

**Vendor:** Microsoft

**Exam Code:** AZ-304

**Exam Name:** Microsoft Azure Architect Design

**Version:** 20.081

## 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.

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**

#### 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**

#### 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

#### HOTSPOT

You have an Azure App Service Web App that includes Azure Blob storage and an Azure SQL Database instance. The application is instrumented by using the Application Insights SDK.

You need to design a monitoring solution for the web app.

Which Azure monitoring services should you use? To answer, select the appropriate Azure monitoring services in the answer area.

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

**Hot Area:**

**Answer Area**

Scenario	Azure monitoring service
Correlate Azure resource usage and performance data with application configuration and performance data.	<ul style="list-style-type: none"> <li>Azure Application Insights</li> <li>Azure Service Map</li> <li>Azure Monitor Logs</li> <li>Azure Activity Log</li> </ul>
Visualize the relationships between application components.	<ul style="list-style-type: none"> <li>Azure Application Insights</li> <li>Azure Service Map</li> <li>Azure Monitor Logs</li> <li>Azure Activity Log</li> </ul>
Track requests and exceptions to a specific line of code within the application.	<ul style="list-style-type: none"> <li>Azure Application Insights</li> <li>Azure Service Map</li> <li>Azure Monitor Logs</li> <li>Azure Activity Log</li> </ul>
Analyze how many users return to the application and how often they select a particular dropdown value.	<ul style="list-style-type: none"> <li>Azure Application Insights</li> <li>Azure Service Map</li> <li>Azure Monitor Logs</li> <li>Azure Activity Log</li> </ul>

**Correct Answer:**

**Answer Area**

Scenario	Azure monitoring service
Correlate Azure resource usage and performance data with application configuration and performance data.	<ul style="list-style-type: none"> <li>Azure Application Insights</li> <li>Azure Service Map</li> <li><b>Azure Monitor Logs</b></li> <li>Azure Activity Log</li> </ul>
Visualize the relationships between application components.	<ul style="list-style-type: none"> <li>Azure Application Insights</li> <li><b>Azure Service Map</b></li> <li>Azure Monitor Logs</li> <li>Azure Activity Log</li> </ul>
Track requests and exceptions to a specific line of code within the application.	<ul style="list-style-type: none"> <li><b>Azure Application Insights</b></li> <li>Azure Service Map</li> <li>Azure Monitor Logs</li> <li>Azure Activity Log</li> </ul>
Analyze how many users return to the application and how often they select a particular dropdown value.	<ul style="list-style-type: none"> <li>Azure Application Insights</li> <li>Azure Service Map</li> <li>Azure Monitor Logs</li> <li><b>Azure Activity Log</b></li> </ul>

**Explanation**

**Explanation/Reference:**  
Explanation:

Note: You can select Logs from either the Azure Monitor menu or the Log Analytics workspaces menu.

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

QUESTION 4

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

**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 5**

**HOTSPOT**

You have an Azure subscription that contains the SQL servers on Azure shown in the following table.

Name	Resource group	Location
SQLsvr1	RG1	East US
SQLsvr2	RG2	West US

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

Name	Resource group	Location	Account kind
storage1	RG1	East US	StorageV2 (general purpose v2)
storage2	RG2	West US	BlobStorage

You create the Azure SQL databases shown in the following table.

Name	Resource group	Server	Pricing tier
SQLdb1	RG1	SQLsvr1	Standard
SQLdb2	RG1	SQLsvr1	Standard
SQLdb3	RG2	SQLsvr2	Premium

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

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

**Hot Area:**

**Answer Area**

Statements	Yes	No
When you enable auditing for SQLdb1, you can store the audit information to storage1.	<input type="radio"/>	<input type="radio"/>
When you enable auditing for SQLdb2, you can store the audit information to storage2.	<input type="radio"/>	<input type="radio"/>
When you enable auditing for SQLdb3, you can store the audit information to storage2.	<input type="radio"/>	<input type="radio"/>

**Correct Answer:**

**Answer Area**

Statements	Yes	No
When you enable auditing for SQLdb1, you can store the audit information to storage1.	<input checked="" type="radio"/>	<input type="radio"/>
When you enable auditing for SQLdb2, you can store the audit information to storage2.	<input type="radio"/>	<input checked="" type="radio"/>
When you enable auditing for SQLdb3, you can store the audit information to storage2.	<input type="radio"/>	<input checked="" type="radio"/>

**Explanation**

**Explanation/Reference:**

Explanation:

Box 1: Yes

Be sure that the destination is in the same region as your database and server.

Box 2: No

Box 3: No

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing>

**QUESTION 6**

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**

**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 7**

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**

**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>

**QUESTION 8**

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**

**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 9**

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**

**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 10**

**HOTSPOT**

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure Active Directory (Azure AD) tenant
East	Sub1, Sub2	East.contoso.com
West	Sub3, Sub4	West.contoso.com

You plan to deploy a custom application to each subscription. The application will contain the following:

- A resource group
- An Azure web app
- Custom role assignments
- An Azure Cosmos DB account

You need to use Azure Blueprints to deploy the application to each subscription.

What is the minimum number of objects required to deploy the application? To answer, select the appropriate options in the answer area.

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

**Hot Area:**

**Answer Area**

Management groups:  ▼

1
2
3
4

Blueprint definitions:  ▼

1
2
3
4

Blueprint assignments:  ▼

1
2
3
4

**Correct Answer:**

**Answer Area**

Management groups:  ▼

1
2
3
4

Blueprint definitions:  ▼

1
2
3
4

Blueprint assignments:  ▼

1
2
3
4

**Explanation**

**Explanation/Reference:**

Explanation:

Box 1: 2

One management group for East, and one for West.

