

DUMPS ARENA

Microsoft Azure Architect Design

Microsoft AZ-304

Version Demo

Total Demo Questions: 15

Total Premium Questions: 247

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Case Study 1	6
Topic 2, Case Study 2	2
Topic 3, Case Study 3	2
Topic 4, Case Study 4	3
Topic 5, Case Study 5	4
Topic 6, Case Study 6	2
Topic 7, Mixed Questions	228
Total	247

QUESTION NO: 1

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

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

You have an Azure Storage v2 account named storage1.

You plan to archive data to storage1.

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

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

Does this meet the goal?

A. Yes

B. No

ANSWER: B**Explanation:**

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

Note:

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

Note: Set retention policies and legal holds

1. Create a new container or select an existing container to store the blobs that need to be kept in the immutable state. The container must be in a general-purpose v2 or Blob storage account.

2. Select Access policy in the container settings. Then select Add policy under Immutable blob storage.

3. Either

- To enable legal holds, select Add Policy. Select Legal hold from the drop-down menu, or
- To enable time-based retention, select Time-based retention from the drop-down menu.

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

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

QUESTION NO: 2

You need to recommend a data storage strategy for WebApp1.

What should you include in the recommendation?

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

ANSWER: A**QUESTION NO: 3**

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 a general-purpose v1 storage account. Create a blob container and copy the files to the blob container.
- B. 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.
- C. Create a general-purpose v1 storage account. 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 Cool default access tier. Create a file share in the storage account and copy the files to the file share.
- E. 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.

ANSWER: C D**Explanation:**

The Cool access tier is optimized for storing data that is infrequently accessed and stored for at least 30 days. Using a file share is cheaper than using a blob container.

Incorrect Answers:

A: Using a file share would be cheaper than using a Blob container.

B, E: 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>

QUESTION NO: 4

Your company wants to use an Azure Active Directory (Azure AD) hybrid identity solution.

You need to ensure that users can authenticate if the internet connection to the on-premises Active Directory is unavailable. The solution must minimize authentication prompts for the users.

What should you include in the solution?

- A. password hash synchronization and Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
- B. pass-through authentication and Azure AD Seamless Single Sign-On (Azure AD Seamless SSO)
- C. an Active Directory Federation Services (AD FS) server

ANSWER: A

Explanation:

With Password hash synchronization + Seamless SSO the authentication is in the cloud.

Incorrect Answers:

Pass-through Authentication and federation rely on on-premises infrastructure.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

QUESTION NO: 5

You deploy an Azure virtual machine that runs an ASP.NET application. The application will be accessed from the internet by the users at your company.

You need to recommend a solution to ensure that the users are pre-authenticated by using their Azure Active Directory (Azure AD) account before they can connect to the ASP.NET application.

What should you include in the recommendation?

- A. a public Azure Load Balancer
- B. Azure Application Gateway
- C. Azure Traffic Manager
- D. an Azure AD enterprise application

ANSWER: D

Explanation:

You can manage service principals in the Azure portal through the Enterprise Applications experience. Service principals are what govern an application connecting to Azure AD and can be considered the instance of the application in your directory.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

QUESTION NO: 6 - (DRAG DROP)

DRAG DROP

You are designing a network connectivity strategy for a new Azure subscription. You identify the following requirements:

- The Azure virtual machines on a subnet named Subnet1 must be accessible only from the computers in your London office.
- Engineers require access to the Azure virtual machines on a subnet named Subnet2 over the Internet on a specific TCP/IP management port.
- The Azure virtual machines in the West Europe Azure region must be able to communicate on all ports to the Azure virtual machines in the North Europe Azure region. ▪ Azure virtual machines on Subnet1 and Subnet2 have public IP addresses.

You need to recommend which components must be used to meet the requirements. The solution must minimize costs and administrative effort whenever possible.

What should you include in the recommendation? To answer, drag the appropriate components to the correct requirements. Each component may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

Components

- An Azure ExpressRoute connection
- A network security group (NSG)
- A new virtual network
- A site-to-site VPN
- Virtual network peering

Answer Area

The Azure virtual machines on Subnet1 must be accessible only from the computers in the London office:
Engineers require access to the Azure virtual machines on Subnet2 over the Internet on a specific TCP/IP management port:
The Azure virtual machines in the West Europe region must be able to communicate on all ports to the Azure virtual machines in the North Europe region:

- Component
- Component
- Component

ANSWER:

Components

- An Azure ExpressRoute connection
- A network security group (NSG)
- A new virtual network
- A site-to-site VPN
- Virtual network peering

Answer Area

The Azure virtual machines on Subnet1 must be accessible only from the computers in the London office:
Engineers require access to the Azure virtual machines on Subnet2 over the Internet on a specific TCP/IP management port:
The Azure virtual machines in the West Europe region must be able to communicate on all ports to the Azure virtual machines in the North Europe region:

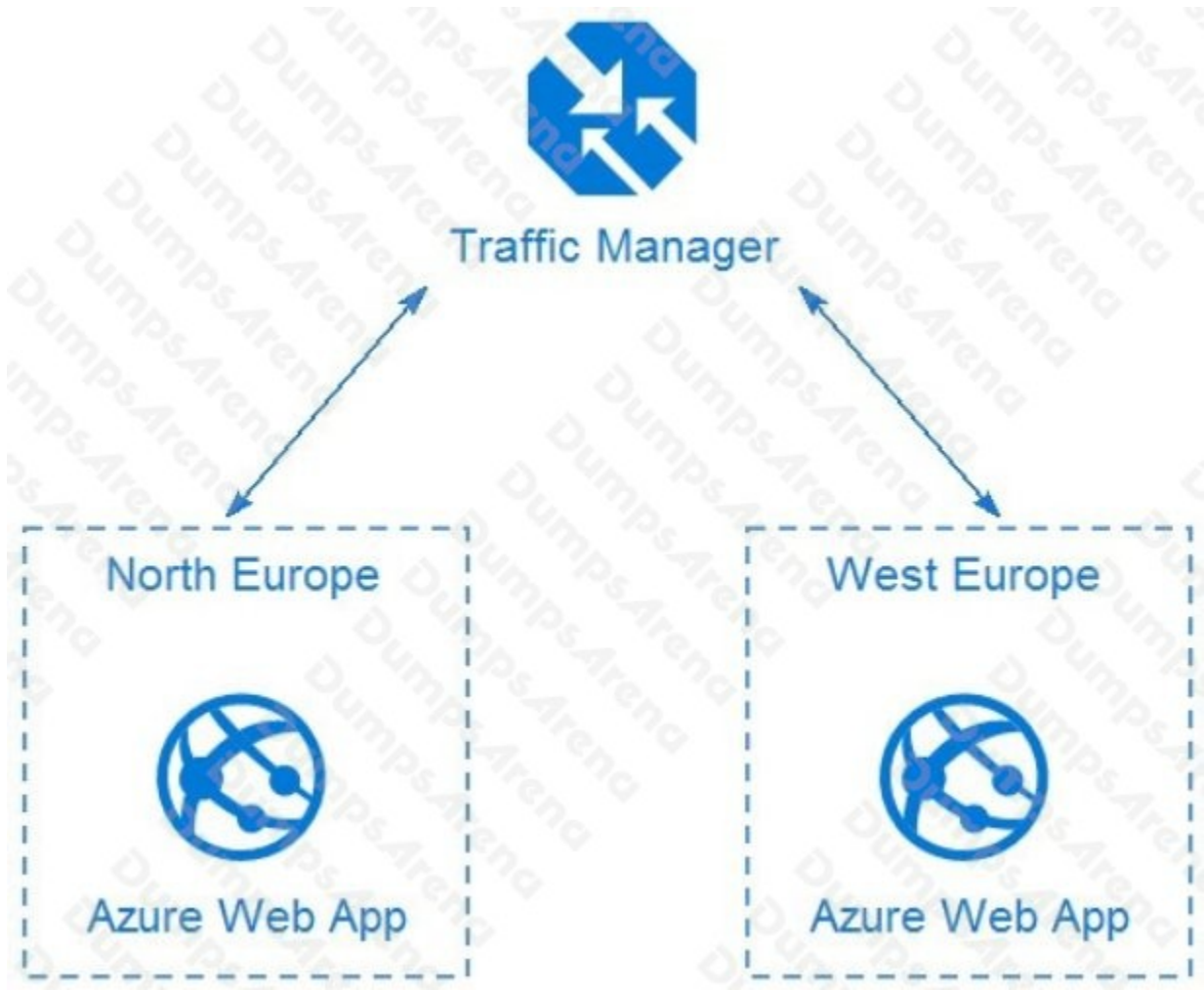
- A site-to-site VPN
- A network security group (NSG)
- Virtual network peering

Explanation:

QUESTION NO: 7 - (HOTSPOT)

HOTSPOT

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



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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area**Statements****Yes****No**

The design supports the technical requirements for redundancy.

The design supports autoscaling.

The design requires a manual configuration if an Azure region fails.

ANSWER:**Answer Area****Statements****Yes****No**

The design supports the technical requirements for redundancy.

The design supports autoscaling.

The design requires a manual configuration if an Azure region fails.

Explanation:

Box 1: Yes

Any new deployments to Azure must be redundant in case an Azure region fails.

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

Box 2: Yes

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

Box 3: No

Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

Reference:

<https://docs.microsoft.com/en-us/azure/traffic-manager/traffic-manager-overview>
<https://blogs.msdn.microsoft.com/hsirtl/2017/07/03/autoscaling-azure-web-apps/>

Design Infrastructure

QUESTION NO: 8 - (HOTSPOT)

HOTSPOT

You plan to deploy a custom database solution that will have multiple instances as shown in the following table.

Host virtual machine	Azure Availability Zone	Azure region
USDB1	1	US East
USDB2	2	US East
USDB3	3	US East
EUDB1	1	West Europe
EUDB2	2	West Europe
EUDB3	3	West Europe

Client applications will access database servers by using db.contoso.com.

You need to recommend load balancing services for the planned deployment. The solution must meet the following requirements:

- Access to at least one database server must be maintained in the event of a regional outage.
- The virtual machines must not connect to the internet directly.

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Global load balancing service:

- ▼
- Azure Application Gateway
- Azure Front Door
- Azure Load Balancer
- Azure Traffic Manager

Availability Zone load balancing service:

- ▼
- Azure Application Gateway
- Azure Front Door
- Azure Load Balancer
- Azure Traffic Manager

ANSWER:

Answer Area

Global load balancing service:

- ▼
- Azure Application Gateway
- Azure Front Door
- Azure Load Balancer
- Azure Traffic Manager

Availability Zone load balancing service:

- ▼
- Azure Application Gateway
- Azure Front Door
- Azure Load Balancer
- Azure Traffic Manager

Explanation:

Box 1: Azure Traffic Manager

Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness. Because Traffic Manager is a DNS-based load-balancing service, it load balances only at the domain level. For that reason, it can't fail over as quickly as Front Door, because of common challenges around DNS caching and systems not honoring DNS TTLs.

Service	Global/regional	Recommended traffic
Azure Front Door	Global	HTTP(S)
Traffic Manager	Global	non-HTTP(S)
Application Gateway	Regional	HTTP(S)
Azure Load Balancer	Regional	non-HTTP(S)

Incorrect Answers:

Front Door is an application delivery network that provides global load balancing and site acceleration service for web applications.

Box 2: Azure Load Balancer

Azure Load Balancer is a high-performance, ultra low-latency Layer 4 load-balancing service (inbound and outbound) for all UDP and TCP protocols. It is built to handle millions of requests per second while ensuring your solution is highly available. Azure Load Balancer is zone-redundant, ensuring high availability across Availability Zones.

Incorrect Answers:

Front Door is an application delivery network that provides global load balancing and site acceleration service for web applications. Reference:

<https://docs.microsoft.com/en-us/azure/architecture/guide/technology-choices/load-balancing-overview>

QUESTION NO: 9

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

You deploy Azure AD Connect.

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

NOTE: Each correct selection is worth one point.

A. Azure AD Privileged Identity Management policies

- B. access reviews
- C. password writeback
- D. Microsoft Cloud App Security Conditional Access App Control
- E. self-service password reset

ANSWER: C E

QUESTION NO: 10

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

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

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

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

NOTE: Each correct selection is worth one point.

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

ANSWER: B D

Explanation:

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

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

Incorrect Answers:

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

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

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

QUESTION NO: 11

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. Azure Active Directory (Azure AD) administrative units
- C. an Azure management group that uses parent groups to create a hierarchy
- D. an Azure policy that enforces tagging rules

ANSWER: D**Explanation:**

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.

Note: Organizing cloud-based resources is a crucial task for IT, unless you only have simple deployments. Use naming and tagging standards to organize your resources for these reasons:

Resource management: Your IT teams will need to quickly locate resources associated with specific workloads, environments, ownership groups, or other important information. Organizing resources is critical to assigning organizational roles and access permissions for resource management.

Reference:

<https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/resource-tagging>
<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies>

QUESTION NO: 12 - (DRAG DROP)

DRAG DROP

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

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

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

What should you recommend for each application? To answer, drag the appropriate services to the correct applications. Each service may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Select and Place:

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

ANSWER:



Explanation:

QUESTION NO: 13

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 Server 1 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 integration account
- B. an On-premises data gateway
- C. an Azure Batch account
- D. an Azure Import/Export job
- E. Azure Data Factory

ANSWER: D E

QUESTION NO: 14

Your company has offices in the United States, Europe, Asia, and Australia.

You have an on-premises app named App1 that uses Azure Table storage. Each office hosts a local instance of App1.

You need to upgrade the storage for App1. The solution must meet the following requirements:

- Enable simultaneous write operations in multiple Azure regions.
- Ensure that write latency is less than 10 ms.
- Support indexing on all columns. ▪ Minimize development effort.

Which data platform should you use?

- A.** Azure SQL Database
- B.** Azure SQL Managed Instance
- C.** Azure Cosmos DB
- D.** Table storage that uses geo-zone-redundant storage (GZRS) replication

ANSWER: D

Explanation:

Azure Cosmos DB Table API has

- Single-digit millisecond latency for reads and writes, backed with <10-ms latency reads and <15-ms latency writes at the 99th percentile, at any scale, anywhere in the world.
- Automatic and complete indexing on all properties, no index management.
- Turnkey global distribution from one to 30+ regions. Support for automatic and manual failovers at any time, anywhere in the world.

Incorrect Answers:

D: Azure Table storage, but has no upper bounds on latency. Reference:

<https://docs.microsoft.com/en-us/azure/cosmos-db/table-support>

QUESTION NO: 15

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

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

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

You need to recommend solutions to manage network traffic.

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

- A.** Configure Azure Traffic Manager.
- B.** Implement Azure ExpressRoute.

- C. Configure a routing table.
- D. Implement an Azure virtual network.

ANSWER: B C

Explanation:

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

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

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

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

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