

**AZ-304**

Number: AZ-304  
Passing Score: 800  
Time Limit: 120 min  
File Version: 1

AZ-304



**Website:** <https://vceplus.com>  
**VCE to PDF Converter:** <https://vceplus.com/vce-to-pdf/>  
**Facebook:** <https://www.facebook.com/VCE.For.All.VN/>  
**Twitter :** [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

<https://vceplus.com/>

## Design Monitoring

### Question Set 1

#### QUESTION 1

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager resource deployments in your subscription.



<https://vceplus.com/>

What should you include in the recommendation?

- A. the Change Tracking management solution
- B. Application Insights
- C. Azure Monitor action groups
- D. Azure Activity Log



**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting date isn't more than 90 days in the past.

Through activity logs, you can determine:

- what operations were taken on the resources in your subscription
- who started the operation
- when the operation occurred
- the status of the operation
- the values of other properties that might help you research the operation

Reference: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs>

## QUESTION 2

You have an Azure subscription that contains an Azure SQL database named DB1.

Several queries that query the data in DB1 take a long time to execute.

You need to recommend a solution to identify the queries that take the longest to execute.

What should you include in the recommendation?

- A. SQL Database Advisor
- B. Azure Monitor
- C. Performance Recommendations
- D. Query Performance Insight

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Query Performance Insight provides intelligent query analysis for single and pooled databases. It helps identify the top resource consuming and long-running queries in your workload. This helps you find the queries to optimize to improve overall workload performance and efficiently use the resource that you are paying for.

Reference: <https://docs.microsoft.com/en-us/azure/azure-sql/database/query-performance-insight-use>

## QUESTION 3

You have an on-premises Hyper-V cluster. The cluster contains Hyper-V hosts that run Windows Server 2016 Datacenter. The hosts are licensed under a Microsoft Enterprise Agreement that has Software Assurance.

The Hyper-V cluster contains 30 virtual machines that run Windows Server 2012 R2. Each virtual machine runs a different workload. The workloads have predictable consumption patterns.

You plan to replace the virtual machines with Azure virtual machines that run Windows Server 2016. The virtual machines will be sized according to the consumption pattern of each workload.



You need to recommend a solution to minimize the compute costs of the Azure virtual machines.

Which two recommendations should you include in the solution? Each correct answer presents part of the solution.

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

- A. Configure a spending limit in the Azure account center.
- B. Create a virtual machine scale set that uses autoscaling.
- C. Activate Azure Hybrid Benefit for the Azure virtual machines.
- D. Purchase Azure Reserved Virtual Machine Instances for the Azure virtual machines.
- E. Create a lab in Azure DevTest Labs and place the Azure virtual machines in the lab.

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

C: For customers with Software Assurance, Azure Hybrid Benefit for Windows Server allows you to use your on-premises Windows Server licenses and run Windows virtual machines on Azure at a reduced cost. You can use Azure Hybrid Benefit for Windows Server to deploy new virtual machines with Windows OS.

D: With Azure Reserved VM Instances (RIs) you reserve virtual machines in advance and save up to 80 percent.

Reference: <https://azure.microsoft.com/en-us/pricing/reserved-vm-instances/>  
<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/hybrid-use-benefit-licensing>

#### **QUESTION 4**

A company has a hybrid ASP.NET Web API application that is based on a software as a service (SaaS) offering.

Users report general issues with the data. You advise the company to implement live monitoring and use ad hoc queries on stored JSON data. You also advise the company to set up smart alerting to detect anomalies in the data.

You need to recommend a solution to set up smart alerting.

What should you recommend?

- A. Azure Site Recovery and Azure Monitor Logs
- B. Azure Data Lake Analytics and Azure Monitor Logs

- C. Azure Application Insights and Azure Monitor Logs
- D. Azure Security Center and Azure Data Lake Store

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Application Insights, a feature of Azure Monitor, is an extensible Application Performance Management (APM) service for developers and DevOps professionals. Use it to monitor your live applications. It will automatically detect performance anomalies, and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app.

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview>

#### QUESTION 5

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. The subscription contains 10 resource groups, one for each department at your company.

Each department has a specific spending limit for its Azure resources.

You need to ensure that when a department reaches its spending limit, the compute resources of the department shut down automatically.

Which two features should you include in the solution? Each correct answer presents part of the solution.

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

- A. Azure Logic Apps
- B. Azure Monitor alerts
- C. the spending limit of an Azure account
- D. Cost Management budgets
- E. Azure Log Analytics alerts

**Correct Answer:** CD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

C: The spending limit in Azure prevents spending over your credit amount. All new customers who sign up for an Azure free account or subscription types that include credits over multiple months have the spending limit turned on by default. The spending limit is equal to the amount of credit and it can't be changed.

D: Turn on the spending limit after removing

This feature is available only when the spending limit has been removed indefinitely for subscription types that include credits over multiple months. You can use this feature to turn on your spending limit automatically at the start of the next billing period.

1. Sign in to the Azure portal as the Account Administrator.
2. Search for Cost Management + Billing.
3. Etc.

Reference: <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/spending-limit>



## Design Identity and Security

### Testlet 1

#### Case Study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

#### To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

#### Existing Environment. Active Directory Environment

The network contains two Active Directory forests named corp.fabrikam.com and rd.fabrikam.com. There are no trust relationships between the forests.

Corp.fabrikam.com is a production forest that contains identities used for internal user and computer authentication.

Rd.fabrikam.com is used by the research and development (R&D) department only.

#### Existing Environment. Network Infrastructure

Each office contains at least one domain controller from the corp.fabrikam.com domain. The main office contains all the domain controllers for the rd.fabrikam.com forest.

All the offices have a high-speed connection to the Internet.

An existing application named WebApp1 is hosted in the data center of the London office. WebApp1 is used by customers to place and track orders. WebApp1 has a web tier that uses Microsoft Internet Information Services (IIS) and a database tier that runs Microsoft SQL Server 2016. The web tier and the database tier are deployed to virtual machines that run on Hyper-V.

The IT department currently uses a separate Hyper-V environment to test updates to WebApp1.

Fabrikam purchases all Microsoft licenses through a Microsoft Enterprise Agreement that includes Software Assurance.

### **Existing Environment. Problem Statements**

The use of WebApp1 is unpredictable. At peak times, users often report delays. At other times, many resources for WebApp1 are underutilized.

### **Requirements. Planned Changes**

Fabrikam plans to move most of its production workloads to Azure during the next few years.

As one of its first projects, the company plans to establish a hybrid identity model, facilitating an upcoming Microsoft Office 365 deployment.

All R&D operations will remain on-premises.

Fabrikam plans to migrate the production and test instances of WebApp1 to Azure and to use the S1 plan.

### **Requirements. Technical Requirements**

Fabrikam identifies the following technical requirements:



- Web site content must be easily updated from a single point.
  - User input must be minimized when provisioning new web app instances.
  - Whenever possible, existing on-premises licenses must be used to reduce cost. ▪
- Users must always authenticate by using their corp.fabrikam.com UPN identity.
- Any new deployments to Azure must be redundant in case an Azure region fails.
  - Whenever possible, solutions must be deployed to Azure by using the Standard pricing tier of Azure App Service.
  - An email distribution group named IT Support must be notified of any issues relating to the directory synchronization services.
  - Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the onpremises network.

### **Requirements. Database Requirements**

Fabrikam identifies the following database requirements:

- Database metrics for the production instance of WebApp1 must be available for analysis so that database administrators can optimize the performance settings.
- To avoid disrupting customer access, database downtime must be minimized when databases are migrated. ▪ Database backups must be retained for a minimum of seven years to meet compliance requirements.

### **Requirements. Security Requirements**

Fabrikam identifies the following security requirements:

- Company information including policies, templates, and data must be inaccessible to anyone outside the company.
  - Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails.
  - Administrators must be able to authenticate to the Azure portal by using their corp.fabrikam.com credentials.
  - All administrative access to the Azure portal must be secured by using multi-factor authentication. ▪
- The testing of WebApp1 updates must not be visible to anyone outside the company.

### QUESTION 1

What should you include in the identity management strategy to support the planned changes?

- A. Move all the domain controllers from corp.fabrikam.com to virtual networks in Azure.
- B. Deploy domain controllers for the rd.fabrikam.com forest to virtual networks in Azure.
- C. Deploy domain controllers for corp.fabrikam.com to virtual networks in Azure.
- D. Deploy a new Azure AD tenant for the authentication of new R&D projects.

**Correct Answer:** C

**Section:** (none)

**Explanation**



**Explanation/Reference:**

Explanation:

Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the onpremises network. (This requires domain controllers in Azure)

Users on the on-premises network must be able to authenticate to corp.fabrikam.com if an Internet link fails. (This requires domain controllers on-premises)

**Design Identity and Security**

### Question Set 2

#### QUESTION 1

You plan to deploy an application named App1 that will run on five Azure virtual machines. Additional virtual machines will be deployed later to run App1.

You need to recommend a solution to meet the following requirements for the virtual machines that will run App1:

- Ensure that the virtual machines can authenticate to Azure Active Directory (Azure AD) to gain access to an Azure key vault, Azure Logic Apps instances, and an Azure SQL database.
  - Avoid assigning new roles and permissions for Azure services when you deploy additional virtual machines. ▪
- Avoid storing secrets and certificates on the virtual machines.

Which type of identity should you include in the recommendation?

- A. a service principal that is configured to use a certificate
- B. a system-assigned managed identity
- C. a service principal that is configured to use a client secret
- D. a user-assigned managed identity

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Managed identities for Azure resources is a feature of Azure Active Directory.

User-assigned managed identity can be shared. The same user-assigned managed identity can be associated with more than one Azure resource.

Incorrect Answers:

B: System-assigned managed identity cannot be shared. It can only be associated with a single Azure resource.

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

## QUESTION 2

You are designing a large Azure environment that will contain many subscriptions.

You plan to use Azure Policy as part of a governance solution.

To which three scopes can you assign Azure Policy definitions? Each correct answer presents a complete solution.

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

- A. management groups
- B. subscriptions
- C. Azure Active Directory (Azure AD) tenants
- D. resource groups
- E. Azure Active Directory (Azure AD) administrative units
- F. compute resources

**Correct Answer:** ABD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources.

Reference: <https://docs.microsoft.com/en-us/azure/governance/policy/overview>

### QUESTION 3

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

You plan to deploy Azure Cosmos DB databases that will use the SQL API.

You need to recommend a solution to provide specific Azure AD user accounts with read access to the Cosmos DB databases.

What should you include in the recommendation?

