

➤ **Vendor: Microsoft**

➤ **Exam Code: AZ-500**

➤ **Exam Name: Microsoft Azure Security Technologies**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [July/2020](#))**

Visit Braindump2go and Download Full Version AZ-500 Exam Dumps

QUESTION 175

SIMULATION

You need to create a web app named Intranet11597200 and enable users to authenticate to the web app by using Azure Active Directory (Azure AD).

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

Answer:

1. In the Azure portal, type **App services** in the search box and select **App services** from the search results.
2. Click the **Create app service** button to create a new app service.
3. In the Resource Group section, click the **Create new** link to create a new resource group.
4. Give the resource group a name such as Intranet11597200RG and click **OK**.
5. In the **Instance Details** section, enter **Intranet11597200** in the **Name** field.
6. In the **Runtime stack** field, select any runtime stack such as **.NET Core 3.1**.
7. Click the **Review + create** button.
8. Click the **Create** button to create the web app.
9. Click the **Go to resource** button to open the properties of the new web app.
10. In the **Settings** section, click on **Authentication / Authorization**.
11. Click the **App Service Authentication** slider to set it to **On**.
12. In the **Action to take when request is not authentication** box, select **Log in with Azure Active Directory**.
13. Click **Save** to save the changes.

QUESTION 176

SIMULATION

You need to enable Advanced Data Security for the SQLdb1 Azure SQL database. The solution must ensure that Azure Advanced Threat Protection (ATP) alerts are sent to User1@contoso.com.

To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

1. In the Azure portal, type **SQL** in the search box, select **SQL databases** from the search results then select **SQLdb1**. Alternatively, browse to **SQL databases** in the left navigation pane.
2. In the properties of SQLdb1, scroll down to the **Security** section and select **Advanced data security**.
3. Click on the **Settings** icon.
4. Tick the **Enable Advanced Data Security at the database level** checkbox.
5. Click **Yes** at the confirmation prompt.
6. In the **Storage account** select a storage account if one isn't selected by default.
7. Under **Advanced Threat Protection Settings**, enter **User1@contoso.com** in the **Send alerts to** box.
8. Click the **Save** button to save the changes.

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/advanced-data-security>

QUESTION 177

SIMULATION

You plan to use Azure Disk Encryption for several virtual machine disks.

You need to ensure that Azure Disk Encryption can retrieve secrets from the KeyVault11641655 Azure key vault.

To complete this task, sign in to the Azure portal and modify the Azure resources.

[AZ-500 Exam Dumps](#) [AZ-500 Exam Questions](#) [AZ-500 PDF Dumps](#) [AZ-500 VCE Dumps](#)

<https://www.braindump2go.com/az-500.html>

Answer:

1. In the Azure portal, type **Key Vaults** in the search box, select **Key Vaults** from the search results then select **KeyVault11641655**. Alternatively, browse to **Key Vaults** in the left navigation pane.
2. In the Key Vault properties, scroll down to the **Settings** section and select **Access Policies**.
3. Select the **Azure Disk Encryption for volume encryption**

Enable Access to:

- ☐ Azure Virtual Machines for deployment ⓘ
- ☐ Azure Resource Manager for template deployment ⓘ
- ☒ Azure Disk Encryption for volume encryption ⓘ

4. Click **Save** to save the changes.

QUESTION 178**SIMULATION**

You need to ensure that User2-11641655 has all the key permissions for KeyVault11641655.
To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

You need to assign the user the **Key Vault Secrets Officer** role.

1. In the Azure portal, type **Key Vaults** in the search box, select **Key Vaults** from the search results then select **KeyVault11641655**. Alternatively, browse to **Key Vaults** in the left navigation pane.
2. In the key vault properties, select **Access control (IAM)**.
3. In the **Add a role assignment** section, click the **Add** button.
4. In the **Role** box, select the **Key Vault Secrets Officer** role from the drop-down list.
5. In the **Select** box, start typing User2-11641655 and select User2-11641655 from the search results.
6. Click the **Save** button to save the changes.

QUESTION 179

You have an Azure web app named WebApp1.

You upload a certificate to WebApp1.

You need to make the certificate accessible to the app code of WebApp1.

What should you do?

- A. Add a user-assigned managed identity to WebApp1.
- B. Add an app setting to the WebApp1 configuration.
- C. Enable system-assigned managed identity for the WebApp1.
- D. Configure the TLS/SSL binding for WebApp1.

Answer: B**Explanation:**

<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code>

QUESTION 180**Case Study 1 - Litware, Inc****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 https://litwareinc.com and http://www.litwareinc.com.
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

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 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.

Hotspot Question

You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.

What should you use in the Azure portal? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

To configure the registration settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

To configure the consent settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

Answer:

Answer Area

To configure the registration settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

To configure the consent settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent>

QUESTION 181

Hotspot Question

Your network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that has the following settings:

- Assignments:
- Include: Group1
- Exclude Group2
- Controls: Require Azure MFA registration
- Enforce Policy: On

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>

QUESTION 182

SIMULATION

The developers at your company plan to publish an app named App11641655 to Azure.

You need to ensure that the app is registered to Azure Active Directory (Azure AD). The registration must use the sign-on URLs of https://app.contoso.com.

To complete this task, sign in to the Azure portal and modify the Azure resources.


Answer:

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 App11641655. 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://app.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).

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.

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

6. Click Register

Explanation:

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

QUESTION 183

Hotspot Question

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

Name	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

You create the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.

Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
 NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input type="radio"/>
You can start VM2.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input checked="" type="radio"/>
You can start VM2.	<input checked="" type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking>

QUESTION 184

Hotspot Question

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Subscription role	Azure AD user role
User1	Owner	None
User2	Contributor	None
User3	Security Admin	None
User4	None	Service administrator

You create a resource group named RG1.

Which users can modify the permissions for RG1 and which users can create virtual networks in RG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users who can modify the permissions for RG1:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Answer:

Answer Area

Users who can modify the permissions for RG1:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

▼

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Explanation:

Box 1: Only an owner can change permissions on resources.

Box 2: A Contributor can create/modify/delete anything in the subscription but cannot change permissions.

QUESTION 185

Hotspot Question

You have a file named File1.yaml that contains the following contents.

```
apiVersion: 2018-10-01
location: eastus
name: containergroup1
properties:
  containers:
  - name: container1
    properties:
      environmentVariables:
      - name: 'Variable1'
        value: 'Value1'
      - name: 'Variable2'
        secureValue: 'Value2'
      image: nginx
      ports: []
      resources:
        requests:
          cpu: 1.0
          memoryInGB: 1.5
      osType: Linux
      restartPolicy: Always
    tags: null
  type: Microsoft.ContainerInstance/containerGroups
```

You create an Azure container instance named container1 by using File1.yaml.

You need to identify where you can access the values of Variable1 and Variable2.

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

NOTE: Each correct selection is worth one point.

Answer Area

Variable1:	<div><div></div><div>▼</div></div> <div>Cannot be accessed</div> <div>Can be accessed from the Azure portal only</div> <div>Can be accessed from inside container1 only</div> <div>Can be accessed from inside container1 and the Azure portal</div>
Variable2:	<div><div></div><div>▼</div></div> <div>Cannot be accessed</div> <div>Can be accessed from the Azure portal only</div> <div>Can be accessed from inside container1 only</div> <div>Can be accessed from inside container1 and the Azure portal</div>

Answer:

Answer Area

Variable1:

▼
Cannot be accessed
Can be accessed from the Azure portal only
Can be accessed from inside container1 only
Can be accessed from inside container1 and the Azure portal

Variable2:

▼
Cannot be accessed
Can be accessed from the Azure portal only
Can be accessed from inside container1 only
Can be accessed from inside container1 and the Azure portal

Explanation:

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

QUESTION 186

Hotspot Question

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

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VM3	VNET2/Subnet2	10.2.1.5	None

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.

You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.

Save Discard Refresh

Allow access from

☐ All networks ☒ Selected networks

Configure network security for your storage accounts. [Learn more.](#)

Virtual networks

Secure your storage account with virtual networks. [+ Add existing virtual network](#)

[+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS	RESOURCE GROUP	SUBSCRIPTION
-----------------	--------	---------------	-----------------	----------------	--------------

No network selected.

Firewall

Add IP ranges to allow access from the internet on your on-premises networks. [Learn more.](#)

Address Range

13.80.73.87



IP address or CIDR

Exceptions

- ☒ Allow trusted Microsoft services to access this storage account ⓘ
- ☐ Allow read access to storage logging from any network
- ☐ Allow read access to storage metrics from any network

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

Answer Area

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>
From VM3 , you can upload a blob to storageacc1.	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
From VM1, you can upload a blob to storageacc1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can upload a blob to storageacc1.	<input type="radio"/>	<input checked="" type="radio"/>
From VM3 , you can upload a blob to storageacc1.	<input type="radio"/>	<input checked="" type="radio"/>

Explanation:

Box 1: Yes

The public IP of VM1 is allowed through the firewall.

Box 2: No

The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is

not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.

Box 3: No

The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.

<https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security>

QUESTION 187

Hotspot Question

You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

Name	Private IP address	Public IP address	Connected to
VM1	10.7.0.4	51.144.245.152	VNET1/Default
VM2	10.8.0.4	104.45.9.227	VNET2/Default

You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption. KeyVault1 is configured as shown in the following exhibit.

Save
 Discard

Allow access from: ☐ All networks ☒ Selected networks

Configure network access control for your key vault. [Learn More](#)

Virtual networks: [+ Add existing virtual networks](#) [+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	RESOURCE GROUP	SUBSCRIPTION
VNET1	default	RG1	...

Firewall:

IPv4 ADDRESS OR CIDR

...

Exception:

Allow trusted Microsoft services to bypass this firewall? ☒ Yes ☐ No

This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	<input type="radio"/>	<input type="radio"/>
From VM2, users can manage the keys and secrets stored in KeyVault1.	<input type="radio"/>	<input type="radio"/>
VM2 can use KeyVault for Azure Disk Encryption	<input type="radio"/>	<input type="radio"/>

Answer:

Answer Area

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, users can manage the keys and secrets stored in KeyVault1.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can use KeyVault for Azure Disk Encryption	<input checked="" type="radio"/>	<input type="radio"/>

QUESTION 188

Drag and Drop Question

You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.

You need to enable Azure Disk Encryption for VM1.

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.

Actions

- Run the Set-AzVMDiskEncryptionExtension cmdlet.
- Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.
- Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.
- Generate a key vault certificate.
- Create an Azure key vault.
- Configure storage1 to use a customer-managed key.

Answer Area

Answer:

Actions

- Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.
- Generate a key vault certificate.
- Configure storage1 to use a customer-managed key.

Answer Area

- Create an Azure key vault.
- Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.
- Run the Set-AzVMDiskEncryptionExtension cmdlet.

Explanation:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

QUESTION 189

Hotspot Question

You have the Azure key vaults shown in the following table.

Name	Location	Azure subscription name
KV1	West US	Subscription1
KV2	West US	Subscription1
KV3	East US	Subscription1
KV4	West US	Subscription2
KV5	East US	Subscription2

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.

You back up Secret1 and Key1.

To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

You can restore the Secret1 backup to:

▼

KV1 only

KV1 and KV2 only

KV1, KV2 and KV3 only

KV1, KV2 and KV4 only

KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to:

▼

KV1 only

KV1 and KV2 only

KV1, KV2 and KV3 only

KV1, KV2 and KV4 only

KV1, KV2, KV3, KV4, and KV5

Answer:

Answer Area

You can restore the Secret1 backup to:

▼

KV1 only

KV1 and KV2 only

KV1, KV2 and KV3 only

KV1, KV2 and KV4 only

KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to:

▼

KV1 only

KV1 and KV2 only

KV1, KV2 and KV3 only

KV1, KV2 and KV4 only

KV1, KV2, KV3, KV4, and KV5

Explanation:



Braindump2go Guarantee All Exams 100% Pass
One Time!

The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.