



CertyIQ

Premium exam material

Get certification quickly with the CertyIQ Premium exam material.
Everything you need to prepare, learn & pass your certification exam easily. Lifetime free updates
First attempt guaranteed success.

<https://www.CertyIQ.com>



CompTIA

About CertyIQ

We here at CertyIQ eventually got enough of the industry's greedy exam paid for. Our team of IT professionals comes with years of experience in the IT industry Prior to training CertyIQ we worked in test areas where we observed the horrors of the paywall exam preparation system.

The misuse of the preparation system has left our team disillusioned. And for that reason, we decided it was time to make a difference. We had to make In this way, CertyIQ was created to provide quality materials without stealing from everyday people who are trying to make a living.

Doubt Support

We have developed a very scalable solution using which we are able to solve 400+ doubts every single day with an average rating of 4.8 out of 5.

<https://www.certyiq.com>

Mail us on - certyiqofficial@gmail.com



Lifetime Free Updates

We provide lifetime free updates to our customers. To make life easier for our valued customers and fulfill their needs



Free Exam PDF

You are sure to pass the exam completely free of charge



Money Back Guarantee

We Provide 100% money back guarantee to our customer in case of any failure

John

October 19, 2022



Thanks you so much for your help. I scored 972 in my exam today. More than 90% were from your PDFs!

October 22, 2022



Passed my exam today with 891 marks. Out of 52 questions, 51 were from certyiq PDFs including Contoso case study. Thank You certyiq team!

Dana

September 04, 2022



Thanks a lot for this updated AZ-900 Q&A. I just passed my exam and got 974, I followed both of your Az-900 videos and the 6 PDF, the PDFs are very much valid, all answers are correct. Could you please create a similar video/PDF for DP900, your content/PDF's is really awesome. The team did a really good job. Thank You 😊.

Henry Rome

2 months ago



These questions are real and 100 % valid. Thank you so much for your efforts, also your 4 PDFs are awesome, I passed the DP900 exam on 1 Sept. With 968 marks. Thanks a lot, buddy!

Esmaria

2 months ago



Simple easy to understand explanations. To anyone out there wanting to write AZ900, I highly recommend 6 PDF's. Thank you so much, appreciate all your hard work in having such great content. Passed my exam Today - 3 September with 942 score.

Ahamed Shibly

2 months ago



Customer support is realy fast and helpful, I just finished my exam and this video along with the 6 PDF helped me pass! Definitely recommend getting the PDFs. Thank you!



(AZ-305)

Designing Microsoft Azure Infrastructure Solutions

Total: **228 Questions**

Link: <https://certyiq.com/papers?provider=microsoft&exam=az-305>

Question: 1

CertyIQ

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

Answer: A**Explanation:**

In Azure Active Directory (Azure AD), create an access review of Application1.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-user-access-with-access-reviews>

Question: 2

CertyIQ

You have an Azure subscription. The subscription has a blob container that contains multiple blobs. Ten users in the finance department of your company plan to access the blobs during the month of April. You need to recommend a solution to enable access to the blobs during the month of April only. Which security solution should you include in the recommendation?

- A. shared access signatures (SAS)
- B. Conditional Access policies
- C. certificates
- D. access keys

Answer: A**Explanation:**

Shared Access Signatures (SAS) allows for limited-time fine grained access control to resources. So you can generate URL, specify duration (for month of April) and disseminate URL to 10 team members. On May 1, the SAS token is automatically invalidated, denying team members continued access.

Reference:

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

Question: 3

CertyIQ

You have an Azure Active Directory (Azure AD) tenant that syncs with an on-premises Active Directory domain. You have an internal web app named WebApp1 that is hosted on-premises. WebApp1 uses Integrated Windows authentication. Some users work remotely and do NOT have VPN access to the on-premises network. You need to provide the remote users with single sign-on (SSO) access to WebApp1. Which two features should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Azure AD Application Proxy
- B. Azure AD Privileged Identity Management (PIM)
- C. Conditional Access policies
- D. Azure Arc
- E. Azure AD enterprise applications
- F. Azure Application Gateway

Answer: AE

Explanation:

A: Application Proxy is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud, and the Application Proxy connector which runs on an on-premises server.

You can configure single sign-on to an Application Proxy application.

E: Add an on-premises app to Azure AD

Now that you've prepared your environment and installed a connector, you're ready to add on-premises applications to Azure AD.

1. Sign in as an administrator in the Azure portal.
2. In the left navigation panel, select Azure Active Directory.
3. Select Enterprise applications, and then select New application.
4. Select Add an on-premises application button which appears about halfway down the page in the On-premises applications section. Alternatively, you can select Create your own application at the top of the page and then select Configure Application Proxy for secure remote access to an on-premise application.
5. In the Add your own on-premises application section, provide the following information about your application.
6. Etc.

Incorrect:

Not C: Conditional Access policies are not required.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application>

Question: 4

CertyIQ

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has a security group named Group1. Group1 is configured for assigned membership. Group1 has 50 members, including 20 guest users.

You need to recommend a solution for evaluating the membership of Group1. The solution must meet the following requirements:

- ⇒ The evaluation must be repeated automatically every three months.
- ⇒ Every member must be able to report whether they need to be in Group1.
- ⇒ Users who report that they do not need to be in Group1 must be removed from Group1 automatically.
- ⇒ Users who do not report whether they need to be in Group1 must be removed from Group1 automatically.

What should you include in the recommendation?

- A. Implement Azure AD Identity Protection.
- B. Change the Membership type of Group1 to Dynamic User.
- C. Create an access review.**
- D. Implement Azure AD Privileged Identity Management (PIM).

Answer: C

Explanation:

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

Reference:

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

Question: 5

CertyIQ

HOTSPOT -

You plan to deploy Azure Databricks to support a machine learning application. Data engineers will mount an Azure Data Lake Storage account to the Databricks file system. Permissions to folders are granted directly to the data engineers.

You need to recommend a design for the planned Databrick deployment. The solution must meet the following requirements:

- ⇒ Ensure that the data engineers can only access folders to which they have permissions.
- ⇒ Minimize development effort.
- ⇒ 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

Databricks SKU:

Premium	
Standard	

Cluster configuration:

Credential passthrough	
Managed identities	
MLflow	
A runtime that contains Photon	
Secret scope	

Answer:

Answer Area

Databricks SKU:

Premium
Standard

Cluster configuration:

Credential passthrough
Managed identities
MLflow
A runtime that contains Photon
Secret scope

Explanation:

Box 1: Premium -

Premium Databricks SKU is required for credential passthrough.

Box 2: Credential passthrough -

Authenticate automatically to Azure Data Lake Storage Gen1 (ADLS Gen1) and Azure Data Lake Storage Gen2 (ADLS Gen2) from Azure Databricks clusters using the same Azure Active Directory (Azure AD) identity that you use to log into Azure Databricks. When you enable Azure Data Lake Storage credential passthrough for your cluster, commands that you run on that cluster can read and write data in Azure Data Lake Storage without requiring you to configure service principal credentials for access to storage.

Reference:

<https://docs.microsoft.com/en-us/azure/databricks/security/credential-passthrough/adls-passthrough>

Question: 6

CertyIQ

HOTSPOT -

You plan to deploy an Azure web app named App1 that will use Azure Active Directory (Azure AD) authentication. App1 will be accessed from the internet by the users at your company. All the users have computers that run Windows 10 and are joined to Azure AD.

You need to recommend a solution to ensure that the users can connect to App1 without being prompted for authentication and can access App1 only from company-owned computers.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

The users can connect to App1 without being prompted for authentication:

	▼
An Azure AD app registration	▼
An Azure AD managed identity	▼
Azure AD Application Proxy	▼

The users can access App1 only from company-owned computers:

	▼
A Conditional Access policy	▼
An Azure AD administrative unit	▼
Azure Application Gateway	▼
Azure Blueprints	▼
Azure Policy	▼

Answer:

Answer Area

The users can connect to App1 without being prompted for authentication:

	▼
An Azure AD app registration	▼
An Azure AD managed identity	▼
Azure AD Application Proxy	▼

The users can access App1 only from company-owned computers:

	▼
A Conditional Access policy	▼
An Azure AD administrative unit	▼
Azure Application Gateway	▼
Azure Blueprints	▼
Azure Policy	▼

Explanation:

Box 1: An Azure AD app registration

Azure active directory (AD) provides cloud based directory and identity management services. You can use Azure AD to manage users of your application and authenticate access to your applications using Azure Active Directory.

You register your application with Azure Active Directory tenant.

Box 2: A conditional access policy

Conditional Access policies at their simplest are if-then statements, if a user wants to access a resource, then they must complete an action.

By using Conditional Access policies, you can apply the right access controls when needed to keep your organization secure and stay out of your user's way when not needed.

Reference:

Question: 7

CertyIQ

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

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

Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.

Several virtual machines exhibit network connectivity issues.

You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.

Solution: Use Azure Traffic Analytics in Azure Network Watcher to analyze the network traffic.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

(Traffic Analytics) under (Network Watcher) gives you statistical data and traffic visualization like total inbound and outbound flows and the number of deployed NSGs. However, it doesn't give you information if packets are allowed or denied. Check screenshot in the following reference: <https://docs.microsoft.com/en-us/azure/network-watcher/traffic-analytics>

(IP Flow Verify) under (Network Watcher) gives you option to verify if traffic is allowed or denied. Check screenshot in the following reference: <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview>

Correct answer is B.

Question: 8

CertyIQ

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

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

Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.

Several virtual machines exhibit network connectivity issues.

You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.

Solution: Use Azure Advisor to analyze the network traffic.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead use Azure Network Watcher IP Flow Verify, which allows you to detect traffic filtering issues at a VM level.

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.

Reference:

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

Question: 9

CertyIQ

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

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

Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.

Several virtual machines exhibit network connectivity issues.

You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.

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

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Azure Network Watcher IP Flow Verify allows you to detect traffic filtering issues at a VM level.

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.

Reference:

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

Question: 10

CertyIQ

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 Monitor to design an alerting strategy for security-related events.

Which Azure Monitor Logs tables should you query? To answer, drag the appropriate tables to the correct log types. Each table 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

Answer:

Tables

AzureActivity

AzureDiagnostics

Event

Syslog

Answer Area

Events from Windows event logs:

Event

Events from Linux system logging:

Syslog

Explanation:

Windows : Event.

Linux : Syslog

Reference:

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

<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/data-sources-syslog>

Question: 11

CertyIQ

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

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

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

NOTE: Each correct selection is worth one point.

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

Answer: CEF

Explanation:

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules.

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

Reference:

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

Question: 12

CertyIQ

DRAG DROP -

Your on-premises network contains a server named Server1 that runs an ASP.NET application named App1.

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

You need to recommend a solution to ensure that users sign in by using their Azure AD account and Azure Multi-Factor Authentication (MFA) when they connect to App1 from the internet.

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

Select and Place:

Features

Answer Area

a public Azure Load Balancer

a managed identity

an internal Azure Load Balancer

a Conditional Access policy

an Azure App Service plan

Azure AD Application Proxy

an Azure AD enterprise application



Answer:

Features

a public Azure Load Balancer

a managed identity

an internal Azure Load Balancer

an Azure App Service plan

Answer Area

Azure AD Application Proxy

an Azure AD enterprise application

a Conditional Access policy



Explanation:

Step 1: Azure AD Application Proxy

Start by enabling communication to Azure data centers to prepare your environment for Azure AD Application Proxy.

Step 2: an Azure AD enterprise application

Add an on-premises app to Azure AD.

Now that you've prepared your environment and installed a connector, you're ready to add on-premises applications to Azure AD.

1. Sign in as an administrator in the Azure portal.
2. In the left navigation panel, select Azure Active Directory.
3. Select Enterprise applications, and then select New application.
4. Etc.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application>

Question: 13

CertyIQ

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

What should you include in the recommendation?

- A. Azure Activity Log
- B. Azure Advisor
- C. Azure Analysis Services

D. Azure Monitor action groups

Answer: A

Explanation:

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

Through activity logs, you can determine:

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

Reference:

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

CertyIQ

Question: 14

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

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

Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.

Several virtual machines exhibit network connectivity issues.

You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.

Solution: Install and configure the Azure Monitoring agent and the Dependency Agent on all the virtual machines. Use VM insights in Azure Monitor to analyze the network traffic.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Use the Azure Monitor agent if you need to:

Collect guest logs and metrics from any machine in Azure, in other clouds, or on-premises.

Use the Dependency agent if you need to:

Use the Map feature VM insights or the Service Map solution.

Note: Instead use Azure Network Watcher IP Flow Verify allows you to detect traffic filtering issues at a VM level.

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.

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview> <https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#dependency-agent>

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.

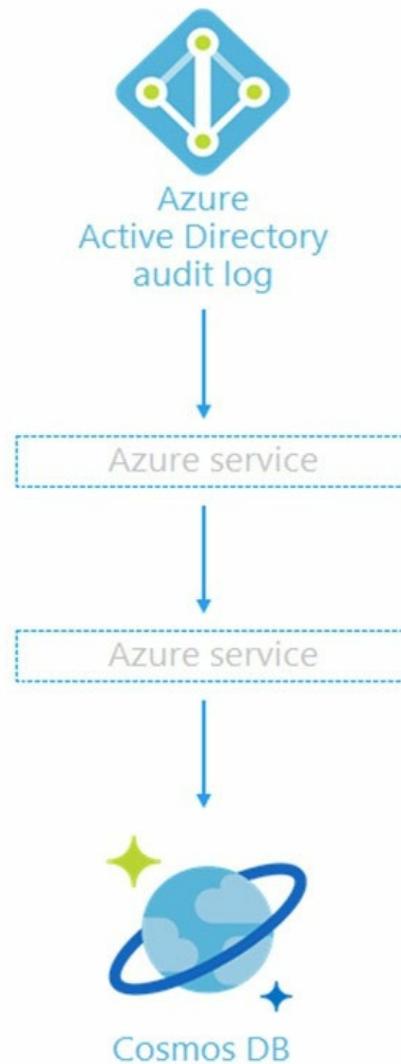
Which services should you include in the design? To answer, drag the appropriate services to the correct targets. Each service may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

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

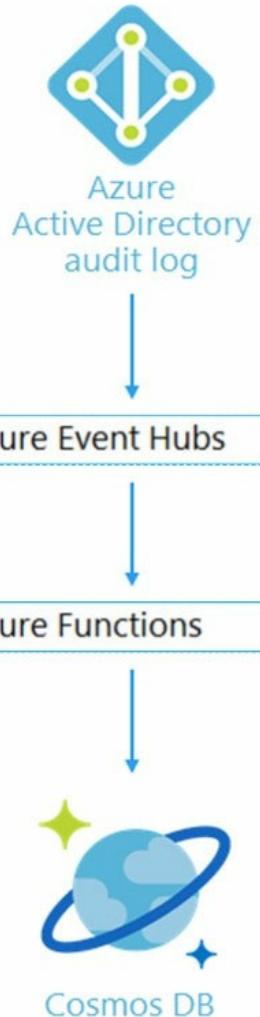
Answer Area

Answer:

Azure Services

- Azure Event Grid
- Azure Event Hubs
- Azure Functions
- Azure Monitor Logs
- Azure Notification Hubs

Answer Area



Explanation:

Box 1: Azure Event Hubs -

You can route Azure Active Directory (Azure AD) activity logs to several endpoints for long term retention and data insights.

The Event Hub is used for streaming.

Box 2: Azure Function -

Use an Azure Function along with a cosmos DB change feed, and store the data in Cosmos DB.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-activity-logs-azure-monitor>

Question: 16

CertyIQ

Your company, named Contoso, Ltd., implements several Azure logic apps that have HTTP triggers. The logic apps provide access to an on-premises web service.

Contoso establishes a partnership with another company named Fabrikam, Inc.

Fabrikam does not have an existing Azure Active Directory (Azure AD) tenant and uses third-party OAuth 2.0 identity management to authenticate its users.

Developers at Fabrikam plan to use a subset of the logic apps to build applications that will integrate with the on-premises web service of Contoso.

You need to design a solution to provide the Fabrikam developers with access to the logic apps. The solution must meet the following requirements:

- ⇒ Requests to the logic apps from the developers must be limited to lower rates than the requests from the users at Contoso.

- ⇒ The developers must be able to rely on their existing OAuth 2.0 provider to gain access to the logic apps.
- ⇒ The solution must NOT require changes to the logic apps.
- ⇒ The solution must NOT use Azure AD guest accounts.

What should you include in the solution?

- A. Azure Front Door
- B. Azure AD Application Proxy
- C. Azure AD business-to-business (B2B)
- D. Azure API Management

Answer: D

Explanation:

Many APIs support OAuth 2.0 to secure the API and ensure that only valid users have access, and they can only access resources to which they're entitled. To use Azure API Management's interactive developer console with such APIs, the service allows you to configure your service instance to work with your OAuth 2.0 enabled API.

Incorrect:

Azure AD business-to-business (B2B) uses guest accounts.

Azure AD Application Proxy is for on-premises scenarios.

Reference:

<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-oauth2>

Question: 17

CertyIQ

HOTSPOT -

You have an Azure subscription that contains 300 virtual machines that run Windows Server 2019.

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

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

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 Azure Monitor agent
- Modify the membership of the Event Log Readers group

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 Azure Monitor agent
Modify the membership of the Event Log Readers group

Explanation:

Box 1: A Log Analytics workspace

Send resource logs to a Log Analytics workspace to enable the features of Azure Monitor Logs.

You must create a diagnostic setting for each Azure resource to send its resource logs to a Log Analytics workspace to use with Azure Monitor Logs.

Box 2: Install the Azure Monitor agent

Use the Azure Monitor agent if you need to:

Collect guest logs and metrics from any machine in Azure, in other clouds, or on-premises.

Manage data collection configuration centrally

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/resource-logs> <https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview#azure-monitor-agent>

Question: 18

CertyIQ

HOTSPOT -

You have several Azure App Service web apps that use Azure Key Vault to store data encryption keys.

Several departments have the following requests to support the web app:

Department	Request
Security	<ul style="list-style-type: none">Review the membership of administrative roles and require users 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	<ul style="list-style-type: none">Enable the applications to access Key Vault and retrieve keys for use in code.
Quality Assurance	<ul style="list-style-type: none">Receive temporary administrator access to create and configure additional web apps in the test environment.

Which service should you recommend for each department's request? To answer, configure the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Security:

Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Development:

Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Quality Assurance:

Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Answer:

Answer Area

Security:

Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Development:

Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Quality Assurance:

Azure AD Privileged Identity Management
Azure Managed Identity
Azure AD Connect
Azure AD Identity Protection

Explanation:

Box 1: Azure AD Privileged Identity Management

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Azure AD and Azure resources

- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce multi-factor authentication to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need roles
- Download audit history for internal or external audit
- Prevents removal of the last active Global Administrator role assignment

Box 2: Azure Managed Identity -

Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication.

Applications may use the managed identity to obtain Azure AD tokens. With Azure Key Vault, developers can use managed identities to access resources. Key

Vault stores credentials in a secure manner and gives access to storage accounts.

Box 3: Azure AD Privileged Identity Management

Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Azure AD and Azure resources

Assign time-bound access to resources using start and end dates

Reference:

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

Question: 19

CertyIQ

HOTSPOT -

Your company has the divisions shown in the following table.

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

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

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Management groups:

▼
1
2
3
4

Blueprint definitions:

▼
1
2
3
4

Blueprint assignments:

▼
1
2
3
4

Answer:

Answer Area

Management groups:

1
2
3
4

Blueprint definitions:

1
2
3
4

Blueprint assignments:

1
2
3
4

Explanation:

Management groups can't span AAD tenant, so you need 2 management groups.

Blueprints definition can be saved within management group which, in turn, means you need 2 blueprint definitions.

Blueprint assignments are at subscription level, therefore you need 4.

Question: 20

CertyIQ

HOTSPOT -

You need to design an Azure policy that will implement the following functionality:

- ⇒ For new resources, assign tags and values that match the tags and values of the resource group to which the resources are deployed.
 - ⇒ For existing resources, identify whether the tags and values match the tags and values of the resource group that contains the resources.
 - ⇒ For any non-compliant resources, trigger auto-generated remediation tasks to create missing tags and values.
- The solution must use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Azure Policy effect to use:

Append
EnforceOPAConstraint
EnforceRegoPolicy
Modify

Azure Active Directory (Azure AD) object and role-based access control (RBAC) role to use for the remediation tasks:

A managed identity with the Contributor role
A managed identity with the User Access Administrator role
A service principal with the Contributor role
A service principal with the User Access Administrator role

Answer:

Answer Area

Azure Policy effect to use:

Append
EnforceOPAConstraint
EnforceRegoPolicy
Modify

Azure Active Directory (Azure AD) object and role-based access control (RBAC) role to use for the remediation tasks:

A managed identity with the Contributor role
A managed identity with the User Access Administrator role
A service principal with the Contributor role
A service principal with the User Access Administrator role

Explanation:

Box 1: Modify -

Modify is used to add, update, or remove properties or tags on a subscription or resource during creation or update. A common example is updating tags on resources such as costCenter. Existing non-compliant resources can be remediated with a remediation task. A single Modify rule can have any number of operations. Policy assignments with effect set as Modify require a managed identity to do remediation.

Incorrect:

* The following effects are deprecated: EnforceOPAConstraint EnforceRegoPolicy

* Append is used to add additional fields to the requested resource during creation or update. A common example is specifying allowed IPs for a storage resource.

Append is intended for use with non-tag properties. While Append can add tags to a resource during a create or update request, it's recommended to use the

Modify effect for tags instead.

Box 2: A managed identity with the Contributor role

The managed identity needs to be granted the appropriate roles required for remediating resources to grant the managed identity.

Contributor - Can create and manage all types of Azure resources but can't grant access to others.

Incorrect:

User Access Administrator: lets you manage user access to Azure resources.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects> <https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

Question: 21

HOTSPOT -

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

CertyIQ

Name	Type	Account Kind	Location
storage1	Azure Storage account	Storage (general purpose v1)	East US
storage2	Azure Storage account	StorageV2 (general purpose v2)	East US
Workspace1	Azure Log Analytics workspace	Not applicable	East US
Workspace2	Azure Log Analytics workspace	Not applicable	East US
Hub1	Azure event hub	Not applicable	East US

You create an Azure SQL database named DB1 that is hosted in the East US Azure region.

To DB1, you add a diagnostic setting named Settings1. Settings1 archive SQLInsights to storage1 and sends SQLInsights to Workspace1.

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

Hot Area:

Answer Area

Statements	Yes	No
You can add a new diagnostic setting that archives SQLInsights logs to storage2.	<input type="radio"/>	<input type="radio"/>
You can add a new diagnostic setting that sends SQLInsights logs to Workspace2.	<input type="radio"/>	<input type="radio"/>
You can add a new diagnostic setting that sends SQLInsights logs to Hub1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can add a new diagnostic setting that archives SQLInsights logs to storage2.	<input checked="" type="radio"/>	<input type="radio"/>
You can add a new diagnostic setting that sends SQLInsights logs to Workspace2.	<input checked="" type="radio"/>	<input type="radio"/>
You can add a new diagnostic setting that sends SQLInsights logs to Hub1.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

Box 1: Yes -

A single diagnostic setting can define no more than one of each of the destinations. If you want to send data to more than one of a particular destination type (for example, two different Log Analytics workspaces), then create multiple settings.

Each resource can have up to 5 diagnostic settings.

Note: This diagnostic telemetry can be streamed to one of the following Azure resources for analysis.

* Log Analytics workspace

* Azure Event Hubs

* Azure Storage

Box 2: Yes -

Box 3: Yes -

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/diagnostic-settings> <https://docs.microsoft.com/en-us/azure/azure-sql/database/metrics-diagnostic-telemetry-logging-streaming-export-configure?tabs=azure-portal>

CertyIQ

Question: 22

You plan to deploy an Azure SQL database that will store Personally Identifiable Information (PII).

You need to ensure that only privileged users can view the PII.

What should you include in the solution?

- A. dynamic data masking
- B. role-based access control (RBAC)
- C. Data Discovery & Classification
- D. Transparent Data Encryption (TDE)

Answer: A

Explanation:

Dynamic data masking limits sensitive data exposure by masking it to non-privileged users.

Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal impact on the application layer. It's a policy-based security feature that hides the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview>

CertyIQ

Question: 23

You plan to deploy an app that will use an Azure Storage account.

You need to deploy the storage account. The storage account must meet the following requirements:

- ⇒ Store the data for multiple users.
- ⇒ Encrypt each user's data by using a separate key.
- ⇒ Encrypt all the data in the storage account by using customer-managed keys.

What should you deploy?

- A. files in a premium file share storage account
- B. blobs in a general purpose v2 storage account
- C. blobs in an Azure Data Lake Storage Gen2 account
- D. files in a general purpose v2 storage account

Answer: B

Explanation:

You can specify a customer-provided key on Blob storage operations. A client making a read or write request

against Blob storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.

Reference:

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

Question: 24

CertyIQ

HOTSPOT -

You have an Azure App Service web app that uses a system-assigned managed identity.

You need to recommend a solution to store the settings of the web app as secrets in an Azure key vault. The solution must meet the following requirements:

- ⇒ Minimize changes to the app code.
- ⇒ Use the principle of least privilege.

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

Key Vault integration method:

Key Vault references in Application settings
Key Vault references in Appsettings.json
Key Vault references in Web.config
Key Vault SDK

Key Vault permissions for the managed identity:

Keys: Get
Keys: List and Get
Secrets: Get
Secrets: List and Get

Answer:

Answer Area

Key Vault integration method:

Key Vault references in Application settings
Key Vault references in Appsettings.json
Key Vault references in Web.config
Key Vault SDK

Key Vault permissions for the managed identity:

Keys: Get
Keys: List and Get
Secrets: Get
Secrets: List and Get

Explanation:

Box 1: Key Vault references in Application settings

Source Application Settings from Key Vault.

Key Vault references can be used as values for Application Settings, allowing you to keep secrets in Key Vault instead of the site config. Application Settings are securely encrypted at rest, but if you need secret management capabilities, they should go into Key Vault.

To use a Key Vault reference for an app setting, set the reference as the value of the setting. Your app can

reference the secret through its key as normal. No code changes are required.

Box 2: Secrets: Get -

In order to read secrets from Key Vault, you need to have a vault created and give your app permission to access it.

1. Create a key vault by following the Key Vault quickstart.
2. Create a managed identity for your application.
3. Key Vault references will use the app's system assigned identity by default, but you can specify a user-assigned identity.
4. Create an access policy in Key Vault for the application identity you created earlier. Enable the "Get" secret permission on this policy.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references> <https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references>

CertyIQ

Question: 25

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

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

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

Which type of identity should you include in the recommendation?

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

Answer: D

Explanation:

Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication.

A user-assigned managed identity:

Can be shared.

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

Common usage:

Workloads that run on multiple resources and can share a single identity.

For example, a workload where multiple virtual machines need to access the same resource.

Incorrect:

Not A: A system-assigned managed identity can't be shared. It can only be associated with a single Azure resource.

Typical usage:

Workloads that are contained within a single Azure resource.

Workloads for which you need independent identities.

For example, an application that runs on a single virtual machine.

Reference:

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

Question: 26

CertyIQ

You have the resources shown in the following table:

Name	Type
AS1	Azure Synapse Analytics instance
CDB1	Azure Cosmos DB SQL API account

CDB1 hosts a container that stores continuously updated operational data.

You are designing a solution that will use AS1 to analyze the operational data daily.

You need to recommend a solution to analyze the data without affecting the performance of the operational data store.

What should you include in the recommendation?

- A. Azure Cosmos DB change feed
- B. Azure Data Factory with Azure Cosmos DB and Azure Synapse Analytics connectors
- C. Azure Synapse Link for Azure Cosmos DB**
- D. Azure Synapse Analytics with PolyBase data loading

Answer: C**Explanation:**

Azure Synapse Link for Azure Cosmos DB creates a tight integration between Azure Cosmos DB and Azure Synapse Analytics. It enables customers to run near real-time analytics over their operational data with full performance isolation from their transactional workloads and without an ETL pipeline.

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/synapse-link-frequently-asked-questions>

Question: 27

CertyIQ

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 setting

Save Discard Delete Provide feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name

Diagnostic1

Category details

Destination details

log

Send to Log Analytics

SQLInsights

Retention (days)

90 ✓

AutomaticTuning

Retention (days)

30 ✓

QueryStoreRuntimeStatistics

Retention (days)

0

QueryStoreWaitStatistics

Retention (days)

0

Errors

Retention (days)

0

DatabaseWaitStatistics

Retention (days)

0

Timeouts

Retention (days)

0

Blocks

Retention (days)

0

Deadlocks

Retention (days)

0

metric

Stream to an event hub

Basic

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

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

Explanation:

Box 1: 90 days -

As per exhibit.

Box 2: 730 days -

How long is the data kept?

Raw data points (that is, items that you can query in Analytics and inspect in Search) are kept for up to 730 days.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/data-retention-privacy>

CertyIQ

Question: 28

You have an application that is used by 6,000 users to validate their vacation requests. The application manages its own credential store.

Users must enter a username and password to access the application. The application does NOT support identity providers.

You plan to upgrade the application to use single sign-on (SSO) authentication by using an Azure Active Directory (Azure AD) application registration.

Which SSO method should you use?

- A. header-based
- B. SAML
- C. password-based**
- D. OpenID Connect

Answer: C

Explanation:

Password - On-premises applications can use a password-based method for SSO. This choice works when applications are configured for Application Proxy.

With password-based SSO, users sign in to the application with a username and password the first time they access it. After the first sign-on, Azure AD provides the username and password to the application. Password-based SSO enables secure application password storage and replay using a web browser extension or mobile app. This option uses the existing sign-in process provided by the application, enables an administrator to manage the passwords, and doesn't require the user to know the password.

Incorrect:

Choosing an SSO method depends on how the application is configured for authentication. Cloud applications can use federation-based options, such as OpenID Connect, OAuth, and SAML.

Federation - When you set up SSO to work between multiple identity providers, it's called federation.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on>

CertyIQ

Question: 29

HOTSPOT -

You have an Azure subscription that contains a virtual network named VNET1 and 10 virtual machines. The virtual machines are connected to VNET1.

You need to design a solution to manage the virtual machines from the internet. The solution must meet the following requirements:

- ⇒ Incoming connections to the virtual machines must be authenticated by using Azure Multi-Factor Authentication (MFA) before network connectivity is allowed.
- ⇒ Incoming connections must use TLS and connect to TCP port 443.
- ⇒ The solution must support RDP and SSH.

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

To provide access to virtual machines on VNET1, use:

- Azure Bastion
- Just-in-time (JIT) VM access
- Azure Web Application Firewall (WAF) in Azure Front Door

To enforce Azure MFA, use:

- An Azure Identity Governance access package
- A Conditional Access policy that has the Cloud apps assignment set to Azure Windows VM Sign-In
- A Conditional Access policy that has the Cloud apps assignment set to Microsoft Azure Management

Answer:

Answer Area

To provide access to virtual machines on VNET1, use:

- Azure Bastion
- Just-in-time (JIT) VM access
- Azure Web Application Firewall (WAF) in Azure Front Door

To enforce Azure MFA, use:

- An Azure Identity Governance access package
- A Conditional Access policy that has the Cloud apps assignment set to Azure Windows VM Sign-In
- A Conditional Access policy that has the Cloud apps assignment set to Microsoft Azure Management

Explanation:

Box 1: Azure bastion

It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS.

While JIT access allows access via RDP or SSH, incoming connections are not TLS TCP 443 (but RDP or SSH when the inbound port is temporarily authorized)

Box 2: A conditional Access policy that has Cloud Apps assignment set to Azure Windows VM Sign-In

You can enforce Conditional Access policies such as multi-factor authentication or user sign-in risk check before authorizing access to Windows VMs in Azure that are enabled with Azure AD sign in. To apply Conditional Access policy, you must select the "Azure Windows VM Sign-In" app from the cloud apps or actions assignment option and then use Sign-in risk as a condition and/or require multi-factor authentication as a grant access control.

Reference:

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

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage?tabs=jit-config-avm%2Cjit-request-asc>

Question: 30

CertyIQ

You are designing an Azure governance solution.

All Azure resources must be easily identifiable based on the following operational information: environment, owner, department and cost center.

You need to ensure that you can use the operational information when you generate reports for the Azure resources.

What should you include in the solution?