When creating a blueprint definition, you'll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is available to assign to any child subscription of that management group.

Box 2: 1

One definition as the you plan to deploy a custom application to each subscription.

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved.

Box 3: 4

One assignment for each subscription.

Reference:

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

**QUESTION 11**

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

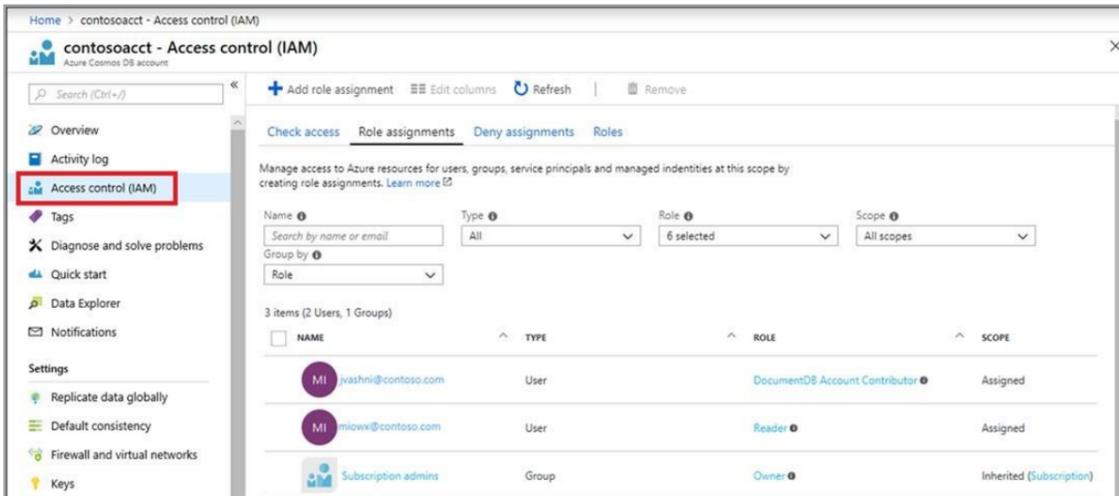
**Correct Answer: C**

**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 12**

**HOTSPOT**

You need to design a resource governance solution for an Azure subscription. The solution must meet the following requirements:

- Ensure that all ExpressRoute resources are created in a resource group named RG1.
- Delegate the creation of the ExpressRoute resources to an Azure Active Directory (Azure AD) group named Networking.
- Use the principle of least privilege.

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

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

**Hot Area:**

**Answer Area**

Ensure that all ExpressRoute resources are created in RG1:

- A custom RBAC role assignment at the level of RG1
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- An Azure Policy assignment at the subscription level that has an exclusion
- Multiple Azure Policy assignments at the resource group level except for RG1

Delegate the creation of the ExpressRoute resources to Networking:

- A custom RBAC role assignment at the level of RG1
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- An Azure Policy assignment at the subscription level that has an exclusion
- Multiple Azure Policy assignments at the resource group level except for RG1

**Correct Answer:**

**Answer Area**

Ensure that all ExpressRoute resources are created in RG1:

- A custom RBAC role assignment at the level of RG1
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- An Azure Policy assignment at the subscription level that has an exclusion**
- Multiple Azure Policy assignments at the resource group level except for RG1

Delegate the creation of the ExpressRoute resources to Networking:

- A custom RBAC role assignment at the level of RG1**
- A custom RBAC role assignment at the subscription level
- An Azure Blueprints assignment that sets locking mode for the level of RG1
- An Azure Policy assignment at the subscription level that has an exclusion
- Multiple Azure Policy assignments at the resource group level except for RG1

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

Box 1: An Azure policy assignment at the subscription level that has an exclusion

