

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

You need to ensure that User2 can implement PIM.
What should you do first?

- A. Assign User2 the Global administrator role.
- B. Configure authentication methods for contoso.com.
- C. Configure the identity secure score for contoso.com.
- D. Enable multi-factor authentication (MFA) for User2.

Answer: A

Explanation:

To start using PIM in your directory, you must first enable PIM.

1. Sign in to the Azure portal as a Global Administrator of your directory.

You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.

Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com References:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started>

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 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 4

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 5

DRAG DROP

You need to configure an access review. The review will be assigned to a new collection of reviews and reviewed by resource owners.

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 an access review program.	
Set Reviewers to Selected users.	
Create an access review audit.	⬅
Create an access review control.	➡
Set Reviewers to Group owners.	⬆
Set Reviewers to Members.	⬇

- A. Mastered
- B. Not Mastered

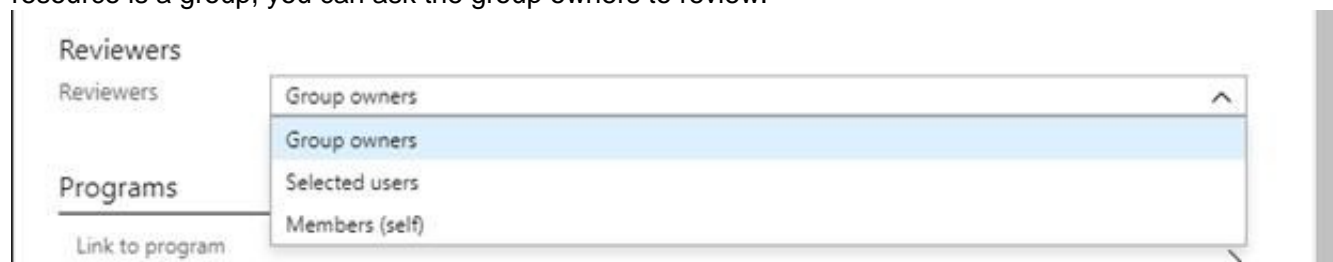
Answer: A

Explanation:

Step 1: Create an access review program Step 2: Create an access review control

Step 3: Set Reviewers to Group owners

In the Reviewers section, select either one or more people to review all the users in scope. Or you can select to have the members review their own access. If the resource is a group, you can ask the group owners to review.



References:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls>

NEW QUESTION 6

HOTSPOT

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

Name	Role	Sign in frequency
User1	Password administrator	Sign in every work day
User2	Password administrator	Sign in bi-weekly
User3	Global administrator, Password administrator	Signs in every month

You configure an access review named Review1 as shown in the following exhibit.

Create an access review

Access reviews enable reviewers to attest to users access.

* Review name

Review1

Description

* Start date

2019-03-01

Frequency

One time

Duration (in days)

1

End

Never

End by

Occurrences

* Number of times

0

* End date

2019-03-20

Users

Scope

Everyone

* Review role membership

Password administrator

Reviewers

Reviewers

Members(self)

Upon completion settings

Auto apply results to resource

Enable

Disable

Should reviewer not respond

Take recommendations

Advanced settings

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

User3 can perform Review1 for

User3 only

User1 and User2 only

User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019

The Password administrator role will be revoked from User2

User2 will retain the Password administrator role

User3 will receive a confirmation request

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: User3 only

Use the Members (self) option to have the users review their own role assignments.

Box 2: User3 will receive a confirmation request

Use the Should reviewer not respond list to specify what happens for users that are not reviewed by the reviewer within the review period. This setting does not impact users who have been reviewed by the reviewers manually. If the final reviewer's decision is Deny, then the user's access will be removed.

No change - Leave user's access unchanged Remove access - Remove user's access Approve access - Approve user's access

Take recommendations - Take the system's recommendation on denying or approving the user's continued access

References:

<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-how-to-start-security-review>

NEW QUESTION 7

DRAG DROP

You create an Azure subscription.

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

Verify your identity by using multi-factor authentication (MFA).

Consent to PIM.

Sign up PIM for Azure AD roles.

Discover privileged roles.

