AZ-301.prepaway.premium.exam.193q

PrepAway

AZ-301

Microsoft Azure Architect Design

Version 8.0

Testlet 1

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

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

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

To start the case study
To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirement, 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.

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.

Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, at 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.

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.
▪ 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 transactions query system remains available without any administrative intervention.

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. legitimate users must be able to

authenticate successfully by using multi-factor authentication.

QUESTION 1
You need to recommend a solution for the collection of security logs for the middle tier of the payment processing system.

What should you include in the recommendation?

A. Azure Event Hubs
B. Azure Notification Hubs
C. the Azure Diagnostics agent
D. the Microsoft Monitoring agent

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Scenario: Collect Windows security logs from all the middle-tier servers and retain the logs for a period of seven years.

The Azure Diagnostics agent should be used when you want to archive logs and metrics to Azure storage.

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agents-overview

Question Set 2

QUESTION 1
HOTSPOT

You deploy several Azure SQL Database instances.

You plan to configure the Diagnostics settings on the databases as shown in the following exhibit.

Diagnostics settings

Save   Discard   Delete

*
Diagnostics

☑ Archive to a storage account

Storage account
fabrikam8977237

☐ Stream to an event hub

☑ Send to Log Analytics
Subscription
Microsoft AZ-101 4
Log Analytics Workspace
FabrikamProductionWorkspace(westeurope)
Log Analytics
fabrikamproductionworkspace

LOG

☑ SQLInsights   Retention (days)   90

☑ AutomaticTuning   Retention (days)   30

☐ QueryStoreRuntimeStatistics   Retention (days)   0

☐ QueryStoreWaitStatistics   Retention (days)   0

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

The amount of time that SQLInsights data will be stored in blob storage is **[answer choice].**

▼
30 days
90 days
730 days
indefinite

The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is **[answer choice].**

▼
30 days
90 days
730 days
indefinite

Correct Answer:

Answer Area

◆ The amount of time that SQLInsights data will be stored in blob storage is **[answer choice].**

▼
30 days
90 days
730 days
indefinite

The maximum amount of time that SQLInsights data can be stored in Azure Log Analytics is **[answer choice].**

▼
30 days
90 days
730 days
indefinite

Section: [none]
Explanation

Explanation/Reference:
Explanation:
In the exhibit, the SQLInsights data is configured to be stored in Azure Log Analytics for 90 days. However, the

question is asking for the "maximum" amount of time that the data can be stored which is 730 days.

QUESTION 2
Your company uses Microsoft System Center Service Manager on its on-premises network.

You plan to deploy several services to Azure.

You need to recommend a solution to push Azure service health alerts to Service Manager.

What should you include in the recommendation?

A. Azure Notification Hubs
B. Azure Event Hubs
C. IT Service Management Connector (ITSM)
D. Application Insights Connector

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/itsmc-overview

QUESTION 3
You have an on-premises Hyper-V cluster. The cluster contains Hyper-V hosts that run Windows Server 2016
Datacenter. The hosts are licensed under a Microsoft Enterprise Agreement that has Software Assurance.

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

Correct Answer: AE
Section: [none]
Explanation

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

E: 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.

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

QUESTION 4
You have an on-premises Active Directory forest and an Azure Active Directory (Azure AD) tenant. All Azure AD users are assigned a Premium P1 license.

You deploy Azure AD Connect.

Which two features are available in this environment that can reduce operational overhead for your company's help desk? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Azure AD Privileged Identity Management policies
B. access reviews
C. self-service password reset
D. Microsoft Cloud App Security Conditional Access App Control
E. password writeback

Correct Answer: CE
Section: [none]
Explanation

Explanation/Reference:

QUESTION 5
You are planning the implementation of an order processing web service that will contain microservices hosted in an Azure Service Fabric cluster.

You need to recommend a solution to provide developers with the ability to proactively identify and fix performance issues. The developers must be able to simulate user connections to the order processing web service from the Internet, as well as simulate user transactions. The developers must be notified if the goals for the transaction response times are not met.

What should you include in the recommendation?

A. container health
B. Azure Network Watcher
C. Application Insights
D. Service Fabric Analytics

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 6
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. Azure Analysis Services
B. Azure Activity Log
C. Azure Monitor action groups
D. Azure Advisor
E. Azure Monitor metrics
F. Azure Log Analytics
G. Application Insights

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
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/resource-group-audit

QUESTION 7
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.	▼ Azure Application Insights Azure Service Map Azure Monitor Logs Azure Activity Log
Visualize the relationships between application components.	▼ Azure Application Insights Azure Service Map Azure Monitor Logs Azure Activity Log
Track requests and exceptions to a specific line of code within the application.	▼ Azure Application Insights Azure Service Map Azure Monitor Logs Azure Activity Log
Analyze how many users return to the application and how often they select a particular dropdown value.	▼ Azure Application Insights Azure Service Map Azure Monitor Logs Azure Activity Log

Correct Answer:

◆

Answer Area

Scenario	Azure monitoring service
Correlate Azure resource usage and performance data with application configuration and performance data.	▼ Azure Application Insights / Azure Service Map / **Azure Monitor Logs** / Azure Activity Log
Visualize the relationships between application components.	▼ Azure Application Insights / **Azure Service Map** / Azure Monitor Logs / Azure Activity Log
Track requests and exceptions to a specific line of code within the application.	▼ **Azure Application Insights** / Azure Service Map / Azure Monitor Logs / Azure Activity Log
Analyze how many users return to the application and how often they select a particular dropdown value.	▼ Azure Application Insights / Azure Service Map / Azure Monitor Logs / **Azure Activity Log**

Section: [none]
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 8
DRAG DROP

You have an Azure Active Directory (Azure AD) tenant. All user accounts are synchronized from an on-premises Active Directory domain and are configured for federated authentication. Active Directory Federation Services (AD FS) servers are published for external connections by using a farm of Web Application Proxy servers.

You need to recommend a solution to monitor the servers that integrate with Azure AD. The solution must meet the following requirements:

- Identify any AD FS issues and their potential resolutions.
- Identify any directory synchronization configuration issues and their potential resolutions
- Notify administrators when there are any issues affecting directory synchronization or AD FS operations.

Which monitoring solution should you recommend for each server type? To answer, drag the appropriate monitoring solutions to the correct server types. Each monitoring solution may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Monitoring Solutions	Answer Area
A Microsoft Office 365 management solution in Azure Monitor	**Monitor**
Active Directory Replication Status Tool	AD FS servers:
An Active Directory Health Check solution in Azure Monitor	Azure AD Connect servers:
An Active Directory Replication Status solution in Azure Monitor	Web Application Proxy servers:
Azure AD Connect Health	
Azure Security Center	

Correct Answer:

Monitoring Solutions	Answer Area
A Microsoft Office 365 management solution in Azure Monitor	**Monitor**
Active Directory Replication Status Tool	AD FS servers: Azure AD Connect Health
An Active Directory Health Check solution in Azure Monitor	Azure AD Connect servers: Azure AD Connect Health
An Active Directory Replication Status solution in Azure Monitor	Web Application Proxy servers: Azure AD Connect Health
Azure AD Connect Health	
Azure Security Center	

Section: [none]
Explanation

Explanation/Reference:

QUESTION 9

You plan to deploy 200 Microsoft SQL Server databases to Azure by using Azure SQL Database and Azure SQL Database Managed Instance.

You need to recommend a monitoring solution that provides a consistent monitoring approach for all deployments. The solution must meet the following requirements:

▪ Support current-state analysis based on metrics collected near real-time, multiple times per minute, and maintained for up to one hour
▪ Support longer term analysis based on metrics collected multiple times per hour and maintained for up to two weeks.
▪ Support monitoring of the number of concurrent logins and concurrent sessions.

What should you include in the recommendation?

A. dynamic management views
B. trace flags
C. Azure Monitor
D. SQL Server Profiler

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 10
DRAG DROP

You plan to move several apps that handle critical line-of-business (LOB) services to Azure.

Appropriate personnel must be notified if any critical resources become degraded or unavailable.

You need to design a monitoring and notification strategy that can handle up to 100 notifications per hour.

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Select and Place:

Actions

Create a resource group containing the critical resources.

Monitor Azure status for warnings and errors.

Create an activity log alert for service health.

Create an action group for alerts to email addresses.

Create an action group for alerts to SMS phone numbers.

Monitor service health for incidents and action required notifications.

Answer Area

Correct Answer:

Actions

Monitor Azure status for warnings and errors.

Create an activity log alert for service health.

Create an action group for alerts to SMS phone numbers.

Answer Area

Create a resource group containing the critical resources.

Create an action group for alerts to email addresses.

Monitor service health for incidents and action required notifications.

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Step 1: Create a resource group containing the critical resources.
In step 2 the action group should be created within this Resource Group.

Step 2: Create an action group for alerts to email addresses.
You configure an action to notify a person by email or SMS, they receive a confirmation indicating they have been added to the action group.

The rate limit thresholds are:
SMS: No more than 1 SMS every 5 minutes.
Voice: No more than 1 Voice call every 5 minutes.
Email: No more than 100 emails in an hour.

Step 3: Monitor service health for incidents and action required notifications
An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor and Service Health alerts use action groups to notify users that an alert has been triggered.

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-rate-limiting

QUESTION 11
DRAG DROP

You manage a solution in Azure.

The solution is performing poorly.

You need to recommend tools to determine causes for the performance issues.

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

NOTE: Each correct selection is worth one point.

Select and Place:

Monitoring solutions

Answer Area

Scenario	Monitoring solution
Azure Log Analytics	Azure Monitor
Metrics on Azure infrastructure	
Functionality of Azure infrastructure	
Security of Azure infrastructure	

Correct Answer:

Monitoring solutions

Azure Log Analytics   Azure Monitor

Answer Area

Scenario	Monitoring solution
Metrics on Azure infrastructure	Azure Monitor
Functionality of Azure infrastructure	Azure Log Analytics
Security of Azure infrastructure	Azure Log Analytics

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: Azure Monitor
Metrics in Azure Monitor are stored in a time-series database which is optimized for analyzing time-stamped data. This makes metrics particularly suited for alerting and fast detection of issues.

Box 2: Azure Log Analytics
Log data collected by Azure Monitor is stored in a Log Analytics workspace, which is based on Azure Data Explorer. Logs in Azure Monitor are especially useful for performing complex analysis across data from a variety of sources.

Box 3: Azure Log Analytics

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform

https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-platform-logs

QUESTION 12
DRAG DROP

You have standard Load balancer configured to support three virtual machines on the same subnet.

You need to recommend a solution to notify administrators when the load balancer fails.

Which metrics should you recommend using to test the load balancer? To answer, drag the appropriate metrics to the correct conditions. Each metric 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:

Metrics

Byte Count	Data Path Availability
Health Probe Status	Packet Count
SNAT Connection Count	SYN Count

Answer Area

Backend instance health: [   ]

Outbound port exhaustion: [   ]

Correct Answer:

Metrics

Byte Count	Data Path Availability
	Packet Count
	SYN Count

Answer Area

Backend instance health: Health Probe Status

Outbound port exhaustion: SNAT Connection Count

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Backend instance health: Health Probe Status
Health Probe Status (DIP Availability): Standard Load Balancer uses a distributed health-probing service that monitors your application endpoint's health according to your configuration settings. This metric provides an aggregate or per-endpoint filtered view of each instance endpoint in the load balancer pool. You can see how Load Balancer views the health of your application, as indicated by your health probe configuration.

Outbound port exhaustion: SNAT connection Count
SNAT connections: Standard Load Balancer reports the number of outbound flows that are masqueraded to the Public IP address front end. Source network address translation (SNAT) ports are an exhaustible resource. This metric can give an indication of how heavily your application is relying on SNAT for outbound originated flows. Counters for successful and failed outbound SNAT flows are reported and can be used to troubleshoot and understand the health of your outbound flows.

Reference:
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-standard-diagnostics

Testlet 1

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

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

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

To start the case study
To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirement, 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.

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.

Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, at 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.

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.
- 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 transactions query system remains available without any administrative intervention.

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. legitimate users must be able to

authenticate successfully by using multi-factor authentication.

QUESTION 1
HOTSPOT

You need to recommend a solution for configuring the Azure Multi-Factor Authentication (MFA) settings.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Azure AD license:

Free
Basic
Premium P1
Premium P2

Access control for the sign-in risk policy:

Allow access and require multi-factor authentication
Allow access and require multi-factor authentication registration
Block access

Access control for the multi-factor authentication registration policy:

Allow access and require multi-factor authentication
Allow access and require multi-factor authentication registration
Block access

Correct Answer:

Answer Area

Azure AD license:

Free
Basic
Premium P1
Premium P2

Access control for the sign-in risk policy:

Allow access and require multi-factor authentication
Allow access and require multi-factor authentication registration
Block access

Access control for the multi-factor authentication registration policy:

Allow access and require multi-factor authentication
Allow access and require multi-factor authentication registration
Block access

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: Premium 1
Azure AD Premium P1 - is an enterprise level edition which provides identity management for on-premise users, remote users and hybrid users accessing applications both locally and over the cloud.

Incorrect:
Not Premium 2: PIM not required. Azure AD Premium P2 - is an edition includes all of the features of Azure AD Premium P1 with the addition of Identity Protection and Privileged Identity Management (PIM).

Box 2: Allow access and require multi-factor authentication
Azure Multi-Factor Authentication provides a means to verify who you are using more than just a username and password. It provides a second layer of security to user sign-ins.

Box 3: Allow access and require authentication registration
In order for users to be able to respond to MFA prompts, they must first register for Azure Multi-Factor Authentication.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-sign-in-risk-policy
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-mfa-policy

QUESTION 2
HOTSPOT

You need to design a solution for securing access to the historical transaction data.

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

The Azure Cosmos DB account will be used to:

▼
Create users and generate resource tokens
Create users and request resource tokens
Generate resource tokens and perform authentication
Request resource tokens and perform authentication

The .NET web service will be used to:

▼
Create users and generate resource tokens
Create users and request resource tokens
Generate resource tokens and perform authentication
Request resource tokens and perform authentication

Correct Answer:

Answer Area

The Azure Cosmos DB account will be used to:

Create users and generate resource tokens
Create users and request resource tokens
Generate resource tokens and perform authentication
Request resource tokens and perform authentication

The .NET web service will be used to:

Create users and generate resource tokens
Create users and request resource tokens
Generate resource tokens and perform authentication
Request resource tokens and perform authentication

Section: [none]
Explanation

Explanation/Reference:

QUESTION 3
HOTSPOT

You need to recommend a solution for the users at Contoso to authenticate to the cloud-based services and the Azure AD-integrated applications.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Install Azure AD Connect and set the user sign-in option to:

Federation with AD FS
Pass-through Authentication
Password Synchronization

Implement load balancing for the components of the authentication solution by using:

Azure Application Gateway and a Basic Load Balancer
Azure Application Gateway and a Standard Load Balancer
Traffic Manager and a Basic Load Balancer
Traffic Manager and a Standard Load Balancer

Correct Answer:

Answer Area

Install Azure AD Connect and set the user sign-in option to:

Federation with AD FS
Pass-through Authentication
Password Synchronization

Implement load balancing for the components of the authentication solution by using:

Azure Application Gateway and a Basic Load Balancer
Azure Application Gateway and a Standard Load Balancer
Traffic Manager and a Basic Load Balancer
Traffic Manager and a Standard Load Balancer

Section: [none]
Explanation

Explanation/Reference:

◆

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 requirement, 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

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

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.

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.

Problem Statements

The use of Web App1 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.

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 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 platform as a service (PaaS).
- 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.

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.

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 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 corp.fabrikam.com to virtual networks in Azure.

C. Deploy a new Azure AD tenant for the authentication of new R&D projects.

D. Deploy domain controllers for the rd.fabrikam.com forest to virtual networks in Azure.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Directory synchronization between Azure Active Directory (Azure AD) and corp.fabrikam.com must not be affected by a link failure between Azure and the 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

Section: [none]
Explanation

Explanation/Reference:

Question Set 3

QUESTION 1
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription named Project1. Only a group named Project1admins is assigned roles in the Project1 subscription. The Project1 subscription contains all the resources for an application named Application1.

Your company is developing a new application named Application2. The members of the Application2 development team belong to an Azure Active Directory (Azure AD) group named App2Dev.

You identify the following requirements for Application2:

- The members of App2Dev must be prevented from changing the role assignments in Azure.
- The members of App2Dev must be able to create new Azure resources required by Application2.
- All the required role assignments for Application2 will be performed by the members of Project1admins.

You need to recommend a solution for the role assignments of Application2.

Solution: Create a new Azure subscription named Project2. Assign Project1admins the Owner role for the Project2 subscription. Assign App2Dev the Contributor role for the Project2 subscription.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 2
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription named Project1. Only a group named Project1admins is assigned roles in the Project1 subscription. The Project1 subscription contains all the resources for an application named Application1.

Your company is developing a new application named Application2. The members of the Application2 development team belong to an Azure Active Directory (Azure AD) group named App2Dev.

You identify the following requirements for Application2:

- The members of App2Dev must be prevented from changing the role assignments in Azure.
- The members of App2Dev must be able to create new Azure resources required by Application2.

- All the required role assignments for Application2 will be performed by the members of Project1admins.

You need to recommend a solution for the role assignments of Application2.

Solution: Create a new Azure subscription named Project2. Assign Project1admins the User Access Administrator role for the Project2 subscription. Assign App2Dev the Owner role for the Project2 subscription.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead, assign Project1admins the Owner role for the Project2 subscription. Assign App2Dev the Contributor role for the Project2 subscription.

QUESTION 3
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription named Project1. Only a group named Project1admins is assigned roles in the Project1 subscription. The Project1 subscription contains all the resources for an application named Application1.

Your company is developing a new application named Application2. The members of the Application2 development team belong to an Azure Active Directory (Azure AD) group named App2Dev.

You identify the following requirements for Application2:

- The members of App2Dev must be prevented from changing the role assignments in Azure.
- The members of App2Dev must be able to create new Azure resources required by Application2.
- All the required role assignments for Application2 will be performed by the members of Project1admins.

You need to recommend a solution for the role assignments of Application2.

Solution: In Project1, create a resource group named Application2RG. Assign Project1admins the Owner role for Application2RG. Assign App2Dev the Contributor role for Application2RG.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:

You should use a separate subscription for Project2.

QUESTION 4
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription that contains a resource group named RG1.

You create an Azure Active Directory (Azure AD) group named ResearchUsers that contains the user accounts of all researchers.

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

▪ The researchers must be allowed to create Azure virtual machines.
▪ The researchers must only be able to create Azure virtual machines by using specific Azure Resource Manager templates.

Solution: Create a lab in Azure DevTest Lab. Configure the DevTest Labs settings. Assign the DevTest Labs User role to the ResearchUsers group.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead: On RG1, assign the Contributor role to the ResearchUsers group. Create a custom Azure Policy definition and assign the policy to RG1.

QUESTION 5
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription that contains a resource group named RG1.

You create an Azure Active Directory (Azure AD) group named ResearchUsers that contains the user accounts of all researchers.

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

▪ The researchers must be allowed to create Azure virtual machines.
▪ The researchers must only be able to create Azure virtual machines by using specific Azure Resource Manager templates.

Solution: Create an Azure DevOps Project. Configure the DevOps Project settings.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead: On RG1, assign the Contributor role to the ResearchUsers group. Create a custom Azure Policy definition and assign the policy to RG1.

QUESTION 6
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription that contains a resource group named RG1.