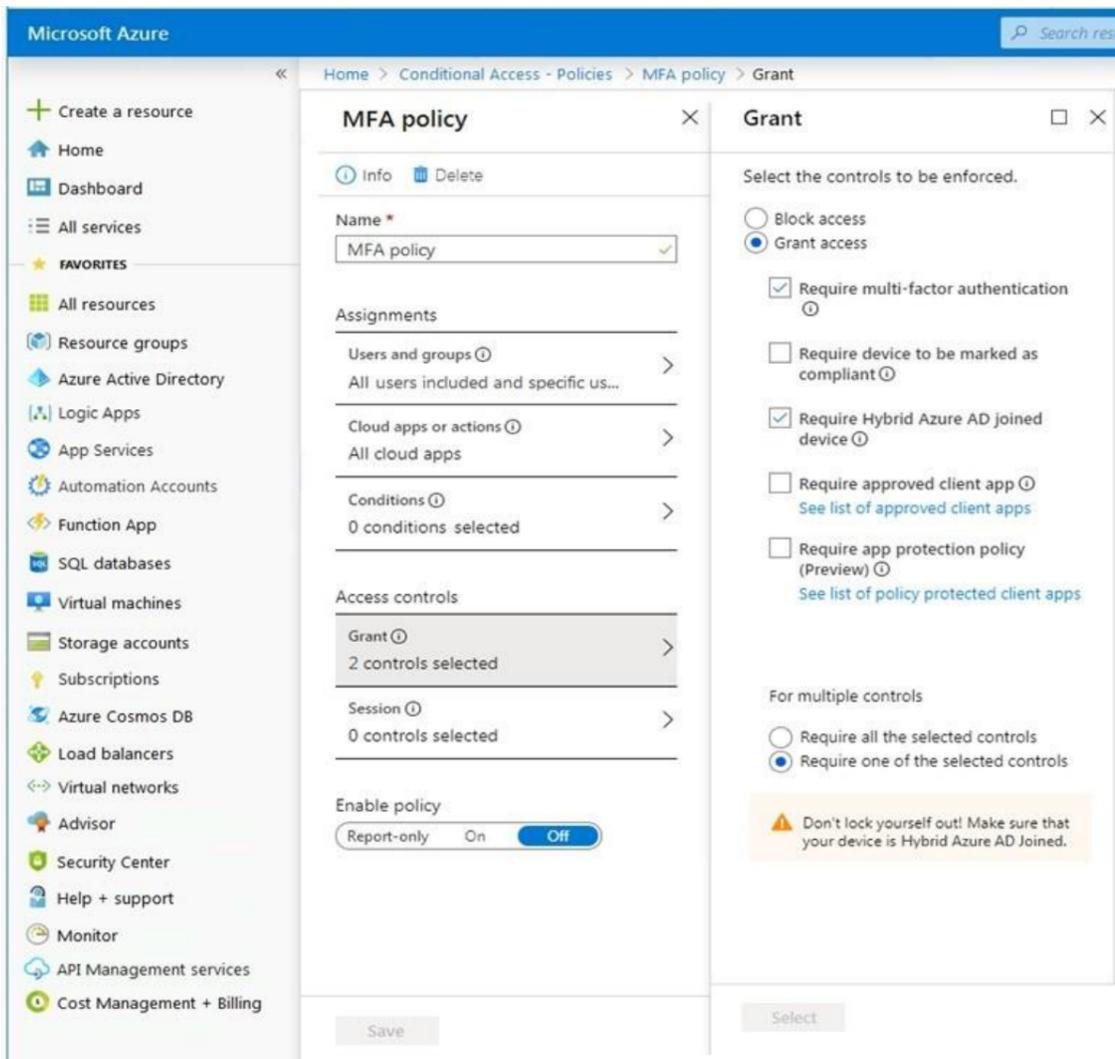
Box 2: A custom RBAC role assignment at the level of RG1

Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope.

Reference:  
<https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage>

**QUESTION 13**

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.)



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**

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

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

**QUESTION 14**

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

**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 15

You have an Azure subscription that contains resources in three Azure regions.

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?

- A. 1
- B. 2
- C. 3
- D. 6

**Correct Answer:** A

**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 16

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

**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 17**

**DRAG DROP**

Your company has users who work remotely from laptops.

You plan to move some of the applications accessed by the remote users to Azure virtual machines. The users will access the applications in Azure by using a point-to-site VPN connection. You will use certificates generated from an on-premises-based Certification authority (CA).

You need to recommend which certificates are required for the deployment.

What should you include in the recommendation? To answer, drag the appropriate certificates to the correct targets. Each certificate 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.

**Select and Place:**

Certificates	Answer Area
A root CA certificate that has the private key	Trusted Root Certification Authorities certificate store on each laptop: Certificate
A root CA certificate that has the public key only	The users' Personal store on each laptop: Certificate
A user certificate that has the private key	The Azure VPN gateway: Certificate
A user certificate that has the public key only	

**Correct Answer:**

Certificates	Answer Area
A root CA certificate that has the private key	Trusted Root Certification Authorities certificate store on each laptop: A root CA certificate that has the public key only
A root CA certificate that has the public key only	The users' Personal store on each laptop: A user certificate that has the private key
A user certificate that has the private key	The Azure VPN gateway: A user certificate that has the public key only
A user certificate that has the public key only	

**Explanation**

**Explanation/Reference:**

**QUESTION 18**

**HOTSPOT**

You are building an application that will run in a virtual machine (VM). The application will use Azure Managed Identity.

The application uses Azure Key Vault, Azure SQL Database, and Azure Cosmos DB.

You need to ensure the application can use secure credentials to access these services.

Which authentication method should you recommend? To answer, select the appropriate options in the answer area.

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

**Hot Area:**

**Answer Area**

Functionality	Authorization method
Azure Key Vault	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; border-bottom: 1px solid gray;">▼</div> <div style="padding: 2px;">                     Hash-based message authentication code (HMAC)                      Azure Managed Identity                      Role-Based Access Controls (RBAC)                      HTTPS encryption                 </div> </div>
Azure SQL	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; border-bottom: 1px solid gray;">▼</div> <div style="padding: 2px;">                     Hash-based message authentication code (HMAC)                      Azure Managed Identity                      Role-Based Access Controls (RBAC)                      HTTPS encryption                 </div> </div>
Cosmos DB	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; border-bottom: 1px solid gray;">▼</div> <div style="padding: 2px;">                     Hash-based message authentication code (HMAC)                      Azure Managed Identity                      Role-Based Access Controls (RBAC)                      HTTPS encryption                 </div> </div>

**Correct Answer:**

**Answer Area**

Functionality	Authorization method
Azure Key Vault	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; border-bottom: 1px solid gray;">▼</div> <div style="padding: 2px;">                     Hash-based message authentication code (HMAC)  <span style="background-color: #d9ead3; padding: 2px;">Azure Managed Identity</span>                      Role-Based Access Controls (RBAC)                      HTTPS encryption                 </div> </div>
Azure SQL	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; border-bottom: 1px solid gray;">▼</div> <div style="padding: 2px;">                     Hash-based message authentication code (HMAC)  <span style="background-color: #d9ead3; padding: 2px;">Azure Managed Identity</span>                      Role-Based Access Controls (RBAC)                      HTTPS encryption                 </div> </div>
Cosmos DB	<div style="border: 1px solid gray; padding: 2px;"> <div style="background-color: #f0f0f0; padding: 2px; border-bottom: 1px solid gray;">▼</div> <div style="padding: 2px;">                     Hash-based message authentication code (HMAC)  <span style="background-color: #d9ead3; padding: 2px;">Azure Managed Identity</span>                      Role-Based Access Controls (RBAC)                      HTTPS encryption                 </div> </div>

**Explanation**

**Explanation/Reference:**

Explanation:

Note: Managed identities for Azure resources is the new name for the service formerly known as Managed Service Identity (MSI).

Reference:

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

**QUESTION 19**

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**

**Explanation**

**Explanation/Reference:**

**QUESTION 20**

DRAG DROP

A company named Contoso, Ltd. has an Azure Active Directory (Azure AD) tenant that uses the Basic license.

You plan to deploy two applications to Azure. The applications have the requirements shown in the following table.

Application name	Requirement
Customer	Users must authenticate by using a personal Microsoft account and multi-factor authentication
Reporting	Users must authenticate by using either Contoso credentials or a personal Microsoft account. You must be able to manage the accounts from Azure AD.

Which authentication strategy should you recommend for each application? To answer, drag the appropriate authentication strategies to the correct applications. Each authentication strategy 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.

**Select and Place:**

<p><b>Authentication Strategies</b></p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">An Azure AD B2C tenant</div> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">An Azure AD v1.0 endpoint</div> <div style="border: 1px solid gray; padding: 2px;">An Azure AD v2.0 endpoint</div>	<p><b>Answer Area</b></p> <p>Customer: <div style="border: 1px solid gray; padding: 2px; display: inline-block;">Authentication strategy</div></p> <p>Reporting: <div style="border: 1px solid gray; padding: 2px; display: inline-block;">Authentication strategy</div></p>
---	--

**Correct Answer:**

<p><b>Authentication Strategies</b></p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">An Azure AD B2C tenant</div> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 5px;">An Azure AD v1.0 endpoint</div> <div style="border: 1px solid gray; padding: 2px;">An Azure AD v2.0 endpoint</div>	<p><b>Answer Area</b></p> <p>Customer: <div style="border: 1px solid gray; padding: 2px; display: inline-block;">An Azure AD v2.0 endpoint</div></p> <p>Reporting: <div style="border: 1px solid gray; padding: 2px; display: inline-block;">An Azure AD B2C tenant</div></p>
---	---

**Explanation**

**Explanation/Reference:**

Explanation:

Box 1: Azure AD V2.0 endpoint

Microsoft identity platform is an evolution of the Azure Active Directory (Azure AD) developer platform. It allows developers to build applications that sign in all Microsoft identities and get tokens to call Microsoft APIs, such as Microsoft Graph, or APIs that developers have built. The Microsoft identity platform consists of: OAuth 2.0 and OpenID Connect standard-compliant authentication service that enables developers to authenticate any Microsoft identity, including:

- Work or school accounts (provisioned through Azure AD)
- Personal Microsoft accounts (such as Skype, Xbox, and Outlook.com)
- Social or local accounts (via Azure AD B2C)

Box 2: Azure AD B2C tenant

Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

Azure Active Directory B2C (Azure AD B2C) integrates directly with Azure Multi-Factor Authentication so that you can add a second layer of security to sign-up and sign-in experiences in your applications.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-reference-mfa>

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-overview>

**QUESTION 21**

HOTSPOT

You manage a network that includes an on-premises Active Directory domain and an Azure Active Directory (Azure AD).

Employees are required to use different accounts when using on-premises or cloud resources. You must recommend a solution that lets employees sign in to all company resources by using a single account. The solution must implement an identity provider.

You need to provide guidance on the different identity providers.

How should you describe each identity provider? To answer, select the appropriate description from each list in the answer area.

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

**Hot Area:**

Identity Provider	Description
synchronized identity	<input type="checkbox"/> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. <input type="checkbox"/> User management occurs on-premises. The on-premises domain controller authenticates employee credentials. <input type="checkbox"/> Both user management and authentication occur in Azure AD.
federated identity	<input type="checkbox"/> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. <input type="checkbox"/> User management occurs on-premises. The on-premises domain controller authenticates employee credentials. <input type="checkbox"/> Both user management and authentication occur in Azure AD.

**Correct Answer:**

Identity Provider	Description
synchronized identity	<input checked="" type="checkbox"/> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. <input type="checkbox"/> User management occurs on-premises. The on-premises domain controller authenticates employee credentials. <input type="checkbox"/> Both user management and authentication occur in Azure AD.
federated identity	<input type="checkbox"/> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. <input checked="" type="checkbox"/> User management occurs on-premises. The on-premises domain controller authenticates employee credentials. <input type="checkbox"/> Both user management and authentication occur in Azure AD.

**Explanation**

**Explanation/Reference:**

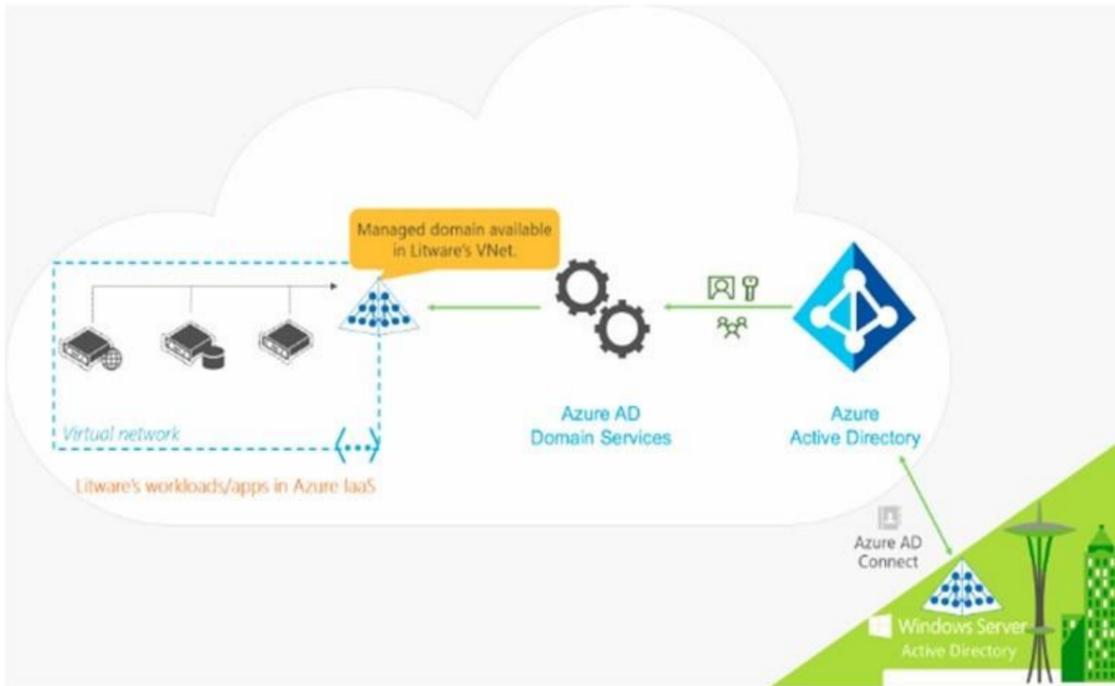
Explanation:

Box1: User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords.

**Azure AD Domain Services for hybrid organizations**

Organizations with a hybrid IT infrastructure consume a mix of cloud resources and on-premises resources. Such organizations synchronize identity information from their on-premises directory to their Azure AD tenant. As hybrid organizations look to migrate more of their on-premises applications to the cloud, especially legacy directory-aware applications, Azure AD Domain Services can be useful to them.

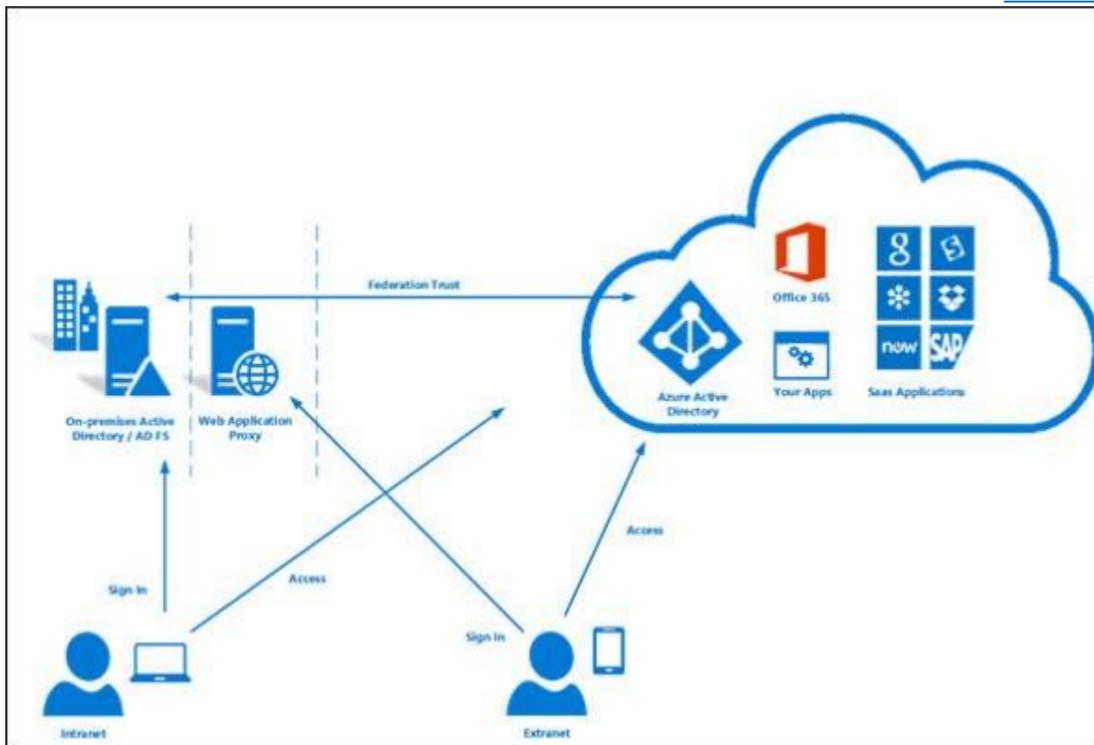
Example: Litware Corporation has deployed Azure AD Connect, to synchronize identity information from their on-premises directory to their Azure AD tenant. The identity information that is synchronized includes user accounts, their credential hashes for authentication (password hash sync) and group memberships.



User accounts, group memberships, and credentials from Litware's on-premises directory are synchronized to Azure AD via Azure AD Connect. These user accounts, group memberships, and credentials are automatically available within the managed domain.

Box 2: User management occurs on-premises. The on-premises domain controller authenticates employee credentials.

You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises.



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview>

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed>

**QUESTION 22**

**HOTSPOT**

You configure the Diagnostics settings for an Azure SQL database as shown in the following exhibit.

**Diagnostics settings** ×

---

Save Discard Delete

---

Name

Diagnostics

Archive to a storage account  
 Stream to an event hub  
 Send to Log Analytics

Subscription

Azure Pass - Sponsorship

Log Analytics Workspace

sk191124 ( westeurope )

---

log

SQLInsights  
 AutomaticTuning  
 QueryStoreRuntimeStatistics  
 QueryStoreWaitStatistics  
 Errors  
 DatabaseWaitStatistics  
 Timeouts  
 Blocks  
 Deadlocks

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.

**Hot Area:**

**Answer Area**

To perform real-time reporting by using Microsoft Power BI, you must first **[answer choice]**.

- clear Send to Log Analytics
- clear SQLInsights
- select Archive to a storage account
- select Stream to an event hub

Diagnostics data can be reviewed in **[answer choice]**.

- Azure Analysis Services
- Azure Application Insights
- Azure SQL Analytics
- Microsoft SQL Server Analysis Services (SSAS)
- SQL Health Check

**Correct Answer:**

**Answer Area**

To perform real-time reporting by using Microsoft Power BI, you must first **[answer choice]**.

- clear Send to Log Analytics
- clear SQLInsights
- select Archive to a storage account
- select Stream to an event hub

Diagnostics data can be reviewed in **[answer choice]**.

- Azure Analysis Services
- Azure Application Insights
- Azure SQL Analytics
- Microsoft SQL Server Analysis Services (SSAS)
- SQL Health Check

**Explanation**

**Explanation/Reference:**

**QUESTION 23**

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?

- 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**

**Explanation**

**Explanation/Reference:**

Reference:

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

**QUESTION 24**

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

**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 25**

**HOTSPOT**

You have an existing implementation of Microsoft SQL Server Integration Services (SSIS) packages stored in an SSISDB catalog on your on-premises network.

The on-premises network does not have hybrid connectivity to Azure by using Site-to-Site VPN or ExpressRoute.

You want to migrate the packages to Azure Data Factory.

You need to recommend a solution that facilitates the migration while minimizing changes to the existing packages. The solution must minimize costs.

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

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

**Hot Area:**

**Correct Answer:**

**Explanation**

**Explanation/Reference:**

Explanation:

Box 1: Azure SQL database

You can't create the SSISDB Catalog database on Azure SQL Database at this time independently of creating the Azure-SSIS Integration Runtime in Azure Data Factory. The Azure-SSIS IR is the runtime environment that runs SSIS packages on Azure.

Box 2: Azure-SQL Server Integration Service Integration Runtime and self-hosted integration runtime

The Integration Runtime (IR) is the compute infrastructure used by Azure Data Factory to provide data integration capabilities across different network environments. Azure-SSIS Integration Runtime (IR) in Azure Data Factory (ADF) supports running SSIS packages.

Self-hosted integration runtime can be used for data movement in this scenario.

Reference:

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

<https://docs.microsoft.com/en-us/sql/integration-services/lift-shift/ssis-azure-connect-to-catalog-database>

**QUESTION 26**

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**

**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 27**

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**

**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 28**

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**

**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 29**

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**

**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>

**QUESTION 30**

HOTSPOT

Your company is designing a multi-tenant application that will use elastic pools and Azure SQL databases. The application will be used by 30 customers.

You need to design a storage solution for the application. The solution must meet the following requirements:

- Operational costs must be minimized.
  - All customers must have their own database.
  - The customer databases will be in one of the following three Azure regions: East US, North Europe, or South Africa North.
- What is the minimum number of elastic pools and Azure SQL Database servers required? To answer, select the appropriate options in the answer area.

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

**Hot Area:**

**Correct Answer:**

**Explanation**

**Explanation/Reference:**

Explanation:

Box 1: 3

The server, its pools & databases must be in the same Azure region under the same subscription.

Box 2: 3

A server can have up to 5000 databases associated to it.

Reference:

<https://vincentlauzon.com/2016/12/18/azure-sql-elastic-pool-overview/>

#### QUESTION 31

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**

**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 32

**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**

**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 33

**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**

**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 34

**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**

**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 35

**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**

**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 41**

You deploy two instances of an Azure web app. One instance is in the East US Azure region and the other instance is in the West US Azure region. The web app uses Azure Blob storage to deliver large files to end users.

You need to recommend a solution for delivering the files to the users. The solution must meet the following requirements:

- Ensure that the users receive files from the same region as the web app that they access.
- Ensure that the files only need to be uploaded once.
- Minimize costs.

What should you include in the recommendation?

- A. Distributed File System (DFS)
- B. read-access geo-redundant storage (RA-GRS)
- C. Azure File Sync
- D. geo-redundant storage (GRS)

**Correct Answer: B**

**Explanation**

**Explanation/Reference:**

**QUESTION 42**

You are developing a web application that provides streaming video to users. You configure the application to use continuous integration and deployment.

The app must be highly available and provide a continuous streaming experience for users.

You need to recommend a solution that allows the application to store data in a geographical location that is closest to the user.

What should you recommend?

- A. Azure Content Delivery Network (CDN)
- B. Azure Redis Cache
- C. Azure App Service Web Apps
- D. Azure App Service Isolated

**Correct Answer: A**

**Explanation**

**Explanation/Reference:**

Explanation:

Azure Content Delivery Network (CDN) is a global CDN solution for delivering high-bandwidth content. It can be hosted in Azure or any other location. With Azure CDN, you can cache static objects loaded from Azure Blob storage, a web application, or any publicly accessible web server, by using the closest point of presence (POP) server. Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various network and routing optimizations.

Reference:

<https://docs.microsoft.com/en-in/azure/cdn/>

**QUESTION 43**

**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 need to deploy resources to host a stateless web app in an Azure subscription. The solution must meet the following requirements:

- Provide access to the full .NET framework.
- Provide redundancy if an Azure region fails.
- Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy a virtual machine scale set that uses autoscaling.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: B**

**Explanation**

**Explanation/Reference:**

Explanation:

Instead, you should deploy two Azure virtual machines to two Azure regions, and you create a Traffic Manager profile.

**QUESTION 44**

**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 need to deploy resources to host a stateless web app in an Azure subscription. The solution must meet the following requirements:

- Provide access to the full .NET framework.
- Provide redundancy if an Azure region fails.
- Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy two Azure virtual machines to two Azure regions, and you deploy an Azure Application Gateway.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: B**

**Explanation**

**Explanation/Reference:**

Explanation:

You need to deploy two Azure virtual machines to two Azure regions, but also create a Traffic Manager profile.

**QUESTION 45**

**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 need to deploy resources to host a stateless web app in an Azure subscription. The solution must meet the following requirements:

- Provide access to the full .NET framework.
- Provide redundancy if an Azure region fails.
- Grant administrators access to the operating system to install custom application dependencies.

Solution: You deploy two Azure virtual machines to two Azure regions, and create a Traffic Manager profile.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: A**

**Explanation**

**Explanation/Reference:**

**QUESTION 46**

**HOTSPOT**

You plan to deploy a network-intensive application to several Azure virtual machines.

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

- Minimizes the use of the virtual machine processors to transfer data
- Minimizes network latency

Which virtual machine size and feature should you use? To answer, select the appropriate options in the answer area.

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

**Hot Area:**

**Correct Answer:**

**Explanation**

**Explanation/Reference:**

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-hpc#h-series>

**QUESTION 47**

You need to recommend a solution to deploy containers that run an application. The application has two tiers. Each tier is implemented as a separate Docker Linux-based image. The solution must meet the following requirements:

- The front-end tier must be accessible by using a public IP address on port 80.
- The backend tier must be accessible by using port 8080 from the front-end tier only.
- Both containers must be able to access the same Azure file share.
- If a container fails, the application must restart automatically.
- Costs must be minimized.

What should you recommend using to host the application?

- A. Azure Kubernetes Service (AKS)
- B. Azure Service Fabric
- C. Azure Container instances

**Correct Answer: C**

**Explanation**

**Explanation/Reference:**

Explanation:

Azure Container Instances enables a layered approach to orchestration, providing all of the scheduling and management capabilities required to run a single container, while allowing orchestrator platforms to manage multi-container tasks on top of it.

Because the underlying infrastructure for container instances is managed by Azure, an orchestrator platform does not need to concern itself with finding an appropriate host machine on which to run a single container.

Azure Container Instances can schedule both Windows and Linux containers with the same API.

Orchestration of container instances exclusively

Because they start quickly and bill by the second, an environment based exclusively on Azure Container Instances offers the fastest way to get started and to deal with highly variable workloads.

Reference:

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-overview>

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-orchestrator-relationship>

**QUESTION 48**

You architect a solution that calculates 3D geometry from height-map data.

You have the following requirements:

- Perform calculations in Azure.
- Each node must communicate data to every other node.
- Maximize the number of nodes to calculate multiple scenes as fast as possible.
- Require the least amount of effort to implement.

You need to recommend a solution.

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 render farm that uses Azure Batch.
- B. Create a render farm that uses virtual machines (VMs).
- C. Enable parallel task execution on compute nodes.

- D. Create a render farm that uses virtual machine (VM) scale sets.
- E. Enable parallel file systems on Azure.

**Correct Answer:** AC

**Explanation**

**Explanation/Reference:**

**QUESTION 49**

Your company plans to publish APIs for its services by using Azure API Management.

You discover that service responses include the AspNet-Version header.

You need to recommend a solution to remove AspNet-Version from the response of the published APIs.

What should you include in the recommendation?

- A. a new product
- B. a modification to the URL scheme
- C. a new policy
- D. a new revision

**Correct Answer:** C

**Explanation**

**Explanation/Reference:**

Explanation:

Set a new transformation policy to transform an API to strip response headers.

Reference:

<https://docs.microsoft.com/en-us/azure/api-management/transform-api>

**QUESTION 50**

You have an Azure subscription that contains a storage account.

An application sometimes writes duplicate files to the storage account.

You have a PowerShell script that identifies and deletes duplicate files in the storage account. Currently, the script is run manually after approval from the operations manager.

You need to recommend a serverless solution that performs the following actions:

- Runs the script once an hour to identify whether duplicate files exist
- Sends an email notification to the operations manager requesting approval to delete the duplicate files
- Processes an email response from the operations manager specifying whether the deletion was approved
- Runs the script if the deletion was approved

What should you include in the recommendation?

