MicrosoftWindowsServer",
        "offer": "WindowsServer",
        "sku": "2012-R2-Datacenter",
        "version": "latest"
    },
}
```

You deploy Template1.

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 Area

Statements	Yes	No
Windows Server 2012 R2 Datacenter will be deployed to the Azure virtual machine.	<input type="radio"/>	<input checked="" type="radio"/>
A custom image of Windows Server will be deployed.	<input checked="" type="radio"/>	<input type="radio"/>
During the deployment of Template1, an administrator will be prompted to select a version of Windows Server.	<input type="radio"/>	<input checked="" type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Windows Server 2012 R2 Datacenter will be deployed to the Azure virtual machine.	<input checked="" type="radio"/>	<input type="radio"/>
A custom image of Windows Server will be deployed.	<input type="radio"/>	<input checked="" type="radio"/>
During the deployment of Template1, an administrator will be prompted to select a version of Windows Server.	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 89

Hotspot Question

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Region
RG1	East US
RG2	West US

RG1 contains the virtual machines shown in the following table.

Name	Region
VM1	West US
VM2	West US
VM3	West US
VM4	West US

RG2 contains the virtual machines shown in the following table.

Name	Region
VM5	East US 2
VM6	East US 2
VM7	West US
VM8	West US 2

All the virtual machines are configured to use premium disks and are accessible from the Internet.

VM1 and VM2 are in an available set named AVSET1. VM3 and VM4 are in the same availability zone and are in an availability set named AVSET2. VM5 and VM6 are in different availability zones.

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 Area

Statements	Yes	No
VM1 is eligible for a Service Level Agreement (SLA) of 99,95 percent.	<input type="radio"/>	<input type="radio"/>
VM3 is eligible for a Service Level Agreement (SLA) of 99,99 percent.	<input type="radio"/>	<input type="radio"/>
VM5 is eligible for a Service Level Agreement (SLA) of 99,99 percent.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
VM1 is eligible for a Service Level Agreement (SLA) of 99,95 percent.	<input checked="" type="radio"/>	<input type="radio"/>
VM3 is eligible for a Service Level Agreement (SLA) of 99,99 percent.	<input type="radio"/>	<input checked="" type="radio"/>
VM5 is eligible for a Service Level Agreement (SLA) of 99,99 percent.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: Yes

VM1 and VM2 are in an available set named AVSET1.

For all Virtual Machines that have two or more instances deployed in the same Availability Set, we [Microsoft] guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.95% of the time.

Box 2: No

VM3 and VM4 are in the same availability zone and are in an availability set named AVSET2.

Box 3: Yes

VM5 and VM6 are in different availability zones.

For all Virtual Machines that have two or more instances deployed across two or more Availability Zones in the same Azure region, we [Microsoft] guarantee you will have Virtual Machine Connectivity to at least one instance at least 99.99% of the time.

References:

https://azure.microsoft.com/en-us/support/legal/sla/virtual-machines/v1_8/

QUESTION 90

Drag and Drop Question

You have an Azure virtual machine named VM1 that runs Windows Server 2016.

You install a line-to-business application on VM1.

You need to create an Azure virtual machine by using VM1 as a custom image.

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.

Actions	Answer Area
Run sysprep.exe on VM1.	
Install Network Load Balancing (NLB) on VM1.	
From Azure CLI, deallocate VM1 and mark VM1 as generalized.	↖ ↘
From Azure CLI, apply a custom script extension.	
Create a virtual machines scale set.	↖ ↘

Answer:

Actions	Answer Area
	Run sysprep.exe on VM1.
Install Network Load Balancing (NLB) on VM1.	
	From Azure CLI, deallocate VM1 and mark VM1 as generalized.
	↖ ↘
From Azure CLI, apply a custom script extension.	Create a virtual machines scale set.
	↖ ↘

Explanation:

Step 1: Run sysprep.exe on VM1.

If a template, or system image is used, System administrators must run the Sysprep tool to clear the SID information. The Sysprep tool is usually one of the last tasks performed by a system administrator when building a server image/template, that way each clone of the template will generalize a new unique SID for every server image copied from the template and will prepare the server for a first time boot.

The end result is a System template that functions as a new unique build every time it is deployed.

Step 2: From Azure CLI, deallocate VM1 and mark VM1 as generalized To create an image, the VM needs to be deallocated. Deallocate the VM with Stop-AzVm. Then, set the state of the VM as generalized with Set-AzVm so that the Azure platform knows the VM is ready for use a custom image

Step 3: Create a virtual machine scale set

Now create a scale set with New-AzVmss that uses the -ImageName parameter to define the custom VM image created in the previous step.

References:

<https://thesolving.com/server-room/when-and-how-to-use-sysprep/>

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/tutorial-use-custom-image->

powershell

QUESTION 91

Hotspot Question

You play to deploy an Azure virtual machine named VM1 by using an Azure Resource Manager template.

You need to complete the template.

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

NOTE: Each correct selection is worth one point.

Answer Area

```
{  
    "type": "Microsoft.Compute/virtualMachines",  
    "apiVersion": "2018-10-01",  
    "name": "VM1",  
    "location": "[parameters('location')]",  
    "dependsOn": [  
        "[resourceId('Microsoft.Storage/storageAccounts/', variables ('Name3'))]",  
        "[resourceId(  
            'Microsoft.Network/publicIPAddresses/',  
            'Microsoft.Network/virtualNetworks/  
            'Microsoft.Network/networkInterfaces/  
            'Microsoft.Network/virtualNetworks/subnets'  
            'Microsoft.Storage/storageAccounts/'  
,  
            variables('Name4'))]"  
    ],  
    "  
    "type": "Microsoft.Network/networkInterfaces",  
    "apiVersion": "2018-11-01",  
    "name": "NIC1",  
    "location": "[parameters('location')]",  
    "dependsOn": [  
        "[resourceId('Microsoft.Network/publicIPAddresses/', variables ('Name1'))]",  
        "[resourceId(  
            'Microsoft.Network/publicIPAddresses/  
            'Microsoft.Network/virtualNetworks/  
            'Microsoft.Network/networkInterfaces/  
            'Microsoft.Network/virtualNetworks/subnets'  
            'Microsoft.Storage/storageAccounts/'  
,  
            variables('Name2'))]"  
    ],  
}
```

Answer:

Answer Area

```
{  
    "type": "Microsoft.Compute/virtualMachines",  
    "apiVersion": "2018-10-01",  
    "name": "VM1",  
    "location": "[parameters('location')]",  
    "dependsOn": [  
        "[resourceId('Microsoft.Storage/storageAccounts/', variables ('Name3'))]",  
        "[resourceId(  
            'Microsoft.Network/publicIPAddresses/'  
            'Microsoft.Network/virtualNetworks/  
            'Microsoft.Network/networkInterfaces/  
            'Microsoft.Network/virtualNetworks/subnets'  
            'Microsoft.Storage/storageAccounts/'  
        ), variables('Name4'))]"  
    ],  
    {  
        "type": "Microsoft.Network/networkInterfaces",  
        "apiVersion": "2018-11-01",  
        "name": "NIC1",  
        "location": "[parameters('location')]",  
        "dependsOn": [  
            "[resourceId('Microsoft.Network/publicIPAddresses/', variables ('Name1'))]",  
            "[resourceId(  
                'Microsoft.Network/publicIPAddresses/'  
                'Microsoft.Network/virtualNetworks/  
                'Microsoft.Network/networkInterfaces/  
                'Microsoft.Network/virtualNetworks/subnets'  
                'Microsoft.Storage/storageAccounts/'  
            ), variables('Name2'))]"  
        ],  
    },  
}
```

Explanation:

Within your template, the dependsOn element enables you to define one resource as a dependent on one or more resources. Its value can be a comma-separated list of resource names.

Box 1: 'Microsoft.Network/networkInterfaces'

This resource is a virtual machine. It depends on two other resources:

Microsoft.Storage/storageAccounts
Microsoft.Network/networkInterfaces

Box 2: 'Microsoft.Network/virtualNetworks/'

The dependsOn element enables you to define one resource as a dependent on one or more resources.

The resource depends on two other resources:

Microsoft.Network/publicIPAddresses
Microsoft.Network/virtualNetworks

```
"resources": [
  {
    ...
  },
  {
    ...
  },
  {
    ...
  },
  {
    ...
  },
  {
    "type": "Microsoft.Network/networkInterfaces",
    "name": "[variables('nicName')]",
    "location": "[parameters('location')]",
    "apiVersion": "2018-08-01",
    "dependsOn": [
      "[resourceId('Microsoft.Network/publicIPAddresses/', variables('publicIPAddressName'))]",
      "[resourceId('Microsoft.Network/virtualNetworks/', variables('virtualNetworkName'))]"
    ],
    "properties": {
      "ipConfigurations": [
        {
          "name": "ipconfig1",
          "properties": {
            "privateIPAllocationMethod": "Dynamic",
            "publicIPAddress": {
              "id": "[resourceId('Microsoft.Network/publicIPAddresses',variables('publicIPAddressName'))]"
            },
            "subnet": {
              "id": "[variables('subnetRef')]"
            }
          }
        }
      ]
    }
  }
],
```

References:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-tutorial-create-templates-with-dependent-resources>

QUESTION 92

Hotspot Question

You plan to create a virtual machine as shown in the following exhibit.

Summary



Validation passed

Basics

Subscription	Microsoft Azure Sponsorship
Resource group	confcompute
Location	East US
Image	Windows Server 2016 Datacenter
Name	vm1
Username	labadmin
Password	*****

Virtual Machine Settings

Virtual machine size	Standard_DC2s
OS disk type	Premium SSD
Virtual network	vnet1
Subnet	subnet1
Subnet address prefix	10.0.0.0/24
Select public inbound ports	None
Boot diagnostics	Enabled
Diagnostic storage account	wmconf1a6f712e904

OK

Download template and parameters

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

The performance of the operating system disk [answer choice].

will decrease over time
will increase over time
is guaranteed to remain the same

Vm1 will use [answer choice] for data protection.

dm-crypt
secure enclaves
secure shell (SSH)

Answer:

Answer Area

The performance of the operating system disk [answer choice].

will decrease over time
will increase over time
is guaranteed to remain the same

Vm1 will use [answer choice] for data protection.

dm-crypt
secure enclaves
secure shell (SSH)

Explanation:

Box 1: is guaranteed to remain the same

OS disk type: Premium SSD

Premium SSD Managed Disks are high performance Solid State Drive (SSD) based Storage designed to support I/O intensive workloads with significantly high throughput and low latency. With Premium SSD Managed Disks, you can provision a persistent disk and configure its size and performance characteristics.

Box 2: secure enclaves

Virtual machine size: Standard_DC2s

DC-series virtual machines are a new family of VMs to protect the confidentiality and integrity of your data and code while it's processed in Azure through the use of secure enclaves.

Incorrect:

Not dm-crypt: Azure Disk Encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. It uses the BitLocker feature of Windows and the DM-Crypt feature of Linux to provide volume encryption for the OS and data disks of Azure virtual machines (VMs).

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-types>
<https://azure.microsoft.com/en-us/pricing/details/virtual-machines/series/>

QUESTION 93

Hotspot Question

You have an Azure Resource Manager template for a virtual machine named Template1. Template1 has the following parameters section.

```
"parameters": {  
    "adminUsername": {  
        "type": "string"  
    },  
    "adminPassword": {  
        "type": "securestring"  
    },  
    "dnsLabelPrefix": {  
        "type": "string"  
    },  
    "windowsOSVersion": {  
        "type": "string"  
        "defaultValue": "2016-Datacenter",  
        "allowedValues": [  
            "2016-Datacenter",  
            "2019-Datacenter"  
        ]  
    },  
    "location": {  
        "type": "String",  
        "allowedValues": [  
            "eastus",  
            "centralus",  
            "westus" ]  
    }  
},
```

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 Area

Statements	Yes	No
When you deploy Template1, you are prompted for a resource group.	<input type="radio"/>	<input type="radio"/>
When you deploy Template1, you are prompted for the Windows operating system version.	<input type="radio"/>	<input type="radio"/>
When you deploy Template1, you are prompted for a location.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
When you deploy Template1, you are prompted for a resource group.	<input checked="" type="radio"/>	<input type="radio"/>
When you deploy Template1, you are prompted for the Windows operating system version.	<input type="radio"/>	<input checked="" type="radio"/>
When you deploy Template1, you are prompted for a location.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: Yes

The Resource group is not specified.

Box 2: No

The default value for the operating system is Windows 2016 Datacenter.

Box 3: Yes

Location is no default value.

References:

<https://docs.microsoft.com/bs-latn-ba/azure/virtual-machines/windows/ps-template>

QUESTION 94

Hotspot Question

You network contains an Active Directory domain that is synced to Azure Active Directory (Azure AD) as shown in the following exhibit.

Microsoft Azure Active Directory Connect

Welcome Tasks Review your solution

Synchronized Directories	
DIRECTORY	ACCOUNT
Adatum.com	ADATUM.COM\MSOL_f14cd290d9f55
Synchronized Settings	
SOURCE ANCHOR	USER PRINCIPAL NAME
mS-DS-ConsistencyGuid	userPrincipalName
SYNC CRITERIA	FILTER OBJECTS TO SYNCHRONIZE BY GROUP
AlwaysProvision	Disabled
AZURE AD APP AND ATTRIBUTE FILTERING	DEVICE WRITEBACK
Disabled	Disabled
DIRECTORY EXTENSION ATTRIBUTE SYNC	EXCHANGE HYBRID DEPLOYMENT
Disabled	Disabled
GROUP WRITEBACK	PASSWORD HASH SYNCHRONIZATION
Disabled	Enabled
PASSWORD WRITEBACK	USER WRITEBACK
Disabled	Disabled
AUTO UPGRADE	EXCHANGE MAIL PUBLIC FOLDERS
Enabled	Disabled
SQL SERVER NAME (localdb)	SQL SERVER INSTANCE NAME .\\ADSync

Previous Exit

You have a user account configured as shown in the following exhibit. 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 Area

Statements	Yes	No
From the Azure portal, an administrator can reset the password of Adam Hobbs.	<input type="radio"/>	<input type="radio"/>
From the Azure portal, an administrator can modify the job title for the user account of Adam Hobbs.	<input type="radio"/>	<input type="radio"/>
From the Azure portal, an administrator can modify the usage location for the user account of Adam Hobbs.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
From the Azure portal, an administrator can reset the password of Adam Hobbs.	<input type="radio"/>	<input checked="" type="radio"/>
From the Azure portal, an administrator can modify the job title for the user account of Adam Hobbs.	<input type="radio"/>	<input checked="" type="radio"/>
From the Azure portal, an administrator can modify the usage location for the user account of Adam Hobbs.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No

Password writeback is disabled.

Note: Having a cloud-based password reset utility is great but most companies still have an on-premises directory where their users exist. How does Microsoft support keeping traditional on-premises Active Directory (AD) in sync with password changes in the cloud? Password writeback is a feature enabled with Azure AD Connect that allows password changes in the cloud to be written back to an existing on-premises directory in real time.

Box 2: No

Box 3: Yes

Yes, there is an Edit link for Location Info.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-sspr-writeback>

QUESTION 95

Hotspot Question

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2

The tenant contains computers that run Windows 10. The computers are configured as shown in the following table.

Name	Member of
Computer1	GroupA
Computer2	GroupA
Computer3	GroupB

You enable Enterprise State Roaming in contoso.com for Group1 and GroupA.

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 Area

Statements	Yes	No
If User1 modifies the desktop background of Computer1, User1 will see the changed background when signing in to Computer3.	<input type="radio"/>	<input type="radio"/>
If User2 modifies the desktop background of Computer1, User2 will see the changed background when signing in to Computer2.	<input type="radio"/>	<input type="radio"/>
If User1 modifies the desktop background of Computer3, User1 will see the changed background when signing in to Computer2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
If User1 modifies the desktop background of Computer1, User1 will see the changed background when signing in to Computer3.	<input checked="" type="radio"/>	<input type="radio"/>
If User2 modifies the desktop background of Computer1, User2 will see the changed background when signing in to Computer2.	<input type="radio"/>	<input checked="" type="radio"/>
If User1 modifies the desktop background of Computer3, User1 will see the changed background when signing in to Computer2.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Enterprise State Roaming provides users with a unified experience across their Windows devices and reduces the time needed for configuring a new device.

Box 1: Yes

Box 2: No

Box 3: Yes

References:

<https://docs.microsoft.com/en-us/azure/active-directory/devices/enterprise-state-roaming-overview>

QUESTION 96

Drag and Drop Question

You have virtual machines (VMs) that run a mission-critical application.

You need to ensure that the VMs never experience down time.

What should you recommend? To answer, drag the appropriate solutions to the correct scenarios. Each solution may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Solutions	Answer Area	
	Scenario	Solution
Fault Domain	Maintain application performance across identical VMs.	
Update Domain	Maintain application availability when an Azure datacenter fails.	
Availability Set		
Scale Sets	Maintain application performance across different VMs.	

Answer:

Solutions	Answer Area	
	Scenario	Solution
Update Domain	Maintain application performance across identical VMs.	Scale Sets
	Maintain application availability when an Azure datacenter fails.	Availability Set
	Maintain application performance across different VMs.	Fault Domain

Explanation:

Box 1: Scale set

A virtual machine scale set allows you to deploy and manage a set of identical, autoscaling virtual machines.

Box 2: Availability Set

An Availability Set is a logical grouping capability for isolating VM resources from each other when they're deployed. Azure makes sure that the VMs you place within an Availability Set run across multiple physical servers, compute racks, storage units, and network switches. If a hardware or software failure happens, only a subset of your VMs are impacted and your overall solution stays operational. Availability Sets are essential for building reliable cloud solutions.

Box 3: Fault domain

A fault domain is a logical group of underlying hardware that share a common power source and network switch, similar to a rack within an on-premises datacenter. As you create VMs within an availability set, the Azure platform automatically distributes your VMs across these fault domains.

This approach limits the impact of potential physical hardware failures, network outages, or power interruptions.

Incorrect Answers:

An update domain is a group of VMs and underlying physical hardware that can be rebooted at the same time.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-create-vmss>

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-availability-sets>

QUESTION 97

Hotspot Question

You have an Azure web app named App1 that has the following configurations:

- The app runs on three instances.
- The minimum number of instances is one.
- The maximum number of instances is five.

You create the following autoscale rules for App1:

- Decrease the instance count by one when the CPU percentage is less than 30.
- Decrease the instance count by one when the memory percentage is less than 50.
- Increase the instance count by one when the CPU percentage is greater than 80.
- Increase the instance count by one when the memory percentage is greater than 75.

You expect App1 to be utilized as shown in the following table.

Day	Hours	CPU	Memory
Monday to Friday	08:00 to 23:59	85%	40%
Monday to Friday	00:00 to 07:59	25%	60%
Saturday to Sunday	00:00 to 23:59	30%	55%

You need to identify the maximum number of instances that will be used by App1 during the expected periods of utilization.

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

NOTE: Each correct selection is worth one point.

Answer Area

Monday to Friday 00:00–07:59:

1
2
3
4
5

Monday to Friday 08:00–23:59:

1
2
3
4
5

Saturday to Sunday 00:00-23:59:

1
2
3
4
5

Answer:

Answer Area

Monday to Friday 00:00–07:59:

1
2
3
4
5

Monday to Friday 08:00–23:59:

1
2
3
4
5

Saturday to Sunday 00:00-23:59:

1
2
3
4
5

Explanation:

Reason: Scale out occur if ANY condition is met while scale in occur ONLY IF ALL condition are met.

So on Monday morning start with 3 instance and scale-out to 4 instance at night, as CPU is 85%. Then Tuesday morning 4 instance persist with NO Scale-in as CPU% is low BUT Memory% is OK; again by Tuesday night 5 instance is SCALED-OUT as CPU% is high. By Wednesday, we operate at 5 instance as we can neither scale-in or scale-out (due to hitting max-instance). Same persist even on Weekend as we cannot scale-in. So we hit max instance by Wednesday and stay there for perpetuity i.e. Box1-Box2-Box3 is 5-5-5.

QUESTION 98

Hotspot Question

From Azure Cosmos DB, you create the containers shown in the following table.

Container ID	Partition key	Unique key
Container1	/category	None
Container2	/id	/importance

You add the following item to Container1.

