Vendor: Microsoft

Exam Code: AZ-500

Exam Name: Microsoft Azure Security Technologies

Version: DEMO

QUESTION 1
Case Study 1 - Litware, Inc
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

You need to meet the identity and access requirements for Group1.

What should you do?

A. Add a members
hip 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 Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

Answer: D
Explanation:
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-dynamic-membership
It states clearly that "You can create a dynamic group for devices or for users, but you can't create a rule that contains both users and devices."
https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/groups-create-rule

QUESTION 2
Case Study 2 - Contoso, Ltd
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*

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

QUESTION 3
Case Study 3 - Fabrikam, Inc
General Overview

Fabrikam, Inc. is a consulting company that has a main office in Montreal and branch offices in Seattle and New York. Fabrikam has IT, human resources (HR), and finance departments.

Existing Environment
Network Environment
Fabrikam has a Microsoft 365 subscription and an Azure subscription named subscription1.

The network contains an on-premises Active Directory domain named Fabrikam.com. The domain contains two organizational units (OUs) named OU1 and OU2. Azure AD Connect cloud sync syncs only OU1.

The Azure resources hierarchy is shown in the following exhibit.

The Azure Active Directory (Azure AD) tenant contains the users shown in the following table.

Name	Type	Directory-synced	Role	Delegated to
User1	User	Yes	User	**None**
Admin1	User	No	User Access Administrator	Tenant Root Group
Admin2	User	No	Security administrator	MG1
Admin3	User	No	Contributor	Subscription1
Admin4	User	No	Owner	RG1
Group1	Group	No	**Not applicable**	**None**

You need to recommend which virtual machines to use to host App1. The solution must meet the technical requirements for KeyVault1.
Which virtual machines should you use?

A. VM1 only
B. VM1 and VM2 only
C. VM1, VM2, and VM4 only
D. VM1, VM2, VM3, and VM4

Answer: D
Explanation:
All VMs can access KV1 through private endpoint in VNET1/Subnet1. All VNETs are peered, so all the traffic traverse Microsoft backbone network without any exposure to public Internet.

The private endpoint can be reached from the same virtual network, regionally peered VNets, globally peered VNets and on premises using private VPN or ExpressRoute connections.
https://docs.microsoft.com/en-us/azure/private-link/private-link-service-overview

The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure. Like traffic between virtual machines in the same network, traffic is routed through Microsoft's private network only.
https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview

QUESTION 4
You have an Azure subscription that contains an Azure SQL database named DB1 in the East US Azure region.
You create the storage accounts shown in the following table.

Name	Location	Performance	Premium account type
storage1	East US	Standard	**Not applicable**
storage2	East US	Premium	Block blobs
storage3	East US	Premium	File shares
storage4	East US 2	Standard	**Not applicable**

You plan to enable auditing for DB1.
Which storage accounts can you use as the auditing destination for DB1?

A. storage1 and storage4 only
B. storage1 only
C. storage1, storage2, storage3, and storage4
D. storage1, storage2, and storage3 only
E. storage2 and storage3 only

Answer: D
Explanation:
The storage account is required in the same region, so storage 1, 2 and 3 should be selected.
https://learn.microsoft.com/en-us/azure/azure-sql/managed-instance/auditing-configure?view=azuresql

QUESTION 5
You are troubleshooting a security issue for an Azure Storage account.
You enable Azure Storage Analytics logs and archive it to a storage account.
What should you use to retrieve the diagnostics logs?

A. Azure Cosmos DB explorer
B. Azure Monitor
C. Microsoft Defender for Cloud
D. Azure Storage Explorer

Answer: D
Explanation:
One of the simplest ways to set/get an Azure Storage Blob's metadata is by using the cross-platform Microsoft Azure Storage Explorer, which is a standalone app from Microsoft that allows you to easily work with Azure Storage data on Windows, macOS and Linux.
Note: All logs are stored in block blobs in a container named $logs, which is automatically created when Storage Analytics is enabled for a storage account.
If you use your storage-browsing tool to navigate to the container directly, you will see all the blobs that contain your logging data. Most storage browsing tools enable you to view the metadata of blobs; you can also read this information using PowerShell or programmatically.

Reference:
https://azure.microsoft.com/en-us/features/storage-explorer/
https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging

QUESTION 6
You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.
You plan to enable passwordless authentication for the tenant.
You need to ensure that User1 can enable the combined registration experience. The solution must use the principle of least privilege.
Which role should you assign to User1?

A. Security administrator
B. Privileged role administrator
C. Authentication administrator
D. Global administrator

Answer: D
Explanation:
https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-authentication-passwordless-deployment#required-roles
Authentication Administrator can only implement and manage authentication methods, NOT implement combined registration experiences.
User admin or Global admin.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-registration-mfa-sspr-combined

QUESTION 7
You have the Azure resource shown in the following table.

Name	Type	Parent
Management1	Management group	Tenant Root Group
Subscription1	Subscription	Management1
RG1	Resource group	Subscription1
RG2	Resource group	Subscription1
VM1	Virtual machine	RG1
VM2	Virtual machine	RG2

You need to meet the following requirements:

- Internet-facing virtual machines must be protected by using network security groups (NSGs).
- All the virtual machines must have disk encryption enabled.