- A. Azure Logic Apps and Azure Functions
- B. Azure Pipelines and Azure Service Fabric
- C. Azure Logic Apps and Azure Event Grid
- D. Azure Functions and Azure Batch

**Correct Answer:** A

**Explanation**

**Explanation/Reference:**

Explanation:

You can schedule a powershell script with Azure Logic Apps.

When you want to run code that performs a specific job in your logic apps, you can create your own function by using Azure Functions. This service helps you create Node.js, C#, and F# functions so you don't have to build a complete app or infrastructure to run code. You can also call logic apps from inside Azure functions. Azure Functions provides serverless computing in the cloud and is useful for performing tasks such as these examples:

Reference:

<https://docs.microsoft.com/en-us/azure/logic-apps/logic-apps-azure-functions>

**QUESTION 56**

You have an on-premises network to which you deploy a virtual appliance.

You plan to deploy several Azure virtual machines and connect the on-premises network to Azure by using a Site-to-Site connection.

All network traffic that will be directed from the Azure virtual machines to a specific subnet must flow through the virtual appliance.

You need to recommend solutions to manage network traffic.

Which two options should you recommend? Each correct answer presents a complete solution.

- A. Configure Azure Traffic Manager.
- B. Implement Azure ExpressRoute.
- C. Configure a routing table.
- D. Implement an Azure virtual network.

**Correct Answer:** BC

**Explanation**

**Explanation/Reference:**

Explanation:

B: Forced tunneling lets you redirect or "force" all Internet-bound traffic back to your on-premises location via a Site-to-Site VPN tunnel for inspection and auditing. This is a critical security requirement for most enterprise IT policies. Without forced tunneling, Internet-bound traffic from your VMs in Azure always traverses from Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic.

Forced tunneling in Azure is configured via virtual network user-defined routes.

C: ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure, Office 365, and Dynamics 365.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a co-location facility. ExpressRoute connections do not go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet.

Reference:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm>

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

**QUESTION 57**

You are developing a sales application that will contain several Azure cloud services and will handle different components of a transaction. Different cloud services will process customer orders, billing, payment, inventory, and shipping.

You need to recommend a solution to enable the cloud services to asynchronously communicate transaction information by using REST messages.

What should you include in the recommendation?

- A. Azure Service Bus
- B. Azure Blob storage
- C. Azure Notification Hubs
- D. Azure Application Gateway

**Correct Answer: A**

**Explanation**

**Explanation/Reference:**

Explanation:

Service Bus is a transactional message broker and ensures transactional integrity for all internal operations against its message stores. All transfers of messages inside of Service Bus, such as moving messages to a dead-letter queue or automatic forwarding of messages between entities, are transactional.

Incorrect Answers:

C: Azure Notification Hubs is a massively scalable mobile push notification engine for quickly sending millions of notifications to iOS, Android, Windows, or Kindle devices.

Reference:

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

**QUESTION 58**

You are designing a message application that will run on an on-premises Ubuntu virtual machine. The application will use Azure Storage queues.

You need to recommend a processing solution for the application to interact with the storage queues. The solution must meet the following requirements:

- Create and delete queues daily.
- Be scheduled by using a CRON job.
- Upload messages every five minutes.

What should developers use to interact with the queues?

- A. Azure CLI
- B. AzCopy
- C. Azure Data Factory
- D. .NET Core

**Correct Answer: D**

**Explanation**

**Explanation/Reference:**

Explanation:

Incorrect Answers:

A: It is not possible to have Linux running in Windows Azure

B: AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/queues/storage-tutorial-queues>

## Design Monitoring

### 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.

#### 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 on-premises 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

**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 on-premises 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)

**QUESTION 2**

**HOTSPOT**

To meet the authentication requirements of Fabrikam, what should you include in the solution? To answer, select the appropriate options in the answer area.

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

**Hot Area:**

**Answer Area**

Minimum number of Azure AD tenants:  ▼

0
1
2
3
4

Minimum number of custom domains to add:  ▼

0
1
2
3
4

Minimum number of conditional access policies to create:  ▼

0
1
2
3
4

**Correct Answer:**

**Answer Area**

Minimum number of Azure AD tenants:  ▼

0
1
2
3
4

Minimum number of custom domains to add:  ▼

0
1
2
3
4

Minimum number of conditional access policies to create:  ▼

0
1
2
3
4

**Explanation**

**Explanation/Reference:**

Explanation:

Box 1: 2

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

Box 2: 1

Box 3: 1

Scenario:

- 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.

Note:

Users must always authenticate by using their corp.fabrikam.com UPN identity.

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.

## Design Monitoring

### Testlet 3

#### 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

## Design Monitoring

### Testlet 4

#### 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 on-premises 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

You need to recommend a solution to meet the database retention requirement.

What should you recommend?

- A. Configure geo-replication of the database.
- B. Configure a long-term retention policy for the database.
- C. Configure Azure Site Recovery.
- D. Use automatic Azure SQL Database backups.

**Correct Answer: B**

**QUESTION 2**

You need to recommend a strategy for migrating the database content of WebApp1 to Azure.

What should you include in the recommendation?

- A. Use Azure Site Recovery to replicate the SQL servers to Azure.
- B. Copy the BACPAC file that contains the Azure SQL database files to Azure Blob storage.
- C. Use SQL Server transactional replication.
- D. Copy the VHD that contains the Azure SQL database files to Azure Blob storage.

**Correct Answer: D**

**Explanation**

**Explanation/Reference:**

Explanation:

Before you upload a Windows virtual machine (VM) from on-premises to Azure, you must prepare the virtual hard disk (VHD or VHDX).

Scenario: 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.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/prepare-for-upload-vhd-image>