

➤ **Vendor: Microsoft**

➤ **Exam Code: AZ-500**

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

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

Visit Braindump2go and Download Full Version AZ-500 Exam Dumps

QUESTION 203

You have an Azure subscription that contains 100 virtual machines and has Azure Security Center Standard tier enabled.

You plan to perform a vulnerability scan of each virtual machine.

You need to deploy the vulnerability scanner extension to the virtual machines by using an Azure Resource Manager template.

Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the user-assigned managed identity
- B. the workspace ID
- C. the Azure Active Directory (Azure AD) ID
- D. the Key Vault managed storage account key
- E. the system-assigned managed identity
- F. the primary shared key

Answer: AC

QUESTION 204

You have an Azure subscription that contains a user named Admin1 and a virtual machine named VM1. VM1 runs Windows Server 2019 and was deployed by using an Azure Resource Manager template. VM1 is the member of a backend pool of a public Azure Basic Load Balancer.

Admin1 reports that VM1 is listed as Unsupported on the Just in time VM access blade of Azure Security Center.

You need to ensure that Admin1 can enable just in time (JIT) VM access for VM1.

What should you do?

- A. Create and configure a network security group (NSG).
- B. Create and configure an additional public IP address for VM1.
- C. Replace the Basic Load Balancer with an Azure Standard Load Balancer.
- D. Assign an Azure Active Directory Premium Plan 1 license to Admin1.

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-request-asc>

QUESTION 205

You have an Azure Active Directory (Azure AD) tenant and a root management group.

You create 10 Azure subscriptions and add the subscriptions to the root management group.

You need to create an Azure Blueprints definition that will be stored in the root management group.

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

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

What should you do first?

- A. Modify the role-based access control (RBAC) role assignments for the root management group.
- B. Add an Azure Policy definition to the root management group.
- C. Create a user assigned identity.
- D. Create a service principal.

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin>

QUESTION 206

You have three on-premises servers named Server1, Server2, and Server3 that run Windows. Server1 and Server2 are located on the Internal network. Server3 is located on the premises network. All servers have access to Azure. From Azure Sentinel, you install a Windows firewall data connector. You need to collect Microsoft Defender Firewall data from the servers for Azure Sentinel. What should you do?

- A. Create an event subscription from Server1, Server2 and Server3
- B. Install the On-premises data gateway on each server.
- C. Install the Microsoft Agent on each server.
- D. Install the Microsoft Agent on Server1 and Server2 install the on-premises data gateway on Server3.

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall>

QUESTION 207

You have an Azure subscription that contains several Azure SQL databases and an Azure Sentinel workspace. You need to create a saved query in the workspace to find events reported by Advanced Threat Protection for Azure SQL Database. What should you do?

- A. From Azure CLI run the Get-AzOperationalInsightsworkspace cmdlet.
- B. From the Azure SQL Database query editor, create a Transact-SQL query.
- C. From the Azure Sentinel workspace, create a Kusto Query Language query.
- D. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.

Answer: C

QUESTION 208

You are collecting events from Azure virtual machines to an Azure Log Analytics workspace. You plan to create alerts based on the collected events. You need to identify which Azure services can be used to create the alerts. Which two services should you identify? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Azure Monitor
- B. Azure Security Center
- C. Azure Analytics Services
- D. Azure Sentinel
- E. Azure Advisor

Answer: AD

QUESTION 209

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

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

Hotspot Question

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

| Name | Type | In resource group |
|--------------------------------------|-----------------|-----------------------|
| 8372f433-2dcd-4361-b5ef-5b188fed87d0 | Subscription ID | <i>Not applicable</i> |
| RG1 | Resource group | <i>Not applicable</i> |
| VM1 | Virtual machine | RG1 |
| VNET1 | Virtual network | RG1 |
| storage | Storage account | RG1 |
| User1 | User account | <i>Not applicable</i> |