What is the minimum number of security that you should create in Azure Security Center?

A. 1
B. 2
C. 3
D. 4

Answer: B
Explanation:
Apply the two policies at the subscription or management group and your covered on both VMs.

QUESTION 8
Hotspot Question

You have an Azure subscription that contains an Azure key vault. The role assignments for the key vault are shown in the following exhibit.

```
[
    {
        "RoleAssignmentId": "3336fcbf-33d8-4c8a-85b6-d8edd964762b",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
        "DisplayName": "User1",
        "SignInName": "User1@contoso.com",
        "RoleDefinitionName": "Owner",
        …
    },
    {
        "RoleAssignment": "9d080a14-246e-4580-8b8b-077bfec22f7c",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-
de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
        "DisplayName": "User2",
        "SignInName": "User2@contoso.com",
        "RoleDefinitionName": "Key Vault Crypto Officer",
        …
    },
    {
        "RoleAssignmentId": "0d61eae6-4612-4ee2-88f3-fb6dab84eb10",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-
de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault1",
        "DisplayName": "User3",
        "SignInName": "User3@contoso.com",
        "RoleDefinitionName": "Key Vault Secrets Officer",
        …
    },
    {
        "RoleAssignmentId": "f1e46302-c5d0-4519-9ee7-128594eea97c",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-
de37baaa7ffa/resourceGroups/RG3/providers/Microsoft.KeyVault/vaults/KeyVault1/keys/Key1",
        "DisplayName": "User4",
        "SignInName": "User4@contoso.com",
        "RoleDefinitionName": "Key Vault Administrator",
        …

    }
]
```


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.

Answer Area

[Answer choice] can create keys in the key vault.

- Only User1
- Only User2
- Only User1 and User4
- Only User1, User2, and User4
- User1, User2, User3, and User4

[Answer choice] can create secrets in the key vault.

- Only User3
- Only User1 and User3
- Only User3 and User4
- Only User1, User3, and User4
- User1, User2, User3, and User4

Answer:

Answer Area

[Answer choice] can create keys in the key vault.

- Only User1
- Only User2
- Only User1 and User4
- Only User1, User2, and User4
- User1, User2, User3, and User4

[Answer choice] can create secrets in the key vault.

- Only User3
- Only User1 and User3
- Only User3 and User4
- Only User1, User3, and User4
- User1, User2, User3, and User4

Explanation:
Box 1: Only User2
Box 2: Only User3

User1 - has ownership at subscription level therefore has access to the control plane of the key vault but not to the data plane. therefore User1 can manage RBAC permissions but cannot create/access keys or secrets (unless they can grant themself 'Key Administrator' access and do this, which again does not show up in this RBACs listed so we cannot assume that)
- Therefore User1 has not access to the keys or secrets in this vault.
User2 - Is a Key VAult Crypto officer for the KeyVault1. so according to this:https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli#azure-built-in-roles-for-key-vault-data-plane-operations, they can manage keys (but not access secrets or manage permissions)
User3 - Is a Secrets officer for the KeyVault1 scope. they can access secrets data in this key vault
User4 - Here's a tricky one. while they are indeed given 'Key Vault Administrator', notice the scope is set to "../KeyVault1/Keys/Key1". So they should only be able to work with that key.

Reference:
https://docs.microsoft.com/en-us/azure/key-vault/general/rbac-guide

QUESTION 9
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

QUESTION 10
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

QUESTION 11
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: C
Explanation:
https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-enable-overview
You can deploy Azure VMs from any region. These VMs aren't limited to the regions supported by the Log Analytics workspace.

QUESTION 12
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

QUESTION 13
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 deploy the On-premises data gateway to the on-premises network.

Does this meet the goal?

A. Yes
B. No

Answer: B
Explanation:
Instead, you 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

QUESTION 14
You have an Azure Active Directory (Azure AD) tenant that contains a user named Admin1.
Admin1 is assigned the Application developer role.

You purchase a cloud app named App1 and register App1 in Azure AD.

Admin1 reports that the option to enable token encryption for App1 is unavailable.

You need to ensure that Admin1 can enable token encryption for App1 in the Azure portal.

What should you do?

A. Upload a certificate for App1.
B. Modify the API permissions of App1.
C. Add App1 as an enterprise application.
D. Assign Admin1 the Cloud application administrator role.

Answer: C
Explanation:
This is a tricky one because uploading a certificate is also required. However, the QUESTION 3states that the Token Encryption option is unavailable. This is because the app is not added as an enterprise application. When the app is added as an enterprise application, the Token Encryption option will be available. Then you can upload the certificate.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/howto-saml-token-encryption

QUESTION 15
You are in the process of configuring an Azure policy via the Azure portal.

Your policy will include an effect that will need a managed identity for it to be assigned.

Which of the following is the effect in question?