You create an Azure Active Directory (Azure AD) group named ResearchUsers that contains the user accounts of all researchers.

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

▪ The researchers must be allowed to create Azure virtual machines.
▪ The researchers must only be able to create Azure virtual machines by using specific Azure Resource Manager templates.

Solution: On RG1, assign the Contributor role to the ResearchUsers group. Create a custom Azure Policy definition and assign the policy to RG1.

Does this meet the goal?

◆
A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 7
A company named Contoso Ltd., has a single-domain Active Directory forest named contoso.com.

Contoso is preparing to migrate all workloads to Azure. Contoso wants users to use single sign-on (SSO) when they access cloud-based services that integrate with Azure Active Directory (Azure AD).

You need to identify any objects in Active Directory that will fail to synchronize to Azure AD due to formatting issues. The solution must minimize costs.

What should you include in the solution?

A. Azure Advisor
B. Microsoft Office 365 IdFix
C. Azure AD Connect Health
D. Password Export Server version 3.1 (PES v3.1) in Active Directory Migration Tool (ADMT)

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 8
HOTSPOT

Your company has an API that returns XML data to internal applications.

You plan to migrate the applications to Azure. You also plan to allow the company's partners to access the API.

You need to recommend an API management solution that meets the following requirements:

▪ Internal applications must receive data in the JSON format once the applications migrate to Azure.
▪ Partner applications must have their header information stripped before the applications receive the data.

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

NOTE: Each correct selection is worth one point.

Hot Area:

◆

Answer Area

Minimum number of APIs to add to Azure API Management:

▼
1
2
3

Minimum number of products to publish in Azure API Management:

▼
1
2
3

Minimum number of policy elements to add:

▼
1
2
3

Correct Answer:

◆

Answer Area

Minimum number of APIs to add to Azure API
Management:

1
2
3

Minimum number of products to publish in
Azure API Management:

1
2
3

Minimum number of policy elements to add:

1
2
3

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-add-products

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-policies

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

QUESTION 9
You have an Azure subscription.

You need to recommend a solution to provide developers with the ability to provision Azure virtual machines.
The solution must meet the following requirements:

- Only allow the creation of the virtual machines in specific regions.
- Only allow the creation of specific sizes of virtual machines.

What should include in the recommendation?

A. conditional access policies
B. Azure Policy
C. Azure Resource Manager templates
D. role-based access control (RBAC)

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 10
HOTSPOT

Your company has 20 web APIs that were developed in-house.

The company is developing 10 web apps that will use the web APIs. The web apps and the APIs are registered in the company's Azure Active Directory (Azure AD) tenant. The web APIs are published by using Azure API Management.

You need to recommend a solution to block unauthorized requests originating from the web apps from reaching the web APIs. The solution must meet the following requirements:

▪ Use Azure AD-generated claims.
▪ Minimize configuration and management effort.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Grant permissions to allow the web apps to access the web APIs by using:	▼
	Azure AD
	Azure API Management
	The web APIs

Configure a JSON Web Token (JWT) validation policy by using:	▼
	Azure AD
	Azure API Management
	The web APIs

Correct Answer:

Answer Area

Grant permissions to allow the web apps to access the web APIs by using:

	▼
Azure AD	
Azure API Management	
The web APIs	

Configure a JSON Web Token (JWT) validation policy by using:

	▼
Azure AD	
Azure API Management	
The web APIs	

Section: [none]
Explanation

Explanation/Reference:

QUESTION 11
HOTSPOT

You are designing an access policy for the sales department at your company.

Occasionally, the developers at the company must stop, start, and restart Azure virtual machines. The development team changes often.

You need to recommend a solution to provide the developers with the required access to the virtual machines. The solution must meet the following requirements:

- Provide permissions only when needed.
- Use the principle of least privilege.
- Minimize costs.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Azure Active Directory (Azure ID) license:	▼
Free	
Basic	
Premium P1	
Premium P2	

Security feature:	▼
Just in time VM access	
A conditional access policy	
Privileged Identity Management for the Azure resources	

Correct Answer:

Answer Area

Azure Active Directory (Azure ID) license:	▼
Free	
Basic	
Premium P1	
Premium P2	

Security feature:	▼
Just in time VM access	
A conditional access policy	
Privileged Identity Management for the Azure resources	

◆

Section: [none]
Explanation

Explanation/Reference:

QUESTION 12
Your network contains an on-premises Active Directory forest.

You discover that when users change jobs within your company, the membership of the user groups are not being updated. As a result, the users can access resources that are no longer relevant to their job.

You plan to integrate Active Directory and Azure Active Directory (Azure AD) by using Azure AD Connect.

You need to recommend a solution to ensure that group owners are emailed monthly about the group memberships they manage.

What should you include in the recommendation?

A. Azure AD access reviews

B. Tenant Restrictions
C. Azure AD Identity Protection
D. conditional access policies

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

QUESTION 13
HOTSPOT

You are designing a software as a service (SaaS) application that will enable Azure Active Directory (Azure AD) users to create and publish surveys. The SaaS application will have a front-end web app and a back-end web API. The web app will rely on the web API to handle updates to customer surveys.

You need to design an authorization flow for the SaaS application. The solution must meet the following requirements:

▪ To access the back-end web API, the web app must authenticate by using OAuth 2 bearer tokens.
▪ The web app must authenticate by using the identities of individual users.

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:

The access tokens will be generated by:

Azure AD
A web app
A web API

Authorization decisions will be performed by:

Azure AD
A web app
A web API

Correct Answer:

Answer Area:

The access tokens will be generated by:

Azure AD
A web app
A web API

Authorization decisions will be performed by:

Azure AD
A web app
A web API

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/lb-lu/azure/architecture/multitenant-identity/web-api

https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-v1-dotnet-webapi

QUESTION 14
HOTSPOT

You have five .NET Core applications that run on 10 Azure virtual machines in the same subscription.

You need to recommend a solution to ensure that the applications can authenticate by using the same Azure Active Directory (Azure AD) identity. The solution must meet the following requirements:

▪ Ensure that the applications can authenticate only when running on the 10 virtual machines.
▪ Minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

To provision the Azure AD identity:

▼
Create a system-assigned **Managed Identities for Azure resources**
Create a user-assigned **Managed Identities for Azure resources**
Register each application in Azure AD

To authenticate request a token by using:

▼
An Azure AD v1.0 endpoint
An Azure AD v2.0 endpoint
An Azure Instance Metadata Service Identity
OAuth2 endpoint

Correct Answer:

Answer Area

To provision the Azure AD identity:

▼
Create a system-assigned **Managed Identities for Azure resources**
Create a user-assigned **Managed Identities for Azure resources**
Register each application in Azure AD

To authenticate request a token by using:

▼
An Azure AD v1.0 endpoint
An Azure AD v2.0 endpoint
An Azure Instance Metadata Service Identity
OAuth2 endpoint

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: Create a system-assigned Managed Identities for Azure resource
The managed identities for Azure resources feature in Azure Active Directory (Azure AD) feature provides
Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate to
any service that supports Azure AD authentication, including Key Vault, without any credentials in your code.

A system-assigned managed identity is enabled directly on an Azure service instance. When the identity is
enabled, Azure creates an identity for the instance in the Azure AD tenant that's trusted by the subscription of
the instance. After the identity is created, the credentials are provisioned onto the instance.

Box 2: An Azure Instance Metadata Service Identity
See step 3 and 5 below.

How a system-assigned managed identity works with an Azure VM
1. Azure Resource Manager receives a request to enable the system-assigned managed identity on a VM.
2. Azure Resource Manager creates a service principal in Azure AD for the identity of the VM. The service
   principal is created in the Azure AD tenant that's trusted by the subscription.
3. Azure Resource Manager configures the identity on the VM by updating the Azure Instance Metadata
   Service identity endpoint with the service principal client ID and certificate.
4. After the VM has an identity, use the service principal information to grant the VM access to Azure

resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.
5. Your code that's running on the VM can request a token from the Azure Instance Metadata service endpoint, accessible only from within the VM

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

QUESTION 15
A company named Contoso, Ltd. has an Azure Active Directory (Azure AD) tenant that is integrated with Microsoft Office 365 and an Azure subscription.

Contoso has an on-premises identity infrastructure. The infrastructure includes servers that run Active Directory Domain Services (AD DS), Active Directory Federation Services (AD FS), Azure AD Connect, and Microsoft Identity Manager (MIM).

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Active Directory forest and an Office 365 tenant. Fabrikam has the same on-premises identity infrastructure as Contoso.

A team of 10 developers from Fabrikam will work on an Azure solution that will be hosted in the Azure subscription of Contoso. The developers must be added to the Contributor role for a resource in the Contoso subscription.

You need to recommend a solution to ensure that Contoso can assign the role to the 10 Fabrikam developers. The solution must ensure that the Fabrikam developers use their existing credentials to access resources.

What should you recommend?

A. Configure an AD FS claims provider trust between the AD FS infrastructures of Fabrikam and Contoso.
B. In the Azure AD tenant of Contoso, enable Azure Active Directory Domain Services (Azure AD DS). Create a one-way forest trust that uses selective authentication between the Active Directory forests of Contoso and Fabrikam.
C. In the Azure AD tenant of Contoso, create guest accounts for the Fabrikam developers.
D. In the Azure AD tenant of Contoso, create cloud-only user accounts for the Fabrikam developers.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Trust configurations - Configure trust from managed forests(s) or domain(s) to the administrative forest
* A one-way trust is required from production environment to the admin forest.
* Selective authentication should be used to restrict accounts in the admin forest to only logging on to the appropriate production hosts.

Reference: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

QUESTION 16
You have a hybrid deployment of Azure Active Directory (Azure AD).

You need to recommend a solution to ensure that the Azure AD tenant can be managed only from the computers on your on-premises network.

What should you include in the recommendation?

A. Azure AD roles and administrators

B. a conditional access policy
C. Azure AD Application Proxy
D. Azure AD Privileged Identity Management

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 17
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains two administrative
user accounts named Admin1 and Admin2.

You create two Azure virtual machines named VM1 and VM2.

You need to ensure that Admin1 and Admin2 are notified when more than five events are added to the security
log of VM1 or VM2 during a period of 120 seconds. The solution must minimize administrative tasks.

What should you create?

A. two action groups and one alert rule
B. one action group and one alert rule
C. five action groups and one alert rule
D. two action groups and two alert rules

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 18
You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains several
administrative user accounts.

You need to recommend a solution to identify which administrative user accounts have **NOT** signed in during
the previous 30 days.

Which service should you include in the recommendation?

A. Azure AD Identity Protection
B. Azure Activity Log
C. Azure Advisor
D. Azure AD Privileged Identity Management (PIM)

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 19

HOTSPOT

Your organization has developed and deployed several Azure App Service Web and API applications. The applications use Azure Key Vault to store several authentication, storage account, and data encryption keys. Several departments have the following requests to support the applications:

Department	Request
Security	• Review membership of administrative roles and require to provide a justification for continued membership • Get alerts about changes in administrator assignments. • See a history of administrator activation, including which changes administrators made to Azure resources.
Development	• Enable the applications to access Azure Key Vault and retrieve keys for use in code.
Quality Assurance	• Receive temporary administrator access to create and configure additional Web and API applications in the test environment.

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

◆

Answer Area

Department	Azure Service
Security	⯆
	Azure AD Privileged Identity Management
	Azure AD Managed Service Identity
	Azure AD Connect
	Azure AD Identity Protection
Development	⯆
	Azure AD Privileged Identity Management
	Azure AD Managed Service Identity
	Azure AD Connect
	Azure AD Identity Protection
Quality Assurance	⯆
	Azure AD Privileged Identity Management
	Azure AD Managed Service Identity
	Azure AD Connect
	Azure AD Identity Protection

Correct Answer:

◆

Answer Area

Department	Azure Service
Security	**Azure AD Privileged Identity Management** ▼
	Azure AD Privileged Identity Management
	Azure AD Managed Service Identity
	Azure AD Connect
	Azure AD Identity Protection
Development	**Azure AD Managed Service Identity** ▼
	Azure AD Privileged Identity Management
	Azure AD Managed Service Identity
	Azure AD Connect
	Azure AD Identity Protection
Quality Assurance	**Azure AD Privileged Identity Management** ▼
	Azure AD Privileged Identity Management
	Azure AD Managed Service Identity
	Azure AD Connect
	Azure AD Identity Protection

Section: [none]
Explanation

Explanation/Reference:

QUESTION 20
You manage a single-domain, on-premises Active Directory forest named contoso.com. The forest functional level is Windows Server 2016.

You have several on-premises applications that depend on Active Directory.

You plan to migrate the applications to Azure.

You need to recommend an identity solution for the applications. The solution must meet the following requirements:

▪ Eliminate the need for hybrid network connectivity.
▪ Minimize management overhead for Active Directory.

What should you recommend?

A. In Azure, deploy an additional child domain to the contoso.com forest.
B. In Azure, deploy additional domain controllers for the contoso.com domain.

C. Implement a new Active Directory forest in Azure.

D. Implement Azure Active Directory Domain Services (Azure AD DS).

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 21
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription named Project1. Only a group named Project1admins is assigned roles in the Project1 subscription. The Project1 subscription contains all the resources for an application named Application1.

Your company is developing a new application named Application2. The members of the Application2 development team belong to an Azure Active Directory (Azure AD) group named App2Dev.

You identify the following requirements for Application2:

▪ The members of App2Dev must be prevented from changing the role assignments in Azure.
▪ The members of App2Dev must be able to create new Azure resources required by Application2.
▪ All the required role assignments for Application2 will be performed by the members of Project1admins.

You need to recommend a solution for the role assignments of Application2.

Solution: In Project1, create a network security group (NSG) named NSG1. Assign Project1admins the Owner role for NSG1. Assign the App2Dev the Contributor role for NSG1.

Does this meet the goal?

◆
A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
You should use a separate subscription for Project2.

QUESTION 22
HOTSPOT

You manage a network that includes an on-premises Active Directory Domain Services 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 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:

Answer Area

Identity provider	Description
synchronized identity	▼
	User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords.
	User management occurs on-premises. The on-premises domain controller authenticates employee credentials.
	Both user management and authentication occur in Azure AD.
federated identity	▼
	User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords.
	User management occurs on-premises. The on-premises domain controller authenticates employee credentials.
	Both user management and authentication occur in Azure AD.

Correct Answer:

Answer Area

Identity provider	Description
synchronized identity	▼
	User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords.
	User management occurs on-premises. The on-premises domain controller authenticates employee credentials.
	Both user management and authentication occur in Azure AD.
federated identity	▼
	User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords.
	User management occurs on-premises. The on-premises domain controller authenticates employee credentials.
	Both user management and authentication occur in Azure AD.

Section: [none]
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.
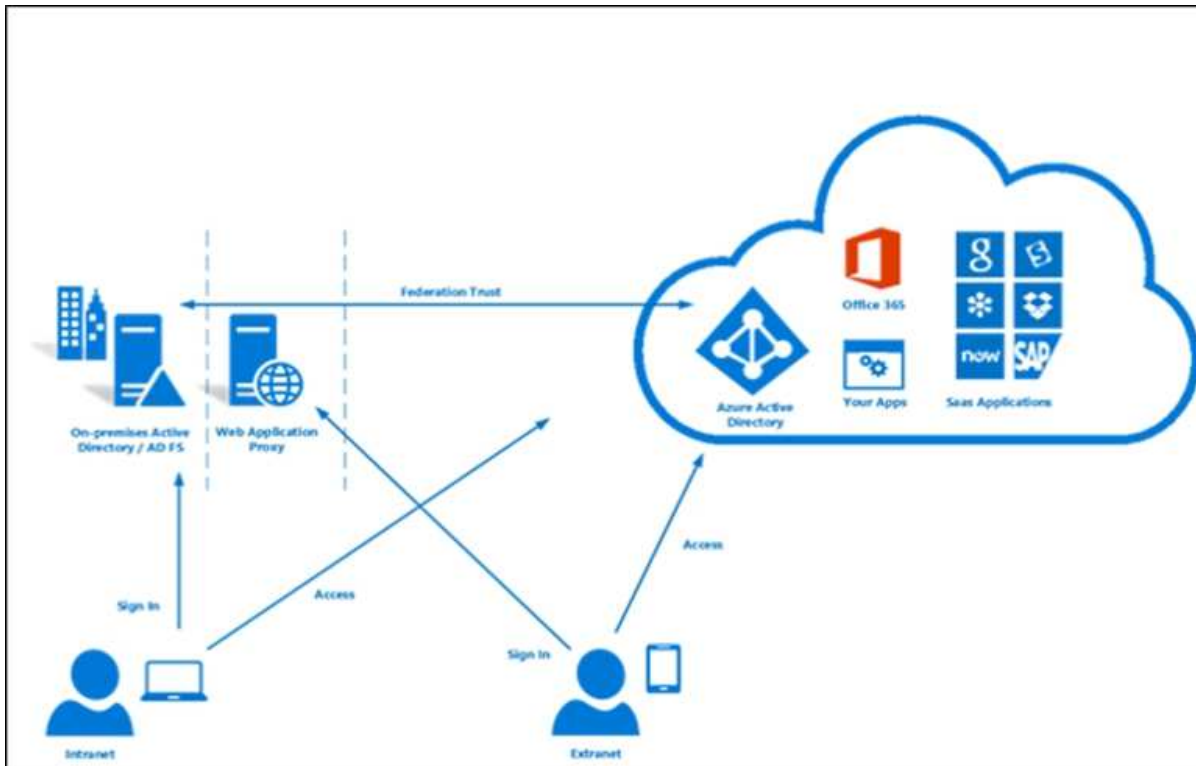
Example: Litware Corporation has deployed Azure AD Connect, to synchronize identity information from their on-premises directory to their Azure AD tenant. The identity information that is synchronized includes user accounts, their credential hashes for authentication (password hash sync) and group memberships.

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-promises 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 23
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure subscription that contains a resource group named RG1.

You create an Azure Active Directory (Azure AD) group named ResearchUsers that contains the user accounts of all researchers.

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

▪ The researchers must be allowed to create Azure virtual machines.
▪ The researchers must only be able to create Azure virtual machines by using specific Azure Resource Manager templates.

Solution: On RG1, assign a custom role-based access control (RBAC) role to the ResearchUsers group.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead: On RG1, assign the Contributor role to the ResearchUsers group. Create a custom Azure Policy definition and assign the policy to RG1.

QUESTION 24
A company deploys Azure Active Directory (Azure AD) Connect to synchronize identity information from their on-premises Active Directory Domain Services (AD DS) directory to their Azure AD tenant. The identity information that is synchronized includes user accounts , credential hashes for authentication (password sync), and group membership. The company plans to deploy several Windows and Linux virtual machines (VMs) to support their applications.

The VMs have the following requirements:

▪ Support domain join, LDAP read, LDAP bind, NTLM and Kerberos authentication, and Group Policy.
▪ Allow users to sign in to the domain using their corporate credentials and connect remotely to the VM by using Remote Desktop.

You need to support the VM deployment.

Which service should you use?

A. Azure AD Domain Services
B. Azure AD Privileged Identity Management
C. Azure AD Managed Service Identity
D. Active Directory Federation Services (AD FS)

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, Kerberos/NTLM authentication that are fully compatible with Windows Server Active Directory.

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

QUESTION 25
DRAG DROP

A company has an existing web application that runs on virtual machines (VMs) in Azure.

You need to ensure that the application is protected from SQL injection attempts and uses a layer-7 load balancer. The solution must minimize disruption to the code for the existing web application.

What should you recommend? To answer, drag the appropriate values to the correct items. Each value 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:

Values

Web Application Firewall (WAF)	
Azure Application Gateway	
Azure Load Balancer	
Azure Traffic Manager	
SSL offloading	
URL-based content routing	

Answer Area

Item	Value
Azure service	
Feature	

Correct Answer:

Values

Azure Load Balancer	
Azure Traffic Manager	
SSL offloading	
URL-based content routing	

Answer Area

Item	Value
Azure service	Azure Application Gateway
Feature	Web Application Firewall (WAF)

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: Azure Application Gateway
Azure Application Gateway provides an application delivery controller (ADC) as a service. It offers various layer 7 load-balancing capabilities for your applications.

Box 2: Web Application Firwewall (WAF)
Application Gateway web application firewall (WAF) protects web applications from common vulnerabilities and exploits.
This is done through rules that are defined based on the OWASP core rule sets 3.0 or 2.2.9.

There are rules that detects SQL injection attacks.

Reference:
https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-faq

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

QUESTION 26
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use the Azure traffic analytics solution in Azure Log Analytics to analyze the network traffic.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

QUESTION 27
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
The Network Watcher Network performance monitor is a cloud-based hybrid network monitoring solution that helps you monitor network performance between various points in your network infrastructure. It also helps you monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.

Note:
IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

IP flow verify looks at the rules for all Network Security Groups (NSGs) applied to the network interface, such as a subnet or virtual machine NIC. Traffic flow is then verified based on the configured settings to or from that network interface. IP flow verify is useful in confirming if a rule in a Network Security Group is blocking ingress or egress traffic to or from a virtual machine.

Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

QUESTION 28
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Install and configure the Log Analytics and Dependency Agents on all VMs. Use the Wire Data solution in Azure Log Analytics to analyze the network traffic.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]

Explanation

Explanation/Reference:
Explanation:
Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

QUESTION 29
HOTSPOT

A company plans to implement an HTTP-based API to support a web app. The web app allows customers to check the status of their orders.

The API must meet the following requirements:

▪ Implement Azure Functions
▪ Provide public read-only operations
▪ Do not allow write operations

You need to recommend configuration options.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Topic	Value
Allowed authentication methods	▼
	All methods
	GET only
	GET and POST only
	GET, POST, and OPTIONS only
Authorization level	▼
	Function
	Anonymous
	Admin

Correct Answer:

Answer Area

Topic	Value
Allowed authentication methods	▼
	All methods
	GET only
	GET and POST only
	GET, POST, and OPTIONS only
Authorization level	▼
	Function
	Anonymous
	Admin

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Allowed authentication methods: GET only

Authorization level: Anonymous
The option is Allow Anonymous requests. This option turns on authentication and authorization in App Service, but defers authorization decisions to your application code. For authenticated requests, App Service also passes along authentication information in the HTTP headers.

This option provides more flexibility in handling anonymous requests.

Reference:
https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization

QUESTION 30
Your network contains an on-premises Active Directory forest named contoso.com. The forest is synced to an Azure Active Directory (Azure AD) tenant named contoso.com and an Azure AD Domain Services (Azure AD DS) domain named contoso-aad.com.

You have an Azure Storage account named Storage1 that contains a file share named Share1.

You configure NTFS permissions on Share1. You plan to deploy a virtual machine that will be used by several users to access Share1.

You need to ensure that the users can access Share1.

Which type virtual machine should you deploy?

A. a virtual machine that runs Windows Server 2016 and is joined to the contoso.com domain
B. a virtual machine that runs Windows 10 and is joined to the contoso-add.com domain
C. a virtual machine that runs Windows 10 and is hybrid Azure AD joined to the contoso.com domain
D. an Azure virtual machine that runs Windows Server 2016 and is joined to the contoso-add.com domain

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
You join the Windows Server virtual machine to the Azure AD DS-managed domain, here named contoso-aad.com.

Note: Azure Files supports identity-based authentication over SMB (Server Message Block) (preview) through Azure Active Directory (Azure AD) Domain Services. Your domain-joined Windows virtual machines (VMs) can access Azure file shares using Azure AD credentials.

Incorrect Answers:
B, C: Azure AD authentication over SMB is not supported for Linux VMs for the preview release. Only Windows Server VMs are supported.

Reference:
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-enable#mount-a-file-share-from-a-domain-joined-vm

QUESTION 31
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM).

Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant.

The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.

You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).

Solution: Deploy one Azure Key Vault to each region. Create two Azure AD service principals. Configure the virtual machines to use Azure Disk Encryption and specify a different service principal for the virtual machines in each region.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
You would also have to import Import the security keys from the HSM into each Azure key vault.

Reference:
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites-aad

QUESTION 32
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM).

Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant.

The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.

You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).

Solution: Export a security key from the on-premises HSM. Create one Azure AD service principal. Configure the virtual machines to use Azure Storage Service Encryption.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
We use the Azure Premium Key Vault with Hardware Security Modules (HSM) backed keys.
The Key Vault has to be in the same region as the VM that will be encrypted.

Reference:
https://www.ciraltos.com/azure-disk-encryption-v2/

QUESTION 33
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM).

Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant.

The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.

You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).

Solution:
▪ Deploy one Azure key vault to each region
▪ Export two security keys from the on-premises HSM
▪ Import the security keys from the HSM into each Azure key vault
▪ Create two Azure AD service principals
▪ Configure the virtual machines to use Azure Disk Encryption
▪ Specify a different service principal for the virtual machines in each region

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
We use the Azure Premium Key Vault with Hardware Security Modules (HSM) backed keys.
The Key Vault has to be in the same region as the VM that will be encrypted.

Note: If you want to use a key encryption key (KEK) for an additional layer of security for encryption keys, add a KEK to your key vault. Use the Add-AzKeyVaultKey cmdlet to create a key encryption key in the key vault. You can also import a KEK from your on-premises key management HSM.

Reference:
https://www.ciraltos.com/azure-disk-encryption-v2/

https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites-aad

QUESTION 34
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Use Azure Advisor to analyze the network traffic.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Note: Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.

With Advisor, you can:

Get proactive, actionable, and personalized best practices recommendations.
Improve the performance, security, and high availability of your resources, as you identify opportunities to reduce your overall Azure spend.
Get recommendations with proposed actions inline.

Reference:
https://docs.microsoft.com/en-us/azure/advisor/advisor-overview

QUESTION 35
Your network contains an Active Directory domain named contoso.com that is federated to an Azure Active Directory (Azure AD) tenant. The on-premises domain contains a VPN server named Server1 that runs Windows Server 2016.

You have a single on-premises location that uses an address space of 172.16.0.0/16.

You need to implement two-factor authentication for users who establish VPN connections to Server1.

What should you include in the implementation?

A. In Azure AD, create a conditional access policy and a trusted named location
B. Install and configure Azure MFA Server on-premises
C. Configure an Active Directory Federation Services (AD FS) server on-premises
D. In Azure AD, configure the authentication methods. From the multi-factor authentication (MFA) service settings, create a trusted IP range

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
You need to download, install and configure the MFA Server.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfaserver-deploy

QUESTION 36
HOTSPOT

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

Save   Discard   Delete

*Name

Diags

[ ] Archive to a storage account

[ ] Stream to an event hub

[✓] Send to Log Analytics

Log Analytics
OMSWkspace1

LOG

[✓] SQLInsights

[✓] AutomaticTuning

[✓] QueryStoreRuntimeStatistics

[✓] QueryStoreWaitStatistics

[✓] Errors

[✓] DatabaseWaitStatistics

[✓] Timeouts

[✓] Blocks

[✓] Deadlocks

[✓] Audit

[✓] SQLSecurityAuditEvents

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

◆

Section: [none]
Explanation

Explanation/Reference:

QUESTION 37
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an Azure AD Connect server to use password hash synchronization and select the **Enable single sign-on** option.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 38
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. In Azure Active Directory (AD) Privileged Identity Management, create a custom role assignment for the Application1 resources
B. Create an Azure Automation runbook that runs the `Get-AzureADUserAppRoleAssignment` cmdlet
C. Create an Azure Automation runbook that runs the `Get-AzureRmRoleAssignment` cmdlet
D. In Azure Active Directory (Azure AD), create an access review of Application1

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 39
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an Azure AD Connect server to use pass-through authentication and select the **Enable single sign-on** option.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 40
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Configure an AD DS server in an Azure virtual machine (VM). Configure bidirectional replication.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 41
HOTSPOT

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

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 authorization methods 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	Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption
Azure SQL	Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption
Cosmos DB	Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption

Correct Answer:

Answer Area

Functionality	Authorization method
Azure Key Vault	Hash-based message authentication code (HMAC) **Azure Managed Identity** Role-Based Access Controls (RBAC) HTTPS encryption
Azure SQL	Hash-based message authentication code (HMAC) **Azure Managed Identity** Role-Based Access Controls (RBAC) HTTPS encryption
Cosmos DB	Hash-based message authentication code (HMAC) **Azure Managed Identity** Role-Based Access Controls (RBAC) HTTPS encryption

Section: [none]
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:

QUESTION 42
You are designing a security solution for a company's Azure Active Directory (Azure AD). The company currently uses Azure AD Premium for all employees. Contractors will periodically access the corporate network based on demand.

You must ensure that all employees and contractors are required to log on by using two-factor authentication. The solution must minimize costs.

You need to recommend a solution.

What should you recommend?

A. Purchase Azure Multi-Factor Authentication licenses for the employees and the contractors
B. Use the Multi-Factor Authentication provider in Azure and configure the usage model for each authentication type
C. Use the Multi-Factor Authentication provider in Azure and configure the usage model for each enabled user
D. Purchase Azure Multi-Factor Authentication licenses for the contractors only

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 43
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure Active Directory (Azure AZD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do **NOT** work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Create an Access Review for Group1.

Does this solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 44
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure Active Directory (Azure AZD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do **NOT** work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: You implement an access package.

Does this solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 45
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure Active Directory (Azure AZD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do **NOT** work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Implement Azure AD Privileged Identity Management.

Does this solution meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 46
Your company has several Azure subscriptions that are part of a Microsoft Enterprise Agreement.

The company's compliance team creates automatic alerts by using Azure Monitor.

You need to recommend a solution to apply the alerts automatically when new subscriptions are added to the Enterprise Agreement.

What should you include in the recommendation?

A. Azure Automation runbooks
B. Azure Log Analytics alerts
C. Azure Monitor action groups
D. Azure Resource Manager templates
E. Azure Policy

Correct Answer: E
Section: [none]
Explanation

Explanation/Reference:

QUESTION 47
You store web access logs data in Azure Blob storage.

You plan to generate monthly reports from the access logs.

You need to recommend an automated process to upload the data to Azure SQL Database every month.
◆
What should you include in the recommendation?

A. Microsoft SQL Server Migration Assistant (SSMA)
B. Azure Data Factory
C. Data Migration Assistant
D. AzCopy

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 48
Your company has the offices shown in the following table.

Location	IP address space	Public NAT segment
Montreal	10.10.0.0/16	190.15.1.0/24
Seattle	172.16.0.0/16	194.25.2.0/24

The network contains an Active Directory domain named contoso.com that is synced to Azure Active Directory (Azure AD).

All users connect to an application hosted in Microsoft 365.

You need to recommend a solution to ensure that all the users use Azure Multi-Factor Authentication (MFA) to connect to the application from one of the offices.

What should you include in the recommendation?

A. a named location and two Microsoft Cloud App Security policies
B. a conditional access policy and two virtual networks
C. a virtual network and two Microsoft Cloud App Security policies
D. a conditional access policy and two named locations

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 49
HOTSPOT

You have an Azure subscription that contains 300 Azure virtual machines that run Windows Server 2016.

You need to centrally monitor all warning events in the System logs of the virtual machines.

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

◆
NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Resource to create in Azure:

| An event hub |
| A Log Analytics workspace |
| A search service |
| A storage account |

Configuration to perform on the virtual machines:

| Create event subscriptions |
| Configure Continuous delivery |
| Install the Microsoft Monitoring Agent |
| Modify the membership of the Event Log Readers Groups |

Correct Answer:

Answer Area

Resource to create in Azure:

An event hub
A Log Analytics workspace
A search service
A storage account

Configuration to perform on the
virtual machines:

Create event subscriptions
Configure Continuous delivery
Install the Microsoft Monitoring Agent
Modify the membership of the Event Log Readers Groups

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-windows-events
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/agent-windows

QUESTION 50
**Note: This question is a part of series of questions that present the same scenario. Each question in
the series contains a unique solution that might meet the stated goals. Some question sets might have
more than one correct solution, while others might not have a correct solution.**

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

Your company has an on-premises Active Directory Domain Services (AD DS) domain and an established
Azure Active Directory (Azure AD) environment.

Your company would like users to be automatically signed in to cloud apps when they are on their corporate
desktops that are connected to the corporate network.

You need to enable single sign-on (SSO) for company users.

Solution: Install and configure an on-premises Active Directory Federation Services (AD FS) server with a trust
established between the AD FS server and Azure AD.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:

Seamless SSO is not applicable to Active Directory Federation Services (ADFS).
Instead install and configure an Azure AD Connect server.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso

QUESTION 51
You have an Azure subscription that contains several resource groups, including a resource group named RG1. RG1 contains several business-critical resources.

A user named admin1 is assigned the Owner role to the subscription.

You need to prevent admin1 from modifying the resources in RG1. The solution must ensure that admin1 can manage the resources in the other resource groups.

What should you use?

A. a management group
B. an Azure policy
C. a custom role
D. an Azure blueprint

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Role-based access control (RBAC) focuses on user actions at different scopes. You might be added to the contributor role for a resource group, allowing you to make changes to that resource group.

Incorrect Answers:
A: If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions.

B: There are a few key differences between Azure Policy and role-based access control (RBAC). Azure Policy focuses on resource properties during deployment and for already existing resources. Azure Policy controls properties such as the types or locations of resources. Unlike RBAC, Azure Policy is a default allow and explicit deny system.

D: Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.

Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/overview

QUESTION 52
HOTSPOT

You deploy Azure service by using Azure Resources Manager templates. The template reference secrets are stored in Azure key Vault.

You need to recommend a solution for accessing the secrets during deployments.

The solution must prevent the users who are performing the deployments from accessing the secrets in the key vault directly.

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

area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Enable the key vaults for template deployment by using:

An access policy for the key vault
An advanced access policy for the key vault
Role-based access control (RBAC)

Restrict access to the secrets in the key vaults by using:

An access policy for the key vault
An advanced access policy for the key vault
Role-based access control (RBAC)

Correct Answer:

Answer Area

Enable the key vaults for template deployment by using:

An access policy for the key vault
An advanced access policy for the key vault
Role-based access control (RBAC)

Restrict access to the secrets in the key vaults by using:

An access policy for the key vault
An advanced access policy for the key vault
Role-based access control (RBAC)

◆

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: An advanced access policy for the key vaults
Enable template deployment
1. In the portal, select your Key Vault.
2. Select Access policies.
3. Select access policies
4. Select Click to show advanced access policies.
5. Show advanced access policies
6. Select Enable access to Azure Resource Manager for template deployment. Then, select Save.

Box 2: Role-based access control (RBAC)
In large teams you may have multiple people deploying resources but don't want to give them access to the actual secrets inside the vault. You can achieve this by creating a custom role that only gives access to the KeyVault for deployment purposes. The deployment user cannot read the secrets within.

Reference:

QUESTION 53
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 application has 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 need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Authentication Strategies

An Azure AD B2C tenant	An Azure AD v2.0 endpoint
An Azure AD v1.0 endpoint	

Answer Area

Customer: [   ]

Reporting: [   ]

Correct Answer:

Authentication Strategies

An Azure AD v1.0 endpoint	

Answer Area

Customer: An Azure AD v2.0 endpoint

Reporting: An Azure AD B2C tenant

Section: [none]
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 54
HOTSPOT

You configure OAuth2 authorization in API Management as shown in the exhibit.

Add OAuth2 service
API Management service

✕

* Display name

Unique name used to reference this authorization server of the p... ✓

* Id ⓘ

✓

Description

Authorization server description

* Client registration page URL

https://contoso.com/register ✓

Authorization grant types

☑ Authorization code

☐ Implicit

☐ Resource owner password

☐ Client credentials

* Authorization endpoint URL

https://login.microsoftonline.com/contoso.onmicrosoft.com/o... ✓

☐ Support state parameter

Create

Authorization Request method

☑ GET

☐ POST

• Token endpoint URL

Token endpoint is used by clients to obtain access tokens in excha...

Additional body parameters using application/x-
www-form-urlencoded format

Use the drop-domain 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

The selected authorization grant type is for

▼
Background services
Headless device authentication
Single page applications
Web applications

To enable custom data in the grant flow, select

▼
Client credentials
Implicit
Resource owner password
Support state parameter

Correct Answer:

Answer Area

The selected authorization grant type is for

▼
Background services
Headless device authentication
Single page applications
Web applications

To enable custom data in the grant flow, select

▼
Client credentials
Implicit
Resource owner password
Support state parameter

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: Web applications
The Authorization Code Grant Type is used by both web apps and native apps to get an access token after a user authorizes an app.

Note: The Authorization Code grant type is used by confidential and public clients to exchange an authorization code for an access token.

After the user returns to the client via the redirect URL, the application will get the authorization code from the URL and use it to request an access token.

Answers:
Not Headless device authentication:
A headless system is a computer that operates without a monitor, graphical user interface (GUI) or peripheral devices, such as keyboard and mouse.

Headless computers are usually embedded systems in various devices or servers in multi-server data center environments. Industrial machines, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines and toys are among the myriad possible hosts of embedded systems.

Box 2: Client Credentials
How to include additional client data
In case you need to store additional details about a client that don't fit into the standard parameter set the custom data parameter comes to help:

POST /c2id/clients HTTP/1.1
Host: demo.c2id.com
Content-Type: application/json
Authorization: Bearer ztucZS1ZyFKgh0tUEruUtiSTXhnexmd6

```
{
  "redirect_uris" : [ "https://myapp.example.com/callback" ],
  "data"          : { "reg_type"  : "3rd-party",
                      "approved"  : true,
                      "author_id" : 792440 }
}
```
The data parameter permits arbitrary content packaged in a JSON object. To set it you will need the master registration token or a one-time access token with a client-reg:data scope.

Incorrect Answers:
Authorization protocols provide a state parameter that allows you to restore the previous state of your application. The state parameter preserves some state object set by the client in the Authorization request and makes it available to the client in the response.

Reference:
https://developer.okta.com/blog/2018/04/10/oauth-authorization-code-grant-type

https://connect2id.com/products/server/docs/guides/client-registration

QUESTION 55
A company has deployed several applications across Windows and Linux Virtual machines in Azure. Log Analytics are being used to send the required data for alerting purposes for the Virtual Machines.

You need to recommend which tables need to be queried for security related queries.

Which of the following would you query for events from Windows Event Logs?

A. Azure Activity
B. Azure Diagnostics
C. Event

D. Syslog

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
This is also given in the Microsoft documentation, wherein you would use the Event Table for the queries on events from Windows Virtual machines

Log queries with Windows Events

The following table provides different examples of log queries that retrieve Windows Event records.

Query	Description
Event	All Windows events.
Event | where EventLevelName == "error"	All Windows events with severity of error.
Event | summarize count() by Source	Count of Windows events by source.
Event | where EventLevelName == "error" | summarize count() by Source	Count of Windows error events by source.

Since this is clearly mentioned, all other options are incorrect
For more information on collecting event data from windows virtual machines, please go ahead and visit the below URL.