You create an Azure role by using the following JSON file.

```
{
  "properties": {
    "roleName": "Role1",
    "description": "",
    "assignableScopes": [
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0",
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Compute/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

You assign Role1 to User1 for RG1.

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 can create a new virtual machine in RG1. | <input type="radio"/> | <input type="radio"/> |
| User can modify the properties of storage1. | <input type="radio"/> | <input type="radio"/> |
| User1 can attach the network interface of VM1 to VNET1. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| User1 can create a new virtual machine in RG1. | <input checked="" type="radio"/> | <input type="radio"/> |
| User can modify the properties of storage1. | <input type="radio"/> | <input checked="" type="radio"/> |
| User1 can attach the network interface of VM1 to VNET1. | <input type="radio"/> | <input checked="" type="radio"/> |

Explanation:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute>

QUESTION 210

SIMULATION

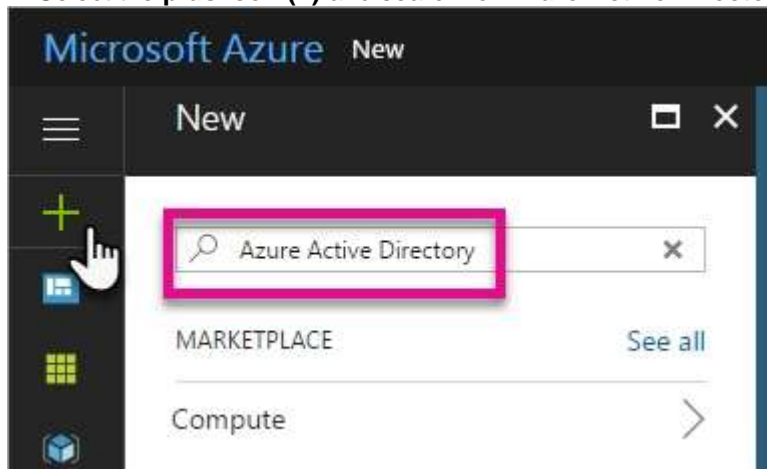
You need to create a new Azure Active Directory (Azure AD) directory named 10317806.onmicrosoft.com. The new directory must contain a user named user10317806 who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

Answer: See the explanation below.

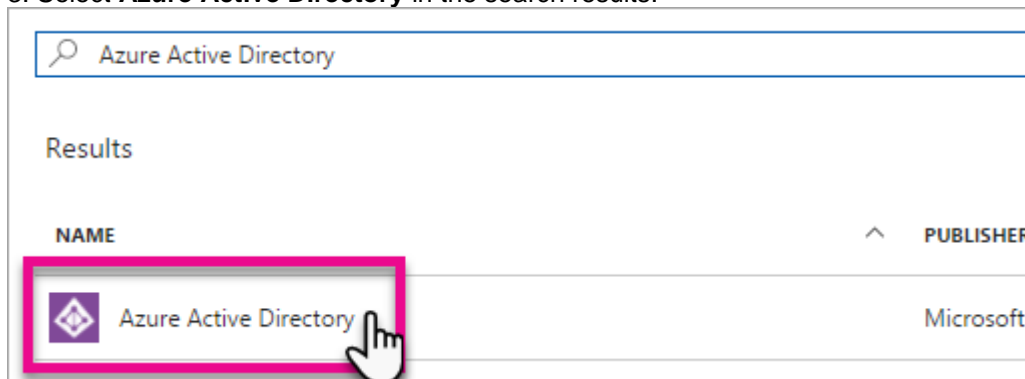
Explanation:

To create a new Azure AD tenant:

1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the **plus icon (+)** and search for **Azure Active Directory**.

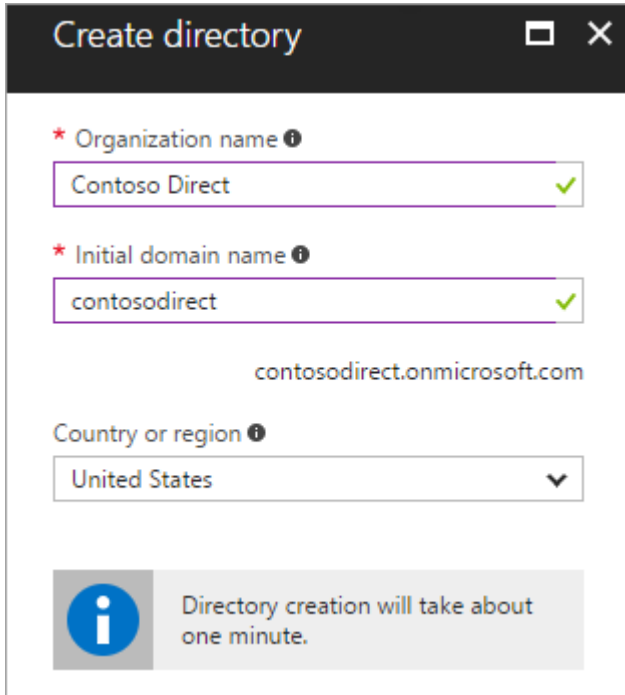


3. Select **Azure Active Directory** in the search results.



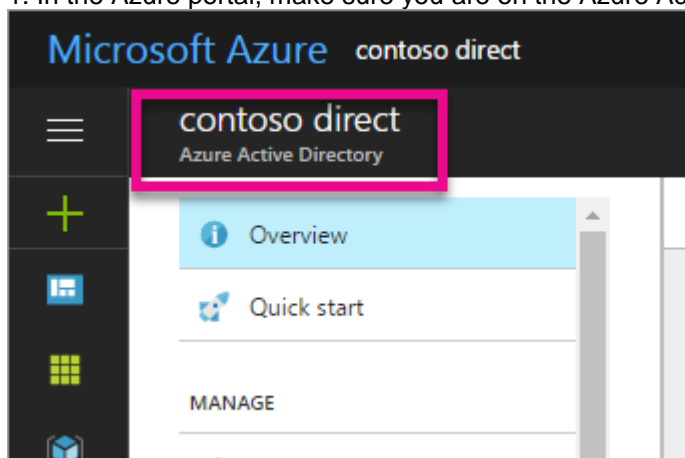
4. Select **Create**.

5. Provide an **Organization name** (10317806) and an **Initial domain name** (10317806). Then select **Create**. This will create the directory named 10317806.onmicrosoft.com.

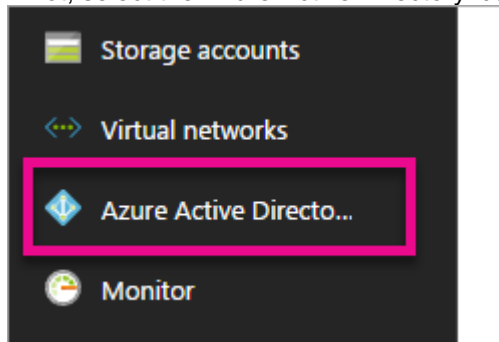


6. After directory creation is complete, select the information box to manage your new directory. To create the user:

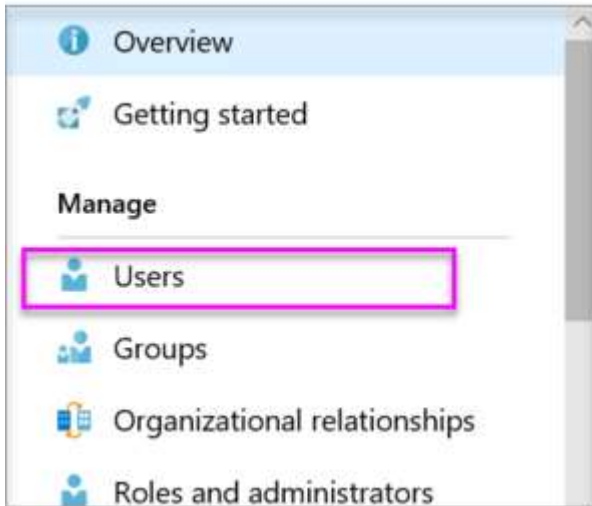
1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



If not, select the Azure Active Directory icon from the left services navigation.



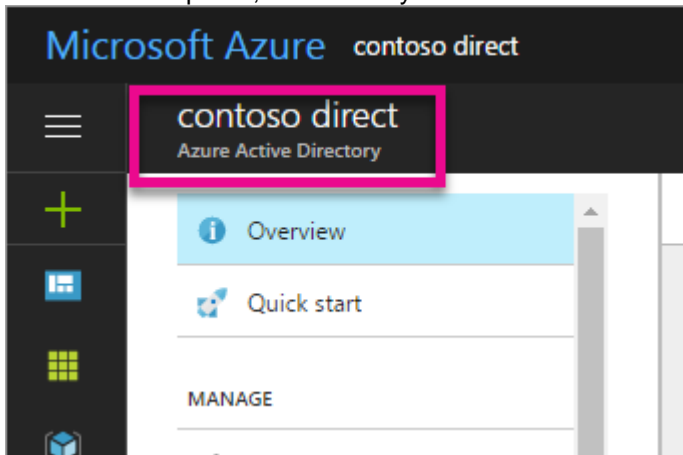
2. Under **Manage**, select **Users**.



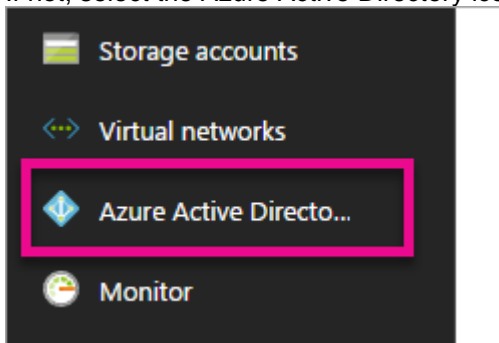
3. Select **All users** and then select **+ New user**.

4. Provide a **Name** and **User name** (user10317806) for the user. When you're done, select **Create**.