```
{
    "id": "1",
    "category": "personal",
    "name": "Name1",
    "description": "Description1"
}
```

You plan to add items to Azure Cosmos DB as shown in the following table.

Name	Content
Item1	{ "id": "1", "category": "personal", "name": "Name1", "description": "Description1" }
Item2	{ "category": "business", "name": "Name2", "description": "Description2", "importance": "High" }
Item3	{ "id": "3", "name": "Name3", "description": "Description3" }
Item4	{ "id": "4", "importance": "Low" }

You need to identify which items can be added successfully to Container1 and Container2.

What should you identify for each container? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Container1:

Item2 only
Item1 and Item2 only
Item3 and Item4 only
Item2, Item3, and Item4 only
Item1, Item2, Item3, and Item4

Container2:

Item4 only
Item2 and Item4 only
Item1, Item3, and Item4 only
Item1, Item2, Item3, and Item4

Answer:

Answer Area

Container1:

Item2 only
Item1 and Item2 only
Item3 and Item4 only
Item2, Item3, and Item4 only
Item1, Item2, Item3, and Item4

Container2:

Item4 only
Item2 and Item4 only
Item1, Item3, and Item4 only
Item1, Item2, Item3, and Item4

Explanation:

“id” is special property which must be unique. That’s why for container 1, item 1 cannot be created again.

If “id” not exists, azure will generate a unique string automatically, so item 2 can be created without “id”.

Unique key is bound to the partition, and it does not necessarily exists. Thus, all items can be created in container 2.

QUESTION 99

Your company has an office in Seattle.

You have an Azure subscription that contains a virtual network named VNET1. You create a site-to-site VPN between the Seattle office and VNET1.

VNET1 contains the subnets shown in the following table.

Name	IP address space
Subnet1	10.1.1.0/24
GatewaySubnet	10.1.200.0/28

You need to redirect all Internet-bound traffic from Subnet1 to the Seattle office.

What should you create?

- A. a route for GatewaySubnet that uses the virtual network gateway as the next hop
- B. a route for GatewaySubnet that uses the local network gateway as the next hop
- C. a route for Subnet1 that uses the local network gateway as the next hop
- D. a route for Subnet1 that uses the virtual network gateway as the next hop

Answer: D

Explanation:

A route with the 0.0.0.0/0 address prefix instructs Azure how to route traffic destined for an IP address that is not within the address prefix of any other route in a subnet's route table. When a subnet is created, Azure creates a default route to the 0.0.0.0/0 address prefix, with the Internet next hop type. We need to create a custom route in Azure to use a virtual network gateway in the Seattle office as the next hop.

References:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

QUESTION 100

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Address space
VNET1	Virtual network	10.1.1.0/24
Subnet1	Subnet	10.1.1.0/24
VM1	Virtual machine	Not applicable

Subnet1 is on VNET1. VM1 connects to Subnet1.

You plan to create a virtual network gateway on VNET1.

You need to prepare the environment for the planned virtual network gateway.

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

NOTE: Each correct selection is worth one point.

- A. Modify the address space used by VNET1.
- B. Modify the address space used by Subnet1.
- C. Create a subnet named GatewaySubnet on VNET1.
- D. Create a local network gateway.
- E. Delete Subnet1.

Answer: AE

QUESTION 101

You have an Azure subscription that contains the resource groups shown in the following table.

Name	Region
RG1	West US
RG2	West US
RG3	East US

You have the Azure SQL servers shown in the following table.

Name	Region	In resource group
Sql1	West US	RG1
Sql2	East US	RG2
Sql3	West US	RG3
Sql4	West US	RG1

You create an Azure SQL database named DB1 on Sql1 in an elastic pool named Poo11. You need to create an Azure SQL database named DB2 in Poo11.

Where should you deploy DB2?

- A. Sql1
- B. Sql2
- C. Sql3
- D. Sql4

Answer: A

Explanation:

The databases in an elastic pool are on a single Azure SQL Database server and share a set number of resources at a set price.

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-elastic-pool>

QUESTION 102

Your company is developing an e-commerce Azure App Service Web App to support hundreds of restaurant locations around the world.

You are designing the messaging solution architecture to support the e-commerce transactions and messages. The e-commerce application has the following features and requirements:

Feature	Requirement
Shopping Cart	<ul style="list-style-type: none">Items in a shopping cart must be processed by an Azure Function within a specified number of minutes. Failure to process should move the items to a failed state for processing by a separate Azure FunctionShopping cart transactions must not be lost and fault conditions must be processed separatelyShopping cart transactions must be read by the inventory and sales systems for further processing
Inventory Distribution	<ul style="list-style-type: none">Items sent to the inventory system must run a separate workflow for each item that includes warehouse, shipping, and order processing updatesInventory uses Azure Blob storage to store inventory items and related informationInventory is processed by using an Azure Logic App
Restaurant Telemetry	<ul style="list-style-type: none">Restaurants stream millions of daily events from all locationsRestaurant data should be captured in Azure Blob storage for conditional processingRestaurant event data should expire after 24 hours

You need to choose the Azure messaging solution to support the Shopping Cart feature.

Which Azure service should you use?

- A. Azure Service Bus
- B. Azure Relay
- C. Azure Event Grid
- D. Azure Event Hub

Answer: A

Explanation:

Microsoft Azure Service Bus is a fully managed enterprise integration message broker. Service Bus is most commonly used to decouple applications and services from each other, and is a reliable and secure platform for asynchronous data and state transfer.

One common messaging scenario is Messaging: transfer business data, such as sales or purchase orders, journals, or inventory movements.

Incorrect Answers:

B: The Azure Relay service enables you to securely expose services that run in your corporate network to the public cloud.

References:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messaging-overview>

QUESTION 103

Drag and Drop Question

You have an Azure virtual machine named VM1 that runs Windows Server 2016.

You install a line-of-business application on VM1.

You need to create a scale set by using VM1 as a custom image.

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.

Actions	Answer Area
From Azure CLI, apply a custom script extension.	
Run <code>sysprep.exe</code> on VM1.	
From Azure CLI, deallocate VM1 and mark VM1 as generalized.	 
Install Network Load Balancing (NLB) on VM1.	
Create a virtual machine scale set.	

Answer:

Actions	Answer Area
From Azure CLI, apply a custom script extension.	Run <code>sysprep.exe</code> on VM1.
From Azure CLI, deallocate VM1 and mark VM1 as generalized.	
Create a virtual machine scale set.	 
Install Network Load Balancing (NLB) on VM1.	

Explanation:

Step 1: Run `sysprep.exe` on VM1.

The final step to prepare your VM for use as a custom image is to generalize the VM. Sysprep removes all your personal account information and configurations, and resets the VM to a clean state for future deployments.

Step 2: From Azure CLI, deallocate VM1 and mark VM1 as generalized. To create an image, the VM needs to be deallocated. Deallocate the VM with `Stop-AzVm`. Then, set the state of the VM as generalized with `Set-AzVm` so that the Azure platform knows the VM is ready for use as a custom image. You can only create an image from a generalized VM. It may take a few minutes to deallocate and generalize the VM. Then create an image of the VM with `New-AzImageConfig` and `New-AzImage`.

Step 3: Create a virtual machine scale set.

Create a scale set with New-AzVmss that uses the -ImageName parameter to define the custom VM image created in the previous step.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/tutorial-use-custom-image-powershell>

QUESTION 104

Hotspot Question

Your company has an Azure Container Registry named Registry1.

You have an Azure virtual machine named Server1 that runs Windows Server 2019.

From Server1, you create a container image named image1.

You need to add image1 to Registry1.

Which command should you run on Server1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

push	/image1
<ul style="list-style-type: none">dockerAzCopyRobocopyesentutl	<ul style="list-style-type: none">registry1.azurecr.ioregistry1.onmicrosoft.comhttps://registry1.onmicrosoft.com\\\registry1.blob.core.windows.net

Answer:

Answer Area

push	/image1
<ul style="list-style-type: none">dockerAzCopyRobocopyesentutl	<ul style="list-style-type: none">registry1.azurecr.ioregistry1.onmicrosoft.comhttps://registry1.onmicrosoft.com\\\registry1.blob.core.windows.net

Explanation:

An Azure container registry stores and manages private Docker container images, similar to the way Docker Hub stores public Docker images. You can use the Docker command-line interface (Docker CLI) for login, push, pull, and other operations on your container registry.

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-get-started-docker-cli>
<https://docs.docker.com/engine/reference/commandline/push/>

QUESTION 105

Hotspot Question

You have an Azure subscription that contains the Azure SQL servers shown in the following table.

Name	Region	In resource group
Sql1	West US	RG1
Sql2	West US	RG1

The subscription contains the elastic pools shown in the following table.

Name	On Azure SQL server
Pool1	Sql1
Pool2	Sql1
Pool3	Sql2

The subscription contains the Azure SQL databases shown in the following table.

Name	On Azure SQL server	Pool
DB1	Sql1	Pool1
DB2	Sql1	Pool2
DB3	Sql1	None

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 Area

Statements	Yes	No
DB1 can be removed from Pool1 and added to Pool2	<input type="radio"/>	<input type="radio"/>
DB2 can be removed from Pool2 and added to Pool3	<input type="radio"/>	<input type="radio"/>
DB3 can be added to Pool1	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
DB1 can be removed from Pool1 and added to Pool2	<input checked="" type="radio"/>	<input type="radio"/>
DB2 can be removed from Pool2 and added to Pool3	<input type="radio"/>	<input checked="" type="radio"/>
DB3 can be added to Pool1	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: Yes

Since the databases are on the same sever and the elastic pools are also on the same server, the databases can be removed from one pool and then added to another pool.

Box 2: No

Since the elastic pool is present on another server, we can't add the database to this pool.

Box 3: Yes

Since both the database and the elastic pool are on the same server , we can add the database to the pool.

QUESTION 106

Hotspot Question

You have an Azure web app named App1 that contains the following autoscale conditions: The default auto created scale condition has a scale mode that has Scale to a specific instance count set to 2.

Scale condition 1 has the following configurations:

- Scale mode: Scale to a specific instance count
- Instance count: 3
- Schedule: Specify start/end dates
- Start date: August 1, 2019, 06:00
- End date: September 1, 2019, 18:00

Scale condition 2 has the following configurations:

- Scale mode: Scale to a specific instance count
- Instance count: 4
- Schedule: Repeat specific days
- Repeat every: Monday
- Start time: 06:00
- End time: 18:00

Scale condition 3 has the following configurations:

- Scale mode: Scale to a specific instance count
- Instance count: 5
- Schedule: Repeat specific days
- Repeat every: Monday
- Start time: 15:00
- End time: 20:00

You need to identify the number of running App1 instances. What should you identify? To

answer, select the appropriate options in the answer area.

Answer Area

Number of App1 instances that run on Monday, August 5, 2019, at 17:00:

2
3
4
5

Number of App1 instances that run on Monday, August 3, 2020, at 16:00:

2
3
4
5

Answer:

Answer Area

Number of App1 instances that run on Monday, August 5, 2019, at 17:00:

2
3
4
5

Number of App1 instances that run on Monday, August 3, 2020, at 16:00:

2
3
4
5

Explanation:

Box 1: 5

Scale condition 1, Scale condition 2, and Scale condition 3 applies. Scale condition 3 takes precedence as it the largest increase in the number of instances.

Box 2: 5

Scale condition 1 does not apply as its end date is exceeded.

Scale condition 2 and Scale condition 3 applies.

Scale condition 3 takes precedence as it the largest increase in the number of instances.

When you configure multiple policies and rules, they could conflict with each other. Autoscale uses the following conflict resolution rules to ensure that there is always a sufficient number of instances running:

Scale-out operations always take precedence over scale-in operations.

When scale-out operations conflict, the rule that initiates the largest increase in the number of instances takes precedence.

When scale in operations conflict, the rule that initiates the smallest decrease in the number of

instances takes precedence.

References:

<https://docs.microsoft.com/en-us/azure/architecture/best-practices/auto-scaling>

QUESTION 107

Hotspot Question

You have an Azure web app named App1 that contains the following autoscale conditions:

The screenshot shows the Azure Auto Scale configuration interface. It includes sections for 'Scale out' rules and 'Scale in' rules, instance limits, schedule, timezone, start time, and end time.

Rules

Scale out

When	(Average) CpuPercentage	>=	50	Action	
When	ASP-RG5-b4a5	(Average) CpuPercentage	>=	50	Increase count by 1
Or	ASP-RG5-b4a5	(Average) CpuPercentage	>=	60	Increase count by 2
Or	ASP-RG5-b4a5	(Average) CpuPercentage	>=	70	Increase count by 3

Scale in

When	(Average) CpuPercentage	<=	30	Action	
When	ASP-RG5-b4a5	(Average) CpuPercentage	<=	30	Decrease count by 1

Add a rule

Instance limits

Minimum	2	Maximum	6	Default	4
---------	---	---------	---	---------	---

Schedule

Specify start/end dates Repeat specific days

Repeat every

Monday Tuesday Wednesday Thursday Friday
 Saturday Sunday

Timezone (UTC-01:00) Amsterdam, Berlin...

Start time 06:00

End time 18:00

Every autoscale condition rule is configured to have a duration of 20 minutes and a cool down time of 10 minutes.

At 06:00, WebApp1 is running four instances.

You need to identify how many instances are running on WebApp1 based on the percentage of the CPU utilization.

How many instances should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

If the WebApp1 CPU utilization is 10 percent at 06:00, at 06:25 WebApp1 will have:

4 instances
3 instances
2 instances
1 instance

If the WebApp1 CPU utilization is 70 percent at 06:00, at 06:25 WebApp1 will have:

4 instances
5 instances
6 instances
7 instances

Answer:

Answer Area

If the WebApp1 CPU utilization is 10 percent at 06:00, at 06:25 WebApp1 will have:

4 instances
3 instances
2 instances
1 instance

If the WebApp1 CPU utilization is 70 percent at 06:00, at 06:25 WebApp1 will have:

4 instances
5 instances
6 instances
7 instances

Explanation:

Box 1: 3

At 6:00 the default 4 instances are running. The CPU utilization averages 10% for 25 minutes. The scale in rules states that 1 instance should be removed when CPU utilization averages 30%

or less over a 20 minute period.

Box 2: 6

At 6:00 the default 4 instances are running. The CPU utilization averages 70% for 25 minutes. The scale out rules states that 3 instances should be added when CPU utilization averages 70% or more over a 20 minute period. However, the maximum number of instances is set at 6.

References:

<https://docs.microsoft.com/en-us/azure/architecture/best-practices/auto-scaling>

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-understanding-settings>

QUESTION 108

Note: This question is part of 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 an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other Identity Governance settings are available.

Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.

You need to ensure that Admin1 can create access reviews in contoso.com.

Solution: You create an access package.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

You do not use access packages for Identity Governance. Instead use Azure AD Privileged Identity Management.

Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:

Conduct access reviews to ensure users still need roles References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview>

QUESTION 109

Note: This question is part of 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 an Azure Active Directory (Azure AD) tenant named contoso.com.

A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other Identity Governance settings are available.

Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.

You need to ensure that Admin1 can create access reviews in contoso.com.

Solution: You assign the Service administrator role to Admin1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead use Azure AD Privileged Identity Management.

Note: PIM essentially helps you manage the who, what, when, where, and why for resources that you care about. Key features of PIM include:

Conduct access reviews to ensure users still need roles

References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

QUESTION 110

Drag and Drop Question

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Region	Resource group
RG1	Resource group	Central US	<i>Not applicable</i>
RG2	Resource group	West US	<i>Not applicable</i>
VM1	Virtual machine	East US	RG2
VNET1	Virtual network	East US	RG1

In RG2, you need to create a new virtual machine named VM2 that will connect to VNET1. VM2 will use a network interface named VM2_Interface.

In which region should you create VM2 and VM2_Interface? To answer, drag the appropriate regions to the correct targets. Each region may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Regions

Central US
East US
West US

Answer Area

VM2:

VM2_Interface:

--

Answer:**Regions**

Central US

Answer Area

VM2:

West US

VM2_Interface:

East US

Explanation:

VM2: West US

In RG2, which is in West US, you need to create a new virtual machine named VM2.

VM2_interface: East US

VM2 will use a network interface named VM2_Interface to connect to VNET1, which is in East US.

References:

<https://docs.microsoft.com/en-us/azure/virtual-network/associate-public-ip-address-vm>**QUESTION 111**

You have an Azure subscription that contains the web apps shown in the following table.

Name	Runtime stack
WebApp1	Java SE
WebApp2	Ruby 2.6
WebApp3	Python 3.7
WebApp4	ASP.NET V4.7

For which web app can you configure a WebJob?

- A. WebApp4
- B. WebApp3
- C. WebApp1
- D. WebApp2

Answer: A

Explanation:

Publishing a .NET Core WebJob to App Service from Visual Studio uses the same tooling as publishing an ASP.NET Core app.

References:

<https://docs.microsoft.com/en-us/azure/app-service/webjobs-dotnet-deploy-vs>

QUESTION 112

You create a container image named Image1 on a developer workstation.

You plan to create an Azure Web App for Containers named WebAppContainer that will use Image1.

You need to upload Image1 to Azure. The solution must ensure that WebAppContainer can use Image1.

To which storage type should you upload Image1?

- A. Azure Container Registry
- B. an Azure Storage account that contains a blob container
- C. an Azure Storage account that contains a file share
- D. Azure Container Instances

Answer: A

Explanation:

Configure registry credentials in web app.

App Service needs information about your registry and image to pull the private image. In the Azure portal, go to Container settings from the web app and update the Image source, Registry and save.

References:

<https://docs.microsoft.com/en-us/azure/devops/pipelines/targets/webapp-on-container-linux>

QUESTION 113

A company's development team is currently developing a Docker/Go based application. The application needs to be deployed to the Azure Web App service using containers on the Linux

platform.

Currently there are no resource groups in place in the company's Azure account that supports the Linux platform.

You must advise on the necessary and minimum number of steps to provide the ability to host the application in the company's Azure account.

Which of the following Azure CLI commands would you recommend implementing for this requirement? (Choose three)

- A. az group update
- B. az webapp update
- C. az group create
- D. az appservice plan create
- E. az webapp create

Answer: CDE

Explanation:

<https://docs.microsoft.com/en-us/azure/app-service/containers/quickstart-docker-go>

QUESTION 114

A company has an on-premise setup and a setup defined in Azure. They have gone ahead and created an Azure Logic App named lead2pass-app. They need this app to query an on-premise SQL database server.

Which of the following steps need to be performed to fulfil this requirement? (Choose three)

- A. Create a Virtual Machine in Azure
- B. Install the On-premise data gateway on the Azure Virtual Machine
- C. From the Azure portal, create an on-premise data gateway
- D. On a computer in the on-premise network, install an on-premise data gateway
- E. From the Logic App Designer, add a connector

Answer: CDE

Explanation:

<https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-gateway-connection>

QUESTION 115

Your company needs to migrate a Virtual Machine, lead2pass-vm, hosted in Amazon Web Services to Azure using Azure Site Recovery. The following resources have been created for the implementation

- A Virtual Network in Azure
- A Replication Policy
- A Recovery Services vault
- An Azure storage account

Which of the following steps would you carry out for the migration? (Choose three)

- A. Install Azure Site Recovery Unified Setup
- B. Enable Windows Powershell remoting on whizlabs-vm
- C. Enable replication for whizlabs-vm
- D. Create an Azure Migrate project
- E. Deploy another server in Amazon Web Services as the configuration server

Answer: ACE

Explanation:

<https://docs.microsoft.com/en-us/azure/site-recovery/migrate-tutorial-aws-azure>

QUESTION 116

A company wants to sync their on-premise AD with Azure AD. They have setup Azure AD connect and configured the setup for Password hash synchronization, Single Sign-On and staging mode is also enabled. After an initial review it can be seen that the Synchronization Service Manager is not displaying any sync jobs.

Which of the following step would need to be carried out to resolve this issue?

- A. Be sure to configure, Azure AD for Pass-through Authentication
- B. Run a full import using the Service Manager
- C. From Azure AD Connect, ensure to disable staging mode
- D. Run a full import from the local on-premise AD

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-staging-server>

QUESTION 117

A company has an on-premise network. They want to setup a site-to-site VPN connection with an Azure Virtual Network named lead2pass-net. The Virtual Network has an address space of 10.0.0.0/16. It also has a subnet with an address space 10.0.0.0/24.

Which of the following steps would you implement for the Site to Site VPN connection? (Choose 4)

- A. Create a gateway subnet
- B. Create a new DNS domain
- C. Create a local gateway
- D. Create a data gateway
- E. Create a VPN gateway
- F. Create a VPN connection

Answer: ACEF

Explanation:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

QUESTION 118

A company has a number of VMWare Virtual Machines that need to be migrated onto Azure. You first have to discover and assess the virtual machines for the migration.

Which of the following steps would you implement for this requirement? (Choose 4)

- A. From the Azure Portal, download the OVA file
- B. Create a collector virtual Machine
- C. From the Azure Portal, download the Azure Site Recovery agent
- D. Configure the collector to start the discovery

- E. Create an assessment
- F. Create a backup policy

Answer: ABDE

Explanation:

<https://docs.microsoft.com/en-us/azure/migrate/tutorial-assessment-vmware>

QUESTION 119

A company is developing an ecommerce web application. One of the modules of the application will be built using a messaging solution architecture. The modules will have the following features

- A Workflow run for several items published on the web application.
- The Workflow would be built using Azure Logic Apps.
- The item data would be stored in Azure BLOB storage.

Which of the following would you additionally incorporate for the module?

- A. Azure Event Grid
- B. Azure Event Hub
- C. Azure HDInsight
- D. Azure Service Bus

Answer: D

Explanation:

Option A is incorrect since this is normally used for event processing.

Option B is incorrect since this is a big data ingestion service.

Option C is incorrect since this is an analytics service.

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-messaging-overview>

QUESTION 120

A company has a set of 10 Virtual Machines created in their Azure subscription.

There is a requirement to ensure that an IT administrator gets an email whenever the following operations are performed on the Virtual Machine

- Restart of the machine
- Whenever the machine is deallocated
- Whenever the machine is powered off

You need to decide on the minimum number of rules and actions groups required in Azure Monitor for this requirement. (Choose two)

- A. Three rules
- B. One rule
- C. One action group
- D. Three action groups

Answer: AC

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview>

QUESTION 121

A company is preparing their Azure environment for the backup of their Azure Virtual Machines. They need to ensure the following when it comes to the backup of the Virtual Machines:

- The Virtual machines need to be backed up daily at 03:00 UTC time
- The backups should be retained for a period of 90 days

Which of the following should you configure in Azure Recovery Services vault?

- A. Backup Policy
- B. Backup Schedule
- C. Backup Logs
- D. Backup Infrastructure

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/backup/backup-introduction-to-azure-backup>

QUESTION 122

A company has a web application named lead2pass-app deployed to Azure. The Web App is deployed using the Azure App Service based on the D1 pricing tier. The application is now being modified and needs to accept connections on HTTPS. Which of the following needs to be done to ensure this requirement can be fulfilled? You have to ensure that the cost is minimized for any changes made.

- A. Scale out the App Service Plan
- B. Scale up the App Service Plan
- C. Change the properties of the Web App
- D. Change the Quota of the Web App

Answer: B

Explanation:

Option A is incorrect since this option is used for Autoscaling purpose.

Options C and D are incorrect since these are read-only features.

<https://azure.microsoft.com/en-us/pricing/details/app-service/plans/>

QUESTION 123

A company is planning on deploying a storage account which will be used to host files shares. These file shares will be used by a number of Virtual Machines hosted in Azure. There is a requirement to ensure the highest possible redundancy for the files that would be stored in the storage account. Which of the following replication technique would you "NOT" employ for the storage account?

- A. Locally redundant storage (LRS)
- B. Zone-redundant storage (ZRS)
- C. Geo-redundant storage (GRS)
- D. Read-access geo-redundant storage (RA-GRS)

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-planning#file-share-redundancy>

QUESTION 124

A development team has been instructed to implement a simple solution in Azure. The primary requirement is to ensure that an IT administrator team is notified whenever any infrastructure level changes are made to a virtual machine defined in their Azure subscription.

Which of the following steps can be used to implement this solution? (Choose two)

- A. Create a workflow using the Azure Logic App service
- B. Create a workflow using the Azure Event Grid service
- C. Use the Event Grid service to check for Virtual Machine level changes
- D. Use the Event Hub service to check for Virtual Machine level changes

Answer: AC

Explanation:

Option B is incorrect since workflows should be defined in the Azure Logic App service.

Option D is incorrect since the Event Hub service is NOT used to check for resource level changes.

<https://docs.microsoft.com/en-us/azure/event-grid/monitor-virtual-machine-changes-event-grid-logic-app>

QUESTION 125

Drag and Drop Question

You are the IT administrator for an Azure subscription that contains 20 virtual machines (VMs). You need to write a Log Analytics query to determine which VMs have not been responsive within the past hour.

How should you complete the query? To answer, drag the appropriate query elements to their correct locations in the answer area. A query element may be used once, more than once, or not at all.

|

 > < Perf where ago(1h) Heartbeat TimeGenerated

Answer:



Explanation:

You should use the following query:

Heartbeat | where TimeGenerated > ago(1h)

This query finds all computers that have had a heartbeat within the past hour. Computers send a heartbeat to let Azure know that they are responsive. The ago(1h) means the timestamp is one hour ago. If TimeGenerated is greater than that timestamp, the heartbeat occurred within the past hour.

You should not use Perf as a source. This source looks at performance counters. In this scenario, you need to search the Heartbeat source, not performance counters.

You should not use the following query:

Heartbeat | where TimeGenerated < ago(1h)

This query finds all computers that have sent a heartbeat before one hour ago.

QUESTION 126

Drag and Drop Question

An Azure key vault named measureup exists in your company's cloud subscription. You want to store a password in the key vault. The password is S3449PT!@90Q.

The name of the entry should be ApplicationPassword. The password should not be stored as plain text.

You need to use PowerShell to store the password in the key vault.

How should you complete the cm diets? To answer, drag the cm diets to the appropriate locations in the answer area. A cmdlet may be used once, more than once, or not at all.