- A. an Azure data catalog that uses the Azure REST API as a data source
- B. an Azure management group that uses parent groups to create a hierarchy
- C. an Azure policy that enforces tagging rules**
- D. Azure Active Directory (Azure AD) administrative units

Answer: C

Explanation:

You apply tags to your Azure resources, resource groups, and subscriptions to logically organize them into a taxonomy. Each tag consists of a name and a value pair.

You use Azure Policy to enforce tagging rules and conventions. By creating a policy, you avoid the scenario of resources being deployed to your subscription that don't have the expected tags for your organization.

Instead of manually applying tags or searching for resources that aren't compliant, you create a policy that automatically applies the needed tags during deployment.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>

Question: 31

CertyIQ

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

Contoso has an on-premises identity infrastructure. The infrastructure includes servers that run Active Directory Domain Services (AD DS) and Azure AD Connect.

Contoso has a partnership with a company named Fabrikam, Inc. Fabrikam has an Active Directory forest and a Microsoft 365 tenant. Fabrikam has the same on-premises identity infrastructure components 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 group 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. In the Azure AD tenant of Contoso, create cloud-only user accounts for the Fabrikam developers.
- B. Configure a forest trust between the on-premises Active Directory forests of Contoso and Fabrikam.
- C. Configure an organization relationship between the Microsoft 365 tenants of Fabrikam and Contoso.
- D. In the Azure AD tenant of Contoso, create guest accounts for the Fabrikam developers.**

Answer: D

Explanation:

You can use the capabilities in Azure Active Directory B2B to collaborate with external guest users and you can use Azure RBAC to grant just the permissions that guest users need in your environment.

Incorrect:

Not B: Forest trust is used for internal security, not external access.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-external-users>

Question: 32

CertyIQ

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure Active Directory (Azure AD) tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1. What should you recommend?

- A. Configure the Azure AD provisioning service.
- B. Enable Azure AD pass-through authentication and update the sign-in endpoint.
- C. Use Azure AD entitlement management to govern external users.**
- D. Configure Azure AD join.

Answer: C

Explanation:

The app is single tenant authentication so users must be present in contoso directory.

<https://docs.microsoft.com/en-us/azure/active-directory/develop/single-and-multi-tenant-apps>

With Azure AD B2B, external users authenticate to their home directory, but have a representation in your directory.

<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users>

A is wrong because its to automate provisioning to third party SaaS app.

[https://docs.microsoft.com/en-us/azure/active-directory/app-provisioning/how-provisioning-works?
source=recommendations](https://docs.microsoft.com/en-us/azure/active-directory/app-provisioning/how-provisioning-works?source=recommendations)

B. is wrong because the application would need to switch to multi tenant..

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-convert-app-to-be-multi-tenant>

Question: 33

CertyIQ

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

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

Explanation:

Box 1: Azure AD -

Grant permissions in Azure AD.

Box 2: Azure API Management -

Configure a JWT validation policy to pre-authorize requests.

Pre-authorize requests in API Management with the Validate JWT policy, by validating the access tokens of each incoming request. If a request does not have a valid token, API Management blocks it.

Reference:

<https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad>

Question: 34

CertyIQ

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

What should you include in the recommendation?

- A. Azure Log Analytics
- B. Azure Arc
- C. Azure Analysis Services
- D. Application Insights

Answer: A

Explanation:

The Activity log is a platform log in Azure that provides insight into subscription-level events. Activity log includes such information as when a resource is modified or when a virtual machine is started.

Activity log events are retained in Azure for 90 days and then deleted.

For more functionality, you should create a diagnostic setting to send the Activity log to one or more of these locations for the following reasons: to Azure Monitor Logs for more complex querying and alerting, and longer retention (up to two years) to Azure Event Hubs to forward outside of Azure to Azure Storage for cheaper, long-term archiving

Note: Azure Monitor builds on top of Log Analytics, the platform service that gathers log and metrics data from all your resources. The easiest way to think about it is that Azure Monitor is the marketing name, whereas Log Analytics is the technology that powers it.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log>

Question: 35

CertyIQ

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure Active Directory (Azure AD) tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

- A. Configure the Azure AD provisioning service.
- B. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).
- C. Use Azure AD entitlement management to govern external users.

D. Configure Azure AD Identity Protection.

Answer: C

Explanation:

Entitlement management is an identity governance capability that enables organizations to manage identity and access lifecycle at scale by automating access request workflows, access assignments, reviews, and expiration. Entitlement management allows delegated non-admins to create access packages that external users from other organizations can request access to. One and multi-stage approval workflows can be configured to evaluate requests, and provision users for time-limited access with recurring reviews. Entitlement management enables policy-based provisioning and deprovisioning of external accounts.

Note: Access Packages -

An access package is the foundation of entitlement management. Access packages are groupings of policy-governed resources a user needs to collaborate on a project or do other tasks. For example, an access package might include: access to specific SharePoint sites, enterprise applications including your custom in-house and SaaS apps like Salesforce.

Microsoft Teams.

Microsoft 365 Groups.

Incorrect:

Not A: Automatic provisioning refers to creating user identities and roles in the cloud applications that users need access to. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change.

Not B: Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:

Provide just-in-time privileged access to Azure AD and Azure resources

Assign time-bound access to resources using start and end dates

Etc.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/6-secure-access-entitlement-management> <https://docs.microsoft.com/en-us/azure/active-directory/app-provisioning/how-provisioning-works> <https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>

Question: 36

CertyIQ

You are developing an app that will read activity logs for an Azure subscription by using Azure Functions.

You need to recommend an authentication solution for Azure Functions. The solution must minimize administrative effort.

What should you include in the recommendation?

- A. an enterprise application in Azure AD
- B. system-assigned managed identities**
- C. shared access signatures (SAS)
- D. application registration in Azure AD

Answer: B

Explanation:

system-assigned managed identities reduce administrative efforts - B makes more sense

<https://learn.microsoft.com/en-us/azure/azure-functions/security-concepts?tabs=v4>

<https://learn.microsoft.com/en-us/azure/app-service/overview-authentication-authorization>

Question: 37

CertyIQ

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

- A. Configure Azure AD join.
- B. Use Azure AD entitlement management to govern external users.**
- C. Enable Azure AD pass-through authentication and update the sign-in endpoint.
- D. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

Answer: B

Explanation:

Use Azure AD entitlement management to govern external users.many times repeated

Question: 38

CertyIQ

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

- A. Configure Azure AD join.
- B. Configure Azure AD Identity Protection.

C. Use Azure AD entitlement management to govern external users.

D. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

Answer: C

Explanation:

When you reach here, this question will no longer be challenging.

Question: 39

CertyIQ

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

What should you include in the recommendation?

- A. Azure Activity Log
- B. Azure Arc
- C. Azure Analysis Services
- D. Azure Monitor metrics

Answer: A

Explanation:

Azure activity log contains required data.

Question: 40

CertyIQ

HOTSPOT

-

You have an Azure subscription that contains an Azure key vault named KV1 and a virtual machine named VM1. VM1 runs Windows Server 2022: Azure Edition.

You plan to deploy an ASP.Net Core-based application named App1 to VM1.

You need to configure App1 to use a system-assigned managed identity to retrieve secrets from KV1. The solution must minimize development effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

Configure App1 to use OAuth 2.0:

▼

- Authorization code grant flows
- Client credentials grant flows
- Implicit grant flows

Configure App1 to use a REST API call to retrieve an authentication token from the:

▼

- Azure Instance Metadata Service (MDS) endpoint
- OAuth 2.0 access token endpoint of Azure AD
- OAuth 2.0 access token endpoint of Microsoft Identity Platform

Answer:

Answer Area

Configure App1 to use OAuth 2.0:

▼

- Authorization code grant flows
- Client credentials grant flows**
- Implicit grant flows

Configure App1 to use a REST API call to retrieve an authentication token from the:

▼

- Azure Instance Metadata Service (MDS) endpoint**
- OAuth 2.0 access token endpoint of Azure AD**
- OAuth 2.0 access token endpoint of Microsoft Identity Platform

Explanation:

Client Credentials grant flows

OAuth2 Access Token endpoint of azure ad

Question: 41

CertyIQ

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

- A. Configure Azure AD join.
- B. Configure Azure AD Identity Protection.

C. Configure a Conditional Access policy.

D. Configure Supported account types in the application registration and update the sign-in endpoint.

Answer: D

Explanation:

Configure Supported account types in the application registration and update the sign-in endpoint.

