

## AZ-500.74q

Number: AZ-500  
Passing Score: 800  
Time Limit: 120 min

AZ-500



**Website:** <https://vceplus.com>  
**VCE to PDF Converter:** <https://vceplus.com/vce-to-pdf/>  
**Facebook:** <https://www.facebook.com/VCE.For.All.VN/>  
**Twitter :** [https://twitter.com/VCE\\_Plus](https://twitter.com/VCE_Plus)

<https://vceplus.com/>

### Microsoft Azure Security Technologies

#### Question Set 1

#### QUESTION 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 a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You deploy the On-premises data gateway to the on-premises network.

Does this meet the goal?



<https://vceplus.com/>

A. Yes

B. No

**Correct Answer: B**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: ▪

Create Azure Virtual Network.

▪ Create a custom DNS server in the Azure Virtual Network.

▪ Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.

- Configure forwarding between the custom DNS server and your on-premises DNS server.

References: <https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

## QUESTION 2

**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 a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You create a site-to-site VPN between the virtual network and the on-premises network.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

**Note:** To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: ▪

Create Azure Virtual Network.

- Create a custom DNS server in the Azure Virtual Network.
- Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
- Configure forwarding between the custom DNS server and your on-premises DNS server.

References:

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

### QUESTION 3

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.

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

- Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant
- Minimizes the number of servers required for the solution.

Which authentication method should you include in the recommendation?

- A. federated identity with Active Directory Federation Services (AD FS)
- B. password hash synchronization with seamless single sign-on (SSO)
- C. pass-through authentication with seamless single sign-on (SSO)

**Correct Answer: B**

**Section: [none]**

**Explanation**

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

Explanation:

Password hash synchronization requires the least effort regarding deployment, maintenance, and infrastructure. This level of effort typically applies to organizations that only need their users to sign in to Office 365, SaaS apps, and other Azure AD-based resources. When turned on, password hash synchronization is part of the Azure AD Connect sync process and runs every two minutes.

Incorrect Answers:

A: A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

C: For pass-through authentication, you need one or more (we recommend three) lightweight agents installed on existing servers. These agents must have access to your on-premises Active Directory Domain Services, including your on-premises AD domain controllers. They need outbound access to the Internet and access to your domain controllers. For this reason, it's not supported to deploy the agents in a perimeter network.

Pass-through Authentication requires unconstrained network access to domain controllers. All network traffic is encrypted and limited to authentication requests.

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

#### QUESTION 4

Your network contains an on-premises Active Directory domain named corp.contoso.com.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You sync all on-premises identities to Azure AD.

You need to prevent users who have a `givenName` attribute that starts with `TEST` from being synced to Azure AD. The solution must minimize administrative effort.

What should you use?

- A. Synchronization Rules Editor
- B. Web Service Configuration Tool
- C. Azure Portal
- D. Active Directory Users and Computers



**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Use the Synchronization Rules Editor and write attribute-based filtering rule.

References: <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

#### QUESTION 5

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

An administrator named Admin1 has access to the following identities:

- An OpenID-enabled user account
- A Hotmail account
- An account in contoso.com

- An account in an Azure AD tenant named fabrikam.com

You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1.

To which accounts can you transfer the ownership of Sub1?

- A. contoso.com only
- B. contoso.com, fabrikam.com, and Hotmail only
- C. contoso.com and fabrikam.com only
- D. contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account

**Correct Answer:** C

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to manage the resources.

Reference: <https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer> <https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-an-account-in-another-azure-ad-tenant>

## QUESTION 6

Your company plans to create separate subscriptions for each department. Each subscription will be associated to the same Azure Active Directory (Azure AD) tenant.

You need to configure each subscription to have the same role assignments.

What should you use?

- A. Azure Security Center
- B. Azure Policy
- C. Azure AD Privileged Identity Management (PIM)
- D. Azure Blueprints

**Correct Answer:** D

**Section:** [none]

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

Explanation:

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as: ▪

Role Assignments

▪ Policy Assignments

▪ Azure Resource Manager templates ▪

Resource Groups

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

**QUESTION 7****HOTSPOT**

You have an Azure Container Registry named Registry1.

You add role assignment for Registry1 as shown in the following table.

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.

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

**Hot Area:**

## Answer Area

Upload images:

	▼
User1 only	
User1 and User4 only	
User1, User3, and User4	
User1, User2, User3, and User4	

Download images:

	▼
User2 only	
User1 and User2 only	
User2 ad User4 only	
User1, User2, and User4	
User1, User2, User3, and User4	

Correct Answer:



## Answer Area

Upload images:

	▼
User1 only	
User1 and User4 only	
User1, User3, and User4	
User1, User2, User3, and User4	

Download images:

	▼
User2 only	
User1 and User2 only	
User2 ad User4 only	
User1, User2, and User4	
User1, User2, User3, and User4	

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Box 1: User1 and User4 only

Owner, Contributor and AcrPush can push images.

Box 2: User1, User2, and User4

All, except AcrImagineSigner, can download/pull images.

Role/Permission	Access Resource Manager	Create/delete registry	Push image	Pull image	Delete image data	Change policies	Sign images
Owner	X	X	X	X	X	X	
Contributor	X	X	X	X	X	X	
Reader	X			X			
AcrPush			X	X			
AcrPull				X			
AcrDelete					X		
AcrImageSigner							X

References:

<https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles>

### QUESTION 8

You have an Azure subscription.

You create an Azure web app named Contoso1812 that uses an S1 App service plan.

You create a DNS record for www.contoso.com that points to the IP address of Contoso1812.

You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL.

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

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

A. Turn on the system-assigned managed identity for Contoso1812.

- B. Add a hostname to Contoso1812.
- C. Scale out the App Service plan of Contoso1812.
- D. Add a deployment slot to Contoso1812.
- E. Scale up the App Service plan of Contoso1812.
- F. Upload a PFX file to Contoso1812.

**Correct Answer:** BF

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either [www.contoso.com](http://www.contoso.com) or [contoso.com](http://contoso.com) as a fully qualified domain name (FQDN). To do this, you have to create three records:

A root "A" record pointing to [contoso.com](http://contoso.com)

A root "TXT" record for verification

A "CNAME" record for the [www](http://www) name that points to the A record

F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.

References: <https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain>

## QUESTION 9

**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 subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

**Solution:** You create a lock on Sa1.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.

References: <https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

#### QUESTION 10

**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 a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** B

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: ▪  
Create Azure Virtual Network.

- Create a custom DNS server in the Azure Virtual Network.
- Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
- Configure forwarding between the custom DNS server and your on-premises DNS server.

References: <https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

#### **QUESTION 11**

Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com.

You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect.

You need to identify which roles and groups are required to perform the planned configuration. The solution must use the principle of least privilege.

Which two roles and groups should you identify? Each correct answer presents part of the solution.

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

- A. the Domain Admins group in Active Directory
- B. the Security administrator role in Azure AD
- C. the Global administrator role in Azure AD
- D. the User administrator role in Azure AD
- E. the Enterprise Admins group in Active Directory

**Correct Answer:** CE

**Section: [none]**

**Explanation**

**Explanation/Reference:**

References:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions>

## QUESTION 12

### DRAG DROP

You create an Azure subscription with Azure AD Premium P2.

You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.

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

**Select and Place:**

Actions	Answer Area
Discover privileged roles.	
Sign up PIM for Azure AD roles.	
Consent to PIM.	
Discover resources.	
Verify your identity by using multi-factor authentication (MFA).	

**Correct Answer:**

Actions	Answer Area
Discover privileged roles.	Consent to PIM.
	Verify your identity by using multi-factor authentication (MFA).
	Sign up PIM for Azure AD roles.
Discover resources.	

Section: [none]

Explanation

Explanation/Reference:



### QUESTION 13

**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 a hybrid configuration of Azure Active Directory (Azure AD).

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You deploy an Azure AD Application Proxy.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: ▪

Create Azure Virtual Network.

- Create a custom DNS server in the Azure Virtual Network.
- Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
- Configure forwarding between the custom DNS server and your on-premises DNS server.

Reference:

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

#### 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.**

You have an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You regenerate the access keys.

Does this meet the goal?

- A. Yes



B. No

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Instead you should create a new stored access policy.

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.

Reference:

<https://docs.microsoft.com/en-us/rest/api/storageservices/Establishing-a-Stored-Access-Policy>

#### **QUESTION 15**

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication.

Database developers must connect to the database instance and authenticate by using their on-premises Active Directory account.

You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.

Which authentication method should you recommend?

- A. Active Directory - Password
- B. Active Directory - Universal with MFA support
- C. SQL Server Authentication
- D. Active Directory - Integrated

**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Use Active Directory password authentication when connecting with an Azure AD principal name using the Azure AD managed domain.

Use this method to authenticate to SQL DB/DW with Azure AD for native or federated Azure AD users. A native user is one explicitly created in Azure AD and being authenticated using user name and password, while a federated user is a Windows user whose domain is federated with Azure AD. The latter method (using user & password) can be used when a user wants to use their windows credential, but their local machine is not joined with the domain (for example, using a remote access). In this case, a Windows user can indicate their domain account and password and can authenticate to SQL DB/DW using federated credentials.

Incorrect Answers:

D: Use Active Directory integrated authentication if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

References: <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure>

### QUESTION 16

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.

You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment. The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

- A. a key vault access policy
- B. a linked template
- C. a parameters file
- D. an automation account

**Correct Answer: C**

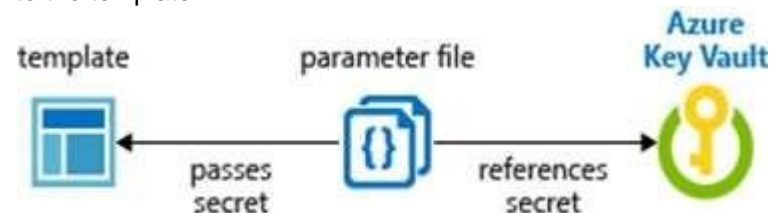
**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

You reference the key vault in the parameter file, not the template. The following image shows how the parameter file references the secret and passes that value to the template.



Reference: <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-keyvault-parameter>

### QUESTION 17

#### SIMULATION

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.

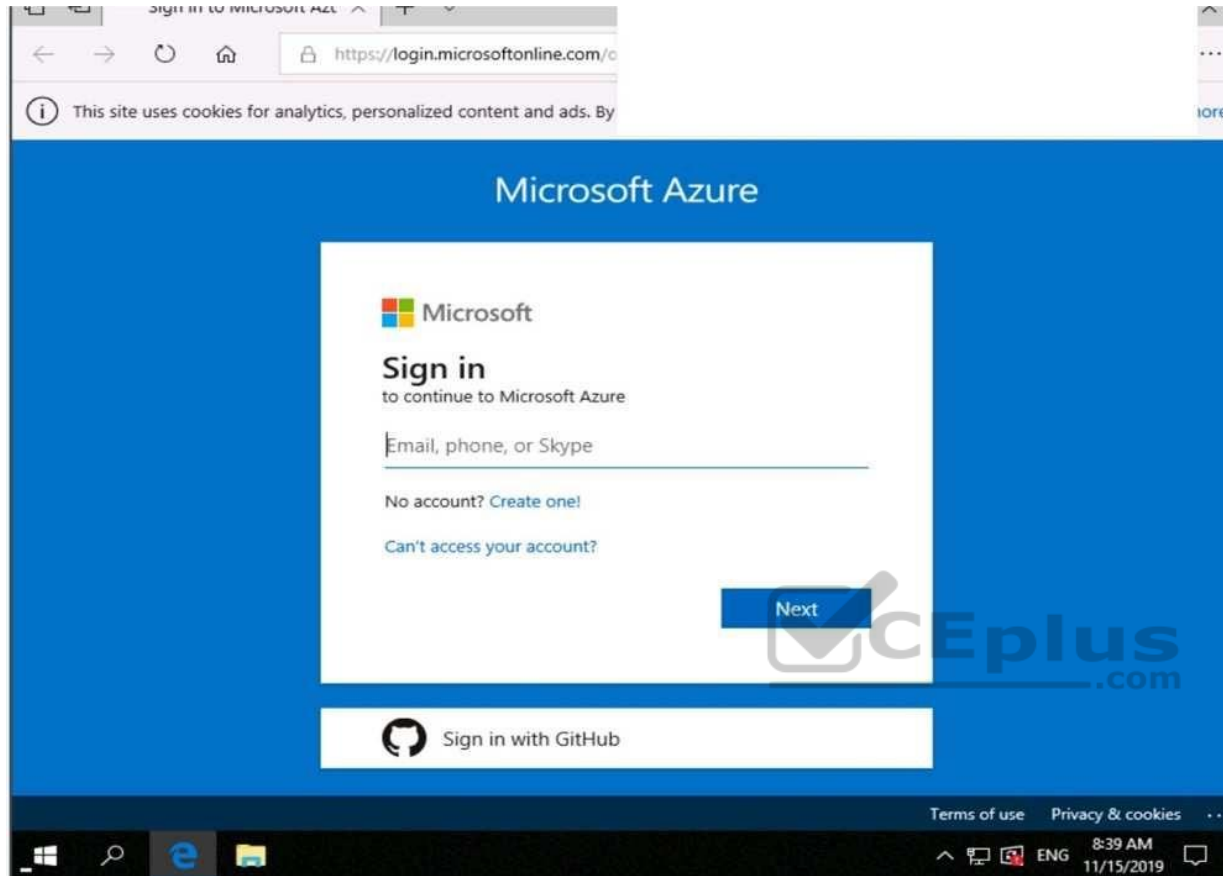
**Azure Username:** User1-10598168@ExamUsers.com

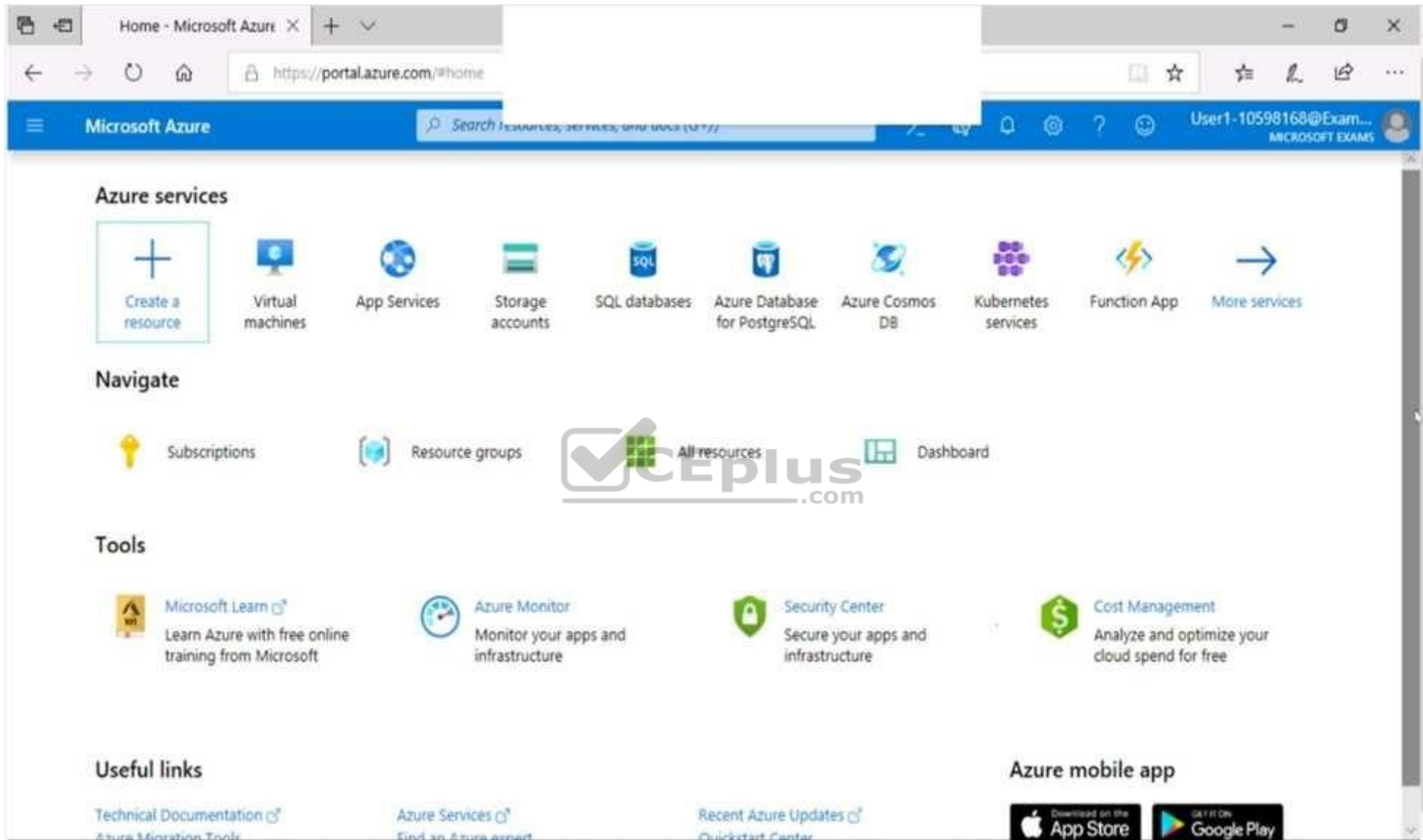
**Azure Password:** Ag1Bh9!#Bd

The following information is for technical support purposes only:

**Lab Instance:** 10598168







The screenshot shows the Microsoft Azure portal home page in a web browser. The browser tab is titled "Home - Microsoft Azure" and the address bar shows "https://portal.azure.com/#home". The page has a blue header with the "Microsoft Azure" logo, a search bar, and a user profile for "User1-10598168@Exam...".

**Azure services**

- Create a resource
- Virtual machines
- App Services
- Storage accounts
- SQL databases
- Azure Database for PostgreSQL
- Azure Cosmos DB
- Kubernetes services
- Function App
- More services

**Navigate**

- Subscriptions
- Resource groups
- All resources
- Dashboard

**Tools**

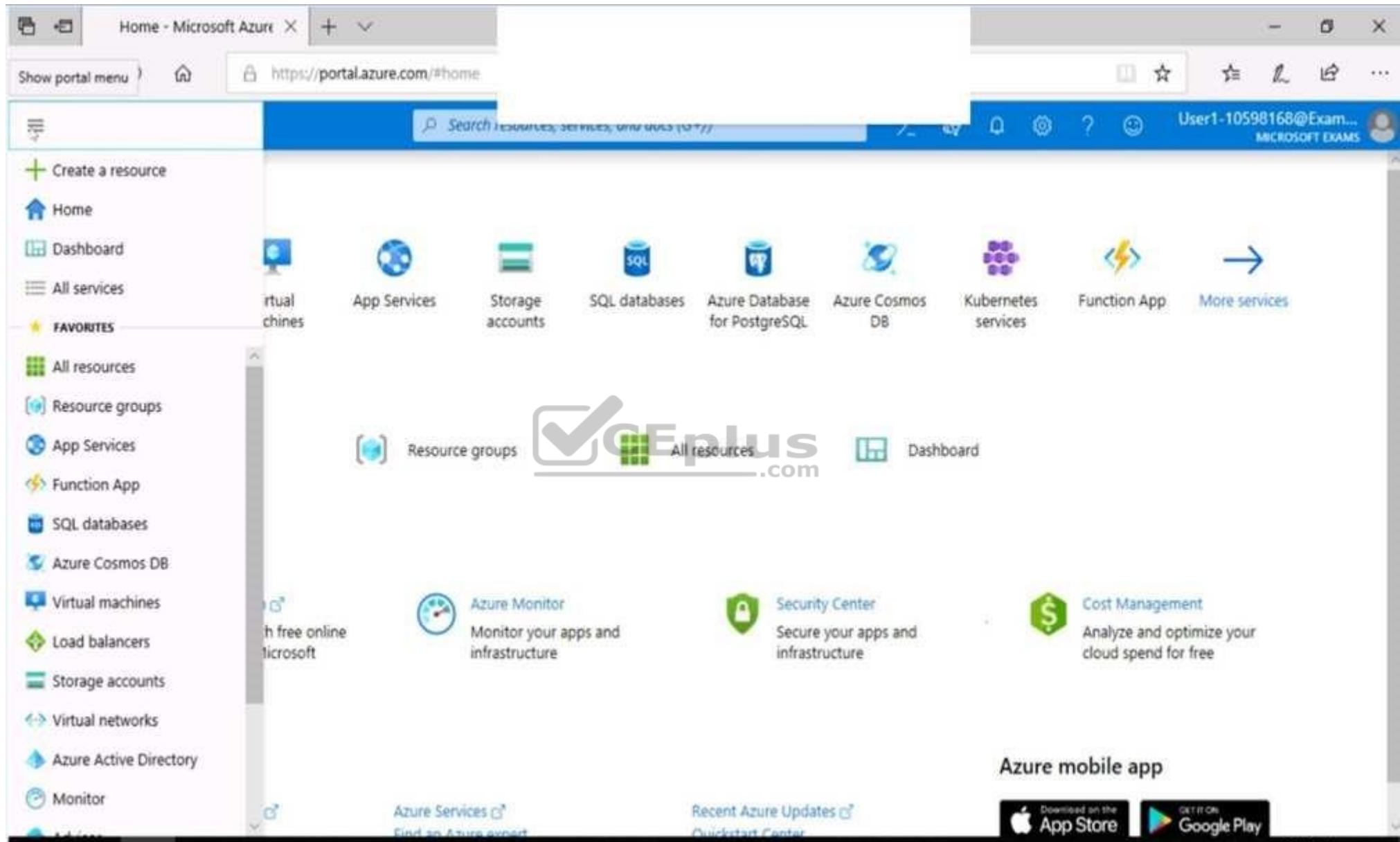
- Microsoft Learn: Learn Azure with free online training from Microsoft
- Azure Monitor: Monitor your apps and infrastructure
- Security Center: Secure your apps and infrastructure
- Cost Management: Analyze and optimize your cloud spend for free

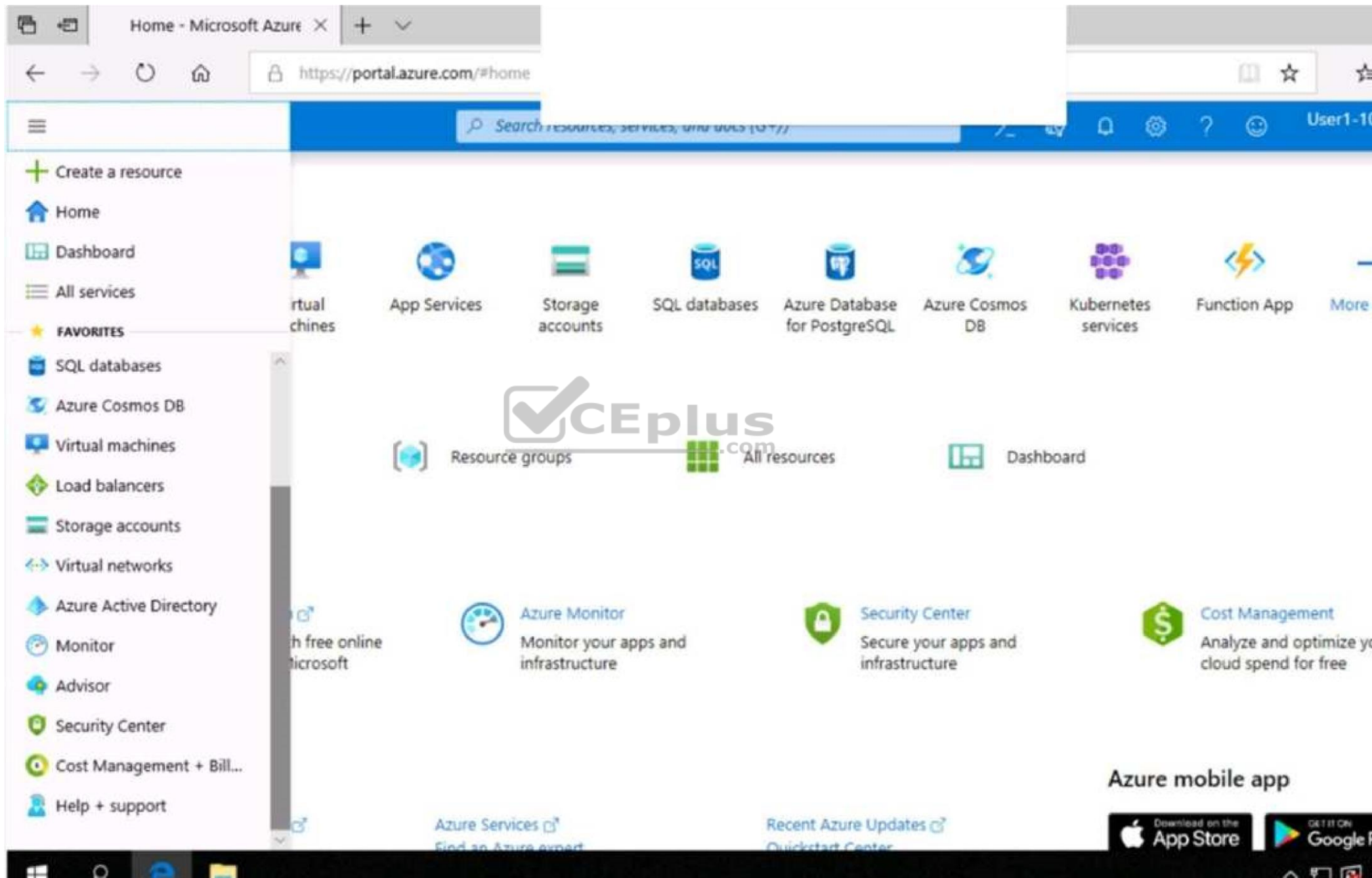
**Useful links**

- Technical Documentation
- Azure Migration Tools
- Azure Services: Find an Azure expert
- Recent Azure Updates
- Quickstart Center

**Azure mobile app**

- Download on the App Store
- GET IT ON Google Play





Home - Microsoft Azure X + -

https://portal.azure.com/#home

Search resources, services, and docs (0/77)

User1-10

FAVORITES

- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Bill...
- Help + support

Virtual machines

App Services

Storage accounts

SQL databases

Azure Database for PostgreSQL

Azure Cosmos DB

Kubernetes services

Function App

More

Resource groups

All resources

Dashboard

Azure Monitor  
Monitor your apps and infrastructure

Security Center  
Secure your apps and infrastructure

Cost Management  
Analyze and optimize your cloud spend for free

Azure mobile app

Download on the App Store

GET IT ON Google Play

Azure Services

Recent Azure Updates

Quickstart Center

The developers at your company plan to create a web app named App10598168 and to publish the app to <https://www.contoso.com>.

You need to perform the following tasks:

- Ensure that App10598168 is registered to Azure Active Directory (Azure AD). ▪

Generate a password for App10598168.

**To complete this task, sign in to the Azure portal.**

**Correct Answer:** See the explanation below.

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:



Step 1: Register the Application

1. Sign in to your Azure Account through the Azure portal.
2. Select Azure Active Directory.
3. Select App registrations.
4. Select New registration.
5. Name the application App10598168 . Select a supported account type, which determines who can use the application. Under Redirect URI, select Web for the type of application you want to create. Enter the URI: <https://www.contoso.com> , where the access token is sent to.



[Dashboard](#) > [Microsoft - App registrations](#) > Register an application

## Register an application

 If you are building an application for external users that will be distributed by Microsoft, you must register as a first party application to meet all security, privacy, and compliance policies. [Read our decision guide](#) 

### \* Name

The user-facing display name for this application (this can be changed later).

example-app 

### Supported account types

Who can use this application or access this API?


- ☒ Accounts in this organizational directory only (Microsoft)
- ☐ Accounts in any organizational directory
- ☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)

[Help me choose...](#)

### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web 

<https://contoso.org/exampleapp> 

6. Click Register

Step 2: Create a new application secret

If you choose not to use a certificate, you can create a new application secret.

7 Select Certificates & secrets.

8. Select Client secrets -> New client secret.

9. Provide a description of the secret, and a duration. When done, select Add.

After saving the client secret, the value of the client secret is displayed. Copy this value because you aren't able to retrieve the key later. You provide the key value with the application ID to sign in as the application. Store the key value where your application can retrieve it.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>



## Testlet 1

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

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

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

### To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question. **Overview**

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

### Existing Environment

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using <a href="https://litwareinc.com">https://litwareinc.com</a> and <a href="http://www.litwareinc.com">http://www.litwareinc.com</a> .
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

### Identity and Access Requirements

Azure Security Center is set to the Free tier.

### Planned changes

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

Litware identifies the following identity and access requirements:

- All San Francisco users and their devices must be members of Group1.
- The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
- Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

### Platform Protection Requirements

Litware identifies the following platform protection requirements:

- Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
- The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
- Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.
- Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
- A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

### Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

### Data and Application Requirements

Litware identifies the following data and applications requirements:

- The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.
- WebApp1 must enforce mutual authentication.

### General Requirements

Litware identifies the following general requirements:

- Whenever possible, administrative effort must be minimized.
- Whenever possible, use of automation must be minimized.

**QUESTION 1**

You need to ensure that users can access VM0. The solution must meet the platform protection requirements.

What should you do? A.

Move VM0 to Subnet1.



<https://vceplus.com/>

- B. On Firewall, configure a network traffic filtering rule.
- C. Assign RT1 to AzureFirewallSubnet.
- D. On Firewall, configure a DNAT rule.



**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Azure Firewall has the following known issue:

Conflict with Azure Security Center (ASC) Just-in-Time (JIT) feature.

If a virtual machine is accessed using JIT, and is in a subnet with a user-defined route that points to Azure Firewall as a default gateway, ASC JIT doesn't work. This is a result of asymmetric routing – a packet comes in via the virtual machine public IP (JIT opened the access), but the return path is via the firewall, which drops the packet because there is no established session on the firewall.

Solution: To work around this issue, place the JIT virtual machines on a separate subnet that doesn't have a user-defined route to the firewall.

Scenario:

VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
-----	-----------------	--

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.

References:

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



## Testlet 2

### Case Study

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

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

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

### To start the case study

To display the first question on this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question. **Overview**

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

### Existing Environment

#### Azure AD

Contoso.com contains the users shown in the following table.



Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	None
User9	Sydney	Owner

Contoso.com contains the security groups shown in the following table.

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	user.city -contains "ON"
Group2	Dynamic user	user.city -match "*on"

### Sub1

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User9 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networkSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

## Sub2

Sub2 contains the virtual networks shown in the following table.

Name	Subnet
VNetwork1	Subnet11, Subnet12, and Subnet13
VNetwork2	Subnet21

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet11
VM2	NIC2	ASG2	Subnet11
VM3	NIC3	None	Subnet12
VM4	NIC4	ASG1	Subnet13
VM5	NIC5	None	Subnet21

All virtual machines have public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

Sub2 contains the network security groups (NSGs) shown in the following table.

Name	Associated to
NSG1	NIC2
NSG2	Subnet11
NSG3	Subnet13
NSG4	Subnet21



NSG1 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG2 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG4 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

## Technical requirements

Contoso identifies the following technical requirements:

- Deploy Azure Firewall to VNetwork1 in Sub2.
- Register an application named App2 in contoso.com.
- Whenever possible, use the principle of least privilege.
- Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

## QUESTION 1

### HOTSPOT

You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2.

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

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

**Hot Area:**

Answer area	Statements	Yes	No
	From VM1, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
	From VM2, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
	From VM1, you can connect to the web server on VM4.	<input type="radio"/>	<input type="radio"/>

**Correct Answer:**

Answer area	Statements	Yes	No
	From VM1, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input checked="" type="radio"/>
	From VM2, you can successfully ping the private IP address of VM4.	<input checked="" type="radio"/>	<input type="radio"/>
	From VM1, you can connect to the web server on VM4.	<input checked="" type="radio"/>	<input type="radio"/>

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Box 1: No. VM4 is in Subnet13 which has NSG3 attached to it.

VM1 is in ASG1. NSG3 would only allow ICMP pings from ASG2 but not ASG1. Only TCP traffic is allowed from ASG1.



NSG3 has the inbound security rules shown in the following table.

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

Box 2: Yes.

VM2 is in ASG2. Any protocol is allowed from ASG2 so ICMP ping would be allowed.

Box3. VM1 is in ASG1. TCP traffic is allowed from ASG1 so VM1 could connect to the web server as connections to the web server would be on ports TCP 80 or TCP 443.

## QUESTION 2

You need to meet the technical requirements for VNetwork1.

What should you do first?

- A. Create a new subnet on VNetwork1.
- B. Remove the NSGs from Subnet11 and Subnet13.
- C. Associate an NSG to Subnet12.
- D. Configure DDoS protection for VNetwork1.

**Correct Answer: A**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.

Azure firewall needs a dedicated subnet named AzureFirewallSubnet.

References:

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal> **Question Set 3**

**QUESTION 1**

You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.

You create a service endpoint for MicrosoftStorage in Subnet1.

You need to ensure that when you deploy Docker containers to VM1, the containers can access Azure Storage resources by using the service endpoint.

What should you do on VM1 before you deploy the container?

- A. Create an application security group and a network security group (NSG).
- B. Edit the docker-compose.yml file.
- C. Install the container network interface (CNI) plug-in.

**Correct Answer:** C

**Section:** [none]

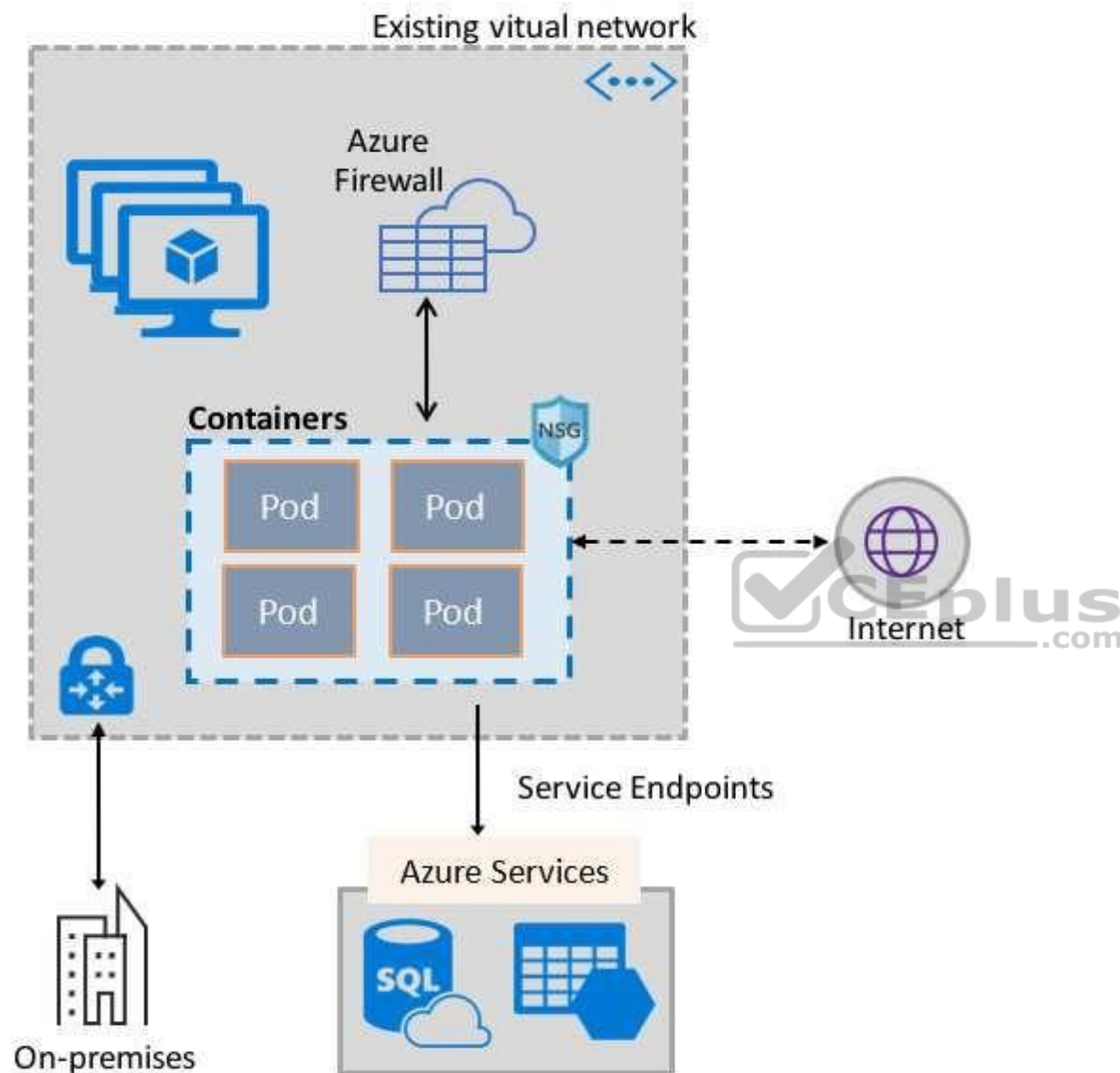
**Explanation**

**Explanation/Reference:**

Explanation:

The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform. The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.

The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:



References:

<https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview> **QUESTION 2**

You have Azure Resource Manager templates that you use to deploy Azure virtual machines.



You need to disable unused Windows features automatically as instances of the virtual machines are provisioned.

What should you use?

- A. device configuration policies in Microsoft Intune
- B. an Azure Desired State Configuration (DSC) virtual machine extension
- C. application security groups
- D. device compliance policies in Microsoft Intune

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.

Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSC-Service so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.

Reference: <https://docs.microsoft.com/en-us/azure/automation/automation-dsc-getting-started>

### QUESTION 3

You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.

You need to use the auto-generated service principal to authenticate to the Azure Container Registry.

What should you create?

- A. an Azure Active Directory (Azure AD) group
- B. an Azure Active Directory (Azure AD) role assignment
- C. an Azure Active Directory (Azure AD) user
- D. a secret in Azure Key Vault

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.

References: <https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks>

**QUESTION 4**

HOTSPOT

You have two Azure virtual machines in the East US2 region as shown in the following table.

Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

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

**Hot Area:**

## Answer Area

VM1: 

	▼
The operating system version	
The tier	
The type	

VM2: 

	▼
The operating system version	
The tier	
The type	

Correct Answer:

## Answer Area

VM1: 

	▼
The operating system version	
The tier	
The type	

VM2: 

	▼
The operating system version	
The tier	
The type	

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

VM1: The Tier

The Tier needs to be upgraded to standard.

Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.

VM2: The type

Need to change the VMtype to any of A, D, DS, G, GS, F, and so on, series IaaS VMs.

Not the operating system version: Ubuntu 16.04 is supported.

References: <https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-overview>  
[https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk\\_LinuxOSSupport](https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-faq#bkmk_LinuxOSSupport)

#### QUESTION 5

You have the Azure virtual machines shown in the following table.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West Europe	RG1
VM3	Windows Server 2016	West Europe	RG2
VM4	Red Hat Enterprise Linux 7.4	East US	RG2

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region.

Which virtual machines can be enrolled in Analytics1?

- A. VM1 only
- B. VM1, VM2, and VM3 only
- C. VM1, VM2, VM3, and VM4
- D. VM1 and VM4 only

**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Note: Create a workspace

- In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics. ▪ Click Create, and then select choices for the following items:

Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.

Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.

For Resource Group, select an existing resource group that contains one or more Azure virtual machines.

Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.

Incorrect Answers:

B, C: A Log Analytics workspace provides a geographic location for data storage. VM2 and VM3 are at a different location.

D: VM4 is a different resource group.

References: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access>

#### QUESTION 6

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the **Exhibit** tab.)



**Basics**

Subscription	Azure Pass - Sponsorship
Resource group	RG1
Region	(US) East US
Kubernetes cluster name	AKScluster
Kubernetes version	1.12.8
DNS name prefix	AKScluster
Node count	3
Node size	Standard_DS_v2

**Scale**

Virtual nodes	Disabled
VM scale sets (preview)	Disabled

**Authentication**

Enable RBAC	No
-------------	----

**Networking**

HTTP application routing	No
Network configuration	Basic

**Monitoring**

Enable container monitoring	No
-----------------------------	----

**Tags**

(none)

You plan to deploy the cluster to production. You disable HTTP application routing.

You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.

What should you do?

- A. Create an AKS Ingress controller.
- B. Install the container network interface (CNI) plug-in.
- C. Create an Azure Standard Load Balancer.
- D. Create an Azure Basic Load Balancer.

**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

References: <https://docs.microsoft.com/en-us/azure/aks/ingress-tls>



## QUESTION 7

**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 use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy definition and assignments that are scoped to resource groups.

Does this meet the goal?

- A. Yes
- B. No



**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

References: <https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/>

#### QUESTION 8

**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 use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a resource graph and an assignment that is scoped to a management group.

Does this meet the goal?

A. Yes

B. No

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Management groups in Microsoft Azure solve the problem of needing to impose governance policy on more than one Azure subscription simultaneously. However, you need to use an initiative, not a resource graph to bundle the policy definitions into a group that can be applied to the management group.

References: <https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/> **QUESTION 9**

**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 Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You add an extension to each virtual machine.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer: A**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.

References: <https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware>

#### **QUESTION 10**

**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 Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You connect to each virtual machine and add a Windows feature.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Microsoft Antimalware is deployed as an extension and not a feature.

References: <https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware>

#### **QUESTION 11**

From Azure Security Center, you create a custom alert rule.

You need to configure which users will receive an email message when the alert is triggered.

What should you do?

- A. From Azure Monitor, create an action group.
- B. From Security Center, modify the Security policy settings of the Azure subscription.
- C. From Azure Active Directory (Azure AD), modify the members of the Security Reader role group.
- D. From Security Center, modify the alert rule.

**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups>

#### **QUESTION 12**

You are configuring and securing a network environment.

You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic.

You need to ensure that all network traffic is routed through VM1.

What should you configure?

- A. a system route
- B. a network security group (NSG)
- C. a user-defined route

**Correct Answer:** C

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Although the use of system routes facilitates traffic automatically for your deployment, there are cases in which you want to control the routing of packets through a virtual appliance. You can do so by creating user defined routes that specify the next hop for packets flowing to a specific subnet to go to your virtual appliance instead, and enabling IP forwarding for the VM running as the virtual appliance.

Note: User Defined Routes

For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:

- Force tunneling to the Internet via your on-premises network.
- Use of virtual appliances in your Azure environment.
- In the scenarios above, you will have to create a route table and add user defined routes to it.

Reference:

<https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.md>

### QUESTION 13

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

Name	Region	Subnet
VNET1	West US	Subnet11 and Subnet12
VNET2	West US 2	Subnet21
VNET3	East US	Subnet31

The subscription contains the virtual machines shown in the following table.

Name	Network interface	Connected to
VM1	NIC1	Subnet11
VM2	NIC2	Subnet11
VM3	NIC3	Subnet12
VM4	NIC4	Subnet21
VM5	NIC5	Subnet31

On NIC1, you configure an application security group named ASG1.

On which other network interfaces can you configure ASG1?

- A. NIC2 only
- B. NIC2, NIC3, NIC4, and NIC5
- C. NIC2 and NIC3 only
- D. NIC2, NIC3, and NIC4 only

**Correct Answer:** C

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in.

Reference:

<https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/>

#### QUESTION 14

You have 15 Azure virtual machines in a resource group named RG1.

All virtual machines run identical applications.

You need to prevent unauthorized applications and malware from running on the virtual machines.

What should you do?

- A. Apply an Azure policy to RG1.
- B. From Azure Security Center, configure adaptive application controls.
- C. Configure Azure Active Directory (Azure AD) Identity Protection.
- D. Apply a resource lock to RG1.

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and non-Azure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs and helps you apply the specific whitelisting rules using this intelligence.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-adaptive-application>

#### **QUESTION 15**

You plan to deploy Azure container instances.

You have a containerized application that validates credit cards. The application is comprised of two containers: an application container and a validation container.

The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.

You need to ensure that the application container and the validation container are scheduled to be deployed together. The containers must communicate to each other only on ports that are not externally exposed.

What should you include in the deployment?

- A. application security groups
- B. network security groups (NSGs)
- C. management groups
- D. container groups

**Correct Answer:** D

**Section:** [none]

**Explanation**

### Explanation/Reference:

Explanation:

Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

Reference:

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

### QUESTION 16

DRAG DROP

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2.

You need to implement VPN gateways for the virtual networks to meet the following requirements:

- VNET1 must have six site-to-site connections that use BGP.
- VNET2 must have 12 site-to-site connections that use BGP. ▪

Costs must be minimized.

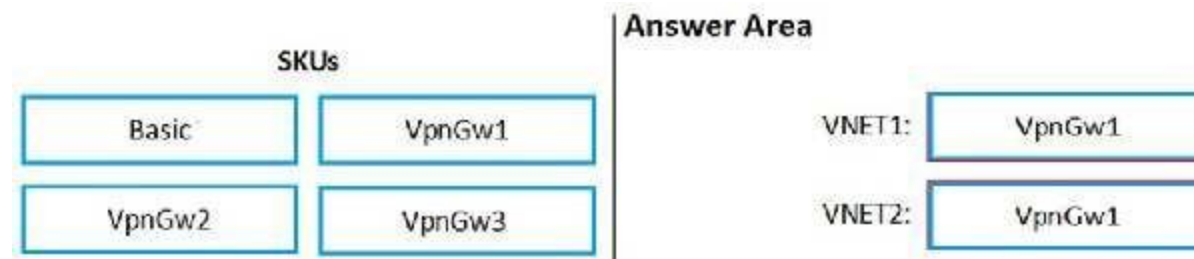
Which VPN gateway SKU should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks. Each SKU may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

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

**Select and Place:**

SKUs		Answer Area	
Basic	VpnGw1	VNET1:	<input type="text"/>
VpnGw2	VpnGw3	VNET2:	<input type="text"/>

**Correct Answer:**



**Section:** [none]

**Explanation**

**Explanation/Reference:**

References: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku>

#### QUESTION 17

You are securing access to the resources in an Azure subscription.

A new company policy states that all the Azure virtual machines in the subscription must use managed disks.

You need to prevent users from creating virtual machines that use unmanaged disks.

What should you do?

- A. Azure Monitor
- B. Azure Policy
- C. Azure Security Center
- D. Azure Service Health

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

#### QUESTION 18

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.



You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.

What should you create?

- A. a secret in Azure Key Vault
- B. a role assignment
- C. an Azure Active Directory (Azure AD) user
- D. an Azure Active Directory (Azure AD) group

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

References: <https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal>

#### QUESTION 19

**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 use Azure Security Center for the centralized policy management of three Azure subscriptions.

You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create an initiative and an assignment that is scoped to a management group.

Does this meet the goal?

- A. Yes
- B. No

**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

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

#### QUESTION 20

You have the Azure virtual machines shown in the following table.

Name	Operating system	State
VM1	Windows Server 2008 R2 Service Pack 1 (SP1)	Running
VM2	Windows Server 2012 R2	Running
VM3	Windows Server 2016	Stopped
VM4	Ubuntu Server 18.04 LTS	Running

For which virtual machine can you enable Update Management?

- A. VM2 and VM3 only
- B. VM2, VM3, and VM4 only
- C. VM1, VM2, and VM4 only
- D. VM1, VM2, VM3, and VM4
- E. VM1, VM2, and VM3 only



**Correct Answer:** C

**Section:** [none]

**Explanation**

**Explanation/Reference:**

References: <https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=%2Fazure%2Fautomation%2Ftoc.json>

#### QUESTION 21

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ConReg1.

You enable content trust for ConReg1.

You need to ensure that User1 can create trusted images in ConReg1. The solution must use the principle of least privilege.

Which two roles should you assign to User1? Each correct answer presents part of the solution.

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

- A. AcrQuarantineReader
- B. Contributor
- C. AcrPush
- D. AcrImageSigner
- E. AcrQuarantineWriter

**Correct Answer:** CD

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles>

## QUESTION 22

You have an Azure Container Registry named ContReg1 that contains a container image named image1.

You enable content trust for ContReg1.

After content trust is enabled, you push two images to ContReg1 as shown in the following table.

Name	Details
image2	Image was pushed with client content trust enabled.
image3	Image was pushed with client content trust disabled.

Which images are trusted images?

- A. image1 and image2 only
- B. image2 only
- C. image1, image2, and image3

**Correct Answer:** B

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

Azure Container Registry implements Docker's content trust model, enabling pushing and pulling of signed images.

To push a trusted image tag to your container registry, enable content trust and push the image with docker push.

To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.

Reference:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust>

### **QUESTION 23**

#### **SIMULATION**

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.

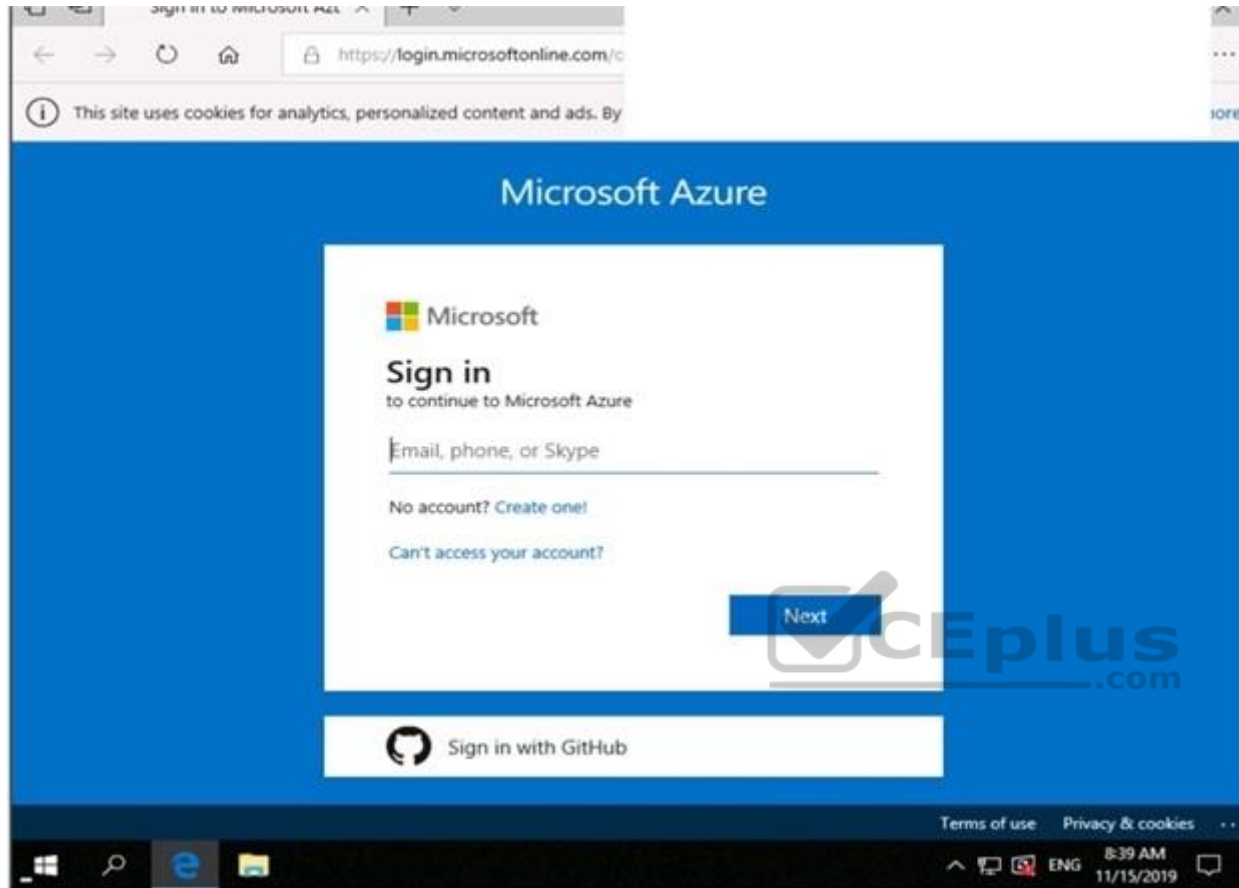
To enter your password, place your cursor in the Enter password box and click on the password below.

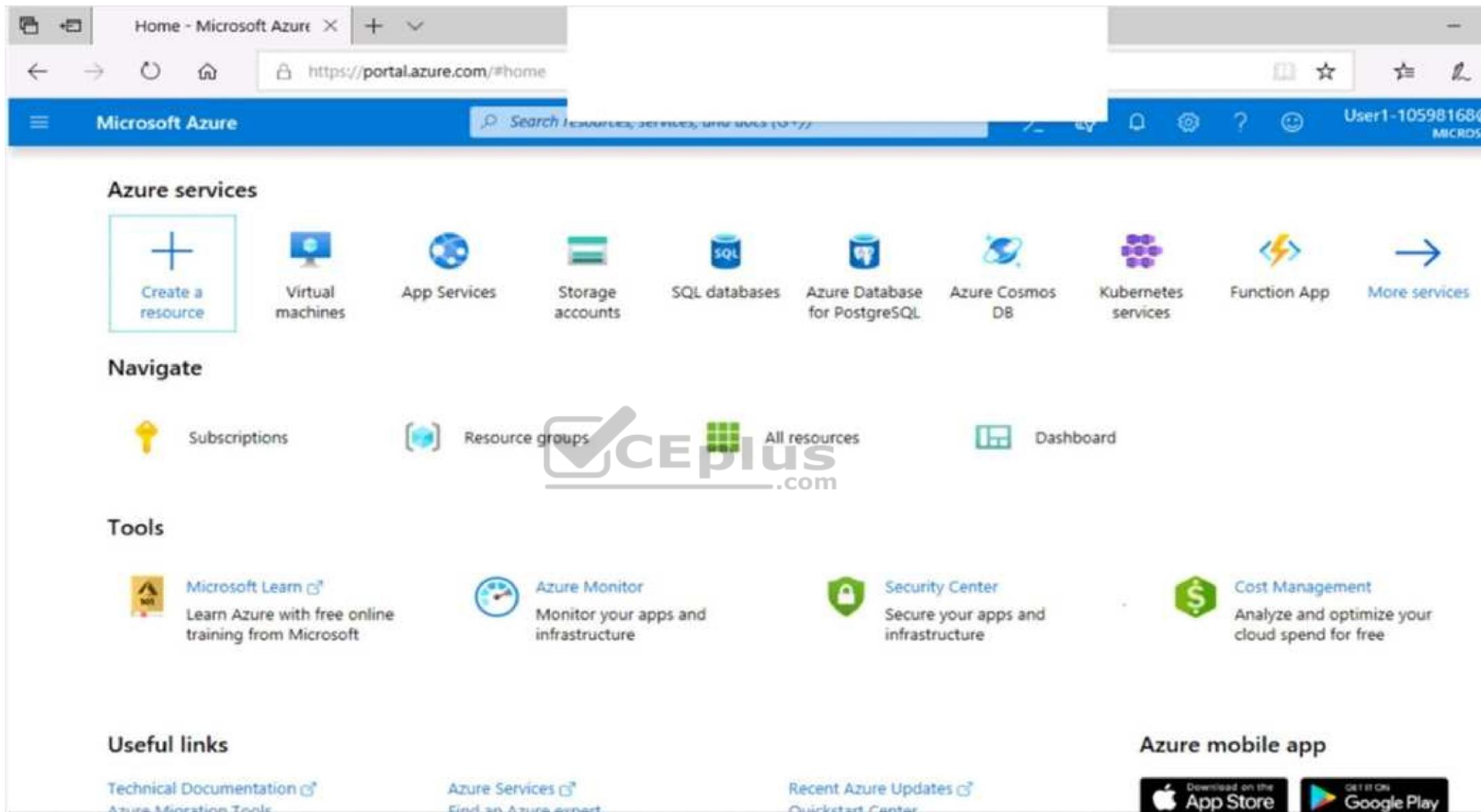
**Azure Username:** User1-10598168@ExamUsers.com

**Azure Password:** Ag1Bh9!#Bd

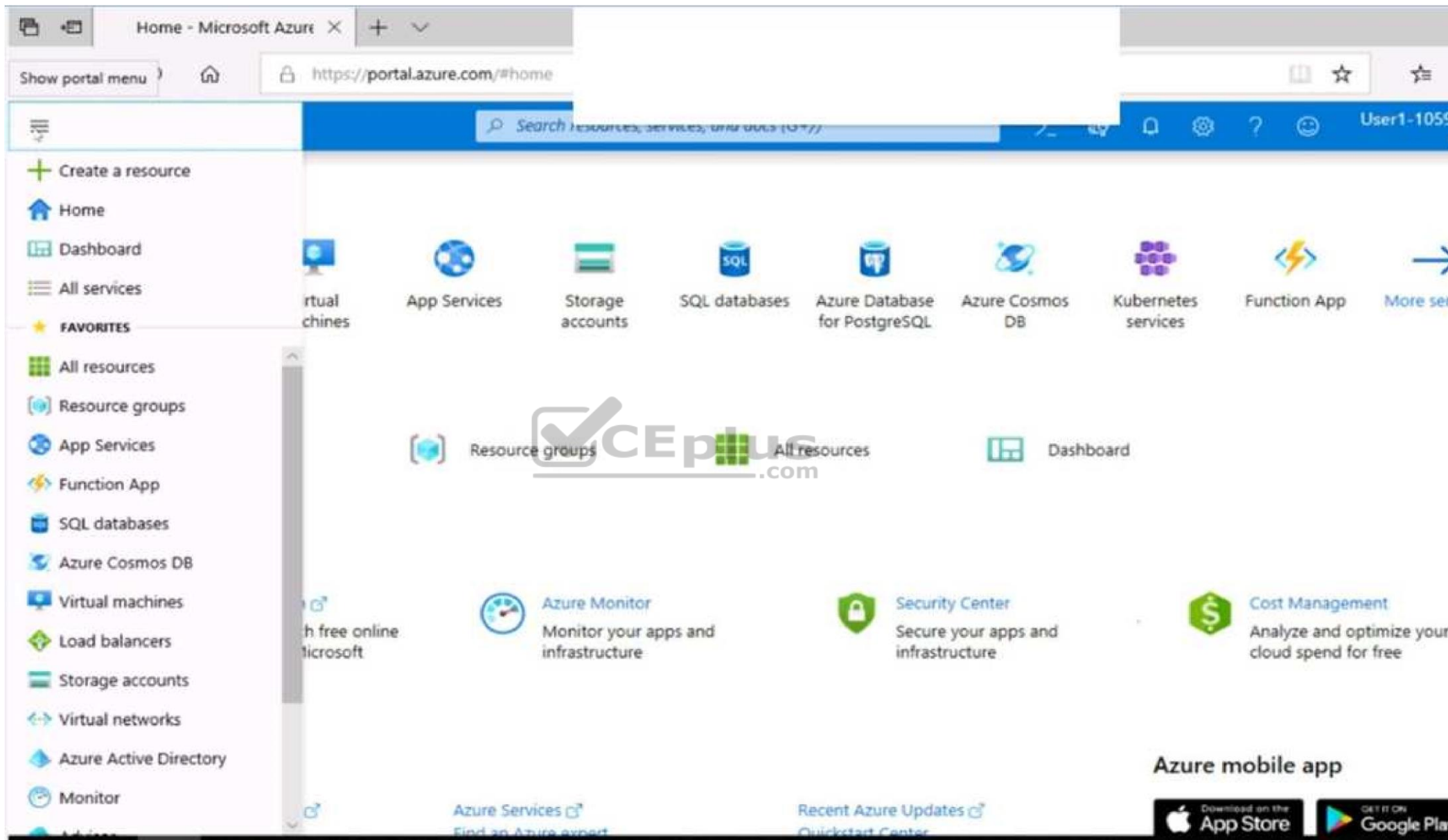
The following information is for technical support purposes only:

**Lab Instance:** 10598168



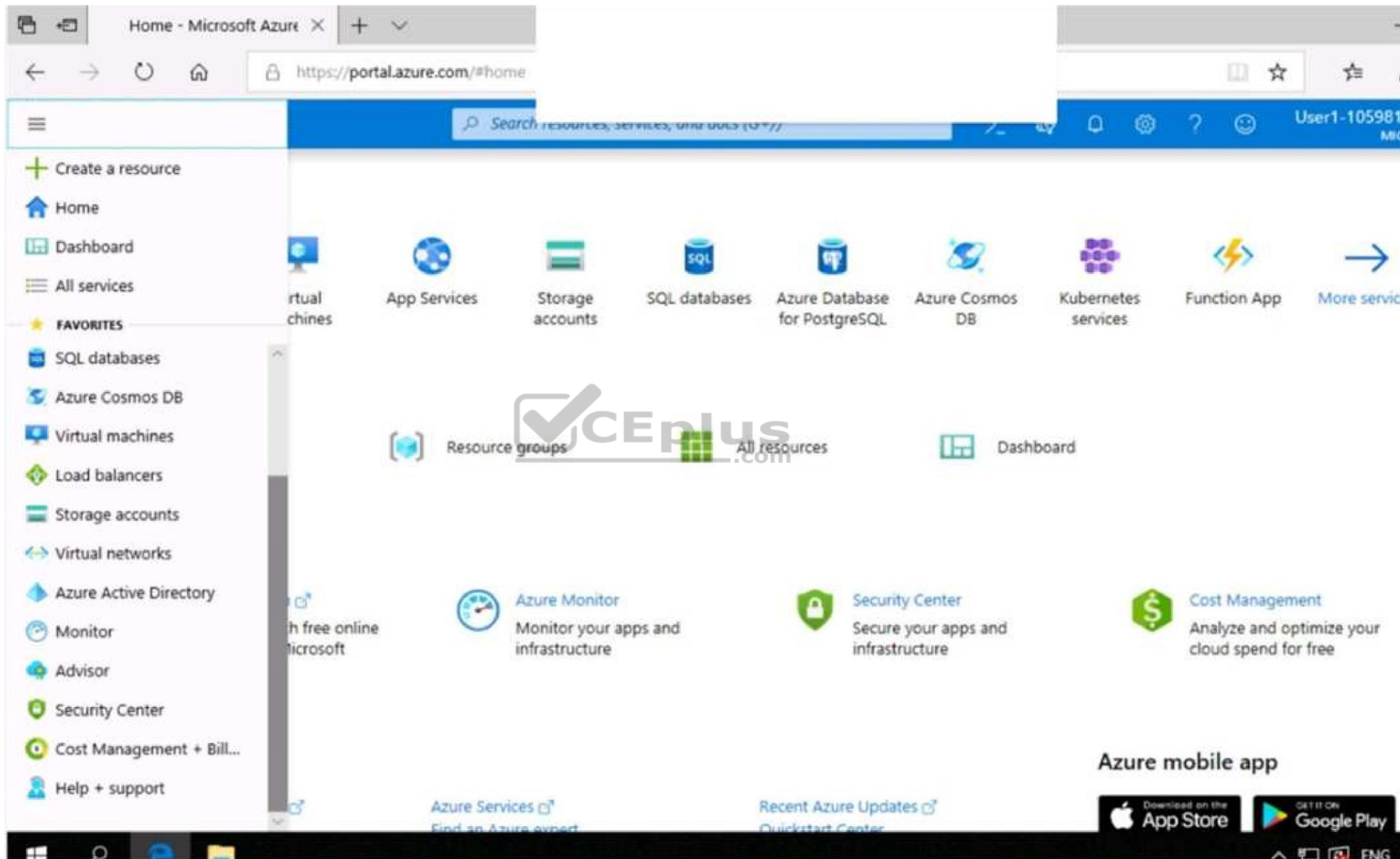


The screenshot shows the Microsoft Azure portal home page. At the top, there's a browser tab labeled 'Home - Microsoft Azure' and a search bar. Below the navigation bar, the 'Azure services' section features a grid of icons for various services: 'Create a resource' (highlighted with a blue border), 'Virtual machines', 'App Services', 'Storage accounts', 'SQL databases', 'Azure Database for PostgreSQL', 'Azure Cosmos DB', 'Kubernetes services', 'Function App', and 'More services'. The 'Navigate' section includes icons for 'Subscriptions', 'Resource groups', 'All resources', and 'Dashboard'. The 'Tools' section lists 'Microsoft Learn' (with a description: 'Learn Azure with free online training from Microsoft'), 'Azure Monitor' (with a description: 'Monitor your apps and infrastructure'), 'Security Center' (with a description: 'Secure your apps and infrastructure'), and 'Cost Management' (with a description: 'Analyze and optimize your cloud spend for free'). At the bottom, the 'Useful links' section contains 'Technical Documentation', 'Azure Services', and 'Recent Azure Updates'. On the right, there's a section for the 'Azure mobile app' with download buttons for the 'App Store' and 'Google Play'.



The image shows the Microsoft Azure portal home page. The browser tab is titled "Home - Microsoft Azure" and the address bar shows "https://portal.azure.com/#home". The left sidebar contains a navigation menu with options like "Create a resource", "Home", "Dashboard", "All services", and a "FAVORITES" section. The main area displays a grid of service tiles including "Virtual machines", "App Services", "Storage accounts", "SQL databases", "Azure Database for PostgreSQL", "Azure Cosmos DB", "Kubernetes services", and "Function App". Below these are tiles for "Resource groups", "All resources", "Dashboard", "Azure Monitor", "Security Center", and "Cost Management". The bottom of the page features a footer with "Azure mobile app" download links for the App Store and Google Play, and a "Recent Azure Updates" section.





The image shows the Microsoft Azure portal home page in a web browser. The browser tab is titled "Home - Microsoft Azure" and the address bar shows "https://portal.azure.com/#home". The page features a blue header with a search bar and user information "User1-105981". A left-hand navigation pane lists various services and favorites. The main content area displays a grid of service tiles including Virtual machines, App Services, Storage accounts, SQL databases, Azure Database for PostgreSQL, Azure Cosmos DB, Kubernetes services, and Function App. Below these are tiles for Resource groups, All resources, Dashboard, Azure Monitor, Security Center, and Cost Management. At the bottom, there are links for Azure Services, Recent Azure Updates, and mobile app download instructions for the App Store and Google Play.

Home - Microsoft Azure

https://portal.azure.com/#home

Search resources, services, and tools (0/??)

User1-105981

Create a resource

Home

Dashboard

All services

FAVORITES

SQL databases

Azure Cosmos DB

Virtual machines

Load balancers

Storage accounts

Virtual networks

Azure Active Directory

Monitor

Advisor

Security Center

Cost Management + Bill...

Help + support

Virtual machines

App Services

Storage accounts

SQL databases

Azure Database for PostgreSQL

Azure Cosmos DB

Kubernetes services

Function App

More services

Resource groups

All resources

Dashboard

Azure Monitor

Monitor your apps and infrastructure

Security Center

Secure your apps and infrastructure

Cost Management

Analyze and optimize your cloud spend for free

Azure mobile app

Download on the App Store

GET IT ON Google Play

Azure Services

Recent Azure Updates



You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.

**To complete this task, sign in to the Azure portal.**

**Correct Answer:** See the explanation below.

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

1. In the Search resources, services, and docs box at the top of the portal, begin typing the name of a virtual machine, VM1 that has a network interface that you want to add to, or remove from, an application security group.
2. When the name of your VM appears in the search results, select it.
3. Under SETTINGS, select Networking. Select Configure the application security groups, select the application security groups that you want to add the network interface to, or unselect the application security groups that you want to remove the network interface from, and then select Save.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface>

## **QUESTION 24**

### **SIMULATION**



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.

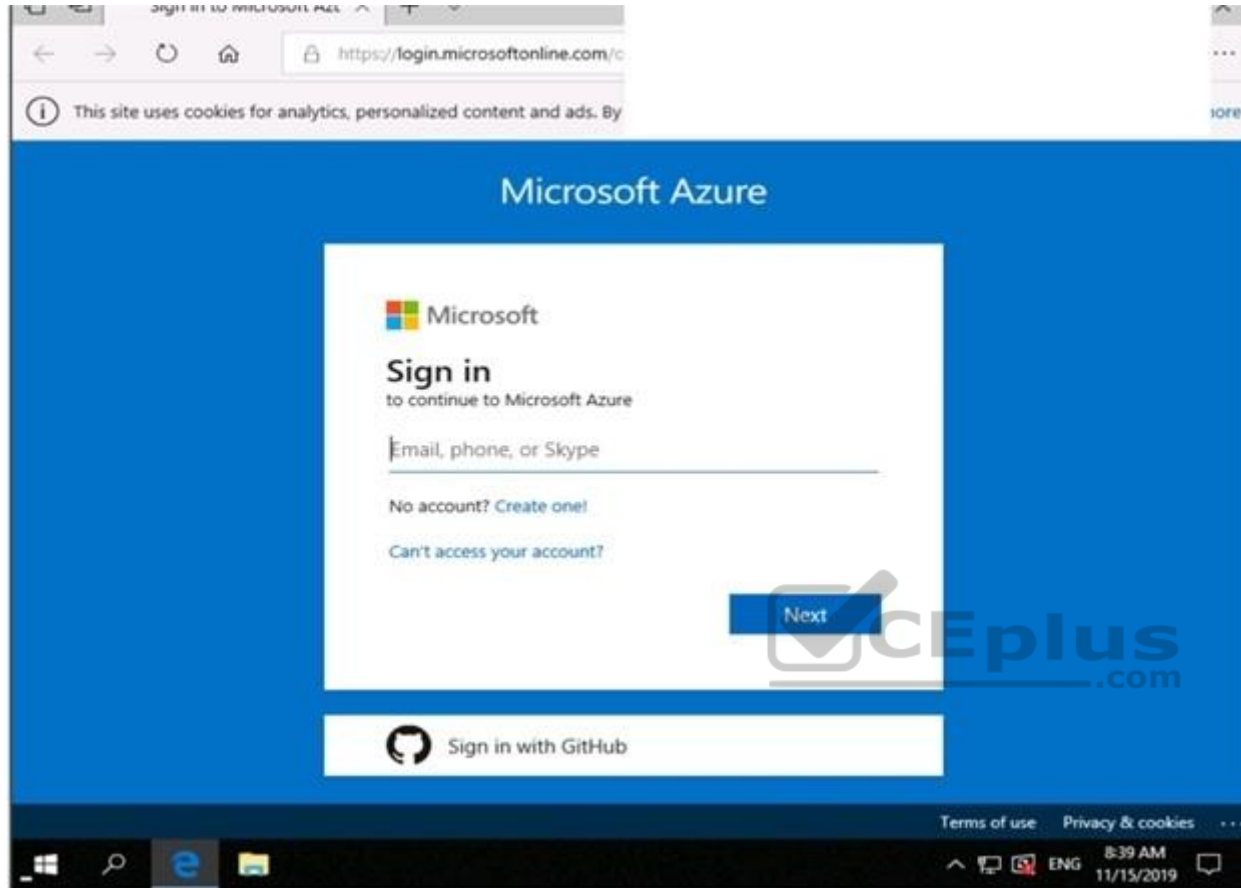
To enter your password, place your cursor in the Enter password box and click on the password below.

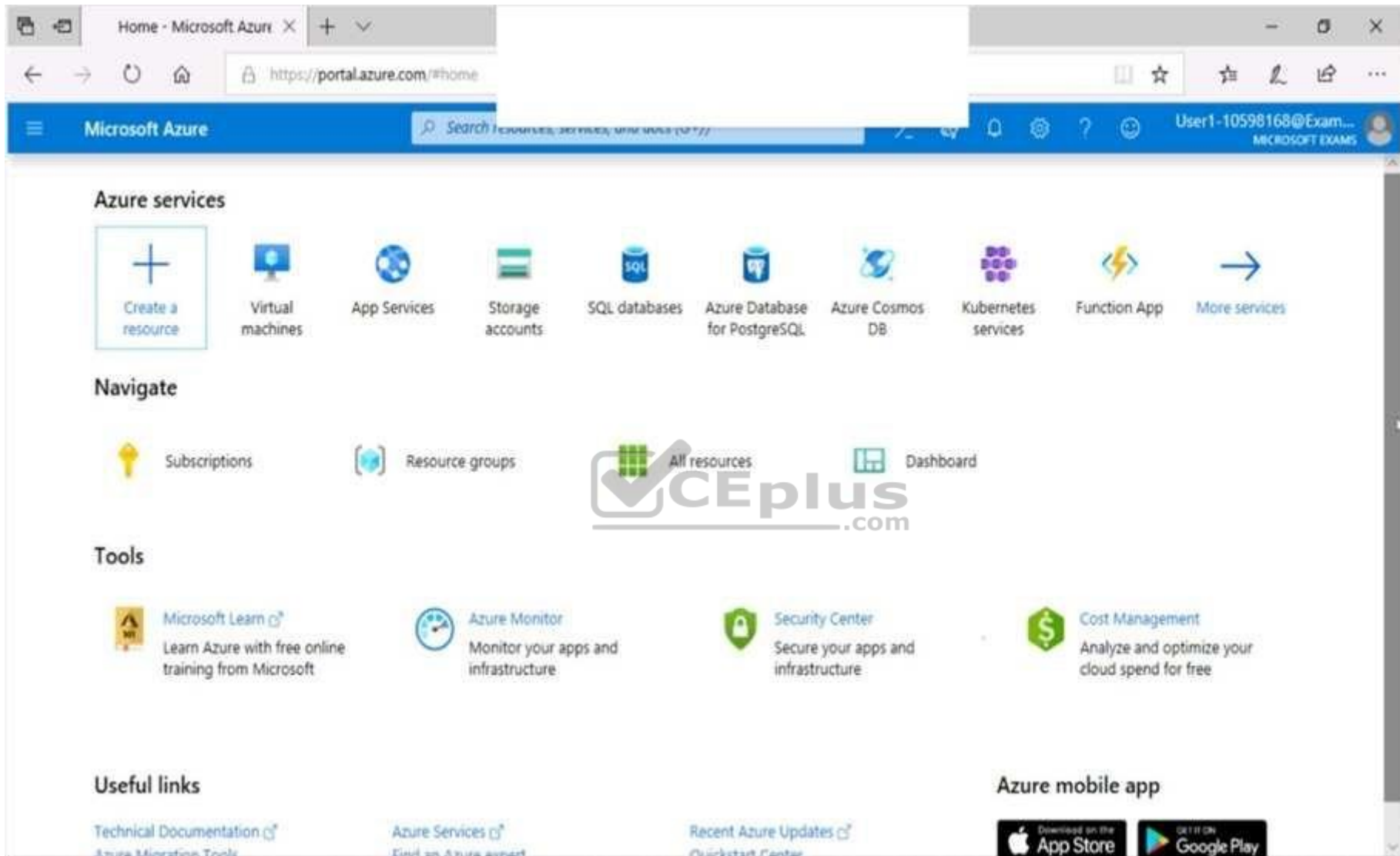
**Azure Username:** User1-10598168@ExamUsers.com

**Azure Password:** Ag1Bh9!#Bd

The following information is for technical support purposes only:

**Lab Instance:** 10598168

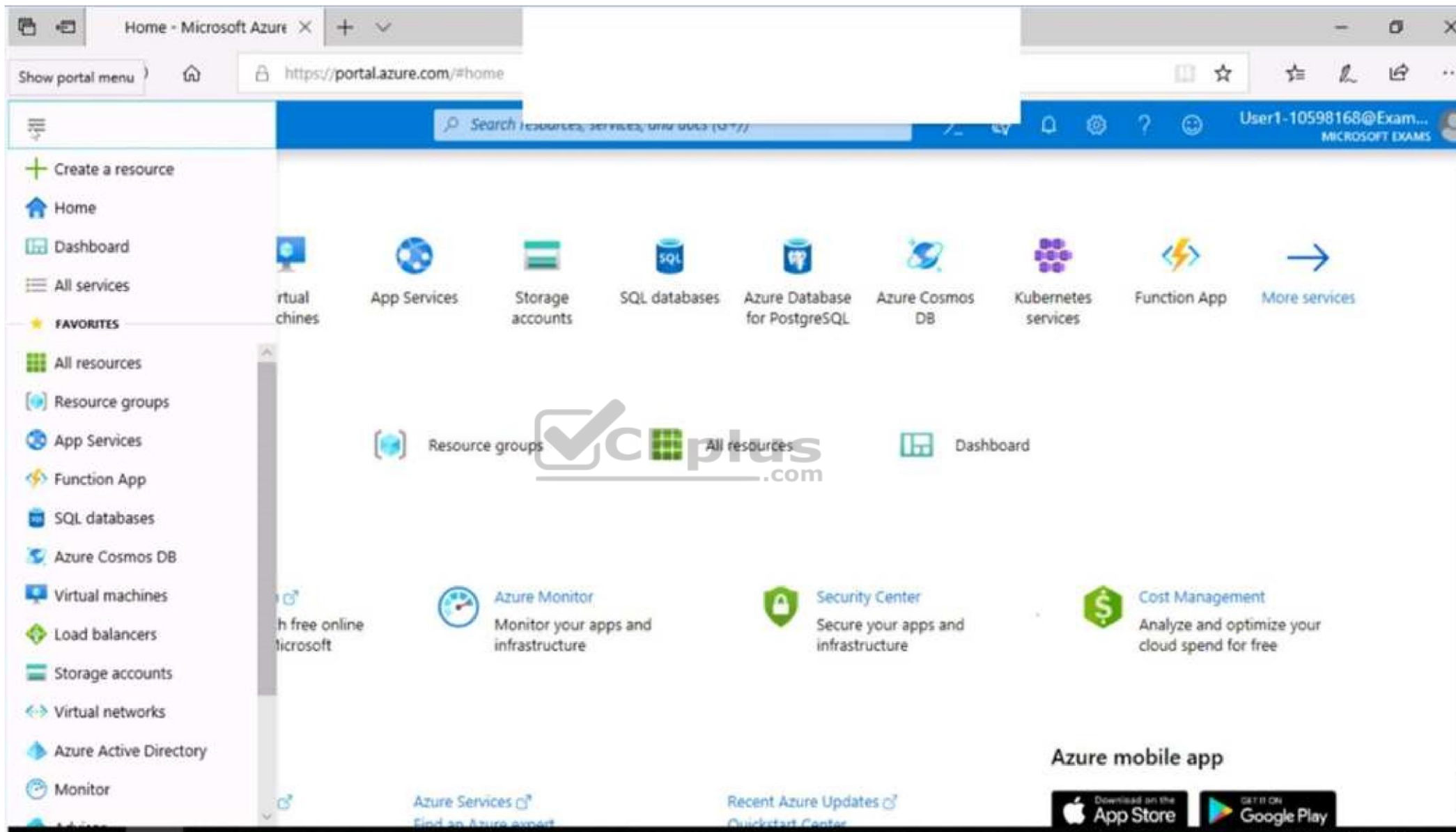











The screenshot shows the Microsoft Azure portal home page in a web browser. The browser's address bar displays <https://portal.azure.com/#home>. The page header includes the Microsoft Azure logo, a search bar, and the user's profile (User1-10598168@Exam... MICROSOFT EXAMS).

The main content area is organized into several sections:

- Azure services:** A row of icons for various services, including "Create a resource", "Virtual machines", "App Services", "Storage accounts", "SQL databases", "Azure Database for PostgreSQL", "Azure Cosmos DB", "Kubernetes services", "Function App", and "More services".
- Navigate:** A row of icons for navigation, including "Subscriptions", "Resource groups", "All resources", and "Dashboard".
- Tools:** A row of icons for tools, including "Microsoft Learn" (Learn Azure with free online training from Microsoft), "Azure Monitor" (Monitor your apps and infrastructure), "Security Center" (Secure your apps and infrastructure), and "Cost Management" (Analyze and optimize your cloud spend for free).
- Useful links:** A row of links for "Technical Documentation", "Azure Services", and "Recent Azure Updates".
- Azure mobile app:** A section at the bottom right with buttons for "Download on the App Store" and "GET IT ON Google Play".



Home - Microsoft Azure X +

Show portal menu  <https://portal.azure.com/#home>      

Search resources, services, and more (Ctrl+K)

User1-10598168@Exam...  
MICROSOFT EXAMS

**FAVORITES**

- Create a resource
- Home
- Dashboard
- All services
- All resources
- Resource groups
- App Services
- Function App
- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor

Virtual machines

App Services

Storage accounts

SQL databases

Azure Database for PostgreSQL

Azure Cosmos DB

Kubernetes services

Function App

More services

Resource groups

All resources

Dashboard

Azure Monitor  
Monitor your apps and infrastructure

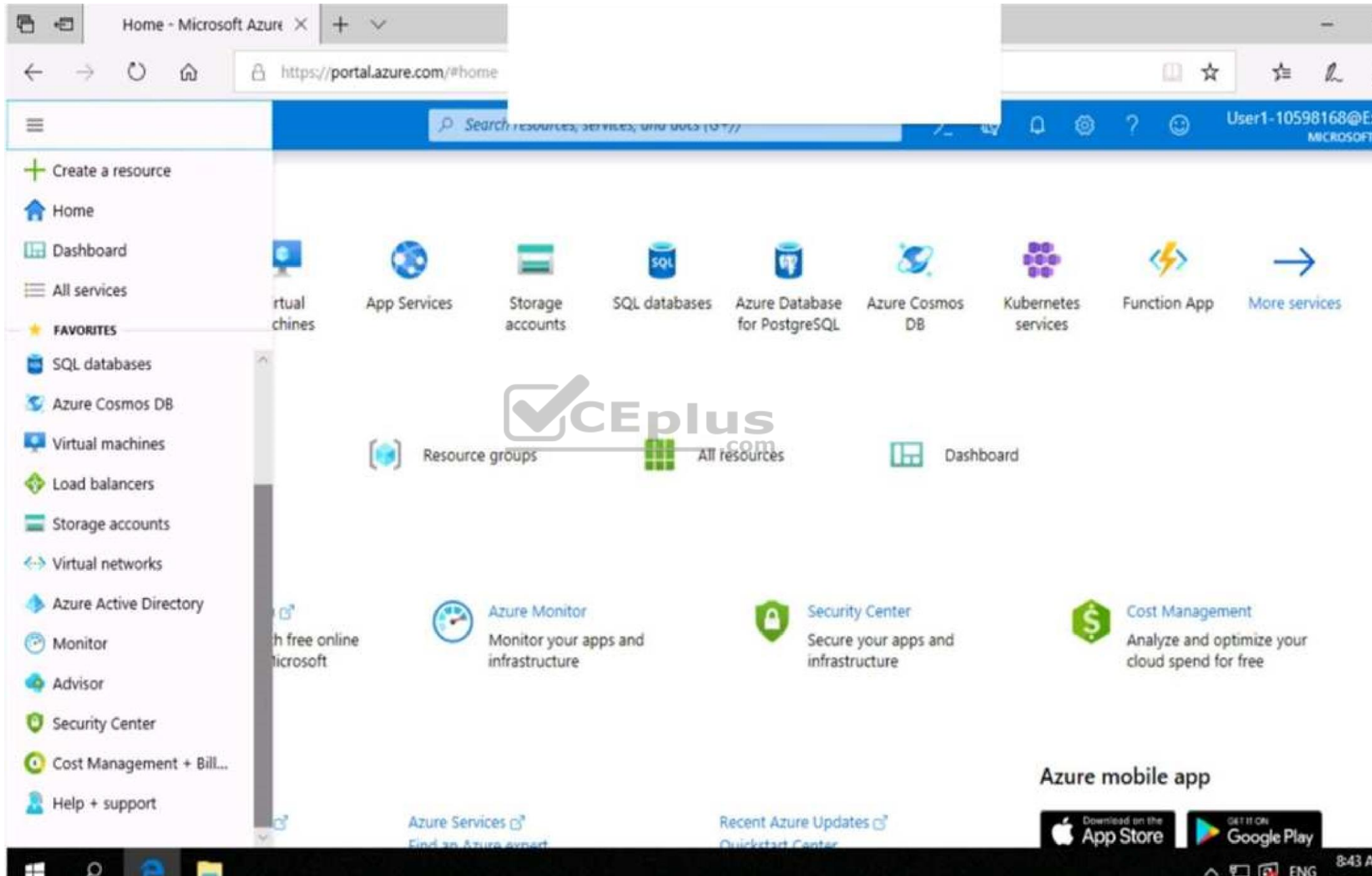
Security Center  
Secure your apps and infrastructure

Cost Management  
Analyze and optimize your cloud spend for free

Azure mobile app

Download on the App Store

GET IT ON Google Play



Home - Microsoft Azure X + -

https://portal.azure.com/#home

Search resources, services, and more (Ctrl+T)

User1-10598168@E MICROSOFT

**FAVORITES**

- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Bill...
- Help + support

Virtual machines

App Services

Storage accounts

SQL databases

Azure Database for PostgreSQL

Azure Cosmos DB

Kubernetes services

Function App

More services

Resource groups

All resources

Dashboard

Azure Monitor  
Monitor your apps and infrastructure

Security Center  
Secure your apps and infrastructure

Cost Management  
Analyze and optimize your cloud spend for free

Azure mobile app

Download on the App Store

GET IT ON Google Play

Azure Services Find an Azure expert

Recent Azure Updates Quickstart Center

You need to perform a full malware scan every Sunday at 02:00 on a virtual machine named VM1 by using Microsoft Antimalware for Virtual Machines.

**To complete this task, sign in to the Azure portal.**

**Correct Answer:** See the explanation below.

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Deploy the Microsoft Antimalware Extension using the Azure Portal for single VM deployment

1. In Azure Portal, go to the Azure VM1's blade, navigate to the Extensions section and press Add.



Dashboard > Virtual machines > devrgvm > devrg > devrgvm - Extensions

## devrgvm - Extensions

Virtual machine

Search (Ctrl+ /)

« + Add

Search to filter items...

NAME	TYPE
CustomScriptExtension	Microsoft.Compute.CustomScriptEx
DependencyAgentWindows	Microsoft.Azure.Monitoring.Depend
enablevmaccess	Microsoft.Compute.VMAccessAgen
IaaS.Diagnostics	Microsoft.Azure.Diagnostics.IaaS
MicrosoftMonitoringAgent	Microsoft.EnterpriseCloud.Monitori
SiteRecovery-Windows	Microsoft.Azure.RecoveryServices.S

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Disks

Size

Security

Extensions

2. Select the Microsoft Antimalware extension and press Create.
3. Fill the "Install extension" form as desired and press OK.

Scheduled: Enable  
Scan type: Full Scan  
day: Sunday





[Dashboard](#) > [Virtual machines](#) > [devrgvm](#) > [devrg](#) > [devrgvm - Extensions](#) > [New resource](#)

## Install extension



Excluded files and locations ⓘ

Excluded file extensions ⓘ

Excluded processes ⓘ

Real-time protection ⓘ

Enable

Disable

Run a scheduled scan ⓘ

Enable

Disable

Scan type ⓘ

Quick

Full

Scan day ⓘ

Saturday



Scan time ⓘ

120



Reference:

<https://www.e-apostolidis.gr/microsoft/azure/azure-vm-antimalware-extension-management/>



## Testlet 1

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

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

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

### To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question. **Overview**

Litware, Inc. is a digital media company that has 500 employees in the Chicago area and 20 employees in the San Francisco area.

### Existing Environment

Litware has an Azure subscription named Sub1 that has a subscription ID of 43894a43-17c2-4a39-8cfc-3540c2653ef4.

Sub1 is associated to an Azure Active Directory (Azure AD) tenant named litwareinc.com. The tenant contains the user objects and the device objects of all the Litware employees and their devices. Each user is assigned an Azure AD Premium P2 license. Azure AD Privileged Identity Management (PIM) is activated.

The tenant contains the groups shown in the following table.

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.
Group2	Security group	A group that has the Dynamic User membership type and contains the Chicago IT team

The Azure subscription contains the objects shown in the following table.

Name	Type	Description
VNet1	Virtual network	VNet1 is a virtual network that contains security-sensitive IT resources. VNet1 contains three subnets named Subnet0, Subnet1, and AzureFirewallSubnet.
VM0	Virtual machine	VM0 is an Azure virtual machine that runs Windows Server 2016, connects to Subnet0, and has just in time (JIT) VM access configured.
VM1	Virtual machine	VM1 is an Azure virtual machine that runs Windows Server 2016 and connects to Subnet0.
SQLDB1	Azure SQL Database	SQLDB1 is an Azure SQL database on a SQL Database server named LitwareSQLServer1.
WebApp1	Web app	WebApp1 is an Azure web app that is accessible by using <a href="https://litwareinc.com">https://litwareinc.com</a> and <a href="http://www.litwareinc.com">http://www.litwareinc.com</a> .
Resource Group1	Resource group	Resource Group1 is a resource group that contains VNet1, VM0, and VM1.
Resource Group2	Resource group	Resource Group2 is a resource group that contains shared IT resources.

Azure Security Center is set to the Free tier.

### Planned changes

Litware plans to deploy the Azure resources shown in the following table.

Name	Type	Description
Firewall1	Azure Firewall	An Azure firewall on VNet1.
RT1	Route table	A route table that will contain a route pointing to Firewall1 as the default gateway and will be assigned to Subnet0.
AKS1	Azure Kubernetes Service (AKS)	A managed AKS cluster

### Identity and Access Requirements

Litware identifies the following identity and access requirements:

- All San Francisco users and their devices must be members of Group1.
- The members of Group2 must be assigned the Contributor role to Resource Group2 by using a permanent eligible assignment.
- Users must be prevented from registering applications in Azure AD and from consenting to applications that access company information on the users' behalf.

### Platform Protection Requirements

Litware identifies the following platform protection requirements:

- Microsoft Antimalware must be installed on the virtual machines in Resource Group1.
- The members of Group2 must be assigned the Azure Kubernetes Service Cluster Admin Role.
- Azure AD users must be able to authenticate to AKS1 by using their Azure AD credentials.
- Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.
- A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

### Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

### Data and Application Requirements

Litware identifies the following data and applications requirements:

- The users in Group2 must be able to authenticate to SQLDB1 by using their Azure AD credentials.
- WebApp1 must enforce mutual authentication.

### General Requirements

Litware identifies the following general requirements:

- Whenever possible, administrative effort must be minimized.

- Whenever possible, use of automation must be minimized.

### QUESTION 1

You need to ensure that you can meet the security operations requirements.

What should you do first?

- A. Turn on Auto Provisioning in Security Center.
- B. Integrate Security Center and Microsoft Cloud App Security.
- C. Upgrade the pricing tier of Security Center to Standard.
- D. Modify the Security Center workspace configuration.

**Correct Answer: C**

**Section: [none]**

**Explanation**

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

Explanation:

The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.

Scenario: Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.



<https://vceplus.com/>

References:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-pricing>

### Question Set 2

**QUESTION 1**

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

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning.

You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Log Analytics agent installed?

- A. VM3 only
- B. VM1 and VM3 only
- C. VM3 and VM4 only
- D. VM1, VM2, VM3, and VM4

**Correct Answer: D**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803

Reference: <https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

## QUESTION 2

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.

You need to create a custom sensitivity label.

What should you do?

- A. Create a custom sensitive information type.
- B. Elevate access for global administrators in Azure AD.
- C. Change Azure Security Center to use Standard-tier pricing.
- D. Enable integration with Microsoft Cloud App Security.

**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

First, you need to create a new sensitive information type because you can't directly modify the default rules.

References: <https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type>

## QUESTION 3

You have an Azure subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts.

What should you use to modify Play1?

- A. Azure DevOps
- B. Azure Application Insights
- C. Azure Monitor
- D. Azure Logic Apps Designer



**Correct Answer:** D

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.

References: <https://docs.microsoft.com/en-us/azure/security-center/security-center-playbooks>

#### **QUESTION 4**

You create a new Azure subscription.

You need to ensure that you can create custom alert rules in Azure Security Center.

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

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

- A. Onboard Azure Active Directory (Azure AD) Identity Protection.
- B. Create an Azure Storage account.
- C. Implement Azure Advisor recommendations.
- D. Create an Azure Log Analytics workspace.
- E. Upgrade the pricing tier of Security Center to Standard.

**Correct Answer:** BD

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

D: You need write permission in the workspace that you select to store your custom alert.

References:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-custom-alert>

#### **QUESTION 5**

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.

You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:

- Alert rules must support dimensions.
- The time it takes to generate an alert must be minimized.
- Alert notifications must be generated only once when the alert is generated and once when the alert is resolved.

Which signal type should you use when you create the alert rules?

- A. Log
- B. Log (Saved Query)
- C. Metric
- D. Activity Log

**Correct Answer: C**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.

Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.

References: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric>

## **QUESTION 6**

**DRAG DROP**

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.

You plan to add the System Update Assessment solution to LAW1.

You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.

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

**Select and Place:**

Actions	Answer Area
Create a new workspace.	
Apply the scope configuration to the solution.	
Create a scope configuration.	
Create a computer group.	
Create a data source.	

**Correct Answer:**

Actions	Answer Area
Create a new workspace.	Create a computer group.
	Create a scope configuration.
	Apply the scope configuration to the solution.
Create a data source.	

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Reference: <https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting>

### QUESTION 7

You have an Azure subscription named Sub1 that contains the virtual machines shown in the following table.

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access.

What should you configure?

- A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- B. an application security group
- C. Azure Active Directory (Azure AD) conditional access
- D. just in time (JIT) VM access

**Correct Answer: D**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.

When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time>

### QUESTION 8

You are troubleshooting a security issue for an Azure Storage account.

You enable the diagnostic logs for the storage account.

What should you use to retrieve the diagnostics logs?

- A. the Security & Compliance admin center
- B. SQL query editor in Azure
- C. File Explorer in Windows
- D. AzCopy

**Correct Answer:** D

**Section:** [none]

**Explanation**

**Explanation/Reference:**

References: <https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

### QUESTION 9

HOTSPOT

You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service.

Which tool can you use to access the contents in Container1 and Share1 by using the SAS? To answer, select the appropriate options in the answer area.

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

Hot Area:

### Answer Area

Tools for Container1: 

	▼
Robocopy.exe	
Azure Storage Explorer	
File Explorer	

Tools for Share1: 

	▼
Robocopy.exe	
Azure Storage Explorer	
File Explorer	

Correct Answer:



## Answer Area

Tools for Container1:

	▼
Robocopy.exe	
Azure Storage Explorer	
File Explorer	

Tools for Share1:

	▼
Robocopy.exe	
Azure Storage Explorer	
File Explorer	

Section: [none]

Explanation

Explanation/Reference:

### QUESTION 10

You have an Azure Storage account named storage1 that has a container named container1.

You need to prevent the blobs in container1 from being modified.

What should you do?

- A. From container1, change the access level.
- B. From container1, add an access policy.
- C. From container1, modify the Access Control (IAM) settings.
- D. From storage1, enable soft delete for blobs.

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

References: <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage?tabs=azure-portal>

#### **QUESTION 11**

You company has an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to create several security alerts by using Azure Monitor.

You need to prepare the Azure subscription for the alerts.

What should you create first?

- A. An Azure Storage account
- B. an Azure Log Analytics workspace
- C. an Azure event hub
- D. an Azure Automation account



**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

#### **QUESTION 12**

You company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights. WebApp1 requires users to authenticate by using OAuth 2.0 client secrets.

Developers at the company plan to create a multi-step web test app that preforms synthetic transactions emulating user traffic to Web App1.

You need to ensure that web tests can run unattended.

What should you do first?

- A. In Microsoft Visual Studio, modify the .webtest file.



- B. Upload the .webtest file to Application Insights.
- C. Register the web test app in Azure AD.
- D. Add a plug-in to the web test app.

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

### QUESTION 13

You are troubleshooting a security issue for an Azure Storage account.

You enable the diagnostic logs for the storage account.

What should you use to retrieve the diagnostics logs?

- A. the Security & Compliance admin center
- B. Azure Security Center
- C. Azure Cosmos DB explorer
- D. AzCopy



**Correct Answer:** D

**Section:** [none]

**Explanation**

**Explanation/Reference:**

### QUESTION 14

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

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning.

You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Microsoft Monitoring agent installed?

- A. VM3 only
- B. VM1 and VM3 only
- C. VM3 and VM4 only
- D. VM1, VM2, VM3, and VM4

**Correct Answer:** D

**Section:** [none]

**Explanation**



**Explanation/Reference:**

Explanation:

When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803.

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-faq>

## Question Set 1

### QUESTION 1

You have an Azure web app named webapp1.

You need to configure continuous deployment for webapp1 by using an Azure Repo.

What should you create first?

- A. an Azure Application Insights service
- B. an Azure DevOps organization
- C. an Azure Storage account
- D. an Azure DevTest Labs lab

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

To use Azure Repos, make sure your Azure DevOps organization is linked to your Azure subscription.

Reference: <https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment>

## QUESTION 2

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

The company develops an application named App1. App1 is registered in Azure AD.

You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users.

What should you configure?

- A. an application permission without admin consent
- B. a delegated permission without admin consent
- C. a delegated permission that requires admin consent
- D. an application permission that requires admin consent

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Delegated permissions - Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.

Incorrect Answers:

A, D: Application permissions - Your client application needs to access the web API directly as itself (no user context). This type of permission requires administrator consent and is also not available for public (desktop and mobile) client applications.

References: <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis>

### QUESTION 3

#### DRAG DROP

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.

You need to delegate the minimum required permissions to App1.

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

Select and Place:

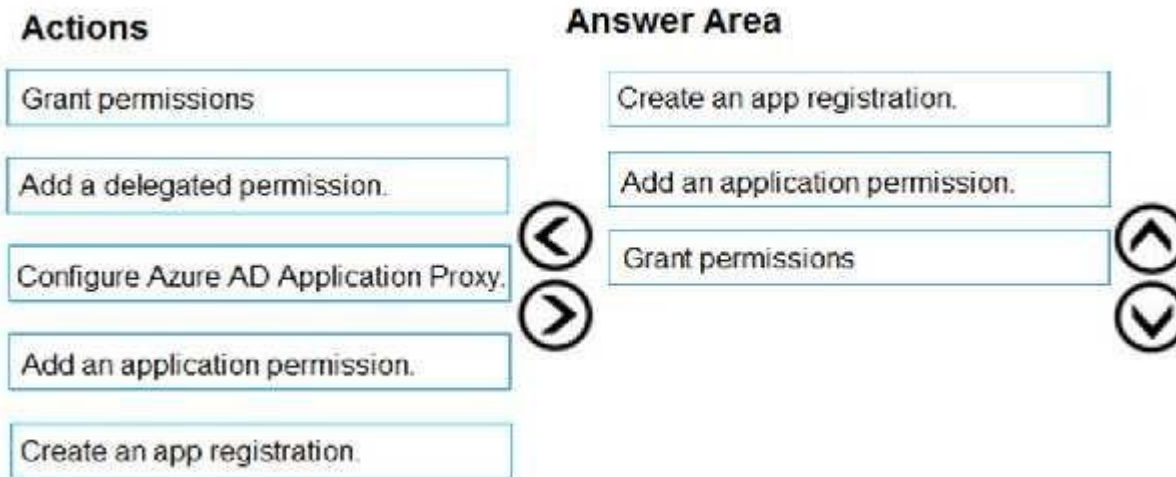


The interface shows a list of actions on the left and an answer area on the right. The actions are:

- Grant permissions
- Add a delegated permission.
- Configure Azure AD Application Proxy.
- Add an application permission.
- Create an app registration.

The answer area is empty. Navigation arrows are present between the actions and the answer area.

Correct Answer:



**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Step 1: Create an app registration

First the application must be created/registered.

Step 2: Add an application permission

Application permissions are used by apps that run without a signed-in user present.

Step 3: Grant permissions

Incorrect Answers:

Delegated permission

Delegated permissions are used by apps that have a signed-in user present.

Application Proxy:

Azure Active Directory's Application Proxy provides secure remote access to on-premises web applications.

References: <https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent>

**QUESTION 4**

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com.

The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.

You need to register App1 in Azure AD.

What information should you obtain from the developer to register the application?

- A. a redirect URI
- B. a reply URL
- C. a key
- D. an application ID

**Correct Answer: A**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.

References: <https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code>

**QUESTION 5**

From the Azure portal, you are configuring an Azure policy.

You plan to assign policies that use the `DeployIfNotExist`, `AuditIfNotExist`, `Append`, and `Deny` effects.

Which effect requires a managed identity for the assignment?

- A. `AuditIfNotExist`
- B. `Append`
- C. `DeployIfNotExist`
- D. `Deny`

**Correct Answer: C**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.

References: <https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources>

### **QUESTION 6**

You have an Azure subscription that contains an Azure key vault named Vault1.

In Vault1, you create a secret named Secret1.

An application developer registers an application in Azure Active Directory (Azure AD).

You need to ensure that the application can use Secret1.

What should you do?

- A. In Azure AD, create a role.
- B. In Azure Key Vault, create a key.
- C. In Azure Key Vault, create an access policy.
- D. In Azure AD, enable Azure AD Application Proxy.

**Correct Answer: A**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

Azure Key Vault provides a way to securely store credentials and other keys and secrets, but your code needs to authenticate to Key Vault to retrieve them.

Managed identities for Azure resources overview makes solving this problem simpler, by giving Azure services an automatically managed identity in Azure Active Directory (Azure AD). You can use this identity to authenticate to any service that supports Azure AD authentication, including Key Vault, without having any credentials in your code.

Example: How a system-assigned managed identity works with an Azure VM



After the VM has an identity, use the service principal information to grant the VM access to Azure resources. To call Azure Resource Manager, use role-based access control (RBAC) in Azure AD to assign the appropriate role to the VM service principal. To call Key Vault, grant your code access to the specific secret or key in Key Vault.

References: <https://docs.microsoft.com/en-us/azure/key-vault/quick-create-net>  
<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

### QUESTION 7

You have an Azure SQL database.

You implement Always Encrypted.

You need to ensure that application developers can retrieve and decrypt data in the database.

Which two pieces of information should you provide to the developers? Each correct answer presents part of the solution.

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

- A. a stored access policy
- B. a shared access signature (SAS)
- C. the column encryption key
- D. user credentials
- E. the column master key



**Correct Answer:** CE

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.

References: <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine>

### QUESTION 8

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



All users have computers that run Windows 10 and are hybrid Azure AD joined.

You have an Azure SQL database that is configured to support Azure AD authentication.

Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account.

You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.

Which authentication method should you instruct the developers to use?

- A. SQL Login
- B. Active Directory – Universal with MFA support
- C. Active Directory – Integrated
- D. Active Directory – Password

**Correct Answer:** C

**Section:** [none]

**Explanation**



**Explanation/Reference:**

Explanation:

Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.

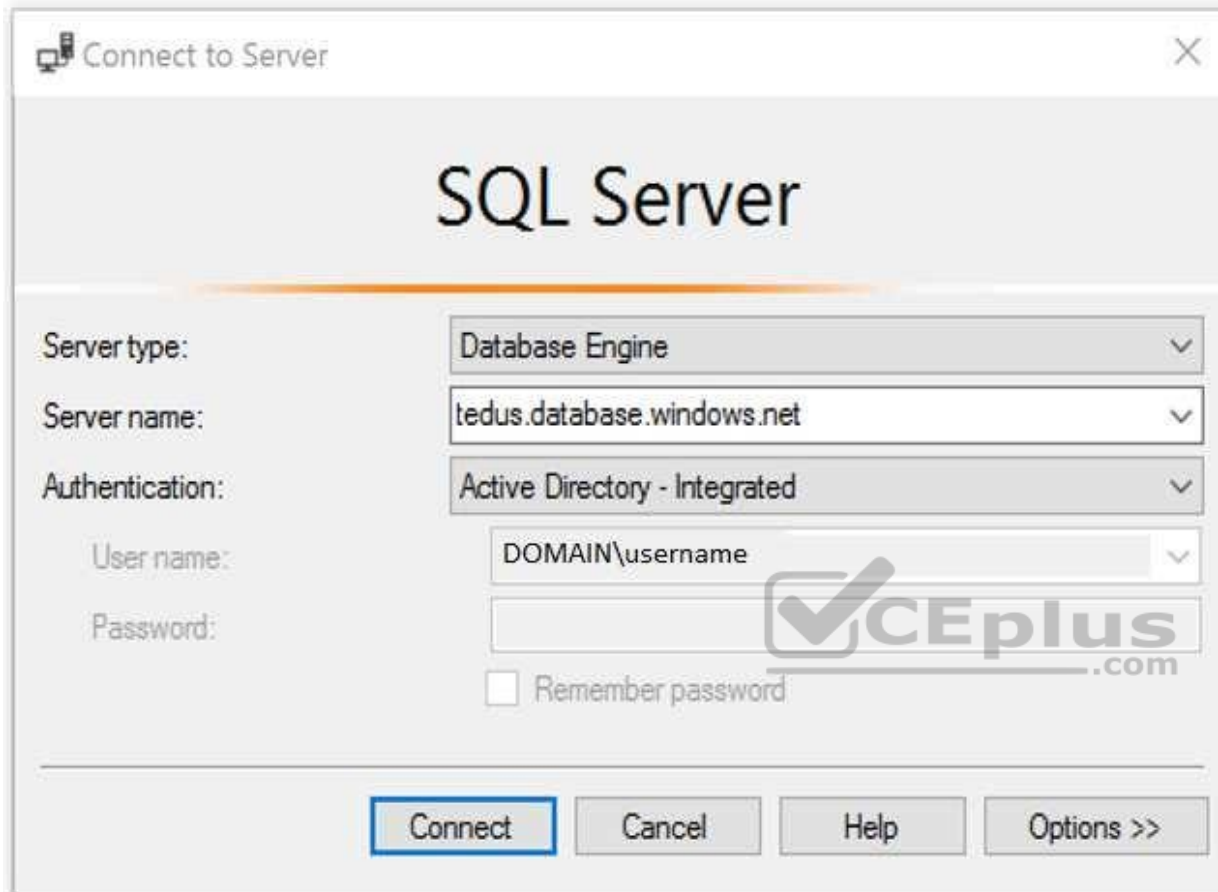
Using an Azure AD identity to connect using SSMS or SSDT

The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.

Active Directory integrated authentication

Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.



2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to. (The AD domain name or tenant ID" option is only supported for Universal with MFA connection options, otherwise it is greyed out.)

References: <https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication-configure.md>

### QUESTION 9

You have an Azure SQL Database server named SQL1.

You turn on Advanced Threat Protection for SQL1 to detect all threat detection types.

Which action will Advanced Threat Protection detect as a threat?

- A. A user updates more than 50 percent of the records in a table.
- B. A user attempts to sign in as `SELECT * FROM table1`.
- C. A user is added to the db\_owner database role.
- D. A user deletes more than 100 records from the same table.

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.

References: <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview>

#### QUESTION 10

##### HOTSPOT

You have the Azure Information Protection labels as shown in the following table.

Name	Use condition	Label is applied	Pattern	Case sensitivity
Label1	Condition1	Automatically	White	On
Label2	Condition2	Automatically	Black	Off

You have the Azure Information Protection policies as shown in the following table.

Name	Applies to	Use label	Set the default label
Global	<i>Not applicable</i>	<i>None</i>	None
Policy1	User1	Label1	None
Policy2	User1	Label2	None

You need to identify how Azure Information Protection will label files.

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

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

Hot Area:

### Answer Area

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

Correct Answer:



## Answer Area

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

	▼
No label	
Label1 only	
Label2 only	
Label1 and Label2	

Section: [none]

Explanation

Explanation/Reference:

Explanation:

Box 1: Label 2 only

How multiple conditions are evaluated when they apply to more than one label

1. The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).
2. The most sensitive label is applied.
3. The last sublabel is applied.

Box 2: No Label

Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad.

References:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

**QUESTION 11**

Your company uses Azure DevOps.

You need to recommend a method to validate whether the code meets the company's quality standards and code review standards.

What should you recommend implementing in Azure DevOps?

- A. branch folders
- B. branch permissions
- C. branch policies
- D. branch locking

**Correct Answer: C**

**Section: [none]**

**Explanation**

**Explanation/Reference:**

Explanation:

Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.

References: <https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azure-devops&viewFallbackFrom=vsts>

**QUESTION 12**

You have an Azure subscription that contains a virtual machine named VM1.

You create an Azure key vault that has the following configurations:

- Name: Vault5
- Region: West US
- Resource group: RG1

You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing up VM1 by using Azure Backup.

Which key vault settings should you configure?

- A. Access policies
- B. Secrets
- C. Keys
- D. Locks

**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

References: <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

### QUESTION 13

You have an Azure subscription named Sub1 that contains the resources shown in the following table.

Name	Type	Region	Resource group
Sa1	Azure Storage account	East US	RG1
VM1	Azure virtual machine	East US	RG 2
KV1	Azure key vault	East US 2	RG1
SQL1	Azure SQL database	East US 2	RG 2

You need to ensure that you can provide VM1 with secure access to a database on SQL1 by using a contained database user.

What should you do?

- A. Enable a managed service identity on VM1.
- B. Create a secret in KV1.
- C. Configure a service endpoint on SQL1.
- D. Create a key in KV1.

**Correct Answer:** B

**Section:** [none]

**Explanation**

**Explanation/Reference:**

### QUESTION 14

You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table:

Name	Region	Resource group
Vault1	West Europe	RG1
Vault2	East US	RG1
Vault3	West Europe	RG2
Vault4	East US	RG2

In Sub1, you create a virtual machine that has the following configurations:

- Name: VM1
- Size: DS2v2
- Resource group: RG1
- Region: West Europe
- Operating system: Windows Server 2016

You plan to enable Azure Disk Encryption on VM1.

In which key vaults can you store the encryption key for VM1?

- A. Vault1 or Vault3 only
- B. Vault1, Vault2, Vault3, or Vault4
- C. Vault1 only
- D. Vault1 or Vault2 only

**Correct Answer:** A

**Section:** [none]

**Explanation**

**Explanation/Reference:**

Explanation:

In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.

Reference:

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



**QUESTION 15**  
**SIMULATION**

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.

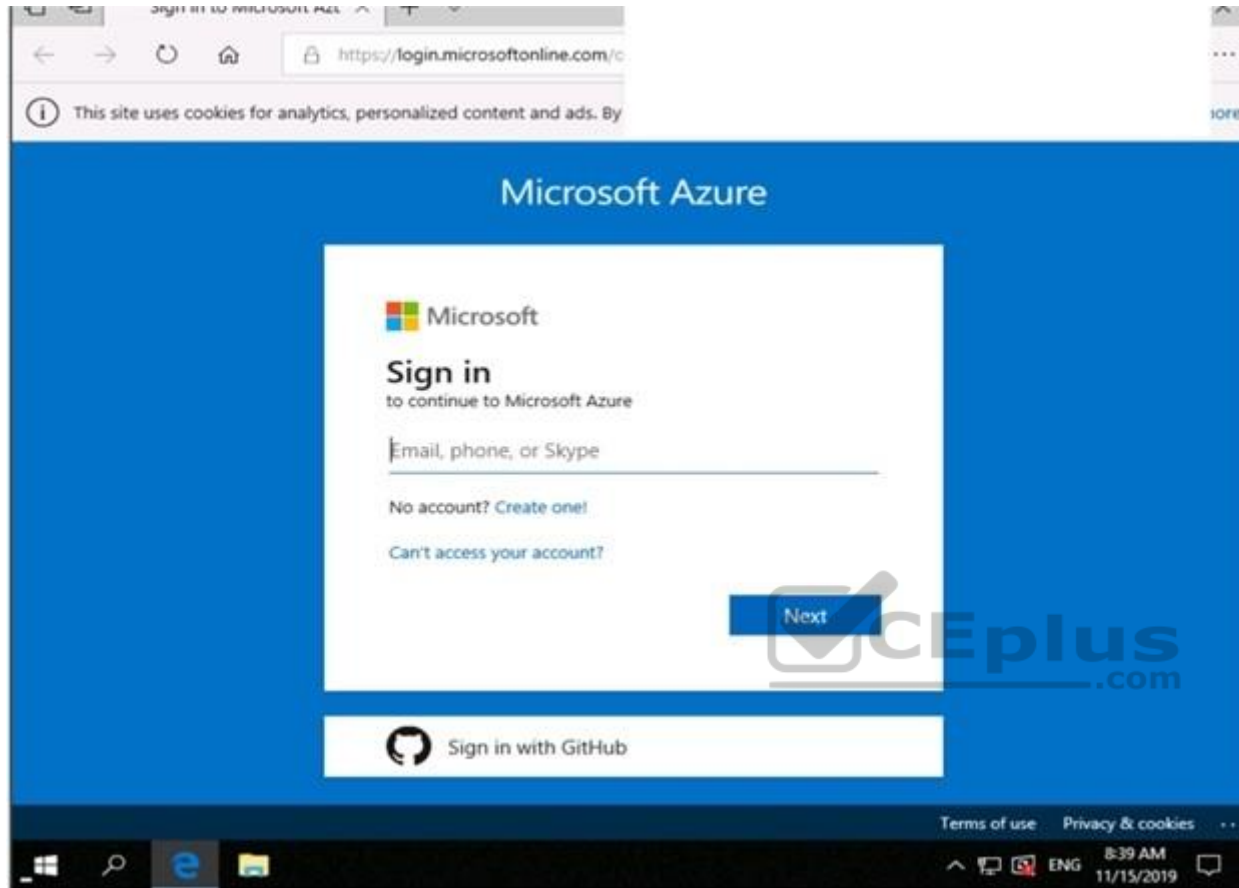
**Azure Username:** User1-10598168@ExamUsers.com

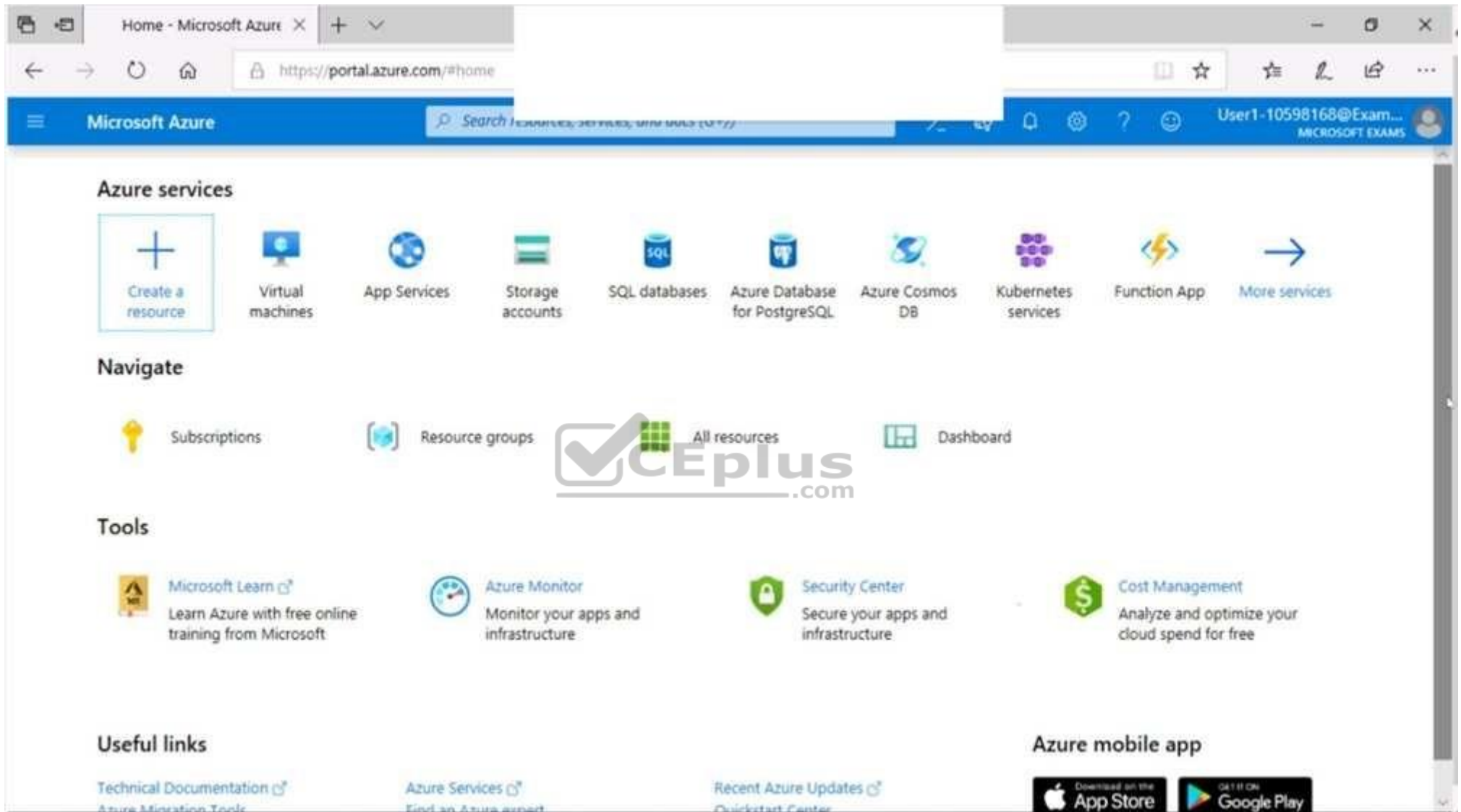
**Azure Password:** Ag1Bh9!#Bd

The following information is for technical support purposes only:

**Lab Instance:** 10598168







The screenshot shows the Microsoft Azure portal home page in a web browser. The browser tab is titled "Home - Microsoft Azure" and the address bar shows "https://portal.azure.com/#home". The page has a blue header with the "Microsoft Azure" logo, a search bar, and a user profile for "User1-10598168@Exam...".

**Azure services**

- Create a resource
- Virtual machines
- App Services
- Storage accounts
- SQL databases
- Azure Database for PostgreSQL
- Azure Cosmos DB
- Kubernetes services
- Function App
- More services

**Navigate**

- Subscriptions
- Resource groups
- All resources
- Dashboard

**Tools**

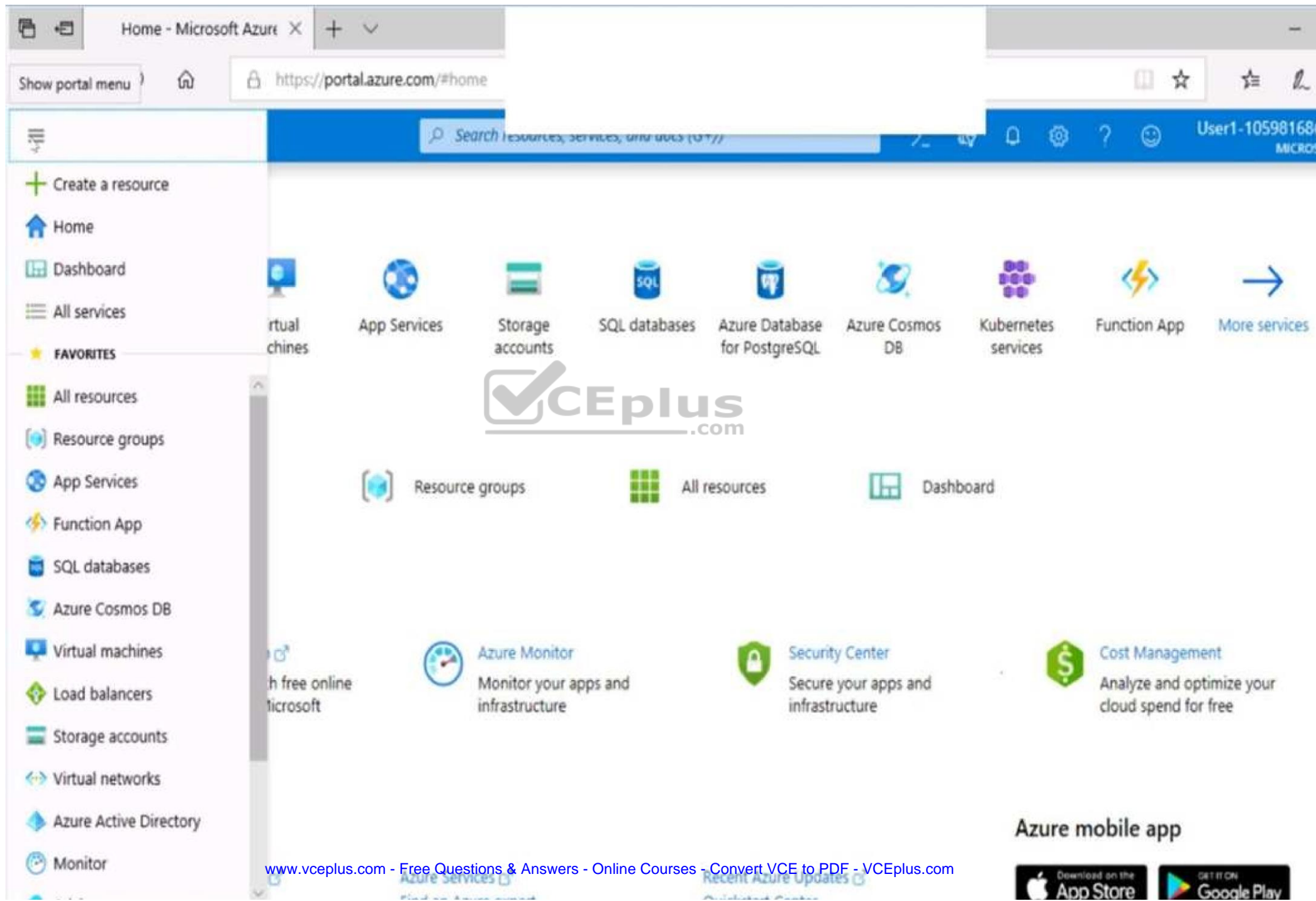
- Microsoft Learn: Learn Azure with free online training from Microsoft
- Azure Monitor: Monitor your apps and infrastructure
- Security Center: Secure your apps and infrastructure
- Cost Management: Analyze and optimize your cloud spend for free

**Useful links**






- Technical Documentation
- Azure Migration Tools
- Azure Services: Find an Azure expert
- Recent Azure Updates
- Quickstart Center







**Azure mobile app**


- Download on the App Store
- GET IT ON Google Play





Home - Microsoft Azure X + -


Show portal menu  <https://portal.azure.com/#home>    


 Search resources, services, and docs (0/77)      User1-10598168 MICROSOFT


 Create a resource


 Home


 Dashboard


 All services


 FAVORITES


 All resources


 Resource groups


 App Services


 Function App


 SQL databases


 Azure Cosmos DB


 Virtual machines

 Load balancers

 Storage accounts

 Virtual networks

 Azure Active Directory

 Monitor

Virtual machines

App Services

Storage accounts

SQL databases


Azure Database for PostgreSQL


Azure Cosmos DB


Kubernetes services


Function App


More services


 Resource groups

 All resources

 Dashboard

 Azure Monitor  
Monitor your apps and infrastructure

 Security Center  
Secure your apps and infrastructure

 Cost Management  
Analyze and optimize your cloud spend for free

Azure mobile app

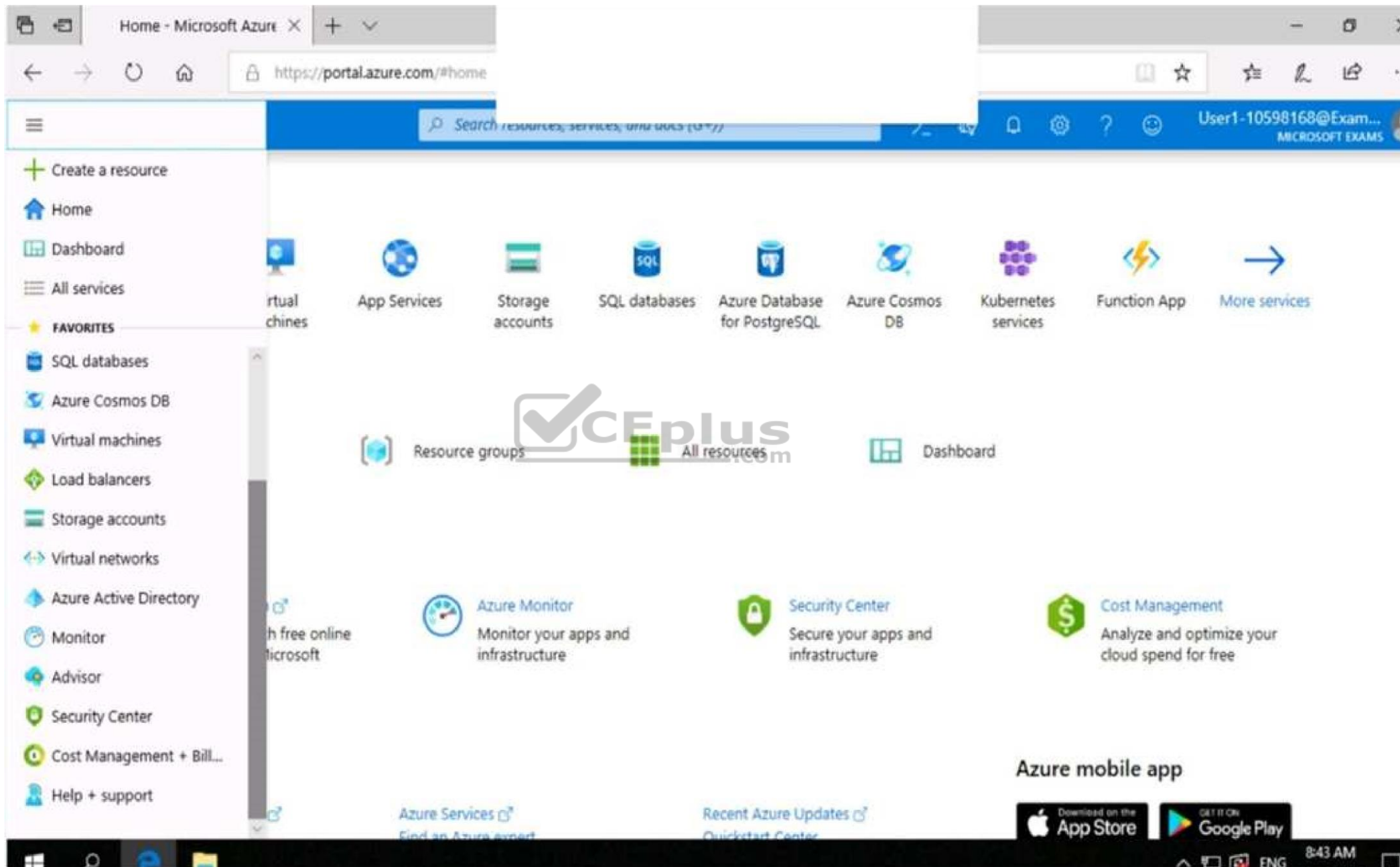
Download on the App Store

GET IT ON Google Play

[www.vceplus.com](https://www.vceplus.com) - Free Questions & Answers - Online Courses - Convert VCE to PDF - VCEplus.com

<https://vceplus.com/>





Home - Microsoft Azure X +

https://portal.azure.com/#home

Search resources, services, and tools (0/??)

User1-10598168@Exam... MICROSOFT EXAMS

FAVORITES

- SQL databases
- Azure Cosmos DB
- Virtual machines
- Load balancers
- Storage accounts
- Virtual networks
- Azure Active Directory
- Monitor
- Advisor
- Security Center
- Cost Management + Bill...
- Help + support

Virtual machines

App Services

Storage accounts

SQL databases

Azure Database for PostgreSQL

Azure Cosmos DB

Kubernetes services

Function App

More services

Resource groups

All resources

Dashboard

Azure Monitor  
Monitor your apps and infrastructure

Security Center  
Secure your apps and infrastructure

Cost Management  
Analyze and optimize your cloud spend for free

Azure mobile app

Download on the App Store

GET IT ON Google Play

8:43 AM

You need to prevent HTTP connections to the rg1lod10598168n1 Azure Storage account.

**To complete this task, sign in to the Azure portal.**

**Correct Answer:** See the explanation below.

**Section:** [none]

**Explanation**

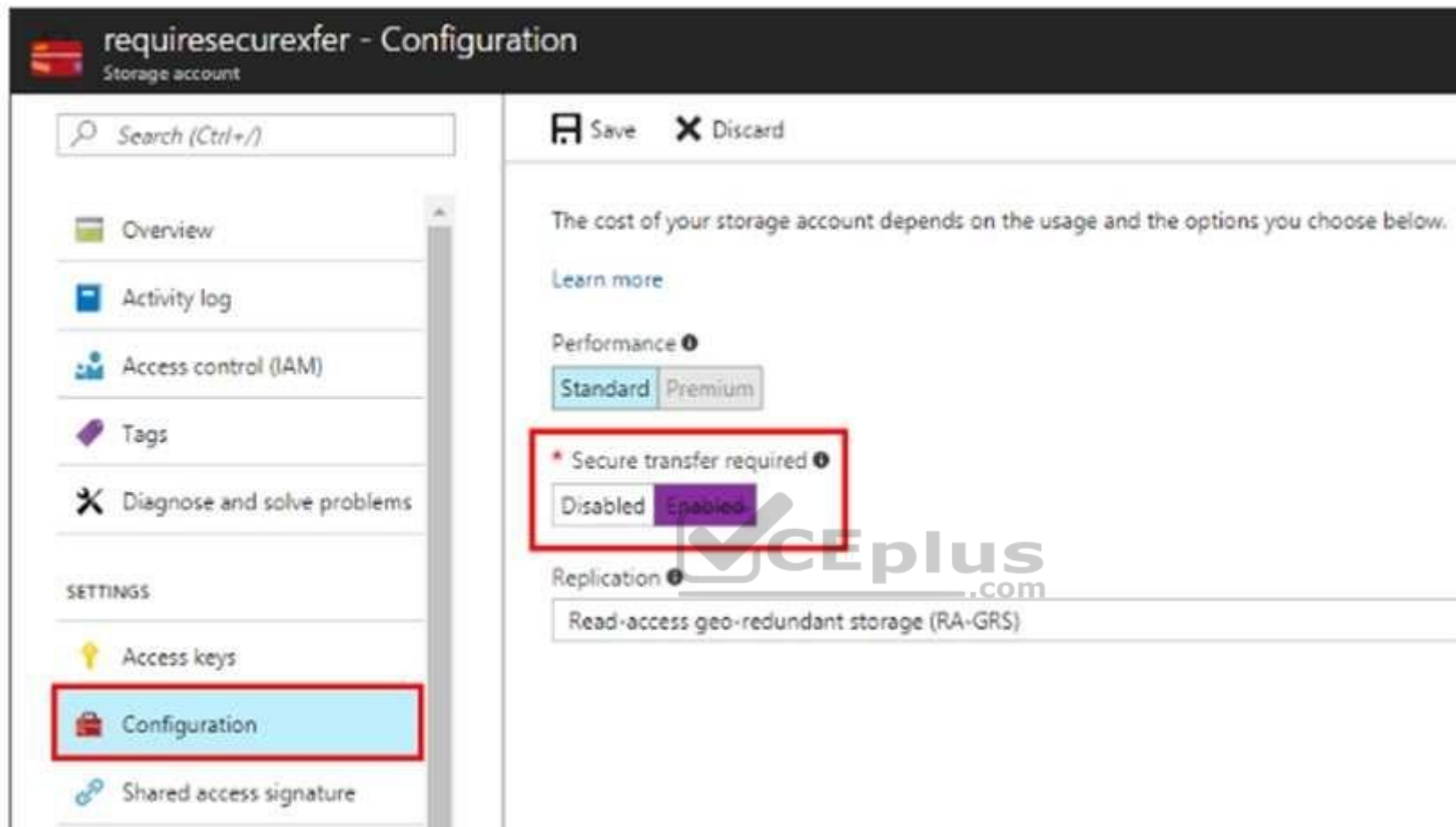
**Explanation/Reference:**

Explanation:

The "Secure transfer required" feature is now supported in Azure Storage account. This feature enhances the security of your storage account by enforcing all requests to your account through a secure connection. This feature is disabled by default.

1. In Azure Portal select you Azure Storage account rg1lod10598168n1.
2. Select Configuration, and Secure Transfer required.





Reference:

<https://techcommunity.microsoft.com/t5/Azure/quot-Secure-transfer-required-quot-is-available-in-Azure-Storage/m-p/82475>





<https://vceplus.com/>