```
$value = [REDACTED] 'S3449PT!@90Q'
- [REDACTED] -Force

[REDACTED] -VaultName 'measureup' -Name 'ApplicationPassword'
- [REDACTED] $value
```



Answer:

```

$value = ConvertTo-SecureString 'S3449PT!@90Q'
    -AsPlainText -Force

Set-AzureKeyVaultSecret -VaultName 'measureup' -Name 'ApplicationPassword'
    -SecretValue $value

```



Explanation:

You should use the following cmdlets:

```

$value = ConvertTo-SecureString 'S3449PT!@90Q' -AsPlainText -Force
Set-AzureKeyVaultSecret -VaultName 'measureup' -Name 'ApplicationPassword' -SecretValue $value

```

The `ConvertTo-SecureString` cmdlet converts a plain text value into a secure (encrypted) string. This meets the requirement of the password not being stored as plain text. The first parameter to this cmdlet is the string to convert. The `-AsPlainText` parameter indicates that the string to convert is plain text. The `-Force` parameter must be used when `-AsPlainText` is used to verify that you understand the implications of using `-AsPlainText`.

The `Set-AzureKeyVaultSecret` cmdlet stores the password in the key vault with the name specified as the `-Name` parameter. The `-SecretValue` parameter specifies the secret. In this scenario, the secret is the encrypted password.

You should not use `Add-AzureKeyVaultKey`. This cmdlet generates a software or hardware key and saves it in a key vault. In this scenario, you need to store a known secret, not generate a key.

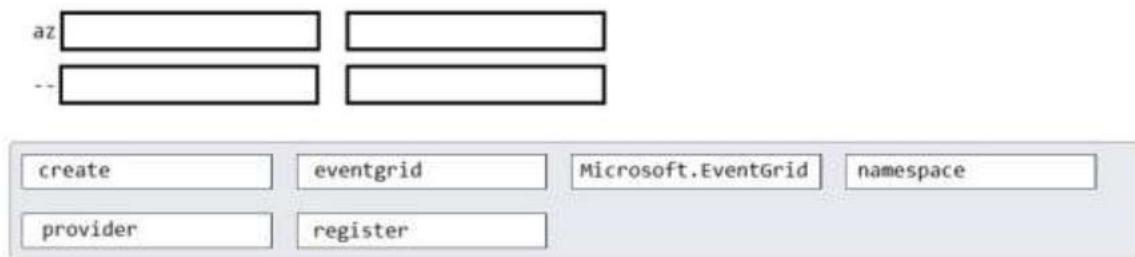
QUESTION 127

Drag and Drop Question

You are the cloud administrator for your company. You want to take advantage of Event Grid so that Service Bus and blob storage events are captured.

You need to use Azure CLI to enable your Azure subscription to send events to Event Grid.

How should you write the command? To answer, drag the appropriate command segment to each location. A command segment may be used once, more than once, or not at all.



Answer:



Explanation:

You should use the following command:

```
az provider register --namespace Microsoft.EventGrid
```

This command registers the Event Grid resource provider. This allows your subscription to send events to Event Grid.

You should not use the eventgrid or create command segments. These two segments allow you to create an Event Grid subscription to either a custom topic or to a resource.

QUESTION 128

You pull a Dockerfile from an online repository. You build a container image from this file, and you want to add it to an Azure Container Registry named mytestreg. The name of image is my-test-app.

You need to deploy the image to the registry.

Which command should you run from your developer computer?

- A. az container create -name mytestreg -image my-test-app
- B. az acr create -name mytestreg\my-test-app
- C. docker push mytestreg.azurecr.io/my-test-app
- D. docker run -p mytestreg my-test-app

Answer: C

Explanation:

You should use the following command: docker push mytestreg.azurecr.io/my-test-app

This command pushes the image named my-test-app to an Azure login server named mytestreg.azurecr.io. You should not use the following command: docker run -p mytestreg my-test-app

This command runs a container locally. In this scenario, you need to deploy the container image. You should not use the following command: az acr create --name mytestreg\my-test-app The az acr create command creates an Azure Container Registry.

You should not use the following command:

```
az container create --name mytestreg --image my-test-app
```

The az container create command creates a container instance in Azure.

QUESTION 129

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.
- Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- Designate a new user named Admin1 as the service admin for the Azure subscription.
- Admin1 must receive email alerts regarding service outages.
- Ensure that a new user named User3 can create network objects for the Azure subscription.

You need to meet the user requirement for Admin1.

What should you do?

- A. From the Subscriptions blade, select the subscription, and then modify the Properties.
- B. From the Subscriptions blade, select the subscription, and then modify the Access control (IAM) settings.
- C. From the Azure Active Directory blade, modify the Properties.
- D. From the Azure Active Directory blade, modify the Groups.

Answer: A

Explanation:

Change the Service administrator for an Azure subscription

- Sign in to Account Center as the Account administrator.
- Select a subscription.
- On the right side, select Edit subscription details.

Scenario: Designate a new user named Admin1 as the service administrator of the Azure subscription.

References:

<https://docs.microsoft.com/en-us/azure/billing/billing-add-change-azure-subscription-administrator>

QUESTION 130**Case Study 1 - Contoso, Ltd****Overview**

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements**Planned Changes**

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.

- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.
- Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- Designate a new user named Admin1 as the service admin for the Azure subscription.
- Admin1 must receive email alerts regarding service outages.
- Ensure that a new user named User3 can create network objects for the Azure subscription.

You need to recommend an identify solution that meets the technical requirements.

What should you recommend?

- federated single-on (SSO) and Active Directory Federation Services (AD FS)
- password hash synchronization and single sign-on (SSO)
- cloud-only user accounts
- Pass-through Authentication and single sign-on (SSO)

Answer: D

Explanation:

With Pass-through Authentication the on-premises passwords are never stored in the cloud in any form.

Scenario:

Prevent user passwords or hashes of passwords from being stored in Azure.

Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

Minimize administrative effort whenever possible.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ptc>

QUESTION 131

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end

- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.
- Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- Designate a new user named Admin1 as the service admin for the Azure subscription.
- Admin1 must receive email alerts regarding service outages.
- Ensure that a new user named User3 can create network objects for the Azure subscription.

You are planning the move of App1 to Azure.

You create a network security group (NSG).

You need to recommend a solution to provide users with access to App1.

What should you recommend?

- A. Create an outgoing security rule for port 443 from the Internet.
Associate the NSG to all the subnets.
- B. Create an incoming security rule for port 443 from the Internet.
Associate the NSG to all the subnets.
- C. Create an incoming security rule for port 443 from the Internet.
Associate the NSG to the subnet that contains the web servers.
- D. Create an outgoing security rule for port 443 from the Internet.
Associate the NSG to the subnet that contains the web servers.

Answer: C

Explanation:

As App1 is public-facing we need an incoming security rule, related to the access of the web servers.

Scenario: You have a public-facing application named App1. App1 is comprised of the following three tiers: a SQL database, a web front end, and a processing middle tier. Each tier is comprised

of five virtual machines. Users access the web front end by using HTTPS only.

QUESTION 132

Case Study 1 - Contoso, Ltd

Overview

Contoso, Ltd. is a manufacturing company that has offices worldwide. Contoso works with partner organizations to bring products to market.

Contoso products are manufactured by using blueprint files that the company authors and maintains.

Existing Environment

Currently, Contoso uses multiple types of servers for business operations, including the following:

- File servers
- Domain controllers
- Microsoft SQL Server servers

Your network contains an Active Directory forest named contoso.com. All servers and client computers are joined to Active Directory.

You have a public-facing application named App1. App1 is comprised of the following three tiers:

- A SQL database
- A web front end
- A processing middle tier

Each tier is comprised of five virtual machines. Users access the web front end by using HTTPS only.

Requirements

Planned Changes

Contoso plans to implement the following changes to the infrastructure:

- Move all the tiers of App1 to Azure.
- Move the existing product blueprint files to Azure Blob storage.
- Create a hybrid directory to support an upcoming Microsoft Office 365 migration project.

Technical Requirements

Contoso must meet the following technical requirements:

- Move all the virtual machines for App1 to Azure.
- Minimize the number of open ports between the App1 tiers.
- Ensure that all the virtual machines for App1 are protected by backups.
- Copy the blueprint files to Azure over the Internet.
- Ensure that the blueprint files are stored in the archive storage tier.
- Prevent user passwords or hashes of passwords from being stored in Azure.
- Use unmanaged standard storage for the hard disks of the virtual machines.
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.
- Minimize administrative effort whenever possible.

User Requirements

Contoso identifies the following requirements for users:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD.
- Designate a new user named Admin1 as the service admin for the Azure subscription.

- Admin1 must receive email alerts regarding service outages.
- Ensure that a new user named User3 can create network objects for the Azure subscription.

Hotspot Question

You need to configure the Device settings to meet the technical requirements and the user requirements.

Which two settings should you modify? To answer, select the appropriate settings in the answer area.

Answer Area

Save Discard

Users may join devices to Azure AD ⓘ All Selected None

Selected
No member selected

Additional local administrators on Azure AD joined devices ⓘ Selected None

Selected
No member selected

Users may register their devices with Azure AD ⓘ All None

Require Multi-Factor Auth to join devices ⓘ Yes No

Maximum number of devices per user ⓘ 50

Users may sync settings and app data across devices ⓘ All Selected None

Selected
No member selected

Answer:

Answer Area

 Save  Discard

Users may join devices to Azure AD 

All

Selected

None

Selected

No member selected

Additional local administrators on Azure AD joined devices 

Selected

None

Selected

No member selected

Users may register their devices with Azure AD 

All

None

Require Multi-Factor Auth to join devices 

Yes

No

Maximum number of devices per user 

50

Users may sync settings and app data across devices 

All

Selected

None

Selected

No member selected

Explanation:

Box 1: Selected

Only selected users should be able to join devices

Box 2: Yes

Require Multi-Factor Auth to join devices.

From scenario:

- Ensure that only users who are part of a group named Pilot can join devices to Azure AD
- Ensure that when users join devices to Azure Active Directory (Azure AD), the users use a mobile phone to verify their identity.

QUESTION 133

Note: This question is part of a series of questions that present the same scenario. Each

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.

Your company is deploying an on-premises application named App1. Users will access App1 by using a URL of <https://app1.contoso.com>.

You register App1 in Azure Active Directory (Azure AD) and publish App1 by using the Azure AD Application Proxy.

You need to ensure that App1 appears in the My Apps portal for all the users.

Solution: You configure the delegated permission for App1 in Azure AD.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

QUESTION 134

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.

Your company is deploying an on-premises application named App1. Users will access App1 by using a URL of <https://app1.contoso.com>.

You register App1 in Azure Active Directory (Azure AD) and publish App1 by using the Azure AD Application Proxy.

You need to ensure that App1 appears in the My Apps portal for all the users.

Solution: You create an offer for App1 and publish the offer to Azure Marketplace.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

QUESTION 135

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.

Your company is deploying an on-premises application named App1. Users will access App1 by using a URL of <https://app1.contoso.com>.

You register App1 in Azure Active Directory (Azure AD) and publish App1 by using the Azure AD Application Proxy.

You need to ensure that App1 appears in the My Apps portal for all the users.

Solution: You create a conditional access policy for App1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

QUESTION 136

You have an Azure SQL database named Db1 that runs on an Azure SQL server named SQLserver1. You need to ensure that you can use the query editor on the Azure portal to query Db1.

What should you do?

- A. Modify the Advanced Data Security settings of Db1
- B. Configure the Firewalls and virtual networks settings for SQLserver1
- C. Copy the ADO.NET connection string of Db1 and paste the string to the query editor
- D. Approve private endpoint connections for SQLserver1

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-connect-query-portal>

QUESTION 137

Your company plans to develop an application that will use a NoSQL database. The database will be used to store transactions and customer information by using JSON documents.

Which two Azure Cosmos DB APIs can developers use for the application? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Cassandra
- B. Gremlin (graph)
- C. MongoDB
- D. Azure Table
- E. Core (SQL)

Answer: BE

Explanation:

The SQL API supports cross-document transactions expressed as JavaScript-stored procedures and triggers. Transactions are scoped to a single partition within each container and executed with ACID semantics as "all or nothing," isolated from other concurrently executing code and user requests. If exceptions are thrown through the server-side execution of JavaScript application code, the entire transaction is rolled back.

Azure Cosmos DB is Microsoft's globally distributed, multi-model database service. Where multi-model means Azure Cosmos DB supports multiple APIs and multiple data models, different APIs use different data formats for storage and wire protocol. For example, SQL uses JSON, MongoDB uses BSON, Table uses EDM, Cassandra uses CQL, Gremlin uses JSON format. As a result, we recommend using the same API for all access to the data in a given account. Each API operates independently, except the Gremlin and SQL API, which are interoperable.

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/faq>

QUESTION 138

You have an Azure Cosmos DB account named Account1. Account1 includes a database named DB1 that contains a container named Container 1. The partition key for Container1 is set to /city. You plan to change the partition key for Container1.

What should you do first?

- A. Delete Container1
- B. Create a new container in DB1
- C. Regenerate the keys for Account1.
- D. Implement the Azure CosmosDB.NET SDK

Answer: B

Explanation:

The good news is that there are two features, the Change Feed Processor and Bulk Executor Library, in Azure Cosmos DB that can be leveraged to achieve a live migration of your data from one container to another. This allows you to re-distribute your data to match the desired new partition key scheme, and make the relevant application changes afterwards, thus achieving the effect of "updating your partition key".

Reference:

<https://devblogs.microsoft.com/cosmosdb/how-to-change-your-partition-key/>

QUESTION 139

You have the Azure virtual networks shown in the following table.

Name	Location
VNET1	East US
VNET2	East US
VNET3	Central US

All the virtual networks are peered.

You have the virtual machines shown in the following table.

Name	Operating system	Connected to
VM1	Red Hat Enterprise Linux 7.7	VNET1
VM2	Windows Server 2019	VNET2
VM3	Windows Server 2019	VNET3

You deploy an Azure bastion named Bastion1 to VNET1.

To which virtual machines can you connect by using Bastion1?

- A. VM1 only
- B. VM1 and VM2 only
- C. VM2 and VM3 only
- D. VM1, VM2, and VM3

Answer: A

Explanation:

Connect to a VM through Azure Bastion.

When you click on Connect in an Azure VM, you have an additional option called Bastion. In order to get this option, the Azure VM must belong to the same virtual network as the Azure Bastion.

Reference:

<https://www.starwindsoftware.com/blog/overview-of-microsoft-azure-bastion>

QUESTION 140

You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

Name	Operating system	Resource group	Location
VM1	Windows Server 2012 R2	RG1	East US
VM2	Windows Server 2016	RG1	West US
VM3	Windows Server 2019	RG2	West US
VM4	Red Hat Enterprise Linux 7.7	RG2	West US
VM5	Ubuntu Server 18.04 LTS	RG1	East US
VM6	CentOS-based 7.7	RG1	East US

You need to ensure that all critical and security updates are applied to each virtual machine every month. What is the minimum number of update deployments you should create?

- A. 4
- B. 6
- C. 1
- D. 2

Answer: A

Explanation:

One for the Windows VMs, and for each type of Linux VM.

Reference:

<https://docs.microsoft.com/en-us/azure/automation/update-management/overview>

QUESTION 141

You have an Azure Active Directory (Azure AD) tenant linked to an Azure subscription. The tenant contains a group named Admins.

You need to prevent users, except for the members of Admins, from using the Azure portal and Azure PowerShell to access the subscription.
What should you do?

- A. From Azure AD, configure the User settings.
- B. From the Azure subscription, assign an Azure policy.
- C. From Azure AD, create a conditional access policy.
- D. From the Azure subscription, configure Access control (IAM).

Answer: C

Explanation:

Typically, you use Conditional Access to control access to your cloud apps. You can also set up policies to control access to Azure management.

The policy you create applies to all Azure management endpoints, including the following:

- Azure portal
- Azure Resource Manager provider
- Classic Service Management APIs
- Azure PowerShell
- Visual Studio subscriptions administrator portal
- Azure DevOps
- Azure Data Factory portal

To create a policy for Azure management, you select Microsoft Azure Management under Cloud apps when choosing the app to which to apply the policy.

The screenshot shows the Microsoft Azure portal interface for creating a new app policy. The left panel is titled 'New' and contains sections for 'Info', 'Assignments', 'Access controls', and 'Enable policy'. The 'Cloud apps' section is currently active, showing a 'Select' dialog. In this dialog, the 'Select' tab is chosen, and 'Microsoft Azure Management' is listed under 'Applications'. A red box highlights the 'MA' icon next to the application name. At the bottom of the 'Cloud apps' panel, there is a 'Done' button.

Incorrect Answers:

A: From User Settings you can only restrict access to Azure Portal, not access to Azure Powershell.

Note: Microsoft allows restricting standard user access to Azure Active Directory administration portal.

1. Log in to Azure portal as Global Administrator
2. Go to Azure Active Directory | User Settings
3. Then click on Yes under Restrict access to Azure AD administration portal

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/conditional-access-azure-management>

<https://www.rebeladmin.com/2019/04/step-step-guide-restrict-azure-ad-administration-portal/>

QUESTION 142

You have Azure virtual machines deployed to three Azure regions. Each region contains a single virtual network that has four virtual machines on the same subnet. Each virtual machine runs an application named App1. App1 is accessible by using HTTPS. Currently, the virtual machines are inaccessible from the internet.

You need to use Azure Front Door to load balance requests for App1 across all the virtual machines. Which additional Azure service should you provision?

- A. a public Azure Load Balancer
- B. Azure Traffic Manager
- C. an internal Azure Load Balancer
- D. Azure Private Link

Answer: C

Explanation:

Can we deploy Azure Load Balancer behind Front Door?

Azure Front Door needs a public VIP or a publicly available DNS name to route the traffic to. Deploying an Azure Load Balancer behind Front Door is a common use case.

Reference:

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq>

QUESTION 143

You create the Azure resources shown in the following table.

Name	Resource type
VM1	Virtual machine
VM2	Virtual machine
Managed1	Managed identity
Managed2	Managed identity

You attempt to add a role assignment to a resource group as shown in the following exhibit.

Add role assignment

Role ⓘ
Reader ⓘ

Assign access to ⓘ
Azure AD user, group, or service principal

Select ⓘ
VM

 VM1

Selected members:

No members selected. Search for and add one or more members you want to assign to the role for this resource.

[Learn more about RBAC](#)

What should you do to ensure that you can assign VM2 the Reader role for the resource group?

- A. Modify the Reader role at the subscription level.
- B. Configure just in time (JIT) VM access on VM2.

- C. Configure Access control (IAM) on VM2.
- D. Assign a managed identity to VM2.

Answer: C

Explanation:

After you've configured an Azure resource with a managed identity, you can give the managed identity access to another resource, just like any security principal.

Use Azure RBAC to assign a managed identity access to another resource

After you've enabled managed identity on an Azure resource, such as an Azure VM or Azure virtual machine scale set:

1. Sign in to the Azure portal using an account associated with the Azure subscription under which you have configured the managed identity.
2. Navigate to the desired resource on which you want to modify access control. In this example, we are giving an Azure virtual machine access to a storage account, so we navigate to the storage account.
3. Select the Access control (IAM) page of the resource, and select + Add role assignment. Then specify the Role, Assign access to, and specify the corresponding Subscription. Under the search criteria area, you should see the resource. Select the resource, and select Save.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/howto-assign-access-portal>

QUESTION 144

You have an Azure Container Registry and an Azure container instance.

You pull an image from the registry, and then update the local copy of the image.

You need to ensure that the updated image can be deployed to the container instance.

The solution must ensure that you can deploy the updated image or the previous version of the image.

What should you do?

- A. Run the docker image push command and specify the tag parameter.
- B. Run the az image copy command and specify the tag parameter.
- C. Run the az aks update command and specify the attach-acr parameter.
- D. Run the kubectl apply command and specify the dry-run parameter.

Answer: B

QUESTION 145

You have an Azure Service Bus and two clients named Client1 and Client2.

You create a Service Bus queue named Queue1 as shown in the exhibit.

Create queue

Service Bus

Name* ✓

Max queue size

Message time to live i

Days	Hours	Minutes	Seconds
14	0	0	0

Lock duration i

Days	Hours	Minutes	Seconds
0	0	0	30

Enable duplicate detection i

Duplicate detection window i

Days	Hours	Minutes	Seconds
0	0	10	0

Enable dead lettering on message expiration i

Enable sessions i

Client1 sends messages to Queue1 as shown in the following table.

Time hh:mm:ss	Message
12:01:01	M3
12:01:02	M2
12:01:03	M1
12:01:04	M3

Client2 reads the messages from Queue1 at 12:01:05.

How will the messages be presented to Client2?

- A. Client2 will read four messages in the following order: M3, M2, M1, and then M3.
- B. Client2 will read three messages in the following order: M3, M2, and then M1.
- C. Client2 will read four messages in the following order; M3, M1, M2, and then M3.
- D. Client2 will read three messages in the following order: M1, M2. and then M3
- E. Client2 will read three messages in the following order: M3, M1, and then M2.

Answer: B

Explanation:

Duplicate is enabled, and the duplication detection window is set to 10 minutes. The second M3 message in the queue will be discarded.

Note 1: Duplicate detection enables the sender resend the same message, and the queue or topic discards any duplicate copies.

Note 2: Queues offer First In, First Out (FIFO) message delivery to one or more competing consumers. That is, receivers typically receive and process messages in the order in which they were added to the queue, and only one message consumer receives and processes each message.

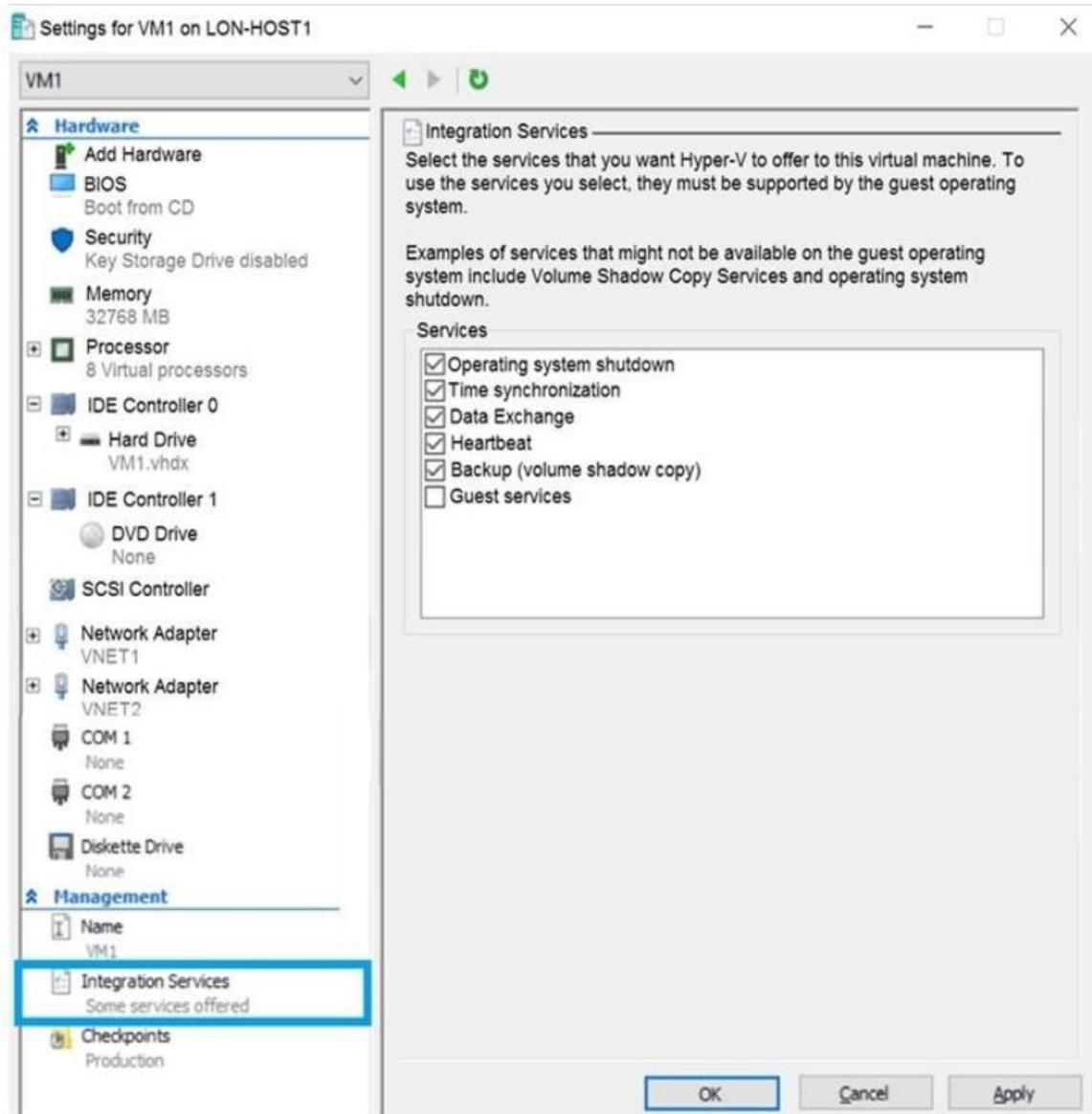
References:

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-queues-topics-subscriptions>

<https://docs.microsoft.com/en-us/azure/service-bus-messaging/duplicate-detection>

QUESTION 146

You have an on-premises virtual machine named VM1 configured as shown in the following exhibit.



VM is started.

You need to create a new virtual machine image in Azure from VM1.

Which three actions should you perform before you create the new image? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Remove the Backup (volume shadow copy) integration service
- B. Generalize VM1
- C. Run Add-AzureRmVhd and specify a blob service container as the destination
- D. Run Add-AzureRmVhd and specify a file share as the destination
- E. Reduce the amount of memory to 16 GB
- F. Convert the disk type to VHD

Answer: BCF

Explanation:

Sysprep removes all your personal account and security information, and then prepares the machine to be used as an image.

The Add-AzureVhd cmdlet uploads on-premises virtual hard disks, in .vhd file format, to a blob storage account as fixed virtual hard disks.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.compute/add-azurermvhd?view=azurermps-6.13.0>

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/capture-image-resource>

QUESTION 147

You have an Azure subscription named Subscription1 that contains an Azure virtual network named VNet1. VNet1 connects to your on-premises network by using Azure ExpressRoute. You need to connect VNet1 to the on-premises network by using a site-to-site VPN.

The solution must minimize cost.

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

NOTE: Each correct selection is worth one point.

- A. Create a VPN gateway that uses the VpnGw1 SKU.
- B. Create a connection.
- C. Create a local site VPN gateway.
- D. Create a gateway subnet.
- E. Create a VPN gateway that uses the Basic SKU.

Answer: ABC

Explanation:

<https://docs.microsoft.com/en-za/archive/blogs/canitpro/step-by-step-configuring-a-site-to-site-vpn-gateway-between-azure-and-on-premise>

QUESTION 148

You plan to create an Azure Storage account named storage1 that will store blobs and be accessed by Azure Databricks.

You need to ensure that you can set permissions for individual blobs by using Azure Active Directory (Azure AD) authentication.

Which Advanced setting should you enable for storage1?

- A. Hierarchical namespace
- B. Large file shares
- C. Blob soft delete
- D. NFSv3

Answer: A

Explanation:

Question: Do I have to enable support for ACLs?

No. Access control via ACLs is enabled for a storage account as long as the Hierarchical Namespace (HNS) feature is turned ON.

Note 1: We [Microsoft] are pleased to share the general availability of Azure Active Directory (AD) based access control for Azure Storage Blobs and Queues. Enterprises can now grant specific data access permissions to users and service identities from their Azure AD tenant using Azure's Role-based access control (RBAC).

Note 2: Azure Data Lake Storage Gen2 implements an access control model that supports both Azure role-based access control (Azure RBAC) and POSIX-like access control lists (ACLs).

You can associate a security principal with an access level for files and directories. These associations are captured in an access control list (ACL). Each file and directory in your storage account has an access control list. When a security principal attempts an operation on a file or directory, An ACL check determines whether that security principal (user, group, service principal, or managed identity) has the correct permission level to perform the operation.

Incorrect Answers:

Blob soft delete protects your data from being accidentally or erroneously modified or deleted. When blob soft delete is enabled for a storage account, blobs, blob versions, and snapshots in that storage account may be recovered after they are deleted, within a retention period that you specify.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-access-control#access-control-lists-on-files-and-directories>

<https://azure.microsoft.com/en-us/blog/azure-storage-support-for-azure-ad-based-access-control-now-generally-available/>

QUESTION 149

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains the users shown in the following table.

Name	Member of
User1	Domain Admins
User2	Domain Users
User3	ADSyncAdmins
User4	Account Operators

You plan to install Azure AD Connect and enable SSO.

You need to specify which user to use to enable SSO. The solution must use the principle of least privilege.

Which user should you specify?

- A. User4
- B. User1
- C. User3
- D. User2

Answer: B

Explanation:

You need to have domain administrator credentials for each Active Directory forest that:

- You synchronize to Azure AD through Azure AD Connect.
- Contains users you want to enable for Seamless SSO.

Note: The domain administrator credentials are not stored in Azure AD Connect or in Azure AD. They're used only to enable Seamless SSO through Azure AD Connect.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso-quick-start>

QUESTION 150

You have an Azure subscription named Subscription1 that is used by several departments at your company. Subscription1 contains the resources in the following table.

Name	Type
Storage1	Storage account
RG1	Resource group
Container1	Blob container
Share1	File share

Another administrator deploys a virtual machine named VM1 and an Azure Storage account named Storage2 by using a single Azure Resource Manager template.

You need to view the template used for the deployment.

From which blade can you view the template that was used for the deployment?

- A. Container1
- B. VM1
- C. Storage2
- D. RG1

Answer: D

Explanation:

You can verify the deployment by exploring the resource group from the Azure portal

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-manager-tutorial>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/template-tutorial-create-first-template?tabs=azure-powershell>

QUESTION 151

A company hosts virtual machines (VMs) in an on-premises datacenter and in Azure. The on-premises and Azure-based VMs communicate using ExpressRoute. The company wants to be able to continue regular operations if the ExpressRoute connection fails. Failover connections must use the Internet and must not require Multiprotocol Label Switching (MPLS) support.

You need to recommend a solution that provides continued operations.

What should you recommend?

- A. Set up a second ExpressRoute connection.
- B. Increase the bandwidth of the existing ExpressRoute connection.
- C. Increase the bandwidth for the on-premises internet connection.
- D. Set up a VPN connection.

Answer: D

Explanation:

<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/hybrid-networking/expressroutevpn-failover>

QUESTION 152

You plan to automate the deployment of a virtual machine scale set that uses the Windows Server 2016 Datacenter image.

You need to ensure that when the scale set virtual machines are provisioned, they have web server components installed.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Create a new virtual machine scale set in the Azure portal.
- B. Create an automation account.
- C. Upload a configuration script.
- D. Modify the extensionProfile section of the Azure Resource Manager template.
- E. Create an Azure policy.

Answer: AD

Explanation:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/tutorial-install-apps-template>

QUESTION 153

You have an Azure subscription that contains a resource group named RG1.

RG1 contains multiple resources.

You need to trigger an alert when the resources in RG1 consume \$1,000 USD.

What should you do?

- A. From Cost Management + Billing, add a cloud connector.
- B. From the subscription, create an event subscription.
- C. From Cost Management + Billing create a budget.
- D. From RG1, create an event subscription.

Answer: C

Explanation:

Create budgets to manage costs and create alerts that automatically notify you are your stakeholders of spending anomalies and overspending.

To set it up, go to the Azure Portal, select 'Cost Management + Billing' -> 'Cost Management' -> 'Go to Cost Management'.

The screenshot shows the Azure Cost Management + Billing dashboard. The left sidebar contains a navigation menu with items like New, Dashboard, Resource groups, All resources, Recent, App Services, SQL databases, Virtual machines (classic), Virtual machines, Cloud services (classic), Subscriptions, Azure Active Directory, Azure AD B2C, Monitor, Security Center, Cost Management + Billing (which is selected and highlighted with a red box), Help + support, and Advisor. Below the sidebar is a 'More services' link. The main content area has a header 'Cost Management + Billing - Cost Management'. It features a search bar, a 'Go to Cost Management' link, and a large graphic of overlapping blue and purple circles. The 'Overview' section includes a 'Cost Management' link (also highlighted with a red box), 'Diagnose and solve problems', 'BILLING ACCOUNT' (with 'Subscriptions' and 'Invoices' options), 'Contact info', 'Billing address', 'Payment methods', and 'SUPPORT + TROUBLESHOOTING' (with 'New support request' option). A descriptive text block says 'Optimize your cloud spend. Maximize your cloud potential.' followed by 'Azure Cost Management by Cloudyn, a Microsoft service, helps you:' and a bulleted list: 'Monitor cloud spend', 'Drive organizational accountability', and 'Optimize cloud efficiency'. Below this is a note: 'The service is available for free to manage your Azure spend.', a 'Learn More' link, and a prominent 'Go to Cost Management' button.

Note: Cost alerts are automatically generated based when Azure resources are consumed. Alerts show all active cost management and billing alerts together in one place. When your consumption reaches a given threshold, alerts are generated by Cost Management. There are three types of cost alerts: budget alerts, credit alerts, and department spending quota alerts.

Reference:

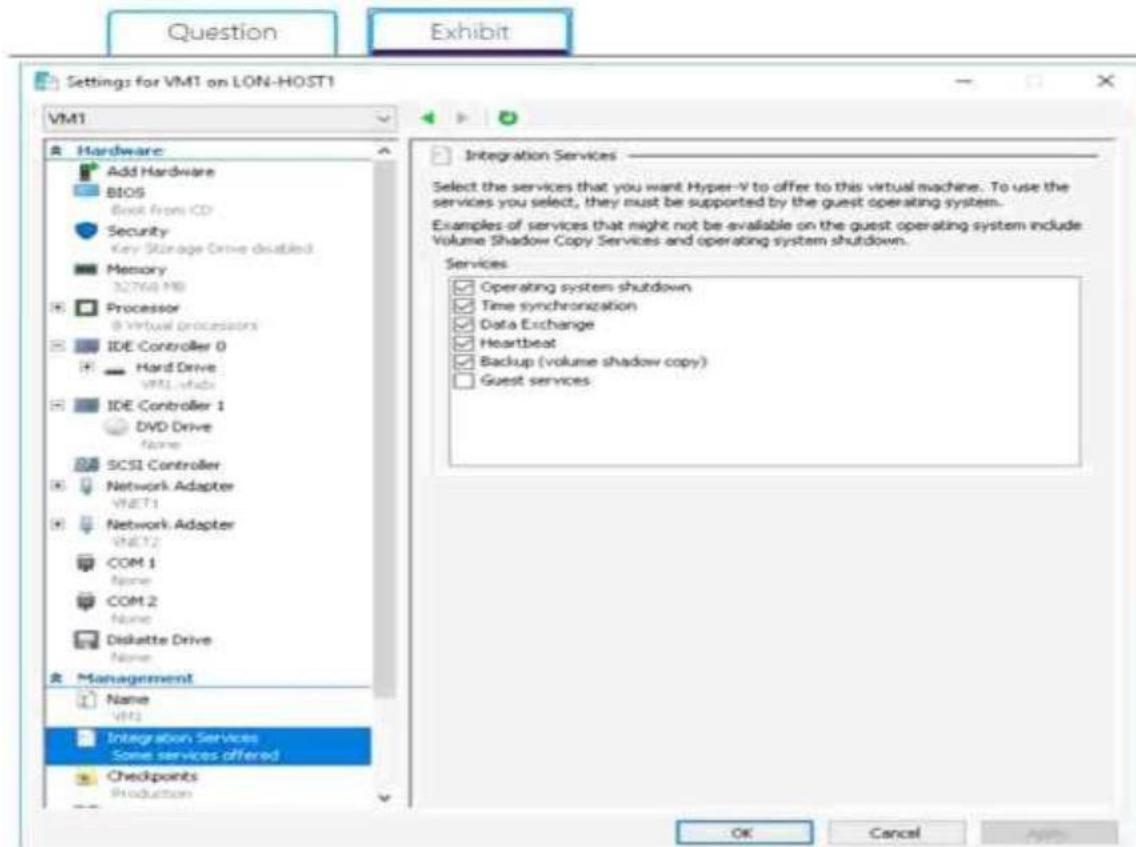
<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/getting-started>

QUESTION 154

You have an Azure subscription.

You have an on-premises virtual machine named VM1.

The settings for VM1 are shown in the exhibit.



You need to ensure that you can use the disks attached to VM1 as a template for Azure virtual machines.

What should you modify on VM1?

- A. the hard drive
- B. Integration Services
- C. the memory
- D. the network adapters
- E. the processor

Answer: A

Explanation:

From the exhibit we see that the disk is in the VHDX format. Before you upload a Windows virtual machines (VM) from on-premises to Microsoft Azure, you must prepare the virtual hard disk (VHD or VHDX). Azure supports only generation 1 VMs that are in the VHD file format and have a fixed sized disk. The maximum size allowed for the VHD is 1,023 GB. You can convert a generation 1 VM from the VHDX file system to VHD and from a dynamically expanding disk to fixed-sized.

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image?toc=azurevirtual-machines-windowstoc.json>

QUESTION 155

You have an Azure subscription that contains the storage accounts shown in the following table.

Name	Contains
Storagecontoso1	A blob service and a table service
Storagecontoso2	A blob service and a file service
Storagecontoso3	A queue service
Storagecontoso4	A file service and a queue service
Storagecontoso5	A table service

You enable Azure Advanced Threat Protection (ATP) for all the storage accounts.

You need to identify which storage accounts will generate Azure ATP alerts.

Which two storage accounts should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. storagecontoso1
- B. storagecontoso2
- C. storagecontoso3
- D. storagecontoso4
- E. storaaecontoso5

Answer: AB

Explanation:

Advanced threat protection for Azure Storage is currently available only for Blob Storage.

<https://docs.microsoft.com/en-us/azure/storage/common/storage-advanced-threat-protection?tabs=azure-portal>

QUESTION 156

Note: This question is part of 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 an Azure Active Directory (Azure AD) tenant that contains a group named Group1. You need to enable multi-factor authentication (MFA) for the users in Group1 only.

Solution: From the Azure portal, you configure an authentication method policy.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

We should use a Conditional Access policy.

Note: There are two ways to secure user sign-in events by requiring multi-factor authentication in Azure AD. The first, and preferred, option is to set up a Conditional Access policy that requires multi-factor authentication under certain conditions. The second option is to enable each user for

Azure Multi-Factor Authentication. When users are enabled individually, they perform multi-factor authentication each time they sign in (with some exceptions, such as when they sign in from trusted IP addresses or when the remembered devices feature is turned on). Enabling Azure Multi-Factor Authentication using Conditional Access policies is the recommended approach. Changing user states is no longer recommended unless your licenses don't include Conditional Access as it requires users to perform MFA every time they sign in.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>

QUESTION 157

Note: This question is part of 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 an Azure Active Directory (Azure AD) tenant that contains a group named Group1. You need to enable multi-factor authentication (MFA) for the users in Group1 only.

Solution: From Multi-Factor Authentication, you select Bulk update, and you provide a CSV file that contains the members of Group1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

We should use a Conditional Access policy.

Note: There are two ways to secure user sign-in events by requiring multi-factor authentication in Azure AD. The first, and preferred, option is to set up a Conditional Access policy that requires multi-factor authentication under certain conditions. The second option is to enable each user for Azure Multi-Factor Authentication. When users are enabled individually, they perform multi-factor authentication each time they sign in (with some exceptions, such as when they sign in from trusted IP addresses or when the remembered devices feature is turned on). Enabling Azure Multi-Factor Authentication using Conditional Access policies is the recommended approach. Changing user states is no longer recommended unless your licenses don't include Conditional Access as it requires users to perform MFA every time they sign in.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>

QUESTION 158

Hotspot Question

You have the Azure SQL Database servers shown in the following table.

Name	Elastic pool
sqlserver1	Pool1
sqlserver2	Pool1, Pool2

You have the Azure SQL databases shown in the following table.

Name	Azure SQL Database server	Elastic pool
DB1	sqlserver1	None
DB2	sqlserver1	Pool1
DB3	sqlserver2	Pool1
DB4	sqlserver2	Pool2

You create a failover group named failover1 that has the following settings:

- Primary server: sqlserver1
- Secondary server: sqlserver2
- Read/Write failover policy: Automatic
- Read/Write grace period (hours): 1 hour

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 Area

Statements	Yes	No
You can add DB1 to failover1.	<input type="radio"/>	<input type="radio"/>
You can add DB3 to failover1.	<input type="radio"/>	<input type="radio"/>
Sqlserver1 and sqlserver2 are in the same Azure region.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can add DB1 to failover1.	<input checked="" type="radio"/>	<input type="radio"/>
You can add DB3 to failover1.	<input type="radio"/>	<input checked="" type="radio"/>
Sqlserver1 and sqlserver2 are in the same Azure region.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

DB1 is on the primary server

Box 2: No

DB3 is on the secondary server.

You can put all or several databases within an elastic pool into the same failover group.

Box 3: No

A failover group is a named group of databases managed by a single server or within a managed instance that can fail over as a unit to another region in case all or some primary databases become unavailable due to an outage in the primary region.

The secondary cannot be in the same region as the primary.

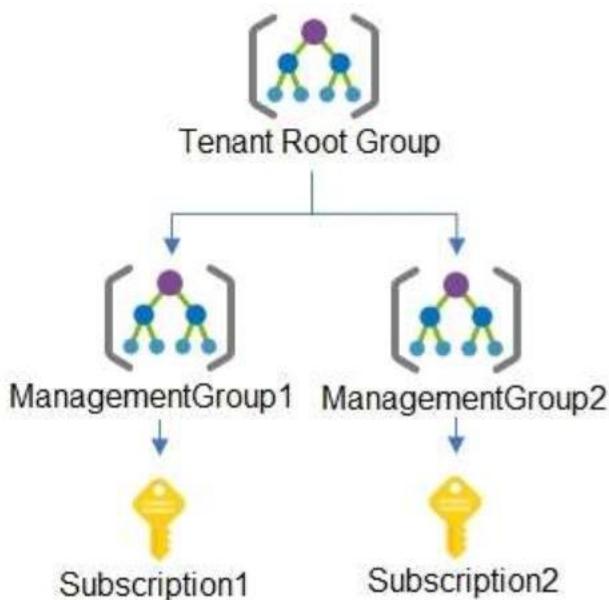
Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/auto-failover-group-overview>

QUESTION 159

Hotspot Question

You have a hierarchy of management groups and Azure subscriptions as shown in the following table.



You create the Azure resources shown in the following table.

Name	Type	Created in
RG1	Resource group	Subscription1
RG2	Resource group	Subscription2
VM2	Virtual machine	RG2

You assign roles to users as shown in the following table.

User name	Role	On resource
User1	Contributor	ManagementGroup1
User2	Contributor	ManagementGroup2
User3	Reader	Tenant Root Group

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

NOTE:

Each correct selection is worth one point

Statements	Yes	No
You can remove User1 from the Contributor role for RG1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM2.	<input type="radio"/>	<input type="radio"/>
You can add User3 as a Contributor for RG1.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
You can remove User1 from the Contributor role for RG1.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can delete VM2.	<input checked="" type="radio"/>	<input type="radio"/>
You can add User3 as a Contributor for RG1.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: No

You cannot remove contributor access only from RG as it's inherited from above.

Box 2: Yes

Contributor role: Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC.

Box 3: Yes

You can add user permission on RG1 as there is no separate deny applied from the above hierarchy.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#contributor>

QUESTION 160

Hotspot Question

You have an Azure subscription that contains a resource group named RG1.

You have a group named Group1 that is assigned the Contributor role for RG1.

You need to enhance security for the virtual machines in RG1 to meet the following requirements:

- Prevent Group1 from assigning external IP addresses to the virtual machines.
- Ensure that Group1 can establish an RDP connection to the virtual machines through a shared external IP address.

What should you use to meet each requirement? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Prevent Group1 from assigning external IP addresses to the virtual machines:

Azure Policy
Azure Bastion
Virtual network service endpoints
Azure Firewall
Azure Web Application Firewall (WAF)

Ensure that Group1 can establish an RDP connection to the virtual machines through a shared external IP address:

Azure Policy
Azure Bastion
Virtual network service endpoints
Azure Firewall
Azure Web Application Firewall (WAF)

Answer:

Prevent Group1 from assigning external IP addresses to the virtual machines:

Azure Policy
Azure Bastion
Virtual network service endpoints
Azure Firewall
Azure Web Application Firewall (WAF)

Ensure that Group1 can establish an RDP connection to the virtual machines through a shared external IP address:

Azure Policy
Azure Bastion
Virtual network service endpoints
Azure Firewall
Azure Web Application Firewall (WAF)

Explanation:

Box 1: Azure Policy

There is a built-in policy in the Azure Policy service that allows you to block public IPs on all NICs of a VM.

Note: Azure Policy is a powerful tool in your Azure toolbox. It allows you to enforce specific governance principals you want to see implemented in your environment. Some key examples of what Azure Policy allows you to do is:

Automatically tag resources
Block VMs from having a public IP
Enforce specific regions
Enforce VM size

Box 2: Azure Bastion

Azure Bastion is a fully managed PaaS service that provides secure and seamless RDP and SSH access to your virtual machines directly through the Azure Portal.

Azure Bastion is provisioned directly in your Virtual Network (VNet) and supports all VMs in your Virtual Network (VNet) using SSL without any exposure through public IP addresses.

Incorrect Answers:

Virtual Network (VNet) service endpoint provides secure and direct connectivity to Azure services over an optimized route over the Azure backbone network. Endpoints allow you to secure your critical Azure service resources to only your virtual networks. Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet.

Reference:

<https://blog.nillsf.com/index.php/2019/11/02/using-azure-policy-to-deny-public-ips-on-specific-vnets/>

<https://azure.microsoft.com/en-us/services/azure-bastion/>

QUESTION 161

Hotspot Question

Your network contains an on-premises Active Directory domain named contoso.com that contains a user named User1. The domain syncs to Azure Active Directory (Azure AD). You have the Windows 10 devices shown in the following table.

Name	Joined to
Device1	On-premises Active Directory
Device2	Azure AD
Device3	Workgroup

The User Sign-In settings are configured as shown in the following exhibit.

PROVISION FROM ACTIVE DIRECTORY



Azure AD Connect cloud provisioning

This feature allows you to manage provisioning from the cloud.

[Manage provisioning \(Preview\)](#)

Azure AD Connect sync

Sync Status	Enabled
Last Sync	Less than 1 hour ago
Password Hash Sync	Enabled

USER SIGN-IN



Federation	Disabled	0 domains
Seamless single sign-on	Enabled	1 domain
Pass-through authentication	Disabled	0 agents

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

NOTE:

Each correct selection is worth one point

Statements	Yes	No
When accessing the Azure portal from Device1, User1 will sign in automatically by using SSO.	<input type="radio"/>	<input checked="" type="radio"/>
When accessing the Azure portal from Device2, User1 will sign in automatically by using SSO.	<input checked="" type="radio"/>	<input type="radio"/>
When accessing the Azure portal from Device3, User1 will sign in automatically by using SSO.	<input type="radio"/>	<input checked="" type="radio"/>

Answer:

Statements	Yes	No
When accessing the Azure portal from Device1, User1 will sign in automatically by using SSO.	<input checked="" type="radio"/>	<input type="radio"/>
When accessing the Azure portal from Device2, User1 will sign in automatically by using SSO.	<input type="radio"/>	<input checked="" type="radio"/>
When accessing the Azure portal from Device3, User1 will sign in automatically by using SSO.	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 162

Hotspot Question

You create a virtual machine scale set named Scale1. Scale1 is configured as shown in the following exhibit.

The subscription contains the Azure SQL databases shown in the following table.

Create a virtual machine scale set

Basics Disks Networking **Scaling** Management Health Advanced ...

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. This automated and elastic behavior reduces the management overhead to monitor and optimize the performance of your application. [Learn more about VMSS scaling](#)

Instance

Initial instance count * ⓘ ✓

Scaling

Scaling policy ⓘ Manual Custom

Minimum number of VMs * ⓘ

Maximum number of VMs * ⓘ ✓

Scale out

CPU threshold (%) * ⓘ

Duration in minutes * ⓘ

Number of VMs to increase by * ⓘ ✓

Scale in

CPU threshold (%) * ⓘ

Number of VMs to decrease by * ⓘ

Diagnostic logs

Collect diagnostic logs from Autoscale Disabled Enabled

Review + create < Previous Next : Management >

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

If Scale1 is utilized at 85 percent for six minutes after it is deployed, Scale1 will be running

▼
2 virtual machines
4 virtual machines
6 virtual machines
10 virtual machines
20 virtual machines

If Scale is first utilized at 25 percent for six minutes after it is deployed, and then utilized at 50 percent for six minutes, Scale1 will be running

▼
2 virtual machines
4 virtual machines
6 virtual machines
10 virtual machines
20 virtual machines

Answer:

Answer Area

If Scale1 is utilized at 85 percent for six minutes after it is deployed, Scale1 will be running

▼
2 virtual machines
4 virtual machines
6 virtual machines
10 virtual machines
20 virtual machines

If Scale is first utilized at 25 percent for six minutes after it is deployed, and then utilized at 50 percent for six minutes, Scale1 will be running

▼
2 virtual machines
4 virtual machines
6 virtual machines
10 virtual machines
20 virtual machines

Explanation:

Box 1:

The Autoscale scale out rule increases the number of VMs by 2 if the CPU threshold is 80% or higher. The initial instance count is 4 and rises to 6 when the 2 extra instances of VMs are added.

Box 2:

The Autoscale scale in rule decreases the number of VMs by 4 if the CPU threshold is 30% or lower. The initial instance count is 4 and thus cannot be reduced to 0 as the minimum instances is set to 2. Instances are only added when the CPU threshold reaches 80%.

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-overview>

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-best-practices>

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/autoscale-common-scale-patterns>

QUESTION 163

Hotspot Question

You have Azure Storage accounts as shown in the following exhibit.

NAME	TYPE	REGION	RESOURCE GROUP	LOCATION	SUBSCRIPTION	ACCESS TIER	REPLICAZ...
storageaccount1	Storage account	Storage	ContosoRG1	East US	Subscription 1	Hot	General-purpose v2 (GPv2)
storageaccount2	Storage account	StorageV2	ContosoRG1	Central US	Subscription 1	Hot	General-purpose v1 (GPv1)
storageaccount3	Storage account	BlobStorage	ContosoRG1	East US	Subscription 1	Hot	General-purpose v2 (GPv2)

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

You can use [answer choice] for Azure Table Storage.

storageaccount1 only
storageaccount2 only
storageaccount3 only
storageaccount1 and storageaccount2 only
storageaccount2 and storageaccount3 only

You can use [answer choice] for Azure Blob storage.

storageaccount3 only
storageaccount2 and storageaccount3 only
storageaccount1 and storageaccount3 only
all the storage accounts

Answer:

You can use [answer choice] for Azure Table Storage.

storageaccount1 only
storageaccount2 only
storageaccount3 only
storageaccount1 and storageaccount2 only
storageaccount2 and storageaccount3 only

You can use [answer choice] for Azure Blob storage.

storageaccount3 only
storageaccount2 and storageaccount3 only
storageaccount1 and storageaccount3 only
all the storage accounts

Explanation:

Note: The three different storage account options are: General-purpose v2 (GPv2) accounts, General-purpose v1 (GPv1) accounts, and Blob storage accounts.

General-purpose v2 (GPv2) accounts are storage accounts that support all of the latest features

for blobs, files, queues, and tables.

- Blob storage accounts support all the same block blob features as GPv2, but are limited to supporting only block blobs.
- General-purpose v1 (GPv1) accounts provide access to all Azure Storage services, but may not have the latest features or the lowest per gigabyte pricing.

References:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-account-options>

QUESTION 164

Hotspot Question

You have several Azure virtual machines on a virtual network named VNet1. You configure an Azure Storage account as shown in the following exhibit.

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
VNet1	1	10.2.0.0/16	Enabled	DemoRG	Production subscript...
Prod	10.2.0.0/24		Enabled	DemoRG	Production subscript...

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account

▼
always
during a backup
never

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account

▼
always
during a backup
never

Answer:

Answer Area

The virtual machines on the 10.2.9.0/24 subnet will have network connectivity to the file shares in the storage account

▼
always
during a backup
never

Azure Backup will be able to back up the unmanaged hard disks of the virtual machines in the storage account

▼
always
during a backup
never

Explanation:

Box 1: always

Endpoint status is enabled.

Box 2: Never

After you configure firewall and virtual network settings for your storage account, select Allow trusted Microsoft services to access this storage account as an exception to enable Azure Backup service to access the network restricted storage account.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-use-files-windows>

<https://azure.microsoft.com/en-us/blog/azure-backup-now-supports-storage-accounts-secured-with-azure-storage-firewalls-and-virtual-networks/>

QUESTION 165

Hotspot Question

You have an Azure subscription that includes an Azure key vault named Vault1.

You create the Azure virtual machines shown in the following table.

Name	Operating system disk type	Use managed disks
VM1	Premium SSD	Yes
VM2	Standard HDD	Yes
VM3	Standard SSD	No

You enable Azure Disk Encryption for all the virtual machines and use the -VolumeType All parameter.

You add data disks to the virtual machines as shown in the following table.

Name	Virtual machine	Storage account type
VM1-Disk1	VM1	Premium SSD
VM2-Disk1	VM2	Standard SSD
VM3-Disk1	VM3	Standard HDD

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
 NOTE: Each correct selection is worth one point.

Statements	Yes	No
VM1-Disk1 is encrypted automatically by using Azure Disk Encryption.	<input type="radio"/>	<input type="radio"/>
VM2-Disk1 is encrypted automatically by using Azure Disk Encryption.	<input type="radio"/>	<input type="radio"/>
VM3-Disk1 is encrypted automatically by using Azure Disk Encryption.	<input type="radio"/>	<input type="radio"/>

Answer:

Statements	Yes	No
VM1-Disk1 is encrypted automatically by using Azure Disk Encryption.	<input checked="" type="radio"/>	<input type="radio"/>
VM2-Disk1 is encrypted automatically by using Azure Disk Encryption.	<input checked="" type="radio"/>	<input type="radio"/>
VM3-Disk1 is encrypted automatically by using Azure Disk Encryption.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Premium and standard, but not basic, account types support disk encryption.
 Disk encryption requires managed disks.

References:

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview>

QUESTION 166

Hotspot Question

You have an Azure subscription named Subscription1. Subscription1 contains the resources in the following table:

Name	Type
RG1	Resource group
RG2	Resource group
VNet1	Virtual network
VNet2	Virtual network

VNet1 is in RG1. VNet2 is in RG2. There is no connectivity between VNet1 and VNet2. An administrator named Admin1 creates an Azure virtual machine VM1 in RG1. VM1 uses a disk named Disk1 and connects to VNet1. Admin1 then installs a custom application in VM1. You need to move the custom application to VNet2. The solution must minimize administrative effort.

Which two actions should you perform? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

First action:

	v
Create a network interface in RG2.	
Detach a network interface.	
Delete VM1.	
Move a network interface to RG2.	

Second action:

	v
Attach a network interface.	
Create a network interface in RG2.	
Create a new virtual machine.	
Move VM1 to RG2.	

Answer:

First action:

	v
Create a network interface in RG2.	
Detach a network interface.	
Delete VM1.	
Move a network interface to RG2.	

Second action:

	v
Attach a network interface.	
Create a network interface in RG2.	
Create a new virtual machine.	
Move VM1 to RG2.	

Explanation:

We cannot just move a virtual machine between networks. What we need to do is identify the disk used by the VM, delete the VM itself while retaining the disk, and recreate the VM in the target virtual network and then attach the original disk to it.

Reference:

<https://blogs.technet.microsoft.com/canitpro/2014/06/16/step-by-step-move-a-vm-to-a-different-vnet-on-azure/>

<https://4sysops.com/archives/move-an-azure-vm-to-another-virtual-network-vnet/#migrate-an-azure-vm-between-vnets>

QUESTION 167

Hotspot Question

You have a web server app named App1 that is hosted in three Azure regions.

You plan to use Azure Traffic Manager to distribute traffic optimally for App1.

You need to enable Real User Measurements to monitor the network latency data for App1.

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

NOTE: Each correct selection is worth one point.

From the Traffic Manager profile:

Select Generate key.
Enable Traffic view.
Configure the Diagnostics settings.
Add a custom header.

From App1:

Embed the Traffic Manager JavaScript code snippet.
Embed the Azure Application Insights JavaScript code snippet.
Configure the Diagnostics settings.
Configure the Application settings.

Answer:

From the Traffic Manager profile:

Select Generate key.
Enable Traffic view.
Configure the Diagnostics settings.
Add a custom header.

From App1:

Embed the Traffic Manager JavaScript code snippet.
Embed the Azure Application Insights JavaScript code snippet.
Configure the Diagnostics settings.
Configure the Application settings.

Explanation:

Box 1: Select Generate key

You can configure your web pages to send Real User Measurements to Traffic Manager by obtaining a Real User Measurements (RUM) key and embedding the generated code to web page.

Obtain a Real User Measurements key

The measurements you take and send to Traffic Manager from your client application are identified by the service using a unique string, called the Real User Measurements (RUM) Key. You can get a RUM key using the Azure portal, a REST API, or by using the PowerShell or Azure CLI.

To obtain the RUM Key using Azure portal:

- From a browser, sign in to the Azure portal. If you don't already have an account, you can sign up for a free one-month trial.
- In the portal's search bar, search for the Traffic Manager profile name that you want to modify, and then click the Traffic Manager profile in the results that are displayed. ?In the Traffic Manager profile blade, click Real User Measurements under Settings.
- Click Generate Key to create a new RUM Key.

Box 2: Embed the Traffic Manager JavaScript code snippet.

Embed the code to an HTML web page

After you have obtained the RUM key, the next step is to embed this copied JavaScript into an HTML page that your end users visit.

This example shows how to update an HTML page to add this script. You can use this guidance to adapt it to your HTML source management workflow.

- Open the HTML page in a text editor
- Paste the JavaScript code you had copied in the earlier step to the BODY section of the HTML (the copied code is on line 8 & 9, see figure 3).

