Braindump2go Guarantee All Exams 100% Pass One Time!

- 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 152
You have an Azure subscription.
You configure the subscription to use a different Azure Active Directory (Azure AD) tenant.
What are two possible effects of the change? Each correct answer presents a complete solution.
NOTE: Each correct selection is worth one point.

A. Role assignments at the subscription level are lost.
B. Virtual machine managed identities are lost.
C. Virtual machine disk snapshots are lost.
D. Existing Azure resources are deleted.

Answer: AB
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory

QUESTION 153
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 generate new SASs.
Does this meet the goal?

A. Yes
B. No

Answer: B
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.
References:

AZ-500 Exam Dumps AZ-500 Exam Questions AZ-500 PDF Dumps AZ-500 VCE Dumps

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

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

QUESTION 154
You have an Azure subscription that contains virtual machines.
You enable just in time (JIT) VM access to all the virtual machines.
You need to connect to a virtual machine by using Remote Desktop.
What should you do first?

A. From Azure Directory (Azure AD) Privileged Identity Management (PIM), activate the Security administrator user role.
B. From Azure Active Directory (Azure AD) Privileged Identity Management (PIM), activate the Owner role for the virtual machine.
C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.
D. From the Azure portal, select the virtual machine and add the Network Watcher Agent virtual machine extension.

Answer: C
Explanation:
https://docs.microsoft.com/en-us/azure/virtual-machines/windows/connect-logon

QUESTION 155
SIMULATION
You need to ensure that connections from the Internet to VNET1\subnet0 are allowed only over TCP port 7777. The solution must use only currently deployed resources.
To complete this task, sign in to the Azure portal.
Answer:
You need to configure the Network Security Group that is associated with subnet0.
1. In the Azure portal, type **Virtual Networks** in the search box, select **Virtual Networks** from the search results then select **VNET1**. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the properties of VNET1, click on **Subnets.** This will display the subnets in VNET1 and the **Network Security Group** associated to each subnet. Note the name of the Network Security Group associated to **Subnet0**.
3. Type **Network Security Groups** into the search box and select the Network Security Group associated with Subnet0.
4. In the properties of the Network Security Group, click on **Inbound Security Rules.**
5. Click the **Add** button to add a new rule.
6. In the **Source** field, select **Service Tag.**
7. In the **Source Service Tag** field, select **Internet.**
8. Leave the **Source port ranges** and **Destination** field as the default values (***** and **All**).
9. In the **Destination port ranges** field, enter **7777.**
10. Change the **Protocol** to **TCP.**
11. Leave the **Action** option as **Allow.**
12. Change the **Priority** to **100.**
13. Change the **Name** from the default **Port_8080** to something more descriptive such as **Allow_TCP_7777_from_Internet.** The name cannot contain spaces.
14. Click the **Add** button to save the new rule.

QUESTION 156
SIMULATION
You need to prevent administrators from performing accidental changes to the Homepage app service plan.
To complete this task, sign in to the Azure portal.
Answer:
You need to configure the Network Security Group that is associated with subnet0.
1. In the Azure portal, type **Virtual Networks** in the search box, select **Virtual Networks** from the search results then select **VNET1**. Alternatively, browse to Virtual Networks in the left navigation pane.
2. In the properties of VNET1, click on **Subnets.** This will display the subnets in VNET1 and the **Network Security Group** associated to each subnet. Note the name of the Network Security Group associated to **Subnet0**.
3. Type **Network Security Groups** into the search box and select the Network Security Group associated with Subnet0.

4. In the properties of the Network Security Group, click on **Inbound Security Rules.**
5. Click the **Add** button to add a new rule.
6. In the **Source** field, select **Service Tag.**
7. In the **Source Service Tag** field, select **Internet.**
8. Leave the **Source port ranges** and **Destination** field as the default values (***** and **All**).
9. In the **Destination port ranges** field, enter **7777.**
10. Change the **Protocol** to **TCP.**
11. Leave the **Action** option as **Allow.**
12. Change the **Priority** to **100.**
13. Change the **Name** from the default **Port_8080** to something more descriptive such as **Allow_TCP_7777_from_Internet.** The name cannot contain spaces.
14. Click the **Add** button to save the new rule.

QUESTION 157
SIMULATION
You need to ensure that a user named Danny11597200 can sign in to any SQL database on a Microsoft SQL server named web11597200 by using SQL Server Management Studio (SSMS) and Azure Active Directory (Azure AD) credentials.
To complete this task, sign in to the Azure portal.
Answer:
You need to configure a 'lock' for the app service plan. A read-only lock ensures that no one can make changes to the app service plan without first deleting the lock.
1. In the Azure portal, type **App Service Plans** in the search box, select **App Service Plans** from the search results then select **Homepage**. Alternatively, browse to App Service Plans in the left navigation pane.
2. In the properties of the app service plan, click on **Locks.**
3. Click the **Add** button to add a new lock.
4. Enter a name in the **Lock name** field. It doesn't matter what name you provide for the exam.
5. For the **Lock type,** select **Read-only.**
6. Click **OK** to save the changes.

QUESTION 158
SIMULATION
You need to configure a Microsoft SQL server named Web11597200 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.
To complete this task, sign in to the Azure portal.
Answer:
You need to provision an Azure AD Admin for the SQL Server.
1. In the Azure portal, type **SQL Server** in the search box, select **SQL Server** from the search results then select the server named web11597200. Alternatively, browse to SQL Server in the left navigation pane.
2. In the SQL Server properties page, click on **Active Directory Admin.**
3. Click the **Set Admin** button.
4. In the **Add Admin** window, search for and select Danny11597200.
5. Click the **Select** button to add Danny11597200.
6. Click the **Save** button to save the changes.

Explanation:
https://docs.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure?tabs=azure-powershell

QUESTION 159
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. security policies in Azure Security Center
D. Azure Logic Apps

Answer: B
Explanation:

The primary use case for the Azure Desired State Configuration (DSC) extension is to bootstrap a VM to the Azure Automation State Configuration (DSC) service. The service provides benefits that include ongoing management of the VM configuration and integration with other operational tools, such as Azure Monitoring. Using the extension to register VM's to the service provides a flexible solution that even works across Azure subscriptions.
https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/dsc-overview

QUESTION 160
SIMULATION
You need to configure network connectivity between a virtual network named VNET1 and a virtual network named VNET2. The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2.
To complete this task, sign in to the Azure portal and modify the Azure resources.
Answer:
You need to configure VNet Peering between the two networks. The questions states, "The solution must ensure that virtual machines connected to VNET1 can communicate with virtual machines connected to VNET2". It doesn't say the VMs on VNET2 should be able to communicate with VMs on VNET1. Therefore, we need to configure the peering to allow just the one-way communication.
1. In the Azure portal, type **Virtual Networks** in the search box, select **Virtual Networks** from the search results then select **VNET1**. Alternatively, browse to **Virtual Networks** in the left navigation pane.
2. In the properties of **VNET1,** click on **Peerings.**
3. In the **Peerings** blade, click **Add** to add a new peering.
4. In the **Name of the peering from VNET1 to remote virtual network** box, enter a name such as **VNET1-VNET2** (this is the name that the peering will be displayed as in VNET1)
5. In the **Virtual Network** box, select **VNET2.**
6. In the **Name of the peering from remote virtual network to VNET1** box, enter a name such as **VNET2-VNET1** (this is the name that the peering will be displayed as in VNET2).
There is an option **Allow virtual network access from VNET to remote virtual network.** This should be left as **Enabled.**
7. For the option **Allow virtual network access from remote network to VNET1,** click the slider button to **Disabled.**
8. Click the **OK** button to save the changes.
Explanation:
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-manage-peering

QUESTION 161
SIMULATION
You need to deploy an Azure firewall to a virtual network named VNET3.
To complete this task, sign in to the Azure portal and modify the Azure resources.
This task might take several minutes to complete. You can perform other tasks while the task completes.
Answer:
To add an Azure firewall to a VNET, the VNET must first be configured with a subnet named **AzureFirewallSubnet** (if it doesn't already exist).
Configure VNET3.
1. In the Azure portal, type **Virtual Networks** in the search box, select **Virtual Networks** from the search results then select **VNET3**. Alternatively, browse to **Virtual Networks** in the left navigation pane.
2. In the **Overview** section, note the **Location (region)** and **Resource Group** of the virtual network. We'll need these when we add the firewall.
3. Click on **Subnets.**
4. Click on **+ Subnet** to add a new subnet.
5. Enter **AzureFirewallSubnet** in the **Name** box. The subnet must be named **AzureFirewallSubnet.**
6. Enter an appropriate IP range for the subnet in the **Address range** box.
7. Click the **OK** button to create the subnet.

Add the Azure Firewall.
1. In the settings of **VNET3** click on **Firewall.**
2. Click the **Click here to add a new firewall** link.
3. The **Resource group** will default to the VNET3 resource group. Leave this default.
4. Enter a name for the firewall in the **Name** box.
5. In the **Region** box, select the same region as VNET3.
6. In the **Public IP address** box, select an available public IP address if one exists, or click **Add new** to add a new public IP address.
7. Click the **Review + create** button.

8. Review the settings and click the **Create** button to create the firewall.

Explanation:

https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-deploy-portal

QUESTION 162

SIMULATION

You need to configure a virtual network named VNET2 to meet the following requirements:

- Administrators must be prevented from deleting VNET2 accidentally.
- Administrators must be able to add subnets to VNET2 regularly.

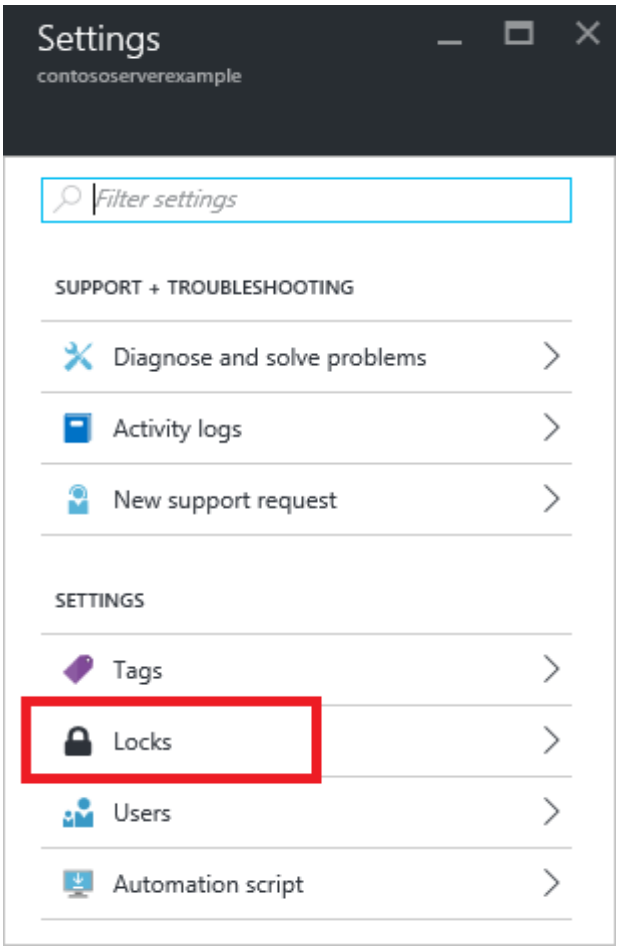
To complete this task, sign in to the Azure portal and modify the Azure resources.

Answer:

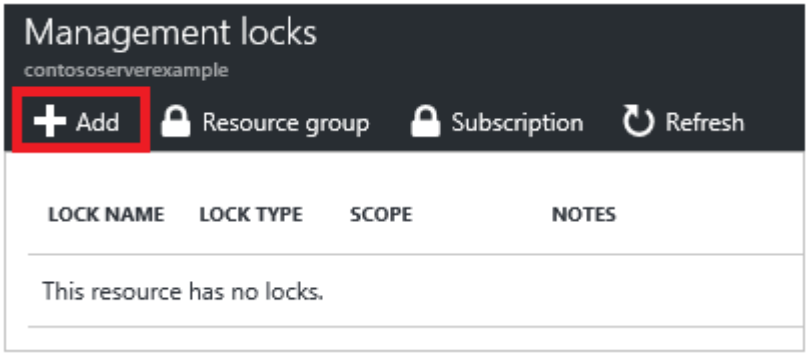
Locking prevents other users in your organization from accidentally deleting or modifying critical resources, such as Azure subscription, resource group, or resource.

Note: In Azure, the term resource refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.

1. In the Azure portal, type **Virtual Networks** in the search box, select **Virtual Networks** from the search results then select **VNET2**. Alternatively, browse to **Virtual Networks** in the left navigation pane.
2. In the Settings blade for virtual network VNET2, select **Locks**.



3. To add a lock, select **Add**.



4. For **Lock type** select **Delete lock**, and click **OK**

Explanation:

https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources