



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.

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 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:

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

NEW QUESTION 2

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
<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Create an access review program.</div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Set Reviewers to Selected users.</div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Create an access review audit. ⬅</div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Create an access review control. ➡</div> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Set Reviewers to Group owners.</div> <div style="border: 1px solid #ccc; padding: 2px;">Set Reviewers to Members.</div>	⬆ ⬇

- A. Mastered
- B. Not Mastered

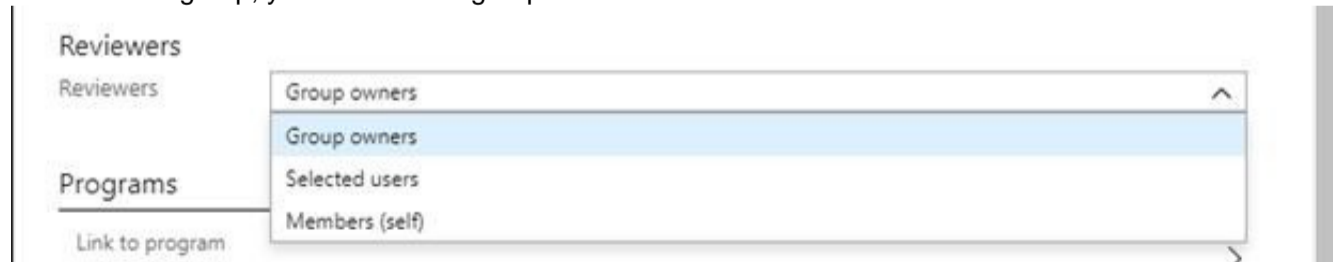
Answer: A

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 3

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

Answer Area

- Verify your identity by using multi-factor authentication (MFA).
- Consent to PIM.
- Sign up PIM for Azure AD roles.
- Discover privileged roles.
- Discover resources.