```
1 <HTML>
2 <HEAD>
3 <TITLE>Webpage powered by Azure</TITLE>
4 </HEAD>
5 <BODY BGCOLOR="#FFFFFF">
6 <H1>Welcome</H1>
7 <P> <B>Hello!</B>
8 <script src="//www.atmrum.net/rum.js"></script>
9 <script>rum.start("0123456789abcdef0123456789abcdff");</script>
10 </BODY>
11 </HTML>
```

Reference:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-create-rum-web-pages>

QUESTION 168

You have an Active Directory forest named contoso.com.

You install and configure Azure AD Connect to use password hash synchronization as the single sign-on (SSO) method. Staging mode is enabled.

You review the synchronization results and discover that the Synchronization Service Manager does not display any sync jobs.

You need to ensure that the synchronization completes successfully.

What should you do?

- A. Run Azure AD Connect and disable staging mode.
- B. From Synchronization Service Manager, run a full import.
- C. Run Azure AD Connect and set the SSO method to Pass-through Authentication.
- D. From Azure PowerShell, run Start-AdSyncSyncCycle -PolicyType Initial.

Answer: A

Explanation:

In staging mode, the server is active for import and synchronization, but it does not run any exports. A server in staging mode is not running password sync or password writeback, even if you selected these features during installation. When you disable staging mode, the server starts exporting, enables password sync, and enables password writeback.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-staging-server>

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-operations>

QUESTION 169

Your on-premises network contains 100 virtual machines that run Windows Server 2019.

You have an Azure subscription that contains an Azure Log Analytics workspace named Workspace1.

You need to collect errors from the Windows event logs on the virtual machines.

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

NOTE: Each correct selection is worth one point.

- A. Create an Azure Event Grid domain.
- B. Deploy the Microsoft Monitoring Agent.
- C. Configure Windows Event Forwarding on the virtual machines.
- D. Create an Azure Sentinel workspace.
- E. Configure the Data Collection settings for Workspace1.

Answer: BE

Explanation:

The Azure Log Analytics agent collects telemetry from Windows and Linux virtual machines in any cloud, on-premises machines, and those monitored by System Center Operations Manager and sends it collected data to your Log Analytics workspace in Azure Monitor.

Note: You may also see the Log Analytics agent referred to as the Microsoft Monitoring Agent (MMA) or OMS Linux agent.

Data is collected using the Log Analytics agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/log-analytics-agent>

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

QUESTION 170

You have an Azure subscription named Subscription1.

You deploy a Linux virtual machine named VM1 to Subscription1.

You need to monitor the metrics and the logs of VM1.

What should you use?

- A. Azure HDInsight
- B. Azure Analysis Services
- C. Linux Diagnostic Extension (LAD) 3.0
- D. the AzurePerformanceDiagnostics extension

Answer: D

Explanation:

You can use extensions to configure diagnostics on your VMs to collect additional metric data. The basic host metrics are available, but to see more granular and VM-specific metrics, you need to install the Azure diagnostics extension on the VM. The Azure diagnostics extension allows additional monitoring and diagnostics data to be retrieved from the VM.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/linux/tutorial-monitoring>

QUESTION 171

You manage an Active Directory domain named contoso.local.

You install Azure AD Connect and connect to an Azure Active Directory (Azure AD) tenant named contoso.com without syncing any accounts.

You need to ensure that only users who have a UPN suffix of contoso.com in the contoso.local domain sync to Azure AD.

What should you do?

- A. Use the Synchronization Service Manager to modify the Metaverse Designer tab.
- B. Use Azure AD Connect to customize the synchronization options.
- C. Use the Synchronization Rules Editor to create a synchronization rule.
- D. Use Synchronization Service Manager to modify the Active Directory Domain Services (AD DS) Connector.

Answer: C

Explanation:

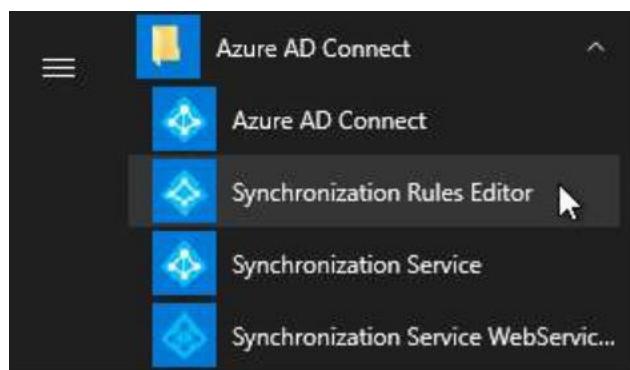
Filtering what objects are synced to Azure AD is a common request and there are many instances where filtering by OU just doesn't cut it. One option is to filter users by their UPN suffix so that only users with the public FQDN as their UPN suffix are synced to Azure AD (e.g., john.doe@acme.com would be synced while jane.doe@internal.acme.com would not).

Filtering can be configured using either the GUI or PowerShell.

Through GUI:

Using The Synchronization Rules Editor

1. Open the Synchronization Rules Editor on the server where Azure AD Connect is installed.

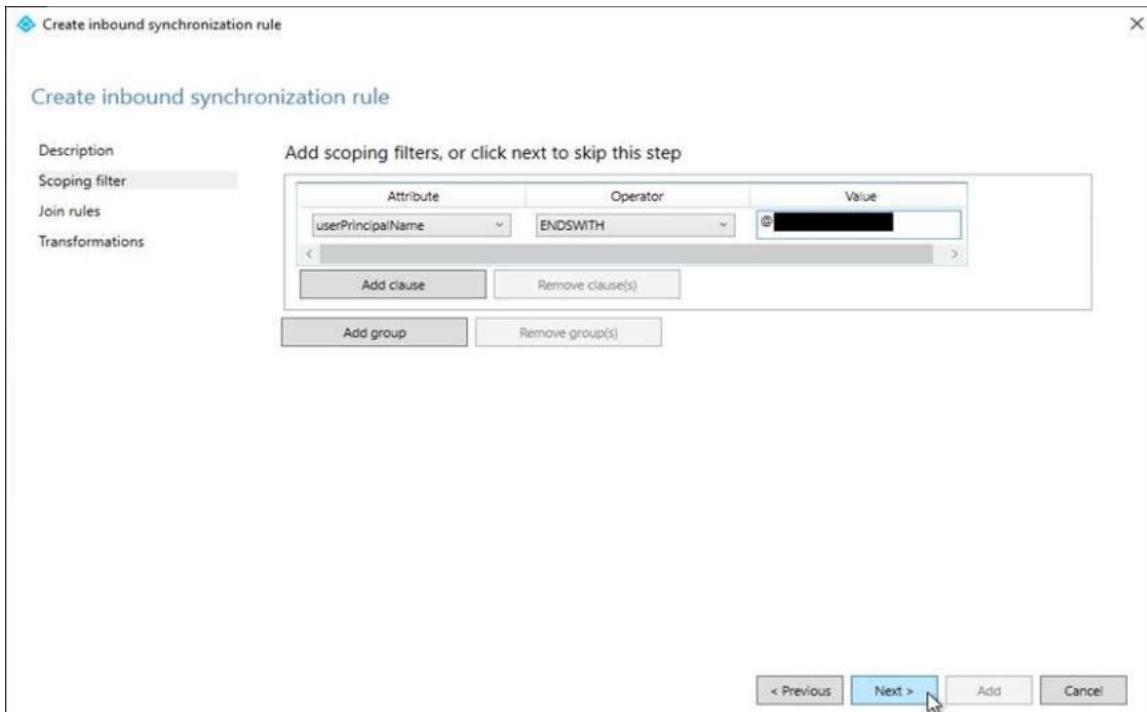


2. Click the Add new rule button on the View and manage your synchronization rules window.
3. Fill out the appropriate fields on the Description tab and click Next >.
4. On the Scoping filter tab, click Add group, then Add clause, add a userPrincipalName attribute filter, and click Next >.

Attribute: userPrincipalName

Operator: ENDSWITH

Value: Your internal UPN suffix prefixed with @ (e.g., @internal.acme.com). Users with this UPN suffix will NOT be synced with Office 365.



Reference:

<https://www.sidekicktech.com/blog/field-notes/2019/upn-suffix-filtering-ad-connect/>

QUESTION 172

You have an Azure SQL database named DB1.

You plan to create the following four tables in DB1 by using the following code.

Table1.