- A. shared access signatures (SAS) and conditional access policies
- B. certificates and Azure Key Vault
- C. a resource token and an Access control (IAM) role assignment
- D. master keys and Azure Information Protection policies

**Correct Answer:** C

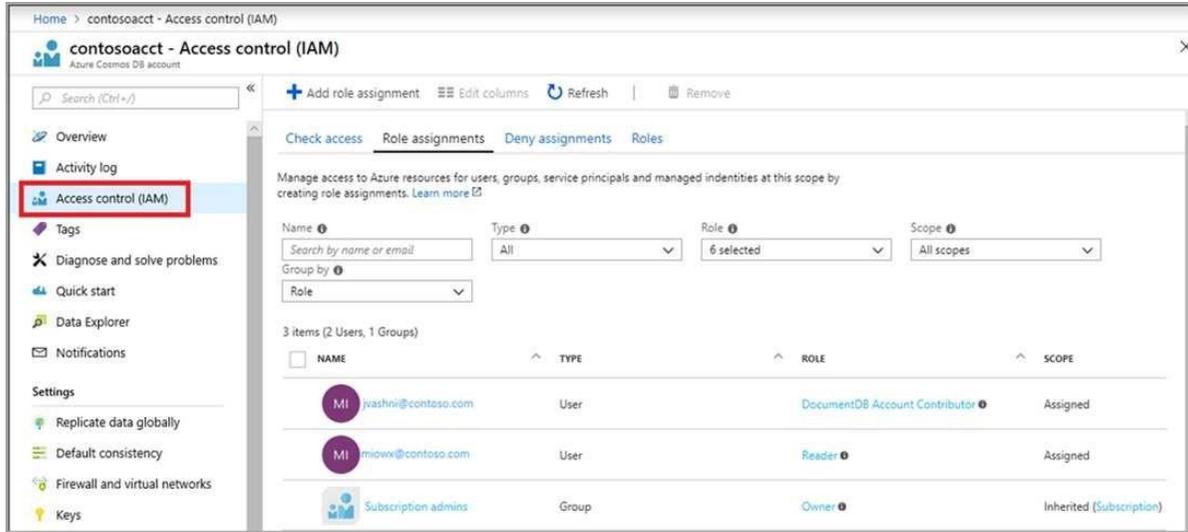
**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

The Access control (IAM) pane in the Azure portal is used to configure role-based access control on Azure Cosmos resources. The roles are applied to users, groups, service principals, and managed identities in Active Directory. You can use built-in roles or custom roles for individuals and groups. The following screenshot shows Active Directory integration (RBAC) using access control (IAM) in the Azure portal:

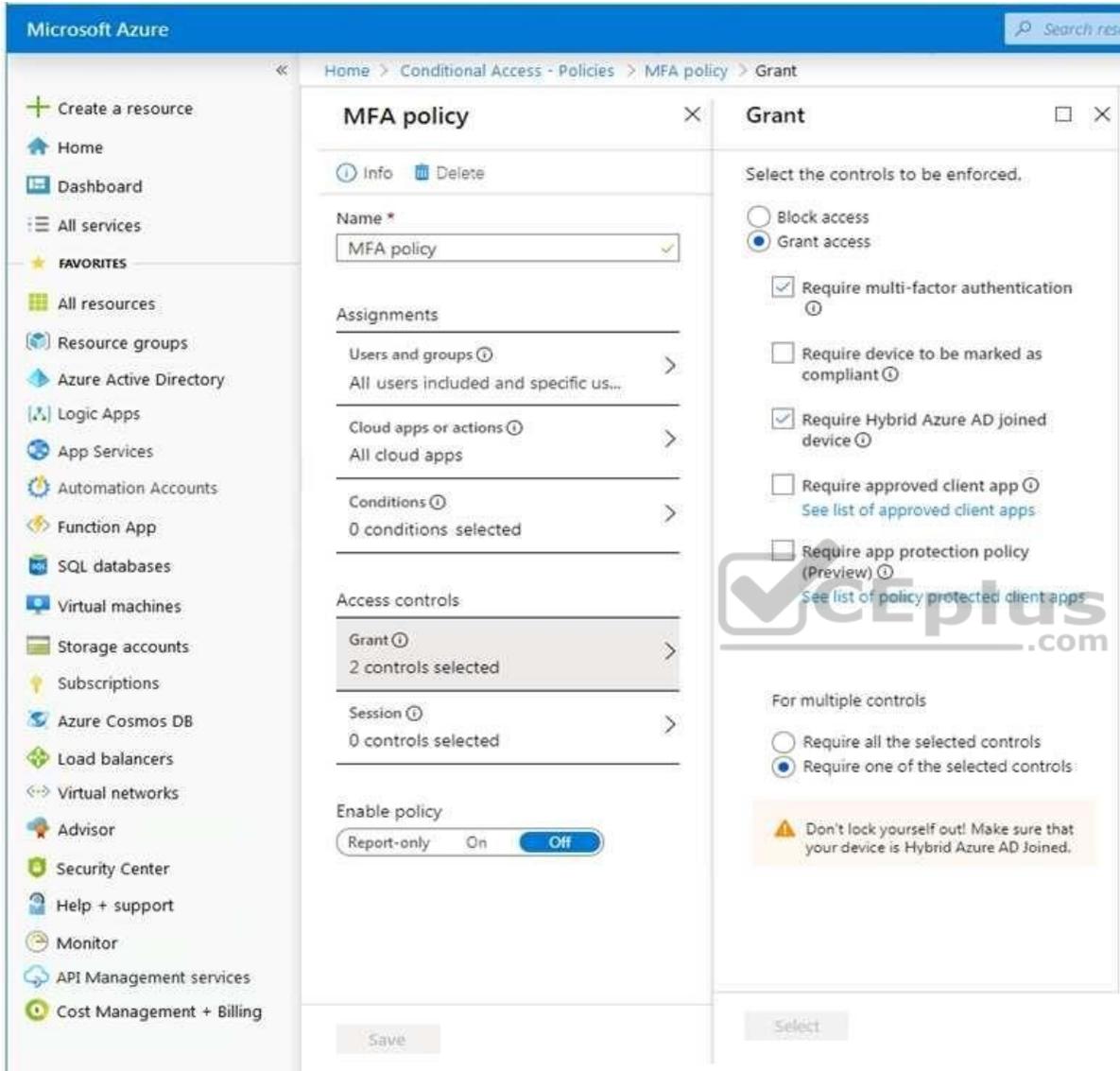


Reference: <https://docs.microsoft.com/en-us/azure/cosmos-db/role-based-access-control>

#### QUESTION 4

You have an Azure Active Directory (Azure AD) tenant and Windows 10 devices.