To enable MFA:

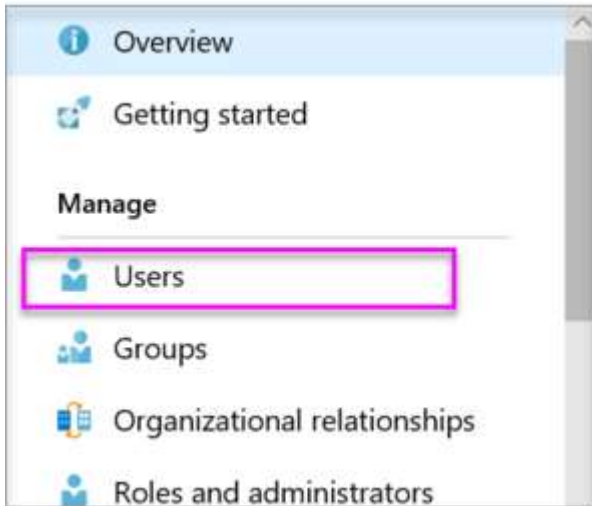
1. In the Azure portal, make sure you are on the Azure Active Directory fly out.



If not, select the Azure Active Directory icon from the left services navigation.



2. Under **Manage**, select **Users**.



3. Click on the **Multi-Factor Authentication** link.

4. Tick the checkbox next to the user's name and click the **Enable** link.

Reference:

<https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant>

QUESTION 211

Hotspot Question

You have the hierarchy of Azure resources shown in the following exhibit.



You create the Azure Blueprints definitions shown in the following table.

| Name | Published at |
|------------|-------------------|
| Blueprint1 | Tenant Root Group |
| Blueprint2 | Subscription1 |

To which objects can you assign Blueprint1 and Blueprint2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Blueprint1:

| |
|---|
| ManagementGroup1 only |
| ManagementGroup1, Subscription1, and RG1 only |
| ManagementGroup1, Subscription1, RG1, and VM1 |
| Subscription1 only |
| Tenant Root Group only |
| Tenant Root Group, ManagementGroup1, and Subscription1 only |

Blueprint2:

| |
|-----------------------------|
| ManagementGroup1 only |
| Subscription1 and RG1 only |
| Subscription1 only |
| Subscription1, RG1, and VM1 |

Answer:

Answer Area

Blueprint1:

| |
|---|
| ManagementGroup1 only |
| ManagementGroup1, Subscription1, and RG1 only |
| ManagementGroup1, Subscription1, RG1, and VM1 |
| Subscription1 only |
| Tenant Root Group only |
| Tenant Root Group, ManagementGroup1, and Subscription1 only |

Blueprint2:

| |
|-----------------------------|
| ManagementGroup1 only |
| Subscription1 and RG1 only |
| Subscription1 only |
| Subscription1, RG1, and VM1 |

Explanation:

Blueprints can only be assigned to subscriptions.

QUESTION 212**Hotspot Question**

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1.

In Azure Monitor, you create the alert rules shown in the following table.

| Name | Resource | Condition |
|-------|--------------------|---|
| Rule1 | RG1 | All security operations |
| Rule2 | RG1 | All administrative operations |
| Rule3 | Azure subscription | All security operations by Admin1 |
| Rule4 | Azure subscription | All administrative operations by Admin1 |

Admin1 performs the following actions on RG1:

- Adds a virtual network named VNET1
- Adds a Delete lock named Lock1

Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Adding VNET1:

▼

Rule2 only

Rule4 only

Rule2 and Rule 4 only

Rule3 and Rule 4 only

Rule1, Rule2, Rule3 and Rule 4