```
CREATE TABLE Table1
(
    StudentId INT IDENTITY PRIMARY KEY,
    PersonId INT REFERENCES Table4 (PersonId),
    Email NVARCHAR(256)
)
```

Table2.

```
CREATE TABLE Table2
(
    StudentId INT REFERENCES Table1 (StudentId),
    CourseId INT REFERENCES Table3 (CourseId),
    Grade DECIMAL(5,2) CHECK (Grade <= 100.00),
    Attempt TINYINT
)
```

Table3.

```
CREATE TABLE Table3
(
    CourseId INT IDENTITY PRIMARY KEY,
    Name NVARCHAR(56) NOT NULL,
    Teacher NVARCHAR(256) NOT NULL
)
```

Table4.

```
CREATE TABLE Table4
(
    PersonId INT IDENTITY PRIMARY KEY,
    FirstName NVARCHAR(128) NOT NULL,
    MiddleInitial NVARCHAR(10),
    LastName NVARCHAR(128) NOT NULL,
    DateOfBirth DATE NOT NULL
)
```

You need to identify which table must be created last.

What should you identify?

- A. Table1
- B. Table2
- C. Table3
- D. Table4

Answer: B

Explanation:

Table1 references Table4. Therefore Table4 must be created before Table1.

Table2 references Table1 and Table3. Therefore Table1 and Table3 must be created before Table2.

Note: FOREIGN KEY REFERENCES is a constraint that provides referential integrity for the data in the column or columns. FOREIGN KEY constraints require that each value in the column exists in the corresponding referenced column or columns in the referenced table. FOREIGN KEY constraints can reference only columns that are PRIMARY KEY or UNIQUE constraints in the referenced table or columns referenced in a UNIQUE INDEX on the referenced table.

Incorrect Answers:

- A: Table1 is referenced by Table2 and should be created before Table2.
- C: Table3 is referenced by Table2 and should be created before Table2.
- D: Table4 is referenced by Table1 and should be created before Table1.

Reference:

<https://docs.microsoft.com/en-us/sql/t-sql/statements/create-table-transact-sql?view=sql-server-ver15>

QUESTION 173

You have an Azure Cosmos DB account named Account1. Account1 includes a database named DB1 that contains a container named Container1. The partition key for Container1 is set to /city.

You plan to change the partition key for Container1.

What should you do first?

- A. Delete Container1.
- B. Create a new Azure Cosmos DB account.
- C. Implement the Azure Cosmos DB.NET.SDK.
- D. Regenerate the keys for Account1.

Answer: B

Explanation:

The Change Feed Processor and Bulk Executor Library, in Azure Cosmos DB can be leveraged to achieve a live migration of your data from one container to another. This allows you to redistribute your data to match the desired new partition key scheme, and make the relevant application changes afterwards, thus achieving the effect of "updating your partition key".

Incorrect Answers:

- A: It is not possible to "update" your partition key in an existing container.

Reference:

<https://devblogs.microsoft.com/cosmosdb/how-to-change-your-partition-key/>

QUESTION 174

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 an app named App1 that uses data from two on-premises Microsoft SQL Server databases named DB1 and DB2.

You plan to move DB1 and DB2 to Azure.

You need to implement Azure services to host DB1 and DB2. The solution must support server-side transactions across DB1 and DB2.

Solution: You deploy DB1 and DB2 as Azure SQL databases each on a different Azure SQL Database server.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead deploy DB1 and DB2 to SQL Server on an Azure virtual machine.

Note: Understanding distributed transactions.

When both the database management system and client are under the same ownership (e.g. when SQL Server is deployed to a virtual machine), transactions are available and the lock duration can be controlled.

Reference:

<https://docs.particular.net/nservicebus/azure/understanding-transactionality-in-azure>

QUESTION 175

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 an app named App1 that uses data from two on-premises Microsoft SQL Server databases named DB1 and DB2.

You plan to move DB1 and DB2 to Azure.

You need to implement Azure services to host DB1 and DB2. The solution must support server-side transactions across DB1 and DB2.

Solution: You deploy DB1 and DB2 as Azure SQL databases on the same Azure SQL Database server.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead deploy DB1 and DB2 to SQL Server on an Azure virtual machine.

Note: Understanding distributed transactions.

When both the database management system and client are under the same ownership (e.g. when SQL Server is deployed to a virtual machine), transactions are available and the lock duration can be controlled.

Reference:

<https://docs.particular.net/nservicebus/azure/understanding-transactionality-in-azure>

QUESTION 176

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 2019. Server1 is a container host.

You are creating a Dockerfile to build a container image.

You need to add a file named File1.txt from Server1 to a folder named C:\Folder1 in the container image.

Solution: You add the following line to the Dockerfile.

Copy-Item File1.txt C:\Folder1\File1.txt

You then build the container image.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Copy is the correct command to copy a file to the container image.

Reference:

https://docs.docker.com/develop/develop-images/dockerfile_best-practices/#add-or-copy

<https://docs.docker.com/engine/reference/builder/>

QUESTION 177

You create an Azure Kubernetes Service (AKS) cluster configured as shown in the exhibit. (Click the Exhibit tab.)

The screenshot shows the 'Create Kubernetes cluster' wizard in the Microsoft Azure portal. The validation step has passed, and the configuration details are as follows:

Category	Setting
Subscription	Subscription1
Resource group	RG1
Region	(Europe) North Europe
Kubernetes cluster name	AKScluster1
Kubernetes version	1.14.8
DNS name prefix	AKScluster1-dns
Node count	2
Node size	Standard_B2s
Virtual nodes	Disabled
VM scale sets	Disabled
Enable RBAC	Yes
HTTP application routing	No
Load balancer	Standard
Network configuration	Basic
Enable container monitoring	Yes
Log Analytics workspace	Workspace852
(none)	

At the bottom, there are buttons for 'Create', '< Previous' and 'Next >', and a link to 'Download a template for automation'.

You deploy a containerized application named App1 to the agentPool node pool.

You need to create a containerized application named App2 that runs on four nodes of size DS3 v2.

What should you do first?

- A. Upgrade the AKS cluster.
- B. Create a new node pool.
- C. Modify the autoscaling settings for the agentPool node.
- D. Enable virtual nodes for the AKS cluster.

Answer: B

Explanation:

Changing the agent size is not allowed. In the future Microsoft plans to support multiple node pools wherein you can create different pools with different VM sizes.

Reference:

<https://github.com/Azure/AKS/issues/132>

QUESTION 178

You create an Azure Kubernetes Service (AKS) cluster and an Azure Container Registry.

You need to perform continuous deployments of a containerized application to the AKS cluster as soon as the image updates in the registry.

What should you use to perform the deployments?

- A. an Azure Automation runbook
- B. a kubectl script from a CRON job
- C. an Azure Resource Manager template
- D. an Azure Pipelines release pipeline

Answer: D

Explanation:

You can implement a Continuous Deployment pipeline.

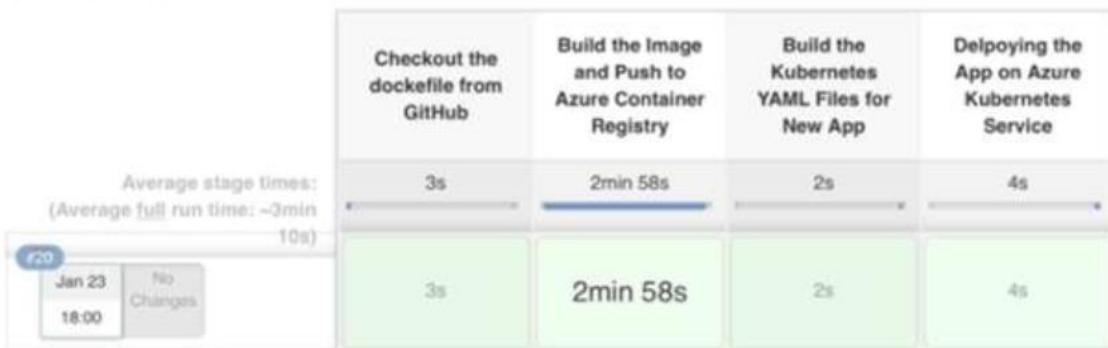
Example:

Pipeline AzurePipeline



[Recent Changes](#)

Stage View



What the pipeline accomplishes :

Stage 1: The code gets pushed in the Github. The Jenkins job gets triggered automatically. The

Dockerfile is checked out from Github.

Stage 2: Docker builds an image from the Dockerfile and then the image is tagged with the build number.

Additionally, the latest tag is also attached to the image for the containers to use.

Stage 3: We have default deployment and service YAML files stored on the Jenkins server.

Jenkins makes a copy of the default YAML files, make the necessary changes according to the build and put them in a separate folder.

Stage 4: kubectl was initially configured at the time of setting up AKS on the Jenkins server. The YAML files are fed to the kubectl util which in turn creates pods and services.

Reference:

<https://medium.com/velotio-perspectives/continuous-deployment-with-azure-kubernetes-service-azure-container-registry-jenkins-ca337940151b>

QUESTION 179

You have an Azure web app that runs in a Premium App Service plan.

Developers plan to update the app weekly.

You need to ensure that the app can be switched from the current version to the new version.

The solution must meet the following requirements:

- Provide the developers with the ability to test the app in Azure prior to switching versions.
- Testing must use the same app instance.
- Ensure that the app version can be rolled back.
- Minimize downtime.

What should you do?

- A. Create a deployment slot.
- B. Copy the App Service plan.
- C. Add an instance of the app to the scale set.
- D. Create an Azure Active Directory (Azure AD) enterprise application.

Answer: A

Explanation:

Azure Functions deployment slots allow your function app to run different instances called "slots". Slots are different environments exposed via a publicly available endpoint. One app instance is always mapped to the production slot, and you can swap instances assigned to a slot on demand.

There are a number of advantages to using deployment slots. The following scenarios describe common uses for slots:

Different environments for different purposes: Using different slots gives you the opportunity to differentiate app instances before swapping to production or a staging slot.

Easy fallbacks: After a swap with production, the slot with a previously staged app now has the previous production app. If the changes swapped into the production slot aren't as you expect, you can immediately reverse the swap to get your "last known good instance" back.

Prewarming

Reference:

<https://docs.microsoft.com/en-us/azure/azure-functions/functions-deployment-slots>

QUESTION 180

Note: This question is part of a series of questions that present the same scenario. Each

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 manage an Active Directory domain named contoso.local.

You install Azure AD Connect and connect to an Azure Active Directory (Azure AD) tenant named contoso.com without syncing any accounts.

You need to ensure that only users who have a UPN suffix of contoso.com in the contoso.local domain sync to Azure AD.

Solution: You use Azure AD Connect to customize the synchronization options.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead use Synchronization Rules Editor to create a synchronization rule.

Note: Filtering what objects are synced to Azure AD is a common request and there are many instances where filtering by OU just doesn't cut it. One option is to filter users by their UPN suffix so that only users with the public FQDN as their UPN suffix are synced to Azure AD (e.g., john.doe@acme.com would be synced while jane.doe@internal.acme.com would not).

Filtering can be configured using either the GUI (Synchronization Rules Editor) or PowerShell.

Reference:

<https://www.sidekicktech.com/blog/field-notes/2019/upn-suffix-filtering-ad-connect/>

QUESTION 181

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 manage an Active Directory domain named contoso.local.

You install Azure AD Connect and connect to an Azure Active Directory (Azure AD) tenant named contoso.com without syncing any accounts.

You need to ensure that only users who have a UPN suffix of contoso.com in the contoso.local domain sync to Azure AD.

Solution: You use Synchronization Rules Editor to create a synchronization rule.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

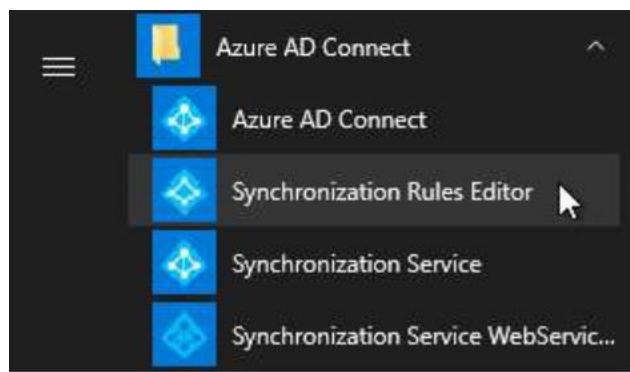
Filtering what objects are synced to Azure AD is a common request and there are many instances where filtering by OU just doesn't cut it. One option is to filter users by their UPN suffix so that only users with the public FQDN as their UPN suffix are synced to Azure AD (e.g., john.doe@acme.com would be synced while jane.doe@internal.acme.com would not).

Filtering can be configured using either the GUI or PowerShell.

Through GUI:

Using The Synchronization Rules Editor

1. Open the Synchronization Rules Editor on the server where Azure AD Connect is installed.

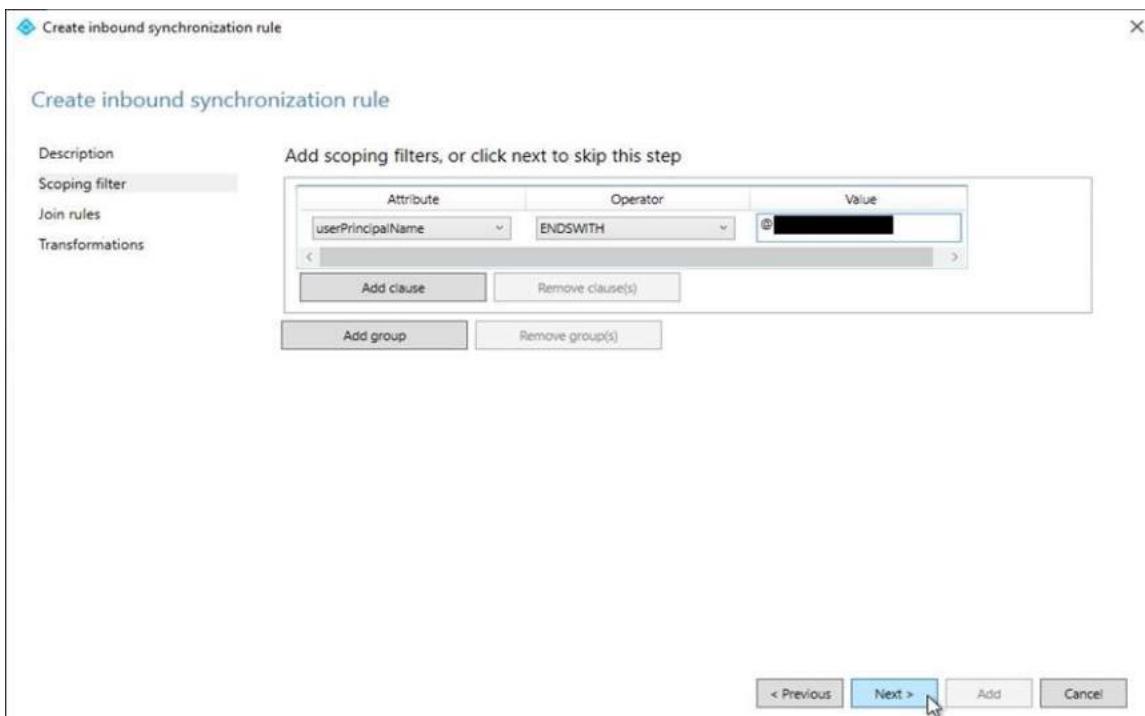


2. Click the Add new rule button on the View and manage your synchronization rules window.
3. Fill out the appropriate fields on the Description tab and click Next >.
4. On the Scoping filter tab, click Add group, then Add clause, add a userPrincipalName attribute filter, and click Next >.

Attribute: userPrincipalName

Operator: ENDSWITH

Value: Your internal UPN suffix prefixed with @ (e.g., @internal.acme.com). Users with this UPN suffix will NOT be synced with Office 365.



Reference:

<https://www.sidekicktech.com/blog/field-notes/2019/upn-suffix-filtering-ad-connect/>

QUESTION 182

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 manage an Active Directory domain named contoso.local.

You install Azure AD Connect and connect to an Azure Active Directory (Azure AD) tenant named contoso.com without syncing any accounts.

You need to ensure that only users who have a UPN suffix of contoso.com in the contoso.local domain sync to Azure AD.

Solution: You use the Synchronization Service Manager to modify the Active Directory Domain Services (AD DS) Connector.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead use Synchronization Rules Editor to create a synchronization rule.

Note: Filtering what objects are synced to Azure AD is a common request and there are many instances where filtering by OU just doesn't cut it. One option is to filter users by their UPN suffix so that only users with the public FQDN as their UPN suffix are synced to Azure AD (e.g., john.doe@acme.com would be synced while jane.doe@internal.acme.com would not).

Filtering can be configured using either the GUI (Synchronization Rules Editor) or PowerShell.

Reference:

<https://www.sidekicktech.com/blog/field-notes/2019/upn-suffix-filtering-ad-connect/>

QUESTION 183

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 an app named App1 that uses data from two on-premises Microsoft SQL Server databases named DB1 and DB2.

You plan to move DB1 and DB2 to Azure.

You need to implement Azure services to host DB1 and DB2. The solution must support server-side transactions across DB1 and DB2.

Solution: You deploy DB1 and DB2 to SQL Server on an Azure virtual machine.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Understanding distributed transactions.

When both the database management system and client are under the same ownership (e.g. when SQL Server is deployed to a virtual machine), transactions are available and the lock duration can be controlled.

Reference:

<https://docs.particular.net/nservicebus/azure/understanding-transactionality-in-azure>

QUESTION 184

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 an Azure Cosmos DB database that contains a container named Container1. The

partition key for Container1 is set to /day. Container1 contains the items shown in the following table.

Name	Content
Item1	{ "id": "1", "day": "Mon", "value": "10" }
Item2	{ "id": "2", "day": "Mon", "value": "15" }
Item3	{ "id": "3", "day": "Tue", "value": "10" }
Item4	{ "id": "4", "day": "Wed", "value": "15" }

You need to programmatically query Azure Cosmos DB and retrieve Item1 and Item2 only.

Solution: You run the following query.