A. AuditIfNotExist
B. Disabled
C. DeployIfNotExist
D. EnforceOPAConstraint

Answer: C
Explanation:
When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.
Reference:
https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources

QUESTION 16
Note: The question is included in a number of questions that depicts the identical set-up. However, every question has a distinctive result. Establish if the solution satisfies the requirements.

Your company's Azure subscription is linked to their Azure Active Directory (Azure AD) tenant.

After an internally developed application is registered in Azure AD, you are tasked with making sure that the application has the ability to access Azure Key Vault secrets on application the users' behalf.

Solution: You configure a delegated permission with no admin consent.

Does the solution meet the goal?

A. Yes
B. No

Answer: A
Explanation:
Delegated permissions -Your client application needs to access the web API as the signed-in user, but with access limited by the selected permission. This type of permission can be granted by a user unless the permission requires administrator consent.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis

QUESTION 17
You need to consider the underlined segment to establish whether it is accurate.

Your Azure Active Directory Azure (Azure AD) tenant has an Azure subscription linked to it.

Your developer has created a mobile application that obtains Azure AD access tokens using the OAuth 2 implicit grant type.

The mobile application must be registered in Azure AD.

You require a redirect URI from the developer for registration purposes.

Select "No adjustment required" if the underlined segment is accurate. If the underlined segment is inaccurate, select the accurate option.

A. No adjustment required
B. a secret
C. a login hint
D. a client ID

Answer: A
Explanation:
For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code

QUESTION 18
You have an Azure subscription that contains a resource group named RG1 and the identities shown in the following table.

Name	Type	Azure AD roles can be assigned to the group
User1	User	*Not applicable*
Group1	Microsoft 365 group	Yes
Group2	Security group	No
Group3	Security group	Yes
Group4	Security group	Yes

You assign Group4 the Contributor role for RG1.
Which identities can you add to Group4 as members?

A. User1 only
B. User1 and Group3 only
C. User1, Group1, and Group3 only
D. User1, Group2, and Group3 only
E. User1, Group1, Group2, and Group3

Answer: A
Explanation:
Group nesting is not supported. A group can't be added as a member of a role-assignable group.
Create a role-assignable group in Azure Active Directory
https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible
Use Azure AD groups to manage role assignments
https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-concept

QUESTION 19
Hotspot Question

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

Name	Azure region	Connected to	Associated network security group (NSG)
VM1	West US	VNET1/Subnet1	None
VM2	West US	VNET1/Subnet2	NSG2
VM3	Central US	VNET2/Subnet1	NSG3
VM4	West US	VNET3/Subnet1	NSG4

VNET1, VNET2, and VNET3 are peered with each other.
You perform the following actions:

```
- Create two application security groups named ASG1 and ASG2 in the
West US region.
- Add the network interface of VM1 to ASG1.
```

The network interfaces of which virtual machines can you add to ASG1 and ASG2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

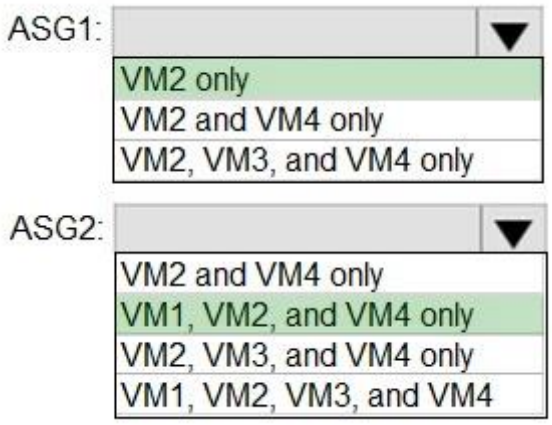
Answer Area

ASG1:
- VM2 only
- VM2 and VM4 only
- VM2, VM3, and VM4 only

ASG2:
- VM2 and VM4 only
- VM1, VM2, and VM4 only
- VM2, VM3, and VM4 only
- VM1, VM2, VM3, and VM4

Answer:

Answer Area



Explanation:
Box1: VM2 only
Add the network interface of VM1 to ASG1. VM1 is in VET1, all available ASGs must be in VNET1.
Box2: VM1, VM2 and VM4 only
The catch is that you cannot add VM1/VM2 and VM4 to ASG2 at the same time. Once you add VM1 or VM2 to ASG2, VM4 is out. Once you add VM4 to ASG2, VM1 and VM2 are out.

QUESTION 20
You have an Azure AD tenant that contains the identities shown in the following table.

Type	Amount
User	1,000
Microsoft 365 group	200
Mail-enabled security group	65
Security group	25

You plan to implement Azure AD Identity Protection.
What is the maximum number of user risk policies you can configure?

A. 1
B. 90
C. 200
D. 265
E. 1000

Answer: A
Explanation:
You can only configure one user risk policy per tenant.
https://janbakker.tech/microsoft-secure-score-series-11-turn-on-user-risk-policy/#:~:text=You%20can%20only%20configure%20one%20user%20risk%20policy%20per%20tenant

Thank You for Trying Our Product

Passleader Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.passleader.com/all-products.html

10% Discount Coupon Code: **ASTR14**