Microsoft
Exam Questions az-500
Microsoft Azure Security Technologies
NEW QUESTION 1
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.
You have an Azure Subscription named Sub1.
You have an Azure Storage account named Sa1 in a resource group named RG1.
Users and applications access the blob service and the file service in Sa1 by using several shared access signatures (SASs) and stored access policies. You discover that unauthorized users accessed both the file service and the blob service.
You need to revoke all access to Sa1. Solution: You generate new SASs. Does this meet the goal?
A. Yes
B. No
Answer: B
Explanation:
Instead you should create a new stored access policy.
To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.
References:

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.
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 3
HOTSPOT
You have an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Role</th>
<th>Sign in frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>User1</td>
<td>Password administrator</td>
<td>Sign in every work day</td>
</tr>
<tr>
<td>User2</td>
<td>Password administrator</td>
<td>Sign in bi-weekly</td>
</tr>
<tr>
<td>User3</td>
<td>Global administrator, Password administrator</td>
<td>Signs in every month</td>
</tr>
</tbody>
</table>

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

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 4
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:

Following the implementation of the planned changes, the IT team must be able to connect to VM0 by using JIT VM access.

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.

<table>
<thead>
<tr>
<th>Name</th>
<th>City</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>User1</td>
<td>Montreal</td>
<td>Global administrator</td>
</tr>
<tr>
<td>User2</td>
<td>MONTREAL</td>
<td>Security administrator</td>
</tr>
<tr>
<td>User3</td>
<td>London</td>
<td>Privileged role administrator</td>
</tr>
<tr>
<td>User4</td>
<td>Ontario</td>
<td>Application administrator</td>
</tr>
<tr>
<td>User5</td>
<td>Seattle</td>
<td>Cloud application administrator</td>
</tr>
<tr>
<td>User6</td>
<td>Seattle</td>
<td>User administrator</td>
</tr>
<tr>
<td>User7</td>
<td>Sydney</td>
<td>Reports reader</td>
</tr>
<tr>
<td>User8</td>
<td>Sydney</td>
<td>None</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Membership type</th>
<th>Dynamic membership rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group1</td>
<td>Dynamic user</td>
<td>user.city -contains &quot;ON&quot;</td>
</tr>
<tr>
<td>Group2</td>
<td>Dynamic user</td>
<td>user.city -match &quot;on&quot;</td>
</tr>
</tbody>
</table>

Sub1
Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6. User2 creates the virtual networks shown in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Resource group</th>
</tr>
</thead>
<tbody>
<tr>
<td>VNET1</td>
<td>RG1</td>
</tr>
<tr>
<td>VNET2</td>
<td>RG2</td>
</tr>
<tr>
<td>VNET3</td>
<td>RG3</td>
</tr>
<tr>
<td>VNET4</td>
<td>RG4</td>
</tr>
</tbody>
</table>

Sub1 contains the locks shown in the following table.
Sub1 contains the Azure policies shown in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Set on</th>
<th>Lock type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock1</td>
<td>RG1</td>
<td>Delete</td>
</tr>
<tr>
<td>Lock2</td>
<td>RG2</td>
<td>Read-only</td>
</tr>
<tr>
<td>Lock3</td>
<td>RG3</td>
<td>Delete</td>
</tr>
<tr>
<td>Lock4</td>
<td>RG3</td>
<td>Read-only</td>
</tr>
</tbody>
</table>

Sub2 contains the network security groups (NSGs) shown in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Associated to</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSG1</td>
<td>NIC2</td>
</tr>
<tr>
<td>NSG2</td>
<td>Subnet1.1</td>
</tr>
<tr>
<td>NSG3</td>
<td>Subnet1.3</td>
</tr>
<tr>
<td>NSG4</td>
<td>Subnet2.1</td>
</tr>
</tbody>
</table>

NSG1 has the inbound security rules shown in the following table.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>65000</td>
<td>Any</td>
<td>Any</td>
<td>VirtualNetwork</td>
<td>VirtualNetwork</td>
<td>Allow</td>
</tr>
<tr>
<td>65001</td>
<td>Any</td>
<td>Any</td>
<td>AzureLoadBalancer</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>65500</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
</tbody>
</table>

NSG2 has the inbound security rules shown in the following table.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>80</td>
<td>TCP</td>
<td>Internet</td>
<td>VirtualNetwork</td>
<td>Allow</td>
</tr>
<tr>
<td>65000</td>
<td>Any</td>
<td>Any</td>
<td>VirtualNetwork</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>65001</td>
<td>Any</td>
<td>Any</td>
<td>AzureLoadBalancer</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>65500</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
</tbody>
</table>

NSG3 has the inbound security rules shown in the following table.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Any</td>
<td>TCP</td>
<td>ASG1</td>
<td>ASG1</td>
<td>Allow</td>
</tr>
<tr>
<td>150</td>
<td>Any</td>
<td>Any</td>
<td>ASG2</td>
<td>VirtualNetwork</td>
<td>Allow</td>
</tr>
<tr>
<td>200</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
<tr>
<td>65000</td>
<td>Any</td>
<td>Any</td>
<td>VirtualNetwork</td>
<td>VirtualNetwork</td>
<td>Allow</td>
</tr>
<tr>
<td>65001</td>
<td>Any</td>
<td>Any</td>
<td>AzureLoadBalancer</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>65500</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
</tbody>
</table>

NSG4 has the inbound security rules shown in the following table.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>65000</td>
<td>Any</td>
<td>Any</td>
<td>VirtualNetwork</td>
<td>VirtualNetwork</td>
<td>Allow</td>
</tr>
<tr>
<td>65001</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Allow</td>
</tr>
<tr>
<td>65500</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
</tbody>
</table>

NSG1, NSG2, NSG3, and NSG4 have the outbound security rules shown in the following table.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Port</th>
<th>Protocol</th>
<th>Source</th>
<th>Destination</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>65000</td>
<td>Any</td>
<td>Any</td>
<td>VirtualNetwork</td>
<td>Internet</td>
<td>Allow</td>
</tr>
<tr>
<td>65001</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Internet</td>
<td>Allow</td>
</tr>
<tr>
<td>65500</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>Deny</td>
</tr>
</tbody>
</table>

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 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 (User3), 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.

<table>
<thead>
<tr>
<th>Name</th>
<th>City</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>User1</td>
<td>Montreal</td>
<td>Global administrator</td>
</tr>
<tr>
<td>User2</td>
<td>MONTREAL</td>
<td>Security administrator</td>
</tr>
<tr>
<td>User3</td>
<td>London</td>
<td>Privileged role administrator</td>
</tr>
<tr>
<td>User4</td>
<td>Ontario</td>
<td>Application administrator</td>
</tr>
<tr>
<td>User5</td>
<td>Seattle</td>
<td>Cloud application administrator</td>
</tr>
<tr>
<td>User6</td>
<td>Seattle</td>
<td>User administrator</td>
</tr>
<tr>
<td>User7</td>
<td>Sydney</td>
<td>Reports reader</td>
</tr>
<tr>
<td>User8</td>
<td>Sydney</td>
<td>None</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Membership type</th>
<th>Dynamic membership rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group1</td>
<td>Dynamic user</td>
<td>user.city -contains &quot;ON&quot;</td>
</tr>
<tr>
<td>Group2</td>
<td>Dynamic user</td>
<td>user.city -match &quot;*on&quot;</td>
</tr>
</tbody>
</table>

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

**NEW QUESTION 6**
You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.
You create a service endpoint for Subnet1.
Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.
You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint.

A. Create an application security group and a network security group (NSG).
B. Edit the docker-compose.yml file.
C. Install the container network interface (CNI) plug-in.

**Answer:** C

**Explanation:**
The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform. The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers and virtual network resources. The plug-in doesn’t rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.
The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:

Existing virtual network

Service Endpoints

On-premises

References:
https://docs.microsoft.com/en-us/azure/virtual-network/container-networking-overview

NEW QUESTION 7
HOTSPOT
You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.
You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed. How should you complete the policy? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.
Hot Area:

A. Mastered
B. Not Mastered

Answer:
A
NEW QUESTION 8
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.

<table>
<thead>
<tr>
<th>Name</th>
<th>Network interface</th>
<th>Application security group assignment</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM1</td>
<td>NIC1</td>
<td>AppGroup12</td>
<td>10.0.0.10</td>
</tr>
<tr>
<td>VM2</td>
<td>NIC2</td>
<td>AppGroup12</td>
<td>10.0.0.11</td>
</tr>
<tr>
<td>VM3</td>
<td>NIC3</td>
<td>AppGroup3</td>
<td>10.0.0.100</td>
</tr>
<tr>
<td>VM4</td>
<td>NIC4</td>
<td>AppGroup4</td>
<td>10.0.0.200</td>
</tr>
</tbody>
</table>

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.

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:

NEW QUESTION 9
HOTSPOT
You suspect that users are attempting to sign in to resources to which they have no access. You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

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

NOTE: Each correct selection is worth one point.

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.
A. Mastered
B. Not Mastered

Answer: A

Explanation:
The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in. let timeframe = 3d;

SecurityEvent
| where TimeGenerated > ago(3d) and AccountType == 'User' and EventID == 4625 // 4625 - failed log in
| summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account
| where failed_login_attempts > 5
| project-away Account1

References:
https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/examples

NEW QUESTION 10
HOTSPOT
You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.
How should you complete the command? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: -EnablePurgeProtection
If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.
Box 2: -EnableSoftDelete
Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.

References:
https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault

NEW QUESTION 11
You have an Azure SQL database.
You implement Always Encrypted.
You need to ensure that application developers can retrieve and decrypt data in the database.
Which two pieces of information should you provide to the developers? Each correct answer presents part of the solution.
NOTE: Each correct selection is worth one point.
A. a stored access policy
B. a shared access signature (SAS)
C. the column encryption key
D. user credentials
E. the column master key

Answer: CE

Explanation:
Always Encrypted uses two types of keys: column encryption keys and column master keys. A column encryption key is used to encrypt data in an encrypted column. A column master key is a key-protecting key that encrypts one or more column encryption keys.
References:

NEW QUESTION 12
Your company uses Azure DevOps. You need to recommend a method to validate whether the code meets the company's quality standards and code review standards. What should you recommend implementing in Azure DevOps?

A. branch folders
B. branch permissions
C. branch policies
D. branch locking

Answer: C

Explanation:
Branch policies help teams protect their important branches of development. Policies enforce your team's code quality and change management standards.
References:

NEW QUESTION 13
......
We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions
2nd - Questions and Answers in PDF Format

az-500 Practice Exam Features:

* az-500 Questions and Answers Updated Frequently
* az-500 Practice Questions Verified by Expert Senior Certified Staff
* az-500 Most Realistic Questions that Guarantee you a Pass on Your First Try
* az-500 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The az-500 Practice Test Here