```
SELECT id FROM c  
WHERE c.day = "Mon" OR c.day = "Tue"
```

You set the EnableCrossPartitionQuery property to False.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Returns Item1 only as EnableCrossPartitionQuery property to False. If EnableCrossPartitionQuery property is set to true, it will return Item1, Item2, and Item3.

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/sql-query-where>

<https://docs.microsoft.com/en-us/dotnet/api/microsoft.azure.documents.client.feedoptions.enablecrosspartitionquery?view=azur>

QUESTION 185

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 manage an Active Directory domain named contoso.local.

You install Azure AD Connect and connect to an Azure Active Directory (Azure AD) tenant named contoso.com without syncing any accounts.

You need to ensure that only users who have a UPN suffix of contoso.com in the contoso.local domain sync to Azure AD.

Solution: You use the Synchronization Service Manager to modify the Metaverse Designer tab.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead use Synchronization Rules Editor to create a synchronization rule.

Note: Filtering what objects are synced to Azure AD is a common request and there are many instances where filtering by OU just doesn't cut it. One option is to filter users by their UPN suffix so that only users with the public FQDN as their UPN suffix are synced to Azure AD (e.g., john.doe@acme.com would be synced while jane.doe@internal.acme.com would not).

Filtering can be configured using either the GUI (Synchronization Rules Editor) or PowerShell.

Reference:

<https://www.sidekicktech.com/blog/field-notes/2019/upn-suffix-filtering-ad-connect/>

QUESTION 186

Your network contains an on-premises Active Directory and an Azure Active Directory (Azure AD) tenant.

You deploy Azure AD Connect and configure pass-through authentication.

Your Azure subscription contains several web apps that are accessed from the Internet.

You plan to use Azure Multi-Factor Authentication (MFA) with the Azure Active Directory tenant.

You need to recommend a solution to prevent users from being prompted for Azure MFA when they access the web apps from the on-premises network.

What should you include in the recommendation?

- A. an Azure policy

- B. trusted IPs
- C. a site-to-site VPN between the on-premises network and Azure
- D. an Azure ExpressRoute circuit

Answer: B

Explanation:

The Trusted IPs feature of Azure Multi-Factor Authentication is used by administrators of a managed or federated tenant. The feature bypasses two-step verification for users who sign in from the company intranet. The feature is available with the full version of Azure Multi-Factor Authentication, and not the free version for administrators.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#trusted-ips>

QUESTION 187

You have the following Azure Active Directory (Azure AD) tenants:

- Contoso.onmicrosoft.com: Linked to a Microsoft Office 365 tenant and syncs to an Active Directory forest named contoso.com by using password hash synchronization
- Contosoazure.onmicrosoft.com: Linked to an Azure subscription named Subscription1

You need to ensure that you can assign the users in contoso.com access to the resources in Subscription1.

What should you do?

- A. Configure contoso.onmicrosoft.com to use pass-through authentication.
- B. Create guest accounts for all the contoso.com users in contosoazure.onmicrosoft.com.
- C. Deploy a second Azure AD Connect server and sync contoso.com to contosoazure.onmicrosoft.com.
- D. Configure Active Directory Federation Services (AD FS) federation between contosoazure.onmicrosoft.com and contoso.com.

Answer: C

Explanation:

Azure AD Connect allows you to quickly onboard to Azure AD and Office 365.

Note: The most common topology is a single on-premises forest, with one or multiple domains, and a single Azure AD tenant. For Azure AD authentication, password hash synchronization is used. The express installation of Azure AD Connect supports only this topology.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-topologies>

QUESTION 188

You have several Azure web apps that use access keys to access databases.

You plan to migrate the access keys to Azure Key Vault. Each app must authenticate by using Azure Active Directory (Azure AD) to gain access to the access keys.

What should you create in Azure to ensure that the apps can access the access keys?

- A. managed identities
- B. managed applications

- C. Azure policies
- D. an App Service plan

Answer: A

Explanation:

Azure Key Vault provides a way to securely store credentials and other secrets, but your code needs to authenticate to Key Vault to retrieve them. Managed identities for Azure resources overview helps to solve this problem by giving Azure services an automatically managed identity in Azure AD. You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having to display credentials in your code.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/tutorial-net-create-vault-azure-web-app>

QUESTION 189

You have an Azure key vault named KV1.

You need to implement a process that will digitally sign the blobs stored in Azure Storage.

What is required in KV1 to sign the blobs?

- A. a key
- B. a secret
- C. a certificate

Answer: B

Explanation:

Use an Azure key vault secret to key of your blob storage account container.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/integrate-databricks-blob-storage>

QUESTION 190

You set the multi-factor authentication status for a user named admin1@contoso.com to Enabled.

Admin1 accesses the Azure portal by using a web browser.

Which additional security verifications can Admin1 use when accessing the Azure portal?

- A. a phone call, an email message that contains a verification code, and a text message that contains an app password.
- B. an app password, a text message that contains a verification code, and a verification code sent from the Microsoft Authenticator app.
- C. an app password, a text message that contains a verification code, and a notification sent from the Microsoft Authenticator app.
- D. a phone call, a text message that contains a verification code, and a notification or a verification code sent from the Microsoft Authenticator app.

Answer: D

Explanation:

The Microsoft Authenticator app can help prevent unauthorized access to accounts and stop fraudulent transactions by pushing a notification to your smartphone or tablet. Users view the notification, and if it's legitimate, select Verify. Otherwise, they can select Deny.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

QUESTION 191

You have an Azure Cosmos DB account named Account1. Account1 includes a database named DB1 that contains a container named Container1. The partition key for Container1 is set to /city.

You plan to change the partition key for Container1.

What should you do first?

- A. Delete Container1.
- B. Create a new container in DB1.
- C. Implement the Azure Cosmos DB.NET.SDK.
- D. Regenerate the keys for Account1.

Answer: B

Explanation:

The Change Feed Processor and Bulk Executor Library, in Azure Cosmos DB can be leveraged to achieve a live migration of your data from one container to another. This allows you to redistribute your data to match the desired new partition key scheme, and make the relevant application changes afterwards, thus achieving the effect of "updating your partition key".

Incorrect Answers:

A: It is not possible to "update" your partition key in an existing container.

Reference:

<https://devblogs.microsoft.com/cosmosdb/how-to-change-your-partition-key/>

QUESTION 192

You plan to automate the deployment of a virtual machine scale set that uses the Windows Server 2016 Datacenter image.

You need to ensure that when the scale set virtual machines are provisioned, they have web server components installed.

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

NOTE: Each correct selection is worth one point.

- A. Upload a configuration script.
- B. Create an Azure policy.
- C. Modify the extensionProfile section of the Azure Resource Manager template.
- D. Create a new virtual machine scale set in the Azure portal.
- E. Create an automation account.

Answer: CD

Explanation:

<https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/tutorial-install-apps-template>

QUESTION 193

Hotspot Question

You plan to deploy five virtual machines to a virtual network subnet.

Each virtual machine will have a public IP address and a private IP address.

Each virtual machine requires the same inbound and outbound security rules.

What is the minimum number of network interfaces and network security groups that you require?
To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Minimum number of network interfaces:

5
10
15
20

Minimum number of network security groups:

1
2
5
10

Answer:

Answer Area

Minimum number of network interfaces:

5
10
15
20

Minimum number of network security groups:

1
2
5
10

Explanation:

Box 1: 5

We have five virtual machines. Each virtual machine will have a public IP address and a private IP address. Each will require a network interface. A public and a private IP address can be assigned to a single network interface.

Box 2: 1

Each virtual machine requires the same inbound and outbound security rules. We can add them to one group.

Reference:

<https://blogs.msdn.microsoft.com/igorpag/2016/05/14/azure-network-security-groups-nsg-best-practices-and-lessons-learned/>

<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-multiple-ip-addresses-portal>

QUESTION 194

Hotspot Question

You deploy an Azure virtual machine scale set named VSS1 that contains 30 virtual machine instances across three zones in the same Azure region. The instances host an application named App1 that must be accessible by using HTTP and HTTPS traffic. Currently, VSS1 is inaccessible from the internet.

You need to use Azure Load Balancer to provide access to App1 across all the instances from the internet by using a single IP address.

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

NOTE: Each correct selection is worth one point.

Answer Area

Minimum number of network security groups (NSGs) to create:

1
3
30

Objects to assign to the network security groups (NSGs):

1 subnet
3 subnets
30 network interfaces

Minimum number of Azure Standard Load Balancer rules to create:

1
2
3
4
6

Answer:

Answer Area

Minimum number of network security groups (NSGs) to create:

1
3
30

Objects to assign to the network security groups (NSGs):

1 subnet
3 subnets
30 network interfaces

Minimum number of Azure Standard Load Balancer rules to create:

1
2
3
4
6

Explanation:

Box 1: 1

Box 2: 30 network interfaces

For a standard load balancer, the VMs in the backend address for are required to have network interfaces that belong to a network security group.

Box 3: 2

On for the HTTP traffic, and one for the HTTPS traffic.

Reference:

<https://docs.microsoft.com/en-us/azure/load-balancer/quickstart-load-balancer-standard-public-cli>

QUESTION 195

Hotspot Question

You have an Azure subscription that contains the resources shown in the following table.

Name	Type	Size
ILB1	Internal load balancer	Basic
ELB1	External load balancer	Standard
AGW1	Azure Application Gateway that has web application firewall (WAF) enabled	Standard
AGW2	Azure Application Gateway	Standard_v2

You need to deploy a load-balancing solution for two Azure web apps named App1 and App2 to meet the following requirements:

- App1 must support command injection protection.
- App2 must be able to use a static IP address.
- App1 must have a Service Level Agreement (SLA) of 99.99 percent.

Which resource should you use as the load-balancing solution for each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

App1:	
ILB1	
ELB1	
AGW1	
AGW2	

App2:	
ILB1	
ELB1	
AGW1	
AGW2	

Answer:

Answer Area

App1:	
ILB1	
ELB1	
AGW1	
AGW2	

App2:	
ILB1	
ELB1	
AGW1	
AGW2	

Explanation:

Box 1: AGW1

Azure Application Gateway offers a web application firewall (WAF) that provides centralized protection of your web applications from common exploits and vulnerabilities. Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. SQL injection and cross-site scripting are among the most common attacks.

Box 2: ELB1

Public IP addresses allow Internet resources to communicate inbound to Azure resources. Public IP addresses also enable Azure resources to communicate outbound to Internet and public-facing Azure services with an IP address assigned to the resource.

Note: In Azure Resource Manager, a public IP address is a resource that has its own properties.

Some of the resources you can associate a public IP address resource with are:

- Virtual machine network interfaces
- Internet-facing load balancers
- VPN gateways
- Application gateways

Reference:

<https://docs.microsoft.com/en-us/azure/application-gateway/waf-overview>

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-ip-addresses-overview-arm>

QUESTION 196

Hotspot Question

You plan to implement an access review to meet the following requirements:

- The access review must be enforced until otherwise configured.
- Each user or group that has access to the Azure environment must be in the scope of the access review.
- The access review must be completed within two weeks.
- A lack of response must not cause changes in the operational environment.
- An administrator creates the access review shown in the answer area.

Which two sections of the access review should you modify to meet the requirements? To answer, select the appropriate sections in the answer area.

NOTE: Each correct selection is worth one point.

Microsoft Azure 1

Home > Identity Governance > Create an access review

Create an access review

Review name * ✓

Description *

Start date * ✓

Frequency ✓

Duration (in days) * ✓

End * Never End by Occurrences

Number of times

End date * ✓

Users

Users to review ✓

Scope Guest users only Everyone

* Group ✓

Reviewers

Reviewers ✓

Programs

Link to program ✓

Upon completion settings

Auto apply results to resource

If reviewers don't respond ✓

Advanced settings

Show recommendations

Require reason on approval

Mail notifications

Reminders

Answer:

Microsoft Azure Search resources, services, and docs (G+)

Home > Identity Governance > Create an access review

Create an access review

Review name* ✓

Description*

Start date* ✓

Frequency

Duration (in days)* ✓

End* Never End by Occurrences

Number of times

End date* ✓

Users

Users to review

Scope Guest users only Everyone

Group ✓

Reviewers

Reviewers

Programs

Link to program ✓

Upon completion settings

Auto apply results to resource Enable Disable

If reviewers don't respond Remove access

Advanced settings

Show recommendations Enable Disable

Require reason on approval Enable Disable

Mail notifications Enable Disable

Reminders Enable Disable

Start

Explanation:

Area 1: Start date..End Date

The access review must be enforced until otherwise configured. We set End: Never

The access review must be completed within two weeks. We set Duration (in days) to 14

Area 2: Upon completion settings

A lack of response must not cause changes in the operational environment. We set 'If reviewers don't respond: No change (which leave user's access unchanged)

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

QUESTION 197

You have an Azure virtual network that contains a subnet named Subnet1. Subnet1 contains 50 virtual machines. Twenty-five of the virtual machines are web servers and the other 25 are application servers.

You need to filter traffic the web servers and the application servers by using application security groups.

Which additional resources should you provision?

- A. Azure Private Link
- B. a network security group (NSG)
- C. a user-defined route
- D. Azure-firewall

Answer: B

QUESTION 198

Your on-premises network contains several Hyper-V hosts. You have an hybrid deployment of Azure Active Directory (Azure AD).

You create an Azure Migrate project.

You need to ensure that you can evaluate virtual machines by using Azure Migrate.

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

NOTE: Each correct selection is worth one point.

- A. Deploy the Azure Migrate appliance to an on-premises Hyper-V host.
- B. Deploy the Microsoft Monitoring Agent to each Hyper-V virtual machine.
- C. Assign the migrate account to the administrator group on each Hyper-V host.
- D. Deploy the Azure Migrate appliance as an Azure virtual machine.
- E. Deploy the Microsoft Monitoring Agent to each Hyper-V host.
- F. Assign the migrate account to the Administrators group on each Hyper-V virtual machine.

Answer: BC

QUESTION 199

You have an Azure subscription that contains the Azure SQL Database servers shown in the following table.

Name	Resource group	Location
SQL1	RG1	West US
SQL2	RG2	West US

The SQL Database servers have the elastic pools shown in the following table.

Name	SQL Database server	vCores	Maximum data size
Pool1	SQL1	2	16 GB
Pool2	SQL2	6	48 GB

SQL1 has the SQL databases shown in the following table.

Name	SQL Database server	vCores	Maximum data size	Elastic pool
DB1	SQL1	4	30 GB	<i>None</i>
DB2	SQL1	2	10 GB	Pool1

What will occur if you add DB1 to Pool1?

- A. The vCores on DB1 will decrease to two.
- B. The maximum data size of Pool1 will increase to 22 GB.
- C. The maximum data size of DB1 will decrease to 6 GB.
- D. The vCores on Pool1 will increase to four.

Answer: D

QUESTION 200

You have an Azure Storage account named storage1 that is accessed by several applications. An administrator manually rotates the access keys for storage1. After the rotation the applications fail to access the storage account. A developer manually modifies the applications to resolve the issue. You need to implement a solution to rotate the access keys automatically. The solution must minimize the need to update the applications once the solution is implemented.

What should you include in the solution?

- A. Azure Key Vault
- B. an Azure Desired State Configuration (DSC) extension
- C. Azure Logic Apps
- D. an Azure AD enterprise application

Answer: B

QUESTION 201

You download an Azure Resource Manager template based on an existing virtual machine. The template will be used to deploy 100 virtual machines.

You need to modify the template to reference an administrative password.

You must prevent the password from being stored in plain text.

What should you create to store the password?

- A. a Recovery Services vault and a backup policy
- B. an Azure Key Vault and an access policy
- C. an Azure Storage account and an access policy
- D. Azure Active Directory (AD) identity protection and an Azure policy

Answer: B

QUESTION 202

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 an app named App1 that uses data from two on-premises Microsoft SQL Server databases named DB1 and DB2.

You plan to move DB1 and DB2 to Azure.

You need to implement Azure services to host DB1 and DB2. The solution must support server-side transactions across DB1 and DB2.

Solution: You deploy DB1 and DB2 to an Azure SQL Database managed instance.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

QUESTION 203

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 an app named App1 that uses data from two on-premises Microsoft SQL Server databases named DB1 and DB2.

You plan to move DB1 and DB2 to Azure.

You need to implement Azure services to host DB1 and DB2. The solution must support server-side transactions across DB1 and DB2.

Solution: You deploy DB1 and DB2 as Azure SQL databases on the same Azure SQL Database server.

Does this meet the goal?

- A. Yes
- B. NO

Answer: B

QUESTION 204

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 an Azure Cosmos DB database that contains a container named Container1. The partition key for Container1 is set to /day. Container1 contains the items shown in the following table.

Name	Content
Item1	{ "id": "1", "day": "Mon", "value": "10" }
Item2	{ "id": "2", "day": "Mon", "value": "15" }
Item3	{ "id": "3", "day": "Tue", "value": "10" }
Item4	{ "id": "4", "day": "Wed", "value": "15" }

You need to programmatically query Azure Cosmos DB and retrieve Item1 and Item2 only.

Solution: You run the following query.