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-windows-events

QUESTION 56
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains a group named Group1. Group1 contains all the administrative user accounts.

You discover several login attempts to the Azure portal from countries where administrative users do **NOT** work.

You need to ensure that all login attempts to the Azure portal from those countries require Azure Multi-Factor Authentication (MFA).

Solution: Implement Azure AD Identity Protection for Group1.

Does this solution meet the goal?

A. Yes
B. No

Correct Answer: B

Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead implement Azure AD Privileged Identity Management.

Note: Azure Active Directory (Azure AD) Privileged Identity Management (PIM) is a service that enables you to manage, control, and monitor access to important resources in your organization.

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

QUESTION 57
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

Your company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.

Several VMs are exhibiting network connectivity issues.

You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.

Solution: Install and configure the Microsoft Monitoring Agent and the Dependency Agent on all VMs. Use the Wire Data solution in Azure Monitor to analyze the network traffic.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Note: Wire Data looks at network data at the application level, not down at the TCP transport layer. The solution doesn't look at individual ACKs and SYNs.

Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

QUESTION 58
You are designing a solution that will host 20 different web applications.

You need to recommend a solution to secure the web applications with a firewall that protects against common web-based attacks including SQL injection, cross-site scripting attacks, and session hijacks. The solution must minimize costs.

Which three Azure features should you recommend? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. VPN Gateway
B. URL-based content routing
C. Multi-site routing
D. Web Application Firewall (WAF)
E. Azure ExpressRoute
F. Azure Application Gateway

Correct Answer: DEF
Section: [none]
Explanation

Explanation/Reference:
Explanation:
The web application firewall (WAF) in Azure Application Gateway helps protect web applications from common web-based attacks like SQL injection, cross-site scripting attacks, and session hijacks. It comes preconfigured with protection from threats identified by the Open Web Application Security Project (OWASP) as the top 10 common vulnerabilities.
ExpressRoute connections do not go over the public Internet and thus can be considered more secure than VPN-based solutions. This allows ExpressRoute connections to offer more reliability, faster speeds, lower latencies, and higher security than typical connections over the Internet.

Reference:
https://azure.microsoft.com/en-us/updates/application-gateway-web-application-firewall-in-public-preview/

https://docs.microsoft.com/en-us/azure/security/fundamentals/overview

QUESTION 59
A company has deployed several applications across Windows and Linux Virtual machines in Azure. Log Analytics are being used to send the required data for alerting purposes for the Virtual Machines.

You need to recommend which tables need to be queried for security related queries.

Which of the following would you query for events from Linux system logging?

A. Azure Activity
B. Azure Diagnostics
C. Event
D. Syslog

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
This is also given in the Microsoft documentation, wherein you would use the Syslog Table for the queries on events from Linux Virtual machines

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

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/data-sources-syslog

◆

Testlet 1

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

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

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

To start the case study
To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirement, 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.

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.

Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, at 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.

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.
▪ 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 transactions query system remains available without any administrative intervention.

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. legitimate users must be able to

authenticate successfully by using multi-factor authentication.

QUESTION 1
You need to recommend a solution for implementing the back-end tier of the payment processing system in Azure.

What should you include in the recommendation?

A. an Azure SQL Database managed instance
B. a SQL Server database on an Azure virtual machine
C. an Azure SQL Database single database
D. an Azure SQL Database elastic pool

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 2
You need to recommend a solution for protecting the content of the payment processing system.

What should you include in the recommendation?

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

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

QUESTION 3
HOTSPOT

You need to recommend a solution for the data store of the historical transaction query system.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Sizing requirements:

| A table that has unlimited capacity |
| A table that has a fixed capacity |
| Multiple tables that have unlimited capacity |
| Multiple tables that have fixed capacity |

Resiliency:

| An additional read region |
| An availability set |
| An availability zone |

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:

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 requirement, 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

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

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 their research and development (R&D) department only.

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.

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.

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 platform as a service (PaaS).
▪ 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.

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.

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 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 data storage strategy for WebApp1.

What should you include in the recommendation?

A. a fixed-size DTU Azure SQL database

B. an Azure virtual machine that runs SQL Server
C. an Azure SQL Database elastic pool
D. a vCore-based Azure SQL database

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

◆

Question Set 3

QUESTION 1
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 would you include in the recommendation?

A. Azure Traffic Manager
B. Azure Notification Hubs
C. Azure Blob storage
D. Azure Queue storage

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Asynchronous messaging can be implemented in a variety of different ways. With queues, topics, and subscriptions, Azure Service Bus supports asynchronism via a store and forward mechanism.

Reference:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-async-messaging

QUESTION 2
You have an Azure subscription that contains an Azure Cosmos DB account.

You need to recommend a solution to generate an alert from Azure Log Analytics when a request charge for a query exceeds 50 request units more than 20 times within a 15-minute window.

What should you recommend?

A. Create a search query to identify when requestCharge_s exceeds 50. Configure an alert threshold of 20 and a period of 15.
B. Create a search query to identify when duration_s exceeds 20 and requestCharge_s exceeds 50. Configure a period of 15.
C. Create a search query to identify when requestCharge_s exceeds 20. Configure a period of 15 and a frequency of 20.
D. Create a search query to identify when duration_s exceeds 20. Configure a period of 15.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 3
You are designing a data protection strategy for Azure virtual machines. All the virtual machines are in the Standard tier and use managed disks.

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

- The use of encryption keys is audited.
- All the data is encrypted at rest always.
- You manage the encryption keys, not Microsoft.

What should you include in the recommendation?

A. BitLocker Drive Encryption (BitLocker)
B. Azure Storage Service Encryption
C. client-side encryption
D. Azure Disk Encryption

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview

QUESTION 4
You have 100 servers that run Windows Server 2012 R2 and host Microsoft SQL Server 2012 R2 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 single databases
B. Azure SQL Database Managed Instance
C. Azure SQL Database elastic pools
D. SQL Server 2016 on Azure virtual machines

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-managed-instance

QUESTION 5
DRAG DROP

You are designing a virtual machine that will run Microsoft SQL Server and will contain two data disks. The first data disk will store log files, and the second data disk will store data. Both disks are P40 managed disks.

You need to recommend a caching policy for each disk. The policy must provide the best overall performance

for the virtual machine.

Which caching policy should you recommend for each disk? To answer, drag the appropriate policies to the correct disks. Each policy 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:

Policies

| None |
| ReadOnly |
| ReadWrite |

Answer Area

Log: | Policy |

Data: | Policy |

Correct Answer:

Policies

| |
| |
| ReadWrite |

Answer Area

Log: | None |

Data: | ReadOnly |

◆

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sql/virtual-machines-windows-sql-performance

QUESTION 6
You plan to create an Azure Cosmos DB account that uses the SQL API. The account will contain data added by a web application. The web application will send data daily.

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

- Sends email notification when data is received from IoT devices.
- Minimizes compute cost.

What should you include in the recommendation?

A. Deploy an Azure logic app that has the Azure Cosmos DB connector configured to use a SendGrid action.

B. Deploy a function app that is configured to use the Consumption plan and a SendGrid binding.

C. Deploy an Azure logic app that has a SendGrid connector configured to use an Azure Cosmos DB action.

D. Deploy a function app that is configured to use the Consumption plan and an Azure Event Hubs binding.

E. Deploy an Azure logic app that has a webhook configured to use a SendGrid action.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
You can send email by using SendGrid bindings in Azure Functions. Azure Functions supports an output binding for SendGrid.

Note: When you're using the Consumption plan, instances of the Azure Functions host are dynamically added and removed based on the number of incoming events.

Reference:
https://docs.microsoft.com/en-us/azure/azure-functions/functions-bindings-sendgrid

https://docs.microsoft.com/en-us/azure/azure-functions/functions-scale#consumption-plan

QUESTION 7
You have Azure virtual machines that run a custom line-of-business web application.

You plan to use a third-party solution to parse event logs from the virtual machines stored in an Azure storage account.

You need to recommend a solution to save the event logs from the virtual machines to the Azure Storage account. The solution must minimize costs and complexity.

What should you include in the recommendation?

A. Azure VM Diagnostics Extension

B. Azure Monitor Metrics

C. event log subscriptions

D. Azure Monitor Logs

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
The Azure Diagnostics VM extension enables you to collect monitoring data, such as performance counters and event logs, from your Windows VM. You can granularly specify what data you want to collect and where you want the data to go, such as an Azure Storage account or an Azure Event Hub.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/extensions-diagnostics

QUESTION 8
DRAG DROP

You are planning an Azure solution that will host production databases for a high-performance application. The solution will include the following components:

▪ Two virtual machines that will run Microsoft SQL Server 2016, will be deployed to different data centers in

the same Azure region, and will be part of an Always On availability group.
▪ SQL Server data that will be backed up by using the Automated Backup feature of the SQL Server IaaS Agent Extension (SQLIaaSExtension)

You identify the storage priorities for various data types as shown in the following table.

Data type	Storage priority
Operating system	Speed and availability
Databases and logs	Speed and availability
Backups	Lowest cost

Which storage type should you recommend for each data type? To answer, drag the appropriate storage types to the correct data types. Each storage type 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:

Storage Types

A geo-redundant storage (GRS) account

A locally-redundant storage (LRS) account

A premium managed disk

A standard managed disk

Answer Area

Operating system: [   ]

Databases and logs: [   ]

Backups: [   ]

Correct Answer:

Storage Types

A geo-redundant storage (GRS) account

A locally-redundant storage (LRS) account

A premium managed disk

A standard managed disk

Answer Area

Operating system: A premium managed disk

Databases and logs: A premium managed disk

Backups: A locally-redundant storage (LRS) account

Section: [none]
Explanation

Explanation/Reference:

QUESTION 9
HOTSPOT

Your company deploys several Linux and Windows virtual machines (VMs) to Azure. The VMs are deployed with the Microsoft Dependency Agent and the Log Analytics Agent installed by using Azure VM extensions. On-premises connectivity has been enabled by using Azure ExpressRoute.

You need to design a solution to monitor the VMs.

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
Analyze Network Security Group (NSG) flow logs for VMs attempting Internet access.	▼ Azure Traffic Analytics Azure ExpressRoute Monitor Azure Service Endpoint Monitor Azure DNS Analytics
Visualize the VMs with their different processes and dependencies on other computers and external processes.	▼ Azure Service Map Azure Activity Log Azure Service Health Azure Advisor

Correct Answer:

Answer Area

Scenario	Azure Monitoring Service
Analyze Network Security Group (NSG) flow logs for VMs attempting Internet access.	▼ **Azure Traffic Analytics** Azure ExpressRoute Monitor Azure Service Endpoint Monitor Azure DNS Analytics
Visualize the VMs with their different processes and dependencies on other computers and external processes.	▼ **Azure Service Map** Azure Activity Log Azure Service Health Azure Advisor

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: Azure Traffic Analytics
Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic flow in your Azure cloud. With traffic analytics, you can:

- Identify security threats to, and secure your network, with information such as open-ports, applications attempting internet access, and virtual machines (VM) connecting to rogue networks.
- Visualize network activity across your Azure subscriptions and identify hot spots.
- Understand traffic flow patterns across Azure regions and the internet to optimize your network deployment for performance and capacity.
- Pinpoint network misconfigurations leading to failed connections in your network.

Box 2: Azure Service Map
Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. With Service Map, you can view your servers in the way that you think of them: as interconnected systems that deliver critical services. Service Map shows connections between servers, processes, inbound and outbound connection latency, and ports across any TCP-connected architecture, with no configuration required other than the installation of an agent.

Reference:
https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics

https://docs.microsoft.com/en-us/azure/azure-monitor/insights/service-map

QUESTION 10
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting.

Solution: Create a resources group for each resource type. Assign tags to each resource group.

Does this meet the goal?

◆
A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

QUESTION 11
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting.

Solution: Place all resources in the same resource group. Assign tags to each resource.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead, create a resources group for each resource type. Assign tags to each resource

Note: Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

QUESTION 12
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

◆
You are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting.

Solution: Create a new subscription for each department.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead, create a resources group for each resource type. Assign tags to each resource

Note: Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

QUESTION 13
HOTSPOT

You plan to deploy logical Azure SQL Database servers to the East US Azure region and the West US Azure region. Each server will contain 20 databases. Each database will be accessed by a different user who resides in a different on-premises location. The databases will be configured to use active geo-replication.

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

▪ Restricts user access to each database
▪ Restricts network access to each database based on each user's respective location
▪ Ensures that the databases remain accessible from client applications if the local Azure region fails

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Configure user access by using:

| ▼ |
| Azure PowerShell |
| The REST API |
| Transact-SQL |

◈ Configure database-level firewall rules by using:

| ▼ |
| Azure PowerShell |
| The REST API |
| Transact-SQL |

Correct Answer:

Answer Area

Configure user access by using:

Azure PowerShell
The REST API
Transact-SQL

Configure database-level firewall rules by using:

Azure PowerShell
The REST API
Transact-SQL

Section: [none]
Explanation

Explanation/Reference:

QUESTION 14
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 passphrase
B. a certificate
C. a key
D. a secret

Correct Answer: C
Section: [none]
Explanation

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

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

QUESTION 15
You deploy Azure App Service Web Apps that connect to on-premises Microsoft SQL Server instances by using Azure ExpressRoute. You plan to migrate the SQL Server instances to Azure.

Migration of the SQL Server instances to Azure must:

- Support automatic patching and version updates to SQL Server.
- Provide automatic backup services.
- Allow for high-availability of the instances.
- Provide a native VNET with private IP addressing.
- Encrypt all data in transit.
- Be in a single-tenant environment with dedicated underlying infrastructure (compute, storage)

You need to migrate the SQL Server instances to Azure.

Which Azure service should you use?

A. Azure SQL Database with elastic pools
B. SQL Server in Docker containers running on Azure Kubernetes Service (AKS)
C. SQL Server Infrastructure-as-a-Service (IaaS) virtual machine (VM)
D. SQL Server in a Docker container running on Azure Container Instances (ACI)
E. Azure SQL Database Managed Instance

Correct Answer: E
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Azure SQL Database Managed Instance configured for Hybrid workloads. Use this topology if your Azure SQL Database Managed Instance is connected to your on-premises network. This approach provides the most simplified network routing and yields maximum data throughput during the migration.

Reference:
https://docs.microsoft.com/en-us/azure/dms/resource-network-topologies

QUESTION 16
You are designing an Azure Web App that includes many static content files.

The application is accessed from locations all over the world by using a custom domain name.

You need to recommend an approach for providing access to the static content with the least amount of latency.

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

NOTE: Each correct selection is worth one point.

A. Configure a custom domain name that is an alias for the Azure Storage domain.
B. Configure a CNAME DNS record for the Azure Content Delivery Network (CDN) domain.
C. Place the static content in Azure Table storage.
D. Place the static content in Azure Blob storage and enable Content Delivery Network (CDN) on the account.

Correct Answer: BD
Section: [none]
Explanation

Explanation/Reference:
Explanation:
D: Add Azure Content Delivery Network (CDN) to a web app in Azure App Service.
B: When you use a CDN endpoint to deliver content, a custom domain is necessary if you would like your own domain name to be visible in your CDN URL. Having a visible domain name can be convenient for your customers and useful for branding purposes.

Create a CNAME DNS record, and associate the custom domain with your CDN endpoint.

Reference:
https://docs.microsoft.com/en-us/azure/cdn/cdn-map-content-to-custom-domain

https://docs.microsoft.com/en-us/azure/cdn/cdn-add-to-web-app

QUESTION 17
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 would you include in the recommendation?

A. Azure Traffic Manager
B. Azure Data Lake
C. Azure Blob storage
D. Azure Service Bus
E. Azure Application Gateway

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Asynchronous messaging can be implemented in a variety of different ways. With queues, topics, and subscriptions, Azure Service Bus supports asynchronism via a store and forward mechanism.

Reference:
https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-async-messaging

QUESTION 18
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 are designing an Azure solution for a company that has four departments. Each department will deploy several Azure app services and Azure SQL databases.

You need to recommend a solution to report the costs for each department to deploy the app services and the databases. The solution must provide a consolidated view for cost reporting.

Solution: Create a separate resource group for each department. Place the resources for each department in its respective resource group.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B

Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead create a resources group for each resource type. Assign tags to each resource group.

Note: Tags enable you to retrieve related resources from different resource groups. This approach is helpful when you need to organize resources for billing or management.

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-using-tags

Testlet 1

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

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

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

To start the case study
To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirement, 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.

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.

Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, at 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.

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.
- 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 transactions query system remains available without any administrative intervention.

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. legitimate users must be able to

authenticate successfully by using multi-factor authentication.

QUESTION 1
You need to recommend a backup solution for the data store of the payment processing system.

What should you include in the recommendation?

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

Correct Answer: B
Section: [none]
Explanation

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

QUESTION 2
You need to recommend a disaster recovery solution for the back-end tier of the payment processing system.

What should you include in the recommendation?

A. Always On Failover Cluster Instances
B. Azure Site Recovery
C. an auto-failover group
D. geo-redundant database backups

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Scenario:
▪ The back-end data store is implemented as a Microsoft SQL Server 2014 database.
▪ If a data center fails, ensure that the payment processing system remains available without any administrative intervention.

Note: Auto-failover groups is a SQL Database feature that allows you to manage replication and failover of a group of databases on a SQL Database server or all databases in a managed instance to another region. It is a declarative abstraction on top of the existing active geo-replication feature, designed to simplify deployment and management of geo-replicated databases at scale.

Reference:
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auto-failover-group

QUESTION 3
You need to recommend a high-availability solution for the middle tier of the payment processing system.

What should you include in the recommendation?

A. the Isolated App service plan
B. availability zones

C. an availability set

D. the Premium App Service plan

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

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 requirement, 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

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

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.

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.

Problem Statements

The use of Web App1 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.

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 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 platform as a service (PaaS).
- 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.

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.

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 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 Azure Site Recovery
C. Configure a long-term retention policy for the database
D. Use automatic Azure SQL Database backups
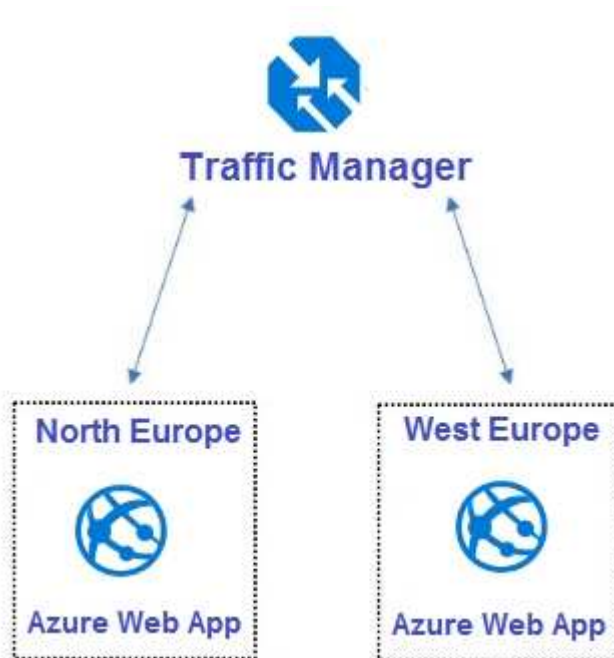
Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 2
HOTSPOT

You design a solution for the web tier of WebApp1 as shown in the exhibit.

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

Hot Area:

Answer Area

Statements	Yes	No
The design supports the technical requirements for redundancy.	O	O
The design supports autoscaling.	O	O
The design requires a manual configuration if an Azure region fails.	O	O

Correct Answer:

Answer Area

Statements	Yes	No
The design supports the technical requirements for redundancy.	⦿	○
The design supports autoscaling.	⦿	○
The design requires a manual configuration if an Azure region fails.	○	⦿

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: Yes
Any new deployments to Azure must be redundant in case an Azure region fails.

Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints. An endpoint is any Internet-facing service hosted inside or outside of Azure. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Box 2: Yes
Recent changes in Azure brought some significant changes in autoscaling options for Azure Web Apps (i.e. Azure App Service to be precise as scaling happens on App Service plan level and has effect on all Web Apps running in that App Service plan).

Box 3: No
Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.
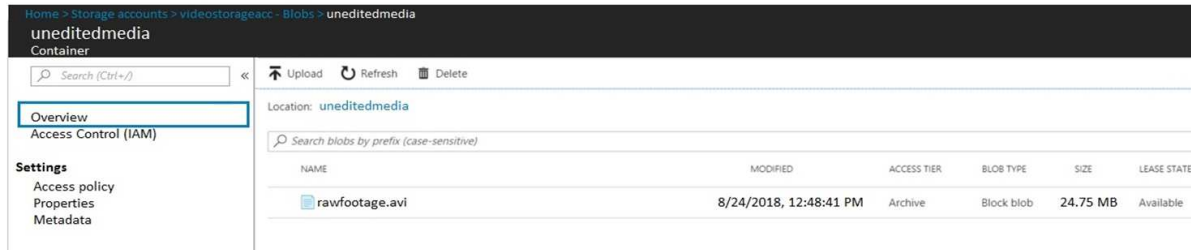
Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview

https://blogs.msdn.microsoft.com/hsirtl/2017/07/03/autoscaling-azure-web-apps/

Question Set 3

QUESTION 1
HOTSPOT

You plan to create a storage account and to save the files as shown in the following exhibit.

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 access the files, you must **[answer choice]**.

generate a snapshot
modify the access tier
modify the blob type

The files will be stored **[answer choice]**.

at the highest storage cost
at the lowest data retrieval cost
at the lowest storage cost

Correct Answer:

Answer Area

To access the files, you must [answer choice].

generate a snapshot
modify the access tier
modify the blob type

The files will be stored [answer choice].

at the highest storage cost
at the lowest data retrieval cost
at the lowest storage cost

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers#archive-access-tier-preview

QUESTION 2
You plan to use Azure Site Recovery to protect several on-premises physical server workloads. Each server workload is independent of the other. The workloads are stateless.

You need to recommend a failover strategy to ensure that if the on-premises data center fails, the workloads are available in Azure as quickly as possible.

Which failover strategy should you include in the recommendation?

A. Latest
B. Latest app-consistent
C. Latest multi-VM processed
D. Latest processed

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-failover

QUESTION 3
DRAG DROP

Your company identifies the following business continuity and disaster recovery objectives for virtual machines that host sales, finance, and reporting applications in the company's on-premises data center:

▪ The finance application requires that data be retained for seven years. In the event of a disaster, the application must be able to run from Azure. The recovery time objective (RTO) is 10 minutes.
▪ The reporting application must be able to recover point-in-time data at a daily granularity. The RTO is eight hours.

- The sales application must be able to fail over to a second on-premises data center.

You need to recommend which Azure services meet the business continuity and disaster recovery objectives. The solution must minimize costs.

What should you recommend for each application? To answer, drag the appropriate services to the correct applications. Each service 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:

Actions		Answer Area	
Azure Backup only		Sales:	Service or Services
Azure Site Recovery only		Finance:	Service or Services
Azure Site Recovery and Azure Backup		Reporting:	Service or Services

Correct Answer:

Actions		Answer Area	
		Sales:	Azure Site Recovery and Azure Backup
		Finance:	Azure Backup only
		Reporting:	Azure Site Recovery only

Section: [none]
Explanation

Explanation/Reference:

QUESTION 4
You plan to move a web application named App1 from an on-premises data center to Azure.

App1 depends on a custom COM component that is installed on the host server.

You need to recommend a solution to host App1 in Azure. The solution must meet the following requirements:

- App1 must be available to users if an Azure data center becomes unavailable.
- Costs must be minimized.

What should you include in the recommendation?

A. In two Azure regions, deploy a Traffic Manager profile and a web app.
B. In two Azure regions, deploy a load balancer and a virtual machine scale set.
C. Deploy a load balancer and a virtual machine scale set across two availability zones.

D. In two Azure regions, deploy a load balancer and a web app.

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 5
You plan to deploy a payroll system to Azure. The payroll system will use Azure virtual machines that run SUSE Linux Enterprise Server and Windows.

You need to recommend a business continuity solution for the payroll system. The solution must meet the following requirements:

▪ Minimize costs.
▪ Provide business continuity if an Azure region fails.
▪ Provide a recovery time objective (RTO) of 120 minutes.
▪ Provide a recovery point objective (RPO) of five minutes.

What should you include in the recommendation?

A. Microsoft System Center Data Protection Manager (DPM)
B. Azure Site Recovery
C. unmanaged disks that use geo-redundant storage (GRS)
D. Azure Backup

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
If your storage account has GRS enabled, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.

Note: The recovery time objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

Incorrect Answers:
B: Azure Site Recovery would not protect against an Azure region failure.

Azure Site Recovery guarantees a two-hour Recovery Time Objective.

Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-grs

https://azure.microsoft.com/en-us/support/legal/sla/site-recovery/v1_0/

QUESTION 6
The accounting department at your company migrates to a new financial accounting software. The accounting department must keep file-based database backups for seven years for compliance purposes. It is unlikely that the backups will be used to recover data.

You need to move the backups to Azure. The solution must minimize costs.

Where should you store the backups?

A. Azure SQL Database
B. Azure Blob storage that uses the Archive tier
C. a Recovery Services vault
D. Azure Blob storage that uses the Cool tier

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 7
HOTSPOT

Your company has two on-premises sites in New York and Los Angeles and Azure virtual networks in the East US Azure region and the West US Azure region. Each on-premises site has Azure ExpressRoute circuits to both regions.

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

▪ Outbound traffic to the Internet from workloads hosted on the virtual networks must be routed through the closest available on-premises site.
▪ If an on-premises site fails, traffic from the workloads on the virtual networks to the Internet must reroute automatically to the other site.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

◆

Routing from the virtual networks to the on-premises locations must be configured by using:	▼
	Azure default routes
	Border Gateway Protocol (BGP)
	User-defined routes

The automatic routing configuration following a failover must be handled by using:	▼
	Border Gateway Protocol (BGP)
	Hot Standby Routing Protocol (HSRP)
	Virtual Router Redundancy Protocol (VRRP)

Correct Answer:

Answer Area

Routing from the virtual networks to the on-premises locations must be configured by using:	▼
	Azure default routes
	Border Gateway Protocol (BGP)
	User-defined routes

The automatic routing configuration following a failover must be handled by using:	▼
	Border Gateway Protocol (BGP)
	Hot Standby Routing Protocol (HSRP)
	Virtual Router Redundancy Protocol (VRRP)

Section: [none]
Explanation

Explanation/Reference:

QUESTION 8
You plan to store data in Azure Blob storage for many years. The stored data will be accessed rarely.

You need to ensure that the data in Blob storage is always available for immediate access. The solution must minimize storage costs.

Which storage tier should you use?

A. Cool
B. Archive
C. Hot

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Azure cool tier is equivalent to the Amazon S3 Infrequent Access (S3-IA) storage in AWS that provides a low cost high performance storage for infrequently access data.

Note: Azure's cool storage tier, also known as Azure cool Blob storage, is for infrequently-accessed data that needs to be stored for a minimum of 30 days. Typical use cases include backing up data before tiering to archival systems, legal data, media files, system audit information, datasets used for big data analysis and more.

The storage cost for this Azure cold storage tier is lower than that of hot storage tier. Since it is expected that the data stored in this tier will be accessed less frequently, the data access charges are high when compared to hot tier. There are no additional changes required in your applications as these tiers can be accessed using APIs in the same manner that you access Azure storage.

Incorrect Answers:
B: Even though Azure archive storage offers the lowest cost in terms of data storage, its data retrieval charges are higher than that of hot and cool tiers. In fact, the data in the archive tier remains offline until the tier of the

data is changed using a process called hydration. The process of hydrating data in the archive storage tier and moving it to either hot or cool tier could take up to 15 hours and, hence, it is only intended for data that can afford that kind of access delay.

C: The storage cost for this Azure cold storage tier is lower than that of hot storage tier.

Reference:
https://cloud.netapp.com/blog/low-cost-storage-options-on-azure

QUESTION 9
HOTSPOT

You have a virtual machine scale set named SS1.

You configure autoscaling as shown in the following exhibit.

Default   **Profile1** ✎

Delete warning	The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode   ⦿ Scale based on a metric   ○ Scale to a specific instance count

Rules

Scale out

| When | SS1 | (Average) Percentage CPU > 75 | Increase instance count by 3 |

Scale in

| When | SS1 | (Average) Percentage CPU < 25 | Decrease instance count by 2 |

➕ Add a rule

Instance limits

Minimum ❶	Maximum ❶	Default ❶
3	15	6

Schedule   This scale condition is executed when none of the other scale condition(s) match

You configure the scale out and scale in rules to have a duration of 10 minutes and a cool down time of 10 minutes.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

If SS1 scales to nine virtual machines, what is the
minimum amount of time before SS1 will scale up?

10 minutes
20 minutes
30 minutes
60 minutes

If SS1 scales to nine virtual machines, and then the
average processor utilization is 30 percent for one
hour, how many virtual machines will be in SS1?

1
3
6
9
12
15

Correct Answer:

Answer Area

If SS1 scales to nine virtual machines, what is the
minimum amount of time before SS1 will scale up?

10 minutes
20 minutes
30 minutes
60 minutes

If SS1 scales to nine virtual machines, and then the
average processor utilization is 30 percent for one
hour, how many virtual machines will be in SS1?

1
3
6
9
12
15

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: 20 Minutes. 10 minutes cool down time after the last scale-up plus 10 minutes duration equals 20
minutes.

Box 2: 9 virtual machines. 30% does not match the scale in requirement of less than 25% so the number of virtual machines will not change.

QUESTION 10
HOTSPOT

You have 20 Azure virtual machines that run Windows Server 2016 based on a custom virtual machine image. Each virtual machine hosts an instance of a VSS-capable web app that was developed in-house. Each instance is accessed by using a public endpoint. Each instance uses a separate database. The average database size is 200 GB.

You need to design a disaster recovery solution for individual instances. The solution must meet the following requirements:

- Provide a recovery time objective (RTO) of six hours
- Provide a recovery point objective (RPO) of eight hours
- Support recovery to a different Azure region
- Support VSS-based backups
- Minimize costs

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Disaster recovery solution:

Azure Site Recovery
Scheduled backups by using an Azure Backup agent
Scheduled backups by using Windows Server Backup
Scheduled virtual machine-level backups

Storage type:

A Recovery Services vault
Premium managed disks
Unmanaged disks in an storage account that uses RA-GRS

Correct Answer:

Answer Area

Disaster recovery solution: ▼

Azure Site Recovery
Scheduled backups by using an Azure Backup agent
Scheduled backups by using Windows Server Backup
Scheduled virtual machine-level backups

Storage type: ▼

A Recovery Services vault
Premium managed disks
Unmanaged disks in an storage account that uses RA-GRS

Section: [none]
Explanation

Explanation/Reference:

QUESTION 11
HOTSPOT

You plan to deploy the backup policy shown in the following exhibit.

Policy1

Associated items   Delete   Save   Discard

Backup frequency

| Daily | ∨ | 6:00 PM | ∨ | (UTC) Coordinated Universal Time | ∨ |

Retention range

☑ Retention of daily backup point.

| * At | For | |
| 6:00 PM ∨ | 90 | Day(s) |

☑ Retention of weekly backup point.

| * On | * At | For | |
| Sunday ∨ | 6:00 PM ∨ | 26 | Week(s) |

☑ Retention of monthly backup point.

Week Based   Day Based

| * On | * Day | * At | For | |
| First ∨ | Sunday ∨ | 6:00 PM ∨ | 36 | Month(s) |

☐ Retention of yearly backup point.

Not Configured

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

Virtual machines that are backed up using the policy can be recovered for up to a maximum of **[answer choice]**.

	▼
90 days	
26 weeks	
36 months	
45 months	

The minimum recovery point objective (RPO) for virtual machines that are backed up by using the policy is **[answer choice]**.

	▼
1 hour	
1 day	
1 week	
1 month	
1 year	

Correct Answer:

Answer Area

Virtual machines that are backed up using the policy can be recovered for up to a maximum of **[answer choice]**.

	▼
90 days	
26 weeks	
36 months	
45 months	

(36 months highlighted)

The minimum recovery point objective (RPO) for virtual machines that are backed up by using the policy is **[answer choice]**.

	▼
1 hour	
1 day	
1 week	
1 month	
1 year	

(1 day highlighted)

Section: [none]
Explanation

Explanation/Reference:

QUESTION 12
HOTSPOT

You have databases in Azure as shown in the following table.

Name	Type	Pricing tier
SQLdb1	Azure SQL Database	Basic
SQLdb2	Azure SQL Database	Standard
SQLdb3	Azure SQL Database	Premium
DW1	Azure SQL Data Warehouse	*Not available*

You are designing a data retention policy.

You need to identify which databases can retain a daily backup for up to 35 days and which databases can retain monthly backups for up to 120 months.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Databases that can retain a daily backup for up to 35 days:

▼
DW1 only
SQLdb2 and SQLdb3 only
SQLdb1, SQLdb2 and SQLdb3 only
SQLdb1, SQLdb2, SQLdb3 and DW1

Databases that can retain monthly backups for up to 120 months:

▼
DW1 only
SQLdb2 and SQLdb3 only
SQLdb1, SQLdb2 and SQLdb3 only
SQLdb1, SQLdb2, SQLdb3 and DW1

Correct Answer:

Answer Area

Databases that can retain a daily backup for up to 35 days:

DW1 only
SQLdb2 and SQLdb3 only
SQLdb1, SQLdb2 and SQLdb3 only
SQLdb1, SQLdb2, SQLdb3 and DW1

Databases that can retain monthly backups for up to 120 months:

DW1 only
SQLdb2 and SQLdb3 only
SQLdb1, SQLdb2 and SQLdb3 only
SQLdb1, SQLdb2, SQLdb3 and DW1

Section: [none]
Explanation

Explanation/Reference:

QUESTION 13
You have an on-premises network and an Azure subscription. The on-premises network has several branch offices.

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

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

What should you include in the recommendation?

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

Correct Answer: B
Section: [none]
Explanation

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

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

Incorrect Answers:
A: Backups would be a slower solution.

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

QUESTION 14
You have an Azure subscription for used for testing and development purposes only. The subscription contains Azure virtual machines that unmanaged, standard hard disk drives (HDD).

You need to recommend a recovery strategy for the virtual machines if an Azure region fails for a sustained period. The recovery time objective (RTO) can be up to seven days. The solution must minimize costs.

What should you include in the recommendation?

A. Store the disks in a Standard_LRS storage account. Configure Azure site Recovery. If a failure occurs, initiate a manual failover.
B. Store the disks in a Standard_GRS storage account. Configure Azure Recovery. If a failure occurs, initiate a manual failover.
C. Store the disks in a Standard_LRS storage account. If a disaster occurs, manually create the virtual machines by used Azure Resources Manager templates.
D. Store the disks in a Standard_GRS storage account. If a disaster occurs, manually create the virtual machines by used Azure Resources Manager templates.

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Geo-redundant storage (GRS) is designed to provide at least 99.99999999999999% (16 9's) durability of objects over a given year by replicating your data to a secondary region that is hundreds of miles away from the primary region. If your storage account has GRS enabled, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.

GRS replicates your data to another data center in a secondary region, but that data is available to be read only if Microsoft initiates a failover from the primary to secondary region.

Incorrect Answers:
A, C: If a datacenter-level disaster (for example, fire or flooding) occurs, all replicas in a storage account using LRS may be lost or unrecoverable. To mitigate this risk, Microsoft recommends using zone-redundant storage (ZRS), geo-redundant storage (GRS), or geo-zone-redundant storage (GZRS).

Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-grs

QUESTION 15
You plan to deploy a payroll system to Azure. The payroll system will use Azure virtual machines that run SUSE Linux Enterprise Server and Windows.

You need to recommend a business continuity solution for the payroll system. The solution must meet the following requirements:

- Minimize costs.
- Provide business continuity if an Azure region fails.
- Provide a recovery time objective (RTO) of 30 minutes.
- Provide a recovery point objective (RPO) of five minutes.

What should you include in the recommendation?

A. Microsoft System Center Data Protection Manager (DPM)

B. Azure Site Recovery

C. unmanaged disks that use geo-redundant storage (GRS)

D. Azure Backup

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
If your storage account has GRS enabled, then your data is durable even in the case of a complete regional outage or a disaster in which the primary region isn't recoverable.

Note: The recovery time objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.

Incorrect Answers:
B: Azure Site Recovery would not protect against an Azure region failure.

Azure Site Recovery guarantees a two-hour Recovery Time Objective.

Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy-grs

https://azure.microsoft.com/en-us/support/legal/sla/site-recovery/v1_0/

QUESTION 16
You have an Azure Storage account that contains the data shown in the following exhibit.

You need to identify which files can be accessed immediately from the storage account.

Which files should you identify?

A. File1.bin only

B. File2.bin only

C. File3.bin only

D. File1.bin and File2.bin only

E. File1.bin, File2.bin, and File3.bin

Correct Answer: D

Section: [none]
Explanation

Explanation/Reference:
Explanation:
Hot - Optimized for storing data that is accessed frequently.
Cool - Optimized for storing data that is infrequently accessed and stored for at least 30 days.
Archive - Optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

Note: Lease state of the blob. Possible values: available|leased|expired|breaking|broken

References:
https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-storage-tiers

Testlet 1

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

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

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

To start the case study
To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirement, 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

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

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.

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.

Problem Statements

The use of Web App1 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.

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 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 platform as a service (PaaS).
- 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.

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.

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 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
HOTSPOT

You are evaluating the components of the migration to Azure that require you to provision an Azure Storage

account.

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
You must provision an Azure Storage account for the SQL Server database migration.	○	○
You must provision an Azure Storage account for the Web site content storage.	○	○
You must provision an Azure Storage account for the Database metric monitoring.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
You must provision an Azure Storage account for the SQL Server database migration.	●	○
You must provision an Azure Storage account for the Web site content storage.	○	●
You must provision an Azure Storage account for the Database metric monitoring.	●	○

Section: [none]
Explanation

Explanation/Reference:

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. Use SQL Server transactional replication
C. Copy the VHD that contains the Azure SQL database files to Azure Blob storage
D. Copy the BACPAC file that contains the Azure SQL database files to Azure Blob storage

Correct Answer: C
Section: [none]
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

QUESTION 3
You need to recommend a strategy for the web tier of WebApp1. The solution must minimize costs.

What should you recommend?

A. Configure the Scale Up settings for a web app
B. Create a runbook that resizes virtual machines automatically to a smaller size outside of business hours
C. Deploy a virtual machine scale set that scales out on a 75 percent CPU threshold
D. Configure the Scale Out settings for a web app

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:

Question Set 2

QUESTION 1
DRAG DROP

You plan to import data from your on-premises environment into Azure. The data is shown in the following table.