You configure a conditional access policy as shown in the exhibit. (Click the **Exhibit** tab.)



Microsoft Azure

Home > Conditional Access - Policies > MFA policy > Grant

### MFA policy

Info Delete

Name \*  
MFA policy

Assignments

Users and groups  
All users included and specific us...

Cloud apps or actions  
All cloud apps

Conditions  
0 conditions selected

Access controls

Grant  
2 controls selected

Session  
0 controls selected

Enable policy  
Report-only On **Off**

### Grant

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app  
[See list of approved client apps](#)

Require app protection policy (Preview)  
[See list of policy protected client apps](#)

For multiple controls

Require all the selected controls

Require one of the selected controls

⚠ Don't lock yourself out! Make sure that your device is Hybrid Azure AD Joined.

Save Select

What is the result of the policy?

- A. All users will always be prompted for multi-factor authentication (MFA).
- B. Users will be prompted for multi-factor authentication (MFA) only when they sign in from devices that are **NOT** joined to Azure AD.
- C. All users will be able to sign in without using multi-factor authentication (MFA).
- D. Users will be prompted for multi-factor authentication (MFA) only when they sign in from devices that are joined to Azure AD.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Either the device should be joined to Azure AD or MFA must be used.

#### **QUESTION 5**

You are designing an Azure resource deployment that will use Azure Resource Manager templates. The deployment will use Azure Key Vault to store secrets.

You need to recommend a solution to meet the following requirements:

- Prevent the IT staff that will perform the deployment from retrieving the secrets directly from Key Vault. ▪
- Use the principle of least privilege.

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

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

- A. Create a Key Vault access policy that allows all get key permissions, get secret permissions, and get certificate permissions.
- B. From Access policies in Key Vault, enable access to the Azure Resource Manager for template deployment.
- C. Create a Key Vault access policy that allows all list key permissions, list secret permissions, and list certificate permissions.
- D. Assign the IT staff a custom role that includes the Microsoft.KeyVault/Vaults/Deploy/Action permission.
- E. Assign the Key Vault Contributor role to the IT staff.

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

B: To access a key vault during template deployment, set `enabledForTemplateDeployment` on the key vault to true.

D: The user who deploys the template must have the Microsoft.KeyVault/vaults/deploy/action permission for the scope of the resource group and key vault.

Incorrect Answers:

E: To grant access to a user to manage key vaults, you assign a predefined key vault Contributor role to the user at a specific scope.

If a user has Contributor permissions to a key vault management plane, the user can grant themselves access to the data plane by setting a Key Vault access policy. You should tightly control who has Contributor role access to your key vaults. Ensure that only authorized persons can access and manage your key vaults, keys, secrets, and certificates.

Reference: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter> <https://docs.microsoft.com/en-us/azure/key-vault/general/overview-security>

**QUESTION 6**

You have an Azure subscription that contains resources in three Azure regions.A ..... **Error! Bookmark not defined.**

B ..... 26

C ..... 26

D ..... 26

**Correct Answer:** ..... 26



You need to implement Azure Key Vault to meet the following requirements:

- In the event of a regional outage, all keys must be readable.
- All the resources in the subscription must be able to access Key Vault.
- The number of Key Vault resources to be deployed and managed must be minimized.

How many instances of Key Vault should you implement?

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

The contents of your key vault are replicated within the region and to a secondary region at least 150 miles away but within the same geography. This maintains high durability of your keys and secrets. See the Azure paired regions document for details on specific region pairs.

Example: Secrets that must be shared by your application in both Europe West and Europe North. Minimize these as much as you can. Put these in a key vault in either of the two regions. Use the same URI from both regions. Microsoft will fail over the Key Vault service internally.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance>

### QUESTION 7

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

You plan to provide users with access to shared files by using Azure Storage. The users will be provided with different levels of access to various Azure file shares based on their user account or their group membership.

You need to recommend which additional Azure services must be used to support the planned deployment.

What should you include in the recommendation?

- A. an Azure AD enterprise application
- B. Azure Information Protection
- C. an Azure AD Domain Services (Azure AD DS) instance
- D. an Azure Front Door instance

**Correct Answer: C**

**Section: (none)**

**Explanation**



**Explanation/Reference:**

Explanation:

Azure Files supports identity-based authentication over Server Message Block (SMB) through two types of Domain Services: on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).

Reference: <https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable>

### QUESTION 8

You have an Azure subscription that contains a custom application named Application1. Application1 was developed by an external company named Fabrikam, Ltd. Developers at Fabrikam were assigned role-based access control (RBAC) permissions to the Application1 components. All users are licensed for the Microsoft 365 E5 plan.

You need to recommend a solution to verify whether the Fabrikam developers still require permissions to Application1. The solution must meet the following requirements:

- To the manager of the developers, send a monthly email message that lists the access permissions to Application1.
- If the manager does not verify an access permission, automatically revoke that permission. ▪ Minimize development effort.

What should you recommend?

- A. Create an Azure Automation runbook that runs the `Get-AzureADUserAppRoleAssignment` cmdlet.
- B. Create an Azure Automation runbook that runs the `Get-AzureRmRoleAssignment` cmdlet.
- C. In Azure Active Directory (Azure AD), create an access review of Application1.
- D. In Azure Active Directory (AD) Privileged Identity Management, create a custom role assignment for the Application1 resources.

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**



## Design Data Storage

### Question Set 1

#### QUESTION 1

You have 100 servers that run Windows Server 2012 R2 and host Microsoft SQL Server 2014 instances. The instances host databases that have the following characteristics:

- The largest database is currently 3 TB. None of the databases will ever exceed 4 TB. ▪
- Stored procedures are implemented by using CLR.

You plan to move all the data from SQL Server to Azure.

You need to recommend an Azure service to host the databases. The solution must meet the following requirements:

- Whenever possible, minimize management overhead for the migrated databases.
- Minimize the number of database changes required to facilitate the migration.
- Ensure that users can authenticate by using their Active Directory credentials.

What should you include in the recommendation?



<https://vceplus.com/>

- A. Azure SQL Database elastic pools
- B. Azure SQL Database Managed Instance
- C. Azure SQL Database single databases
- D. SQL Server 2016 on Azure virtual machines

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-managed-instance>**QUESTION 2**

You are designing an order processing system in Azure that will contain the Azure resources shown in the following table.

Name	Type	Purpose
App1	Web app	Processes customer orders
Function1	Function	Check product availability at vendor 1
Function2	Function	Check product availability at vendor 2
storage1	Storage account	Stores order processing logs

The order processing system will have the following transaction flow:

- A customer will place an order by using App1.
- When the order is received, App1 will generate a message to check for product availability at vendor 1 and vendor 2.
- An integration component will process the message, and then trigger either Function1 or Function2 depending on the type of order.
- Once a vendor confirms the product availability, a status message for App1 will be generated by Function1 or Function2. ▪ All the steps of the transaction will be logged to storage1.

Which type of resource should you recommend for the integration component?

- A. an Azure Data Factory pipeline
- B. an Azure Service Bus queue
- C. an Azure Event Grid domain
- D. an Azure Event Hubs capture

**Correct Answer:** A**Section:** (none)**Explanation****Explanation/Reference:**

Explanation:

A data factory can have one or more pipelines. A pipeline is a logical grouping of activities that together perform a task.

The activities in a pipeline define actions to perform on your data.

Data Factory has three groupings of activities: data movement activities, data transformation activities, and control activities.

Azure Functions is now integrated with Azure Data Factory, allowing you to run an Azure function as a step in your data factory pipelines.

Reference: <https://docs.microsoft.com/en-us/azure/data-factory/concepts-pipelines-activities>

### QUESTION 3

You have 70 TB of files on your on-premises file server.

You need to recommend solution for importing data to Azure. The solution must minimize cost.

What Azure service should you recommend?

- A. Azure StorSimple
- B. Azure Batch
- C. Azure Data Box
- D. Azure Stack

**Correct Answer:** C  
**Section:** (none)  
**Explanation**



#### **Explanation/Reference:**

Explanation:

Microsoft has engineered an extremely powerful solution that helps customers get their data to the Azure public cloud in a cost-effective, secure, and efficient manner with powerful Azure and machine learning at play. The solution is called Data Box.

Data Box and is in general availability status. It is a rugged device that allows organizations to have 100 TB of capacity on which to copy their data and then send it to be transferred to Azure.

Incorrect Answers:

A: StoreSimple would not be able to handle 70 TB of data.

Reference: <https://www.vembu.com/blog/what-is-microsoft-azure-data-box-disk-edge-heavy-gateway-overview/>

### QUESTION 4

You have an Azure subscription that contains 100 virtual machines.

You plan to design a data protection strategy to encrypt the virtual disks.

You need to recommend a solution to encrypt the disks by using Azure Disk Encryption. The solution must provide the ability to encrypt operating system disks and data disks.

What should you include in the recommendation?

- A. a certificate
- B. a key
- C. a passphrase
- D. a secret

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

For enhanced virtual machine (VM) security and compliance, virtual disks in Azure can be encrypted. Disks are encrypted by using cryptographic keys that are secured in an Azure Key Vault. You control these cryptographic keys and can audit their use.

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

#### **QUESTION 5**

You have data files in Azure Blob storage.

You plan to transform the files and move them to Azure Data Lake Storage.

You need to transform the data by using mapping data flow.

Which Azure service should you use?

- A. Azure Data Box Gateway
- B. Azure Storage Sync
- C. Azure Data Factory
- D. Azure Databricks

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

You can use Copy Activity in Azure Data Factory to copy data from and to Azure Data Lake Storage Gen2, and use Data Flow to transform data in Azure Data Lake Storage Gen2.

Reference: <https://docs.microsoft.com/en-us/azure/data-factory/connector-azure-data-lake-storage>

**QUESTION 6**

You have an Azure virtual machine named VM1 that runs Windows Server 2019 and contains 500 GB of data files.

You are designing a solution that will use Azure Data Factory to transform the data files, and then load the files to Azure Data Lake Storage.

What should you deploy on VM1 to support the design?

- A. the Azure Pipelines agent
- B. the Azure File Sync agent
- C. the On-premises data gateway
- D. the self-hosted integration runtime in Azure

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

The integration runtime (IR) is the compute infrastructure that Azure Data Factory uses to provide data-integration capabilities across different network environments. For details about IR, see Integration runtime overview.

A self-hosted integration runtime can run copy activities between a cloud data store and a data store in a private network. It also can dispatch transform activities against compute resources in an on-premises network or an Azure virtual network. The installation of a self-hosted integration runtime needs an on-premises machine or a virtual machine inside a private network.

Reference:

<https://docs.microsoft.com/en-us/azure/data-factory/create-self-hosted-integration-runtime>

**Design Data Storage**

**Testlet 2**

## Case Study

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

### To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question. **Overview**

Contoso, Ltd, is a US-based financial services company that has a main office in New York and a branch office in San Francisco.

### Existing Environment. Payment Processing System

Contoso hosts a business-critical payment processing system in its New York data center. The system has three tiers: a front-end web app, a middle-tier web API, and a back-end data store implemented as a Microsoft SQL Server 2014 database. All servers run Windows Server 2012 R2.

The front-end and middle-tier components are hosted by using Microsoft Internet Information Services (IIS). The application code is written in C# and ASP.NET. The middle-tier API uses the Entity Framework to communicate to the SQL Server database. Maintenance of the database is performed by using SQL Server Agent jobs.

The database is currently 2 TB and is not expected to grow beyond 3 TB.

The payment processing system has the following compliance-related requirements:

- Encrypt data in transit and at rest. Only the front-end and middle-tier components must be able to access the encryption keys that protect the data store.
- Keep backups of the data in two separate physical locations that are at least 200 miles apart and can be restored for up to seven years.
- Support blocking inbound and outbound traffic based on the source IP address, the destination IP address, and the port number.
- Collect Windows security logs from all the middle-tier servers and retain the logs for a period of seven years.

- Inspect inbound and outbound traffic from the front-end tier by using highly available network appliances. ▪
- Only allow all access to all the tiers from the internal network of Contoso.

Tape backups are configured by using an on-premises deployment of Microsoft System Center Data Protection Manager (DPM), and then shipped offsite for long term storage.

### **Existing Environment. Historical Transaction Query System**

Contoso recently migrated a business-critical workload to Azure. The workload contains a .NET web service for querying the historical transaction data residing in Azure Table Storage. The .NET web service is accessible from a client app that was developed in-house and runs on the client computers in the New York office. The data in the table storage is 50 GB and is not expected to increase.

### **Existing Environment. Current Issues**

The Contoso IT team discovers poor performance of the historical transaction query system, as the queries frequently cause table scans.

### **Requirements. Planned Changes**

Contoso plans to implement the following changes:

- Migrate the payment processing system to Azure.
- Migrate the historical transaction data to Azure Cosmos DB to address the performance issues. **Requirements.**

### **Migration Requirements**

Contoso identifies the following general migration requirements:

- Infrastructure services must remain available if a region or a data center fails. Failover must occur without any administrative intervention.
  - Whenever possible, Azure managed services must be used to minimize management overhead. ▪
- Whenever possible, costs must be minimized.

Contoso identifies the following requirements for the payment processing system:

- If a data center fails, ensure that the payment processing system remains available without any administrative intervention. The middle-tier and the web front end must continue to operate without any additional configurations.
- Ensure that the number of compute nodes of the front-end and the middle tiers of the payment processing system can increase or decrease automatically based on CPU utilization.
- Ensure that each tier of the payment processing system is subject to a Service Level Agreement (SLA) of 99.99 percent availability.
- Minimize the effort required to modify the middle-tier API and the back-end tier of the payment processing system.
- Payment processing system must be able to use grouping and joining tables on encrypted columns.

- Generate alerts when unauthorized login attempts occur on the middle-tier virtual machines.
  - Ensure that the payment processing system preserves its current compliance status. ▪
- Host the middle tier of the payment processing system on a virtual machine

Contoso identifies the following requirements for the historical transaction query system:

- Minimize the use of on-premises infrastructure services.
- Minimize the effort required to modify the .NET web service querying Azure Cosmos DB.
- Minimize the frequency of table scans.
- If a region fails, ensure that the historical transaction query system remains available without any administrative intervention.

### **Requirements. Information Security Requirements**

The IT security team wants to ensure that identity management is performed by using Active Directory. Password hashes must be stored on-premises only.

Access to all business-critical systems must rely on Active Directory credentials. Any suspicious authentication attempts must trigger a multi-factor authentication prompt automatically.

#### **QUESTION 1**

You need to recommend a solution for protecting the content of the payment processing system.

What should you include in the recommendation?

- A. Always Encrypted with deterministic encryption
- B. Always Encrypted with randomized encryption
- C. Transparent Data Encryption (TDE)
- D. Azure Storage Service Encryption

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**Design Business Continuity**

**Question Set 1**

#### **QUESTION 1**

Your company purchases an app named App1.

You plan to run App1 on seven Azure virtual machines in an Availability Set. The number of fault domains is set to 3. The number of update domains is set to 20.

You need to identify how many App1 instances will remain available during a period of planned maintenance.

How many App1 instances should you identify?

- A. 1
- B. 2
- C. 6
- D. 7

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Only one update domain is rebooted at a time. Here there are 7 update domain with one VM each (and 13 update domain with no VM).

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

## QUESTION 2

**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 Storage v2 account named storage1.

You plan to archive data to storage1.

You need to ensure that the archived data cannot be deleted for five years. The solution must prevent administrators from deleting the data.

Solution: You create an Azure Blob storage container, and you configure a legal hold access policy.

Does this meet the goal?

- A. Yes

B. No

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Use an Azure Blob storage container, but use a time-based retention policy instead of a legal hold.

Note:

Immutable storage for Azure Blob storage enables users to store business-critical data objects in a WORM (Write Once, Read Many) state. This state makes the data non-erasable and non-modifiable for a user-specified interval. For the duration of the retention interval, blobs can be created and read, but cannot be modified or deleted. Immutable storage is available for general-purpose v2 and Blob storage accounts in all Azure regions.

Note: Set retention policies and legal holds

1. Create a new container or select an existing container to store the blobs that need to be kept in the immutable state. The container must be in a general-purpose v2 or Blob storage account.
2. Select Access policy in the container settings. Then select Add policy under Immutable blob storage.

Either

3a. To enable legal holds, select Add Policy. Select Legal hold from the drop-down menu.

Or

3b. To enable time-based retention, select Time-based retention from the drop-down menu.

4. Enter the retention interval in days (acceptable values are 1 to 146000 days).

Reference: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage> <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutability-policies-manage>

### **QUESTION 3**

**Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.**

**After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.**

You have an Azure Storage v2 account named storage1.

You plan to archive data to storage1.

You need to ensure that the archived data cannot be deleted for five years. The solution must prevent administrators from deleting the data.

Solution: You create a file share and snapshots.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

Instead you could create an Azure Blob storage container, and you configure a legal hold access policy.

Reference: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage>

#### **QUESTION 4**

**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 Storage v2 account named storage1.

You plan to archive data to storage1.

You need to ensure that the archived data cannot be deleted for five years. The solution must prevent administrators from deleting the data.

Solution: You create a file share, and you configure an access policy.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Instead of a file share, an immutable Blob storage is required.

Time-based retention policy support: Users can set policies to store data for a specified interval. When a time-based retention policy is set, blobs can be created and read, but not modified or deleted. After the retention period has expired, blobs can be deleted but not overwritten.

Note: Set retention policies and legal holds

1. Create a new container or select an existing container to store the blobs that need to be kept in the immutable state. The container must be in a general-purpose v2 or Blob storage account.
2. Select Access policy in the container settings. Then select Add policy under Immutable blob storage.
3. To enable time-based retention, select Time-based retention from the drop-down menu.
4. Enter the retention interval in days (acceptable values are 1 to 146000 days).

Reference: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage> <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutability-policies-manage>

#### QUESTION 5

**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 on-premises Hyper-V cluster that hosts 20 virtual machines. Some virtual machines run Windows Server 2016 and some run Linux.

You plan to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

Solution: You recommend implementing an Azure Storage account, and then running AzCopy.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Explanation:

AzCopy only copy files, not the disks.

Instead use Azure Site Recovery.

Reference: <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview>

## QUESTION 6

**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 on-premises Hyper-V cluster that hosts 20 virtual machines. Some virtual machines run Windows Server 2016 and some run Linux.

You plan to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

Solution: You recommend implementing an Azure Storage account that has a file service and a blob service, and then using the Data Migration Assistant.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Data Migration Assistant is used to migrate SQL databases.

Instead use Azure Site Recovery.

Reference: <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview>

#### QUESTION 7

**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 on-premises Hyper-V cluster that hosts 20 virtual machines. Some virtual machines run Windows Server 2016 and some run Linux.

You plan to migrate the virtual machines to an Azure subscription.

You need to recommend a solution to replicate the disks of the virtual machines to Azure. The solution must ensure that the virtual machines remain available during the migration of the disks.

Solution: You recommend implementing a Recovery Services vault, and then using Azure Site Recovery.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Site Recovery can replicate on-premises VMware VMs, Hyper-V VMs, physical servers (Windows and Linux), Azure Stack VMs to Azure.

Note: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.

Reference: <https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-overview>

### QUESTION 8

You are designing a storage solution that will use Azure Blob storage. The data will be stored in a cool access tier or an archive access tier based on the access patterns of the data.

You identify the following types of infrequently accessed data:

- Telemetry data: Deleted after two years
- Promotional material: Deleted after 14 days
- Virtual machine audit data: Deleted after 200 days

A colleague recommends using the archive access tier to store the data.

Which statement accurately describes the recommendation?

- A. Storage costs will be based on a minimum of 30 days.
- B. Access to the data is guaranteed within five minutes.
- C. Access to the data is guaranteed within 30 minutes.
- D. Storage costs will be based on a minimum of 180 days.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

The following table shows a comparison of premium performance block blob storage, and the hot, cool, and archive access tiers.

	<b>Premium performance</b>	<b>Hot tier</b>	<b>Cool tier</b>	<b>Archive tier</b>
<b>Availability</b>	99.9%	99.9%	99%	Offline
<b>Availability (RA-GRS reads)</b>	N/A	99.99%	99.9%	Offline
<b>Usage charges</b>	Higher storage costs, lower access, and transaction cost	Higher storage costs, lower access, and transaction costs	Lower storage costs, higher access, and transaction costs	Lowest storage costs, highest access, and transaction costs
<b>Minimum object size</b>	N/A	N/A	N/A	N/A
<b>Minimum storage duration</b>	N/A	N/A	30 days <sup>1</sup>	180 days
<b>Latency (Time to first byte)</b>	Single-digit milliseconds	milliseconds	milliseconds	hours <sup>2</sup>

Reference: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers>

### QUESTION 9

You are planning to deploy an application named App1 that will run in containers on Azure Kubernetes Service (AKS) clusters. The AKS clusters will be distributed across four Azure regions.

You need to recommend a storage solution for App1. Updated container images must be replicated automatically to all the AKS clusters.

Which storage solution should you recommend?

- A. Azure Cache for Redis
- B. Azure Content Delivery Network (CDN)
- C. Premium SKU Azure Container Registry
- D. geo-redundant storage (GRS) accounts

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

Enable geo-replication for container images.

Best practice: Store your container images in Azure Container Registry and geo-replicate the registry to each AKS region.