```
SELECT day  
WHERE value = "10"
```

You set the `EnableCrossPartitionQuery` property to `False`.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Returns Item1 only as EnableCrossPartitionQuery property to False. If EnableCrossPartitionQuery property is set to true, it will return Item1 and Item3.

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/sql-query-where>

QUESTION 205

You have an Azure subscription that contains an Azure Sentinel workspace. Sentinel is configured to monitor several Azure resources.

You need to send notification emails to resource owners when alerts or recommendations are generated for a resource.

What should you use?

- A. Logic Apps Designer
- B. Azure Security Center
- C. Azure Pipelines
- D. Azure Machine Learning Studio

Answer: A

Explanation:

Currently there is no built-in functionality that notifies you via email if there is an incident that is generated in Azure Sentinel. However, you can set up an Azure Logic App playbook to send incident information to your email.

Reference:

<https://azsec.azurewebsites.net/2020/01/19/notify-azure-sentinel-alert-to-your-email-automatically/>

QUESTION 206

Hotspot Question

You have an Azure subscription named Subscription1.

Subscription1 contains the virtual machines in the following table:

Name	IP address
VM1	10.0.1.4
VM2	10.0.2.4
VM3	10.0.3.4

Subscription1 contains a virtual network named VNet1 that has the subnets in the following table.

Name	Address space	Connected virtual machine
Subnet1	10.0.1.0/24	VM1
Subnet2	10.0.2.0/24	VM2
Subnet3	10.0.3.0/24	VM3

VM3 has multiple network adapters, including a network adapter named NIC3. IP forwarding is enabled on NIC3. Routing is enabled on VM3.

You create a route table named RT1 that contains the routers in the following table.

Address prefix	Next hop type	Next hop address
10.0.1.0/24	Virtual appliance	10.0.3.4
10.0.2.0/24	Virtual appliance	10.0.3.4

You apply RT1 to Subnet1 and Subnet2.

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 Area

- | Statements | Yes | No |
|---|-----------------------|-----------------------|
| VM3 can establish a network connection to VM1. | <input type="radio"/> | <input type="radio"/> |
| If VM3 is turned off VM2 can establish a network connection to VM1. | <input type="radio"/> | <input type="radio"/> |
| VM1 can establish a network connection to VM2. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

- | Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| VM3 can establish a network connection to VM1. | <input checked="" type="radio"/> | <input type="radio"/> |
| If VM3 is turned off VM2 can establish a network connection to VM1. | <input type="radio"/> | <input checked="" type="radio"/> |
| VM1 can establish a network connection to VM2. | <input checked="" type="radio"/> | <input type="radio"/> |

Explanation:

IP forwarding enables the virtual machine a network interface is attached to:

- Receive network traffic not destined for one of the IP addresses assigned to any of the IP configurations assigned to the network interface.
- Send network traffic with a different source IP address than the one assigned to one of a network interface's IP configurations.

The setting must be enabled for every network interface that is attached to the virtual machine that receives traffic that the virtual machine needs to forward. A virtual machine can forward traffic whether it has multiple network interfaces or a single network interface attached to it.

Box 1: Yes

The routing table allows connections from VM3 to VM1 and VM2. And as IP forwarding is enabled on VM3, VM3 can connect to VM1.

Box 2: No

VM3, which has IP forwarding, must be turned on, in order for VM2 to connect to VM1.

Box 3: Yes

The routing table allows connections from VM1 and VM2 to VM3. IP forwarding on VM3 allows VM1 to connect to VM2 via VM3.

References:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>

<https://www.quora.com/What-is-IP-forwarding>

QUESTION 207

Hotspot Question

Your network contains an on-premises Active Directory domain. The domain contains the Hyper-V failover clusters shown in the following table.

Name	Number of nodes	Number of virtual machines
Cluster1	2	12
Cluster2	4	10
Cluster3	6	40

You plan to assess and migrate the virtual machines by using Azure Migrate.

What is the minimum number of Azure Migrate appliances and Microsoft Azure Recovery Services (MARS) agents required?

NOTE: Each correct select is worth one point.



Answer:

Azure Migrate appliances:	<table border="1"><tr><td>1</td></tr><tr><td>2</td></tr><tr><td>3</td></tr><tr><td>4</td></tr></table>	1	2	3	4
1					
2					
3					
4					
MARS agents:	<table border="1"><tr><td>1</td></tr><tr><td>2</td></tr><tr><td>3</td></tr><tr><td>4</td></tr></table>	1	2	3	4
1					
2					
3					
4					

QUESTION 208

Hotspot Question

You have an Azure subscription that contains the virtual networks shown in the following table.

Name	Location	Virtual machine
Vnet1	North Europe	VM1
Vnet2	West Europe	VM2

You create an Azure Cosmos DB account as shown in the exhibit.

For each of the following statements, select yes if the statement is true. Otherwise, select no.

Answer Area

Statements	Yes	No
Cosmos75246 is accessible by using a public IP address.	<input type="radio"/>	<input type="radio"/>
VM1 can read from cosmos75246.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can read from cosmos75246.	<input type="radio"/>	<input checked="" type="radio"/>

Answer:

Answer Area

Statements	Yes	No
Cosmos75246 is accessible by using a public IP address.	<input checked="" type="radio"/>	<input type="radio"/>
VM1 can read from cosmos75246.	<input type="radio"/>	<input checked="" type="radio"/>
VM2 can read from cosmos75246.	<input type="radio"/>	<input checked="" type="radio"/>

QUESTION 209

Hotspot Question

You have an Azure subscription named Subscription1.

In Subscription1, you create an alert rule named Alert1. The Alert1 action group is configured as shown in the following exhibit.

```
PS Azure:> Get-AzureRmActionGroup

ResourceGroupName: default-activitylogalerts
GroupShortName: AG1
Enabled: True
EmailReceivers: {Action1_-EmailAction-}
SmsReceivers: {Action1_-SMSAction-}
WebhookReceivers: {}
Id: /subscriptions/a4fde29b-d56a-4f6c-8298-6c53cd0b720c/resourceGroups/default-activitylogalerts/providers/microsoft.insights/actionGroups/ActionGroup1
Name: ActionGroup1
Type: Microsoft.Insights/ActionGroups
Location: Global
Tags: {}
```

Alert1 alert criteria is triggered every minute.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

The number of email messages that Alert1 will send in an hour is [answer choice].

0
4
6
12
60

The number of SMS messages that Alert1 will send in an hour is [answer choice].

0
4
6
12
60

Answer:

The number of email messages that Alert1 will send in an hour is [answer choice].

0
4
6
12
60

The number of SMS messages that Alert1 will send in an hour is [answer choice].

0
4
6
12
60

Explanation:

Box 1: 60

One alert per minute will trigger one email per minute.

Box 2: 12

No more than 1 SMS every 5 minutes can be send, which equals 12 per hour. Note: Rate limiting is a suspension of notifications that occurs when too many are sent to a particular phone number, email address or device. Rate limiting ensures that alerts are manageable and actionable.

The rate limit thresholds are:

SMS: No more than 1 SMS every 5 minutes.

Voice: No more than 1 Voice call every 5 minutes.

Email: No more than 100 emails in an hour.

Other actions are not rate limited.

References:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/monitoring-and-diagnostics/monitoring-overview-alerts.md>

QUESTION 210

Hotspot Question

You have an on-premises data center and an Azure subscription. The data center contains two VPN devices. The subscription contains an Azure virtual network named VNet1. VNet1 contains a gateway subnet.

You need to create a site-to-site VPN. The solution must ensure that if a single instance of an Azure VPN gateway fails, or a single on-premises VPN device fails, the failure will not cause an interruption that is longer than two minutes.

What is the minimum number of public IP addresses, virtual network gateways, and local network gateways required in Azure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area:

Public IP addresses:

1
2
3
4

Virtual network gateways:

1
2
3
4

Local network gateways:

1
2
3
4

Answer:

Answer Area:

Public IP addresses:

▼
1
2
3
4

Virtual network gateways:

▼
1
2
3
4

Local network gateways:

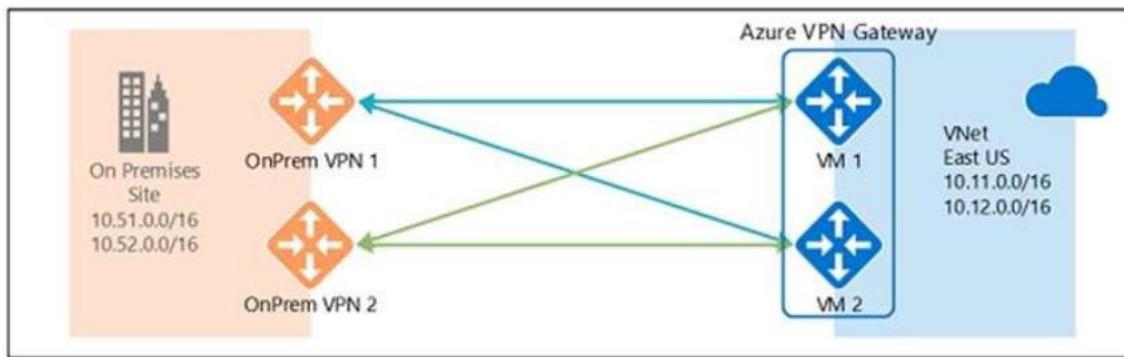
▼
1
2
3
4

Explanation:

Box 1: 4

Two public IP addresses in the on-premises data center, and two public IP addresses in the VNET.

The most reliable option is to combine the active-active gateways on both your network and Azure, as shown in the diagram below.



Box 2: 2

Every Azure VPN gateway consists of two instances in an active-standby configuration. For any planned maintenance or unplanned disruption that happens to the active instance, the standby instance would take over (failover) automatically, and resume the S2S VPN or VNet-to-VNet connections.

Box 3: 2

Dual-redundancy: active-active VPN gateways for both Azure and on-premises networks

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-highlyavailable>

QUESTION 211

You are creating an app that will transcribe speech-to-text in Chinese. The app will use the Speech service in Azure and will authenticate by using a service principal. You configure the app to use the Application ID of the service principal and the client secret. Which other value should you add to the app to authenticate to the Speech service?

- A. Subscription ID
- B. Tenant ID
- C. Application Name
- D. Resource Group ID

Answer: D

QUESTION 212

You have an Azure subscription that contains the resources shown in the following table.

Name	Type
Vault1	Azure Key vault
VM1	Virtual machine
VM2	Virtual machine

A certificate named Certificate1 is stored in Vault1. You need to grant VM1 and VM2 access to Certificate1 by using the same security principal. What should you do?

- A. Create an Azure Active Directory (Azure AD) user.
Create an access policy for Vault1.
Assign the access policy to the user.
Configure a user-assigned managed identity for VM1 and VM2.
- B. Create a managed identity.
Assign the Key Vault Reader role-based access control (RBAC) role for Vault1 to the managed identity.
Configure a system-assigned managed identity for VM1 and VM2.
- C. Create an Azure Active Directory (Azure AD) user.
Assign the Key Vault Reader role-based access control (RBAC) role for Vault1 to the user.
Configure a user-assigned managed identity for VM1 and VM2.
- D. Create a managed identity.
Add the Vault1 access policy to the managed identity.
Configure a user-assigned managed identity for VM1 and VM2.

Answer: C

QUESTION 213

You manage a solution in Azure that consists of a single application which runs on a virtual machine (VM). Traffic to the application has increased dramatically. The application must not experience any downtime and scaling must be dynamically defined. You need to define an auto-scale strategy to ensure that the VM can handle the workload. Which three options should you recommend? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Deploy application automatic vertical scaling.
- B. Create a VM availability set.
- C. Create a VM scale set.
- D. Deploy application automatic horizontal scaling.
- E. Deploy a custom auto-scale implementation.

Answer: CDE

QUESTION 214

Note: This question is part of 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 an Azure Active Directory (Azure AD) tenant named contoso.com. A user named Admin1 attempts to create an access review from the Azure Active Directory admin center and discovers that the Access reviews settings are unavailable. Admin1 discovers that all the other Identity Governance settings are available, Admin1 is assigned the User administrator, Compliance administrator, and Security administrator roles.

You need to ensure that Admin1 can create access reviews in contoso.com.

Solution: You purchase an Azure Active Directory Premium P2 license for contoso.com.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

QUESTION 215

You monitor Azure virtual machines by using Azure Monitor.

You plan to restart the virtual machines when CPU usage exceeds 95 percent for more than 30 minutes.

You need to create an alert in Azure Monitor to restart the virtual machines.

The solution must minimize administrative effort.

Which type of action should you use in the alert?

- A. Automation Runbook
- B. Logic App
- C. Webhook
- D. ITSM

Answer: A

Explanation:

Automation runbooks allows you to automatically perform standard remediations in response to VM alerts, like restarting or stopping the VM.

Previously, during VM alert rule creation you were able to specify an Automation webhook to a

runbook in order to run the runbook whenever the alert triggered. However, this required you to do the work of creating the runbook, creating the webhook for the runbook, and then copying and pasting the webhook during alert rule creation. With this new release, the process is much easier because you can directly choose a runbook from a list during alert rule creation, and you can choose an Automation account which will run the runbook or easily create an account.

Reference:

<https://azure.microsoft.com/en-us/blog/automatically-remediate-azure-vm-alerts-with-automation-runbooks/>

QUESTION 216

You have an Azure subscription that contains a policy-based virtual network gateway named GW1 and a virtual network named Vnet1.

You need to ensure that you can configure a point to-site connection from an on-premises computer to VNet1.

Which two actions should you perform? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point

- A. Delete GW1.
- B. Reset GW1.
- C. Add a service endpoint to VNet1.
- D. Add a connection to GW1.
- E. Add a public IP address space to VNet1.
- F. Create a route-based virtual network gateway.

Answer: AF

QUESTION 217

You have a server named Server1 that runs Windows Server 2019.

Server1 is a container host.

You plan to create a container image.

You create the following instructions in a text editor.

```
LABEL maintainer="User1@contoso.com"

RUN dism.exe /online /enable-feature /all /featurename:iis-webserver /NoRestart

RUN echo "Hello World!" > c:\inetpub\wwwroot\index.html
```

You need to be able to automate the container image creation by using the instructions. To which file should you save the instructions?

- A. Dockerfile
- B. daemon.json
- C. dockerconfig.json
- D. dockerconfig.json

Answer: A

QUESTION 218

You plan to create an Azure logic app that will access secrets stored in an Azure key vault.

You need to ensure that the logic app can authenticate to the key vault by using Azure Active Directory (Azure AD). What should you do?

- A. Turn on the system-assigned managed identity.
- B. Add an Azure Active Directory authorization policy.
- C. Create an app registration.
- D. Modify the access keys.

Answer: B

QUESTION 219

You have a resource group named RG5. The access controls for RG5 are configured as shown in the following exhibit.

Check access Role assignments Role assignments Deny assignments Classic administrators Roles

Manage access to Azure resources for users, groups, and service principals at this scope by creating role assignments. [Learn More](#)

Name	Type	Role	Scope
<input type="text"/> Search by name or email	All	3 selected	
Scope	Group by	Role	
All scopes			
3 items (3 Users)			
<input type="checkbox"/> NAME	TYPE	ROLE	SCOPE
 User 1 User1@...	User	Network Contributor	This resource
 prvi prvi@sk...	User	Owner	Subscription (Inherited)
SECURITY ADMIN			
 User 2 User2@...	User	Security Admin	This resource

Which users can deploy virtual networks to RG5?

- A. User1, User2, and prvi
- B. Only User1 and User2
- C. Only User1
- D. Only prvi and User1

Answer: D

Explanation:

User1, the Network Contributor, can create and manage networks, but not access to them. Prvi, the Owner, can create and manage resources of all types.

References:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

QUESTION 220

You create the user-assigned identities shown in the following table.

Name	Resource group	Location
Identity1	RG1	West US
Identity2	RG1	Central US
Identity3	RG2	West US

You create a virtual machine that has the following configurations:

- Name: VM1
- Location: West US
- Resource group: RG1

Which managed identities can you add to VM1?

- A. Identity1 and Identity2 only
- B. Identity1 only
- C. Identity1, Identity2 and Identity3
- D. Identity1 and Identity3 only

Answer: B

QUESTION 221

Hotspot Question

You have an Azure subscription that contains a virtual network named VNet1. VNet1 uses an IP address space of 10.0.0.0/16 and contains the subnets in the following table.

Name	IP address range
Subnet0	10.0.0.0/24
Subnet1	10.0.1.0/24
Subnet2	10.0.2.0/24
GatewaySubnet	10.0.254.0/24

Subnet1 contains a virtual appliance named VM1 that operates as a router.

You create a routing table named RT1.

You need to route all inbound traffic to VNet1 through VM1.

How should you configure RT1? To answer, select the appropriate options in the answer area.

Answer Area

Address prefix:	<input type="text" value="10.0.0.0/16"/> <input type="text" value="10.0.1.0/24"/> <input type="text" value="10.0.254.0/24"/>
Next hop type:	<input type="text" value="Virtual appliance"/> <input type="text" value="Virtual network"/> <small>None for Next hop type.</small> <input type="text" value="Virtual network gateway"/>
Assigned to:	<input type="text" value="GatewaySubnet"/> <input type="text" value="Subnet0"/> <input type="text" value="Subnet1 and Subnet2"/>

Answer:**Answer Area**

Address prefix:	<input type="text" value="10.0.0.0/16"/> <input checked="" type="text" value="10.0.1.0/24"/> <input type="text" value="10.0.254.0/24"/>
Next hop type:	<input type="text" value="Virtual appliance"/> <input checked="" type="text" value="Virtual network"/> <small>None for Next hop type.</small> <input type="text" value="Virtual network gateway"/>
Assigned to:	<input checked="" type="text" value="GatewaySubnet"/> <input type="text" value="Subnet0"/> <input type="text" value="Subnet1 and Subnet2"/>

Explanation:

Box 1: 10.0.1.0/24

Address space of sbbnet 1 as routing should be made through vm1.

Box 2: Virtual Network

Next hop needs to be made for virtual network.

Box 3: Gateway Subnet

Should be made through vnet gateway and that used gateway subnet only.

References:<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview>**QUESTION 222****Hotspot Question**

You are designing a virtual network to support a web application.

The web application uses Blob storage to store large images.

The web application will be deployed to an Azure App Service Web App.

You have the following requirements:

- Secure all communications by using Secured Socket layer (SSL) SSL encryption and decryption must be processed efficiently to support high traffic load on the web application
- Protect the web application from web vulnerabilities and attacks without modification to backend

code

- Optimize web application responsiveness and reliability by routing HTTP request and responses to the endpoint with the lowest network latency for the client.

You need to configure the Azure components to meet the requirements.

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

NOTE: Each correct selection is worth one point.

Requirement	Component
SSL Encrypt / Decrypt	<input type="checkbox"/> Azure Application Gateway <input type="checkbox"/> Azure Monitor <input type="checkbox"/> Azure Security Center <input type="checkbox"/> Azure Traffic Manager
Protect from web vulnerabilities	<input type="checkbox"/> Azure Application Gateway <input type="checkbox"/> Azure Monitor <input type="checkbox"/> Azure Security Center <input type="checkbox"/> Azure Traffic Manager
Optimize responsiveness and reliability	<input type="checkbox"/> Azure Application Gateway <input type="checkbox"/> Azure Monitor <input type="checkbox"/> Azure Security Center <input type="checkbox"/> Azure Traffic Manager

Answer:

Requirement	Component
SSL Encrypt / Decrypt	<div style="border: 1px solid black; padding: 5px;"> Azure Application Gateway Azure Monitor Azure Security Center Azure Traffic Manager </div>
Protect from web vulnerabilities	<div style="border: 1px solid black; padding: 5px;"> Azure Application Gateway Azure Monitor Azure Security Center Azure Traffic Manager </div>
Optimize responsiveness and reliability	<div style="border: 1px solid black; padding: 5px;"> Azure Application Gateway Azure Monitor Azure Security Center Azure Traffic Manager </div>

Explanation:

Box 1: Azure application Gateway

Azure Application Gateway supports end-to-end encryption of traffic. Application Gateway terminates the SSL connection at the application gateway. The gateway then applies the routing rules to the traffic, re-encrypts the packet and forwards the packet to the appropriate back-end server based on the routing rules defined. Any response from the web server goes through the same process back to the end user.

Box 2: Azure application Gateway

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/ag-overview>

Box 3: Azure Traffic Manager

Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally services across global Azure regions, while providing high availability and responsiveness.

References:

<https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-end-to-end-ssl-powershell>

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview>

<https://docs.microsoft.com/en-us/azure/security-center/security-center-intro>