Discover resources.

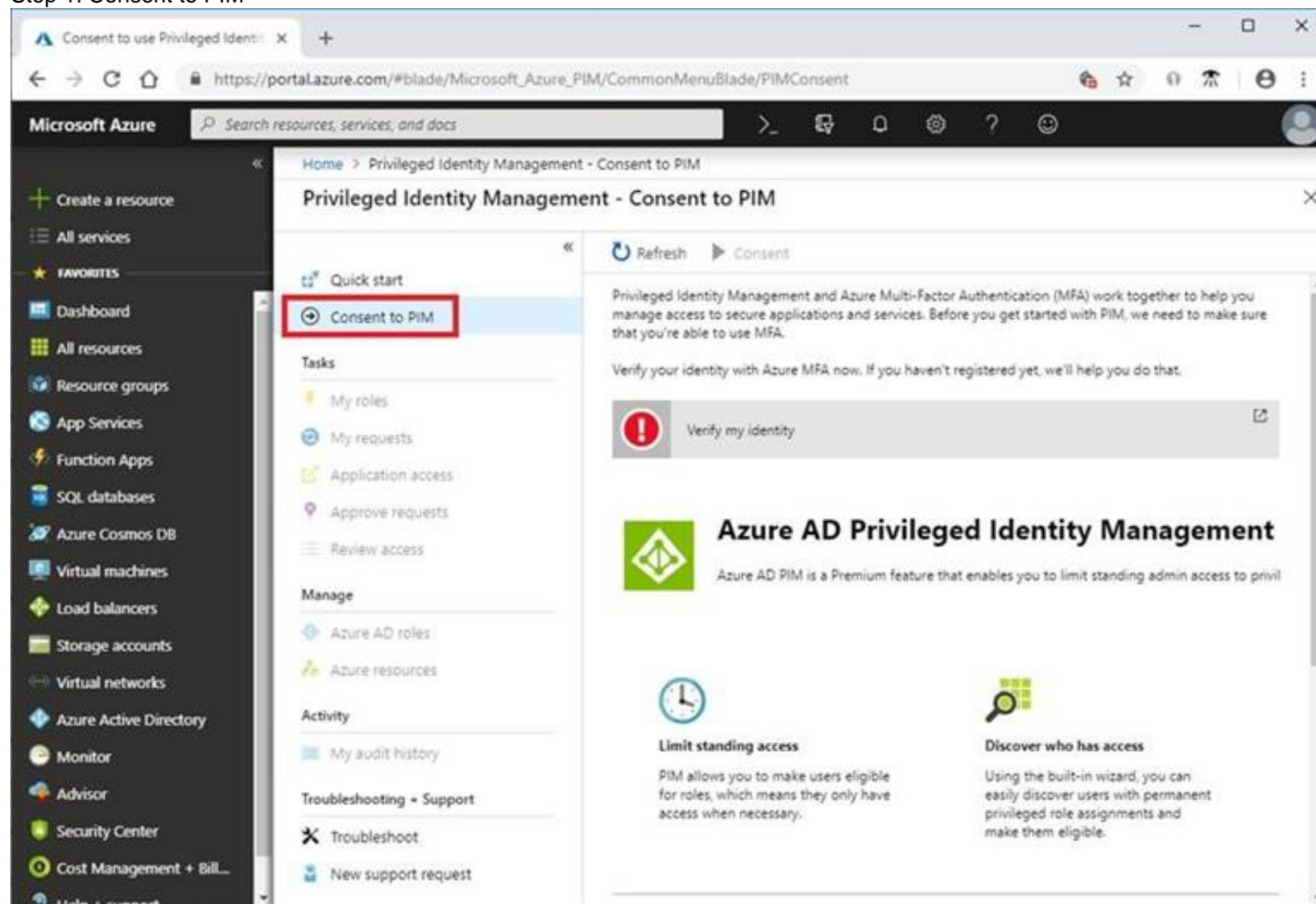
Answer Area

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Step 1: Consent to PIM



Step: 2 Verify your identity by using multi-factor authentication (MFA)

Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account.

Step 3: Sign up PIM for Azure AD roles

Once you have enabled PIM for your directory, you'll need to sign up PIM to manage Azure AD roles.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-getting-started>

NEW QUESTION 8

HOTSPOT

Your company has two offices in Seattle and New York. Each office connects to the Internet by using a NAT device. The offices use the IP addresses shown in the following table.

Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.16.0.0/16	194.25.2.0/24

The company has an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Multi-factor authentication (MFA) status
User1	Enabled
User2	Enforced

The MFA service settings are configured as shown in the exhibit. (Click the Exhibit tab.)

trusted ips [\(learn more\)](#)

☒ Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

10.10.0.0/16

194.25.2.0/24

verification options [\(learn more\)](#)

- Methods available to users:
- ☒ Call to phone
 - ☒ Text message to phone

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

	Yes	No
If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app.	<input type="radio"/>	<input type="radio"/>
If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Box 2: No
Use of Microsoft Authenticator is not required.
Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process. Box 3: No
The New York IP address subnet is included in the "skip multi-factor authentication for request.
References:
<https://www.cayosoft.com/difference-enabling-enforcing-mfa/>

NEW QUESTION 9
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 Blueprints
- C. Azure AD Privileged Identity Management (PIM)
- D. Azure Policy

Answer: C

Explanation:
The Azure AD Privileged Identity Management (PIM) service also allows Privileged Role Administrators to make permanent admin role assignments.
References:
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-add-role-to-user>

NEW QUESTION 10
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.
- B. On Firewall, configure a network traffic filtering rule.
- C. Assign RT1 to AzureFirewallSubnet.
- D. On Firewall, configure a DNAT rule.

Answer: A

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

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

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

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. 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

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.

NEW QUESTION 10

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 15

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 compliance policies in Microsoft Intune
- B. Azure Automation State Configuration
- C. application security groups
- D. Azure Advisor

Answer: B

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.

References:

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

NEW QUESTION 16

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

Answer: B

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>

NEW QUESTION 19

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 23

HOTSPOT

You have an Azure subscription named Sub1.

You create a virtual network that contains one subnet. On the subnet, you provision the virtual machines shown in the following table.

Name	Network interface	Application security group assignment	IP address
VM1	NIC1	AppGroup12	10.0.0.10
VM2	NIC2	AppGroup12	10.0.0.11
VM3	NIC3	AppGroup3	10.0.0.100
VM4	NIC4	AppGroup4	10.0.0.200

Currently, you have not provisioned any network security groups (NSGs). You need to implement network security to meet the following requirements:

- _ Allow traffic to VM4 from VM3 only.
- _ Allow traffic from the Internet to VM1 and VM2 only. Minimize the number of NSGs and network security rules.

How many NSGs and network security rules should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

NSGs:	<div><div></div><div>▼</div></div> <div><div>1</div><div>2</div><div>3</div><div>4</div></div>
Network security rules:	<div><div></div><div>▼</div></div> <div><div>1</div><div>2</div><div>3</div><div>4</div></div>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

NSGs: 2

Network security rules: 3

Not 2: You cannot specify multiple service tags or application groups) in a security rule.

References:
<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

NEW QUESTION 25

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 27

You have an 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

Answer: A

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>

NEW QUESTION 29

HOTSPOT

You assign User8 the Owner role for RG4, RG5, and RG6.
In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

User8 can create virtual networks in:

RG4 only

RG6 only

RG4 and RG6 only

RG4, RG5, and RG6

User8 can create NSGs in:

RG4 only

RG4 and RG5 only

RG4 and RG6 only

RG4, RG5, and RG6

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: RG4 only
Virtual Networks are not allowed for Rg5 and Rg6.
Box 2: Rg4,Rg5, and Rg6 Scenario:
Contoso has two Azure subscriptions named Sub1 and Sub2.
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6. You assign User8 the Owner role for RG4, RG5, and RG6
User8 city Sidney, Role:None
Note: A network security group (NSG) contains a list of security rules that allow or deny network traffic to resources connected to Azure Virtual Networks (VNet). NSGs can be associated to subnets, individual VMs (classic), or individual network interfaces (NIC) attached to VMs (Resource Manager).
References:
<https://docs.microsoft.com/en-us/azure/governance/policy/overview>

