



Microsoft

Exam Questions az-500

Microsoft Azure Security Technologies

About ExamBible

[Your Partner of IT Exam](#)

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1

- (Exam Topic 4)

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

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Enabled
User2	Group1	Disabled
User3	Group1	Disabled

You create and enforce an Azure AD Identity Protection sign-in risk policy that has the following settings: ➤ Assignments: Include Group1, exclude Group2

➤ Conditions: Sign-in risk level: Medium and above

➤ Access Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Azure AD.

What should you identify for each user? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

When User1 signs in from an anonymous IP address, the user will:

▼

Be blocked

Be prompted for MFA

Sign in by using a username and password only

When User2 signs in from an unfamiliar location, the user will:

▼

Be blocked

Be prompted for MFA

Sign in by using a username and password only

When User3 signs in from an infected device, the user will:

▼

Be blocked

Be prompted for MFA

Sign in by using a username and password only

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies> <https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks>

NEW QUESTION 2

- (Exam Topic 4)

Lab Task

Task 3

You need to ensure that a user named Danny-31330471 can sign in to any SQL database on a Microsoft SQL server named web31330471 by using SQL Server Management Studio (SSMS) and Azure AD credentials.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Create and register an Azure AD application. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name, such as SQLServerCTP1, and select the supported account types, such as Accounts in this organization directory only.

Grant application permissions. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Directory.Read.All permission to the application and grant admin consent for your organization.

Create and assign a certificate. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to create a self-signed certificate and upload it to the application. You also need to store the certificate in Azure Key Vault and grant access policies to the application and your SQL Server.

Configure Azure AD authentication for SQL Server through Azure portal. You can use the Azure portal to do this. You need to select your SQL Server resource and enable Azure AD authentication. You also need to select your Azure AD application as the Azure AD admin for your SQL Server.

Create logins and users. You can use SSMS or Transact-SQL to do this. You need to connect to your SQL Server as the Azure AD admin and create a login for Danny-31330471. You also need to create a user for Danny-31330471 in each database that he needs access to.

Connect with a supported authentication method. You can use SSMS or SqlClient to do this. You need to specify the Authentication connection property in the connection string as Active Directory Password or Active Directory Integrated. You also need to provide the username and password of Danny-31330471.

NEW QUESTION 3

- (Exam Topic 4)

You have an Azure web app named WebApp1. You upload a certificate to WebApp1.

You need to make the certificate accessible to the app code of WebApp1. What should you do?

- A. Add a user-assigned managed identity to WebApp1.
- B. Add an app setting to the WebApp1 configuration.
- C. Enable system-assigned managed identity for the WebApp1.
- D. Configure the TLS/SSL binding for WebApp1.

Answer: B

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate-in-code>

NEW QUESTION 4

- (Exam Topic 4)

You are testing an Azure Kubernetes Service (AKS) cluster. The cluster is configured as shown in the exhibit. (Click the Exhibit tab.)

BASICS	
Subscription	Microsoft Azure Sponsorship
Resource group	AzureBackupRG_eastus2_1
Region	East US
Kubernetes cluster name	akscluster2
Kubernetes version	1.1 1.5
DNS name prefix	akscluster2
Node count	3
Node size	Standard_DS2_v2
Virtual nodes (preview)	Disabled
AUTHENTICATION	
Enable RBAC	No
NETWORKING	
HTTP application routing	Yes
Network configuration	Basic
MONITORING	
Enable container monitoring	No
TAGS	

You plan to deploy the cluster to production. You disable HTTP application routing.
You need to implement application routing that will provide reverse proxy and TLS termination for AKS services by using a single IP address.
What should you do?

- A. Create an AKS Ingress controller.
- B. Install the container network interface (CNI) plug-in.
- C. Create an Azure Standard Load Balancer.
- D. Create an Azure Basic Load Balancer.

Answer: A

Explanation:

An ingress controller is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.
References:
<https://docs.microsoft.com/en-us/azure/aks/ingress-tls>

NEW QUESTION 5

- (Exam Topic 4)

On Monday, you configure an email notification in Microsoft Defender for Cloud to notify user1@contoso.com about alerts that have a severity level of Low, Medium, or High. On Tuesday, Microsoft Defender for Cloud generates the security alerts shown in the following table.

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will user1 @contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday:

4

1

2

3

4

Total number of Microsoft Defender for Cloud email notifications on Tuesday:

7

3

4

7

9

11

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack on Tuesday:

4

1

2

3

4

Total number of Microsoft Defender for Cloud email notifications on Tuesday:

7

3

4

7

9

11

NEW QUESTION 6

- (Exam Topic 4)

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 has an Active Directory forest with a single domain, named weylanindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of password hash synchronization and seamless SSO. Does the solution meet the goal?

- A. Yes
- B. No

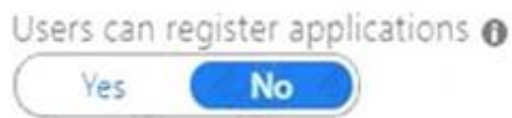
Answer: B

NEW QUESTION 7

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant and a user named User1. The App registrations settings for the tenant are configured as shown in the following exhibit.

App registrations



You plan to deploy an app named App1.
You need to ensure that User1 can register App1 in Azure AD. The solution must use the principle of least privilege.
Which role should you assign to User1?

- A. App Configuration Data Owner for the subscription
- B. Managed Application Contributor for the subscription
- C. Cloud application administrator in Azure AD
- D. Application developer in Azure AD.

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-by-task>

NEW QUESTION 8

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud. The subscription contains the Azure Policy definitions shown in the following table.

Name	Type	Category
Policy1	Policy	Regulatory Compliance
Policy2	Policy	Security Center
Initiative1	Initiative	Regulatory Compliance
Initiative2	Initiative	Security Center

Which definitions can be assigned as a security policy in Defender for Cloud?

- A. Policy1 and Policy2 only
- B. Initiative1 and Initiative2 only
- C. Policy1 and Initiative1 only
- D. Policy2 and Initiative2 only
- E. Policy1, Policy2, Initiative1, and Initiative2

Answer: D

NEW QUESTION 9

- (Exam Topic 4)

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

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

From Azure AD Privileged Identity Management (PIM), you configure the settings for the Security Administrator role as shown in the following exhibit.

Settings

X

Assignment

☒ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

☒ Allow permanent active assignment

Expire active assignments after

1 Month

☐ Require Azure Multi-Factor Authentication on active assignment

☒ Require justification on active assignment

Activation

Activation maximum duration (hours)

5

☐ Require Azure Multi-Factor Authentication on activation

☐ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

Select approvers

No member or group selected

From PIM, you assign the Security Administrator role to the following groups:

- > Group1: Active assignment type, permanently assigned
- > Group2: Eligible assignment type, permanently eligible

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can only activate the Security Administrator role in five hours.	<input type="radio"/>	<input type="radio"/>
If User2 activates the Security Administrator role, the user will be assigned the role immediately.	<input type="radio"/>	<input type="radio"/>
User3 can activate the Security Administrator role.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

Eligible Type: A role assignment that requires a user to perform one or more actions to use the role. If a user has been made eligible for a role, that means they can activate the role when they need to perform privileged tasks. There's no difference in the access given to someone with a permanent versus an eligible role assignment. The only difference is that some people don't need that access all the time.

You can choose from two assignment duration options for each assignment type (eligible and active) when you configure settings for a role. These options become the default maximum duration when a user is assigned to the role in Privileged Identity Management.

Use the Activation maximum duration slider to set the maximum time, in hours, that a role stays active before it expires. This value can be from one to 24 hours.

Box 2: Yes

Active Type: A role assignment that doesn't require a user to perform any action to use the role. Users assigned as active have the privileges assigned to the role

Box 3: Yes

User3 is member of Group2. Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure> <https://docs.microsoft.com/bs-cyrl-ba/azure/active-directory/privileged-identity-management/pim-resource-roles>

NEW QUESTION 10

- (Exam Topic 4)

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

Name	Member of	Multi-factor authentication (MFA) status
User1	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

Azure AD Privileged Identity Management (PIM) is enabled for the tenant. In PIM, the Password Administrator role has the following settings:

- Maximum activation duration (hours): 2
- Send email notifying admins of activation: Disable
- Require incident/request ticket number during activation: Disable
- Require Azure Multi-Factor Authentication for activation: Enable
- Require approval to activate this role: Enable
- Selected approver: Group1

You assign users the Password Administrator role as shown in the following table.

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
When User1 signs in, the user is assigned the Password Administrator role automatically.	<input type="radio"/>	<input type="radio"/>
User2 can request to activate the Password Administrator role.	<input type="radio"/>	<input type="radio"/>
If User3 wants to activate the Password Administrator role, the user can approve their own request.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

YES (Already active)

YES (The user will be prompted for MFA regardless the MFA Status of the user) NO (Even the user is included in the group, a user can't approve itself)

<https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-deployment-plan> (Require approval section)

NEW QUESTION 10

- (Exam Topic 4)

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	In resource group
cont1	Container instance	RG1
VNET1	Virtual network	RG1
App1	App Service app	RG1
VM1	Virtual machine	RG1
User1	User	Not applicable

You create a custom RBAC role in Subscription1 by using the following JSON file.


```
{
  "Name": "Role1",
  "IsCustom": true,
  "Description": "Role1 description",
  "Actions": [
    "*/Read",
    "Microsoft.Compute/*"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/subscriptions/923a419a-4358-40fb-b4a9-b8af43dd0c92/resourceGroups/RG1"
  ]
}
```

You assign Role1 to User1 on RG1.

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
User1 can add VM1 to VNET1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop App1.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop cont1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/resource-provider-operations#microsoftcompu>

NEW QUESTION 11

- (Exam Topic 4)

You have three on-premises servers named Server1, Server2, and Server3 that run Windows Server1 and Server2 and located on the Internal network. Server3 is located on the premises network. All servers have access to Azure.

From Azure Sentinel, you install a Windows firewall data connector.

You need to collect Microsoft Defender Firewall data from the servers for Azure Sentinel. What should you do?

- A. Create an event subscription from Server1, Server2 and Server3
- B. Install the On-premises data gateway on each server.
- C. Install the Microsoft Agent on each server.
- D. Install the Microsoft Agent on Server1 and Server2 install the on-premises data gateway on Server3.

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/connect-windows-firewall>

NEW QUESTION 13

- (Exam Topic 4)

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

Name	Type	Attached to	NSG
NSG1	Network security group (NSG)	VM5	<i>Not applicable</i>
NSG2	Network security group (NSG)	Subnet1	<i>Not applicable</i>
Subnet1	Subnet	<i>Not applicable</i>	<i>Not applicable</i>
VM5	Virtual machine	Subnet1	NSG1

An IP address of 10.1.0.4 is assigned to VM5. VM5 does not have a public IP address. VM5 has just in time (JIT) VM access configured as shown in the following exhibit.

JIT VM access configuration

VM5








+ Add  Save  Discard

Configure the ports for which the just-in-time VM access will be applicable

Port	Protocol	Allowed source IPs	IP range	Time range (hours)	
3389	Any	Per request	N/A	3 hours	...

You enable JIT VM access for VM5.

NSG1 has the inbound rules shown in the following exhibit.

Priority	Name	Port	Protocol	Source	Destination	Action
100	 SecurityCenter-JITRule-...	3389	Any	Any	10.1.0.4	 Allow
1000	SecurityCenter-JITRule_341...	3389	Any	Any	10.1.0.4	 Deny
1001	RDP	3389	TCP	Any	Any	 Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow
65001	AllowAzureLoadBalancerIn...	Any	Any	AzureLoadBalancer	Any	 Allow
65500	DenyAllInBound	Any	Any	Any	Any	 Deny

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input type="radio"/>	<input type="radio"/>
Remote Desktop access to VM5 is blocked.	<input type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
Deleting the security rule that has a priority of 100 will revoke the approved JIT access request.	<input checked="" type="radio"/>	<input type="radio"/>
Remote Desktop access to VM5 is blocked.	<input checked="" type="radio"/>	<input type="radio"/>
An Azure Bastion host will enable Remote Desktop access to VM5 from the internet.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 15

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named sql1. You plan to audit sql1.

You need to configure the audit log destination. The solution must meet the following requirements:

- > Support querying events by using the Kusto query language.
- > Minimize administrative effort. What should you configure?

- A. an event hub
B. a storage account

C. a Log Analytics workspace

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/tutorial-log-analytics-wizard>

NEW QUESTION 17

- (Exam Topic 4)

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.

F. Upload a PFX file to Contoso1812

Answer: BF

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

F: To use HTTPS, you need to upload a PFX file to the Azure Web App. The PFX file will contain the SSL certificate required for HTTPS.

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

NEW QUESTION 18

- (Exam Topic 4)

You have an Azure subscription that contains an instance of Azure Firewall Standard named AzFWL You need to identify whether you can use the following features with AzFW1:

- TLS inspection
- Threat intelligence
- The network intrusion detection and prevention systems (IDPS) What can you use?

A. TLS inspection only

B. threat intelligence only

C. TLS inspection and the IDPS only

D. threat intelligence and the IDPS only

E. TLS inspection, threat intelligence, and the IDPS

Answer: E

NEW QUESTION 20

- (Exam Topic 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 an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

You need to deploy Microsoft Antimalware to the virtual machines. Solution: You add an extension to each virtual machine.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

You can use Visual Studio to enable and configure the Microsoft Antimalware service. This entails selecting Microsoft Antimalware extension from the dropdown list under Installed Extensions and click Add to configure with default antimalware configuration.

References:

<https://docs.microsoft.com/en-us/azure/security/fundamentals/antimalware>

NEW QUESTION 22

- (Exam Topic 4)

You network contains an on-premises Active Directory domain that syncs to an Azure Active Directory (Azure AD) tenant. The tenant contains the users shown in the following table.

Name	Source
User1	Azure AD
User2	Azure AD
User3	On-premises Active Directory

The tenant contains the groups shown in the following table.

Name	Members
Group1	User1, User2, User3
Group2	User2

You configure a multi-factor authentication (MFA) registration policy that and the following settings:

- Assignments:
- Include: Group1
- Exclude Group2

Controls: Require Azure MFA registration Enforce Policy: On

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
User1 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>
User2 must configure MFA during the user's next Azure AD authentication.	<input type="radio"/>	<input checked="" type="radio"/>
User3 will be prompted to configure MFA registration during the user's next Azure AD authentication.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 24

- (Exam Topic 4)

You plan to implement an Azure function named Function1 that will create new storage accounts for containerized application instances.

You need to grant Function1 the minimum required privileges to create the storage accounts. The solution must minimize administrative effort.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Assign role to:

A group account

A system-assigned managed identity

A user account

A user-assigned managed identity

Role assignment to create:

Built-in role assignment

Classic administrator role assignment

Custom role-based access control (RBAC) role assignment

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview> <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/howto-assign-access>

NEW QUESTION 25

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL Database logic server named SQL1 and an Azure virtual machine named VM1. VM1 uses a private IP address only.

The Firewall and virtual networks settings for SQL1 are shown in the following exhibit.

Save Discard Add client IP

Deny public network access

Yes No

Click here to create a new private endpoint.
Create Private Endpoint

Minimum TLS Version

1.0 1.1 1.2

Connection Policy

Default Proxy Redirect

Allow Azure services and resources to access this server

Yes No

Client IP address 89.212.25.106

Rule name Start IP End IP

No firewall rules configured.

Virtual networks

+ Add existing virtual network + Create new virtual network

Rule name Virtual network Subnet

No vnet rules for this server.

You need to ensure that VM1 can connect to SQL1. The solution must use the principle of least privilege. What should you do?

- A. Add an existing virtual network.
B. Set Connection Policy to Proxy.
C. Create a new firewall rule.
D. Set Allow Azure services and resources to access this server to Yes.

Answer: C

NEW QUESTION 27

- (Exam Topic 4)

You have an Azure subscription that contains an app named App1. App1 has the app registration shown in the following table.

API	Permission	Type	Admin consent required	Status
Microsoft.Graph	User.Read	Delegated	No	None
Microsoft.Graph	Calendars.Read	Delegated	No	None

You need to ensure that App1 can read all user calendars and create appointments. The solution must use the principle of least privilege. What should you do?

- A. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.
- B. Add a new Application API permission for Microsoft.Graph Calendars.ReadWrite.
- C. Select Grant admin consent.
- D. Add a new Delegated API permission for Microsoft.Graph Calendars.ReadWrite.Shared.

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/graph/permissions-reference#calendars-permissions>

NEW QUESTION 32

- (Exam Topic 4)

You have an Azure subscription that contains the following Azure firewall:

- Name: Fw1
- Azure region: UK West
- Private IP address: 10.1.3.4
- Public IP address: 23.236.62.147

The subscription contains. The virtual networks shown in the following table.

Name	Location	IP address space	Peered with
Vnet1	UK West	10.1.0.0/16	Vnet2
Vnet2	East US	10.2.0.0/16	Vnet1, Vnet3
Vnet3	West US	10.3.0.0/16	Vnet2,

The subscription contains the subnets shown in the following table.

Name	Virtual network	IP address range
Subnet1-1	Vnet1	10.1.1.0/24
Subnet1-2	Vnet1	10.1.2.0/24
AzureFirewallSubnet	Vnet1	10.1.3.0/24
Subnet2-1	Vnet2	10.2.1.0/24
Subnet3-1	Vnet3	10.3.1.0/24

The subscription contains the routes shown in the following table.

Name	Subnet	IP address prefix	Next hop type	Next hop IP address
Rt1	Subnet1-1	0.0.0.0/0	Virtual appliance	10.1.3.4
Rt2	Subnet1-2	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt3	Subnet2-1	10.1.1.0/24	Virtual appliance	10.1.3.4
Rt4	Subnet3-1	10.2.1.0/24	Virtual appliance	10.1.3.4

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	<input type="radio"/>	<input type="radio"/>
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	<input type="radio"/>	<input type="radio"/>
Traffic from Subnet3-1 to the internet is routed through Fw1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-2 is routed through Fw1.	<input checked="" type="radio"/>	<input type="radio"/>
Traffic from Subnet2-1 to Subnet 1-1 is routed through Fw1.	<input type="radio"/>	<input checked="" type="radio"/>
Traffic from Subnet3-1 to the internet is routed through Fw1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 35

- (Exam Topic 4)

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

Name	Multi-factor authentication (MFA) status
User1	Disabled
User2	Disabled
User3	Enforced

In Azure AD Privileged Identity Management (PIM), the Role settings for the Contributor role are configured as shown in the exhibit. (Click the Exhibit tab.)

Role settings

Assignment

☐ Allow permanent eligible assignment

Expire eligible assignments after

3 Months

☐ Allow permanent active assignment

Expire active assignments after

1 Month

☒ Require Multi-Factor Authentication on active assignment

☒ Require justification on active assignment

Activation

Activation maximum duration (hours)

8

☒ Require Multi-Factor Authentication on activation

☒ Require justification on activation

☐ Require ticket information on activation

☐ Require approval to activate

Select approvers

No member or group selected

You assign users the Contributor role on May 1, 2019 as shown in the following table.

Name	Assignment type
User1	Eligible
User2	Active
User3	Active

For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
On May 15, 2019, User1 can activate the Contributor role.	<input type="radio"/>	<input type="radio"/>
On May 15, 2019, User2 can use the Contributor role.	<input type="radio"/>	<input type="radio"/>
On June 15, 2019, User3 can activate the Contributor role.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-resource-roles-assi>

NEW QUESTION 37

- (Exam Topic 4)

You are configuring just in time (JIT) VM access to a set of Azure virtual machines.

You need to grant users PowerShell access to the virtual machine by using JIT VM access. What should you configure? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Permission that must be granted to users on VM:

Read

Update

View

Write

TCP port that must be allowed:

22

25

3389

5986

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

- * 1. Read permission
* 2. 5986

<https://docs.microsoft.com/en-us/azure/security-center/just-in-time-explained#what-permissions-are-needed-to-c>

NEW QUESTION 42

- (Exam Topic 4)

You have an Azure AD tenant that contains a user named User1. You purchase an App named App1.

User1 needs to publish App1 by using Azure AD Application Proxy. Which role should you assign to User1?

- A. Hybrid identity Administrator
B. Cloud App Security Administrator
C. Application Administrator
D. Cloud Application Administrator

Answer: C

NEW QUESTION 43

- (Exam Topic 4)

You have an Azure Active directory tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You plan to create an Azure file share that will contain folders and files.

Which identity store can you use to assign permissions to the Azure file share and folders within the share? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Azure files share:

Folders in the file share:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Azure files share:

Folders in the file share:

NEW QUESTION 48

- (Exam Topic 4)

You have been tasked with configuring an access review, which you plan to assigned to a new collection of reviews. You also have to make sure that the reviews can be reviewed by resource owners.

You start by creating an access review program and an access review control. You now need to configure the Reviewers.

Which of the following should you set Reviewers to?

- A. Selected users.
- B. Members (Self).
- C. Group Owners.
- D. Anyone.

Answer: C

Explanation:

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.

Graphical user interface, application Description automatically generated with medium confidence

Reviewers

Reviewers

Programs

Link to program

Group owners

Group owners

Selected users

Members (self)

Reference:

<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 50

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a group named Group1 You need to ensure that the members of Group1 sign in by using passwordless authentication What should you do?

- A. Configure the Microsoft Authenticator authentication method policy.
- B. Configure the certificate-based authentication (CBA) policy.
- C. Configure the sign-in risk policy.
- D. Create a Conditional Access policy.

Answer: A

NEW QUESTION 52

- (Exam Topic 4)

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 Storage Explorer
- B. SQL query editor in Azure
- C. Azure Monitor

D. Azure Cosmos DB explorer

Answer: A

NEW QUESTION 54

- (Exam Topic 4)

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.

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:

References:

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

NEW QUESTION 58

- (Exam Topic 4)

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: D

NEW QUESTION 60

- (Exam Topic 4)

You have an Azure subscription that contains a virtual network. The virtual network contains the subnets shown in the following table.

Name	Has a network security group (NSG) associated to the virtual subnet
Subnet1	Yes
Subnet2	No

The subscription contains the virtual machines shown in the following table.

Name	Has an NSG associated to the network adaptor of the virtual machine	Connected to
VM1	No	Subnet1
VM2	No	Subnet2
VM3	No	Subnet1
VM4	Yes	Subnet2

You enable just in time (JIT) VM access for all the virtual machines. You need to identify which virtual machines are protected by JIT. Which virtual machines should you identify?

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

Answer: C**Explanation:**

An NSG needs to be enabled, either at the VM level or the subnet level. Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time>

NEW QUESTION 62

- (Exam Topic 4)

You have an Azure Sentinel deployment.

You need to create a scheduled query rule named Rule1. What should you use to define the query rule logic for Rule1?

- A. a Transact-SQL statement
- B. a JSON definition
- C. GraphQL
- D. a Kusto query

Answer: D**Explanation:**

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-detect-threats-custom>

NEW QUESTION 64

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password. place your cursor in the Enter password box and click on the password below. Azure Username: User1-28681041@ExamUsers.com

Azure Password: GpOAe4@IDg

If the Azure portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only: Lab Instance: 28681041

Task 6

You need to email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes.

- A. Mastered
- B. Not Mastered

Answer: A**Explanation:**

To email an alert to a user named admin1@contoso.com if the average CPU usage of a virtual machine named VM1 is greater than 70 percent for a period of 15 minutes, you can follow these steps:

- In the Azure portal, search for and select the virtual machine named VM1.
- In the left pane, select Alerts.
- Select New alert rule.
- In the New alert rule pane, enter the following information:
- Name: Enter a name for the alert rule.
- Description: Enter a description for the alert rule.
- Condition: Select Metric measurement.

- Resource: Select the virtual machine named VM1.
- Metric: Select Percentage CPU.
- Operator: Select Greater than.
- Threshold: Enter 70.
- Aggregation type: Select Average.
- Period: Select 15 minutes.
- In the Actions pane, select Add action group.
- In the Add action group pane, enter the following information:
- Name: Enter a name for the action group.
- Short name: Enter a short name for the action group.
- Email recipient: Enter the email address of the user you want to receive the alert. For example, admin1@contoso.com.
- Select OK.

NEW QUESTION 65

- (Exam Topic 4)

You have an Azure subscription and the computers shown in the following table.

Name	Operating system	Description
VM1	Windows Server 2012 R2	Azure virtual machine
VM2	Red Hat Enterprise Linux (RHEL) 8.2	Azure virtual machine
Server1	Windows Server 2019	On-premises physical computer connected to Microsoft Defender for Cloud
VMSS1_0	Windows Server 2022	Azure virtual machine in a virtual machine scale set

You need to perform a vulnerability scan of the computers by using Microsoft Defender for Cloud. Which computers can you scan?

- A. VM1 only
- B. VM1 and VM2 only
- C. Server1 and VMSS1.0 only
- D. VM1, VM2, and Server1 only
- E. VM1, VM2, Server1, and VMSS1.0

Answer: A

NEW QUESTION 67

- (Exam Topic 4)

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

Name	Type
storage1	Storage account
KeyVault1	Azure key vault

You need to configure storage1 to regenerate keys automatically every 90 days. Which cmdlet should you run?

- A. set -A=StorageAccount
- B. Add-A:StorogcAccountmanagementPolicyAction
- C. Set-A;StorageAccountimangementPolicy
- D. Add-AsKeyVaultmanageStorageAccount

Answer: D

NEW QUESTION 68

- (Exam Topic 4)

You have an Azure subscription that contains 100 virtual machines and has Azure Security Center Standard tier enabled.

You plan to perform a vulnerability scan of each virtual machine.

You need to deploy the vulnerability scanner extension to the virtual machines by using an Azure Resource Manager template.

Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. the user-assigned managed identity
- B. the workspace ID
- C. the Azure Active Directory (Azure AD) ID
- D. the Key Vault managed storage account key
- E. the system-assigned managed identity
- F. the primary shared key

Answer: AC

NEW QUESTION 72

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant. You have the deleted objects shown in the following table.

Name	Type	Deleted on
Group1	Security group	April 5, 2020
Group2	Office 365 group	April 5, 2020
User1	User	March 25, 2020
User2	User	April 30, 2020

On May 4, 2020, you attempt to restore the deleted objects by using the Azure Active Directory admin center. Which two objects can you restore? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Group1
- B. Group2
- C. User2
- D. User1

Answer: BC

Explanation:

Deleted users and deleted Office 365 groups are available for restore for 30 days. You cannot restore a deleted security group.

Reference:

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

NEW QUESTION 73

- (Exam Topic 4)

You have an Azure subscription that contains two virtual machines named VM1 and VM2 that run Windows Server 2019.

You are implementing Update Management in Azure Automation. You plan to create a new update deployment named Update1.

You need to ensure that Update1 meets the following requirements:

- Automatically applies updates to VM1 and VM2.
- Automatically adds any new Windows Server 2019 virtual machines to Update1. What should you include in Update1?

- A. a security group that has a Membership type of Dynamic Device
- B. a security group that has a Membership type of Assigned
- C. a Kusto query language query
- D. a dynamic group query

Answer: D

NEW QUESTION 75

- (Exam Topic 4)

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.

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

- 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).
- The most sensitive label is applied.
- 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 80

- (Exam Topic 4)

You create an Azure subscription with Azure AD Premium P2.

You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure 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.

Actions

Discover privileged roles.

Sign up PIM for Azure AD roles.

Consent to PIM.

Discover resources.

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

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- * 1. Verify your identity with MFA
- * 2. Consent to PIM
- * 3. Sign up PIM for AAD Roles

NEW QUESTION 82

- (Exam Topic 4)

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

Name	Operating system
VM1	Windows Server 2016
VM2	Ubuntu Server 18.04 LTS

From Azure Security Center, you turn on Auto Provisioning. You deploy the virtual machines shown in the following table.

Name	Operating system
VM3	Windows Server 2016
VM4	Ubuntu Server 18.04 LTS

On which virtual machines is the Microsoft Monitoring agent installed?

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

Answer: D

Explanation:

When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created.

Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803.

References:

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

NEW QUESTION 85

- (Exam Topic 4)

You have an Azure subscription that contains a user named UseR1. You need to ensure that UseR1 can perform the following tasks:

- Create groups.
- Create access reviews for role-assignable groups.
- Assign Azure AD roles to groups.

The solution must use the principle of least privilege. Which role should you assign to User1?

- A. Groups administrator
- B. Authentication administrator
- C. Identity Governance Administrator
- D. Privileged role administrator

Answer: C

NEW QUESTION 90

- (Exam Topic 4)

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

Name	Virtual network	Location
Subnet11	VNet1	West US
Subnet12	VNet1	West US
Subnet21	VNet2	West US

The subscription contains Azure web app named WebApp1 that has the following configurations.

- * Region West Us
- * Virtual network VNet1
- * VNet integration on: Enabled
- * Outbound subnet: Subnet11
- * Windows plan (West US): ASP1

You plan to deploy an Azure web app named WebApp2 that will have the following settings:

- * Region: West US
- * VNet integration on-Enabled
- * Windows plan (West UAS): WebApp2?

To which subnets can you integrate WebApp2?

- A. Subnet11 only
- B. Subnet2 only
- C. Subnet11 or subnet12 only
- D. Subnet2 or Subnet21 only
- E. Subnet11, subnet2, or Subnet21

Answer: C

NEW QUESTION 92

- (Exam Topic 4)

You have an Azure subscription named Sub1. Sub1 has an Azure Storage account named Storage1 that contains the resources shown in the following table.

Name	Type
Container1	Blob container
Share1	File share

You generate a shared access signature (SAS) to connect to the blob service and the file service.

Which tool can you use to access the contents in Container1 and Share! by using the SAS? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Tools for Container1:	<input type="checkbox"/> Robocopy.exe <input type="checkbox"/> Azure Storage Explorer <input type="checkbox"/> File Explorer
Tools for Share1:	<input type="checkbox"/> Robocopy.exe <input type="checkbox"/> Azure Storage Explorer <input type="checkbox"/> File Explorer

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 94

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud.

You have an Amazon Web Services (AWS) account.

You need to ensure that when you deploy a new AWS Elastic Compute Cloud (EC2) instance, the Microsoft Defender for Servers agent installs automatically. What should you configure first?

- A. the log Analytics agent
- B. the Azure Monitor agent
- C. the native cloud connector
- D. the classic cloud connector

Answer: A

NEW QUESTION 96

- (Exam Topic 4)

Lab Task

Task 1

You need to ensure that connections from the Internet to VNET1\subnet0 are allowed only over TCP port 7777. The solution must use only currently deployed resources.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

You need to configure the Network Security Group that is associated with subnet0.

* 1. In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the search results then select VNET1. Alternatively, browse to Virtual Networks in the left navigation pane.

* 2. In the properties of VNET1, click on Subnets. This will display the subnets in VNET1 and the Network Security Group associated to each subnet. Note the name of the Network Security Group associated to Subnet0.

* 3. Type Network Security Groups into the search box and select the Network Security Group associated with Subnet0.

* 4. In the properties of the Network Security Group, click on Inbound Security Rules.

* 5. Click the Add button to add a new rule.

* 6. In the Source field, select Service Tag.

* 7. In the Source Service Tag field, select Internet.

* 8. Leave the Source port ranges and Destination field as the default values (* and All).

* 9. In the Destination port ranges field, enter 7777.

* 10. Change the Protocol to TCP.

* 11. Leave the Action option as Allow.

* 12. Change the Priority to 100.

* 13. Change the Name from the default Port_8080 to something more descriptive such as Allow_TCP_7777_from_Internet. The name cannot contain spaces.

* 14. Click the Add button to save the new rule.

NEW QUESTION 100

- (Exam Topic 4)

You have a web app hosted on an on-premises server that is accessed by using a URL of <https://www.contoso.com>. You plan to migrate the web app to Azure.

You will continue to use <https://www.contoso.com>. You need to enable HTTPS for the Azure web app. What should you do first?

- A. Export the public key from the on-premises server and save the key as a P7b file.
- B. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using TripleDES.
- C. Export the public key from the on-premises server and save the key as a CER file.
- D. Export the private key from the on-premises server and save the key as a PFX file that is encrypted by using AES256.

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/app-service/configure-ssl-certificate#private-certificate-requirements>

NEW QUESTION 101

- (Exam Topic 4)

You have two Azure virtual machines in the East US2 region as shown in the following table.

Name	Operating system	Type	Tier
VM1	Windows Server 2008 R2	A3	Basic
VM2	Ubuntu 16.04-DAILY-LTS	L4s	Standard

You deploy and configure an Azure Key vault.

You need to ensure that you can enable Azure Disk Encryption on VM1 and VM2.

What should you modify on each virtual machine? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

VM1: ▼

The operating system version

The tier

The type

VM2: ▼

The operating system version

The tier

The type

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

VM1: The Tier

The Tier needs to be upgraded to standard.

Disk Encryption for Windows and Linux IaaS VMs is in General Availability in all Azure public regions and Azure Government regions for Standard VMs and VMs with Azure Premium Storage.

VM2: the operating system

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/generation-2#generation-1-vs-generation-2-ca>

NEW QUESTION 103

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1 and an Azure Container Registry named ConReg1.

You enable content trust for ContReg1.

You need to ensure that User1 can create trusted images in ContReg1. The solution must use the principle of least privilege.

Which two roles should you assign to User1? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. AcrQuarantineReader
- B. Contributor
- C. AcrPush
- D. AcrImageSigner
- E. AcrQuarantineWriter

Answer: CD

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/container-registry/container-registry-content-trust> <https://docs.microsoft.com/en-us/azure/container-registry/container-registry-roles>

NEW QUESTION 108

- (Exam Topic 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 use Azure Security Center for the centralized policy management of three Azure subscriptions. You use several policy definitions to manage the security of the subscriptions.

You need to deploy the policy definitions as a group to all three subscriptions.

Solution: You create a policy initiative and assignments that are scoped to resource groups. Does this meet the goal?

- A. Yes
- B. No

Answer: B

NEW QUESTION 112

- (Exam Topic 4)

You have an Azure subscription that contains a user named Admin1 and a virtual machine named VM1. VM1 runs Windows Server 2019 and was deployed by using an Azure Resource Manager template. VM1 is the member of a backend pool of a public Azure Basic Load Balancer.

Admin1 reports that VM1 is listed as Unsupported on the Just in time VM access blade of Azure Security Center.

You need to ensure that Admin1 can enable just in time (JIT) VM access for VM1. What should you do?

- A. Create and configure an additional public IP address for VM 1.
- B. Replace the Basic Load Balancer with an Azure Standard Load Balancer.
- C. Assign an Azure Active Directory Premium Plan 1 license to Admin1.
- D. Create and configure a network security group (NSG).

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-just-in-time?tabs=jit-config-asc%2Cjit-re>

NEW QUESTION 115

- (Exam Topic 4)

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

Name	Type	Resource group
RG1	Resource group	Not applicable
RG2	Resource group	Not applicable
RG3	Resource group	Not applicable
SQL1	Azure SQL Database	RG3

Transparent Data Encryption (TDE) is disabled on SQL1.

You assign policies to the resource groups as shown in the following table.

Name	Condition	Effect if condition is false	Assignment
Policy1	TDE enabled	Deny	RG1, RG2
Policy2	TDE enabled	DeployIfNotExists	RG2, RG3
Policy3	TDE enabled	Audit	RG1

You plan to deploy Azure SQL databases by using an Azure Resource Manager (ARM) template. The databases will be configured as shown in the following table.

Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
SQL1 will have TDE enabled automatically.	<input type="radio"/>	<input type="radio"/>
The deployment of SQL2 will fail.	<input type="radio"/>	<input type="radio"/>
SQL3 will be deployed and marked as noncompliant.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/effects>

NEW QUESTION 120

- (Exam Topic 4)

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant. From the Azure portal, you register an enterprise application.

Which additional resource will be created in Azure AD?

- A. a service principal
- B. an X.509 certificate
- C. a managed identity
- D. a user account

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added>

NEW QUESTION 125

- (Exam Topic 4)

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

Name	Type
storage1	Storage account
Vault1	Azure Key vault
Vault2	Azure Key vault

You plan to deploy the virtual machines shown in the following table.

Name	Role
VM1	<ul style="list-style-type: none">Storage Blob Data Reader for storage1Key Vault Reader for Vault1
VM2	<ul style="list-style-type: none">Storage Blob Data Reader for storage1Key Vault Reader for Vault1
VM3	<ul style="list-style-type: none">Storage Blob Data Reader for storage1Key Vault Reader for Vault1Key Vault Reader for Vault2
VM4	<ul style="list-style-type: none">Storage Blob Data Reader for storage1Key Vault Reader for Vault1Key Vault Reader for Vault2

You need to assign managed identities to the virtual machines. The solution must meet the following requirements:

- Assign each virtual machine the required roles.
- Use the principle of least privilege.

What is the minimum number of managed identities required?

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

Answer: B

Explanation:

We have two different sets of required permissions. VM1 and VM2 have the same permission requirements. VM3 and VM4 have the same permission requirements.

A user-assigned managed identity can be assigned to one or many resources. By using user-assigned managed identities, we can create just two managed identities: one with the permission requirements for VM1 and VM2 and the other with the permission requirements for VM3 and VM4.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

NEW QUESTION 129

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.com

You need to configure diagnostic settings for contoso.com. The solution must meet the following requirements:

- Retain logs for two years.
- Query logs by using the Kusto query language
- Minimize administrative effort. Where should you store the logs?

- A. an Azure Log Analytics workspace
- B. an Azure event hub
- C. an Azure Storage account

Answer: A

Explanation:
<https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/get-started-queries>

NEW QUESTION 130

- (Exam Topic 4)
You have an Azure subscription that contains an Azure Sentinel workspace.
Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.
You need to identify which Azure Sentinel components to configure to meet the following requirements:

- When Azure Sentinel identifies a threat, an incident must be created.
- A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.

Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

When Azure Sentinel identifies a threat, an incident must be created:

Analytics

Data connectors

Playbooks

Workbooks

A ticket must be logged in the service management platform when an incident is created in Azure Sentinel:

Analytics

Data connectors

Playbooks

Workbooks

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Reference:
<https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts> <https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook>

NEW QUESTION 132

- (Exam Topic 4) You have an Azure subscription. You plan to create a storage account.
You need to use customer-managed keys to encrypt the tables in the storage account.
From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Cmdlets

New-AzStorageAccountKey

New-AzStorageTable

Register-AzProviderFeature

New-AzStorageAccount

Register-AzResourceProvider

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Text, table Description automatically generated with medium confidence
Reference:
<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=pow>

NEW QUESTION 133

- (Exam Topic 4)
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.

NSGs:

▼

1

2

3

4

Network security rules:

▼

1

2

3

4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NSGs: 1
 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 136

- (Exam Topic 4)
 From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1. You perform the following actions:

- Push a Windows image named Image1 to Registry1.
- Push a Linux image named Image2 to Registry1.
- Push a Windows image named Image3 to Registry1.
- Modify Image1 and push the new image as Image4 to Registry1.
- Modify Image2 and push the new image as Image5 to Registry1.

Which two images will be scanned for vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Image4
- B. Image2
- C. Image1
- D. Image3
- E. Image5

Answer: BC

NEW QUESTION 138

- (Exam Topic 4)
 You have an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Member of	Multi-factor authentication (MFA) status
User1	Group1, Group2	Disabled
User2	Group2	Disabled

The tenant contains the named locations shown in the following table.

Name	IP address range	Trusted location
Seattle	193.77.10.0/24	Yes
Boston	154.12.18.0/24	No

You create the conditional access policies for a cloud app named App1 as shown in the following table.

Name	Include	Exclude	Condition	Grant
Policy1	Group1	Group2	Locations: Boston	Block access
Policy2	Group1	None	Locations: Any location	Grant access, Require multi-factor authentication
Policy3	Group2	Group1	Locations: Boston	Block access
Policy4	User2	None	Locations: Any location	Grant access, Require multi-factor authentication

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can access App1 from an IP address of 154.12.18.10.	<input type="radio"/>	<input checked="" type="radio"/>
User2 can access App1 from an IP address of 193.77.10.15.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can access App1 from an IP address of 154.12.18.34.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 140

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Files share named share1 and a user named User1. Identity-based authentication is configured for share1. User1 attempts to access share1 from a Windows 10 device by using SMB. Which type of token will Azure Files use to authorize the request?

- A. OAuth 20
- B. JSON Web Token (JWT)
- C. Kerberos
- D. SAML

Answer: C

Explanation:

<https://learn.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service>

NEW QUESTION 141

- (Exam Topic 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 an Azure Subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016. You need to encrypt VM1 disks by using Azure Disk Encryption. 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.

Actions	Answer Area
Configure secrets for the Azure key vault.	
Create an Azure key vault.	
Run Set-AzureRmStorageAccount.	
Configure access policies for the Azure key vault.	
Run Set-AzureRmVmDiskEncryptionExtension.	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/encrypt-disks>

NEW QUESTION 146

- (Exam Topic 4)

You have a Azure subscription.

You enable Azure Active Directory (Azure AD) Privileged identify (PIM).

Your company's security policy for administrator accounts has the following conditions:

- * The accounts must use multi-factor authentication (MFA).
- * The account must use 20-character complex passwords.
- * The passwords must be changed every 180 days.
- * The account must be managed by using PIM.

You receive alerts about administrator who have not changed their password during the last 90 days. You need to minimize the number of generated alerts.

Which PIM alert should you modify?

- A. Roles don't require multi-factor authentication for activation.
B. Administrator aren't using their privileged roles
C. Roles are being assigned outside of Privileged identity Management
D. Potential state accounts in a privileged role.

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-how-to-configure>

NEW QUESTION 149

- (Exam Topic 4)

You have an Azure subscription that contains a storage account named storage1 and several virtual machines. The storage account and virtual machines are in the same Azure region. The network configurations of the virtual machines are shown in the following table.

Name	Public IP address	Connected to
VM1	52.232.128.194	VNET1/Subnet1
VM2	52.233.129.82	VNET2/Subnet2
VM3	52.233.130.11	VNET3/Subnet3

The virtual network subnets have service endpoints defined as shown in the following table.

Name	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET2/Subnet2	None
VNET3/Subnet3	Microsoft.KeyVault

You configure the following Firewall and virtual networks settings for storage1:

- Allow access from: Selected networks
- Virtual networks: VNET3\Subnet3
- Firewall – Address range: 52.233.129.0/24

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
VM1 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM2 can connect to storage1.	<input type="radio"/>	<input type="radio"/>
VM3 can connect to storage1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: No
VNet1 has a service endpoint configure for Azure Storage. However, the Azure storage does not allow access from VNet1 or the public IP address of VM1.
Box 2: Yes
VNet2 does not have a service endpoint configured. However, the Azure storage allows access from the public IP address of VM2.
Box 3: No
Azure storage allows access from VNet3. However, VNet3 does not have a service endpoint for Azure storage. The Azure storage also does not allow access from the public IP of VM3.

NEW QUESTION 150

- (Exam Topic 4)
You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure Service (AKS) cluster AKS1.
You discover that AKS1 cannot be accessed by using accounts from Contoso.com
You need to ensure AKS1 can be accessed by using accounts from Contoso.com The solution must minimize administrative effort.
What should you do first?

A. From Azure recreate AKS1,
B. From AKS1, upgrade the version of Kubernetes.
C. From Azure AD, implement Azure AD Premium P2.
D. From Azure AD, configure the User settings

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/aks/azure-ad-integration-cli>

NEW QUESTION 154

- (Exam Topic 4)
You have an Azure subscription that contains a user named User1. User1 is assigned the Reader role for the subscription.
You plan to create a custom role named Role1 and assign Role1 to User1.
You need to ensure that User1 can create and manage application security groups by using the Azure portal. Which two permissions should you add to Role1? To answer, select the appropriate permission in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Add permissions

Microsoft Monitoring Insights Microsoft.SecurityGraph	Microsoft Monitoring Insights Enable your workforce to be productive on all their devices, while keeping your organization's information protected.	Microsoft Monitoring Insights Microsoft.DynamicsTelemetry	Microsoft Network Connect cloud and on-premises infrastructure and services to provide your customers and users the best.
Microsoft Operations Management A simplified management solution for any enterprise	Microsoft Policy Insights Summarize policy states for the subscription level policy definition.	Microsoft Portal Build, manage, and monitor all Azure products in a single, unified console.	Microsoft Power BI Dedicated Manage Power BI Premium dedicated capacities for exclusive use by an organization.
Microsoft Power Platform Microsoft.PowerPlatform	Microsoft Project Babylon Microsoft.ProjectBabylon	Microsoft Purview Microsoft.Purview	Microsoft Resource Graph Powerful tool to query, explore, and analyze your cloud resources at scale.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

* 1. Microsoft Portal 2. Microsoft Network
<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-services-resource-providers>

NEW QUESTION 155

- (Exam Topic 4)
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:
<https://docs.microsoft.com/en-us/azure/devops/repos/git/branch-policies?view=azuredevops&viewFallbackFrom=vsts>

NEW QUESTION 160

- (Exam Topic 4)
You have an Azure subscription named Subscription1 that contains a resource group named RG1 and a user named User1. User1 is assigned the Owner role for RG1.
You create an Azure Blueprints definition named Blueprint1 that includes a resource group named RG2 as shown in the following exhibit.

Edit blueprint

BasicsArtifacts

Add artifacts to the blueprint. Add resource groups to organize where the artifacts should be deployed and assigned.

NAME	ARTIFACT TYPE	PARAMETERS
▼ Subscription		
+ Add artifact...		
▼ RG2	Resource group	2 out of 2 parameters populated
User1 (User1@sk200628outlook.onmicrosoft.com) : Tag Contributor	Role assignment	1 out of 1 parameters populated
+ Add artifact...		

You assign Blueprint1 to Subscription1 by using the following settings: > Lock assignment: Read Only
> Managed Identity: System assigned
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Statements	Yes	No
A locking mode of Read Only will be assigned to RG1.	<input type="radio"/>	<input type="radio"/>
User1 can add tags to RG2.	<input type="radio"/>	<input type="radio"/>
You can remove User1 from the Tag Contributor role for RG2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Graphical user interface, text, application Description automatically generated
Reference:
<https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking>

NEW QUESTION 164

- (Exam Topic 4)
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 DSCService 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 167

- (Exam Topic 4)

You have an Azure key vault named Vault1 that stores the resources shown in following table.

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

- A. Key1 Only
- B. Cert1 only
- C. Key1 and Secret1 only
- D. Key1 and Cert1 only
- E. Secret1 and Cert1 only
- F. Key1, Secret1, and Cert1

Answer: C

NEW QUESTION 169

- (Exam Topic 4)

You have the Azure virtual machines shown in the following table.

Name	Location	Connected to
VM1	West US 2	VNET1/Subnet1
VM2	West US 2	VNET1/Subnet1
VM3	West US 2	VNET1/Subnet2
VM4	East US	VNET2/Subnet3
VM5	West US 2	VNET5/Subnet5

Each virtual machine has a single network interface.

You add the network interface of VM1 to an application security group named ASG1.

You need to identify the network interfaces of which virtual machines you can add to ASG1. What should you identify?

- A. VM2 only
- B. VM2, VM3, VM4, and VM5
- C. VM2, VM3, and VM5 only
- D. Vm2 and Vm3 only

Answer: D

Explanation:

Reference:

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

NEW QUESTION 174

- (Exam Topic 4)

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

Name	Type	Description
RG1	Resource group	Used to store virtual machines
RG2	Resource group	Used to store virtual networks
ServerAdmins	Security group	Used to manage virtual machines

You need to ensure that ServerAdmins can perform the following tasks: Create virtual machine to the existing virtual network in RG2 only.

The solution must use the principle of least privilege.

Which two role-based access control (RBAC) roles should you assign to ServerAdmins? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Contributor role for the subscription
- B. the Network Contributor role for RG2
- C. A custom RBAC role for the subscription
- D. a custom RBAC role for RG2
- E. the Network Contributor role for RG1.
- F. the Virtual Machine Contributor role for RG1.

Answer: DF

NEW QUESTION 176

- (Exam Topic 4)

You have an Azure subscription named Sub1.

In Azure Security Center, you have a workflow automation named WF1. WF1 is configured to send an email message to a user named User1.

You need to modify WF1 to send email messages to a distribution group named Alerts. What should you use to modify WF1?

- A. Azure Application Insights
- B. Azure Monitor
- C. Azure Logic Apps Designer
- D. Azure DevOps

Answer: C

Explanation:

Reference:

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

<https://docs.microsoft.com/en-us/learn/modules/resolve-threats-with-azure-security-center/6-exerciseconfigure-p>

NEW QUESTION 181

- (Exam Topic 4)

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 has discovery enabled and contains several inventory assets.

You need to identify which inventory assets are vulnerable to the most critical web app security risks. Which Defender EASM dashboard should you use?

- A. Attack Surface Summary
- B. GDPRCompliance
- C. Security Posture
- D. OWASPTopIO

Answer: D

NEW QUESTION 186

- (Exam Topic 4)

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

Name	Subscription role	Azure AD user role
User1	Owner	None
User2	Contributor	None
User3	Security Admin	None
User4	None	Service administrator

You create a resource group named RG1.

Which users can modify the permissions for RG1 and which users can create virtual networks in RG1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Users who can modify the permissions for RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

Users who can create virtual networks in RG1:

User1 only

User1 and User2 only

User1 and User3 only

User1, User2 and User3 only

User1, User2, User3, and User4

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Box 1: Only an owner can change permissions on resources.

Box 2: A Contributor can create/modify/delete anything in the subscription but cannot change permissions.

NEW QUESTION 188

- (Exam Topic 4)

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.
- 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 191

- (Exam Topic 4)

You are configuring and securing a network environment.

You deploy an Azure virtual machine named VM1 that is configured to analyze network traffic. You need to ensure that all network traffic is routed through VM1. What should you configure?

- A. a system route
- B. a network security group (NSG)
- C. a user-defined route

Answer: C

Explanation:

Although the use of system routes facilitates traffic automatically for your deployment, there are cases in which you want to control the routing of packets through a virtual appliance. You can do so by creating user defined routes that specify the next hop for packets flowing to a specific subnet to go to your virtual appliance instead, and enabling IP forwarding for the VM running as the virtual appliance.

Note: User Defined Routes

For most environments you will only need the system routes already defined by Azure. However, you may need to create a route table and add one or more routes in specific cases, such as:

- Force tunneling to the Internet via your on-premises network.
- Use of virtual appliances in your Azure environment.
- In the scenarios above, you will have to create a route table and add user defined routes to it.

Reference:

<https://github.com/uglide/azure-content/blob/master/articles/virtual-network/virtual-networks-udr-overview.md>

NEW QUESTION 193

- (Exam Topic 4)

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 197

- (Exam Topic 4)

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The company develops an application named App1. App1 is registered in Azure AD. You need to ensure that App1 can access secrets in Azure Key Vault on behalf of the application users. What should you configure?

- A. an application permission without admin consent
- B. a delegated permission without admin consent
- C. a delegated permission that requires admin consent
- D. an application permission that requires admin consent

Answer: B

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.

NEW QUESTION 202

- (Exam Topic 4)

You have an Azure subscription named Subscription1 that contains the resources shown in the following table.

Name	Type	Description
EventHub1	Azure Event Hubs	Not applicable
Adf1	Azure Data Factory	Not applicable
NVA1	Network virtual appliance (NVA)	The NVA sends security event messages in the Common Event Format (CEF).

You have an Azure subscription named Subscription2 that contains the following resources:

- An Azure Sentinel workspace
- An Azure Event Grid instance

You need to ingest the CEF messages from the NVAs to Azure Sentinel. NOTE: Each correct selection is worth one point.

Answer Area

Subscription1: ☐ An Azure Log Analytics agent on a Linux virtual machine
☐ A Data Factory pipeline
☐ An Event Hubs namespace
☐ An Azure Service Bus queue

Subscription2: ☐ A new Azure Log Analytics workspace
☐ A new Azure Sentinel data connector
☐ A new Azure Sentinel playbook
☐ A new Event Grid resource provider

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Subscription1: ☐ An Azure Log Analytics agent on a Linux virtual machine
☐ A Data Factory pipeline
☒ An Event Hubs namespace
☐ An Azure Service Bus queue

Subscription2: ☒ A new Azure Log Analytics workspace
☐ A new Azure Sentinel data connector
☐ A new Azure Sentinel playbook
☐ A new Event Grid resource provider

NEW QUESTION 205

- (Exam Topic 4)

You have an Azure Storage account named storage1 that has a container named container1. You need to prevent the blobs in container1 from being modified. What should you do?

- A. From container1, change the access level.
- B. From container1 add an access policy.
- C. From container1, modify the Access Control (IAM) settings.
- D. From storage1, enable soft delete for blobs.

Answer: B

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-immutable-storage?tabs=azure-portal>

NEW QUESTION 209

- (Exam Topic 4)

You have a Azure subscription that contains an Azure Container Registry named Registry1. The subscription uses the Standard use tier of Azure Security Center.

You upload several container images to Register1.
You discover that vulnerability security scans were not performed
You need to ensure that the images are scanned for vulnerabilities when they are uploaded to Registry1. What should you do?

- A. From the Azure portal modify the Pricing tier settings.
- B. From Azure CLI, lock the container images.
- C. Upload the container images by using AzCopy
- D. Push the container images to Registry1 by using Docker

Answer: A

Explanation:

Reference:
<https://charbelnemnom.com/scan-container-images-in-azure-container-registry-with-azure-security-center/>

NEW QUESTION 212

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud.
You have an Amazon Web Service (AWS) account named AWS1 that is connected to defender for Cloud.
You need to ensure that AWS foundational Security Best Practices. The solution must minimize administrative effort.
What should you do in Defender for Cloud?

- A. Create a new customer assessment.
- B. Assign a built-in assessment.
- C. Assign a built-in compliance standard.
- D. Create a new custom standard.

Answer: C

NEW QUESTION 216

- (Exam Topic 4)

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

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

Contoso.com contains a group naming policy. The policy has a custom blocked word list rule that includes the word Contoso.
Which users can create a group named Contoso Sales in contoso.com? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Users who can create a security group named Contoso Sales:

<input type="checkbox"/> Admin1 only
<input type="checkbox"/> Admin1 and Admin2 only
<input type="checkbox"/> Admin1 and Admin3 only
<input type="checkbox"/> Admin1, Admin2, and Admin3

Users who can create an Office 365 group named Contoso Sales:

<input type="checkbox"/> Admin1 only
<input type="checkbox"/> Admin1 and Admin2 only
<input type="checkbox"/> Admin1 and Admin3 only
<input type="checkbox"/> Admin1, Admin2, and Admin3

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-naming-policy>

NEW QUESTION 218

- (Exam Topic 4)

From Azure Security, you create a custom alert rule.
You need to configure which users will receive an email message when the alert is triggered. What should you do?

- A. From Azure Monitor, create an action group.
- B. From Security Center, modify the Security policy settings of the Azure subscription.
- C. From Azure Active Directory (Azure AD). modify the members of the Security Reader role group.
- D. From Security Center, modify the alert rule.

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups>

NEW QUESTION 219

- (Exam Topic 4)

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

Name	Operating system
Computer1	Windows 10
Computer2	Windows Server 2022
Computer3	SUSE Linux Enterprise Server (SLES)

You need to enable file integrity monitoring in Microsoft Defender for Cloud. Which computers will support file integrity monitoring?

- A. Computer1 only
- B. Computer 1 and Computer2 only
- C. Computer1 and Computer2 only
- D. Computer1, Computer2, and Computer3

Answer: B

NEW QUESTION 222

- (Exam Topic 4)

You have an Azure key vault named KeyVault1 that contains the items shown in the following table.

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In KeyVault1 the following events occur in sequence:

- Item1 is deleted.
- Item2 and Policy1 are deleted.

For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
You can recover Policy1.	<input type="radio"/>	<input type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input type="radio"/>
You can add a new secret named Item2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
You can recover Policy1.	<input type="radio"/>	<input checked="" type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input checked="" type="radio"/>
You can add a new secret named Item2.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 226

- (Exam Topic 4)

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2. You need to implement VPN gateways for the virtual networks

- * VNET1 must have six site-to-site connections that use BGP.
- * VNET2 must have 12 site-to-site connections that use BGP.
- * Costs must be minimized.

NOTE: Each correct selection is worth one point

A. Mastered
B. Not Mastered

Explanation:

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways#gwsku>

- (Exam Topic 4)

You have the hierarchy of Azure resources shown in the following exhibit.



To which objects can you assign Blueprint1 and Blueprint2? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Blueprint1:

ManagementGroup1 only
ManagementGroup1, Subscription1, and RG1 only
ManagementGroup1, Subscription1, RG1, and VM1
Subscription1 only
Tenant Root Group only
Tenant Root Group, ManagementGroup1, and Subscription1 only

Blueprint2:

ManagementGroup1 only
Subscription1 and RG1 only
Subscription1 only
Subscription1, RG1, and VM1

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Blueprints can only be assigned to subscriptions.

NEW QUESTION 235

- (Exam Topic 4)

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

Name	Subscription role	Azure Active Directory (Azure AD) user role	Multi-factor authentication (MFA) status
User1	Owner	Authentication administrator	Enabled
User2	<i>None</i>	Global administrator	Enforced
User3	<i>None</i>	Global administrator	Disabled

Which users can enable Azure AD Privileged Identity Management (PIM)?

- A. User2 and User3 only
- B. User1 and User2 only
- C. User2 only
- D. User1 only

Answer: B

Explanation:

Reference:

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

NEW QUESTION 236

- (Exam Topic 4)

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

Name	Type
VM1	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Key vault

You plan to enable Azure Defender for the subscription. Which resources can be protected by using Azure Defender?

- A. VM1, VNET1, storage1, and Vault1
- B. VM1, VNET1, and storage1 only
- C. VM1, storage1, and Vault1 only
- D. VM1 and VNET1 only
- E. VM1 and storage1 only

Answer: A

Explanation:

Reference:

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

NEW QUESTION 237

- (Exam Topic 4)

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:

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.

NEW QUESTION 241

- (Exam Topic 4)

On Monday, you configure an email notification in Azure Security Center to notify user user1@contoso.com. On Tuesday, Security Center generates the security alerts shown in the following table.

Time	Description	Severity
01:00	Failed RDP brute force attack	Medium
01:01	Successful RDP brute force attack	High
06:10	Suspicious process executed	High
09:00	Malicious SQL activity	High
11:15	Network communication with a malicious machine detected	Low
13:30	Suspicious process executed	High
14:00	Failed RDP brute force attack	Medium
16:01	Successful RDP brute force attack	High
23:20	Possible outgoing spam activity detected	Low
23:25	Modified system binary discovered in dump file	High
23:30	Malicious SQL activity	High

How many email notifications will user1@contoso.com receive on Tuesday? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Total number of Security Center email notifications about an RDP

brute force attack on Tuesday:

▼

☐ 1
 ☐ 2
 ☐ 3
 ☐ 4

Total number of Security Center email notifications on Tuesday:

▼

☐ 3
 ☐ 4
 ☐ 6
 ☐ 9
 ☐ 11

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>

NEW QUESTION 245

- (Exam Topic 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 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 regenerate the Azure storage account access keys. Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Generating new storage account keys will invalidate all SAS's that were based on the previous keys.

NEW QUESTION 246

- (Exam Topic 4)

You have a Microsoft Sentinel deployment.

You need to connect a third-party security solution to the deployment. The third-party solution will send Common Event Format (CEF-formatted messages.

What should you include in the solution? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Deploy:

Forward events to Microsoft Sentinel by using:

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Deploy:

Forward events to Microsoft Sentinel by using:

NEW QUESTION 248

- (Exam Topic 4)

You have an Azure subscription that contains several Azure SQL databases and an Azure Sentinel workspace.

You need to create a saved query in the workspace to find events reported by Advanced Threat Protection for Azure SQL Database.

What should you do?

A. From Azure CLI run the Get-AzOperationalInsightsworkspace cmdlet.

B. From the Azure SQL Database query editor, create a Transact-SQL query.

C. From the Azure Sentinel workspace, create a Kusto Query Language query.

D. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.

Answer: C

NEW QUESTION 252

- (Exam Topic 4)

You have an Azure subscription that contains a resource group named RG1 and the network security groups (NSGs) shown in the following table.

Name	Location	Flow logs status
NSG1	West Europe	Off
NSG2	West Europe	Off

You create the Azure policy shown in the following exhibit.

Basics	Parameters	Remediation	Non-compliance messages	Review + create
Basics				
Scope			Azure Pass - Sponsorship/RG1	
Exclusions			Azure Pass - Sponsorship/RG1/NSG1	
Policy definition			Flow logs should be enabled for every network security group	
Assignment name			Flow logs should be enabled for every network security group	
Description			Description1	
Policy enforcement			Enabled	
Assigned by			Admin1	
Parameters				
effect			Audit	
Remediation				
Create managed identity			Yes	
Managed identity location			westeurope	
Create a remediation task			No	
Non-compliance messages				
Default non-compliance message			Message1	

You assign the policy to RG1.
What will occur if you assign the policy to NSG1 and NSG2?

- A. Flow logs will be enabled for NSG1 and NSG2.
- B. Flow logs will be enabled for NSG2 only.
- C. Flow logs will be disabled for NSG1 and NSG2.
- D. Flow logs will be enabled for NSG1 only.

Answer: B

NEW QUESTION 256

- (Exam Topic 4)

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 has an Active Directory forest with a single domain, named weylandindustries.com. They also have an Azure Active Directory (Azure AD) tenant with the same name.

You have been tasked with integrating Active Directory and the Azure AD tenant. You intend to deploy Azure AD Connect.

Your strategy for the integration must make sure that password policies and user logon limitations affect user accounts that are synced to the Azure AD tenant, and that the amount of necessary servers are reduced.

Solution: You recommend the use of federation with Active Directory Federation Services (AD FS). Does the solution meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

A federated authentication system relies on an external trusted system to authenticate users. Some companies want to reuse their existing federated system investment with their Azure AD hybrid identity solution. The maintenance and management of the federated system falls outside the control of Azure AD. It's up to the organization by using the federated system to make sure it's deployed securely and can handle the authentication load.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

NEW QUESTION 260

- (Exam Topic 4)

HOTSPOT

Your company has an Azure subscription named Subscription1 that contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Billing administrator
User3	Owner
User4	Account Admin

The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User:

▼

User1

User2

User3

User4

Tool:

▼

Azure Account Center

Azure Cloud Shell

Azure PowerShell

Azure Security Center

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1; User2

Billing Administrator

Select Transfer billing ownership for the subscription that you want to transfer.

Enter the email address of a user who's a billing administrator of the account that will be the new owner for the subscription.

Box 2: Azure Account Center Azure Account Center can be used. Reference:

<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transfer-billing-ownership-of-an-azu>

NEW QUESTION 265

- (Exam Topic 4)

You have an Azure web app named webapp1.

You need to configure continuous deployment for webapp1 by using an Azure Repo.

What should you create first?

- A. an Azure Application Insights service
- B. an Azure DevOps organization
- C. an Azure Storage account
- D. an Azure DevTest Labs lab

Answer: B

NEW QUESTION 268

- (Exam Topic 4)

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: C

Explanation:

"You may need to configure the target resource to allow access from your application. For example, if you request a token to Key Vault, you need to make sure you have added an access policy that includes your application's identity. Otherwise, your calls to Key Vault will be rejected, even if they include the token"

<https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity?tabs=dotnet>

NEW QUESTION 273

- (Exam Topic 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	<i>Not applicable</i>
storage2	East US	Premium	Block blobs
storage3	East US	Premium	File shares
storage4	East US 2	Standard	<i>Not applicable</i>

You plan to enable auditing for DB1.

Which storage accounts can you use as the auditing destination for DB1?

- A. storage1 only
- B. storage1 and storage4 only
- C. Storage2 and storage3 only
- D. storage1, storage2 and storage3 only

Answer: C

NEW QUESTION 277

- (Exam Topic 4)

You are troubleshooting a security issue for an Azure Storage account. You enable the diagnostic logs for the storage account.

What should you use to retrieve the diagnostics logs?

- A. Azure Storage Explorer
- B. SQL query editor in Azure
- C. File Explorer in Windows
- D. Azure Security Center

Answer: A

Explanation:

If you want to download the metrics for long-term storage or to analyze them locally, you must use a tool or write some code to read the tables. You must download the minute metrics for analysis. The tables do not appear if you list all the tables in your storage account, but you can access them directly by name. Many storage-browsing tools are aware of these tables and enable you to view them directly (see Azure Storage Client Tools for a list of available tools). Microsoft provides several graphical user interface (GUI) tools for working with the data in your Azure Storage account. All of the tools outlined in the following table are free.

Azure Storage client tool	Supported platforms	Block Blob	Page Blob	Append Blob	Tables	Queues	Files
Azure portal	Web	Yes	Yes	Yes	Yes	Yes	Yes
Azure Storage Explorer	Windows, OSX	Yes	Yes	Yes	Yes	Yes	Yes
Microsoft Visual Studio Cloud Explorer	Windows	Yes	Yes	Yes	Yes	Yes	No

References:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-metrics?toc=%2fazure%2fstorage%2f> <https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers>

NEW QUESTION 280

- (Exam Topic 4)

Your company recently created an Azure subscription.

You have been tasked with making sure that a specified user is able to implement Azure AD Privileged Identity Management (PIM).

Which of the following is the role you should assign to the user?

- A. The Global administrator role.
- B. The Security administrator role.
- C. The Password administrator role.
- D. The Compliance administrator role.

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

Reference:

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

NEW QUESTION 281

- (Exam Topic 4)

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

Answer: D**Explanation:**

Just as a blueprint allows an engineer or an architect to sketch a project's design parameters, Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of

Azure resources that implements and adheres to an organization's standards, patterns, and requirements.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts such as:

- Role Assignments
- Policy Assignments
- Azure Resource Manager templates
- Resource Groups

Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>**NEW QUESTION 283**

- (Exam Topic 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 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 lock on Sa1. Does this meet the goal?

- A. Yes
- B. No

Answer: B**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 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 288**

- (Exam Topic 4)

















You have the Azure virtual networks shown in the following table.

Name	Location	Subnet	Peered network
VNET1	East US	Subnet1	VNET2
VNET2	West US	Subnet2, Subnet3	VNET1
VNET4	East US	Subnet4	None




You have the Azure virtual machines shown in the following table.

Name	Application security group	Network security group (NSG)	Connected to	Public IP address
VM1	ASG1	NSG1	Subnet1	No
VM2	ASG2	NSG1	Subnet2	No
VM3	ASG2	NSG1	Subnet3	Yes
VM4	ASG4	NSG1	Subnet4	Yes

The firewalls on all the virtual machines allow ping traffic. NSG1 is configured as shown in the following exhibit. Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
110	 Allow_RDP	3389	Any	Any	Any	 Allow ...
130	 Rule1	Any	Any	 ASG1	Any	 Allow ...
140	 Rule2	Any	Any	 ASG2	Any	 Allow ...
150	 Rule3	Any	Any	 ASG4	Any	 Allow ...
160	 Rule4	Any	Any	Any	Any	 Deny ...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow ...
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	 Allow ...
65500	DenyAllInBound	Any	Any	Any	Any	 Deny ...

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	 Allow ...
65001	AllowInternetOutBou...	Any	Any	Any	Internet	 Allow ...
65500	DenyAllOutBound	Any	Any	Any	Any	 Deny ...

For each of the following statements, select Yes if the statement is true. Otherwise, select No.

NOTE: Each correct selection is worth one point.

Statements	Yes	No
VM1 can ping VM3 successfully.	<input type="radio"/>	<input type="radio"/>
VM2 can ping VM4 successfully.	<input type="radio"/>	<input type="radio"/>
VM3 can be accessed by using Remote Desktop from the internet.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
 B. Not Mastered

Answer: A

Explanation:

Box 1: Yes

VM1 and VM3 are on peered VNets. The firewall rules with a source of ASG1 and ASG2 allow 'any' traffic on 'any' protocol so pings are allowed between VM1 and VM3.

Box 2: No

VM2 and VM4 are on separate VNets and the VNets are not peered. Therefore, the pings would have to go over the Internet. VM4 does have a public IP and the firewall allows pings. However, for VM2 to be able to ping VM4, VM2 would also need a public IP address. In Azure, pings don't go out through the default gateway as they would in a physical network. For an Azure VM to ping external IPs, the VM must have a public IP address assigned to it.

Box 3: Yes

VM3 has a public IP address and the firewall allows traffic on port 3389.

NEW QUESTION 289

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud.

You need to use Defender for Cloud to review regulatory compliance with the Azure CIS 1.4,0 standard. The solution must minimize administrative effort.

What should you do first?

- A. Assign an Azure policy.
 B. Manually add the Azure CIS 1.4.0 standard.
 C. Disable one of the Out of the box standards.
 D. Add a custom initiative.

Answer: A

NEW QUESTION 290

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Blob storage account bolb1. You need to configure attribute-based access control (ABAC) for blob1.

Which attributes can you use in access conditions?

- A. blob index tags only
- B. blob index tags and container names only
- C. file extensions and container names only
- D. blob index tags, file extensions, and container names

Answer: A

NEW QUESTION 295

- (Exam Topic 4)

You have an Azure subscription that contains the resources show in the following table.

Name	Type
DB1	Azure Cosmos DB account
VM1	Virtual machine
VM2	Virtual machine
VNET1	Virtual network
NSG1	Network security group (NSG)

Both VM1 and VM2 connect to VNET1 and are configured to use NSG1. You need to ensure that only VM1 and VM2 can access DB1. What should you do?

- A. Add the IP address range of VNET1 to the Firewall setting of DB1.
- B. For NSG1, configure a rule that has a service tag.
- C. Create an application security group.
- D. Configure DB1 to allow access from only VNET1.

Answer: B

NEW QUESTION 299

- (Exam Topic 4)

You have an Azure subscription that contains a user named Admin1 and a resource group named RG1. In Azure Monitor, you create the alert rules shown in the following table.

Name	Resource	Condition
Rule1	RG1	All security operations
Rule2	RG1	All administrative operations
Rule3	Azure subscription	All security operations by Admin1
Rule4	Azure subscription	All administrative operations by Admin1

Admin1 performs the following actions on RG1:

- > Adds a virtual network named VNET1
- > Adds a Delete lock named Lock1

Which rules will trigger an alert as a result of the actions of Admin1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Adding VNET1:

Rule2 only
Rule4 only
Rule2 and Rule 4 only
Rule3 and Rule 4 only
Rule1, Rule2, Rule3 and Rule 4

Adding Lock1:

Rule2 only
Rule4 only
Rule2 and Rule 4 only
Rule3 and Rule 4 only
Rule1, Rule2, Rule3 and Rule 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Adding VNET1:

Adding Lock1:

NEW QUESTION 301

- (Exam Topic 4)

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.

Answer Area

ASG1:

ASG2:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

ASG1:

ASG2:

NEW QUESTION 304

- (Exam Topic 4)

You have an on-premises network and an Azure subscription.

You have the Microsoft SQL Server instances shown in the following table.

Name	Type
sql1	Azure SQL managed instance
sql2	SQL Server 2019 on an Azure virtual machine that runs Windows Server 2019
sql3	SQL Server 2019 on an Azure virtual machine that runs Red Hat Enterprise Linux (RHEL) 8.3
sql4	On-premises physical server that runs Windows Server 2016 and has SQL Server 2016 installed

You plan to implement Microsoft Defender for SQL.

Which SQL Server instances will be protected by Microsoft Defender for SQL?

- A. sql1 and sql2 only
- B. sql1, sql2, and sql3 only
- C. sql1 sql2 and so.14 only
- D. sql1, sql2, sql3, and sql4

Answer: D

NEW QUESTION 306

- (Exam Topic 4)

You have an Azure subscription that contains the Azure Active Directory (Azure AD) resources shown in the following table.

Name	Description
User1	User
Group1	Security group that has a Membership type of Dynamic Device
Managed1	Managed identity
App1	Enterprise application

You create the groups shown in the following table.

Name	Description
Group5	Security group that has a Membership type of Assigned
Group6	Microsoft 365 group that has a Membership type of Assigned

Which resources can you add to Group5 and Group6? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Group5: ▼

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

Group6: ▼

- User1 only
- User1 and Group1 only
- User1, Group1, and Managed1 only
- User1, Group1, Managed1, and App1

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

NEW QUESTION 311

- (Exam Topic 4)

You have an Azure subscription that contains an Azure SQL database named SQL1. You plan to deploy a web app named App1.

You need to provide App1 with read and write access to SQL1. The solution must meet the following requirements:

- Provide App1 with access to SQL1 without storing a password.
- Use the principle of least privilege.
- Minimize administrative effort.

Which type of account should App1 use to access SQL1, and which database roles should you assign to App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Account type: ▼

- Azure Active Directory User
- Managed identity
- Service Principal

Roles: ▼

- db_datawriter only
- db_datareader and db_datawriter
- db owner only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/tutorial-connect-msi-sql-database?tabs=windowsclient%2Cd>

NEW QUESTION 313

- (Exam Topic 4)

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1. You have 500 Azure virtual machines that run Windows Server 2016 and are enrolled in LAW1.

You plan to add the System Update Assessment solution to LAW1.

You need to ensure that System Update Assessment-related logs are uploaded to LAW1 from 100 of the virtual machines only.

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.

Actions	Answer Area
Create a new workspace.	
Apply the scope configuration to the solution.	
Create a scope configuration.	
Create a computer group.	
Create a data source.	

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

<https://docs.microsoft.com/en-us/azure/azure-monitor/insights/solution-targeting>

NEW QUESTION 314

- (Exam Topic 4)

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.

User1:	<div><div></div><div>A key vault access policy Azure Information Protection Azure Policy Managed identities for Azure resources RBAC</div></div>
User2:	<div><div></div><div>A key vault access policy Azure Information Protection Azure Policy Managed identities for Azure resources RBAC</div></div>

- 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 315

- (Exam Topic 3)

You need to meet the technical requirements for the finance department users. Which CAPolicy1 settings should you modify?

- A. Cloud apps or actions
- B. Conditions
- C. Grant
- D. Session

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-session-life>

NEW QUESTION 320

- (Exam Topic 3)

You implement the planned changes for ASG1 and ASG2.

In which NSGs can you use ASG1. and the network interfaces of which virtual machines can you assign to ASG2?

Answer Area

NSGs:	<div>NSG2 only</div> <div>NSG2 and NSG4 only</div> <div>NSG2, NSG3, and NSG4</div>
Virtual machines:	<div>VM3 only</div> <div>VM2 and VM4 only</div> <div>VM1, VM2, and VM4 only</div> <div>VM2, VM3, and VM4 only</div> <div>VM1, VM2, VM3, and VM4</div>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, chat or text message Description automatically generated

NEW QUESTION 325

- (Exam Topic 3)

You need to perform the planned changes for OU2 and User1.

Which tools should you use? To answer, drag the appropriate tools to the correct resources. Each tool 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.

Tools	Answer Area
The Azure portal	OU2: Tool
Azure AD Connect	User1: Tool
The Active Directory admin center	
Active Directory Sites and Services	
Active Directory Users and Computers	

- A. Mastered
B. Not Mastered

Answer: A

Explanation:
Table Description automatically generated

NEW QUESTION 326
- (Exam Topic 3)
You need to encrypt storage1 to meet the technical requirements. Which key vaults can you use?

- A. KeyVault1 only
B. KeyVault2 and KeyVault3 only
C. KeyVault1 and KeyVault3 only
D. KeyVault1 KeyVault2 and KeyVault3

Answer: B

Explanation:
The storage account and the key vault must be in the same region and in the same Azure Active Directory (Azure AD) tenant, but they can be in different subscriptions.
Storage1 is in the West US region. KeyVault1 is the only key vault in the same region. Reference:
<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview>

NEW QUESTION 331
- (Exam Topic 2)
You are evaluating the security of VM1, VM2, and VM3 in Sub2.
For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area	Statements	Yes	No
	From the Internet, you can connect to the web server on VM1 by using HTTP.	<input type="radio"/>	<input type="radio"/>
	From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input type="radio"/>
	From the Internet, you can connect to the web server on VM3 by using HTTP.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From the Internet, you can connect to the web server on VM1 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>
From the Internet, you can connect to the web server on VM2 by using HTTP.	<input type="radio"/>	<input checked="" type="radio"/>
From the Internet, you can connect to the web server on VM3 by using HTTP.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 335

- (Exam Topic 2)

You are evaluating the security of the network communication between the virtual machines in Sub2. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
From VM1, you can successfully ping the public IP address of VM2.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the private IP address of VM3.	<input type="radio"/>	<input type="radio"/>
From VM1, you can successfully ping the public IP address of VM5.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Yes, Yes No

NEW QUESTION 339

- (Exam Topic 2)

You are evaluating the effect of the application security groups on the network communication between the virtual machines in Sub2. For each of the following statements, select Yes if the statement is true. Otherwise, select No. NOTE: Each correct selection is worth one point.

Statements	Yes	No
From VM1, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
From VM2, you can successfully ping the private IP address of VM4.	<input type="radio"/>	<input type="radio"/>
From VM1, you can connect to the web server on VM4.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: No. VM4 is in Subnet13 which has NSG3 attached to it. VM1 is in ASG1. NSG3 would only allow ICMP pings from ASG2 but not ASG1. Only TCP traffic is allowed from ASG1. 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

Box 2: Yes.
VM2 is in ASG2. Any protocol is allowed from ASG2 so ICMP ping would be allowed.
Box3. VM1 is in ASG1. TCP traffic is allowed from ASG1 so VM1 could connect to the web server as connections to the web server would be on ports TCP 80 or TCP 443.

NEW QUESTION 341

- (Exam Topic 1)
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.

Actions

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.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
From the Azure portal, create an Azure AD administrator for LitwareSQLServer1 Connect to SQLDB1 by using SSMS
In SQLDB1, create contained database users <https://www.youtube.com/watch?v=pEPyPsGEevw>

NEW QUESTION 344

- (Exam Topic 1)
You need to ensure that the Azure AD application registration and consent configurations meet the identity and access requirements.
What should you use in the Azure portal? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

To configure the registration settings:

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

To configure the consent settings:

Azure AD – User settings

Azure AD – App registrations settings

Enterprise Applications – User settings

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent>

NEW QUESTION 347

- (Exam Topic 1)

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: D

Explanation:

<https://docs.microsoft.com/en-us/azure/firewall/tutorial-firewall-dnat>

NEW QUESTION 351

- (Exam Topic 1)

You need to configure WebApp1 to meet the data and application requirements.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Upload a public certificate.
- B. Turn on the HTTPS Only protocol setting.
- C. Set the Minimum TLS Version protocol setting to 1.2.
- D. Change the pricing tier of the App Service plan.
- E. Turn on the Incoming client certificates protocol setting.

Answer: BE

Explanation:

Refer <https://docs.microsoft.com/en-us/azure/app-service/app-service-web-configure-tls-mutual-auth>

NEW QUESTION 356

.....

Relate Links

100% Pass Your az-500 Exam with Examible Prep Materials

<https://www.examible.com/az-500-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.examible.com/>