

az-500 Dumps

Microsoft Azure Security Technologies

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



NEW QUESTION 1

You need to meet the identity and access requirements for Group1.
What should you do?

- A. Add a membership rule to Group1.
- B. Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.
- C. Modify the membership rule of Group1.
- D. Change the membership type of Group1 to Assign
- E. Create two groups that have dynamic membership
- F. Add the new groups to Group1.

Answer: B

Explanation:

Incorrect Answers:

A, C: You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices.

D: For assigned group you can only add individual members. Scenario:

Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1. The tenant currently contain this group:

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.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership>

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal>

Testlet 2

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.

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

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

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

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

Sub1

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

User2 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	networksSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

Name	Subnet
VNetwork1	Subnet1.1, Subnet1.2 and Subnet1.3
VNetwork2	Subnet2.1

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet1.1
VM2	NIC2	ASG2	Subnet1.1
VM3	NIC3	None	Subnet1.2
VM4	NIC4	ASG1	Subnet1.3
VM5	NIC5	None	Subnet2.1

All virtual machines have the 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	Subnet1.1
NSG3	Subnet1.3
NSG4	Subnet2.1

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

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.m.

NEW 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 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 new stored access policy. Does this meet the goal?

- A. Yes
- B. No

Answer: A

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 effects all of the shared access signatures associated with it.

References:

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

NEW QUESTION 3

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 (AzureAD). 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

Answer: A

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>

NEW QUESTION 4

HOTSPOT

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

Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	None	Enabled
User3	Group1	123 555 7891	Required

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

▪ Assignment: Include Group1, Exclude Group2 Conditions: Sign-in risk of Medium and above Access: Allow access, Require password change
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
If User1 signs in from an unfamiliar location, he must change his password.	<input type="radio"/>	<input type="radio"/>
If User2 signs in from an anonymous IP address, she must change her password.	<input type="radio"/>	<input type="radio"/>
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: Yes
User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.
Box 2: Yes
User2 is member of Group1. Sign in from anonymous IP address is risk level Medium.
Box 3: No
Sign-ins from IP addresses with suspicious activity is low.
Note:

Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

▪ Azure AD Identity protection can detect six types of suspicious sign-in activities: Users with leaked credentials
▪ Sign-ins from anonymous IP addresses Impossible travel to atypical locations Sign-ins from infected devices
▪ Sign-ins from IP addresses with suspicious activity Sign-ins from unfamiliar locations
These six types of events are categorized in to 3 levels of risks – High, Medium & Low: References:
<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

NEW QUESTION 5

HOTSPOT

What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Group1:

No members
Only User2
Only User2 and User4
User1, User2, User3, and User4

Group2:

No members
Only User3
Only User1 and User3
User1, User2, User3, and User4

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: User1, User2, User3, User4

Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.

Box 2: Only User3

Match "*on" is only true for London (User3).

Scenario:

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

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"

References:

<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership>

NEW QUESTION 6

HOTSPOT

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.

Hot Area:

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"/>

A. Mastered

B. Not Mastered

Answer: A

Explanation:

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"/>

References:

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

NEW QUESTION 7

HOTSPOT

You have an Azure key vault.

You need to delegate administrative access to the key vault to meet the following requirements:

_ Provide a user named User1 with the ability to set advanced access policies for the key vault. Provide a user named User2 with the ability to add and delete certificates in the key vault. Use the principle of least privilege.

What should you use to assign access to each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User1:

	▼
A key vault access policy	
Azure Information Protection	
Azure Policy	
Managed identities for Azure resources	
RBAC	

User2:

	▼
A key vault access policy	
Azure Information Protection	
Azure Policy	
Managed identities for Azure resources	
RBAC	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

User1: RBAC

_ RBAC is used as the Key Vault access control mechanism for the management plane. It would allow a user with the proper identity to: set Key Vault access policies

_ create, read, update, and delete key vaults set Key Vault tags

Note: Role-based access control (RBAC) is a system that provides fine-grained access management of Azure resources. Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs.

User2: A key vault access policy

A key vault access policy is the access control mechanism to get access to the key vault data plane. Key Vault access policies grant permissions separately to keys, secrets, and certificates.

References:

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

NEW QUESTION 8

HOTSPOT

You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016.

You need to automate the deployment of the Microsoft Monitoring Agent to all the servers by using an Azure Resource Manager template. How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
{
  "type": "Microsoft.Compute/virtualMachines/extensions",
  "name": "[concat(parameter('vmname'), /OMSExtension)]",
  "apiVersion": "[variables('apiVersion')]",
  "location": "[resourceGroup().location]",
  "dependsOn": [
    "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
  ],
  "properties": {
    "publisher": "Microsoft.EnterpriseCloud.Monitoring",
    "type": "MicrosoftMonitoringAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "settings": {
      "[variable('var1')]"
      "AzureADApplicationID"
      "WorkspaceID"
      "WorkspaceName"
      "WorkspaceURL"
    },
    "protectedSettings": {
      "[variable('var2')]"
      "AzureADApplicationSecret"
      "StorageAccountKey"
      "WorkspaceID"
      "WorkspaceKey"
    }
  }
}
```

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

```
{
  "type": "Microsoft.Compute/virtualMachines/extensions",
  "name": "[concat(parameter('vmname'), /OMSExtension)]",
  "apiVersion": "[variables('apiVersion')]",
  "location": "[resourceGroup().location]",
  "dependsOn": [
    "[concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]"
  ],
  "properties": {
    "publisher": "Microsoft.EnterpriseCloud.Monitoring",
    "type": "MicrosoftMonitoringAgent",
    "typeHandlerVersion": "1.0",
    "autoUpgradeMinorVersion": true,
    "settings": {
      "[variable('var1')]"
      "AzureADApplicationID"
      "WorkspaceID"
      "WorkspaceName"
      "WorkspaceURL"
    },
    "protectedSettings": {
      "[variable('var2')]"
      "AzureADApplicationSecret"
      "StorageAccountKey"
      "WorkspaceID"
      "WorkspaceKey"
    }
  }
}
```

References:

<https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/>

NEW QUESTION 9

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 first?

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

Answer: A

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>

NEW QUESTION 10

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.

Answer: BD

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>

NEW QUESTION 10

HOTSPOT

You need to create Role1 to meet the platform protection requirements.

How should you complete the role definition of Role1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

```
(
  "Name" | "Role1",
  "Id" | "11111111-1111-1111-1111-111111111111",
  "IsCustom" : true,
  "Description": "VM storage operator"
  "Actions" : [
    [
      "Microsoft.Compute/disk/*",
      "Microsoft.Resources/storageAccounts/*",
      "Microsoft.Storage/storageAccounts/disk/*"
    ],
    "NotActions": [
      ],
    "AssignableScopes" : [
      ]
  ]
)
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Scenario: 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.

Azure RBAC template managed disks "Microsoft.Storage/" References:

<https://blogs.msdn.microsoft.com/azureedu/2017/02/11/new-managed-disk-storage-option-for-your-azure-vms/>

NEW QUESTION 15

DRAG DROP

You have an Azure subscription named Sub1 that contains an Azure Storage account named Contosostorage1 and an Azure key vault named Contosokeyvault1.

You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1.

You need to implement prerequisites to ensure that you can implement the runbook.

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

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a user-assigned managed identity.

Create a connection resource in the Azure Automation account.

Answer Area

⬅️

➡️

⬆️

⬆️

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Create an Azure Automation account
Runbooks live within the Azure Automation account and can execute PowerShell scripts.

Step 2: Import PowerShell modules to the Azure Automation account
Under ‘Assets’ from the Azure Automation account Resources section select ‘to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.

Step 3: Create a connection resource in the Azure Automation account
You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created ‘run as accounts’ above. This can be found under Assets -> Connections. After the authentication code, run the same code above to get all the keys from the vault.

```
$connectionName = "AzureRunAsConnection" try
{
# Get the connection "AzureRunAsConnection "
$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName
"Logging in to Azure..." Add-AzureRmAccount `
-ServicePrincipal `
-TenantId $servicePrincipalConnection.TenantId `
-ApplicationId $servicePrincipalConnection.ApplicationId `
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint
}
```

References:
<https://www.rahulpnath.com/blog/accessing-azure-key-vault-from-azure-runbook/>

NEW QUESTION 18

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your az-500 Exam with Our Prep Materials Via below:

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