Reference:

<https://learn.microsoft.com/en-us/security/zero-trust/develop/identity-supported-account-types>

<https://learn.microsoft.com/en-us/azure/active-directory/develop/howto-modify-supported-accounts>

CertyIQ

Question: 42

You have an Azure AD tenant named contoso.com that has a security group named Group1. Group1 is configured for assigned memberships. Group1 has 50 members, including 20 guest users.

You need to recommend a solution for evaluating the membership of Group1. The solution must meet the following requirements:

- The evaluation must be repeated automatically every three months.
- Every member must be able to report whether they need to be in Group1.
- Users who report that they do not need to be in Group1 must be removed from Group1 automatically.
- Users who do not report whether they need to be in Group1 must be removed from Group1 automatically.

What should you include in the recommendation?

- A. Implement Azure AD Identity Protection.
- B. Change the Membership type of Group1 to Dynamic User.
- C. Create an access review.**
- D. Implement Azure AD Privileged Identity Management (PIM).

Answer: C

Explanation:

Based on the requirements below:

The evaluation must be repeated automatically every three months.

- Every member must be able to report whether they need to be in Group1.
- Users who report that they do not need to be in Group1 must be removed from Group1 automatically.
- Users who do not report whether they need to be in Group1 must be removed from Group1 automatically.

The correct answer should be - C. Create an access review.

<https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview>

CertyIQ

Question: 43

HOTSPOT

You have an Azure subscription named Sub1 that is linked to an Azure AD tenant named contoso.com.

You plan to implement two ASP.NET Core apps named App1 and App2 that will be deployed to 100 virtual machines in Sub1. Users will sign in to App1 and App2 by using their contoso.com credentials.

App1 requires read permissions to access the calendar of the signed-in user. App2 requires write permissions to access the calendar of the signed-in user.

You need to recommend an authentication and authorization solution for the apps. The solution must meet the following requirements:

- Use the principle of least privilege.
- 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.

Answer Area

Authentication:

- Application registration in Azure AD
- A system-assigned managed identity
- A user-assigned managed identity

Authorization:

- Application permissions
- Azure role-based access control (Azure RBAC)
- Delegated permissions

Answer:

Answer Area

Authentication:

- Application registration in Azure AD
- A system-assigned managed identity
- A user-assigned managed identity**

Authorization:

- Application permissions
- Azure role-based access control (Azure RBAC)
- Delegated permissions**

Explanation:

Box 1: A user-assigned managed identity

Box 2: Delegated permissions

The question states that we have to minimize the administrative effort and managed identities do just that. Additionally we have 100 VMs so user-assigned managed identity can be used as it can be shared unlike system-assigned one. I researched a bit and found one helpful article which contains this sentence:

"Previously, when we did not have managed identities, we created an application registration for the resource. Using a secret or certificate to authenticate with Azure. This created a lot of overhead, as it required secret management, key rotation, etc. With managed identities, Azure takes care of this for us."

So I believe that although app registration could be used, it wouldn't reduce admin effort as much as Managed Identity.

<https://adatum.no/azure/azure-active-directory/azure-application-registrations-enterprise-app-managed-identities>

Question: 44

CertyIQ

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

- A. Enable Azure AD pass-through authentication and update the sign-in endpoint.
- B. Use Azure AD entitlement management to govern external users.**
- C. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).
- D. Configure Azure AD Identity Protection.

Answer: B

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-overview#what-can-i-do-with-entitlement-management>

Here are some of capabilities of entitlement management:

- Select connected organizations whose users can request access. When a user who isn't yet in your directory requests access, and is approved, they're automatically invited into your directory and assigned access. When their access expires, if they have no other access package assignments, their B2B account in your directory can be automatically removed.

Question: 45

CertyIQ

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

- A. Configure the Azure AD provisioning service.
- B. Enable Azure AD pass-through authentication and update the sign-in endpoint.
- C. Configure Supported account types in the application registration and update the sign-in endpoint.**
- D. Configure Azure AD join.

Answer: C

Explanation:

Reference:

<https://learn.microsoft.com/en-us/security/zero-trust/develop/identity-supported-account-types>

Question: 46

HOTSPOT

You have an Azure AD tenant that contains a management group named MG1.

You have the Azure subscriptions shown in the following table.

Name	Management group
Sub1	MG1
Sub2	MG2
Sub3	Tenant Root Group

The subscriptions contain the resource groups shown in the following table.

Name	Subscription
RG1	Sub1
RG2	Sub2
RG3	Sub3

The subscription contains the Azure AD security groups shown in the following table.

Name	Member of
Group1	Group3
Group2	Group3
Group3	<i>None</i>

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

You perform the following actions:

Assign User3 the Contributor role for Sub1.

Assign Group1 the Virtual Machine Contributor role for MG1.

Assign Group3 the Contributor role for the Tenant Root Group.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can create a new virtual machine in RG1.	<input type="radio"/>	<input type="radio"/>
User2 can grant permissions to Group2.	<input type="radio"/>	<input type="radio"/>
User3 can create a storage account in RG2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 can create a new virtual machine in RG1.	<input checked="" type="checkbox"/>	<input type="radio"/>
User2 can grant permissions to Group2.	<input type="radio"/>	<input checked="" type="checkbox"/>
User3 can create a storage account in RG2.	<input checked="" type="checkbox"/>	<input type="radio"/>

Explanation:

Since Group 1 is assigned VM contributor to MG1, it will be able to create a new VM in RG1. User 2 is not able to grant permission to Group 2 because it is just a member with contributor role. Since Group 3 has Contributor role for the Tenant Root Group, User3 can create storage account in RG2

Question: 47

CertyIQ

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

- A.Configure Azure AD Identity Protection.
- B.Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).
- C.Configure Supported account types in the application registration and update the sign-in endpoint.**
- D.Configure a Conditional Access policy.

Answer: C

Explanation:

Configure Supported account types in the application registration and update the sign-in endpoint.

CertyIQ

Question: 48

Your company has the divisions shown in the following table.

Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

- A.Use Azure AD entitlement management to govern external users.**
- B.Enable Azure AD pass-through authentication and update the sign-in endpoint.
- C.Configure a Conditional Access policy.
- D.Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

Answer: A

Explanation:

This has been repeated many times and has two answers based on the provided possibilities: Its either Use Azure AD entitlement management to govern external usersOrConfigure Supported account types in the application registration and update the sign-in endpointBoth answers will lead you to the same solution.

CertyIQ

Question: 49

You have an Azure subscription that contains 1,000 resources.

You need to generate compliance reports for the subscription. The solution must ensure that the resources can be grouped by department.

What should you use to organize the resources?

- A.application groups and quotas
- B.Azure Policy and tags**

- C.administrative units and Azure Lighthouse
- D.resource groups and role assignments

Answer: B

Explanation:

Azure Policy and tags

CertyIQ

Question: 50

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

What should you include in the recommendation?

- A.Azure Arc
- B.Azure Monitor metrics
- C.Azure Advisor
- D.Azure Log Analytics**

Answer: D

Explanation:

Azure Log Analytics

CertyIQ

Question: 51

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

What should you include in the recommendation?

- A.Azure Monitor action groups
- B.Azure Arc
- C.Azure Monitor metrics
- D.Azure Activity Log**

Answer: D

Explanation:

Azure Activity Log is a correct answer.

CertyIQ

Question: 52

DRAG DROP

-

You have an Azure AD tenant that contains an administrative unit named MarketingAU. MarketingAU contains 100

users.

You create two users named User1 and User2.

You need to ensure that the users can perform the following actions in MarketingAU:

- User1 must be able to create user accounts.
- User2 must be able to reset user passwords.

Which role should you assign to each user? To answer, drag the appropriate roles to the correct users. Each role may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Roles

- Helpdesk Administrator for MarketingAU
- Helpdesk Administrator for the tenant
- User Administrator for MarketingAU
- User Administrator for the tenant

Answer Area

- | | |
|--------|------|
| User1: | Role |
| User2: | Role |

Answer:

Answer Area

- | | |
|-------|--------------------------------------|
| User1 | User Administrator for MarketingAU |
| User2 | Helpdesk Administrator for Marketing |

Question: 53

CertyIQ

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

What should you include in the recommendation?

- A.Azure Arc
- B.Azure Log Analytics
- C.Application insights
- D.Azure Monitor action groups

Answer: B

Explanation:

Azure Log Analytics

Question: 54

CertyIQ

You have an Azure subscription.

