

- **Vendor: Microsoft**
- **Exam Code: AZ-301**
- **Exam Name: Microsoft Azure Architect Design**
- **New Updated Questions from [Braindump2go](#) (Updated in [July/2020](#))**

### **Visit Braindump2go and Download Full Version AZ-301 Exam Dumps**

#### **QUESTION 247**

You have an Azure SQL database named DB1 that contains multiple tables.  
You need to improve the performance of DB1. The solution must minimize administrative effort.  
What should you use?

- A. Azure Monitor
- B. Azure Advisor
- C. Query Performance Insight
- D. automatic tuning

**Answer: D**

**Explanation:**

Azure SQL Database and Azure SQL Managed Instance automatic tuning provides peak performance and stable workloads through continuous performance tuning based on AI and machine learning.

Automatic tuning is a fully managed intelligent performance service that uses built-in intelligence to continuously monitor queries executed on a database, and it automatically improves their performance.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/automatic-tuning-overview>

#### **QUESTION 248**

Use the following login credentials as needed:

To enter your username, place your cursor in the **Sign in** box and click on the username below.

To enter your password, place your cursor in the **Enter password** box and click on the password below.

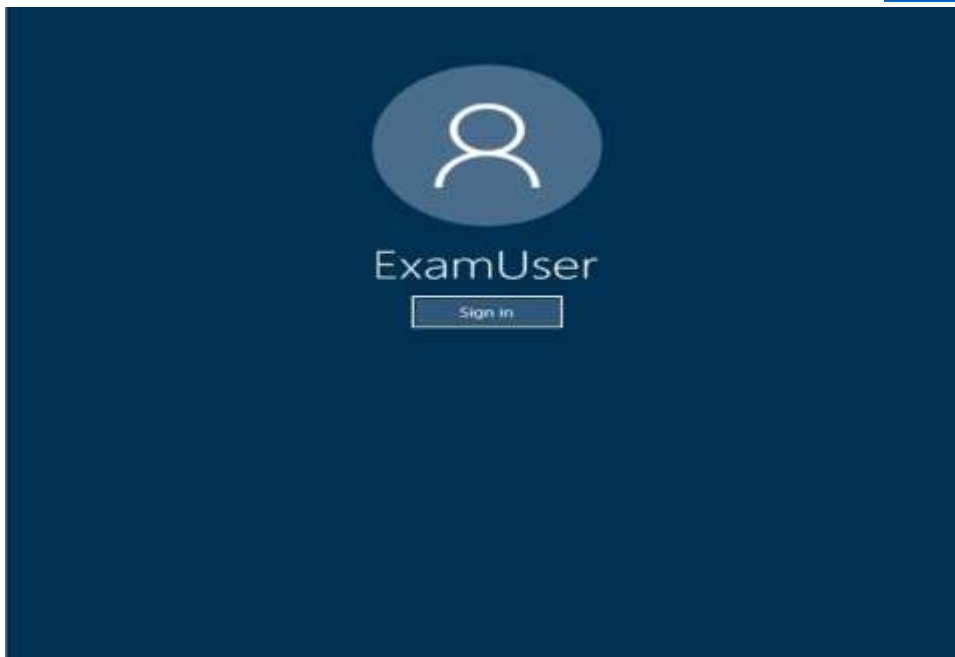
**Azure Username:** User1-10989444@ExamUsers.com

**Azure Password:** KJn29!aBBB

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

**Lab Instance:** 10989444



You need to recommend a solution to ensure that connections to NWVM1 and NWVM3 are load balanced. What should you recommend?

**NOTE: To answer this question, sign in to the Azure portal and explore an Azure resource group named ResourceGroup1lod10989444.**

- A. one Recovery Services vault
- B. one Azure Traffic Manager
- C. one Azure Load Balancer

D. two Azure Load Balancers

**Answer: C**

**Explanation:**

The job of Azure Load Balancer is to direct traffic inside a region.

Incorrect Answers:

B: The job of Azure Traffic Manager is to route traffic globally based on flexible policies, enabling an excellent user experience that aligns with how you've structured your application across the world.

Reference:

<https://www.concurrency.com/blog/w/azure-traffic-manager-vs-azure-load-balancer>

#### **QUESTION 249**

A company has a hybrid ASP.NET Web API application that is based on a software as a service (SaaS) offering. Users report general issues with the data. You advise the company to implement live monitoring and use ad hoc queries on stored JSON data. You also advise the company to set up smart alerting to detect anomalies in the data. You need to recommend a solution to set up smart alerting. What should you recommend?

- A. Azure Security Center and Azure Data Lake Store
- B. Azure Data Lake Analytics and Azure Monitor Logs
- C. Azure Application Insights and Azure Monitor Logs
- D. Azure Site Recovery and Azure Monitor Logs

**Answer: B**

**Explanation:**

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

Reference:

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

#### **QUESTION 250**

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

Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant. The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.

You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker). Solution: Deploy one Azure Key Vault to each region. Configure virtual machines to use Azure Disk Encryption. Use a different Key Vault for encrypting virtual machine disks in each region.

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

The security key from the on-premises HSM need to be exported.

Reference:

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

#### QUESTION 251

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

Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant. The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.

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

**Solution:** Export a security key from the on-premises HSM. Deploy Azure Key Vault and import the security key to Azure Key Vault. Configure the virtual machines to use Azure Storage encryption.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

**Explanation:**

The Key Vault has to be in the same region as the VM that will be encrypted.

Reference:

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

#### QUESTION 252

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

Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant. The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016. Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.

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

**Solution:**

- Deploy one Azure Key Vault to each region
- Export two security keys from the on-premises HSM
- Import the security keys from the HSM into each Azure Key Vault
- Configure the virtual machines to use Azure Disk Encryption
- Use a different Key Vault for encrypting virtual machine disks in each region

Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**Explanation:**

We use the Azure Premium Key Vault with Hardware Security Modules (HSM) backed keys.

The Key Vault has to be in the same region as the VM that will be encrypted.

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

Reference:

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

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

**QUESTION 253**

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

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

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

A team of 10 developers from Fabrikam will work on an Azure solution that will be hosted in the Azure subscription of Contoso. The developers must be added to the Contributor role for a resource 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. Configure an AD FS claims provider trust between the AD FS infrastructures of Fabrikam and Contoso.
- B. Configure an organization relationship between the Office 365 tenants of Fabrikam and Contoso.
- C. In the Azure AD tenant of Contoso, create guest accounts for the Fabrikam developers.
- D. Configure a forest trust between the on-premises Active Directory forests of Contoso and Fabrikam.

**Answer: D**

**Explanation:**

Trust configurations - Configure trust from managed forests(s) or domain(s) to the administrative forest A one-way trust is required from production environment to the admin forest.

Selective authentication should be used to restrict accounts in the admin forest to only logging on to the appropriate production hosts.

Reference:

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

**QUESTION 254**

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

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

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

Solution: Install and configure an on-premises Active Directory Federation Services (AD FS) server and establish federation with Azure AD.

Does the solution meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

Seamless SSO is not applicable to Active Directory Federation Services (ADFS).

Instead install and configure an Azure AD Connect server.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-ssso>

**QUESTION 255**

Use the following login credentials as needed:

To enter your username, place your cursor in the **Sign in** box and click on the username below.

To enter your password, place your cursor in the **Enter password** box and click on the password below.

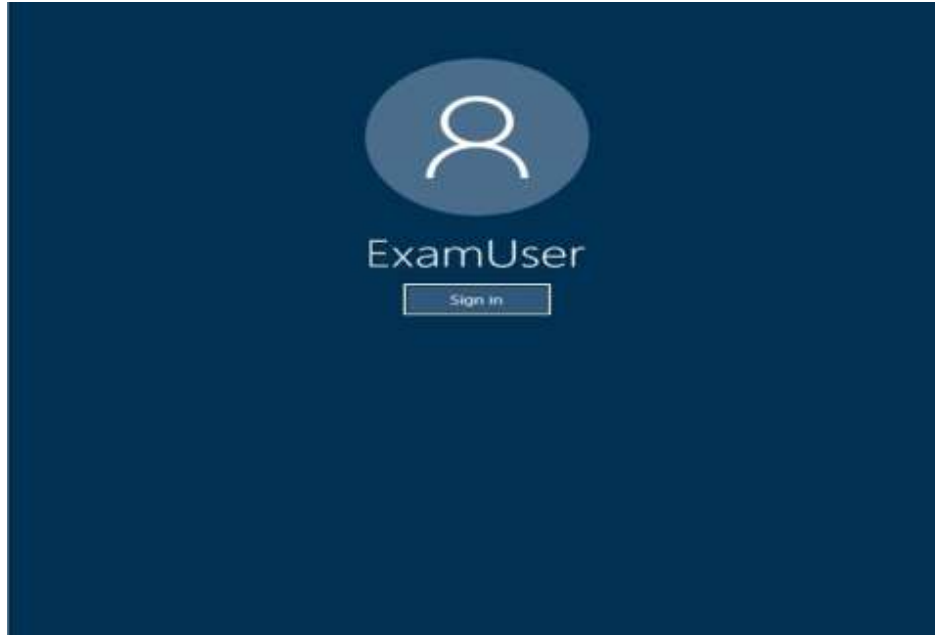
**Azure Username:** User1-10989444@ExamUsers.com

**Azure Password:** KJn29!aBBB

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only:

**Lab Instance:** 10989444



An administrator named Admin1 attempts to create several G-series virtual machines and receives an error message.



You need to recommend a solution to ensure that Admin1 can create the virtual machines.  
What should you recommend?

**NOTE: To answer this question, sign in to the Azure portal and explore an Azure resource group named ResourceGroup1lod10989444.**

- A. Modify a restriction policy.
- B. Remove a resource lock.
- C. Remove a tag.
- D. Modify a permission assigned to Admin1.

**Answer: B**

**Explanation:**

Lock resources to prevent unexpected changes.

As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources.

Reference:

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

#### QUESTION 256

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

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

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

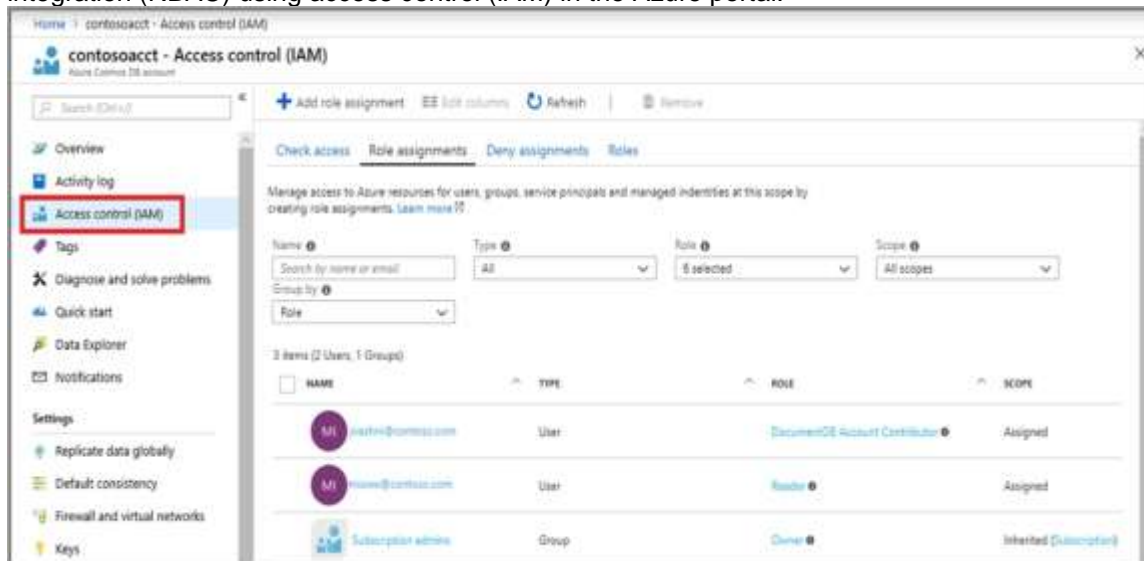
What should you include in the recommendation?

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

**Answer: A**

**Explanation:**

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



Reference:

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

#### QUESTION 257

You use Azure Application Insights.  
You plan to use continuous export.  
You need to store Application Insights data for five years.  
Which Azure service should you use?

- A. Azure SQL Database
- B. Azure Storage
- C. Azure Monitor Logs
- D. Azure Backup

**Answer: B**

**Explanation:**

Create a Continuous Export.

1. In the Application Insights resource for your app under configure on the left, open Continuous Export and choose Add:
2. Choose the telemetry data types you want to export.
3. Create or select an Azure storage account where you want to store the data.  
Click Add, Export Destination, Storage account, and then either create a new store or choose an existing store.
4. Create or select a container in the storage.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/export-telemetry#continuous-export-advanced-storage-configuration>