NEW QUESTION 30

HOTSPOT

Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

Answer Area

Virtual networks that User2 can modify:

▼
VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

Virtual networks that User2 can delete:

▼
VNET4 only
VNET4 and VNET1 only
VNET4, VNET3, and VNET1 only
VNET4, VNET3, VNET2, and VNET1

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: VNET4 and VNET1 only

RG1 has only Delete lock, while there are no locks on RG4. RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only

There are no locks on RG4, while the other resource groups have either Delete or Read-only locks.

Note: As an administrator, you may need to lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. You can set the lock level to CanNotDelete or ReadOnly. In the portal, the locks are called Delete and Read-only respectively.

_ CanNotDelete means authorized users can still read and modify a resource, but they can't delete the resource.

_ ReadOnly means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Scenario:

User2 is a Security administrator.

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

References:

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

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

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 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.

NEW QUESTION 35

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

What should you do first?

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

Answer: C

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. References:

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

Question Set 3

NEW QUESTION 39

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 44

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 48

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

Answer: C

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>

NEW QUESTION 52

DRAG DROP

You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines. You are planning the monitoring of Azure services in the subscription.

You need to retrieve the following details:

- _ Identify the user who deleted a virtual machine three weeks ago.
- _ Query the security events of a virtual machine that runs Windows Server 2016.

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting 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:

Settings	Answer Area
Activity log	
Logs	Identify the user who deleted a virtual machine three weeks ago: <input type="text"/>
Metrics	Query the security events of a virtual machine that runs Windows Server 2016: <input type="text"/>
Service Health	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box1: Activity log

Azure activity logs provide insight into the operations that were performed on resources in your subscription. Activity logs were previously known as “audit logs” or “operational logs,” because they report control-plane events for your subscriptions.

Activity logs help you determine the “what, who, and when” for write operations (that is, PUT, POST, or DELETE). Box 2: Logs

Log Integration collects Azure diagnostics from your Windows virtual machines, Azure activity logs, Azure Security Center alerts, and Azure resource provider logs. This integration provides a unified dashboard for all your assets, whether they're on-premises or in the cloud, so that you can aggregate, correlate, analyze, and

alert for security events.

References:

<https://docs.microsoft.com/en-us/azure/security/azure-log-audit>

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 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.





NEW QUESTION 54

DRAG DROP

You need to configure SQLDB1 to meet the data and application requirements.

Which three actions should you recommend be performed 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
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.	
In SQLDB1, create contained database users.	
Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS).	 
In Azure AD, create a system-assigned managed identity.	 
In Azure AD, create a user-assigned managed identity.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Connect to SQLDB1 by using Microsoft SQL Server Management Studio (SSMS)

Step 2: In SQLDB1, create contained database users.

Create a contained user in the database that represents the VM's system-assigned identity.

Step 3: In Azure AD, create a system-assigned managed identity.

A system-assigned identity for a Windows virtual machine (VM) can be used to access an Azure SQL server. Managed Service Identities are automatically managed by Azure and enable you to authenticate to services that support Azure AD authentication, without needing to insert credentials into your code.

References:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql>

Question Set 2

NEW QUESTION 55

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:

Actions	Answer Area
Grant permissions	
Add a delegated permission.	
Configure Azure AD Application Proxy.	⬅️
Add an application permission.	➡️
Create an app registration.	
	⬆️
	⬆️

- A. Mastered
B. Not Mastered

Answer: A

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>

NEW QUESTION 58

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.

Answer: A

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>

NEW QUESTION 60

You have an Azure SQL Database server named SQL1.

You plan to 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 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.

Answer: B

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>

NEW QUESTION 64

HOTSPOT

You have the Azure Information Protection conditions shown in the following table.

Name	Pattern	Case sensitivity
Condition1	White	On
Condition2	Black	Off

You have the Azure Information Protection labels 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

- A. Mastered
- B. Not Mastered

Answer: A

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>

NEW QUESTION 66

.....

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>