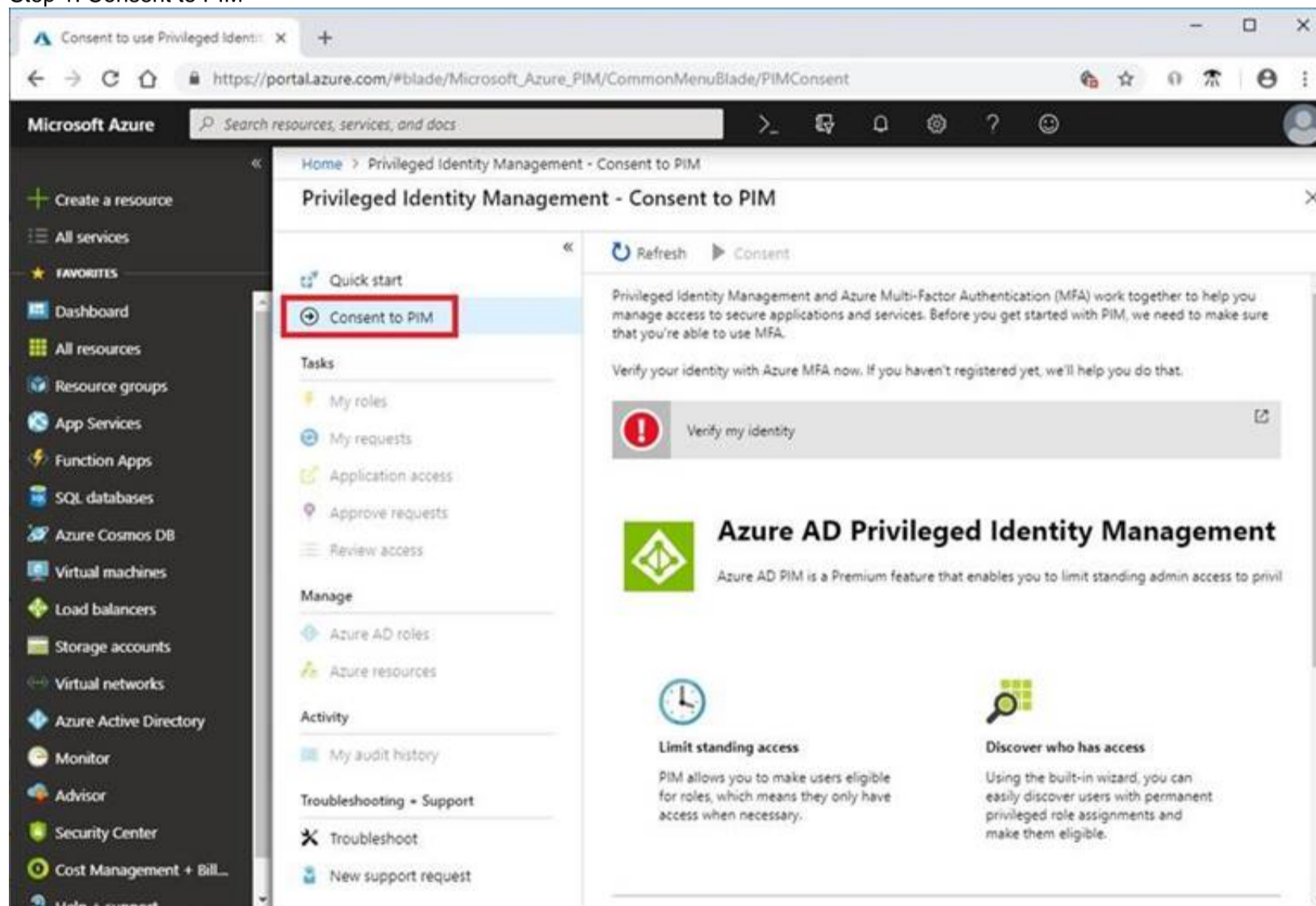


- A. Mastered
- B. Not Mastered

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 4

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. Yes No
- If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. Yes No
- If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone Yes No

- 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 5

You have an Azure subscription.

You create an Azure web app named Contoso1812 that uses an S1 App service plan.

You create a DNS record for www.contoso.com that points to the IP address of Contoso1812.

You need to ensure that users can access Contoso1812 by using the https://www.contoso.com URL. Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Turn on the system-assigned managed identity for Contoso1812.
- B. Add a hostname to Contoso1812.
- C. Scale out the App Service plan of Contoso1812.
- D. Add a deployment slot to Contoso1812.
- E. Scale up the App Service plan of Contoso1812.

Answer: BE

Explanation:

B: You can configure Azure DNS to host a custom domain for your web apps. For example, you can create an Azure web app and have your users access it using either www.contoso.com or contoso.com as a fully qualified domain name (FQDN).

To do this, you have to create three records:

A root "A" record pointing to contoso.com A root "TXT" record for verification

A "CNAME" record for the www name that points to the A record

E: To map a custom DNS name to a web app, the web app's App Service plan must be a paid tier (Shared, Basic, Standard, Premium or Consumption for Azure Functions). I

Scale up the App Service plan: Select any of the non-free tiers (D1, B1, B2, B3, or any tier in the Production category). References:

<https://docs.microsoft.com/en-us/azure/dns/dns-web-sites-custom-domain>

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 6

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 7

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 8

DRAG DROP

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

Name	Region	Description
HubVNet	East US	HubVNet is a virtual network connected to the on-premises network by using a site-to-site VPN that has BGP route propagation enabled. HubVNet contains a subnet named HubVNetSubnet0.
SpokeVNet	East US	SpokeVNet is a virtual network connected to HubVNet by using VNet peering. SpokeVNet contains a subnet named SpokeVNetSubnet0.

The Azure virtual machines on SpokeVNetSubnet0 can communicate with the computers on the on-premises network. You plan to deploy an Azure firewall to HubVNet.

You create the following two routing tables:

- RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway

You need to ensure that traffic between SpokeVNetSubnet0 and the on-premises network flows through the Azure firewall.

To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet 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:

Subnets

- Azure FirewallSubnet
- GatewaySubnet
- HubVNetSubnet0

Answer Area

RT1:

RT2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Subnets

- Azure FirewallSubnet
- GatewaySubnet
- HubVNetSubnet0

Answer Area

- RT1: GatewaySubnet
- RT2: HubVNetSubnet0

NEW QUESTION 9

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 10

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 10

HOTSPOT

You have Azure virtual machines that have Update Management enabled. The virtual machines are configured as shown in the following table.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West US	RG1
VM3	Windows Server 2016	West US	RG2
VM4	Ubuntu Server 18.04 LTS	West US	RG2
VM5	Red Hat Enterprise Linux 7.4	East US	RG1
VM6	CentOS 7.5	East US	RG1

You schedule two update deployments named Update1 and Update2. Update1 updates VM3. Update2 updates VM6.

Which additional virtual machines can be updated by using Update1 and Update2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Update1: ▼

VM2 only
VM4 only
VM1 and VM2 only
VM1, VM2, VM4, VM5, and VM6

Update2: ▼

VM5 only
VM1 and VM5 only
VM4 and VM5 only
VM1, VM2, and VM5 only
VM1, VM2, VM3, VM4, and VM5

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Update1: VM1 and VM2 only

VM3: Windows Server 2016 West US RG2

Update2: VM4 and VM5 only VM6: CentOS 7.5 East US RG1

For Linux, the machine must have access to an update repository. The update repository can be private or public. References:
<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>

NEW QUESTION 13

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: ▼

1
2
3
4

Network security rules: ▼

1
2
3
4

- 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 17

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 21

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

What should you do first?

- A. Turn on Auto Provisioning in Security Center.
- B. Integrate Security Center and Microsoft Cloud App Security.
- C. Upgrade the pricing tier of Security Center to Standard.
- D. 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 25

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.

Hot Area:

Answer Area

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and  == 4625
    

|              |
|--------------|
| ActivityID   |
| DataType     |
| EventID      |
| QuantityUnit |

| Summarize failed_login_attempts= 

|            |
|------------|
| Count(),   |
| Countif(), |
| Makeset(), |
| Split(),   |

latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5
```

- 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 = 1d; SecurityEvent | where TimeGenerated > ago(1d) | where 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 27

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 28

HOTSPOT

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. You plan to implement an application that will consist of the resources shown in the following table.

Name	Type	Description
CosmosDBAccount1	Azure Cosmos DB account	A Cosmos DB account containing a database Named CosmosDB1 that serves as a back-end tier of the application
WebApp1	Azure web app	A web app configured to serve as the middle tier of the application

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens. You need to identify which tasks will

be implemented in CosmosDB1 and WebApp1.
 Which task should you identify for each resource? To answer, select the appropriate options in the answer area.
 NOTE: Each correct selection is worth one point.
 Hot Area:

Answer Area

CosmosDB1: ▼

- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

WebApp1: ▼

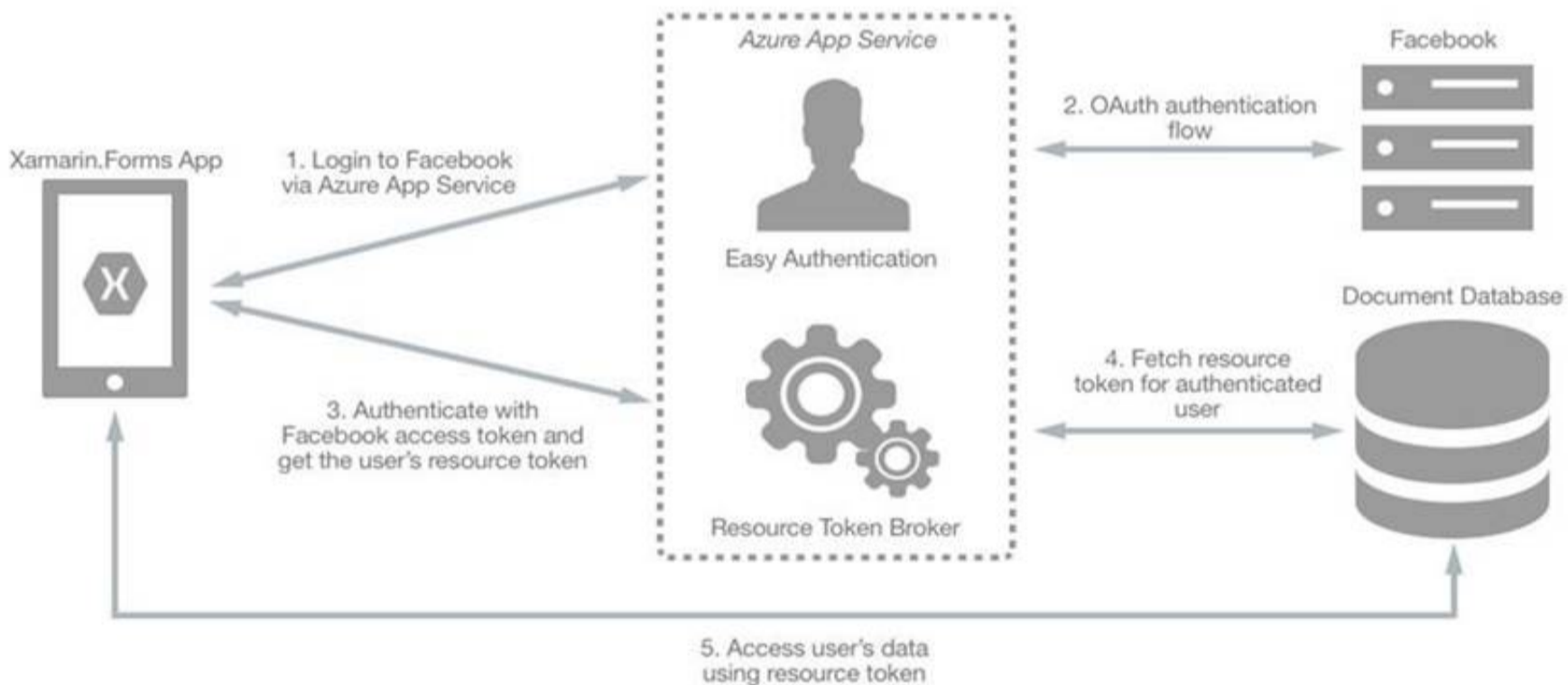
- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

CosmosDB1: Create database users and generate resource tokens.
 Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.
 WebApp1: Authenticate Azure AD users and relay resource tokens
 A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:



References:
<https://docs.microsoft.com/en-us/xamarin/xamarin-forms/data-cloud/cosmosdb/authentication>

NEW QUESTION 32

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.
 Hot Area:

Answer Area

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'
```

`-Location 'East US'` ▼ ▼

- EnabledForDeployment
- EnablePurgeProtection
- Tag

- Confirm
- DefaultProfile
- EnableSoftDelete
- SKU

- 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/azurearm.keyvault/new-azurearmkeyvault>

NEW QUESTION 34

You have a hybrid configuration of Azure Active Directory (Azure AD).

All users have computers that run Windows 10 and are hybrid Azure AD joined.

You have an Azure SQL database that is configured to support Azure AD authentication.

Database developers must connect to the SQL database by using Microsoft SQL Server Management Studio (SSMS) and authenticate by using their on-premises Active Directory account.

You need to tell the developers which authentication method to use to connect to the SQL database from SSMS. The solution must minimize authentication prompts.

Which authentication method should you instruct the developers to use?

- A. SQL Login
- B. Active Directory – Universal with MFA support
- C. Active Directory – Integrated
- D. Active Directory – Password

Answer: C

Explanation:

Azure AD can be the initial Azure AD managed domain. Azure AD can also be an on-premises Active Directory Domain Services that is federated with the Azure AD.

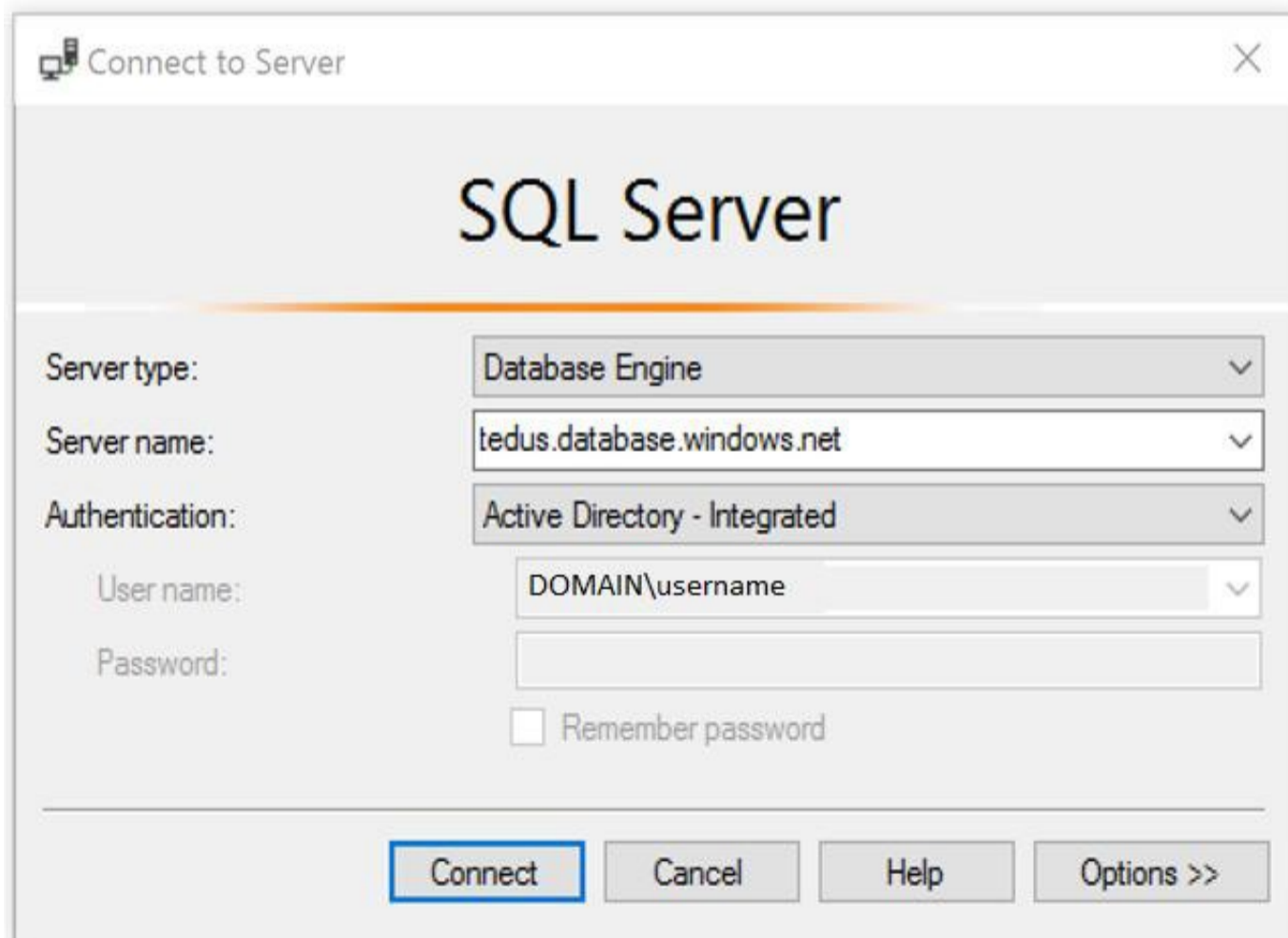
Using an Azure AD identity to connect using SSMS or SSDT

The following procedures show you how to connect to a SQL database with an Azure AD identity using SQL Server Management Studio or SQL Server Database Tools.

Active Directory integrated authentication

Use this method if you are logged in to Windows using your Azure Active Directory credentials from a federated domain.

1. Start Management Studio or Data Tools and in the Connect to Server (or Connect to Database Engine) dialog box, in the Authentication box, select Active Directory - Integrated. No password is needed or can be entered because your existing credentials will be presented for the connection.



2. Select the Options button, and on the Connection Properties page, in the Connect to database box, type the name of the user database you want to connect to. (The AD domain name or tenant ID" option is only supported for Universal with MFA connection options, otherwise it is greyed out.)

References:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/sql-database/sql-database-aad-authentication-configure.md>

NEW QUESTION 35

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 36

.....

Thank You for Trying Our Product

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 FirstTry
- * az-500 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The az-500 Practice Test Here](#)