To deploy and run your applications in AKS, you need a way to store and pull the container images. Container Registry integrates with AKS, so it can securely store your container images or Helm charts. Container Registry supports multimaster geo-replication to automatically replicate your images to Azure regions around the world.

Geo-replication is a feature of Premium SKU container registries.

Note:

When you use Container Registry geo-replication to pull images from the same region, the results are:

Faster: You pull images from high-speed, low-latency network connections within the same Azure region.

More reliable: If a region is unavailable, your AKS cluster pulls the images from an available container registry.

Cheaper: There's no network egress charge between datacenters.

Reference:

<https://docs.microsoft.com/en-us/azure/aks/operator-best-practices-multi-region>

#### **QUESTION 10**

You have an on-premises network and an Azure subscription. The on-premises network has several branch offices.

A branch office in Toronto contains a virtual machine named VM1 that is configured as a file server. Users access the shared files on VM1 from all the offices.

You need to recommend a solution to ensure that the users can access the shared files as quickly as possible if the Toronto branch office is inaccessible.

What should you include in the recommendation?

- A. an Azure file share and Azure File Sync
- B. a Recovery Services vault and Windows Server Backup
- C. a Recovery Services vault and Azure Backup
- D. Azure blob containers and Azure File Sync

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

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.

You need an Azure file share in the same region that you want to deploy Azure File Sync.

Incorrect Answer:

C: Backups would be a slower solution.

Reference:

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

**Design Business Continuity**

**Testlet 2**

**Case Study**

This is a case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

### **To start the case study**

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question. **Overview**

Contoso, Ltd, is a US-based financial services company that has a main office in New York and a branch office in San Francisco.

### **Existing Environment. Payment Processing System**

Contoso hosts a business-critical payment processing system in its New York data center. The system has three tiers: a front-end web app, a middle-tier web API, and a back-end data store implemented as a Microsoft SQL Server 2014 database. All servers run Windows Server 2012 R2.

The front-end and middle-tier components are hosted by using Microsoft Internet Information Services (IIS). The application code is written in C# and ASP.NET. The middle-tier API uses the Entity Framework to communicate to the SQL Server database. Maintenance of the database is performed by using SQL Server Agent jobs.

The database is currently 2 TB and is not expected to grow beyond 3 TB.

The payment processing system has the following compliance-related requirements:

- Encrypt data in transit and at rest. Only the front-end and middle-tier components must be able to access the encryption keys that protect the data store.
  - Keep backups of the data in two separate physical locations that are at least 200 miles apart and can be restored for up to seven years.
  - Support blocking inbound and outbound traffic based on the source IP address, the destination IP address, and the port number.
  - Collect Windows security logs from all the middle-tier servers and retain the logs for a period of seven years.
  - Inspect inbound and outbound traffic from the front-end tier by using highly available network appliances. ▪
- Only allow all access to all the tiers from the internal network of Contoso.

Tape backups are configured by using an on-premises deployment of Microsoft System Center Data Protection Manager (DPM), and then shipped offsite for long term storage.

### **Existing Environment. Historical Transaction Query System**

Contoso recently migrated a business-critical workload to Azure. The workload contains a .NET web service for querying the historical transaction data residing in Azure Table Storage. The .NET web service is accessible from a client app that was developed in-house and runs on the client computers in the New York office. The data in the table storage is 50 GB and is not expected to increase.

### **Existing Environment. Current Issues**

The Contoso IT team discovers poor performance of the historical transaction query system, as the queries frequently cause table scans.

### **Requirements. Planned Changes**

Contoso plans to implement the following changes:

- Migrate the payment processing system to Azure.
- Migrate the historical transaction data to Azure Cosmos DB to address the performance issues. **Requirements.**

### **Migration Requirements**

Contoso identifies the following general migration requirements:

- Infrastructure services must remain available if a region or a data center fails. Failover must occur without any administrative intervention.
  - Whenever possible, Azure managed services must be used to minimize management overhead.
- Whenever possible, costs must be minimized.

Contoso identifies the following requirements for the payment processing system:

- If a data center fails, ensure that the payment processing system remains available without any administrative intervention. The middle-tier and the web front end must continue to operate without any additional configurations.
- Ensure that the number of compute nodes of the front-end and the middle tiers of the payment processing system can increase or decrease automatically based on CPU utilization.
- Ensure that each tier of the payment processing system is subject to a Service Level Agreement (SLA) of 99.99 percent availability.
- Minimize the effort required to modify the middle-tier API and the back-end tier of the payment processing system.
- Payment processing system must be able to use grouping and joining tables on encrypted columns.

- Generate alerts when unauthorized login attempts occur on the middle-tier virtual machines.
- Ensure that the payment processing system preserves its current compliance status.

Host the middle tier of the payment processing system on a virtual machine

Contoso identifies the following requirements for the historical transaction query system:

- Minimize the use of on-premises infrastructure services.

- Minimize the effort required to modify the .NET web service querying Azure Cosmos DB.
- Minimize the frequency of table scans.
- If a region fails, ensure that the historical transaction query system remains available without any administrative intervention.

### Requirements. Information Security Requirements

The IT security team wants to ensure that identity management is performed by using Active Directory. Password hashes must be stored on-premises only.

Access to all business-critical systems must rely on Active Directory credentials. Any suspicious authentication attempts must trigger a multi-factor authentication prompt automatically.

### QUESTION 1

You need to recommend a backup solution for the data store of the payment processing system.

What should you include in the recommendation?

- A. Microsoft System Center Data Protection Manager (DPM)
- B. Azure Backup Server
- C. Azure SQL long-term backup retention
- D. Azure Managed Disks



**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-long-term-backup-retention-configure>



<https://vceplus.com/>