You plan to deploy a monitoring solution that will include the following:

- Azure Monitor Network Insights
- Application Insights
- Microsoft Sentinel
- VM insights

The monitoring solution will be managed by a single team.

What is the minimum number of Azure Monitor workspaces required?

- A.1
- B.2
- C.3
- D.4

Answer: A**Explanation:**

1. A. 1 You only need a single Azure Monitor Log Analytics workspace for all these monitoring solutions. Here's why:- Azure Monitor Network Insights, Application Insights, Microsoft Sentinel, and VM insights, all of these components can send their data to a Log Analytics workspace. - The workspace is a unique environment for Azure Monitor log data. Each workspace has its own data repository and configuration, and data sources and solutions are configured to store their data in a workspace. Therefore, a single Azure Monitor Log Analytics workspace can be utilized to collect and analyze data from all the components of the monitoring solution. This will also enable a unified management and analysis of the collected data.

Question: 55

CertyIQ

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

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

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

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

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

What should you include in the recommendation?

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

Answer: B**Explanation:**

SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance

preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.

Reference:

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

CertyIQ

Question: 56

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 from Server1 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 Logic Apps integration account
- B. an Azure Import/Export job
- C. Azure Data Factory
- D. an Azure Analysis services On-premises data gateway
- E. an Azure Batch account

Answer: BC

Explanation:

B: You can use the Azure Import/Export service to securely export large amounts of data from Azure Blob storage. The service requires you to ship empty drives to the Azure datacenter. The service exports data from your storage account to the drives and then ships the drives back.

C: Big data requires a service that can orchestrate and operationalize processes to refine these enormous stores of raw data into actionable business insights.

Azure Data Factory is a managed cloud service that's built for these complex hybrid extract-transform-load (ETL), extract-load-transform (ELT), and data integration projects.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-from-blobs> <https://docs.microsoft.com/en-us/azure/data-factory/introduction>

CertyIQ

Question: 57

You have an Azure subscription that contains two applications named App1 and App2. App1 is a sales processing application. When a transaction in App1 requires shipping, a message is added to an Azure Storage account queue, and then App2 listens to the queue for relevant transactions.

In the future, additional applications will be added that will process some of the shipping requests based on the specific details of the transactions.

You need to recommend a replacement for the storage account queue to ensure that each additional application will be able to read the relevant transactions.

What should you recommend?

- A. one Azure Data Factory pipeline
- B. multiple storage account queues
- C. one Azure Service Bus queue
- D. one Azure Service Bus topic

Answer: D

Explanation:

A queue allows processing of a message by a single consumer. In contrast to queues, topics and subscriptions provide a one-to-many form of communication in a publish and subscribe pattern. It's useful for scaling to large numbers of recipients. Each published message is made available to each subscription registered with the topic. Publisher sends a message to a topic and one or more subscribers receive a copy of the message, depending on filter rules set on these subscriptions.

Reference:

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

Question: 58

CertyIQ

HOTSPOT -

You need to design a storage solution for an app that will store large amounts of frequently used data. The solution must meet the following requirements:

- ⇒ Maximize data throughput.
- ⇒ Prevent the modification of data for one year.
- ⇒ Minimize latency for read and write operations.

Which Azure Storage account type and storage service 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

Storage account type:

BlobStorage	
BlockBlobStorage	
FileStorage	
StorageV2 with Premium performance	
StorageV2 with Standard performance	

Storage service:

Blob	
File	
Table	

Answer:

Answer Area

Storage account type:

BlobStorage
BlockBlobStorage
FileStorage
StorageV2 with Premium performance
StorageV2 with Standard performance

Storage service:

Blob
File
Table

Explanation:

Box 1: BlockBlobStorage -

Block Blob is a premium storage account type for block blobs and append blobs. Recommended for scenarios with high transaction rates, or scenarios that use smaller objects or require consistently low storage latency.

Box 2: Blob -

The Archive tier is an offline tier for storing blob data that is rarely accessed. The Archive tier offers the lowest storage costs, but higher data retrieval costs and latency compared to the online tiers (Hot and Cool). Data must remain in the Archive tier for at least 180 days or be subject to an early deletion charge.

Reference:

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

Question: 59

CertyIQ

HOTSPOT -

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

Name	Type	Performance
storage1	StorageV2	Standard
storage2	StorageV2	Premium
storage3	BlobStorage	Standard
storage4	FileStorage	Premium

You plan to implement two new apps that have the requirements shown in the following table.

Name	Requirement
App1	Use lifecycle management to migrate app data between storage tiers
App2	Store app data in an Azure file share

Which storage accounts should you recommend using for each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

App1:

- Storage1 and storage2 only
- Storage1 and storage3 only
- Storage1, storage2, and storage3 only
- Storage1, storage2, storage3, and storage4

App2:

- Storage4 only
- Storage1 and storage4 only
- Storage1, storage2, and storage4 only
- Storage1, storage2, storage3, and storage4

Answer:

Answer Area

App1:

Storage1 and storage2 only
Storage1 and storage3 only
Storage1, storage2, and storage3 only
Storage1, storage2, storage3, and storage4

App2:

Storage4 only
Storage1 and storage4 only
Storage1, storage2, and storage4 only
Storage1, storage2, storage3, and storage4

Explanation:

Box 1: Storage1 and storage3 only

Need to use Standard accounts.

Data stored in a premium block blob storage account cannot be tiered to hot, cool, or archive using Set Blob Tier or using Azure Blob Storage lifecycle management

Box 2: Storage1 and storage4 only

Azure File shares requires Premium accounts. Only Storage1 and storage4 are premium.

Reference:

<https://docs.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview#feature-support> <https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-file-share?tabs=azure-portal#basics>

Question: 60

CertyIQ

You are designing an application that will be hosted in Azure.

The application will host video files that range from 50 MB to 12 GB. The application will use certificate-based authentication and will be available to users on the internet.

You need to recommend a storage option for the video files. The solution must provide the fastest read performance and must minimize storage costs.

What should you recommend?

- A. Azure Files
- B. Azure Data Lake Storage Gen2
- C. Azure Blob Storage**
- D. Azure SQL Database

Answer: C

Explanation:

Blob Storage: Stores large amounts of unstructured data, such as text or binary data, that can be accessed from anywhere in the world via HTTP or HTTPS. You can use Blob storage to expose data publicly to the

world, or to store application data privately.

Max file in Blob Storage. 4.77 TB.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/digital-media-video>

CertyIQ

Question: 61

You are designing a SQL database solution. The solution will include 20 databases that will be 20 GB each and have varying usage patterns.

You need to recommend a database platform to host the databases. The solution must meet the following requirements:

- ⇒ The solution must meet a Service Level Agreement (SLA) of 99.99% uptime.
- ⇒ The compute resources allocated to the databases must scale dynamically.
- ⇒ The solution must have reserved capacity.

Compute charges must be minimized.

What should you include in the recommendation?

- A. an elastic pool that contains 20 Azure SQL databases
- B. 20 databases on a Microsoft SQL server that runs on an Azure virtual machine in an availability set
- C. 20 databases on a Microsoft SQL server that runs on an Azure virtual machine
- D. 20 instances of Azure SQL Database serverless

Answer: A

Explanation:

The compute and storage redundancy is built in for business critical databases and elastic pools, with a SLA of 99.99%.

Reserved capacity provides you with the flexibility to temporarily move your hot databases in and out of elastic pools (within the same region and performance tier) as part of your normal operations without losing the reserved capacity benefit.

Reference:

<https://azure.microsoft.com/en-us/blog/understanding-and-leveraging-azure-sql-database-sla/>

CertyIQ

Question: 62

HOTSPOT -

You have an on-premises database that you plan to migrate to Azure.

You need to design the database architecture to meet the following requirements:

- ⇒ Support scaling up and down.
- ⇒ Support geo-redundant backups.
- ⇒ Support a database of up to 75 TB.
- ⇒ Be optimized for online transaction processing (OLTP).

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Service:

Azure SQL Database
Azure SQL Managed Instance
Azure Synapse Analytics
SQL Server on Azure Virtual Machines

Service tier:

Basic
Business Critical
General Purpose
Hyperscale
Premium
Standard

Answer:

Answer Area

Service:

Azure SQL Database
Azure SQL Managed Instance
Azure Synapse Analytics
SQL Server on Azure Virtual Machines

Service tier:

Basic
Business Critical
General Purpose
Hyperscale
Premium
Standard

Explanation:

Box 1: Azure SQL Database -

Azure SQL Database:

Database size always depends on the underlying service tiers (e.g. Basic, Business Critical, Hyperscale).

It supports databases of up to 100 TB with Hyperscale service tier model.

Active geo-replication is a feature that lets you to create a continuously synchronized readable secondary database for a primary database. The readable secondary database may be in the same Azure region as the primary, or, more commonly, in a different region. This kind of readable secondary databases are also known as geo-secondaries, or geo-replicas.

Azure SQL Database and SQL Managed Instance enable you to dynamically add more resources to your database with minimal downtime.

Box 2: Hyperscale -

Incorrect Answers:

- ⇒ SQL Server on Azure VM: geo-replication not supported.
- ⇒ Azure Synapse Analytics is not optimized for online transaction processing (OLTP).
- ⇒ Azure SQL Managed Instance max database size is up to currently available instance size (depending on the number of vCores).

Max instance storage size (reserved) - 2 TB for 4 vCores

- 8 TB for 8 vCores
- 16 TB for other sizes

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/active-geo-replication-overview> <https://medium.com/awesome-azure/azure-difference-between-azure-sql-database-and-sql-server-on-vm-comparison-azure-sql-vs-sql-server-vm-cf02578a1188>

Question: 63

CertyIQ

You are planning an Azure IoT Hub solution that will include 50,000 IoT devices. Each device will stream data, including temperature, device ID, and time data. Approximately 50,000 records will be written every second. The data will be visualized in near real time. You need to recommend a service to store and query the data. Which two 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 Event Grid
- C. Azure Cosmos DB SQL API
- D. Azure Time Series Insights

Answer: CD**Explanation:**

D: Time Series Insights is a fully managed service for time series data. In this architecture, Time Series Insights performs the roles of stream processing, data store, and analytics and reporting. It accepts streaming data from either IoT Hub or Event Hubs and stores, processes, analyzes, and displays the data in near real time.

C: The processed data is stored in an analytical data store, such as Azure Data Explorer, HBase, Azure Cosmos DB, Azure Data Lake, or Blob Storage.

Reference:

<https://docs.microsoft.com/en-us/azure/architecture/data-guide/scenarios/time-series>

Question: 64

CertyIQ

You are designing an application that will aggregate content for users.

You need to recommend a database solution for the application. The solution must meet the following requirements:

- ⇒ Support SQL commands.
- ⇒ Support multi-master writes.
- ⇒ Guarantee low latency read operations.

What should you include in the recommendation?

- A. Azure Cosmos DB SQL API
- B. Azure SQL Database that uses active geo-replication
- C. Azure SQL Database Hyperscale
- D. Azure Database for PostgreSQL

Answer: A**Explanation:**

With Cosmos DB's novel multi-region (multi-master) writes replication protocol, every region supports both writes and reads. The multi-region writes capability also enables:

Unlimited elastic write and read scalability.

99.999% read and write availability all around the world.

Guaranteed reads and writes served in less than 10 milliseconds at the 99th percentile.

Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/distribute-data-globally>

Question: 65

CertyIQ

HOTSPOT -

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

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

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

Name	Resource group	Location	Account kind
storage1	RG1	East US	StorageV2 (general purposev2)
storage2	RG2	Central US	BlobStorage

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

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

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

Answer:**Answer Area**

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

Explanation:

Box 1: Yes -

Auditing works fine for a Standard account.

Box 2: No -

Auditing limitations: Premium storage is currently not supported.

Box 3: No -

Auditing limitations: Premium storage is currently not supported.

Reference:

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

Question: 66

CertyIQ

DRAG DROP -

You plan to import data from your on-premises environment to 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 2014 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:

Tools
AzCopy
Azure Cosmos DB Data Migration Tool
Data Management Gateway
Data Migration Assistant

Answer Area

From the SQL Server 2012 database: Tool

Answer:

Tools
AzCopy
Azure Cosmos DB Data Migration Tool
Data Management Gateway
Data Migration Assistant

Answer Area

From the SQL Server 2012 database: Data Migration Assistant

From the table in the SQL Server 2014 database: Azure Cosmos DB Data Migration Tool

Explanation:

Box 1: Data Migration Assistant -

The Data Migration Assistant (DMA) helps you upgrade to a modern data platform by detecting compatibility issues that can impact database functionality in your new version of SQL Server or Azure SQL Database. DMA recommends performance and reliability improvements for your target environment and allows you to move your schema, data, and uncontained objects from your source server to your target server.

Incorrect:

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

Box 2: Azure Cosmos DB Data Migration Tool

Azure Cosmos DB Data Migration Tool can be used to migrate a SQL Server Database table to Azure Cosmos.

Reference:

<https://docs.microsoft.com/en-us/sql/dma/dma-overview>

<https://docs.microsoft.com/en-us/azure/cosmos-db/cosmosdb-migrationchoices>

Question: 67

CertyIQ

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. Data Migration Assistant (DMA)
- C. AzCopy
- D. Azure Data Factory

Answer: D

Explanation:

You can create Data Factory pipelines that copies data from Azure Blob Storage to Azure SQL Database. The configuration pattern applies to copying from a file-based data store to a relational data store.

Required steps:

- Create a data factory.
- Create Azure Storage and Azure SQL Database linked services.
- Create Azure Blob and Azure SQL Database datasets.
- Create a pipeline contains a Copy activity.
- Start a pipeline run.
- Monitor the pipeline and activity runs.

Reference:

<https://docs.microsoft.com/en-us/azure/data-factory/tutorial-copy-data-dot-net>

Question: 68

CertyIQ

You have an Azure subscription.

Your on-premises network contains a file server named Server1. Server1 stores 5 TB of company files that are accessed rarely.

You plan to copy the files to Azure Storage.

You need to implement a storage solution for the files that meets the following requirements:

- ⇒ The files must be available within 24 hours of being requested.
- ⇒ Storage costs must be minimized.

Which two possible storage solutions achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Create an Azure Blob Storage account that is configured for the Cool default access tier. Create a blob container, copy the files to the blob container, and set each file to the Archive access tier.
- B. Create a general-purpose v1 storage account. Create a blob container and copy the files to the blob container.
- C. Create a general-purpose v2 storage account that is configured for the Cool default access tier. Create a file share in the storage account and copy the files to the file share.
- D. Create a general-purpose v2 storage account that is configured for the Hot default access tier. Create a blob container, copy the files to the blob container, and set each file to the Archive access tier.
- E. Create a general-purpose v1 storage account. Create a file share in the storage account and copy the files to the file share.

Answer: AD

Explanation:

To minimize costs: The Archive tier is optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

Reference:

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

CertyIQ

Question: 69

You have an app named App1 that uses two on-premises Microsoft SQL Server databases named DB1 and DB2.

You plan to migrate DB1 and DB2 to Azure

You need to recommend an Azure solution to host DB1 and DB2. The solution must meet the following requirements:

- ⇒ Support server-side transactions across DB1 and DB2.
- ⇒ Minimize administrative effort to update the solution.

What should you recommend?

- A. two Azure SQL databases in an elastic pool
- B. two databases on the same Azure SQL managed instance**
- C. two databases on the same SQL Server instance on an Azure virtual machine
- D. two Azure SQL databases on different Azure SQL Database servers

Answer: B

Explanation:

Elastic database transactions for Azure SQL Database and Azure SQL Managed Instance allow you to run transactions that span several databases.

SQL Managed Instance enables system administrators to spend less time on administrative tasks because the service either performs them for you or greatly simplifies those tasks.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/elastic-transactions-overview?view=azuresql>

Thank you

Thank you for being so interested in the premium exam material.
I'm glad to hear that you found it informative and helpful.

But Wait

I wanted to let you know that there is more content available in the full version. The full paper contains additional sections and information that you may find helpful, and I encourage you to download it to get a more comprehensive and detailed view of all the subject matter.

[Download Full Version Now](#)



Future is Secured

100% Pass Guarantee



24/7 Customer Support

Mail us - certyiqofficial@gmail.com



Free Updates

Lifetime Free Updates!

Total: **228 Questions**

Link: <https://certyiq.com/papers?provider=microsoft&exam=az-305>