Adding Lock1:

▼

Rule2 only

Rule4 only

Rule2 and Rule 4 only

Rule3 and Rule 4 only

Rule1, Rule2, Rule3 and Rule 4

Answer:

Answer Area

Adding VNET1:

| |
|--------------------------------|
| ▼ |
| Rule2 only |
| Rule4 only |
| Rule2 and Rule 4 only |
| Rule3 and Rule 4 only |
| Rule1, Rule2, Rule3 and Rule 4 |

Adding Lock1:

| |
|--------------------------------|
| ▼ |
| Rule2 only |
| Rule4 only |
| Rule2 and Rule 4 only |
| Rule3 and Rule 4 only |
| Rule1, Rule2, Rule3 and Rule 4 |

QUESTION 213

Hotspot Question

You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.

Query1 returns a subset of security events generated by Azure AD.

You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1.

You need to ensure that you can add Playbook1 to the new rule.

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

NOTE: Each correct selection is worth one point.

Answer Area

Create the rule and set the type to:

| | |
|--------------------------------------|---|
| | ▼ |
| Fusion | |
| Microsoft Security incident creation | |
| Scheduled | |

Configure the playbook to include:

| | |
|------------------------------------|---|
| | ▼ |
| A managed connector | |
| A system-assigned managed identity | |
| A trigger | |
| Diagnostic settings | |

Answer:**Answer Area**

Create the rule and set the type to:

| | |
|--------------------------------------|---|
| | ▼ |
| Fusion | |
| Microsoft Security incident creation | |
| Scheduled | |

Configure the playbook to include:

| | |
|------------------------------------|---|
| | ▼ |
| A managed connector | |
| A system-assigned managed identity | |
| A trigger | |
| Diagnostic settings | |

Explanation:<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom><https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>**QUESTION 214**

Hotspot Question

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

| Name | Type | Attached to | NSG |
|---------|------------------------------|----------------|----------------|
| NSG1 | Network security group (NSG) | VM5 | Not applicable |
| NSG2 | Network security group (NSG) | Subnet1 | Not applicable |
| Subnet1 | Subnet | Not applicable | Not applicable |
| VM5 | Virtual machine | Subnet1 | NSG1 |

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address. VM5 has just in time (JIT) VM access configured as shown in the following exhibit.

JIT VM access configuration



VM5

+ Add  Save  Discard

Configure the ports for which the just-in-time VM access will be applicable

| Port | Protocol | Allowed source IPs | IP range | Time range (hours) | |
|------|----------|--------------------|----------|--------------------|-----|
| 3389 | Any | Per request | N/A | 3 hours | ... |

You enable JIT VM access for VM5.

NSG1 has the inbound rules shown in the following exhibit.

| Priority | Name | Port | Protocol | Source | Destination | Action |
|----------|---|------|----------|-------------------|----------------|---|
| 100 |  SecurityCenter-JITRule-... | 3389 | Any | Any | 10.1.0.4 |  Allow |
| 1000 | SecurityCenter-JITRule_341... | 3389 | Any | Any | 10.1.0.4 |  Deny |
| 1001 | RDP | 3389 | TCP | Any | Any |  Allow |
| 65000 | AllowVnetInBound | Any | Any | VirtualNetwork | VirtualNetwork |  Allow |
| 65001 | AllowAzureLoadBalancerIn... | Any | Any | AzureLoadBalancer | Any |  Allow |
| 65500 | DenyAllInBound | Any | Any | Any | Any |  Deny |

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 |
|--|-----------------------|-----------------------|
| Deleting the security rule that has a priority of 100 will revoke the approved JIT access request. | <input type="radio"/> | <input type="radio"/> |
| Remote Desktop access to VM5 is blocked. | <input type="radio"/> | <input type="radio"/> |
| An Azure Bastion host will enable Remote Desktop access to VM5 from the internet. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| Deleting the security rule that has a priority of 100 will revoke the approved JIT access request. | <input checked="" type="radio"/> | <input type="radio"/> |
| Remote Desktop access to VM5 is blocked. | <input checked="" type="radio"/> | <input type="radio"/> |
| An Azure Bastion host will enable Remote Desktop access to VM5 from the internet. | <input type="radio"/> | <input checked="" type="radio"/> |

QUESTION 215

Hotspot Question

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

| Name | Role |
|--------|----------------------|
| Admin1 | Global administrator |
| Admin2 | Group administrator |
| Admin3 | User administrator |

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.

Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Users who can create a security group named Contoso Sales:

Admin1 only
Admin1 and Admin2 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

Admin1 only
Admin1 and Admin2 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3

Answer:

Answer Area

Users who can create a security group named Contoso Sales:

| |
|----------------------------|
| Admin1 only |
| Admin1 and Admin2 only |
| Admin1 and Admin3 only |
| Admin1, Admin2, and Admin3 |

Users who can create an Office 365 group named Contoso Sales:

| |
|----------------------------|
| Admin1 only |
| Admin1 and Admin2 only |
| Admin1 and Admin3 only |
| Admin1, Admin2, and Admin3 |

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy>

QUESTION 216

Drag and Drop Question

You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant.

You create an Azure Policy initiative named SecurityPolicyInitiative1.

You identify which standard role assignments must be configured on all new resource groups.

You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created.

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 | Answer Area |
|--|-------------|
| Publish an Azure Blueprints version | |
| Assign an Azure blueprint. | |
| Create a policy assignment. | |
| Create a custom role-based access control (RBAC) role. | |
| Create a dedicated management subscription. | |
| Create an Azure Blueprints definition. | |
| Create an initiative assignment. | |

Answer:

| Actions | Answer Area |
|---|---|
| <input type="checkbox"/> | <input type="checkbox"/> Create an Azure Blueprints definition. |
| <input type="checkbox"/> | <input type="checkbox"/> Publish an Azure Blueprints version |
| <input type="checkbox"/> Create a policy assignment. | <input type="checkbox"/> Assign an Azure blueprint. |
| <input type="checkbox"/> Create a custom role-based access control (RBAC) role. | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> Create a dedicated management subscription. | <input checked="" type="checkbox"/> |
| <input type="checkbox"/> | |
| <input type="checkbox"/> Create an initiative assignment. | |

Explanation:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal>
<https://docs.microsoft.com/en-us/azure/azure-australia/azure-policy>

QUESTION 217

Hotspot Question

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses. Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Detect suspicious threats:

A Kusto query language query
A Transact-SQL query
An Azure PowerShell query
An Azure Sentinel playbook

Automate responses:

An Azure Functions app
An Azure PowerShell script
An Azure Sentinel playbook
An Azure Sentinel workbook

Answer:

Answer Area

Detect suspicious threats:

| |
|--|
| <input checked="" type="checkbox"/> A Kusto query language query |
| <input type="checkbox"/> A Transact-SQL query |
| <input type="checkbox"/> An Azure PowerShell query |
| <input type="checkbox"/> An Azure Sentinel playbook |

Automate responses:

| |
|--|
| <input type="checkbox"/> An Azure Functions app |
| <input type="checkbox"/> An Azure PowerShell script |
| <input checked="" type="checkbox"/> An Azure Sentinel playbook |
| <input type="checkbox"/> An Azure Sentinel workbook |

Explanation:<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom><https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>**QUESTION 218**

Hotspot Question

You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1. You need to configure App1 to store and access the secrets in Vault1.

How should you configure App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Configure App1 to authenticate by using a:

| |
|---|
| <input checked="" type="checkbox"/> Key |
| <input type="checkbox"/> Certificate |
| <input type="checkbox"/> Passphrase |
| <input type="checkbox"/> User-assigned managed identity |
| <input type="checkbox"/> System-assigned managed identity |

Configure a Key Vault reference for App1 from the:

| |
|--|
| <input checked="" type="checkbox"/> Extensions blade |
| <input type="checkbox"/> General settings tab |
| <input type="checkbox"/> TLS/SSL settings blade |
| <input type="checkbox"/> Application settings tab |

Answer:

Answer Area

Configure App1 to authenticate by using a:

| |
|----------------------------------|
| Key |
| Certificate |
| Passphrase |
| User-assigned managed identity |
| System-assigned managed identity |

Configure a Key Vault reference for App1 from the:

| |
|--------------------------|
| Extensions blade |
| General settings tab |
| TLS/SSL settings blade |
| Application settings tab |

Explanation:

<https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet>

QUESTION 219

Hotspot Question

You have an Azure key vault named KeyVault1 that contains the items shown in the following table.

| Name | Type |
|---------|---------------|
| Item1 | Key |
| Item2 | Secret |
| Policy1 | Access policy |

In KeyVault, the following events occur in sequence:

- Item1 is deleted
- Administrator enables soft delete
- Item2 and Policy1 are deleted.

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 recover Policy1. | <input type="radio"/> | <input type="radio"/> |
| You can add a new key named Item1. | <input type="radio"/> | <input type="radio"/> |
| You can add a new secret named Item2. | <input type="radio"/> | <input type="radio"/> |

Answer:

Answer Area

| Statements | Yes | No |
|---------------------------------------|----------------------------------|----------------------------------|
| You can recover Policy1. | <input checked="" type="radio"/> | <input type="radio"/> |
| You can add a new key named Item1. | <input checked="" type="radio"/> | <input type="radio"/> |
| You can add a new secret named Item2. | <input type="radio"/> | <input checked="" type="radio"/> |

Explanation:

<https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>