On-premises source	Azure target
A Microsoft SQL Server 2012 database	An Azure SQL database
A table in a Microsoft SQL Server 2008 database	An Azure Cosmos DB account that uses the SQL API

What should you recommend using to migrate the data? To answer, drag the appropriate tools to the correct data sources. Each tool 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:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/dms/tutorial-sql-server-to-azure-sql

QUESTION 2
You have an on-premises deployment of MongoDB.

You plan to migrate MongoDB to an Azure Cosmos DB account that uses the MongoDB API.

You need to recommend a solution for migrating MongoDB to Azure Cosmos DB.

What should you include in the recommendation?

A. mongorestore
B. Data Migration Assistant
C. Azure Storage Explorer
D. Azure Cosmos DB Data Migration Tool

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/cosmos-db/mongodb-migrate

QUESTION 3
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
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Set a new transformation policy to transform an API to strip response headers.

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

QUESTION 4
Your company has 300 virtual machines hosted in a Vmware environment. The virtual machines vary in size and have various utilization levels.

You plan to move all the virtual machines to Azure.

You need to recommend how many and what size Azure virtual machines will be required to move the current workloads to Azure. The solution must minimize administrative effort.

What should you use to make the recommendation?

A. Azure Advisor
B. Azure Migrate
C. Azure Pricing calculator
D. Azure Cost Management

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 5
**Note: This question is a part of series of questions that present the same scenario. Each question in
the series contains a unique solution that might meet the stated goals. Some question sets might have
more than one correct solution, while others might not have a correct solution.**

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

You are designing an Azure solution for a company that wants to move a .NET Core web application from an
on-premises data center to Azure. The web application relies on a Microsoft SQL Server 2016 database on
Windows Server 2016. The database server will not move to Azure.

A separate networking team is responsible for configuring network permissions.

The company uses Azure ExpressRoute and has an ExpressRoute gateway connected to an Azure virtual
network named VNET1.

You need to recommend a solution for deploying the web application.

Solution:
Deploy the web application to a web app hosted in a Standard App Service plan. Create and configure an
Azure App Service Hybrid Connections endpoint.
On the on-premises network, deploy the Hybrid Connection Manager. Configure the Hybrid Connection
Manager to access both the Hybrid Connection endpoint and the SQL Server instance.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead, use VNet Integration.

Note: VNet Integration gives your web app access to resources in your virtual network. VNet Integration is often
used to enable access from apps to a databases and web services running in your VNet.

Reference:
https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet

QUESTION 6
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

A company has custom ASP.NET and Java applications that run old versions of Windows and Linux. The company plans to place applications in containers.

You need to design a solution that includes networking, service discovery, and load balancing for the applications. The solution must support storage orchestration.

Solution: You create an Azure virtual network, public IP address, and load balancer. Then add virtual machines (VMs) to the solution and deploy individual containers on them.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead you should deploy each application to an Azure Container instance.

Note: Docker Containers are the global standard and are natively supported in Azure, offering enterprises an interesting and flexible way to migrate legacy apps for both future proofing and cost benefits.

Reference:
https://docs.microsoft.com/en-us/dotnet/standard/modernize-with-azure-and-containers/modernize-existing-apps-to-cloud-optimized/deploy-existing-net-apps-as-windows-containers

QUESTION 7
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

A company has custom ASP.NET and Java applications that run old versions of Windows and Linux. The company plans to place applications in containers.

You need to design a solution that includes networking, service discovery, and load balancing for the applications. The solution must support storage orchestration.

Solution: Deploy a Kubernetes cluster that has the desired number of instances of the applications.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead you should deploy each application to an Azure Container instance.

Note: Docker Containers are the global standard and are natively supported in Azure, offering enterprises an interesting and flexible way to migrate legacy apps for both future proofing and cost benefits.

Reference:
https://docs.microsoft.com/en-us/dotnet/standard/modernize-with-azure-and-containers/modernize-existing-apps-to-cloud-optimized/deploy-existing-net-apps-as-windows-containers

QUESTION 8
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

A company has custom ASP.NET and Java applications that run old versions of Windows and Linux. The company plans to place applications in containers.

You need to design a solution that includes networking, service discovery, and load balancing for the applications. The solution must support storage orchestration.

Solution: You deploy each application to an Azure Container instance.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Docker Containers are the global standard and are natively supported in Azure, offering enterprises an interesting and flexible way to migrate legacy apps for both future proofing and cost benefits.

Containers are modular and portable. Docker containers are supported on any server operating system (Linux and Windows), in any major public cloud (Microsoft Azure, Amazon AWS, Google, IBM), and in on-premises and private or hybrid cloud environments.

Reference:
https://docs.microsoft.com/en-us/dotnet/standard/modernize-with-azure-and-containers/modernize-existing-apps-to-cloud-optimized/deploy-existing-net-apps-as-windows-containers

QUESTION 9
HOTSPOT

You have a web application that uses a MongoDB database. You plan to migrate the web application to Azure.

You must migrate to Cosmos DB while minimizing code and configuration changes.

You need to design the Cosmos DB configuration.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Option	Value
MongoDB compatibility	Database / API / Collection / Account
API	Cassandra API / DocumentDB API / Graph API / MongoDB API / Table API

◆

Correct Answer:

Answer Area

Option	Value
MongoDB compatibility	Database **API** Collection Account
API	Cassandra API DocumentDB API Graph API **MongoDB API** Table API

Section: [none]
Explanation

Explanation/Reference:
Explanation:

MongoDB compatibility: API

API: MongoDB API
Azure Cosmos DB comes with multiple APIs:
- SQL API, a JSON document database service that supports SQL queries. This is compatible with the former Azure DocumentDB.
- MongoDB API, compatible with existing Mongo DB libraries, drivers, tools and applications.
- Cassandra API, compatible with existing Apache Cassandra libraries, drivers, tools, and applications.
- Azure Table API, a key-value database service compatible with existing Azure Table Storage.
- Gremlin (graph) API, a graph database service supporting Apache Tinkerpop's graph traversal language, Gremlin.

Reference:
https://docs.microsoft.com/en-us/azure/cosmos-db/create-mongodb-dotnet

QUESTION 10
You manage an application instance. The application consumes data from multiple databases. Application code references database tables using a combination of the server, database, and table name.

You need to migrate the application instance to Azure.

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

NOTE: Each correct selection is worth one point.

A. SQL Server Stretch Database
B. SQL Server in an Azure virtual machine
C. Azure SQL Database
D. SQL Managed Instance

Correct Answer: AD
Section: [none]
Explanation

Explanation/Reference:
Explanation:
A: Access your SQL Server data seamlessly regardless of whether it's on-premises or stretched to the cloud. You set the policy that determines where data is stored, and SQL Server handles the data movement in the background. The entire table is always online and queryable. And, Stretch Database doesn't require any changes to existing queries or applications - the location of the data is completely transparent to the application.

D: The managed instance deployment model is designed for customers looking to migrate a large number of apps from on-premises or IaaS, self-built, or ISV provided environment to fully managed PaaS cloud environment, with as low migration effort as possible. Using the fully automated Data Migration Service (DMS) in Azure, customers can lift and shift their on-premises SQL Server to a managed instance that offers compatibility with SQL Server on-premises and complete isolation of customer instances with native VNet support.

Reference:
https://docs.microsoft.com/en-us/sql/sql-server/stretch-database/stretch-database

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

QUESTION 11
You have 100 Microsoft SQL Server Integration Services (SSIS) packages that are configured to use 10 on-premises SQL Server databases as their destinations.

You plan to migrate the 10 on-premises databases to Azure SQL Database.

You need to recommend a solution to host the SSIS packages in Azure. The solution must ensure that the packages can target the SQL Database instances as their destinations.

What should you include in the recommendation?

A. SQL Server Migration Assistant (SSMA)
B. Azure Data Factory
C. Data Migration Assistant
D. Azure Data Catalog

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 12

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

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

A company has custom ASP.NET and Java applications that run on old versions of Windows and Linux. The company plans to place applications in containers.

You need to design a solution that includes networking, service discovery, and load balancing for the applications. The solution must support storage orchestration.

Solution: You deploy each application to an Azure Web App that has container support.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
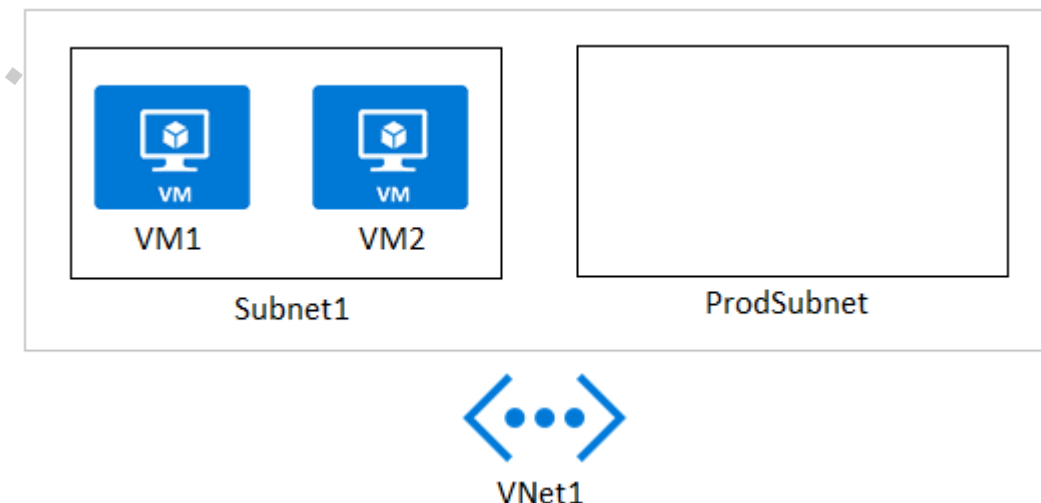**Section: [none]**
Explanation

Explanation/Reference:

QUESTION 13
HOTSPOT

Your company develops a web service that is deployed to an Azure virtual machine named VM1. The web service allows an API to access real-time data from VM1.

The current virtual machine deployment is shown in the Deployment exhibit. (Click the **Deployment** tab).

The chief technology officer (CTO) sends you the following email message: "Our developers have deployed the web service to a virtual machine named VM1. Testing has shown that the APIs is accessible from VM1 and VM2. Our partners must be able to connect to the API over the Internet. Partners will use this data in application that they develop".

You deploy an Azure API Management (APIM) service. The relevant API Management configuration is shown in the API exhibit. (Click the **API** tab).

Virtual network	Off	External	Internal

LOCATION	VIRTUAL NETWORK	SUBNET
North Europe	VNet1	ProdSubnet

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
The API is available to partners over the Internet	○	○
The APIM instance can access real-time from VM1	○	○
A VPN gateway is required for partner access	○	○

Correct Answer:

◆ ## Answer Area

Statements	Yes	No
The API is available to partners over the Internet	⬤	○
The APIM instance can access real-time from VM1	⬤	○
A VPN gateway is required for partner access	○	⬤

Section: [none]
Explanation

Explanation/Reference:

Reference:

https://docs.microsoft.com/en-us/azure/api-management/api-management-using-with-vnet

◆

Testlet 1

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

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

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

To start the case study
To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirement, 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.

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.

Current Issues

The Contoso IT team discovers poor performance of the historical transaction query system, at 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.

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.
▪ 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 transactions query system remains available without any administrative intervention.

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. legitimate users must be able to

authenticate successfully by using multi-factor authentication.

QUESTION 1
You need to recommend a compute solution for the middle tier of the payment processing system.

What should you include in the recommendation?

A. Azure Kubernetes Service (AKS)
B. virtual machine scale sets
C. availability sets
D. App Service Environments (ASEs)

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 2
You need to recommend a solution for the network configuration of the front-end tier of the payment processing.

What should you include in the recommendation?

A. Azure Application Gateway
B. Traffic Manager
C. a Standard Load Balancer
D. a Basic load Balancer

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Scenario:
▪ 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.

With Azure Load Balancer, you can scale your applications and create high availability for your services. Load Balancer supports inbound and outbound scenarios, provides low latency and high throughput, and scales up to millions of flows for all TCP and UDP applications.

Azure Load Balancer is available in two SKUs: Basic and Standard. There are differences in scale, features, and pricing. Standard SLA guarantees a 99.99% for data path with two healthy virtual machines. Basic SLA does not exist.

Reference:
https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

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 requirement, 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

Fabrikam, Inc. is an engineering company that has offices throughout Europe. The company has a main office in London and three branch offices in Amsterdam, Berlin, and Rome.

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.

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.

Problem Statements

The use of Web App1 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.

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 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 platform as a service (PaaS).
- 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.

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.

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 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 notification solution for the IT Support distribution group.

What should you include in the recommendation?

A. Azure Network Watcher
B. an action group
C. a SendGrid account with advanced reporting
D. Azure AD Connect Health

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-health-operations

Question Set 3

QUESTION 1
You need to recommend a data storage solution that meets the following requirements:

- Ensures that application can access the data by using a REST connection
- Hosts 20 independent tables of varying sizes and usage patterns
- Automatically replicates the data to a second Azure region
- Minimizes costs

What should you recommend?

A. an Azure SQL Database elastic database pool that uses active geo-replication
B. tables in an Azure Storage account that uses geo-redundant storage (GRS)
C. tables in an Azure Storage account that use read-access geo-redundant storage (RA-GR)
D. an Azure SQL database that uses active geo-replication

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 2
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 updated once.
- Minimize costs.

What should you include in the recommendation?

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

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 3
Your company has an on-premises Windows HPC cluster. The cluster runs an intrinsically parallel, compute-intensive workload that performs financial risk modelling.

You plan to migrate the workload to Azure Batch.

You need to design a solution that will support the workload. The solution must meet the following

requirements:

- Support the large-scale parallel execution of Azure Batch jobs.
- Minimize cost.

What should you include in the solution?

A. Basic A-series virtual machines

B. low-priority virtual machines

C. burstable virtual machines

D. Azure virtual machine sizes that support the Message Passing Interface (MPI) API

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/batch/batch-technical-overview

QUESTION 4
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	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	

Correct Answer:

Certificates

A root CA certificate that has the private key	
A root CA certificate that has the public key	
A user certificate that has the private key	
A user certificate that has the public key	

Answer Area

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

Section: [none]
Explanation

Explanation/Reference:

QUESTION 5
DRAG DROP

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016 and Linux.

You need to use Azure Log Analytics design an alerting strategy for security-related events.

Which Log Analytics tables should you query? To answer, drag the appropriate tables to the correct log types. Each value 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:

Tables

AzureActivity
AzureDiagnostics
Event
Syslog

Answer Area

Events from Windows event logs:	Table
Events from Linux system logging:	Table

Correct Answer:

Tables

AzureActivity
AzureDiagnostics
Event
Syslog

Answer Area

Events from Windows event logs:

Event

Events from Linux system logging:

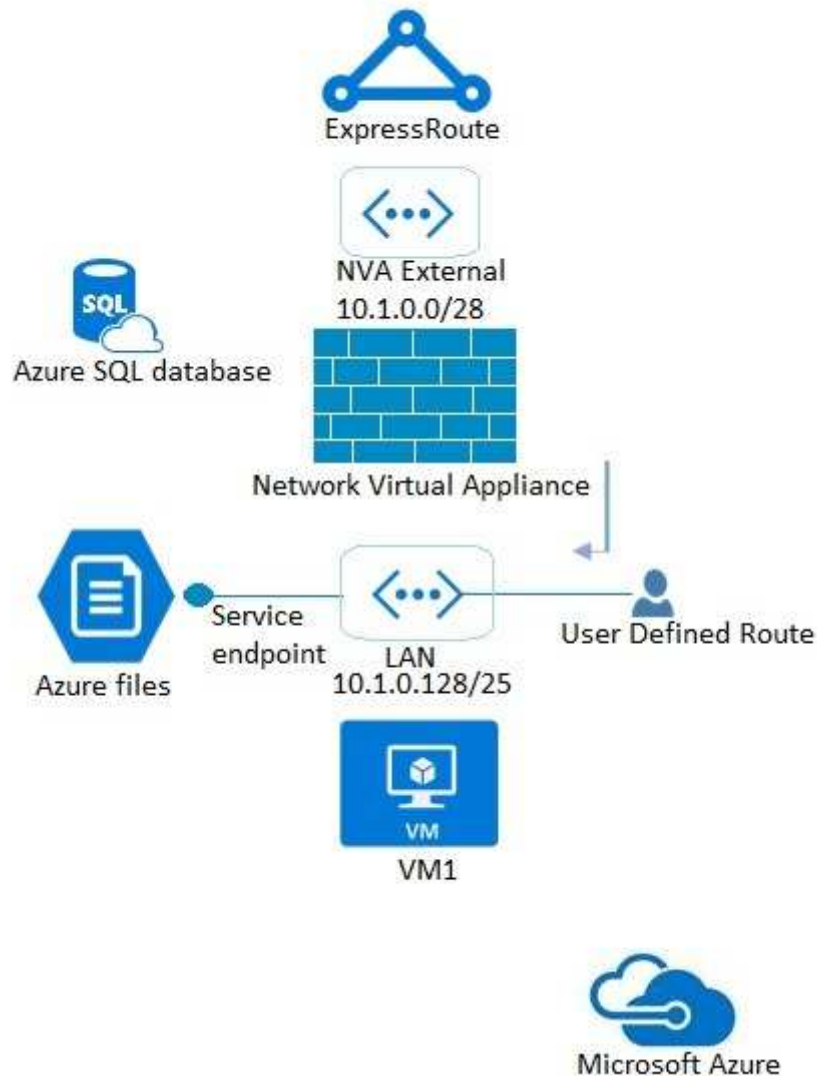| |
|---|
| Syslog |

Section: [none]
Explanation

Explanation/Reference:

QUESTION 6
HOTSPOT

You have the network topology shown in the following exhibit.

◆

You have a user-defined route that has a default route of 0.0.0.0/0 and the next hop set to the network virtual appliance.

You configure the Azure Storage account to use virtual network service endpoints.

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
From VM1, traffic destined to the Azure Key Management Service will be routed to the network virtual appliance.	◯	◯
From VM1, traffic destined to the Azure file share will be routed to the Internet.	◯	◯
From VM1, traffic destined to the Azure SQL database will be routed to the Internet.	◯	◯

Correct Answer:

Answer Area

Statements	Yes	No
From VM1, traffic destined to the Azure Key Management Service will be routed to the network virtual appliance.	◉	◯
From VM1, traffic destined to the Azure file share will be routed to the Internet.	◯	◉
From VM1, traffic destined to the Azure SQL database will be routed to the Internet.	◯	◉

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-udr-overview

QUESTION 7
You are designing a container solution in Azure that will include two containers. One container will host a web API that will be available to the public. The other container will perform health monitoring of the web API and will remain private. The two containers will be deployed together as a group.

You need to recommend a compute service for the containers. The solution must minimize costs and maintenance overhead.

What should you include in the recommendation?

A. Azure Service Fabric
B. Azure Container Service
C. Azure Kubernetes Service (AKS)
D. Azure Container Instances

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

Reference:
https://docs.microsoft.com/en-us/azure/container-instances/container-instances-multi-container-group

QUESTION 8
HOTSPOT

Your company has three branch offices and an Azure subscription. Each branch office contains a Hyper-V host that hosts application servers.

You need to recommend a storage solution for the branch offices. The solution must ensure that the application servers can connect to a central storage device by using iSCSI connections. Data saved to the iSCSI storage device from the application servers must be uploaded to Azure automatically.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Branch office Hyper-V hosts:	▼
	Azure File Sync agent
	Azure Site Recovery agent
	Azure StorSimple Virtual Array
	Distributed File System Replication

Azure subscription:	▼
	Azure file share
	Azure File Sync
	Azure Site Recovery vault
	Azure Storage account

Correct Answer:

Answer Area

Branch office Hyper-V hosts:

Azure File Sync agent
Azure Site Recovery agent
Azure StorSimple Virtual Array
Distributed File System Replication

Azure subscription:

Azure file share
Azure File Sync
Azure Site Recovery vault
Azure Storage account

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/storsimple/storsimple-ova-overview

QUESTION 9
DRAG DROP

You have an on-premises network that uses an IP address space of 172.16.0.0/16.

You plan to deploy 25 virtual machines to a new Azure subscription.

You identify the following technical requirements:

- All Azure virtual machines must be placed on the same subnet named Subnet1.
- All the Azure virtual machines must be able to communicate with all on-premises servers.
- The servers must be able to communicate between the on-premises network and Azure by using a site-to-site VPN.

You need to recommend a subnet design that meets the technical requirements.

What should you include in the recommendation? To answer, drag the appropriate network addresses to the correct subnets. Each network address 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:

Network Addresses

172.16.0.0/16

172.16.1.0/28

192.168.0.0/24

192.168.1.0/28

Answer Area

Subnet1: Network address

Gateway subnet: Network address

Correct Answer:

Network Addresses

172.16.0.0/16

172.16.1.0/28

Answer Area

Subnet1: 192.168.0.0/24

Gateway subnet: 192.168.1.0/28

Section: [none]
Explanation

Explanation/Reference:

QUESTION 10
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are migrating an on-premises application to Azure. One component of the application is a legacy Windows native executable that performs image processing.

The image processing application must run every hour. During times that the image processing application is not running, it should not be consuming any Azure compute resources.

You need to ensure that the image processing application runs correctly every hour.

Solution: Create an Azure WebJob that runs the image processing application every hour.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead use an Azure Logic Apps, which helps you automate workflows that run on a schedule.

Reference:
https://docs.microsoft.com/en-us/azure/logic-apps/tutorial-build-schedule-recurring-logic-app-workflow

QUESTION 11
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are migrating an on-premises application to Azure. One component of the application is a legacy Windows native executable that performs image processing.

The image processing application must run every hour. During times that the image processing application is not running, it should not be consuming any Azure compute resources.

You need to ensure that the image processing application runs correctly every hour.

Solution: Create an Azure Function to run the image processing application every hour.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead use an Azure Logic Apps, which helps you automate workflows that run on a schedule.

Reference:
https://docs.microsoft.com/en-us/azure/logic-apps/tutorial-build-schedule-recurring-logic-app-workflow

QUESTION 12
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are migrating an on-premises application to Azure. One component of the application is a legacy Windows native executable that performs image processing.

The image processing application must run every hour. During times that the image processing application is not running, it should not be consuming any Azure compute resources.

You need to ensure that the image processing application runs correctly every hour.

Solution: Create a Logic App to run the image processing application every hour.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Azure Logic Apps helps you automate workflows that run on a schedule.

Reference:
https://docs.microsoft.com/en-us/azure/logic-apps/tutorial-build-schedule-recurring-logic-app-workflow

QUESTION 13
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are designing an Azure solution for a company that wants to move a .NET Core web application from an on-premises data center to Azure. The web application relies on a Microsoft SQL Server 2016 database on Windows Server 2016. The database server will not move to Azure.

A separate networking team is responsible for configuring network permissions.

The company uses Azure ExpressRoute and has an ExpressRoute gateway connected to an Azure virtual network named VNET1.

You need to recommend a solution for deploying the web application.

Solution: Deploy the web application to a web app hosted in a Premium App Service plan. Configure VNET Integration for the App Service plan.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
VNet Integration gives your web app access to resources in your virtual network. VNet Integration is often used to enable access from apps to a databases and web services running in your VNet.

Reference:

QUESTION 14
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are designing an Azure solution for a company that wants to move a .NET Core web application from an on-premises data center to Azure. The web application relies on a Microsoft SQL Server 2016 database on Windows Server 2016. The database server will not move to Azure.

A separate networking team is responsible for configuring network permissions.

The company uses Azure ExpressRoute and has an ExpressRoute gateway connected to an Azure virtual network named VNET1.

You need to recommend a solution for deploying the web application.

Solution: Deploy the web application by using an Azure Kubernetes Service (AKS) container on VNET1.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead, use VNet Integration.

Note: VNet Integration gives your web app access to resources in your virtual network. VNet Integration is often used to enable access from apps to a databases and web services running in your VNet.

Reference:
https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet

QUESTION 15
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are designing an Azure solution for a company that wants to move a .NET Core web application from an on-premises data center to Azure. The web application relies on a Microsoft SQL Server 2016 database on Windows Server 2016. The database server will not move to Azure.

A separate networking team is responsible for configuring network permissions.

The company uses Azure ExpressRoute and has an ExpressRoute gateway connected to an Azure virtual network named VNET1.

You need to recommend a solution for deploying the web application.

Solution: Deploy the web application to a web app hosted in an isolated App Service plan on VNET1.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead, use VNet Integration.

Note: VNet Integration gives your web app access to resources in your virtual network. VNet Integration is often used to enable access from apps to a databases and web services running in your VNet.

Reference:
https://docs.microsoft.com/en-us/azure/app-service/web-sites-integrate-with-vnet

QUESTION 16
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You 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
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead, you should deploy an Azure virtual machine to two Azure regions, and you create a Traffic Manager profile.

QUESTION 17
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You 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 an Azure virtual machine to two Azure regions, and you create a Traffic Manager profile.

Does this meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 18
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You 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 an Azure virtual machine to two Azure regions, and you deploy an Azure Application Gateway.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
You deploy an Azure virtual machine to two Azure regions, but also create a Traffic Manager profile.

QUESTION 19
You plan to deploy an API by using Azure API Management.

You need to recommend a solution to protect the API from a distributed denial of service (DDoS) attack.

What should you recommend?

A. Create network security groups (NSGs).
B. Enable quotas.
C. Enable rate limiting.
D. Strip the Powered-By responsible header.

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:

QUESTION 20
You manage on-premises networks and Azure virtual networks.

You need a secure private connection between the on-premises networks and the Azure virtual networks. The connection must offer a redundant pair of cross connections to provide high availability.

What should you recommend?

A. ExpressRoute
B. Azure Load Balancer
C. virtual network peering
D. VPN Gateway

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

◆

QUESTION 21
DRAG DROP

An organization has an on-premises server that runs Windows Server 2003. The server hosts an IIS-based stateless web application that uses forms authentication. The application consists of classic Active Server Pages (ASP) pages and third-party components (DLLs) that are registered in the Windows registry.

The deployment process for the web application is manual and is prone to errors. The deployment process makes it difficult to roll out updates, scale out, and recover after failures.

You need to design a modernization approach for the web application that meets the following requirements:

▪ Improve the deployment process.
▪ Ensure that the application can run in the cloud.
▪ Minimize changes to application code.
▪ Minimize administrative effort required to implement the modernization solution.

What should you recommend? To answer, drag the appropriate actions to the correct approaches. Each action 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 point.

Select and Place:

Answer Area

Actions

Package the existing application in a container.
Configure the application to run in a web role.
Implement Azure functions.
Use Azure Container services.
Use a Web application.

Approach	Action
Modernization	
Deployment	

Correct Answer:

Answer Area

Actions

Configure the application to run in a web role.
Implement Azure functions.
Use a Web application.

Approach	Action
Modernization	Use Azure Container services.
Deployment	Package the existing application in a container.

Section: [none]
Explanation

Explanation/Reference:

◆

QUESTION 22
You use a virtual network to extend an on-premises IT environment into the cloud. The virtual network has two virtual machines (VMs) that store sensitive data.

The data must only be available using internal communication channels. Internet access to those VMs is not permitted.

You need to ensure that the VMs cannot access the Internet.

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

NOTE: Each correct selection is worth one point.

A. network interface (NIC)
B. Source Network Address Translation (SNAT)
C. Azure ExpressRoute
D. Network Security Groups (NSG)

Correct Answer: CD

Section: [none]
Explanation

Explanation/Reference:

QUESTION 23
Your company plans to migrate its on-premises data to Azure.

You need to recommend which Azure services can be used to store the data. The solution must meet the following requirements:

- Encrypt all data while at rest.
- Encrypt data only by using a key generated by the company.

Which two possible services can you recommend? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Azure Table storage
B. Azure Backup
C. Azure Blob storage
D. Azure Queue storage
E. Azure Files

Correct Answer: CE
Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption-customer-managed-keys

QUESTION 24
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. Enable parallel file systems on Azure.
C. Enable parallel task execution on compute nodes.
D. Create a render farm that uses virtual machine (VM) scale sets.
E. Create a render farm that uses virtual machines (VMs).

Correct Answer: AC
Section: [none]

Explanation

Explanation/Reference:

QUESTION 25
HOTSPOT

You are designing an Azure web app.

You plan to deploy the web app to the North Europe Azure region and the West Europe Azure region.

You need to recommend a solution for the web app. The solution must meet the following requirements:

▪ Users must always access the web app from the North Europe region, unless the region fails.
▪ The web app must be available to users if an Azure region is unavailable.
▪ Deployment costs must be minimized.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Request routing method: ▼

| A Traffic Manager profile |
| Azure Application Gateway |
| Azure Load Balancer |

Request routing configuration: ▼

| Cookie-based session affinity |
| Performance traffic routing |
| Priority traffic routing |
| Weighted traffic routing |

Correct Answer:

Answer Area

Request routing method:
[dropdown ▼]
A Traffic Manager profile
Azure Application Gateway
Azure Load Balancer

Request routing configuration:
[dropdown ▼]
Cookie-based session affinity
Performance traffic routing
Priority traffic routing
Weighted traffic routing

Section: [none]
Explanation

Explanation/Reference:

QUESTION 26
DRAG DROP

You need to design an architecture to capture the creation of users and the assignment of roles. The captured data must be stored in Azure Cosmos DB.

Which Azure services should you include in the design? To answer, drag the appropriate services to the correct targets. Each service 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:

Azure Services

Azure Event Grid

Azure Event Hubs

Azure Functions

Azure Monitor Logs

Azure Notification Hubs

Answer Area

Azure
Active Directory
audit log

↓

[ ]

↓

[ ]

↓

Cosmos DB

Correct Answer:

Azure Services

Azure Event Grid

Azure Monitor Logs

Azure Notification Hubs

Answer Area

Azure
Active Directory
audit log

↓

Azure Event Hubs

↓

Azure Functions

↓

Cosmos DB

Section: [none]
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 27
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 App Service Web Apps
B. Azure App Service Isolated
C. Azure Redis Cache
D. Azure Content Delivery Network (CDN)

Correct Answer: D
Section: [none]
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 28
HOTSPOT

Your company deploys an Azure App Service Web App.

During testing the application fails under load. The application cannot handle more than 100 concurrent user sessions. You enable the Always On feature. You also configure auto-scaling to increase counts from two to 10 based on HTTP queue length.

You need to improve the performance of the application.
◆
Which solution should you use for each application scenario? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Scenario	Solution
Store content close to end users.	▼
	Azure Redis Cache
	Azure Traffic Manager
	Azure Content Delivery Network
	Azure Application Gateway
Store content close to the application.	▼
	Azure Redis Cache
	Azure Traffic Manager
	Azure Content Delivery Network
	Azure Application Gateway

Correct Answer:

Answer Area

Scenario	Solution
Store content close to end users.	▼
	Azure Redis Cache
	Azure Traffic Manager
	Azure Content Delivery Network
	Azure Application Gateway
Store content close to the application.	▼
	Azure Redis Cache
	Azure Traffic Manager
	Azure Content Delivery Network
	Azure Application Gateway

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: Content Delivery Network
A content delivery network (CDN) is a distributed network of servers that can efficiently deliver web content to users. CDNs store cached content on edge servers in point-of-presence (POP) locations that are close to end users, to minimize latency.

Azure Content Delivery Network (CDN) offers developers a global solution for rapidly delivering high-bandwidth content to users by caching their content at strategically placed physical nodes across the world. Azure CDN can also accelerate dynamic content, which cannot be cached, by leveraging various network optimizations using CDN POPs. For example, route optimization to bypass Border Gateway Protocol (BGP).

Box 2: Azure Redis Cache
Azure Cache for Redis is based on the popular software Redis. It is typically used as a cache to improve the performance and scalability of systems that rely heavily on backend data-stores. Performance is improved by temporarily copying frequently accessed data to fast storage located close to the application. With Azure Cache for Redis, this fast storage is located in-memory with Azure Cache for Redis instead of being loaded from disk by a database.

Reference:
https://docs.microsoft.com/en-us/azure/azure-cache-for-redis/cache-overview

QUESTION 29
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You 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 web app in an Isolated App Service plan.

Does this meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead, you should deploy an Azure virtual machine to two Azure regions, and you create a Traffic Manager profile.

QUESTION 30
You are designing an Azure solution.

The network traffic for the solution must be securely distributed by providing the following features:

▪ HTTPS protocol

▪ Round robin routing
▪ SSL offloading

You need to recommend a load balancing option.

What should you recommend?

A. Azure Load Balancer
B. Azure Traffic Manager
C. Azure Internal Load Balancer (ILB)
D. Azure Application Gateway

Correct Answer: D
Section: [none]
Explanation

Explanation/Reference:
Explanation:
If you are looking for Transport Layer Security (TLS) protocol termination ("SSL offload") or per-HTTP/HTTPS request, application-layer processing, review Application Gateway.

Application Gateway is a layer 7 load balancer, which means it works only with web traffic (HTTP, HTTPS, WebSocket, and HTTP/2). It supports capabilities such as SSL termination, cookie-based session affinity, and round robin for load-balancing traffic. Load Balancer load-balances traffic at layer 4 (TCP or UDP).

Reference:
https://docs.microsoft.com/en-us/azure/application-gateway/application-gateway-faq

QUESTION 31
You manage a solution in Azure.

You must collect usage data including MAC addresses from all devices on the network.

You need to recommend a monitoring solution.

What should you recommend?

A. Activity Log Analytics
B. Azure Network Security Group Analytics
C. Network Performance Monitor
D. Azure Application Gateway Analytics
E. Azure Wire Data

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
A network security group (NSG) includes rules that allow or deny traffic to a virtual network subnet, network interface, or both. When you enable diagnostic logging for an NSG, you can log the following categories of information:

Event: Entries are logged for which NSG rules are applied to VMs, based on MAC address. The status for these rules is collected every 60 seconds.
Rule counter: Contains entries for how many times each NSG rule is applied to deny or allow traffic.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-nsg-manage-log

QUESTION 32
A partner manages on-premises and Azure environments. The partner deploys an on-premises solution that needs to use Azure services. The partner deploys a virtual appliance.

All network traffic that is directed 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.

NOTE: Each correct selection is worth one point.

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

Correct Answer: CD
Section: [none]
Explanation

Explanation/Reference:
Explanation:
C: 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.

D: 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 33
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are migrating an on-premises application to Azure. One component of the application is a legacy Windows native executable that performs image processing.

The image processing application must run every hour. During times that the image processing application is

not running, it should not be consuming any Azure compute resources.

You need to ensure that the image processing application runs correctly every hour.

Solution: Create an Azure Batch application that runs the image processing application every hour.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Instead use an Azure Logic Apps, which helps you automate workflows that run on a schedule.

Reference:
https://docs.microsoft.com/en-us/azure/logic-apps/tutorial-build-schedule-recurring-logic-app-workflow

QUESTION 34
HOTSPOT

You have an Azure subscription that contains 300 Azure virtual machines that run Windows Server 2016.

You need to centrally monitor all warning events in the System logs of the virtual machines.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

◆

Resource to create in Azure:

▼
Resource Agent
Dependency Agent
Monitor Agent

Configuration to perform on the virtual machines:

▼
Virtual Machine Scale Set
Dependency Agent
Azure Monitor

Correct Answer:

Answer Area

Resource to create in Azure:

▼
Resource Agent
Dependency Agent
Monitor Agent

Configuration to perform on the virtual machines:

▼
Virtual Machine Scale Set
Dependency Agent
Azure Monitor

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Resource to create in Azure: Dependency Agent
The Map feature in Azure Monitor for VMs gets its data from the Microsoft Dependency agent. The
Dependency agent relies on the Log Analytics agent for its connection to Log Analytics. So your system must
have the Log Analytics agent installed and configured with the Dependency agent.

Whether you enable Azure Monitor for VMs for a single Azure VM or you use the at-scale deployment method,
use the Azure VM Dependency agent extension to install the agent as part of the experience.

In a hybrid environment, you can download and install the Dependency agent manually. If your VMs are hosted
outside Azure, use an automated deployment method

Configuration to perform on the virtual machines: Enable Virtual Machine Scale Set
To set up Azure Monitor for VMs:
▪ Enable a single Azure VM or virtual machine scale set by selecting Insights (preview) directly from the VM
◆ or virtual machine scale set.
▪ Enable two or more Azure VMs and virtual machine scale sets by using Azure Policy. This method ensures
  that on existing and new VMs and scale sets, the required dependencies are installed and properly
  configured. Noncompliant VMs and scale sets are reported, so you can decide whether to enable them and
  to remediate them.
▪ Enable two or more Azure VMs or virtual machine scale sets across a specified subscription or resource
  group by using PowerShell.

Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-enable-overview

QUESTION 35
You plan to run an image rendering workload in Azure. The workload uses parallel compute processes.

What is the best service to use to run the workload? More than one answer choice may achieve the goal.
Select the **BEST** answer.

A. an Azure virtual machine scale set
B. Azure Kubernetes Service (AKS)
C. Azure Batch

D. Azure Container Service

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Azure Batch works well with intrinsically parallel (also known as "embarrassingly parallel") workloads. Intrinsically parallel workloads are those where the applications can run independently, and each instance completes part of the work. When the applications are executing, they might access some common data, but they do not communicate with other instances of the application. Intrinsically parallel workloads can therefore run at a large scale, determined by the amount of compute resources available to run applications simultaneously.

Reference:
https://docs.microsoft.com/en-us/azure/batch/batch-technical-overview

QUESTION 36
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. Azure Activity Log
C. Azure Monitor action groups
D. Azure Advisor

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
The Azure Activity Log provides insight into subscription-level events that have occurred in Azure. This includes a range of data, from Azure Resource Manager operational data to updates on Service Health events.

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.

Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-audit

QUESTION 37
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are designing a storage solution to support on-premises resources and Azure-hosted resources.

You need to provide on-premises storage that has built-in replication to Azure.

Solution: You include Azure Blob storage in the design.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Azure StorSimple replicates to Azure Blob storage.

QUESTION 38
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are designing a storage solution to support on-premises resources and Azure-hosted resources.

You need to provide on-premises storage that has built-in replication to Azure.

Solution: You include Azure Data Lake Storage in the design.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 39
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are designing a storage solution to support on-premises resources and Azure-hosted resources.

You need to provide on-premises storage that has built-in replication to Azure.

Solution: You include Azure Table Storage in the design.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 40
Note: This question is a part of series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

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

You are designing a storage solution to support on-premises resources and Azure-hosted resources.

You need to provide on-premises storage that has built-in replication to Azure.

Solution: You include Azure StorSimple in the design.

Does the solution meet the goal?

A. Yes
B. No

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 41
You use Azure virtual machines to run a custom application that uses an Azure SQL Database instance on the back end.

The IT department at your company recently enabled forced tunneling.

Since the configuration change, developers have noticed degraded performance when they access the database.

You need to recommend a solution to minimize latency when accessing the database. The solution must minimize costs.

What should you include in the recommendation?

A. Azure SQL Database Managed Instance
B. virtual network service endpoints
C. Always On availability groups
D. Azure virtual machines that run Microsoft SQL Server servers

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 42
DRAG DROP

You are designing a network connectivity strategy for a new Azure subscription. You identify the following requirements:

▪ The Azure virtual machines on a subnet named Subnet1 must be accessible only from the computers in your London office.
▪ Engineers require access to the Azure virtual machine on a subnet named Subnet2 over the Internet on a specific TCP/IP management port.
▪ The Azure virtual machines in the West Europe Azure region must be able to communicate on all ports to the Azure virtual machines in the North Europe Azure region.

You need to recommend which components must be used to meet the requirements. The solution must minimize costs and administrative effort whenever possible.

What should you include in the recommendation? To answer, drag the appropriate components to the correct requirements. Each component 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:

Correct Answer:

Section: [none]
Explanation

Explanation/Reference:

QUESTION 43
You develop a new Azure Web App that uses multiple Azure blobs and static content. The Web App uses a large number of JavaScript files and cascading style sheets. Some of these files contain references to other files. Users are geographically dispersed.

You need to minimize the time to load individual pages.

What should you do?

A. Migrate the Web App to Azure Service Fabric
B. Use an Azure Content Delivery Network (CDN)
C. Implement an Azure Redis Cache
D. Create a services layer by using an Azure-hosted ASP.NET web API
E. Enable the Always On feature of the Web App

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:

QUESTION 44

You have 100 Standard_F2s_v2 Azure virtual machines. Each virtual machine has two network adapters.

You need to increase the network performance of the workloads running on the virtual machines. The solution must meet the following requirements:

- The CPU-to-memory ratio must remain the same.
- The solution must minimize costs.

What should you do?

A. Configure NIC teaming
B. Enable RDMA over InfiniBand
C. Enable SR-IOV
D. Install an additional network adapter

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Accelerated networking enables single root I/O virtualization (SR-IOV) to a VM, greatly improving its networking performance. This high-performance path bypasses the host from the datapath, reducing latency, jitter, and CPU utilization, for use with the most demanding network workloads on supported VM types.

Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-cli

QUESTION 45
You have a .NET web service named Service1 that has the following requirements:

- Must read and write temporary files to the local file system.
- Must write to the Windows Application event log.

You need to recommend a solution to host Service1 in Azure. The solution must meet the following requirements:

- Minimize maintenance overhead.
- Minimize costs.

What should you include in the recommendation?

A. an Azure virtual machine scale set
B. an Azure function
C. an App Service Environment
D. an Azure web app

Correct Answer: A
Section: [none]
Explanation

Explanation/Reference:

QUESTION 46
You have an Azure subscription that contains an Azure Blob storage account named store1.

You have an on-premises file server named Server1 that runs Windows Server 2016. Server1 stores 500 GB of company files.

You need to store a copy of the company files in store1.

Which two possible Azure services achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. an Azure Import/Export job
B. an integration account
C. an Azure Batch account
D. Azure data Factory
E. an On-premises data gateway

Correct Answer: AD
Section: [none]
Explanation

Explanation/Reference:

QUESTION 47
You have a web app named App1 that is hosted on-premises and on four Azure virtual machines. Each virtual machine is in a different region.

You need to recommend a solution to ensure that users will always connect to the closest instance of App1. The solution must prevent the users from attempting to connect to a failed instance of App1.

Which two possible recommendations achieve the goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Azure Front Door Service
B. Azure Load Balancer
C. round-robin DNS
D. Azure Traffic Manager
E. Azure Application Gateway

Correct Answer: AD
Section: [none]
Explanation

Explanation/Reference:

QUESTION 48
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:

Answer Area

Virtual machine size:

Compute optimized Standard_F8s
General purpose Standard_B8ms
High performance compute Standard_H16r
Memory optimized Standard_E16s_v3

Feature:

Receive side scaling (RSS)
Remote Direct Memory Access (RDMA)
Single root I/O virtualization (SR-IOV)
Virtual Machine Multi-Queue (VMMQ)

Correct Answer:

Answer Area

Virtual machine size:

Compute optimized Standard_F8s
General purpose Standard_B8ms
High performance compute Standard_H16r
Memory optimized Standard_E16s_v3

Feature:

Receive side scaling (RSS)
Remote Direct Memory Access (RDMA)
Single root I/O virtualization (SR-IOV)
Virtual Machine Multi-Queue (VMMQ)

Section: [none]
Explanation

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

QUESTION 49
You are designing a microservices architecture that will support a web application.

The solution must meet the following requirements:

- Allow independent upgrades to each microservice
- Deploy the solution on-premises and to Azure
- Set policies for performing automatic repairs to the microservices
- Support low-latency and hyper-scale operations

You need to recommend a technology.

What should you recommend?

A. Azure Service Fabric
B. Azure Container Service
C. Azure Container Instance
D. Azure Virtual Machine Scale Set

Correct Answer: A
Section: [none]
Explanation

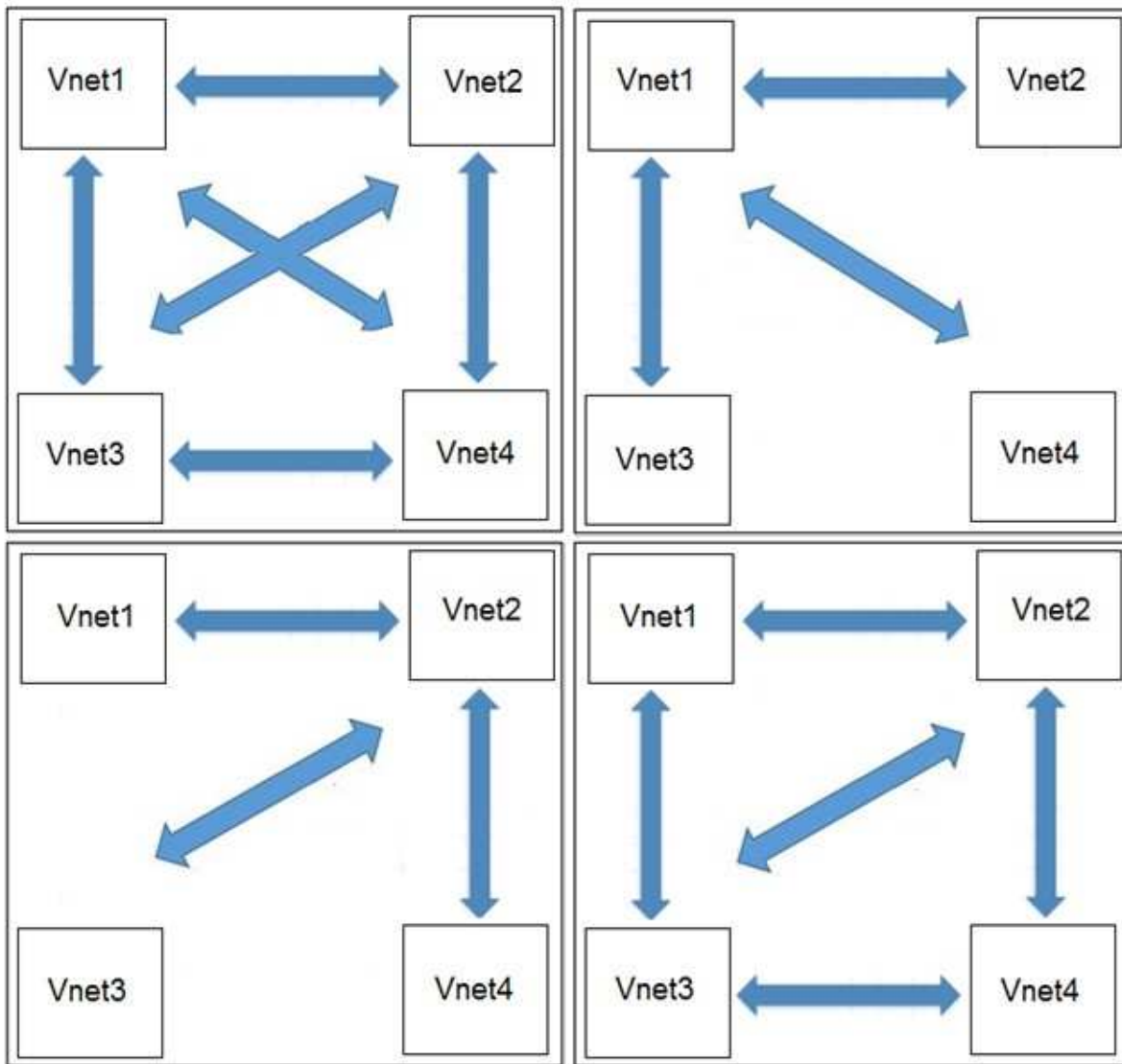**Explanation/Reference:**

QUESTION 50
HOTSPOT

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

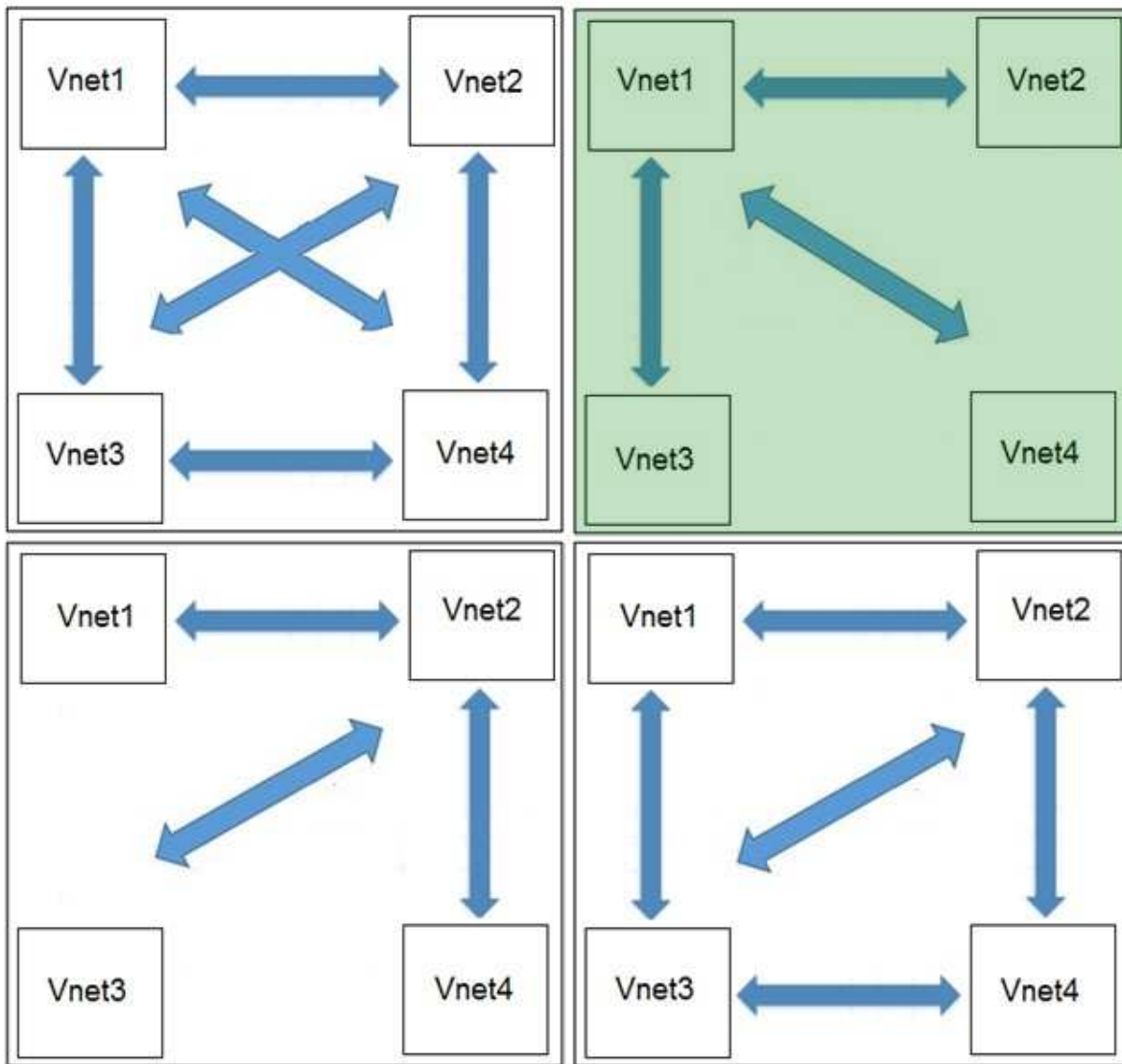| Virtual network name	Subscription name	Virtual network type
Vnet1	Subscription1	Classic mode
Vnet2	Subscription1	Resource Manager
Vnet3	Subscription1	Resource Manager
Vnet4	Subscription2	Resource Manager

You need to recommend a virtual network peering solution to ensure that the resources connected to any other virtual network. The solution must minimize administrative effort. Which virtual network peering topology should you recommend? To answer, select the appropriate topology in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Correct Answer:

◆

Section: [none]
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-connect-different-deployment-models-portal

QUESTION 51
You are designing a solution for a company to deploy software for testing and production.

The solution must meet the following requirements:

- Applications must be deployed to several different environments and must run without installation of dependencies.
- Existing published application must be ported to the new solution.
- Application developers must be given flexibility when architecting their code.

You need to recommend a solution for hosting applications.

What should you select?

A. Azure worker role
B. Azure Kubernetes Service
C. Azure Functions
D. Azure Batch

Correct Answer: B
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Kubernetes is open-source orchestration software for deploying, managing, and scaling containers. The fully managed Azure Kubernetes Service (AKS) makes deploying and managing containerized applications easy. It offers serverless Kubernetes.

Reference:
https://azure.microsoft.com/en-us/services/kubernetes-service/

QUESTION 52
You have 100 Standard_F2s_v2 Azure virtual machines. Each virtual machine has two network adapters.

You need to increase the network performance of the workloads running on the virtual machines. The solution must meet the following requirements:

▪ The CPU-to-memory ratio must remain the same.
▪ The solution must minimize costs.

What should you do?

A. Configure NIC teaming
B. Enable RDMA over InfiniBand
C. Enable Accelerated Networking.
D. Install an additional network adapter

Correct Answer: C
Section: [none]
Explanation

Explanation/Reference:
Explanation:
Accelerated networking enables single root I/O virtualization (SR-IOV) to a VM, greatly improving its networking performance. This high-performance path bypasses the host from the datapath, reducing latency, jitter, and CPU utilization, for use with the most demanding network workloads on supported VM types.
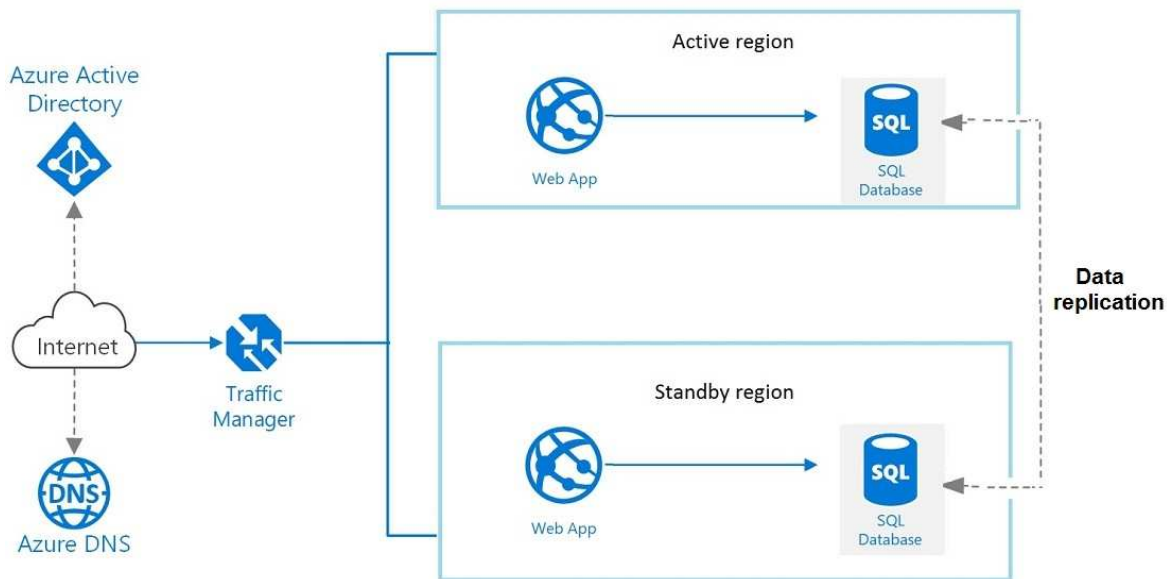
Reference:
https://docs.microsoft.com/en-us/azure/virtual-network/create-vm-accelerated-networking-cli

QUESTION 53
HOTSPOT

You have the application architecture shown in the following exhibit.

Use the drop-down menus to select 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 change the front end to an ative/active architecture in which both regions process incoming connections, you must **[answer choice]**.

add a load balancer to each region
add an Azure Application Gateway to each region
add an Azure content delivery network (CDN)
modify the Azure Traffic Manager routing method

To control the threshold for failing over the front end to the standby region, you must configure the **[answer choice]**.

an Application Insights availability test
Azure SQL Database failover groups
Connection Monitor in Azure Network Watcher
Endpoint monitor settings in Azure Traffic Manager

Correct Answer:

Answer Area

To change the front end to an ative/active
architecture in which both regions process
incoming connections, you must **[answer
choice]**.

▼
add a load balancer to each region
add an Azure Application Gateway to each region
add an Azure content delivery network (CDN)
modify the Azure Traffic Manager routing method

To control the threshold for failing over the
front end to the standby region, you must
configure the **[answer choice]**.

▼
an Application Insights availability test
Azure SQL Database failover groups
Connection Monitor in Azure Network Watcher
Endpoint monitor settings in Azure Traffic Manager

Section: [none]
Explanation

Explanation/Reference:
Explanation:

Box 1: Modify the Azure Traffic Manager routing
Azure Traffic Manager supports six traffic-routing methods to determine how to route network traffic to the
various service endpoints.

Box 2: Endpoint monitor settings in the Azure Traffic Manager
Azure Traffic Manager includes built-in endpoint monitoring and automatic endpoint failover. This feature helps
you deliver high-availability applications that are resilient to endpoint failure, including Azure region failures.

To configure endpoint monitoring, you must specify the following settings on your Traffic Manager profile:
Protocol, Port, Path, custom header settings, etc.

Reference:
https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-routing-methods

https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-monitoring

QUESTION 54
HOTSPOT

You are designing a solution for a stateless front-end application named Application1. Application1 will be
hosted on two Azure virtual machines named VM1 and VM2.

You plan to load balance connections to VM1 and VM2 from the Internet by using one Azure load balancer.

You need to recommend the minimum number of required public IP addresses.

How many public IP addresses should you recommend using for each resource? To answer, select the
appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Load balancer:

▼
0
1
2
3

VM1:

▼
0
1
2
3

VM2:

▼
0
1
2
3

Correct Answer:

◆

Answer Area

Load balancer:

0
1
2
3

VM1:

0
1
2
3

VM2:

0
1
2
3

Section: [none]
Explanation

Explanation/Reference: