



"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks.com

Warning: Keep connected with our support team
for latest updates

Question: 1

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

What should you do?

- A. Add a membership rule to Group1.
- B. Delete Group1. Create a new group named Group1 that has a membership type of Office 365. Add users and devices to the group.
- C. Modify the membership rule of Group1.
- D. Change the membership type of Group1 to Assigned. Create two groups that have dynamic memberships. Add the new groups to Group1.

Answer:

Explanation:

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

Scenario:

Litware identifies the following identity and access requirements: All San Francisco users and their devices must be members of Group1.

The tenant currently contain this group:

Name	Type	Description
Group 1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.

Reference:

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

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-groups-create-azure-portal>

Question: 2

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>

Question: 3

You need to ensure that you can meet the security operations requirements. What should you do first?

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

Answer: C

Explanation:

The Standard tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The Standard tier also adds advanced threat detection capabilities, which uses built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more.

Scenario: Security Operations Requirements

Litware must be able to customize the operating system security configurations in Azure Security Center.

Reference:

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

Question: 4

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: B,E

Explanation:

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

Question: 5

HOTSPOT

You need to create Role1 to meet the platform protection requirements.

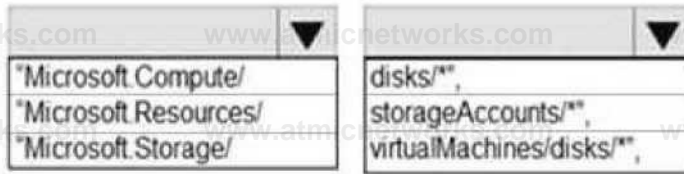
How should you complete the role definition of Role1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```

    "Name": "Role1",
    "Id": "11111111-1111-1111-1111-111111111111",
    "IsCustom" : true,
    "Description": "VM storage operator"
    "Actions" : [

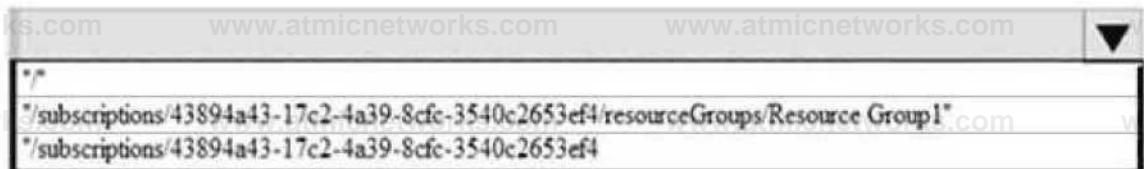
```



```

    ],
    "NotActions": [
    ],
    "AssignableScopes" : [

```



Answer:

Explanation:

- 1) Microsoft.Compute/
- 2) disks
- 3) /subscription/{subscriptionId}/resourceGroups/{Resource Group Id}

A new custom RBAC role named Role1 must be used to delegate the administration of the managed disks in Resource Group1. Role1 must be available only for Resource Group1.

Question: 6

DRAG DROP

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

Which three actions should you recommend be performed in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

From the Azure portal, create an Azure AD administrator for LitwareSQLServer1.

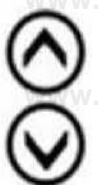
In SQLDB1, create contained database users.

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



Answer:

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=pEPyPsGEeww>

Question: 7

HOTSPOT

You need to deploy Microsoft Antimalware to meet the platform protection requirements.

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

NOTE: Each correct selection is worth one point.

Create a custom policy definition that has effect set to:

- Append
- Deny
- DeployIfNotExists

Create a policy assignment and modify:

- The Create a Managed Identify setting
- The exclusion settings
- The scope

Answer:

Explanation:

1. DeployIfNotExists
2. Scope

Question: 8

DRAG DROP

You need to deploy AKS1 to meet the platform protection requirements.

Which four 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.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions

Answer Area

Deploy an AKS cluster.

Create a client application.

Create a server application.

Create an RBAC binding.

Create a custom RBAC role.

Answer:

Explanation:

Create a server application.

Create a client application.

Deploy an AKS cluster.

Create an RBAC binding.

Scenario: Azure AD users must be to authenticate to AKS1 by using their Azure AD credentials.

Litewire plans to deploy AKS1, which is a managed AKS (Azure Kubernetes Services) cluster.

Step 1: Create a server application

To provide Azure AD authentication for an AKS cluster, two Azure AD applications are created. The first application is a server component that provides user authentication.

Step 2: Create a client application

The second application is a client component that's used when you're prompted by the CLI for authentication. This client application uses the server application for the actual authentication of the credentials provided by the client.

Step 3: Deploy an AKS cluster.

Use the az group create command to create a resource group for the AKS cluster.

Use the az aks create command to deploy the AKS cluster.

Step 4: Create an RBAC binding.

Before you use an Azure Active Directory account with an AKS cluster, you must create role-binding or cluster role-binding. Roles define the permissions to grant, and bindings apply them to desired users. These assignments can be applied to a given namespace, or across the entire cluster.

Reference:

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

Question: 9

HOTSPOT

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	

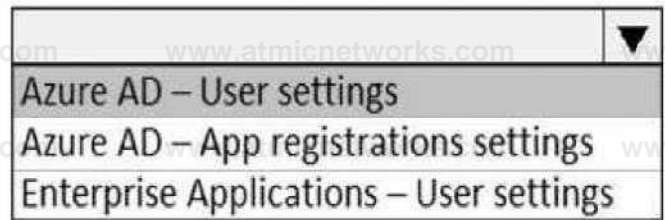
To configure the consent settings:

	▼
Azure AD – User settings	
Azure AD – App registrations settings	
Enterprise Applications – User settings	

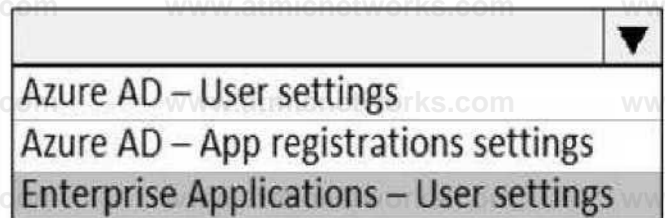
Answer:

Explanation:

To configure the registration settings:



To configure the consent settings:



Reference:

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

Topic 2, Contoso

Overview

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other question on this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next sections of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question on this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

Overview

Contoso, Ltd. is a consulting company that has a main office in Montreal and two branch offices in

Seattle and New York.

The company hosts its entire server infrastructure in Azure.

Contoso has two Azure subscriptions named Sub1 and Sub2. Both subscriptions are associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

Technical requirements

Contoso identifies the following technical requirements:

- Deploy Azure Firewall to VNetWork1 in Sub2.
- Register an application named App2 in contoso.com.
- Whenever possible, use the principle of least privilege.
- Enable Azure AD Privileged Identity Management (PIM) for contoso.com

Existing Environment

Azure AD

Contoso.com contains the users shown in the following table.

Name	City	Role
User1	Montreal	Global administrator
User2	MONTREAL	Security administrator
User3	London	Privileged role administrator
User4	Ontario	Application administrator
User5	Seattle	Cloud application administrator
User6	Seattle	User administrator
User7	Sydney	Reports reader
User8	Sydney	None

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

Name	Membership type	Dynamic membership rule
Group1	Dynamic user	user.city -contains "ON"
Group2	Dynamic user	user.city -match "*on"

Sub1

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User2 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	RG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Sub1 contains the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Allowed resource types	networkSecurityGroups	RG4
Not allowed resource types	virtualNetworks/subnets	RG5
Not allowed resource types	networksSecurityGroups	RG5
Not allowed resource types	virtualNetworks/virtualNetworkPeerings	RG6

Sub2

Name	Subnet
VNetwork1	Subnet1.1, Subnet1.2 and Subent1.3
VNetwork2	Subnet2.1

Sub2 contains the virtual machines shown in the following table.

Name	Network interface	Application security group	Connected to
VM1	NIC1	ASG1	Subnet1.1
VM2	NIC2	ASG2	Subnet1.1
VM3	NIC3	None	Subnet1.2
VM4	NIC4	ASG1	Subnet1.3
VM5	NIC5	None	Subnet2.1

All virtual machines have the public IP addresses and the Web Server (IIS) role installed. The firewalls for each virtual machine allow ping requests and web requests.

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

Name Associated to

NSG1	NIC2
NSG2	Subnet1
NSG3	Subnet1.3
NSG4	Subnet2.1

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

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	80	TCP	Internet	VirtualNetwork	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	TCP	ASG1	ASG1	Allow
150	Any	Any	ASG2	VirtualNetwork	Allow
200	Any	Any	Any	Any	Deny
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
100	Any	Any	Any	Any	Allow
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	AzureLoadBalancer	Any	Allow
65500	Any	Any	Any	Any	Deny

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

Priority	Port	Protocol	Source	Destination	Action
65000	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	Any	Any	Any	Internet	Allow
65500	Any	Any	Any	Any	Deny

Contoso identifies the following technical requirements:

Deploy Azure Firewall to VNetwork1 in Sub2.

Register an application named App2 in contoso.com.

Whenever possible, use the principle of least privilege.

Enable Azure AD Privileged Identity Management (PIM) for contoso.com.

Question: 10

You need to ensure that User2 can implement PIM.

What should you do first?

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

Answer: D

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>

Question: 11

HOTSPOT

What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Group1:

	▼
No members	
Only User2	
Only User2 and User4	
User1, User2, User3, and User4	

Group2:

	▼
No members	
Only User3	
Only User1 and User3	
User1, User2, User3, and User4	

Answer:

Explanation:

Box 1: User1, User2, User3, User4

Contains "ON" is true for Montreal (User1), MONTREAL (User2), London (User 3), and Ontario (User4) as string and regex operations are not case sensitive.

Box 2: User1, User2, User3, User4

Reference:

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

Question: 12

HOTSPOT

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

^°

From VM1, you can successfully ping the public IP address of VM2. 0

From VM1, you can successfully ping the private IP address of VM3. 0

From VM1, you can successfully ping the public IP address of VM5 0

Answer:

Explanation:

Yes,

Yes

No

Question: 13

HOTSPOT

You assign User8 the Owner role for RG4, RG5, and RG6.

In which resource groups can User8 create virtual networks and NSGs? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User8 can create virtual networks in:

	▼
RG4 only	
RG6 only	
RG4 and RG6 only	
RG4, RG5, and RG6	

User8 can create NSGs in:

	▼
RG4 only	
RG4 and RG5 only	
RG4 and RG6 only	
RG4, RG5, and RG6	

Answer:

Explanation:

Box1: RG6 only as there is not option for RG5 & RG6 which it should be.

Box2: RG4 & RG6

Question: 14

HOTSPOT

: 2

HOTSPOT

Which virtual networks in Sub1 can User2 modify and delete in their current state? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Virtual networks that User2 can modify:

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

Virtual networks that User2 can delete:

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

Answer:

Explanation:

Virtual networks that User2 can modify:

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

Virtual networks that User2 can delete:

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

Box 1: VNET4 and VNET1 only

RG1 has only Delete lock, while there are no locks on RG4.

RG2 and RG3 both have Read-only locks.

Box 2: VNET4 only

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

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

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

ReadOnly means authorized users can read a resource, but they can't delete or update the resource.

Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Scenario:

User2 is a Security administrator.

Sub1 contains six resource groups named RG1, RG2, RG3, RG4, RG5, and RG6.

User2 creates the virtual networks shown in the following table.

Name	Resource group
VNET1	RG1
VNET2	FRG2
VNET3	RG3
VNET4	RG4

Sub1 contains the locks shown in the following table.

Name	Set on	Lock type
Lock1	RG1	Delete
Lock2	RG2	Read-only
Lock3	RG3	Delete
Lock4	RG3	Read-only

Reference:

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

Question: 15

HOTSPOT

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.

From VM2, you can successfully ping the private IP address of VM4.

From VM1, you can connect to the web server on VM4.

Answer:

Explanation:

Statements

Yes

No

From VM1, you can successfully ping the private IP address of VM4.

From VM2, you can successfully ping the private IP address of VM4.

From VM1, you can connect to the web server on VM4.

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		AzureLoadBaiancer	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.

Question: 16

You need to meet the technical requirements for VNetwork1.

What should you do first?

- A. Create a new subnet on VNetwork1.
- B. Remove the NSGs from Subnet11 and Subnet13.
- C. Associate an NSG to Subnet12.
- D. Configure DDoS protection for VNetwork1.

Answer: A

Explanation:

From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.

Azure firewall needs a dedicated subnet named AzureFirewallSubnet.

Reference:

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

Question: 17

HOTSPOT

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.

From the Internet, you can connect to the web server on VM2 by using HTTP.

From the Internet, you can connect to the web server on VM3 by using HTTP.

Answer:

Explanation:

Yes No

From the Internet, you can connect to the web server on VM1 by using HTTP. 0

0

From the Internet, you can connect to the web server on VM2 by using HTTP. 0 0

From the Internet, you can connect to the web server on VM3 by using HTTP. 0

Topic 3, Fabrikam inc

Overview

This is a case study. Case studies are not timed separately. You can use as much exam time as you would like to complete each case. However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the Next button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an All Information tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the Question button to return to the question.

General Overview

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

Existing Environment

Network Environment

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

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

The Azure resources hierarchy is shown in the following exhibit.



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

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

Azure AD contains the resources shown in the following table.

Name	Type	Setting
CAPolicy1	Conditional access policy	Users in the finance department must use multi-factor authentication (MFA) when accessing Microsoft SharePoint Online
Sentinel1	Azure Sentinel workspace	Not applicable
SecPoll	Azure Policy definition	Security configuration for virtual machines

Subscription1 Resources

Subscription1 contains the virtual networks shown in the following table.

Name	Subnet	Location	Peer
VNET1	Subnet1, Subnet2	West US	VNET2, VNET3
VNET2	Subnet1	Central US	VNET1, VNET3
VNET3	Subnet1	West US	VNET1, VNET2

Subscription1 contains the network security groups (NSGs) shown in the following table.

Name	Location
NSG2	West US
NSG3	Central US
NSG4	West US

Subscription1 contains the virtual machines shown in the following table.

Name	Operating system	Location	Connected to	Associated NSG
VM1	Windows Server 2019	West US	VNET1/Subnet1	None
VM2	CentOS-based 8.2	West US	VNET1/Subnet2	NSG2
VM3	Windows Server 2016	Central US	VNET2/Subnet1	NSG3
VM4	Ubuntu Server 18.04 LTS	West US	VNET3/Subnet1	NSG4

Subscription1 contains the Azure key vaults shown in the following table.

Name	Location	Pricing tier	Private endpoint
KeyVault1	West US	Standard	VNET1/Subnet1
KeyVault2	Central US	Premium	None
KeyVault3	East US	Premium	VNET1/Subnet1, VNET2/Subnet1, VNET3/Subnet1

Subscription1 contains a storage account named storage1 in the West US Azure region.

Planned Changes and Requirements

Planned Changes

Fabrikam plans to implement the following changes:

Create two application security groups as shown in the following table.

Name	Location
ASG1	West US
ASG2	Central US

Associate the network interface of VM1 to ASG1.

Deploy SecPol1 by using Azure Security Center.

Deploy a third-party app named App1. A version of App1 exists for all available operating systems.

Create a resource group named RG2.

Sync OU2 to Azure AD.

Add User1 to Group1.

Technical Requirements

Fabrikam identifies the following technical requirements:

The finance department users must reauthenticate after three hours when they access SharePoint Online.

Storage1 must be encrypted by using customer-managed keys and automatic key rotation.

From Sentinel1, you must ensure that the following notebooks can be launched:

Entity Explorer – Account

Entity Explorer – Windows Host

Guided Investigation Process Alerts

VM1, VM2, and VM3 must be encrypted by using Azure Disk Encryption.

Just in time (JIT) VM access for VM1, VM2, and VM3 must be enabled.

App1 must use a secure connection string stored in KeyVault1.

KeyVault1 traffic must NOT travel over the internet.

Question: 18

DRAG DROP

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

Answer:

Explanation:

OU2: Azure AD Connect

User1: The Azure portal

Table Description automatically generated

Question: 19

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-lifetime>

Question: 20

HOTSPOT

You need to configure support for Azure Sentinel notebooks to meet the technical requirements.

What is the minimum number of Azure container registries and Azure Machine Learning workspaces required?

Container registries:

www.atmicnetworks.com	▼
0	
1	
2	
3	

Workspaces:

www.atmicnetworks.com	▼
0	
1	
2	
3	

Answer:

Explanation:

Container registries:

	▼
0	
1	
2	
3	

Workspaces:

	▼
0	
1	
2	
3	

Table Description automatically generated with medium confidence

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/notebooks>

Question: 21

From Azure Security Center, you need to deploy SecPol1.

What should you do first?

- A. Enable Azure Defender.
- B. Create an Azure Management group.
- C. Create an initiative.
- D. Configure continuous export.

Answer: B

Explanation:

Reference:

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/security-center/custom-security-policies.md>

<https://zimmergren.net/create-custom-security-center-recommendation-with-azure-policy/>

Question: 22

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>

Question: 23

HOTSPOT

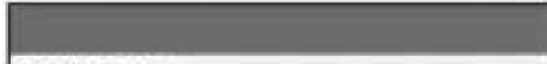
You need to delegate the creation of RG2 and the management of permissions for RG1. Which users can perform each task? To answer select the appropriate options in the answer area. NOTE: Each correct selection is worth one point

Create RGZ



Admin2 And AdniinJ only
Admin! and AdiniM only
Admin?, Admin?,, and Admm4 only
Adrntnl, Admin?, Minin?, and Admm4

Manage RG1 permissions:

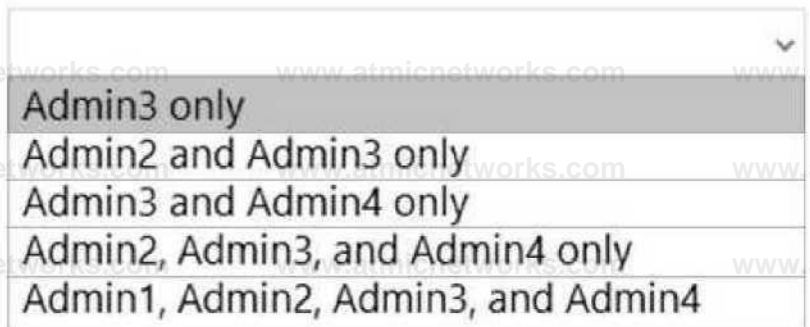


Adminl and Adm®4 only
Admin? and MmKJ only
Admml Admin? and Admin* only
Admml, Mr.m2, Mmmj, and Admin*

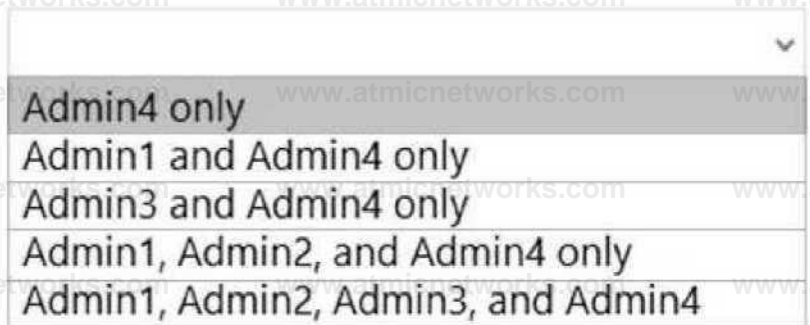
Answer:

Explanation:

Create RG2:



Manage RG1 permissions:



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

Box 1: Admin3 only

The Contributor role has the necessary write permissions to create the resource group.

Box 2: Admin4 only

You need Owner level access to be able to manage permissions. The Contributor role can do most things but cannot modify permissions on existing objects.

Question: 24

You plan to configure Azure Disk Encryption for VM4. Which key vault can you use to store the encryption key?

- A. KeyVault1
- B. KeyVault3
- C. KeyVault2

Answer: A

Explanation:

The key vault needs to be in the same subscription and same region as the VM. VM4 is in West US. KeyVault1 is the only key vault in the same region as the VM.

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

Question: 25

HOTSPOT

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:

NSG2 only
NSG2 and NSG4 only
NSG2, NSG3, and NSG4

Virtual machines: I

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

Answer:

Explanation:

NSGs:

	▼
NSG2 only	
NSG2 and NSG4 only	
NSG2, NSG3, and NSG4	

Virtual machines:

	▼
VM3 only	
VM2 and VM4 only	
VM1, VM2, and VM4 only	
VM2, VM3, and VM4 only	
VM1, VM2, VM3, and VM4	

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

Question: 26

You plan to implement JIT VM access. Which virtual machines will be supported?

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

Answer: A

Explanation:

Topic 4, Fabrikam, Inc.

Case Study

Overview

Existing Environment

Network Environment

Cloud Environment

Sub1 Resources

Fabrikam, Inc. is a consulting company. The company has a main office in New York City and branch offices in Amsterdam and Singapore.

The on-premises network contains a datacenter in each office.

Fabrikam has two Azure subscriptions named Sub1 and Sub2 and a Microsoft 365 subscription that includes Microsoft 365 E5 licenses.

All the subscriptions are linked to a Microsoft Entra tenant named fabrikam.com that contains the identities shown in the following table.

Name	type	Microsoft Entra role	Azure role assignment forSub1
Admin 1	User	Privileged Authentication Administrator	Resource Policy Contributor
Admm2	User	Compliance Administrator	User Access Administrator
Admin3	User	Authentication Administrator	Contributor
Admm4	User	Global Administrator	None
User1	User	None	Reader
AKS1	System-assigned managed identity	None	None
ID1	User-assigned managed identity	None	None

The tenant contains the groups shown in the following table.

Name	Type	Role assignments allowed
Group1	Security	Yes
Group2	Security	No
Group3	Microsoft 365	Yes
Group4	Microsoft 365	No

All devices are enrolled in Microsoft Intune.

Sub2 Resources

Sub1 contains a resource group named RG1 that contains the resources shown in the following table.

Name	Description	Location
SQLServer 1	Azure SQL Database logical server	East US
SQLdb1	Database on SQLServer1	East US
VM1	Virtual machine	East US
AKS1	Azure Kubernetes Service (AKS) cluster	East US
Registry1	Azure container registry	East US
storage1	Storage account	East US
AKV1	Azure key vault	East US

SQLServer1 uses Microsoft SQL Server authentication.

Sub1 has an Azure Web Application Firewall (WAF) named WAF1 that has the following types of rule sets:

- Bot Manager 1.1
- Azure-managed Default Rule Set (DRS)

Sub1 has the following compliance standards assigned in Microsoft Defender for Cloud:

- MIST SP 800-53 Rev. 4
- Microsoft cloud security benchmark (MCSB)
- System and Organization Controls (SOC) 2 Type 2

Planned Changes and Requirements

Planned Changes

Sub2 contains a resource group named RG2.

Fabrikam plans to implement the following changes:

- Deploy the following key vaults to RG1:
 - o AKV2 in the West Europe Azure region
 - o AKV3 in the Central US Azure region
 - o AKV4 in the East US Azure region
- Deploy the following key vaults to RG2:
 - o AKV5 in the East US region
- Configure VM1 to read data from storage1.
- Create function apps that have the following hosting plans:
 - o Fa1: Flex Consumption hosting plan
 - o Fa2: Consumption hosting plan
 - o Fa3: Dedicated hosting plan
- For WAF1, implement rate limiting rules based on the request location.
- Enable the NIST SP 800-53 Rev. 5 compliance standard in Defender for Cloud.
- Create a new storage account named storage2 that supports Azure Table storage.
- Enforce multifactor authentication (MFA) when database administrators access SQLdb1.
- Implement ExpressRoute circuits to the on-premises network as shown in the following table.

Name	Location	Deployment type
ER1	West Europe	ExpressRoute with a connectivity provider
ER2	West Europe	ExpressRoute Metro with a connectivity provider
ER3	East US	ExpressRoute Direct
ER4	Southeast Asia	ExpressRoute Metro Direct

- For RG1, create a new Privileged Identity Management (PIM) eligible role assignment that assigns the Contributor role to supported groups.

Technical Requirements

Fabrikam has the following technical requirements:

- If VM1 is deleted, the permissions for VM1 must be removed automatically.
- The AKS1 managed identity must only be able to pull images from Registry1.
- The ID1 managed identity must be able to push images to and pull images from Registry 1.
- All the data in the storage accounts must be encrypted by using Fabrikam-managed keys.
- All outbound traffic from the function apps to the on-premises network must use ExpressRoute circuits.
- ExpressRoute connectivity between the on-premises network and the Azure environment must be encrypted by using Layer 2 or Layer 3 encryption.

Question: 27

You implement the planned changes for the key vaults.

To which key vaults can you restore AKV1 backups?

- A. AKV4only
- B. AKV3 and AKV4 only
- C. AKV4 and AKV5 only
- D. AKV2, AKV3, and AKV4 only

E. AKV2, AKV3, AKV4, and AKV5

Answer: C

Explanation:

Question: 28

HOTSPOT

You need to configure the AKS1 and ID1 managed identities to meet the technical requirements. The solution must follow the principle of least privilege.

Which role should you assign to each identity? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



ID1; | AcrPush
AcrPull

Contributor
Owner Reader

Answer:

Explanation:

Answer Area

AKS1: AcrPull

ID1 AcrPush

Question: 29

You need to implement the planned change for VM1 to access storage1. The solution must meet the technical requirements.

What should you do first?

- A. Configure a system-assigned managed identity on VM1.
- B. Configure federated identity credentials for ID1.

- C. Assign the Storage Blob Data Reader role to storage 1.
- D. Assign ID1 to VM1.
- E. Add a role assignment condition to storage1.

Answer: A

Explanation:

Question: 30

You need to implement the planned change for WAF1. The solution must minimize administrative effort What should you do?

- A. Create an Azure policy.
- B. Modify the Azure-managed DRS.
- C. Add a custom rule.
- D. Modify the Bot Manager 1.1 rule set.

Answer: C

Explanation:

Question: 31

You need to delegate a user to implement the planned change for Defender for Cloud. The solution must follow the principle of least privilege.

Which user should you choose?

- A. Admin1
- B. Admin2
- C. Admin3
- D. Admin4

Answer: B

Explanation:

Question: 32

HOTSPOT

You need to recommend an encryption solution for the planned ExpressRoute implementation. The solution must meet the technical requirements.

Which ExpressRoute circuit should you recommend for each type of encryption? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Layer 2 encryption ER3 and ER4 only |

- ER1 only
- ER3 only
- ER1 and ER2 only
- ER2 and ER4 only

Layer 3 encryption: [ER1, ER2, ER3, and ER4 *]

- ER1 only
- ERB only
- ER1 and ER2 only
- ER2 and ER4 only
- ER3 and ER4 only

Answer:

Explanation:

Answer Area

Layer 2 encryption ER3 and ER4 only

Layer 3 encryption: ER1, ER2, ER3, and ER4 *

Question: 33

You need to implement the planned change for SQLdb1.
Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Create a compliance policy.
- B. Configure Microsoft Entra authentication for SQLServer1.
- C. Create a Conditional Access policy.
- D. Configure a user-assigned managed identity for SQLdb1.
- E. Configure Federated client identity for SQLdb1.

Answer: B, C

Explanation:

Topic 5, Mix Questions

Question: 34

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared ACCESS signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You generate new SASs.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead you should create a new stored access policy.

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier.

Changing the signed identifier breaks the associations between any existing signatures and the stored access policy.

Deleting or renaming the stored access policy immediately affects all of the shared access signatures associated with it.

Reference:

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

Question: 35

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have an Azure Subscription named Sub1.

You have an Azure Storage account named Sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in Sa1 by using several shared ACCESS signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service.

You need to revoke all access to Sa1.

Solution: You create a new stored access policy.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Shared access signatures provides access to a particular resource such as blog. Stored access policies are a group of Shared Access Signatures (SAS). In order to revoke access to a SAS you can either:

1. Rotate the Key1 or Key 2, that is the access keys used to sign the SAS. Rotating the access keys used to sign the SAS, invalidates any previously signed SAS hence revoking the SAS issued before
2. Remove the stored access policy which an SAS is linked to. If a Stored Access Policy is removed, it also invalidates

the SASs linked to the Stored Access Policy.

Question: 36

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You deploy the On-premises data gateway to the on-premises network.

Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

Create Azure Virtual Network.

Create a custom DNS server in the Azure Virtual Network.

Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.

Configure forwarding between the custom DNS server and your on-premises DNS server.

Reference:

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

Question: 37

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You create a site-to-site VPN between the virtual network and the on-premises network. Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

You can connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions: Create Azure Virtual Network.

Create a custom DNS server in the Azure Virtual Network.

Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.

Configure forwarding between the custom DNS server and your on-premises DNS server.

Reference:

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>

Question: 38

Your network contains an Active Directory forest named contoso.com. The forest contains a single domain.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to deploy Azure AD Connect and to integrate Active Directory and the Azure AD tenant.

You need to recommend an integration solution that meets the following requirements:

Ensures that password policies and user logon restrictions apply to user accounts that are synced to the Tenant

Minimizes the number of servers required for the solution.

Which authentication method should you include in the recommendation?

- A. federated identity with Active Directory Federation Services (AD FS)
- B. password hash synchronization with seamless single sign-on (SSO)
- C. pass-through authentication with seamless single sign-on (SSO)

Answer: C

Explanation:

1. Ensures that password policies and user logon restrictions apply to user accounts that are synced to the tenant

>> Pass-Through Authentication enforce on-premises user account states, password policies, and sign-in hours.

2. Minimizes the number of servers required for the solution.

>> Pass-through needs a lightweight agent to be installed one (or more) on-premises servers.

>> PW Hash also require installing Azure AD Connect on your existing DC.

Question: 39

Your network contains an on-premises Active Directory domain named corp.contoso.com.

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You sync all on-premises identities to Azure AD.

You need to prevent users who have a givenName attribute that starts with TEST from being synced to Azure AD. The solution must minimize administrative effort.

What should you use?

- A. Synchronization Rules Editor
- B. Web Service Configuration Tool
- C. the Azure AD Connect wizard
- D. Active Directory Users and Computers

Answer: A

Explanation:

Use the Synchronization Rules Editor and write attribute-based filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

Question: 40

DRAG DROP

You are implementing conditional access policies.

You must evaluate the existing Azure Active Directory (Azure AD) risk events and risk levels to configure and implement the policies.

You need to identify the risk level of the following risk events:

Users with leaked credentials

Impossible travel to atypical locations

Sign ins from IP addresses with suspicious activity

Which level should you identify for each risk event? To answer, drag the appropriate levels to the correct risk events. Each level 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.

Levels

Answer Area

High

Impossible travel to atypical locations:

Low

Users with leaked credentials:

Medium

Sign ins from IP addresses with suspicious activity:

Answer:

Explanation:

Medium

High

Medium

Refer <https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events#sign-ins-from-ip-addresses-with-suspicious-activity>

Question: 41

HOTSPOT

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

Name	Member of	Mobile phone	Multi-factor authentication (MFA) status
User1	Group1	123 555 7890	Disabled
User2	Group1, Group2	None	Enabled
User3	Group1	123 555 7891	Required

You create and enforce an Azure AD Identity Protection user risk policy that has the following settings:

Assignment: Include Group1, Exclude Group2

Conditions: Sign-in risk of Medium and above

Access: Allow access, Require password change

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

If User1 signs in from an unfamiliar location, he must change his password.

If User2 signs in from an anonymous IP address, she must change her password.

If User3 signs in from a computer containing malware that is communicating Q with known bot servers, he must change his password.

Answer:

Explanation:

Answer Area

Statements

Yes

No

If User1 signs in from an unfamiliar location, he must change his password.

If User2 signs in from an anonymous IP address, she must change her password.

If User3 signs in from a computer containing malware that is communicating Q with known bot servers, he must change his password.

Box 1: Yes

User1 is member of Group1. Sign in from unfamiliar location is risk level Medium.

Box 2: Yes

User2 is member of Group1. Sign in from anonymous IP address is risk level Medium.

Box 3: No

Sign-ins from IP addresses with suspicious activity is low.

Note:

Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

Azure AD Identity protection can detect six types of suspicious sign-in activities:

Users with leaked credentials

Sign-ins from anonymous IP addresses

Impossible travel to atypical locations

Sign-ins from infected devices

Sign-ins from IP addresses with suspicious activity

Sign-ins from unfamiliar locations

These six types of events are categorized in to 3 levels of risks – High, Medium & Low:

Reference:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

Question: 42

DRAG DROP

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

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

Create an access review program

Set Reviewers to Selected users.

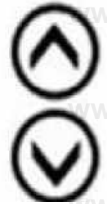
Create an access review audit.

Create an access review control

Set Reviewers to Group owners

Set Reviewers to Members

Explanation:



Answer:

Answer Area

Create an access review program

Create an access review control.

Set Reviewers to Group owners

Step 1: Create an access review program

Step 2: Create an access review control

Step 3: Set Reviewers to Group owners

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

Reviewers	Group Owner!	A
Reviewers	Group owneen	
Programs	Selected users	
Link to prooem	Member! ist!!)	

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>

Question: 43

HOTSPOT

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

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

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

Create an access review

Access reviews enable reviewers to attest to users access.

Review name **Review1**

Description

Start date **2019-03-01**

Frequency **One time**

End date **2019-03-20**

Number of items

Users

Scope Everyone

Review role membership **Password administrator**

Reviewers **Members(self)**

Auto apply results to resource **Enable**

Auto apply results to resource **Enable**

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

NOTE: Each correct selection is worth one point.

User3 can perform Review1 for

- User3 only
- User1 and User2 only
- User1, User2, and User3

If User2 fails to complete Review1 by March 20,2019

The Password administrator role will be revoked from User2
User2 will retain the Password administrator role
User3 will receive a confirmation request

Answer:

Explanation:

User3 can perform Review for

User3 only
User1 and User2 only
User1, User2, and User3

If User2 fails to complete Review by March 20,2019

The Password administrator role will be revoked from User2
User2 will retain the Password administrator role
User3 will receive a confirmation request

Box 1: User3 only

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

Box 2: User3 will receive a confirmation request

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

No change - Leave user's access unchanged

Remove access - Remove user's access

Approve access - Approve user's access

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

Reference:

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

Question: 44

DRAG DROP

You create an Azure subscription.

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

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

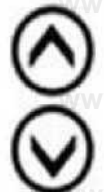
Verify your identity by using multi-factor authentication (MFA).

Consent to PIM

Sign up PIM for Azure AD roles

Discover privileged roles

Discover resources



Answer:

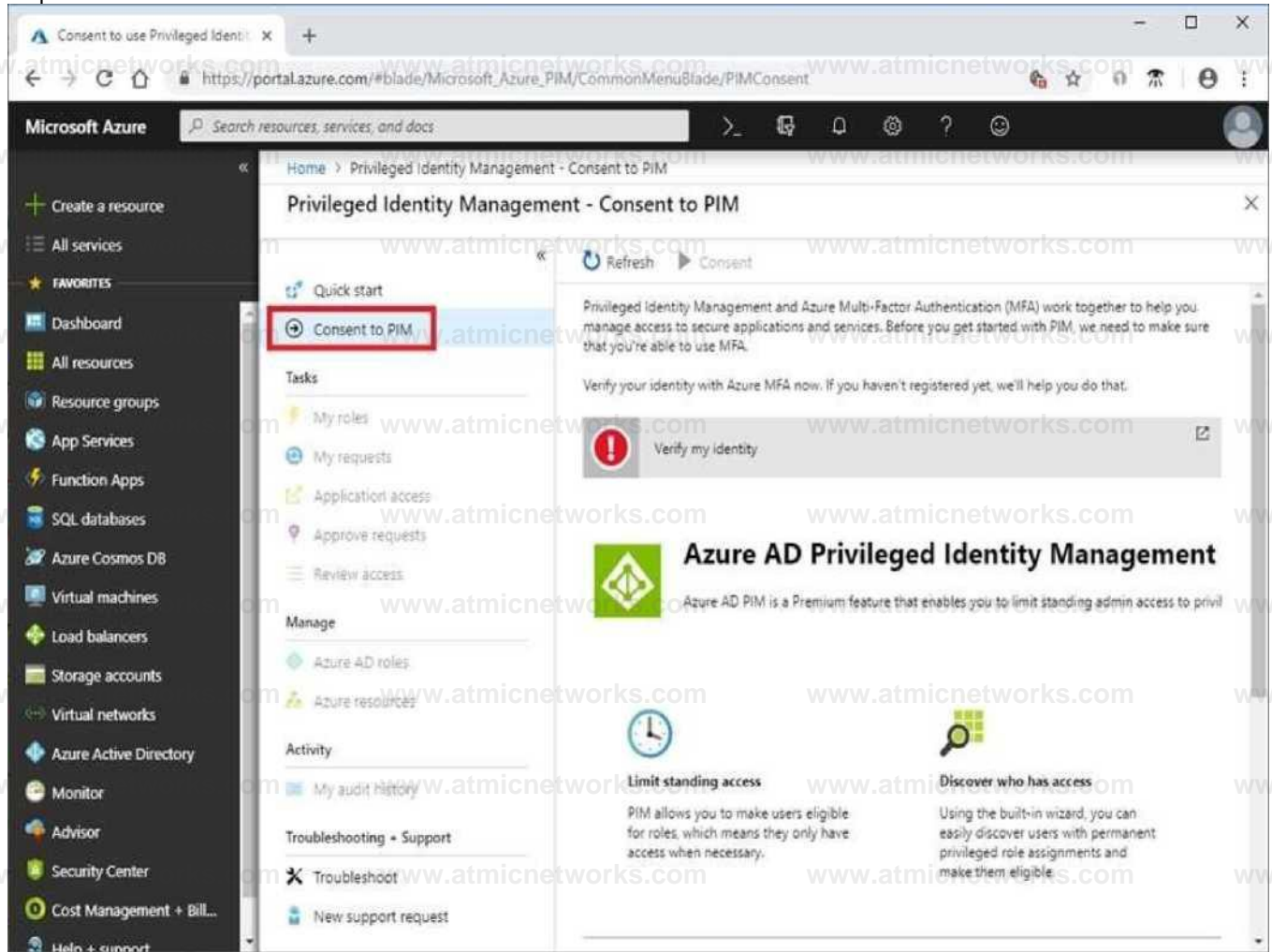
Explanation:

Consent to PIM

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

Sign up PIM for Azure AD roles.

Step 1: Consent to PIM



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

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

Step 3: Sign up PIM for Azure AD roles

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

Reference:

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

Question: 45

HOTSPOT

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

Location	IP address space	Public NAT segment
Seattle	10.10.0.0/16	190.15.1.0/24
New York	172.160.0/16	194.25.2.0/24

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

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

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



✓

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

NOTE: Each correct selection is worth one point.

Yes

No

If User1 signs in to Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone. Q 0

If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. Q Q

If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone. Q Q

Answer:

Explanation:

Yes

No

If User1 signs into Azure from a device that uses an IP address of 134.18.14.10, User1 must be authenticated by using a phone. Q 0

If User2 signs in to Azure from a device in the Seattle office, User2 must be authenticated by using the Microsoft Authenticator app. Q Q

If User2 signs in to Azure from a device in the New York office, User1 must be authenticated by using a phone. Q Q

Box 2: No

Use of Microsoft Authenticator is not required.

Note: Microsoft Authenticator is a multifactor app for mobile devices that generates time-based codes used during the Two-Step Verification process.

Box 3: No

The New York IP address subnet is included in the "skip multi-factor authentication for request."

Reference:

<https://www.cayosoft.com/difference-enabling-enforcing-mfa/>

Question: 46

HOTSPOT

You have an Azure Container Registry named Registry1.

You add role assignment for Registry1 as shown in the following table.

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

Which users can upload images to Registry1 and download images from Registry1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Upload images:

	▼
User1 only	
User1 and User4 only	
User1, User3, and User4	
User1, User2, User3, and User4	

Download images:

	▼
User2 only	
User1 and User2 only	
User2 ad User4 only	
User1, User2, and User4	
User1, User2, User3, and User4	

Answer:

Explanation:

Upload images:

	▼
User1 only	
User1 and User4 only	
User1, User3, and User4	
User1, User2, User3, and User4	

Download images:

	▼
User2 only	
User1 and User2 only	
User2 ad User4 only	
User1, User2, and User4	
User1, User2, User3, and User4	

Box 1: User1 and User4 only
 Owner, Contributor and AcrPush can push images.

Box 2: User1, User2, and User4

Role/Permission	Access Resource Manager	Create/delete registry	image	Pun image	Delete image data	Change policies	Sign images
Owner	X	X	X	X	X	X	
Contributor	X	X	X	X	X	X	
Reader	X			X			
AcrPush			X	X			
AcrPull				X			
AcrDelete					X		

All, except AcrImagineSigner, can download/pull images.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-roles>

Question: 47

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: B,F

Explanation:

8: 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.

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

Question: 48

You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named Subnet1.

You create a service endpoint for Subnet1.

Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 18.04.

You need to deploy Docker containers to VM1. The containers must be able to access Azure Storage resources and Azure SQL databases by using the service endpoint.

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

Answer: C

Explanation:

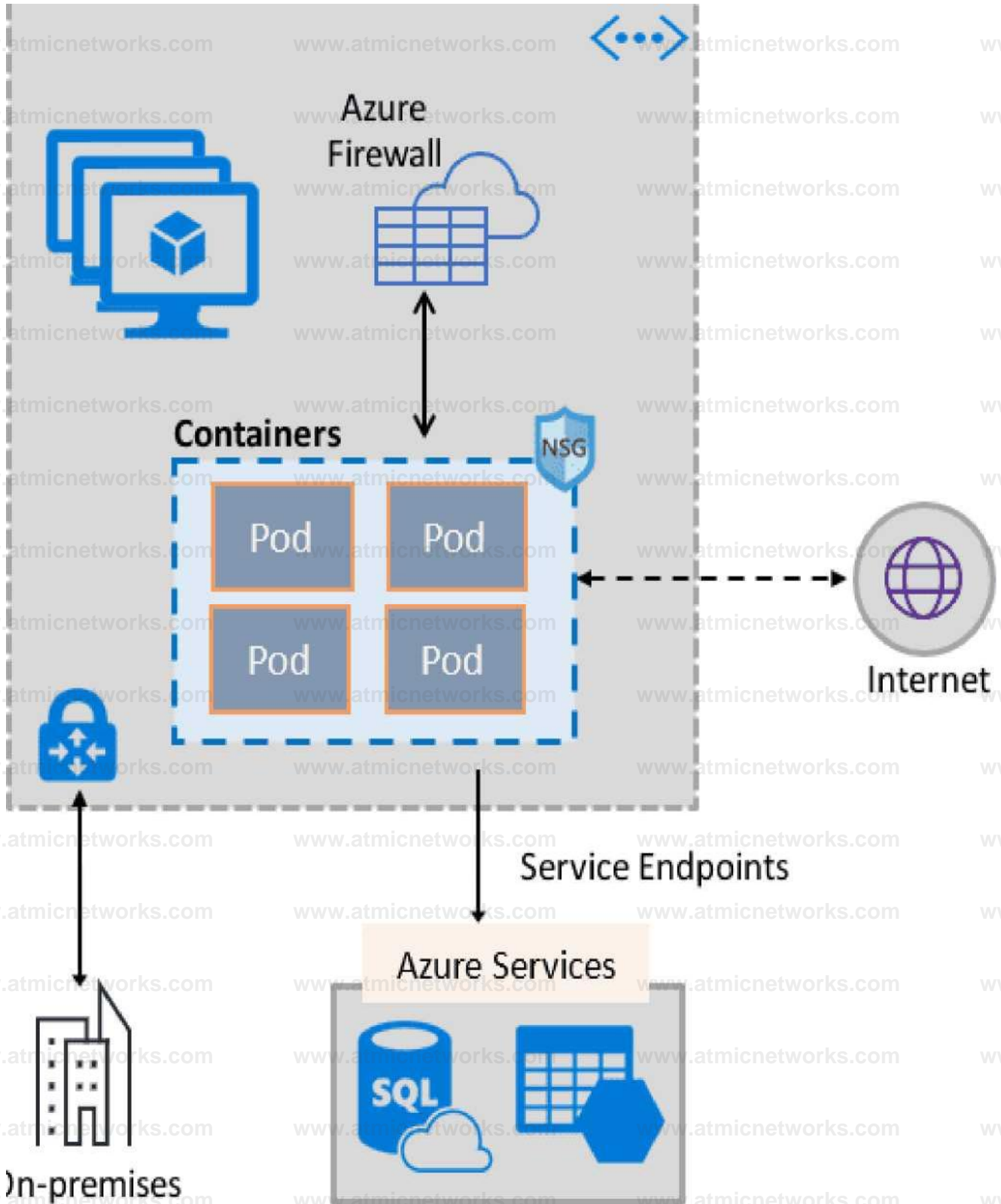
The Azure Virtual Network container network interface (CNI) plug-in installs in an Azure Virtual Machine. The plug-in supports both Linux and Windows platform.

The plug-in assigns IP addresses from a virtual network to containers brought up in the virtual machine, attaching them to the virtual network, and connecting them directly to other containers

and virtual network resources. The plug-in doesn't rely on overlay networks, or routes, for connectivity, and provides the same performance as virtual machines.

The following picture shows how the plug-in provides Azure Virtual Network capabilities to Pods:

Existing virtual network



On-premises
Reference:

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

Question: 49

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.

Reference:

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

Question: 50

DRAG DROP

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

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

The Azure virtual machines on SpokeVNetSubnet0 can communicate with the computers on the onpremises network.

You plan to deploy an Azure firewall to HubVNet.

You create the following two routing tables:

RT1: Includes a user-defined route that points to the private IP address of the Azure firewall as a next hop address

RT2: Disables BGP route propagation and defines the private IP address of the Azure firewall as the default gateway

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

To which subnet should you associate each route table? To answer, drag the appropriate subnets to the correct route tables. Each subnet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Subnets

Azure FirewallSubnet

GatewaySubnet

HubVNetSubnet0

Answer Area

RT1:

RT2:

Answer:

Explanation:

Answer Area

RT1: GatewaySubnet

RT2: HubVNetSubnet0

Question: 51
HOTSPOT

You have an Azure subscription. The subscription contains Azure virtual machines that run Windows Server 2016.

You need to implement a policy to ensure that each virtual machine has a custom antimalware virtual machine extension installed.

How should you complete the policy? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```
"if" : (
  "allot": [
    ("field" : "type", "equals": "Microsoft.Compute/virtualMachines",
      {
        "field" : "Microsoft.Compute/imageSKU", "equals" : "2016-Datacenter",

"then" : { "effect" ; "
          Append
          Deny _____ DeployIfNotExists

"details" : ( "type" ; "Microsoft.Guestconfiguration/guestConfigurationAsslgnments",
  "roleDefinitionsIds" : [
    "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abad-012345678910" I,
    "name" : "customExtension", "deployment" : { "properties" : ( "mode"; "incremental". "parameters" :
      ( ), "
        existencecondition resources template"
```

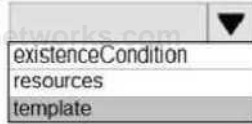
Answer:

Explanation:

```

"then" : ( "effect" ; "
Append Deny DeployIfNotExists "details" : (
"type" ; "Microsoft.Guestconfiguration/guestConfigurationAssignments", "roleDefinitionsIds" : [
"/providers/Microsoft.authorization/roleDefinitions/1234 5678 -1234-5678-abcd-012345678910" ],
"name" : "customExtension"; "deployment" : {
"properties" : ( ."mode"; "incremental".
"parameters" : {
}
}
)
)

```



Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

The details property of the DeployIfNotExists effects has all the subproperties that define the related resources to match and the template deployment to execute.

Deployment [required]

This property should include the full template deployment as it would be passed to the Microsoft.Resources/deployment

Reference:

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

Question: 52

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.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/container-registry/container-registry-auth-aks>

Question: 53

HOTSPOT

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

Name	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

You create the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.

Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

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

NOTE: Each correct selection is worth one point.

Answer Area

Statements

You can start VM1.

Yes

No

You can start VM2.

You can create a virtual machine in RG2.

Answer:

Explanation:

Answer Area

Statements

You can start VM1.

Yes

No

You can start VM2.

You can create a virtual machine in RG2.

Reference:

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

Question: 54

HOTSPOT

You have Azure virtual machines that have Update Management enabled. The virtual machines are

configured as shown in the following table.

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West US	RG1
VM3	Windows Server 2016	West US	RG2
VM4	Ubuntu Server 18 04 LTS	West US	RG2
VM5	Red Hat Enterprise Linux 7 4	East US	RG1
VM6	CemOS 7.5	East US	RG1

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

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

NOTE: Each correct selection is worth one point.

Update1:

▼

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

Update2:

▼

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

Answer:

Explanation:

Update1:

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

Update2:

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

Update1: VM1 and VM2 only
VM3: Windows Server 2016 West US RG2

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

For Linux, the machine must have access to an update repository. The update repository can be private or public.

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management>

Question: 55

HOTSPOT

You have an Azure subscription named Sub1.

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

following table.

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

Currently, you have not provisioned any network security groups (NSGs).

You need to implement network security to meet the following requirements:

Allow traffic to VM4 from VM3 only.

Allow traffic from the Internet to VM1 and VM2 only.

Minimize the number of NSGs and network security rules.

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

NOTE: Each correct selection is worth one point.

NSGs:

	▼
1	
2	
3	
4	

Network security rules:

	▼
1	
2	
3	
4	

Answer:

Explanation:

NSGs: 1

Network security rules: 3

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

Reference:

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

Question: 56

HOTSPOT

You have an Azure key vault.

You need to delegate administrative access to the key vault to meet the following requirements:

Provide a user named User1 with the ability to set advanced access policies for the key vault.

Provide a user named User2 with the ability to add and delete certificates in the key vault.

Use the principle of least privilege.

What should you use to assign access to each user? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User1:

	▼
A key vault access policy	
Azure Information Protection	
Azure Policy	
Managed identities for Azure resources	
RBAC	

User2:

	▼
A key vault access policy	
Azure Information Protection	
Azure Policy	
Managed identities for Azure resources	
RBAC	

Answer:

Explanation:

User1:

	▼
A key vault access policy	
Azure Information Protection	
Azure Policy	
Managed identities for Azure resources	
RBAC	

User2:

	▼
A key vault access policy	
Azure Information Protection	
Azure Policy	
Managed identities for Azure resources	
RBAC	

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.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

Question: 57

HOTSPOT

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-DA1LY-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

Answer:

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

Reference:

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

Question: 58

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.

Incorrect Answers:

B,C,A: Log Analytics workspace provides a geographic location for data storage. VM2 and VM3 are at a different location.

E. VM4 is a different resource group.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/manage-access>

Question: 59

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 akscluster2 1.1 1.5
Kubernetes cluster name	akscluster2 3
Kubernetes version	Standard_DS2_v2 Disabled
DNS name prefix	
Node count	
Node size	
Virtual nodes (preview)	

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.

Reference:
<https://docs.microsoft.com/en-us/azure/aks/ingress-tls>

Question: 60

HOTSPOT

You plan to use Azure Log Analytics to collect logs from 200 servers that run Windows Server 2016.

You need to automate the deployment of the Microsoft Monitoring Agent to all the servers by using an Azure Resource Manager template.

How should you complete the template? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

```

"type" : "Microsoft.Compute/virtualMachines/extensions" "name" : "[concat(parameter('vmname*'),
/OMSExtension]", "apiVersion" : "[variables('apiVersion')]", "location" : "[resourceGroup().location]",
"dependsOn" : [
concat('Microsoft.Compute/virtualMachines/', parameters('vmName'))]

"properties" : {
"publisher" : "Microsoft.Enterprisecloud.Monitoring" "type" : "MicrosoftMonitoringAgent",
"typeHandlerVersion" : "1.0", "autoUpgradeMinorVersion" : true, "settings" : (
[variable('vari')]

AzureADApp call on D
'WorkspaceID'
'WorkspaceName'
'WorkspaceURL'

"protectedSettings" : {
: "[variable('var2')]

'AzureADApp call on Sec rel' 'StorageAccountKey' 'WorkspaceID' 'WorkspaceKey'

```

Answer:

Explanation:

```

properties" : {
  "publisher" : "Microsoft.Enterprise
"type" : "MicrosoftMonitoringAgent
"typeHandlerVersion" : " "autoUpgradeMinorVersion
"settings" : {
  true.
  "AzureADApplication@* 'Workspace@' 'WorkspaceName' 'WorkspaceURL'
  "protectedSettings
  ' AzureADApph cati onSecret 'StorageAccountKey' 'Workspace@'
  'WorkspaceKey'
}

```

Reference:

<https://blogs.technet.microsoft.com/manageabilityguys/2015/11/19/enabling-the-microsoft-monitoring-agent-in-windows-json-templates/>

Question: 61

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You are assigned the Global administrator role for the tenant. You are responsible for managing Azure Security Center settings.

You need to create a custom sensitivity label.

What should you do first?

- A. Create a custom sensitive information type.
- B. Elevate access for global administrators in Azure AD.
- C. Upgrade the pricing tier of the Security Center to Standard.
- D. Enable integration with Microsoft Cloud App Security.

Answer: A

Explanation:

First, you need to create a new sensitive information type because you can't directly modify the default rules.

Reference:

<https://docs.microsoft.com/en-us/office365/securitycompliance/customize-a-built-in-sensitive-information-type>

Question: 62

HOTSPOT

You suspect that users are attempting to sign in to resources to which they have no access.

You need to create an Azure Log Analytics query to identify failed user sign-in attempts from the last three days. The results must only show users who had more than five failed sign-in attempts.

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

NOTE: Each correct selection is worth one point.

```
let timeframe = 3d;
SecurityEvent
| where TimeGenerated > ago(3d)
| where AccountType == 'User' and
| Summarize failed_login_attempts=
latest_failed_login=arg_max(TimeGenerated by Account
| where failed_login_attempts > 5
```

▼	==4625
ActivityID	
DataType	
EventID	
QuantityUnit	

▼	
Count()	
Countif()	
Makeset()	
Split()	

Answer:

Explanation:

```
let timeframe = 3d; SecurityEvent | where TimeGenerated >
ago(3d) | where Account Type == 'User' and
Summarize failed_login_attempts=
latest_failed_login=arg_max(TimeGenerated by Account
where failed_login_attempts > 5
```

- ActivityID
- DataType
- EventID
- Quantityunit
- Count()
- Countif()
- Makeset()
- Split()

The following example identifies user accounts that failed to log in more than five times in the last day, and when they last attempted to log in.

```
let timeframe = 1d; SecurityEvent | where TimeGenerated > ago(1d) | where AccountType == 'User' and EventID == 4625 // 4625 - failed log in | summarize failed_login_attempts=count(), latest_failed_login=arg_max(TimeGenerated, Account) by Account | where failed_login_attempts > 5 | project-away Account1
```

Reference:

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

Question: 63

You have an Azure subscription named Sub1.

In Azure Security Center, you have a security playbook named Play1. Play1 is configured to send an email message to a user named User1.

You need to modify Play1 to send email messages to a distribution group named Alerts.

What should you use to modify Play1?

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

Answer: D

Explanation:

You can change an existing playbook in Security Center to add an action, or conditions. To do that you just need to click on the name of the playbook that you want to change, in the Playbooks tab, and Logic App Designer opens up.

Reference:

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

Question: 64

You create a new Azure subscription.

You need to ensure that you can create custom alert rules in Azure Security Center.

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

NOTE: Each correct selection is worth one point.

- A. Onboard Azure Active Directory (Azure AD) Identity Protection.
- B. Create an Azure Storage account.
- C. Implement Azure Advisor recommendations.
- D. Create an Azure Log Analytics workspace.
- E. Upgrade the pricing tier of Security Center to Standard.

Answer: D,E

Explanation:

D: You need write permission in the workspace that you select to store your custom alert.

Reference:

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

Question: 65

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1. You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.

You need to configure alerts based on the data collected by LAW1. The solution must meet the following requirements:

Alert rules must support dimensions.

The time it takes to generate an alert must be minimized.

Alert notifications must be generated only once when the alert is generated and once when the alert is resolved.

Which signal type should you use when you create the alert rules?

- A. Log
- B. Log (Saved Query)
- C. Metric
- D. Activity Log

Answer: C

Explanation:

Metric alerts in Azure Monitor provide a way to get notified when one of your metrics cross a threshold. Metric alerts work on a range of multi-dimensional platform metrics, custom metrics, Application Insights standard and custom metrics.

Note: Signals are emitted by the target resource and can be of several types. Metric, Activity log, Application Insights, and Log.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric>

Question: 66

DRAG DROP

You have an Azure subscription that contains 100 virtual machines. Azure Diagnostics is enabled on all the virtual machines.

You are planning the monitoring of Azure services in the subscription.

You need to retrieve the following details:

Identify the user who deleted a virtual machine three weeks ago.

Query the security events of a virtual machine that runs Windows Server 2016.

What should you use in Azure Monitor? To answer, drag the appropriate configuration settings to the correct details. Each configuration setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Settings Answer Area

Activity log

Logs

Identify the user who deleted a virtual machine three weeks ago:

Metrics

Query the security events of a virtual machine that runs
Windows Server 2016:

Service Health

Answer:

Explanation:

Identify the user who deleted a virtual machine three weeks ago:

Activity log

Query the security events of a virtual machine that runs
Windows Server 2016:

Logs

Box1: Activity log

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

Activity logs help you determine the "what, who, and when" for write operations (that is, PUT, POST, or DELETE).

Box 2: Logs

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

Reference:

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

Question: 67

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.

Incorrect Answers:

A,D: Application permissions - Your client application needs to access the web API directly as itself

(no user context). This type of permission requires administrator consent and is also not available for public (desktop and mobile) client applications.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-access-web-apis>

Question: 68

DRAG DROP

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

The company is developing an application named App1. App1 will run as a service on server that runs Windows Server 2016. App1 will authenticate to contoso.com and access Microsoft Graph to read directory data.

You need to delegate the minimum required permissions to App1.

Which three actions should you perform in sequence from the Azure portal? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

Answer Area

Grant permissions

Add a delegated permission.

Configure Azure AD Application Proxy

Add an application permission.

Create an app registration.



Answer:

Explanation:

Create an app registration.

Add an application permission.

Grant permissions

Step 1: Create an app registration
First the application must be created/registered.

Step 2: Add an application permission
Application permissions are used by apps that run without a signed-in user present.

Step 3: Grant permissions

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-permissions-and-consent>

Question: 69

Your company has an Azure subscription named Sub1 that is associated to an Azure Active Directory Azure (Azure AD) tenant named contoso.com.

The company develops a mobile application named App1. App1 uses the OAuth 2 implicit grant type to acquire Azure AD access tokens.

You need to register App1 in Azure AD.

What information should you obtain from the developer to register the application?

- A. a redirect URI
- B. a reply URL
- C. a key
- D. an application ID

Answer: A

Explanation:

For Native Applications you need to provide a Redirect URI, which Azure AD will use to return token responses.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v1-protocols-oauth-code>

Question: 70

From the Azure portal, you are configuring an Azure policy.

You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects.

Which effect requires a managed identity for the assignment?

- A. AuditIfNotExist
- B. Append
- C. DeployIfNotExist
- D. Deny

Answer: C

Explanation:

When Azure Policy runs the template in the deployIfNotExists policy definition, it does so using a managed identity.

Reference:

<https://docs.microsoft.com/bs-latn-ba/azure/governance/policy/how-to/remediate-resources>

Question: 71
HOTSPOT

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to implement an application that will consist of the resources shown in the following table.

Name	Type	Description
CosmosDB Account!	Azure Cosmos DB account	A Cosmos DB account containing a database Named CosmosDB 1 that serves as a back-end tier of the application
WebAppl	Azure web app	A web app configured to serve as the middle tier of the application

Users will authenticate by using their Azure AD user account and access the Cosmos DB account by using resource tokens.

You need to identify which tasks will be implemented in CosmosDB1 and WebApp1.

Which task should you identify for each resource? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

CosmosDBI:

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

Web App 1:

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

Answer:

Explanation:

CosmosDBI:

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

WebApp1:

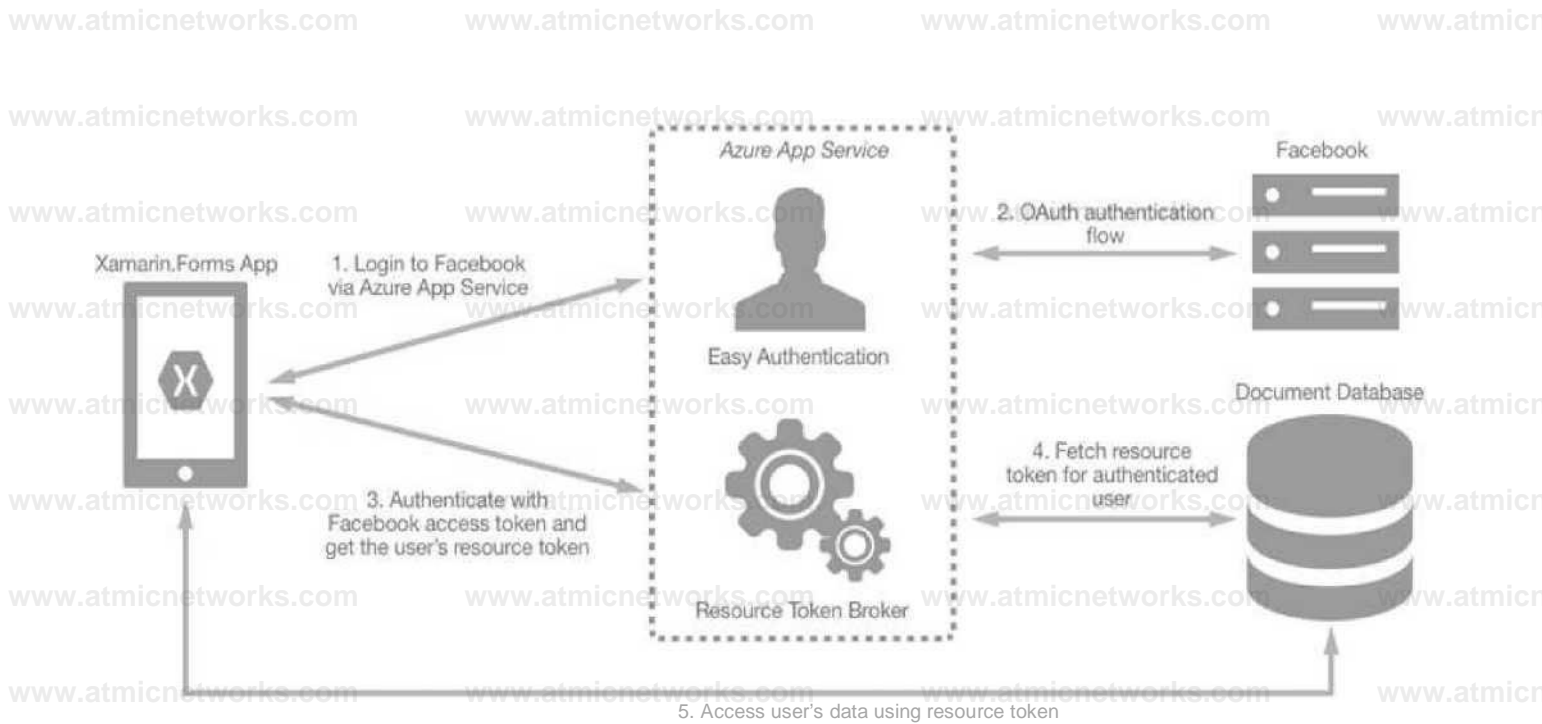
- Authenticate Azure AD users and generate resource tokens.
- Authenticate Azure AD users and relay resource tokens.
- Create database users and generate resource tokens.

CosmosDB1: Create database users and generate resource tokens.

Azure Cosmos DB resource tokens provide a safe mechanism for allowing clients to read, write, and delete specific resources in an Azure Cosmos DB account according to the granted permissions.

WebApp1: Authenticate Azure AD users and relay resource tokens

A typical approach to requesting, generating, and delivering resource tokens to a mobile application is to use a resource token broker. The following diagram shows a high-level overview of how the sample application uses a resource token broker to manage access to the document database data:



Reference:

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

Question: 72

HOTSPOT

You need to create an Azure key vault. The solution must ensure that any object deleted from the key vault be retained for 90 days.

How should you complete the command? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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

```
-Location 'East US'
```

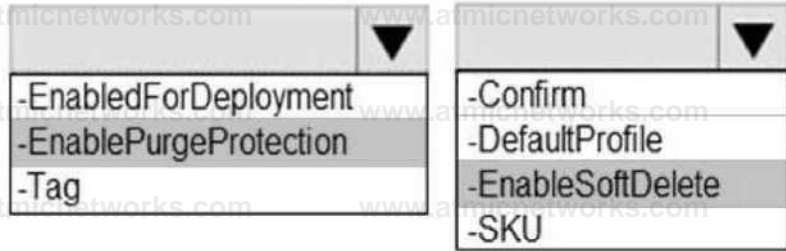
<input type="checkbox"/> -EnabledForDeployment
<input type="checkbox"/> -EnablePurgeProtection
<input type="checkbox"/> -Tag

<input type="checkbox"/> -Confirm
<input type="checkbox"/> -DefaultProfile
<input type="checkbox"/> -EnableSoftDelete
<input type="checkbox"/> -SKU

Answer:

Explanation:

```
New-AzureRmKeyVault -VaultName 'KeyVault1' -ResourceGroupName 'RG1'  
-Location 'East US'
```



Box 1: -EnablePurgeProtection

If specified, protection against immediate deletion is enabled for this vault; requires soft delete to be enabled as well.

Box 2: -EnableSoftDelete

Specifies that the soft-delete functionality is enabled for this key vault. When soft-delete is enabled, for a grace period, you can recover this key vault and its contents after it is deleted.

Reference:

<https://docs.microsoft.com/en-us/powershell/module/azurermskeyvault/new-azurermskeyvault>

Question: 73

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>

Question: 74

You have an Azure SQL database.

You implement Always Encrypted.

You need to ensure that application developers can retrieve and decrypt data in the database.

What information should you provide to the developers? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a stored access policy
- B. a shared access signature (SAS)

- C. the column encryption key
- D. user credentials
- E. the column master key

Answer: C,E

Explanation:

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

Reference:

<https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/always-encrypted-database-engine>

Question: 75

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

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

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

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

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

Which authentication method should you instruct the developers to use?

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

Answer: C

Explanation:

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

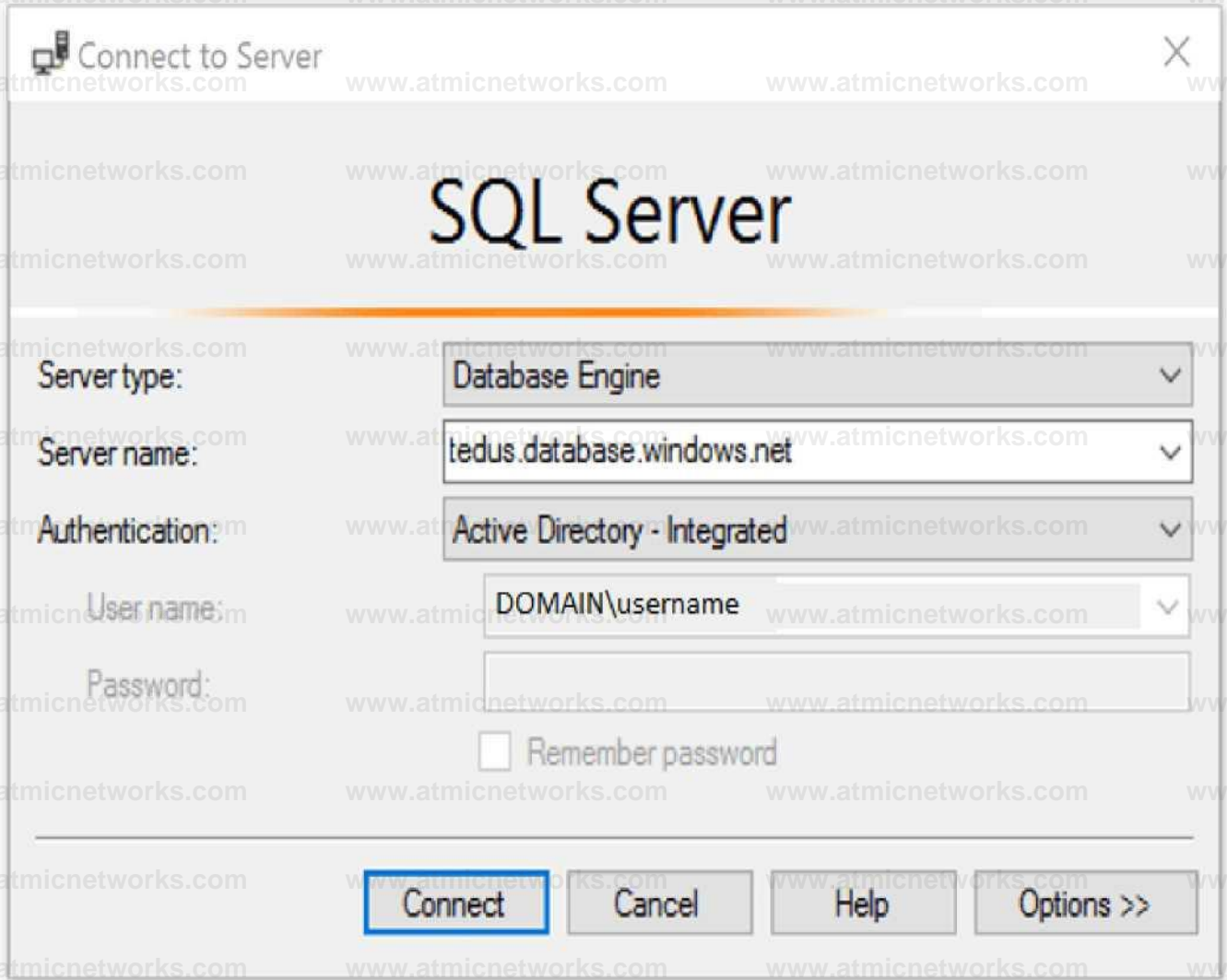
Using an Azure AD identity to connect using SSMS or SSDT

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

Active Directory integrated authentication

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

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



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

Reference:

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

Question: 76

DRAG DROP

You have an Azure subscription named Sub1 that contains an Azure Storage account named

Contosostorage1 and an Azure key vault named Contosokeyvault1.

You plan to create an Azure Automation runbook that will rotate the keys of Contosostorage1 and store them in Contosokeyvault1.

You need to implement prerequisites to ensure that you can implement the runbook.

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

Run Set-AzureRmKeyVaultAccessPolicy

Create an Azure Automation account

Import PowerShell modules to the Azure Automation account

Create a user-assigned managed identity

Create a connection resource in the Azure Automation account.



Answer:

Explanation:

Create an Azure Automation account.

Import PowerShell modules to the Azure Automation account.

Create a connection resource in the Azure Automation account.

Step 1: Create an Azure Automation account

Runbooks live within the Azure Automation account and can execute PowerShell scripts.

Step 2: Import PowerShell modules to the Azure Automation account

Under 'Assets' from the Azure Automation account Resources section select 'to add in Modules to the runbook. To execute key vault cmdlets in the runbook, we need to add AzureRM.profile and AzureRM.key vault.

Step 3: Create a connection resource in the Azure Automation account

You can use the sample code below, taken from the AzureAutomationTutorialScript example runbook, to authenticate using the Run As account to manage Resource Manager resources with your runbooks. The AzureRunAsConnection is a connection asset automatically created when we created 'run as accounts' above. This can be found under Assets -> Connections. After the authentication code, run the same code above to get all the keys from the vault.

```
$connectionName = "AzureRunAsConnection" try
{
# Get the connection "AzureRunAsConnection "
$servicePrincipalConnection=Get-AutomationConnection -Name $connectionName
```

```
"Logging in to Azure..."
Add-AzureRmAccount `
-ServicePrincipal `
-TenantId $servicePrincipalConnection.TenantId `
-ApplicationId $servicePrincipalConnection.ApplicationId `
-CertificateThumbprint $servicePrincipalConnection.CertificateThumbprint }
```

Reference:

<https://www.rahulnath.com/blog/accessing-azure-key-vault-from-azure-runbook/>

Question: 77

You have an Azure SQL Database server named SQL1.

You plan to turn on Advanced Threat Protection for SQL1 to detect all threat detection types.

Which action will Advanced Threat Protection detect as a threat?

- A. A user updates more than 50 percent of the records in a table.
- B. A user attempts to sign as SELECT * from table1.
- C. A user is added to the db_owner database role.
- D. A user deletes more than 100 records from the same table.

Answer: B

Explanation:

Advanced Threat Protection can detect potential SQL injections: This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection-overview>

Question: 78

HOTSPOT

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

Name	Pattern	Case sensitivity
Condition 1	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
Policy 1	Useri	Label 1	None
Policy2	Useri	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	

Answer:

Explanation:

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	

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.

Reference:

<https://docs.microsoft.com/en-us/azure/information-protection/configure-policy-classification>

Question: 79

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.

Reference:

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

Question: 80

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.

Reference:

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

Question: 81

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

You need to configure the environment to support the planned authentication.

Solution: You deploy Azure Active Directory Domain Services (Azure AD DS) to the Azure subscription.

Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/hdinsight/domain-joined/apache-domain-joined-configure-using-azure-adds>

Question: 82

Your network contains an Active Directory forest named contoso.com. You have an Azure Directory (Azure AD) tenant named contoso.com.

You plan to configure synchronization by using the Express Settings installation option in Azure AD Connect.

You need to identify which roles and groups are required to perform the planned configurations. The solution must use the principle of least privilege.

Which two roles and groups should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. the Domain Admins group in Active Directory
- B. the Security administrator role in Azure AD
- C. the Global administrator role in Azure AD
- D. the User administrator role in Azure AD
- E. the Enterprise Admins group in Active Directory

Answer: C,E

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions>

Question: 83

DRAG DROP

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

The answer area consists of five empty rectangular boxes stacked vertically, intended for the user to drag and drop the selected actions from the 'Actions' list into the correct sequence.

Answer:

Explanation:

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

Question: 84

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 definition and assignments that are scoped to resource groups.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Reference:

<https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/>

Question: 85

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.

/457

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

Solution: You create a resource graph and an assignment that is scoped to a management group.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/governance/management-groups/create>

Question: 86

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.

Reference:

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

Question: 87

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 connect to each virtual machine and add a Windows feature.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Microsoft Antimalware is deployed as an extension and not a feature.

Reference:

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

Question: 88

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:

Reference:

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

Question: 89

HOTSPOT

/457

You create an alert rule that has the following settings:

Resource: RG1

Condition: All Administrative operations

Actions: Action groups configured for this alert rule: ActionGroup1

Alert rule name: Alert1

You create an action rule that has the following settings:

Scope: VM1

Filter criteria: Resource Type = "Virtual Machines"

Define on this scope: Suppression

Suppression config: From now (always)

Name: ActionRule1

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

If you start VM1, an alert is triggered.

If you start VM2, an alert is triggered.

If you add a tag to RG1, an alert is triggered.

Answer:

Explanation:

Statements

Yes

No

If you start VM1, an alert is triggered.

If you start VM2, an alert is triggered.

If you add a tag to RG1, an alert is triggered.

Box 1:

The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.

Box 2:

The scope for the action rule is not set to VM2.

Box 3:

Adding a tag is not an administrative operation.

Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log>

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

Question: 90

DRAG DROP

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

- Create a new workspace.
- Apply the scope configuration to the solution.
- Create a scope configuration.
- Create a computer group.
- Create a data source.

Answer Area

Empty answer boxes for the actions listed on the left.

Answer:

Explanation:

- Create a computer group.
- Create a scope configuration.
- Apply the scope configuration to the solution.

Reference:

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

Question: 91

DRAG DROP

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.

/457

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-AzureRmDiskEncryptionExtension.

Answer:**Explanation:**

Create an Anne key vault

Configure access policies for the Azure key vault

Run Set-AzureRmDiskEncryptionExtension *

Reference:

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

Question: 92

You have an Azure subscription that contains a virtual machine named VM1.

You create an Azure key vault that has the following configurations:

Name: Vault5

Region: West US

Resource group: RG1

You need to use Vault5 to enable Azure Disk Encryption on VM1. The solution must support backing

up VM1 by using Azure Backup.

/457

Which key vault settings should you configure?

- A. Access policies
- B. Secrets
- C. Keys
- D. Locks

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault>

Question: 93

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

Name	Type	Region	Resource group
Sal	Azure Storage account	East US	RG1
VM1	Azure virtual machine	East US	RG2
KV1	Azure key vault	East US 2	RG1
SQL1	Azure SQL database	East US 2	RG2

You need to ensure that you can provide VM1 with secure access to a database on SQL1 by using a contained database user.

What should you do?

- A. Enable a managed service identity on VM1.
- B. Create a secret in KV1.
- C. Configure a service endpoint on SQL1.
- D. Create a key in KV1.

Answer: A

Explanation:

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

Question: 94

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

/457

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 access keys.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

To revoke a stored access policy, you can either delete it, or rename it by changing the signed identifier. Changing the signed identifier breaks the associations between any existing signatures and the stored access policy. Deleting or renaming the stored access policy immediately effects all of the shared access signatures associated with it.

Reference:

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

Question: 95

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. security policies in Azure Security Center
- B. Azure Logic Apps
- C. an Azure Desired State Configuration (DSC) virtual machine extension
- D. Azure Advisor

Answer: C

Explanation:

Question: 96

You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table.

Name	Region	Resource group
Vault1	West Europe	RG1
Vault2	East US	RG1
Vaults	West Europe	RG2
Vault-4	East US	RG2

/457

In Sub1, you create a virtual machine that has the following configurations:

- Name: VM1
- Size: DS2v2
- Resource group: RG1
- Region: West Europe
- Operating system: Windows Server 2016

You plan to enable Azure Disk Encryption on VM1.

In which key vaults can you store the encryption key for VM1?

- A. Vault1 or Vault3 only
- B. Vault1, Vault2, Vault3, or Vault4
- C. Vault1 only
- D. Vault1 or Vault2 only

Answer: C

Explanation:

"Your key vault and VMs must be in the same subscription. Also, to ensure that encryption secrets don't cross regional boundaries, Azure Disk Encryption requires the Key Vault and the VMs to be colocated in the same region."

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

Question: 97

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

Explanation:

Question: 98

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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

You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials.

/457

You need to configure the environment to support the planned authentication.

Solution: You deploy an Azure AD Application Proxy.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.

Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:

Create Azure Virtual Network.

Create a custom DNS server in the Azure Virtual Network.

Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.

Configure forwarding between the custom DNS server and your on-premises DNS server.

Reference:

<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

Question: 99

HOTSPOT

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
User?	Group1	Disabled
user 3	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.

User2 can request to activate the Password Administrator role.

If User3 wants to activate the Password Administrator role, the user can approve their own request.

Answer:

Explanation:

7457

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)

Question: 100

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure SQL Database instance that is configured to support Azure AD authentication.

Database developers must connect to the database instance and authenticate by using their onpremises Active Directory account.

You need to ensure that developers can connect to the instance by using Microsoft SQL Server Management Studio. The solution must minimize authentication prompts.

Which authentication method should you recommend?

- A. Active Directory - Password
- B. Active Directory - Universal with MFA support
- C. SQL Server Authentication
- D. Active Directory - Integrated

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure>

Question: 101

You plan to use Azure Resource Manager templates to perform multiple deployments of identically configured Azure virtual machines. The password for the administrator account of each deployment is stored as a secret in different Azure key vaults.

You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment. The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

- A. a key vault access policy
- B. a linked template
- C. a parameters file
- D. an automation account

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter?tabs=azure-cli#reference-secrets-with-dynamic-id>

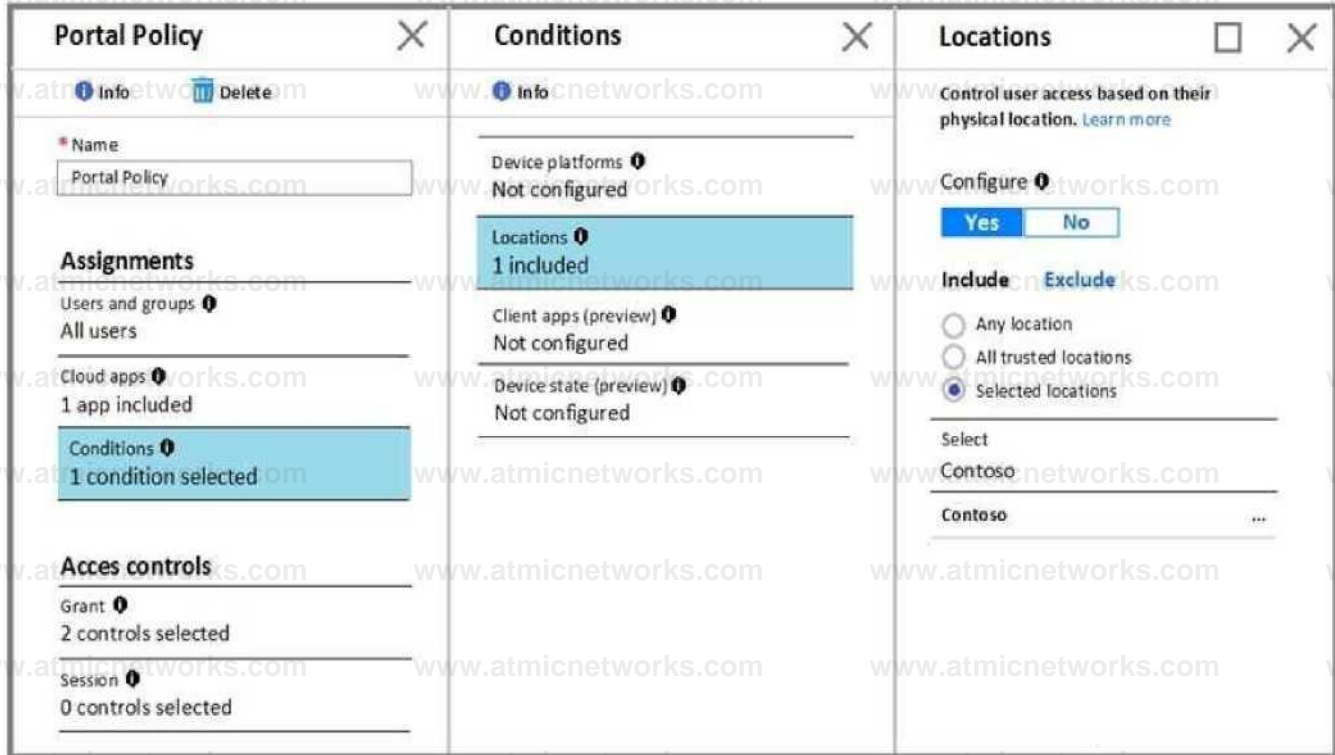
Question: 102

HOTSPOT

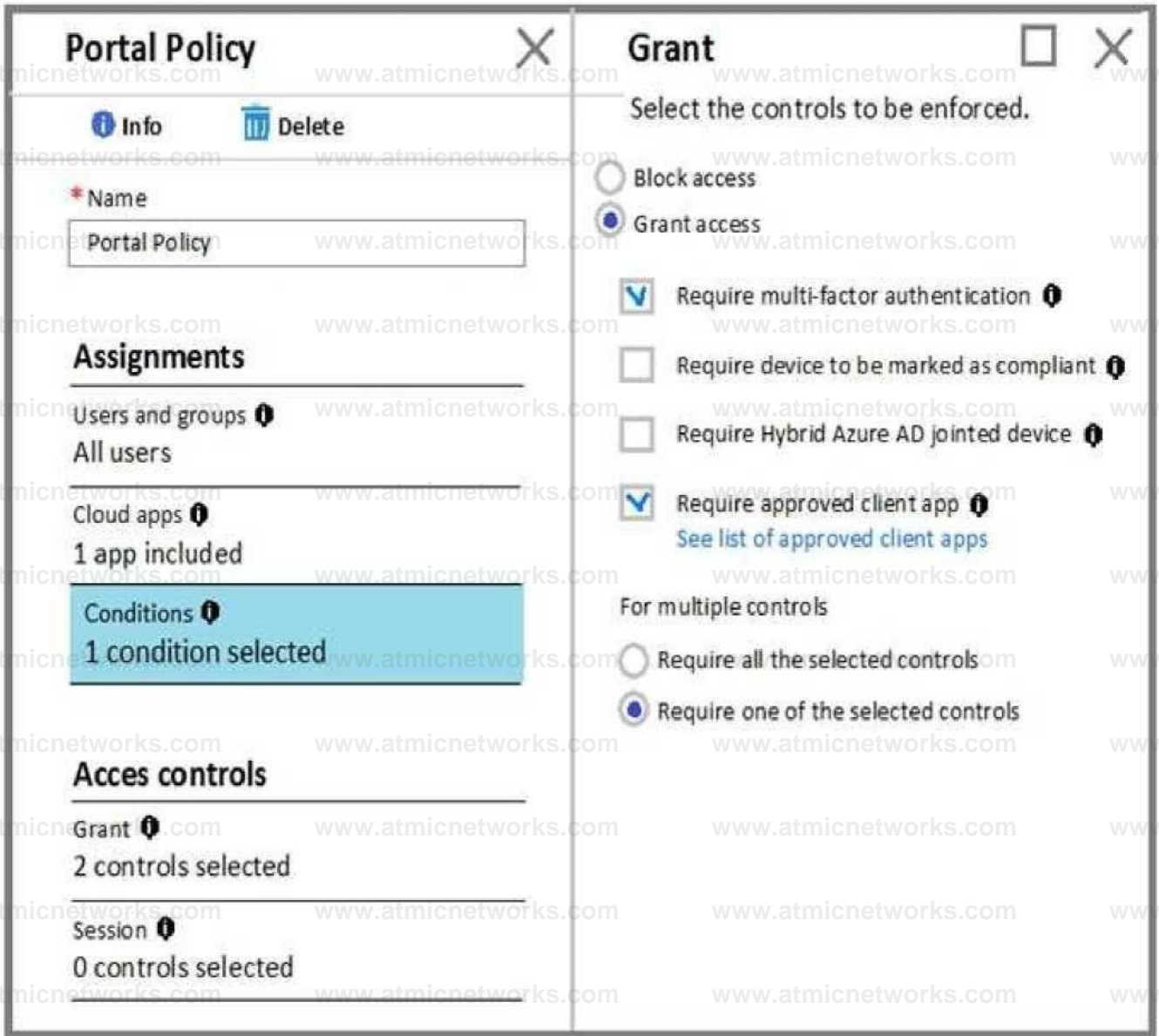
You create a new Azure subscription that is associated to a new Azure Active Directory (Azure AD) tenant.

You create one active conditional access policy named Portal Policy. Portal Policy is used to provide access to the Microsoft Azure Management cloud app.

The Conditions settings for Portal Policy are configured as shown in the Conditions exhibit. (Click the Conditions tab.)



The Grant settings for Portal Policy are configured as shown in the Grant exhibit. (Click the Grant tab.)



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
Users from the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	Q	Q
Users from the Contoso named location must use multi-factor authentication (MFA) to access the web services hosted in the Azure subscription.	Q	Q
Users external to the Contoso named location must use multi-factor authentication (MFA) to access the Azure portal.	Q	Q

Answer:

Explanation:

Box 1: No

The Contoso location is excluded

Box 2: NO

Box 3: NO

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>

Question: 103

You have an Azure subscription named Sub1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com.

An administrator named Admin1 has access to the following identities:

An OpenID-enabled user account

A Hotmail account

An account in contoso.com

An account in an Azure AD tenant named fabrikam.com

You plan to use Azure Account Center to transfer the ownership of Sub1 to Admin1.

To which accounts can you transfer the ownership of Sub1?

- A. contoso.com only
- B. contoso.com, fabrikam.com, and Hotmail only
- C. contoso.com and fabrikam.com only
- D. contoso.com, fabrikam.com, Hotmail, and OpenID-enabled user account

Answer: C

Explanation:

When you transfer billing ownership of your subscription to an account in another Azure AD tenant, you can move the subscription to the new account's tenant. If you do so, all users, groups, or service principals who had role based access (RBAC) to manage subscriptions and its resources lose their access. Only the user in the new account who accepts your transfer request will have access to **manage the resources**.

Reference:

<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer>

<https://docs.microsoft.com/en-us/azure/billing/billing-subscription-transfer#transferring-subscription-to-anaccount-in-another-azure-ad-tenant>

Question: 104

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>

Question: 105

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>

Question: 106

HOTSPOT

You have a network security group (NSG) bound to an Azure subnet.

You run Get-AzureRmNetworkSecurityRuleConfig and receive the output shown in the following exhibit.

/457

```

Name : DenyStorageAccess
Description Protocol SourcePortRange :
DestinationPortRange SourceAddressPrefix : *
DestinationAddressPrefix : {*}
SourceApplicationSecurityGroups : {*}
DestinationApplicationSecurityGroups : {*}
Access : {Storage}
Priority Direction : []
: []
: Deny 105
: Outbound
:
Name ProvisioningState Description : S storageEA2Allow
Protocol SourcePortRange : Succeeded
DestinationPortRange SourceAddressPrefix :
DestinationAddressPrefix : *
SourceApplicationSecurityGroups : {*}
DestinationApplicationSecurityGroups : {443}
Access Priority Direction : {*}
: {Storage/EastUS2}
: []
: []
: Allow 104
: Outbound
:
Name : Contoso FTP
Description Protocol SourcePortRange :
DestinationPortRange SourceAddressPrefix : TCP
DestinationAddressPrefix : {*}
SourceApplicationSecurityGroups : {21}
DestinationApplicationSecurityGroups : {1.2.3.4/32}
Access Priority Direction : {10.0.0.5/32}
: []
: []
: Allow
: 504
: Inbound

```

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

/457

NOTE: Each correct selection is worth one point.

Traffic destined for an Azure Storage account is [answer choice].

	▼
able to connect to East US	
able to connect to East US 2	
able to connect to West Europe	
prevented from connecting to all regions	

FTP connections from 1.2.3.4 to 10.0.0.10/32 are [answer choice].

	▼
allowed	
dropped	
forwarded	

Answer:

Explanation:

Box 1: able to connect to East US 2

The StorageEA2Allow has DestinationAddressPrefix {Storage/EastUS2}

Box 2: dropped

Reference:

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

Question: 107

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

Name	Region	Subnet
VNET1	West US	Subnet11 and Subnet12
VNET2	West US 2	Subnet21
VNET3	East US	Subnet31

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

Name	Network interface	Connected to
VM1	NIC1	Subnet11
VM2	NIC2	Subnet11
VM3	NIC3	Subnet12
VM4	NIC4	Subnet21
VM5	NIC5	Subnet31

On NIC1, you configure an application security group named ASG1.

On which other network interfaces can you configure ASG1?

- A. NIC2 only
- B. NIC2, NIC3, NIC4, and NIC5
- C. NIC2 and NIC3 only
- D. NIC2, NIC3, and NIC4 only

Answer: C

Explanation:

Only network interfaces in NVET1, which consists of Subnet11 and Subnet12, can be configured in ASG1, as all network interfaces assigned to an application security group have to exist in the same virtual network that the first network interface assigned to the application security group is in. Reference:

<https://azure.microsoft.com/es-es/blog/applicationsecuritygroups/>

Question: 108

You have 15 Azure virtual machines in a resource group named RG1.

All virtual machines run identical applications.

You need to prevent unauthorized applications and malware from running on the virtual machines.

What should you do?

- A. Apply an Azure policy to RG1.
- B. From Azure Security Center, configure adaptive application controls.
- C. Configure Azure Active Directory (Azure AD) Identity Protection.
- D. Apply a resource lock to RG1.

Answer: B

Explanation:

Adaptive application control is an intelligent, automated end-to-end application whitelisting solution from Azure Security Center. It helps you control which applications can run on your Azure and nonAzure VMs (Windows and Linux), which, among other benefits, helps harden your VMs against malware. Security Center uses machine learning to analyze the applications running on your VMs

and helps you apply the specific whitelisting rules using this intelligence.

Reference:

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

Question: 109

You plan to deploy Azure container instances.

You have a containerized application that validates credit cards. The application is comprised of two containers: an application container and a validation container.

The application container is monitored by the validation container. The validation container performs security checks by making requests to the application container and waiting for responses after every transaction.

You need to ensure that the application container and the validation container are scheduled to be deployed together. The containers must communicate to each other only on ports that are not externally exposed.

What should you include in the deployment?

- A. application security groups
- B. network security groups (NSGs)
- C. management groups
- D. container groups

Answer: D

Explanation:

Azure Container Instances supports the deployment of multiple containers onto a single host using a container group. A container group is useful when building an application sidecar for logging, monitoring, or any other configuration where a service needs a second attached process.

Reference:

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-container-groups>

Question: 110

HOTSPOT

You create resources in an Azure subscription as shown in the following table.

Name	Typ*	Region
RG1	Resource group	West Europe
VNET1	Azure virtual network	West Europe
ContosoI901	Azure Storage account	West Europe

VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24.

Subnet2 has a network ID of 10.1.1.0/24.

Contoso1901 is configured as shown in the exhibit. (Click the Exhibit tab.)

```
PS C:\> (Get-AzStorageAccount RG1 contoso1901).NetworkRuleSet

ByPass          : Logging, Metrics
DefaultAction   : Deny
IpRules         : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-
                    dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/
                    virtualNetworks/VNET1/subnets/Subnet1,...]
```

```
PS C:\> (Get-AzStorageAccount RG1 contoso1901).NetworkRuleSet.IpRules

Action IPAddressOrRange
Allow 193.77.0.0/16
```

```
PS C:\> (Get-AzStorageAccount RG1 contoso1901).NetworkRules

Action VirtualNetworkResourceId State
Allow /subscriptions/a90c8c8f-d8bc-4112-abfb-dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1 Succeeded

PS C:\>_
```

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
An Azure virtual machine on Subnet1 can access data in Contoso1901.	<input checked="" type="radio"/>	<input type="radio"/>
An Azure virtual machine on Subnet2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Statements

Yes

No

An Azure virtual machine on Subnet1 can access data in ContosoI901.

U

An Azure virtual machine on Subnet? can access data in ContosoI901.

A computer on the Internet that has an IP address of 193.77.10.2 can access Q data in ContosoI901.

Box 1: Yes

Access from Subnet1 is allowed.

Box 2: No

No access from Subnet2 is allowed.

Box 3: Yes

Access from IP address 193.77.10.2 is allowed.

Question: 111

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

Explanation:

Instead use a management group.

Management groups in Microsoft Azure solve the problem of needing to impose governance policy ON more than one Azure subscription simultaneously.

Reference:

<https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-managementgroups/>

Question: 112

You have an Azure subscription named Sub1 that contains the virtual machines shown in the following table.

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

You need to ensure that the virtual machines in RG1 have the Remote Desktop port closed until an authorized user requests access.

What should you configure?

- A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- B. an application security group
- C. Azure Active Directory (Azure AD) conditional access
- D. just in time (JIT) VM access

Answer: D

Explanation:

Just-in-time (JIT) virtual machine (VM) access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.

When a user requests access to a VM, Security Center checks that the user has Role-Based Access Control (RBAC) permissions that permit them to successfully request access to a VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.

Reference:

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

Question: 113

You have 10 virtual machines on a single subnet that has a single network security group (NSG).

You need to log the network traffic to an Azure Storage account.

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

NOTE: Each correct selection is worth one point.

A. Install the Network Performance Monitor solution.

B. Enable Azure Network Watcher.

C. Enable diagnostic logging for the NSG.

D. Enable NSG flow logs.

E. Create an Azure Log Analytics workspace.

Answer: D

Explanation:

A network security group (NSG) enables you to filter inbound traffic to, and outbound traffic from, a virtual machine (VM). You can log network traffic that flows through an NSG with Network Watcher's NSG flow log capability. Steps include:

Create a VM with a network security group

Enable Network Watcher and register the Microsoft.Insights provider

Enable a traffic flow log for an NSG, using Network Watcher's NSG flow log capability

Download logged data

View logged data

Reference:

<https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal>

Question: 114

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 Log Analytics 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 On, Security Center provisions the Log Analytics 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

Reference:

<https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>

Question: 115

You have an Azure subscription named Sub1 that contains the Azure key vaults shown in the following table:

Name	Region	Resource group
Vault1	West Europe	RG1
Vault2	East US	RG1
Vault3	West Europe	RG2
Vault4	East US	RG2

In Sub1, you create a virtual machine that has the following configurations:

Name: VM1

Size: DS2v2

Resource group: RG1

Region: West Europe

Operating system: Windows Server 2022

You plan to enable Azure Disk Encryption on VM1.

In which key vaults can you store the encryption key for VM1?

- A. Vault1 or Vault3 only
- B. Vault1, Vault2, Vault3, or Vault4
- C. Vault1 only

D. Vault1 or Vault2 only

Answer: A

Explanation:

In order to make sure the encryption secrets don't cross regional boundaries, Azure Disk Encryption needs the Key Vault and the VMs to be co-located in the same region. Create and use a Key Vault that is in the same region as the VM to be encrypted.

Reference:

<https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites>

Question: 116

HOTSPOT

You have an Azure subscription that contains an Azure key vault named Vault1.

On January 1, 2019, Vault1 stores the following secrets.

```
Enabled      : False
Expires
NotBefore   : 5/1/19 12:00:00 AM
Created     : 12/20/18 2:55:00 PM
Updated    : 12/20/18 2:55:00 PM
ContentType
Tags
TagTable
VaultName   : vault1
Name        : password1
Version Id  : https://vault1.vault.azure.net:443/secrets/Password1

Enabled     : True
Expires    : 5/1/19 12:00:00 AM
NotBefore  : 3/1/19 12:00:00 AM
Created    : 12/20/18 3:00:00 PM
Updated    : 12/20/18 3:00:00 PM
ContentType
Tags       •
TagTable
VaultName  : vault1
Name       : Password2
Version Id : https://vault1.vault.azure.net:443/secrets/Password2
```

Which can each secret be used by an application? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Password1:

	▼
Never	
Always	
Only after May 1, 2019	

Password2:

	▼
Never	
Always	
Only between March 1, 2019 and May 1, 2019	

Answer:

Explanation:

Password1:

	▼
Never	
Always	
Only after May 1, 2019	

Password2:

	▼
Never	
Always	
Only between March 1, 2019 and May 1, 2019	

Box 1: Never
Password1 is disabled.

Box 2: Only between March 1, 2019 and May 1,

Password2:

Expires : 5/1/19 12:00:00 AM
NotBefore : 3/1/19 12:00:00 AM

Reference: <https://docs.microsoft.com/en-us/powershell/module/azurermskeyvault/set-azurekeyvaultsecretattribute>

Question: 117

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

Explanation:

To use Azure Repos, make sure your Azure DevOps organization is linked to your Azure subscription.

Reference:

<https://docs.microsoft.com/en-us/azure/app-service/deploy-continuous-deployment>

Question: 118

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 an initiative and an assignment that is scoped to a management group.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

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

Question: 119

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. the Security & Compliance admin center
- B. SQL query editor in Azure
- C. File Explorer in Windows
- D. AzCopy

Answer: D

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/storage-analytics-logging?toc=%2fazure%2fstorage%2fblobs%2ftoc.json>

Question: 120

HOTSPOT

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

Answer:

Explanation:

1. Read permission
2. 5986

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

Question: 121

HOTSPOT

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

Name	Type	Region	Resource group
SOLI	Azure SQL database	East US	RG1
AnalyticsI	Azure Log Analytics workspace	East US	RG1
Analytics?	Azure Log Analytics workspace	East US	RG2
Analytics;	Azure Log Analytics workspace	West Europe	RG1

You create the Azure Storage accounts shown in the following table.

Name	Region	Resource group	Storage account type	Access tier (default)
Storage!	East US	RG1	Blob	Cool
Storage?	East US	RG2	General purpose V1	Not applicable
Storage^	West Europe	RG1	General purpose V2	Hot

You need to configure auditing for SQL1.

Which storage accounts and Log Analytics workspaces can you use as the audit log destination? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Storage accounts that can be used as the audit log destination:

- Storage! only
- Storage? only
- Storage! and Storage? only
- Storage!, Storage?, and Storage^

Log Analytics workspaces that can be used as the audit log destination:

- Analytics I only
- Analytics I and Analytics? only
- Analytics I and Analytics? only
- Analytics I, Analytics?, and Analytics?

Answer:

Explanation:

Storage accounts that can be used as the audit log destination:

- Storageonly
- Storage2 only
- Storage and Storage? only
- Storage, Storage?, and Storage3

Log Analytics workspaces that can be used as the audit log destination:

- Analytics only
- Analytics and Analytics? only
- Analytics and Analytics3 only
- Analytics, Analytics?, and Analytics3

Question: 122

HOTSPOT

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 Share1 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:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer

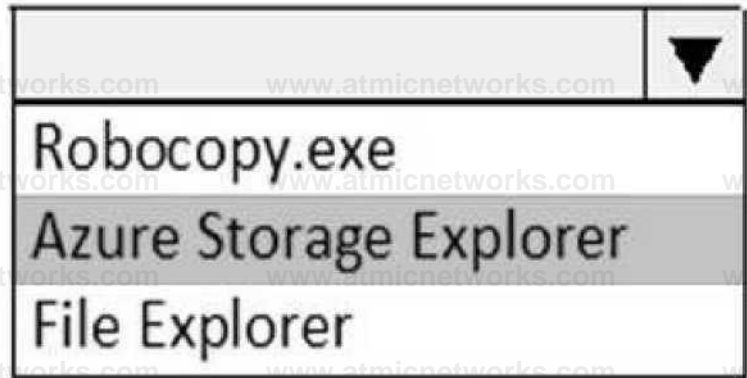
Tools for Share1:

- Robocopy.exe
- Azure Storage Explorer
- File Explorer

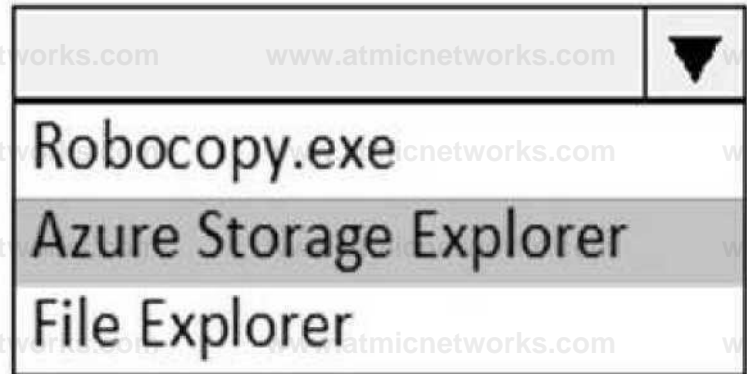
Answer:

Explanation:

Tools for Container1:



Tools for Share1:



Question: 123

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:

Reference:

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

Question: 124

HOTSPOT

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"/> |

Answer:

Explanation:

Answer Area*

Statements

Yea No

User1 can access Appl from an IP address of 154.12.18.34

User1 can access Appl from an IP address of 193.77.10.15.

User1 can access Appl from an IP address of 154.12.18.34

Question: 125

DRAG DROP

You are configuring network connectivity for two Azure virtual networks named VNET1 and VNET2.

You need to implement VPN gateways for the virtual networks to meet the following requirements: * 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.

Which VPN gateway SKU should you use for each virtual network? To answer, drag the appropriate SKUs to the correct networks.

Each SKU 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

Answer Area

Answer

Explanation:

VNET1

VpnGwl

VNET2

VpnGwl

Reference:

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

Question: 126

You are securing access to the resources in an Azure subscription.

A new company policy states that all the Azure virtual machines in the subscription must use managed disks.

You need to prevent users from creating virtual machines that use unmanaged disks. What should you use?

- A. Azure Monitor
- B. Azure Policy
- C. Azure Security Center
- D. Azure Service Health

Answer: B

Explanation:

Question: 127

HOTSPOT

You have an Azure subscription named Sub 1 that is associated to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Global administrator
User2	Security administrator
User3	Security reader
User4	License administrator

Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD Identity Protection.

Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

- Users who can onboard Azure AD Identity Protection:
- User1 only
 - User1 and User2 only
 - User1, User 2, and User3 only
 - User1, User 2 Users, and User 4 only
- Users who can remediate users and configure policies:
- User1 and User2 only
 - User1 and Users only
 - User1, User 2 and Users only
 - User1, User 2 Users, and User4

Answer

Explanation:

Users who can onboard Azure AD Identity Protection:

User1 only	
User1 and User2 only	
User1, User2, and User3 only	
User1, User2, User3, and User4 only	

Users who can remediate users and configure policies:

User1 and User2 only	
User1 and User3 only	
User1, User2, and User3 only	
User1, User2, User3, and User4	

Question: 128
HOTSPOT

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.		
From VM1, you can successfully ping the private IP address of VM3.	<input type="radio"/>	
From VM1, you can successfully ping the private IP address of VM5.		

Answer:

Explanation:

- Q1: No { and it should not be allowed as only TCP 80 is allowed from the "Internet" service tag
- Q2: Yes {as it should be for VMs in the same local subnet pinging each other on private IP and no NSG configured}
- Q3: Yes {VM5 is in subnet where 1st rule of NSG allows any traffic from any source to the destination}

Question: 129

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: C,D

Explanation:

Reference:

<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>

Question: 130

DRAG DROP

You have an Azure subscription that contains the following resources:

A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.

A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

You need to ensure that Remote Desktop connections can be established to VM1 from the internet.

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

- Configure a network security group (NSG).
- Create a network rule collection.
- Create a NAT rule collection.
- Create a new subnet.
- Deploy Azure Application Gateway.
- Deploy Azure Firewall.

Answer Area

Three empty rectangular boxes for the answer area.

Answer:

Explanation:

Create a new subnet.

Deploy Azure Firewall.

Create a NAT rule collection.

Question: 131

DRAG DROP

You have an Azure subscription named Sub1.

You have an Azure Active Directory (Azure AD) group named Group1 that contains all the members of your IT team.

You need to ensure that the members of Group1 can stop, start, and restart the Azure virtual machines in Sub1. The solution must use the principle of least privilege.

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

Create a JSON file.

Run the Update-AzureRmManagementGroup cmdlet.

Create an XML file.

Run the New-AzureRmRoleDefinition cmdlet.

Run the New-AzureRmRoleAssignment cmdlet.

Answer Area

Three empty rectangular boxes for the answer area.

Answer:

Explanation:

Create a JSON file.

Run the `New-AzureRmRoleDefinition` cmdlet.

Run the `New-AzureRmRoleAssignment` cmdlet.

Reference:

<https://www.petri.com/cloud-security-create-custom-rbac-role-microsoft-azure>

Question: 132

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

Name	Operating system	State
VM1	Windows Server 2008 R2 Service Pack 1 (SP1)	Running
VM2	Windows Server 2012R2	Running
VM3	Windows Server 2016	Stopped
VM4	Ubuntu Server 18.04 LTS	Running

For which virtual machine can you enable Update Management?

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

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/automation/automation-update-management?toc=%2Fazure%2Fautomation%2Ftoc.json>

Question: 133

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.

You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.

What should you create?

- A. a secret in Azure Key Vault
- B. a role assignment
- C. an Azure Active Directory (Azure AD) user
- D. an Azure Active Directory (Azure AD) group

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/aks/kubernetes-service-principal>

Question: 134

Your company has an Azure Active Directory (Azure AD) tenant named contoso.com.

You plan to create several security alerts by using Azure Monitor.

You need to prepare the Azure subscription for the alerts.

What should you create first?

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

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/learn/quick-create-workspace>

Question: 135

Your company has an Azure subscription named Sub1. Sub1 contains an Azure web app named WebApp1 that uses Azure Application Insights. WebApp1 requires users to authenticate by using OAuth 2.0 client secrets.

Developers at the company plan to create a multi-step web test app that performs synthetic transactions emulating user traffic to Web App1.

You need to ensure that web tests can run unattended.

What should you do first?

- A. In Microsoft Visual Studio, modify the .webtest file.
- B. Upload the .webtest file to Application Insights.
- C. Register the web test app in Azure AD.
- D. Add a plug-in to the web test app.

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/app/availability-multistep>

Question: 136

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.

Reference:

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

Question: 137

HOTSPOT

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

Name	Type
User1	Azure Active Directory (Azure AD) user
User2	Azure Active Directory (Azure AD) user
Group1	Azure Active Directory (Azure AD) group
Vault1	Azure key vault

User1 is a member of Group1. Group1 and User2 are assigned the Key Vault Contributor role for Vault1.

On January 1, 2019, you create a secret in Vault1. The secret is configured as shown in the exhibit. (Click the Exhibit tab.)

Create a secret

Upload options

Manual

Name ⓘ

Password1

Value

••••••••

Content type (optional)

Set activation date? Yes No

Activation Date

2019 03 01 R 12 00 00 AM

(UTC+00:00) -- Current Time Zone —

Set expiration date? No Yes

Expiration Date

2020 03 01 12 00 00 AM

(UTC+00:00) -- Current Time Zone —

Enabled?

No

User2 is assigned an access policy to Vault1. The policy has the following configurations:

Key Management Operations: Get, List, and Restore

Cryptographic Operations: Decrypt and Unwrap Key

Secret Management Operations: Get, List, and Restore

Group1 is assigned an access to Vault1. The policy has the following configurations:

Key Management Operations: Get and Recover

Secret Management Operations: List, Backup, and Recover

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

Statements

Yes No

On January 1, 2019, User1 can view the value of Password.

On June 1, 2019, User2 can view the value of Password.

Q

On June 1, 2019, User1 can view the value of Password.

Q

Answer:

Explanation:

Statements

Yes

No

On January 1, 2019, User1 can view the value of Password1.

On June 1, 2019, User2 can view the value of Password1.

On June 1, 2019, User1 can view the value of Password1.

Question: 138

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso1812.onmicrosoft.com that contains the users shown in the following table.

Name	Username	Type
User1	User1@contoso1812.onmicrosoft.com	Member
User?	User2@contoso1812.onmicrosoft.com	Member
User3	User3@contoso1812.onmicrosoft.com	Member
User4	User4@oirtlook.com	Guest

You create an Azure Information Protection label named Label1. The Protection settings for Label1 are configured as shown in the exhibit. (Click the Exhibit tab.)

Protection

Contoso1812 - Azure Information Protection

Protections settings ⓘ

Azure (cloud key) **HYOK (AD RMS)**

Select the protection action type ⓘ

- Set permissions
- Set user-defined permissions (Preview)

USERS

PERMISSIONS

AuthenticatedUsers

Viewer

User1@contoso1812.onmicrosoft.com

Co-Author

User2@contoso1812.onmicrosoft.com

Reviewer

[+Add permissions](#)

Label1 is applied to a file named File1.

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 print File.

Q

Q)

User3 can read File.

Q

O

User4 can print File.

Q

Q

Explanation:

Answer:

Statements

Yes

No

User1 can print File1.

User3 can read File1.

User4 can print File1.

Question: 139

HOTSPOT

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

Name	Member of
User1	Group1
User 2	Group?
User 3	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

Allow permanent eligible assignment Expire eligible assignments after

3 Months

Allow permanent active assignment

Expire active assignments after t 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

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.

If User2 activates the Security Administrator role, the user Q will be assigned the role immediately.

User3 can activate the Security Administrator role. O

Answer:

Explanation:

Statements

Yes

No

User1 can only activate the Security Administrator role in five hours.

I

|

If User2 activates the Security Administrator role, the user Q will be assigned the role immediately.

Q

User3 can activate the Security Administrator role. Q

Q

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-configure-role-settings>

Question: 140

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

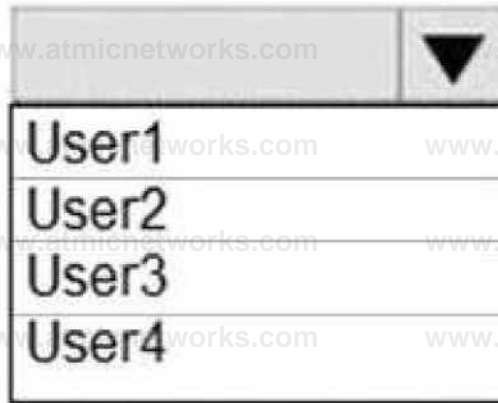
The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

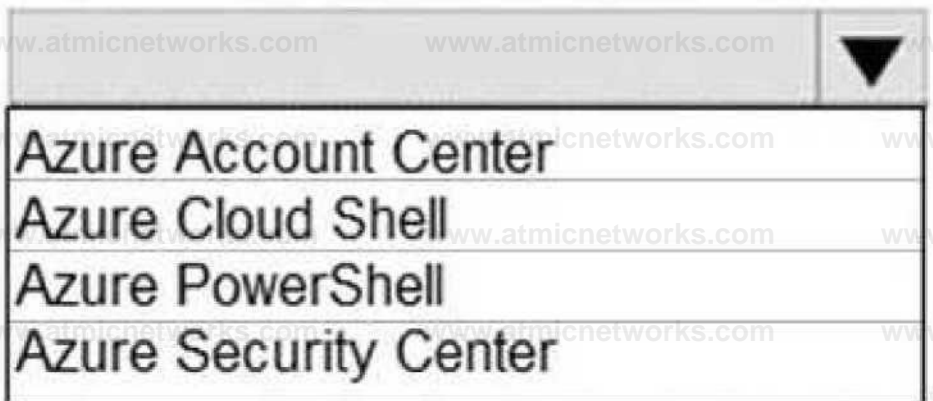
Which user can transfer the ownership and which tool should the user use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

User:



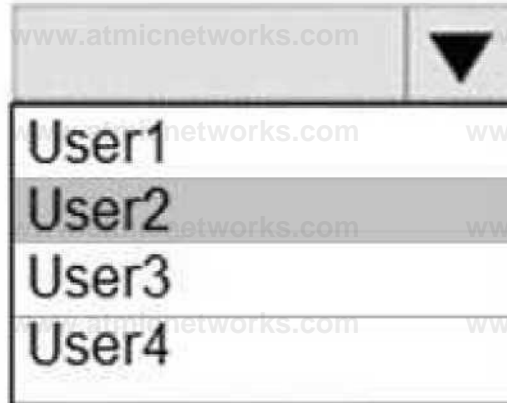
Tool:



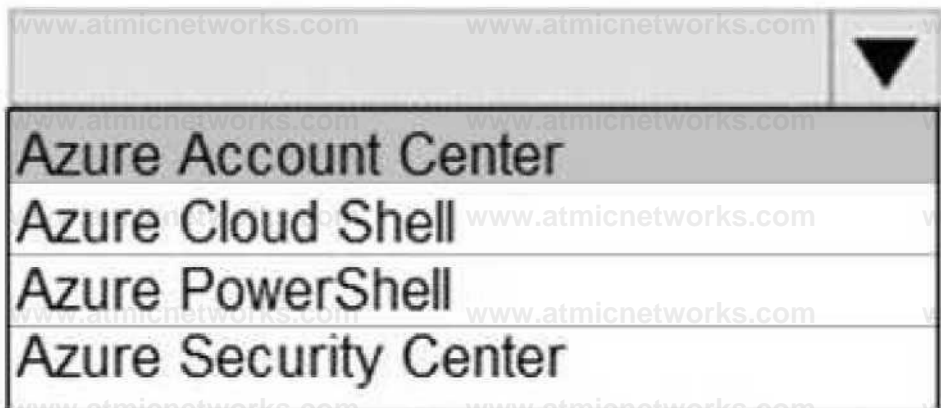
Answer:

Explanation:

User:



Tool:



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-azure-subscription>

Question: 141

You have an Azure Container Registry named ContReg1 that contains a container image named image1.

You enable content trust for ContReg1.

After content trust is enabled, you push two images to ContReg1 as shown in the following table.

Name	Details
image2	Image was pushed with client content trust enabled.
image3	Image was pushed with client content trust disabled.

Which images are trusted images?

- A. image1 and image2 only
- B. image2 only
- C. image1, image2, and image3

Answer: B

Explanation:

Azure Container Registry implements Docker's content trust model, enabling pushing and pulling of signed images.

To push a trusted image tag to your container registry, enable content trust and push the image with docker push.

To work with trusted images, both image publishers and consumers need to enable content trust for their Docker clients. As a publisher, you can sign the images you push to a content trust-enabled registry.

Reference:

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

Question: 142

HOTSPOT

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	Group 1, Group2	Enabled
User2	Group 1	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	

Answer:

Explanation:

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	

Reference:

[http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-](http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/)

[access-policies/](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>

Question: 143

HOTSPOT

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)



Require Multi-Factor Authentication on activation

Require justification on activation

Require ticket information on activation

Require approval to activate

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

On May 15,2019, User2 can use the Contributor role.

On June 15,2019, User3 can activate the Contributor role.

Answer:

Explanation:

Statements

Yes

No

On May 15,2019, User1 can activate the Contributor role

On May 15,2019, User2 can use the Contributor role.

On June 15,2019, User3 can activate the Contributor role.

Reference:

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

Question: 144
HOTSPOT

You have an Azure subscription that contains the alerts shown in the following exhibit.

All Alerts

+ New alert rule | Edit columns | Manage alert rules | View classic alerts | Refresh | Change state

Don't see a subscription? Open Directory + Subscription settings

Subscription: Azure Pass - Sponsorship | Resource group: Type to start filtering... | Resource Type: 0 selected | Resource: Type to start filtering... | Time range: Past hour

Monitor service: 15 selected | Monitor condition: 2 selected | Severity: Sev 4 | Alert state: 3 selected | Smart group id: Smart group id

All Alerts | Alerts By Smart Group (Preview)

KAMI	OWMIY	MONITOR C_	AUM CW1	AIICI..	MONITOR MRV.	siGNAi net	RODIM	W_
Alert1	I Sev4	A Hud	New		Activitylog Ad	L^	6/6/2019, 11^23:53 ..	Azure...
Alert1	I Sev4	A Fired	Acknowledged		Activitylog Ad	io«	6/6/2019.11:23:52..	Azure...
Alert?	I Sev4	A Fired	Acknowledged		Activitylog Ad-	log	6/6/2019.11:23:25..	Azure...
Alert?	I Sev4	A Fired	Closed		Activitylog Ad	Log	6/6/2019.11 23:24 ...	Azure...

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

NOTE: Each correct selection is worth one point.

The state of Alert1 that was fired at 11:23:52

▼

- cannot be changed
- can be changed to Closed only
- can be changed to New only
- can be changed to New or Closed

The state of Alert2 that was fired at 11:23:24

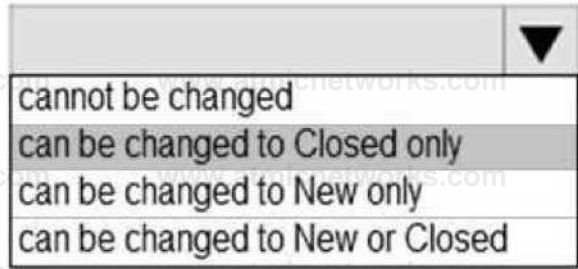
▼

- cannot be changed
- can be changed to Acknowledged only
- can be changed to New only
- can be changed to New or Acknowledged

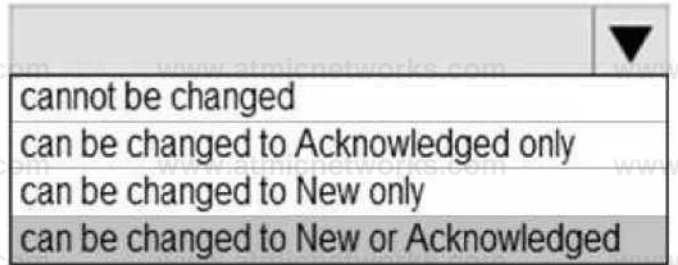
Answer:

Explanation:

The state of Alert1 that was fired at 11:23:52



The state of Alert2 that was fired at 11:23:24



Reference:

<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-overview>

Question: 145

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

Reference:

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

<https://docs.microsoft.com/en-us/azure/storage/common/storage-explorers>

Question: 146

You have a web app named WebApp1.

You create a web application firewall (WAF) policy named WAF1.

You need to protect WebApp1 by using WAF1.

What should you do first?

- A. Deploy an Azure Front Door.
- B. Add an extension to WebApp1.
- C. Deploy Azure Firewall.

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/frontdoor/quickstart-create-front-door>

Question: 147

HOTSPOT

You work at a company named Contoso, Ltd. that has the offices shown in the following table.

Name	IP address space
Boston	180.15.10.0/24
Seattle	132.32.15.0/24

Contoso has an Azure Active Directory (Azure AD) tenant named contoso.com. All contoso.com users have Azure Multi-Factor Authentication (MFA) enabled. The tenant contains the users shown in the following table.

Name	User device	Last sign-in	During last sign-in, user selected Don't ask again for 14 days
User1	Device1	June 1	Yes
User2	Device?	June 3	No

The multi-factor settings for contoso.com are configured as shown in the following exhibit.

multi-factor authentication

users service settings

app passwords [\(learn more\)](#)

- Allow users to create app passwords to sign in to non-browser apps

Do not allow users to create app passwords to sign in to non-browser apps

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

Skip multi-factor authentication for requests from federated users on my intranet Skip multi-factor authentication for requests from following range of IP address subnets

180.15.10.0/24

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

Methods available to users:

call to phone

Text message to phone

Notification through mobile app

Verification code from mobile app or hardware token

remember multi-factor authentication [\(learn more\)](#)

Allow users to remember multi-factor authentication on devices they trust Davs before a device must re-authenticate (1-60): 14

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 to Device1 from the Seattle office on June 10, the user will be prompted for MFA.	<input type="radio"/>
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA.	<input type="radio"/>
When User1 signs in to to a new device from the Seattle office on June 7, the user will be prompted for MFA.	<input type="radio"/>

Answer:

Explanation:

Answer Area

Statements	Yes No
When User1 signs in to Device1 from the Seattle office on June 10 the user will be prompted for MFA	<input checked="" type="radio"/>
When User2 signs in to Device2 from the Boston office on June 5, the user will be prompted for MFA	<input type="radio"/>
When User1 signs in to a new device from the Seattle office on June 7 the user will be prompted for MFA	<input checked="" type="radio"/>

Question: 148

You have an Azure subscription.

You configure the subscription to use a different Azure Active Directory (Azure AD) tenant.

What are two possible effects of the change? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Role assignments at the subscription level are lost.
- B. Virtual machine managed identities are lost.
- C. Virtual machine disk snapshots are lost.
- D. Existing Azure resources are deleted.

Answer: A,B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory>

Question: 149

You have an Azure subscription that contains virtual machines.

You enable just in time (JIT) VM access to all the virtual machines.

You need to connect to a virtual machine by using Remote Desktop.

What should you do first?

- A. From Azure Directory (Azure AD) Privileged Identity Management (PIM), activate the Security administrator user role.
- B. From Azure Active Directory (Azure AD) Privileged Identity Management (PIM), activate the Owner role for the virtual machine.
- C. From the Azure portal, select the virtual machine, select Connect, and then select Request access.
- D. From the Azure portal, select the virtual machine and add the Network Watcher Agent virtual machineextension.

Answer: C

Explanation:

Reference:

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

Question: 150

HOTSPOT

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"/>

Answer:

Explanation:

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"/>

Question: 151

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

Name	Operating system
VM1	Windows 10
VM2	Windows Server 2016
VM3	Windows Server 2019
VM4	Ubuntu Server 18.04 LTS

You create an MDM Security Baseline profile named Profile1.

You need to identify to which virtual machines Profile1 can be applied.

Which virtual machines should you identify?

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

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/mem/intune/protect/security-baselines>

Question: 152

HOTSPOT

You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

Name	Private IP address	Public IP address	Connected to
VM1	10.7.0.4	51.144.245.152	VNET1/Default
VM2	10.8.0.4	104.45.9.227	VNET2/Default

You set the Key Vault access policy to Enable access to Azure Disk Encryption for volume encryption.

KeyVault1 is configured as shown in the following exhibit.

01 Save X Discard

Allow access from:

All networks • Selected networks

0 Configure network access control for your key vault. Learn More

Virtual networks: 0

+ Add existing virtual networks + Add new virtual network

VIRTUAL NETWORK

SUBNET

RESOURCE GROUP

SUBSCRIPTION

VNET1

default

RG1

...

Firewall: 0

IPv4 ADDRESS OR CIDR

IPv4 address or CIDR

Exception:

Allow trusted Microsoft services to bypass this

• Yes No

firewall? 0

0 This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

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, users can manage the keys and secrets stored in KeyVault1.

From VM2, users can manage the keys and secrets stored in KeyVault1.

VM2 can use KeyVault for Azure Disk Encryption

Answer:

Explanation:

Answer AIM Statamants

Yet No

Hom VM1, users can manage the keys and secrets stored in Key Vault 1

from VM2 users can manage the keys and secrets stored in Key Vault 1

VM2 can use Key Vault! for Acute Disk Encryption.

Question: 153
HOTSPOT

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

Name	Resource group	Status
VM1	RG1	Stopped (Deallocated)
VM2	RG2	Stopped (Deallocated)

You create the Azure policies shown in the following table.

Policy definition	Resource type	Scope
Not allowed resource types	virtualMachines	RG1
Allowed resource types	virtualMachines	RG2

You create the resource locks shown in the following table.

Name	Type	Created on
Lock1	Read-only	VM1
Lock2	Read-only	RG2

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

NOTE: Each correct selection is worth one point.

Statements

Yes

No

You can start VM1.

You can start VM2.

You can create a virtual machine in RG2.

Answer:

Explanation:

NO
NO
NO

1 .) cannot perform write operation because following scope(s) are locked:
'subscriptions/xxxx/resourceGroups/xxx' Please remove the lock and try again.

2 .) When creating a VM in a resource group with a Read Only lock an error is shown:
"The selected resource group is read only"

3 .) Because of the read only lock virtual machines cannot be started nor stopped when the lock is added after the machine started. (not part of this use case, but still good to know.

The article referenced in the answer states different because that is scoped to blueprints.
In the Lock Resources pages is states the following regarding starting VMs:

"A ReadOnly lock on a resource group that contains a virtual machine prevents all users from starting or restarting the virtual machine. These operations require a POST request."

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

Question: 154

HOTSPOT

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
UserB	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 create virtual networks in RG1:

▼

Used only

Used and User2 only

Used and User3 only

Used, User2 and User3 only

User1, User2, User3, and User4

Users who can modify the permissions for RG1:

Used only

Used and User2 only

User1 and User3 only

Used, User2 and User3 only

Used, User2, User3, and User4

Answer:

Explanation:

Users who can modify the permissions for RG1:

A dropdown menu with a downward arrow in the top right corner. The menu is open, showing five options. The first option, 'User1 only', is highlighted with a grey background. The other options are 'User1 and User2 only', 'User1 and User3 only', 'User1, User2 and User3 only', and 'User1, User2, User3, and User4'.

Users who can create virtual networks in RG1:

A dropdown menu with a downward arrow in the top right corner. The menu is open, showing five options. The second option, 'User1 and User2 only', is highlighted with a grey background. The other options are 'User1 only', 'User1 and User3 only', 'User1, User2 and User3 only', and 'User1, User2, User3, and User4'.

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.

Question: 155

You have an Azure virtual machine named VM1.

From Azure Security Center, you get the following high-severity recommendation: "Install endpoint protection solutions on virtual machine".

You need to resolve the issue causing the high-severity recommendation.

What should you do?

- A. Add the Microsoft Antimalware extension to VM1.
- B. Install Microsoft System Center Security Management Pack for Endpoint Protection on VM1.
- C. Add the Network Watcher Agent for Windows extension to VM1.
- D. Onboard VM1 to Microsoft Defender Advanced Threat Protection (Microsoft Defender ATP).

Answer: A

Explanation:

Reference:

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

Question: 156

HOTSPOT

You have a file named File1.yaml that contains the following contents.

```
apiVersion: 2018-10-01 location: eastus name: containergroup1
properties:
```

containers:

■ name: container!

properties: environmentvariables:

- name: 'Variable!' value: 'Value!'

- name: 'Variable?' secureValue: 'Value?' image: nginx ports:

[] resources:

requests: cpu: 1.0 memoryInGB: 1.5 osType: Linux

restartPolicy: Always tags: null

type: Microsoft.ContainerInstance/containerGroups

You create an Azure container instance named container1 by using File1.yaml.

You need to identify where you can access the values of Variable1 and Variable2.

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

NOTE: Each correct selection is worth one point.

Variable1:

	▼
Cannot be accessed	
Can be accessed from the Azure portal only	
Can be accessed from inside container1 only	
Can be accessed from inside container1 and the Azure portal	

Variable2:

	▼
Cannot be accessed	
Can be accessed from the Azure portal only	
Can be accessed from inside container1 only	
Can be accessed from inside container1 and the Azure portal	

Answer:

Explanation:

Variable1:

	▼
Cannot be accessed	
Can be accessed from the Azure portal only	
Can be accessed from inside container1 only	
Can be accessed from inside container1 and the Azure portal	

Variable2:

	▼
Cannot be accessed	
Can be accessed from the Azure portal only	
Can be accessed from inside container1 only	
Can be accessed from inside container1 and the Azure portal	

Reference:

<https://docs.microsoft.com/en-us/azure/container-instances/container-instances-environment-variables>

Question: 157

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	
Subnet2	Yes 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>

Question: 158

HOTSPOT

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

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.4	13.80.73.87
VM2	VNET2/Subnet2	10.2.1.4	213.199.133.190
VMS	VNET2/Subnet2	10.2.1.5	<i>None</i>

Subnet1 and Subnet2 have a Microsoft.Storage service endpoint configured.

You have an Azure Storage account named storageacc1 that is configured as shown in the following exhibit.

R X 0 Refresh

Allow access from
All networks • Selected networks

Configure network security for your storage accounts. | [ir](#) | [H](#)®

Virtual networks

Secure your storage account with virtual networks. - : virtual nnwfk
[+ Add new virtual network](#)

VIRTUAL SUBNET ADDRESS ENDPOINT RESOURCE SUBSCRIPTION NETWORK RANGE STATUS GROUP

No network selected.

Firewall

Add IP ranges to allow access from the internet on your on-premises networks, [earn more.](#)

Address Range

13.80.73.87
| IP address or CIDR

Exceptions

- Allow trusted Microsoft services to access this storage account 0
- Allow read access to storage logging from any network
- Allow read access to storage metrics from any network

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

Statements	Yes	No
From VM1, you can upload a blob to storageacd.	0	0
From VM2r, you can upload a blob to storageacd.	0	0
From VMS, you can upload a blob to storageacd.	0	0

Answer:

Explanation:

Statements

Yes No

From VM1, you can upload a blob to storageacc. 0 0

From VM2, you can upload a blob to storageacc. 0 0

From VMS, you can upload a blob to storageacc. 0 0

Box 1: Yes

The public IP of VM1 is allowed through the firewall.

Box 2: No

The allowed virtual network list is empty so VM2 cannot access storageacc1 directly. The public IP address of VM2 is not in the allowed IP list so VM2 cannot access storageacc1 over the Internet.

Box 3: No

The allowed virtual network list is empty so VM3 cannot access storageacc1 directly. VM3 does not have a public IP address so it cannot access storageacc1 over the Internet.

Reference:

<https://docs.microsoft.com/en-gb/azure/storage/common/storage-network-security>

Question: 159

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>

Question: 160

HOTSPOT

You have the Azure key vaults shown in the following table.

Name	Location	Azure subscription name
KV1	West US	Subscription!
KV2	West US	Subscription!
KV3	East US	Subscription!
KV4	West US	Subscription?
KV5	East US	Subscription?

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.

You back up Secret1 and Key1.

To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

You can restore the Secret1 backup to:

	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	
	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	

You can restore the Key1 backup to:

Answer:

Explanation:

You can restore the Secret1 backup to:

	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	

You can restore the Key1 backup to:

	▼
KV1 only	
KV1 and KV2 only	
KV1, KV2 and KV3 only	
KV1, KV2 and KV4 only	
KV1, KV2, KV3, KV4, and KV5	

The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.

<https://docs.microsoft.com/en-us/azure/key-vault/general/backup?tabs=azure-cli>

Question: 161

You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center. You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort. What should you create?

- A. an alert rule
- B. a playbook
- C. a function app
- D. a runbook

Answer: B

Explanation:

Question: 162

You have an Azure subscription named Subscription1. You deploy a Linux virtual machine named VM1 to Subscription1.

You need to monitor the metrics and the logs of VM1. D18912E1457D5D1DDCBD40AB3BF70D5D

What should you use?

- A. the AzurePerformanceDiagnostics extension
- B. Azure HDInsight
- C. Linux Diagnostic Extension (LAD) 3.0
- D. Azure Analysis Services

Answer: A

Explanation:

Question: 163

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

The User administrator role is assigned to a user named Admin1.

An external partner has a Microsoft account that uses the user1@outlook.com sign in.

Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: "Unable to invite user user1@outlook.com Generic authorization exception."

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant. What should you do?

- A. From the Roles and administrators blade, assign the Security administrator role to Admin1.
- B. From the Organizational relationships blade, add an identity provider.
- C. From the Custom domain names blade, add a custom domain.
- D. From the Users blade, modify the External collaboration settings.

Answer: D

Explanation:

You need to allow guest invitations in the External collaboration settings.

Question: 164

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: B,C

Explanation:

Question: 165

You have an Azure subscription that contains a resource group named RG1 and a security group serverless RG1 contains 10 virtual machine, a virtual network VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.

You need to ensure that NSG1 only RDP connections to the virtual for a maximum of 60 minutes when a member of ServerAdmins requests access.

What should you configure?

- A. an Azure Active Directory (Azure AD) Privileged identity Management (PIM) role assignment.
- B. a just in time (JIT) VM access policy in Azure Security Center
- C. an azure policy assigned to RG1.
- D. an Azure Bastion host on VNET1.

Answer: B

Explanation:

Reference:

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

Question: 166

HOTSPOT

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	Not applicable
NSG2	Network security group (NSG)	Subnet1	Not applicable
Subnet1	Subnet	Not applicable	Not applicable
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

X

T Add In! Sa^{ve} X 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	<input checked="" type="radio"/> Allow
1000	SecurityCenter-JITRule_341...	3389	Any	Any	10.1.0.4	<input type="radio"/> Deny
1001	RDP	3389	TCP	Any	Any	<input checked="" type="radio"/> Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	<input checked="" type="radio"/> Allow
65001	AllowAzureLoadBalancerin...	Any	Any	AzureLoad Balancer	Any	<input checked="" type="radio"/> Allow
65500	DenyAllInBound	Any	Any	Any	Any	<input type="radio"/> 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"/>

Answer:

Explanation:

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"/>

Question: 167

DRAG DROP

You have five Azure subscriptions linked to a single Azure Active Directory (Azure AD) tenant.

You create an Azure Policy initiative named SecurityPolicyInitiative1.

You identify which standard role assignments must be configured on all new resource groups.

You need to enforce SecurityPolicyInitiative1 and the role assignments when a new resource group is created.

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

- Publish an Azure Blueprints version
- Assign an Azure blueprint.
- Create a policy assignment.
- Create a custom role-based access control (RBAC) role.
- Create a dedicated management subscription.
- Create an Azure Blueprints definition.
- Create an initiative assignment.



Answer:

Explanation:

- Create an Azure Blueprints definition.
- Publish an Azure Blueprints version
- Assign an Azure blueprint.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/create-blueprint-portal>

<https://docs.microsoft.com/en-us/azure/azure-australia/azure-policy>

Question: 168

You have an Azure subscription that contains an Azure key vault and an Azure Storage account. The key vault contains customer-managed keys. The storage account is configured to use the customer-managed keys stored in the key vault.

You plan to store data in Azure by using the following services:

- * Azure Files
- * Azure Blob storage
- * Azure Log Analytics
- * Azure Table storage
- * Azure Queue storage

Which two services data encryption by using the keys stored in the key vault? Each correct answer present a complete solution.

NOTE: Each correct selection is worth one point.

- A. Queue storage
- B. Table storage
- C. Azure Files
- D. Blob storage

Answer: C,D

Explanation:

<https://docs.microsoft.com/en-us/azure/storage/common/account-encryption-key- create?tabs=portal>

Question: 169

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>

Question: 170

HOTSPOT

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

Name	Type
Item1	Key

Item2	Secret
Policy!	Access policy

In KeyVault, the following events occur in sequence:

Item1 is deleted
 Administrator enables soft delete
 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.

You can add a new key named Item1.

You can add a new secret named Item2.

Answer:

Explanation:

NO. Policies cannot be recovered

YES, Item1 is permanently deleted

NO, You cannot use the same name cause Item2 is in Seoft-deleted status

<https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>

Question: 171

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 ensured 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/>

Question: 172

HOTSPOT

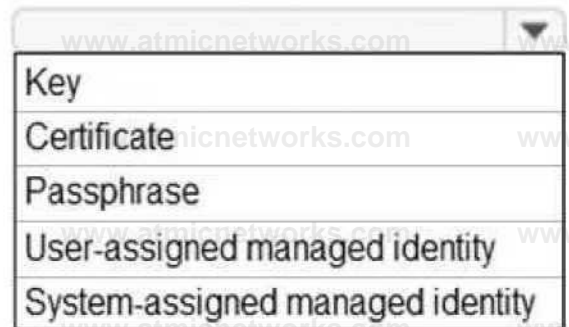
You have an Azure subscription that contains a web app named App1 and an Azure key vault named Vault1.

You need to configure App1 to store and access the secrets in Vault1.

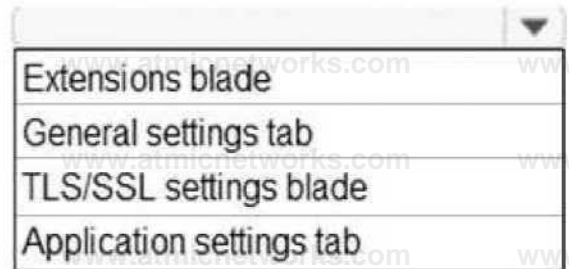
How should you configure App1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Configure App1 to authenticate by using a:



Configure a Key Vault reference for App1 from the:



Answer:

Explanation:

Configure App1 to authenticate by using a:

- Key
- Certificate
- Passphrase
- User-assigned managed identity

System-assigned managed identity

Configure a Key Vault reference for App1 from the: i Extensions blade

General settings tab

TLS/SSL settings blade Application settings

tab

Reference:

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

Question: 173

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: D,F

Explanation:

Question: 174

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

Users can register applications 0

(Yes **SB**)

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>

Question: 175

You have an Azure subscription named Subscription1 that contains an Azure Active Directory (Azure AD) tenant named contoso.com and a resource group named RG1.

You create a custom role named Role1 for contoso.com.

You need to identify where you can use Role1 for permission delegation.

What should you identify?

- A. contoso.com only
- B. contoso.com and RGT only
- C. contoso.com and Subscription1 only
- D. contoso.com, RG1, and Subscription1

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>

Question: 176

You have an Azure subscription that contains an Azure Active Directory (Azure AD) tenant.

When a developer attempts to register an app named App1 in the tenant, the developer receives the error message shown in the following exhibit.

You do not have access

X

Access denied

You do not have access

You don't have permission to register applications in the sk200S10outlook (Default Directory) directory. To request access, contact your administrator.

Summary

Session ID	Resource ID
f8e55e67dl0141b4bf0c7ac5115b3be7	Not available
Extension	Content
Microsoft_AAD_RegisteredApps	CreateApplicationBlade
Error code	
403	

You need to ensure that the developer can register App1 in the tenant.

What should you do for the tenant?

- A. Modify the User settings
- B. Set Enable Security default to Yes.
- C. Modify the Directory properties.
- D. Configure the Consent and permissions settings for enterprise applications.

Answer: A

Explanation:

Reference:

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

Question: 177

HOTSPOT

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

Name	Type
User1	User
User2	User
User!	User
Group1	Security group
Group2	Security group
1 Appl	Enterprise application

User2 is the owner of Group2.

The user and group settings for App1 are configured as shown in the following exhibit.

+ Add user /:

CO

^; j -'

::=E Columns '7

Got feedback?

Q The application will appear on the access panel for assigned users. Set "visible to users?" to no in properties to prevent this. *4 }first

100 shown, to search all users & groups enter a display name.

DISPLAY NAME

OBJECT TYPE

ROLE ASSIGNED

 Group1

Group

Default Access

You enable self-service application access for App1 as shown in the following exhibit.

Allow users to request access to this fl^^ No application? Q

To which group should assigned users be added? 0

Select group

Group?

Require approval before granting access to this application? 0 No

Who is allowed to approve access to this application? 0

Select approvers

1 users selected

To which role should users be assigned in this application? 0

User3 is configured to approve access to Appl.

You need to identify the owners of Group2 and the users of Appl.

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

NOTE: Each correct selection is worth one point.

Group2 owners:

- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users:

- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Answer:

Explanation:

Group2 owners:

- User2 only
- User3 only
- User1 and User2 only
- User2 and User3 only
- User1, User2, and User3

App1 users:

- Group1 members only
- Group2 members only
- Group1 and Group2 members only
- Group1 and Group2 members and User1 only
- Group1 and Group2 members, User1, and User3 only

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access>

Question: 178

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>

Question: 179

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

Explanation:

Question: 180

HOTSPOT

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

Name	Type	In resource group
8372f433-2dcd-4361-b5ef-5b188fed87d0	Subscription ID	<i>Not applicable</i>
RG1	Resource group	<i>Not applicable</i>
VM1	Virtual machine	RG1
VNET1	Virtual network	RG1
storage	Storage account	RG1
User1	User account	<i>Not applicable</i>

You create an Azure role by using the following JSON file.

```
"properties":{ "roleName": "Role1", "description": "", "assignableScopes": [
"/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0",
"/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1 "
]
"permissions": [ { "actions": ( "Microsoft.Compute/*"
L "notActions": [], "dataActions": [], "notDataActions": [] } ]
}
```

You assign Role1 to User1 for 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

User can create a new virtual machine in RG1

User can modify the properties of storage 1.

User can attach the network interface of VM1 to VNET1

Answer:

Explanation:

NO

NO

NO

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute>

Question: 181

HOTSPOT

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

Answer Area

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

Subscription2: An Azure Service Bus queue

Subscription3: A new Azure Log Analytics workspace
 A new Azure Sentinel data connector
 A new Azure Sentinel playbook
 A new Event Grid resource provider

Answer:

Explanation: 3,1

Question: 182

HOTSPOT

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious threats and automate responses.

Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Detect suspicious threats:

- A Kusto query language query
- A Transact-SQL query
- An Azure PowerShell query
- An Azure Sentinel playbook

Automate responses:

- An Azure Functions app
- An Azure PowerShell script
- An Azure Sentinel playbook
- An Azure Sentinel workbook

Answer:

Explanation:

Detect suspicious threats:

- A Kusto query language query
- A Transact-SQL query
- An Azure PowerShell query
- An Azure Sentinel playbook

Automate responses:

- An Azure Functions app
- An Azure PowerShell script
- An Azure Sentinel playbook
- An Azure Sentinel workbook

Reference:

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

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

Question: 183

You are collecting events from Azure virtual machines to an Azure Log Analytics workspace.

You plan to create alerts based on the collected events

You need to identify which Azure services can be used to create the alerts.

Which two services should you identify? Each correct answer presents a complete solution NOTE: Each correct selection is worth one point.

- A. Azure Monitor
- B. Azure Security Center
- C. Azure Analytics Services
- D. Azure Sentinel
- E. Azure Advisor

Answer: A,D

Explanation:

<https://docs.microsoft.com/en-us/azure/analysis-services/analysis-services-overview>

Question: 184

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>

Question: 185

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

Answer: A,C

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal>

Question: 186

HOTSPOT

You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.

Query1 returns a subset of security events generated by Azure AD.

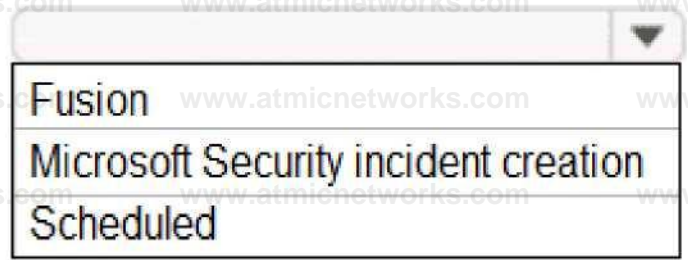
You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1.

You need to ensure that you can add Playbook1 to the new rule.

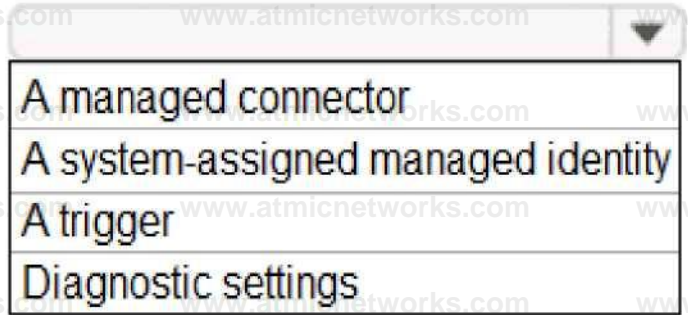
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Create the rule and set the type to:



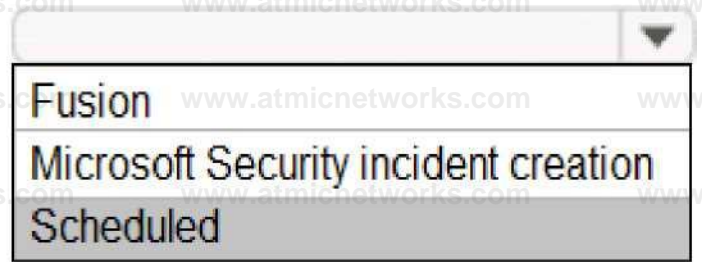
Configure the playbook to include:



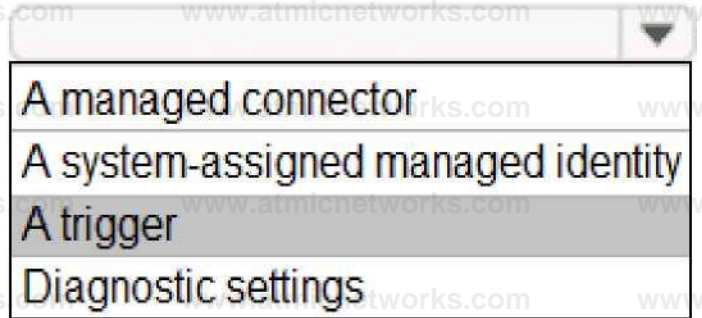
Answer:

Explanation:

Create the rule and set the type to:



Configure the playbook to include:



Reference:

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

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

Question: 187

You have an Azure subscription that contains the Azure Log Analytics workspaces shown in the following table.

Name	Location	Description
Workspace1	East US	Used by Azure Sentinel
Workspace2	West US	<i>Not applicable</i>

You create the virtual machines shown in the following table.

Name	Location	Operating system	Connected to
VM1	East US	Windows Server 2019	<i>None</i>
VM2	East US	Windows Server 2019	Workspace2
VM3	West US	Windows Server 2019	<i>None</i>
VM4	West US	Windows Server 2019	Workspace2

You plan to use Azure Sentinel to monitor Windows Defender Firewall on the virtual machines.

Which virtual machines you can connect to Azure Sentinel?

- A. VM1 and VM3 only
- B. VM1 Only
- C. VM1 and VM2 only

D. VM1, VM2, VM3 and VM4

Answer: D

Explanation:

Reference:

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

Question: 188

You have an Azure Active Directory (Azure AD) tenant and a root management group.

You create 10 Azure subscriptions and add the subscriptions to the root management group.

You need to create an Azure Blueprints definition that will be stored in the root management group. What should you do first?

- A. Add an Azure Policy definition to the root management group.
- B. Modify the role-based access control (RBAC) role assignments for the root management group.
- C. Create a user-assigned identity.
- D. Create a service principal.

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin>

Question: 189

HOTSPOT

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



Tenant Root Group



ManagementGroup1



Subscription1



RG1



VM1

You create the Azure Blueprints definitions shown in the following table.

Name	Published at
Blueprint	Tenant Root Group
Blueprint	Subscription1

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.

Blueprint!:

ManagementGroup! only

ManagementGroup!, Subscription!, and RG1 only

ManagementGroup!, Subscription!, RG!, and VM!

Subscription! only

Tenant Root Group only

Tenant Root Group, ManagementGroup!, and Subscription! only

Blueprint2:

ManagementGroup! only

Subscription! and RG! only

Subscription! only

Subscription!, RG!, and VM!

Answer:

Explanation:

- Blueprint: ▼ ManagementGroup! only
- ManagementGroup!, Subscription!, and RG1 only
 - ManagementGroup!, Subscription!, RG1, and VM1
 - Subscription! only
 - Tenant Root Group only
 - Tenant Root Group, ManagementGroup!, and Subscription! only

Blueprint: _____

- ManagementGroup! only
- Subscription! and RG! only
- Subscription! only
- Subscription!, RG!, and VM!

Blueprints can only be assigned to subscriptions.

Question: 190

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-request-asc>

Question: 191

HOTSPOT

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

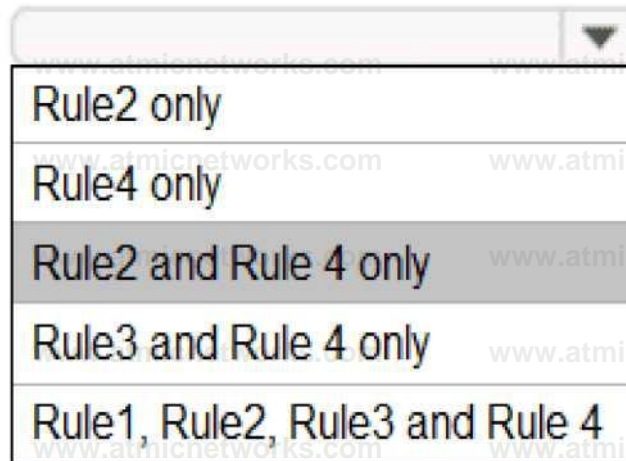
Adding Lock1:

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

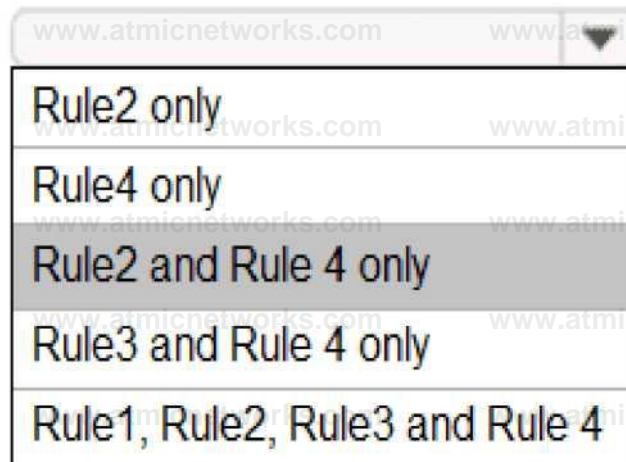
Answer:

Explanation:

Adding VNET1:



Adding Lock1:



Question: 192

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains a user named User1. You plan to publish several apps in the tenant. You need to ensure that User1 can grant admin consent for the published apps.

Which two possible user roles can you assign to User1 to achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Application developer
- B. Security administrator
- C. Application administrator
- D. User administrator
- E. Cloud application administrator

Answer: C,E

Explanation:

Reference:

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

Question: 193

HOTSPOT

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

Name	Role
Admin 1	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:

 Admin1 only
 Admin1 and Admin2 only
 Admin1 and Admin3 only
 Admin1, Admin2, and Admin3

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

 Admin1 only
 Admin1 and Admin2 only
 Admin1 and Admin3 only
 Admin1, Admin2, and Admin3

Answer:

Explanation:

Users who can create a security group named Contoso Sales:

Admin1 only
Admin1 and Admin2 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3

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

Admin1 only
Admin1 and Admin2 only
Admin1 and Admin3 only
Admin1, Admin2, and Admin3

Reference:

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

Question: 194

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-security-alerts?tabs=new>

Question: 195

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: B,C

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>

Question: 196

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD). Azure AD Connect is installed on a domain member server named Server1.

You need to ensure that a domain administrator for the adatum.com domain can modify the synchronization options. The solution must use the principle of least privilege.

Which Azure AD role should you assign to the domain administrator?

- A. Security administrator
- B. Global administrator
- C. User administrator

Answer: B

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/reference-connect-accounts-permissions>

Question: 197

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	None	Global administrator	Enforced
User3	None	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>

Question: 198

You have an Azure subscription.

You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.

Which property of the RBAC role definition should you configure?

- A. NotActions []
- B. DataActions []
- C. AssignableScopes []
- D. Actions []

Answer: D

Explanation:

To 'Read a storage account', ie. list the blobs in the storage account, you need an 'Action' permission. To read the data in a storage account, ie. open a blob, you need a 'DataAction' permission.

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions>

Question: 199

You have an Azure subscription linked to an Azure Active Directory Premium Plan 1 tenant. You plan to implement Azure Active Directory (Azure AD) Identity Protection. You need to ensure that you can configure a user risk policy and a sign-in risk policy.

What should you do first?

- A. Purchase Azure Active Directory Premium Plan 2 licenses for all users.
- B. Register all users for Azure Multi-Factor Authentication (MFA).
- C. Enable security defaults for Azure AD.
- D. Upgrade Azure Security Center to the standard tier.

Answer: A

Explanation:

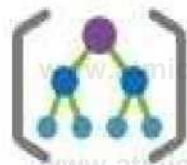
Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-risk-based-sspr-mfa>

Question: 200

HOTSPOT

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



Tenant Root Group



ManagementGroup1



ManagementGroup2



Subscription1



Subscription2



RG1



RG2



RG3



VM2

RG1, RG2, and RG3 are resource groups.

RG2 contains a virtual machine named VM1.

You assign role-based access control (RBAC) roles to the users shown in the following table.

Name	Role	Added to resource
User1	Contributor	Tenant Root Group
User2	Virtual Machine Contributor	Subscription2
User3	Virtual Machine Administrator Login	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.

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM2	<input type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Statements	Yes	No
User1 can deploy virtual machines to RG1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM2	<input type="radio"/>	<input type="radio"/>
User3 can reset the password of the built-in Administrator account of VM2.	<input type="radio"/>	<input type="radio"/>

Question: 201

HOTSPOT

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	

Explanation:

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	

Answer:

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>

Question: 202
HOTSPOT

You have an Azure subscription.

You need to create and deploy an Azure policy that meets the following requirements:

When a new virtual machine is deployed, automatically install a custom security extension. Trigger an autogenerated remediation task for non-compliant virtual machines to install the extension.

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

NOTE: Each correct selection is worth one point.

Definition effect:

- Append
- DeployIfNotExists
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

Assignment remediation task:

- A managed identity that has the Contributor role
- A managed identity that has the User Access Administrator role
- A service principal that has the Contributor role
- A service principal that has the User Access Administrator role

Answer:

Explanation:

Definition effect

- Append
- DeployIfNotExists
- EnforceOPAConstraint
- EnforceRegoPolicy
- Modify

Assignment remediation task:

- A managed identity that has the Contributor role
- A managed identity that has the User Access Administrator role
- A service principal that has the Contributor role
- A service principal that has the User Access Administrator role

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources>

Question: 203

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

Name	Type	Category
Initiative1	Initiative definition	Security Center
Initiative2	Initiative definition	My Custom Category
Policy1	Policy definition	Security Center
Policy2	Policy definition	My Custom Category

You need to identify which initiatives and policies you can add to Subscription1 by using Azure Security Center.

What should you identify?

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

Answer: D

Explanation:

Reference:

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

Question: 204

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-playbook>

Question: 205

You have an Azure resource group that contains 100 virtual machines.

You have an initiative named Initiative1 that contains multiple policy definitions. Initiative1 is assigned to the resource group.

You need to identify which resources do NOT match the policy definitions.

What should you do?

- A. From Azure Security Center, view the Regulatory compliance assessment.
- B. From the Policy blade of the Azure Active Directory admin center, select Compliance.
- C. From Azure Security Center, view the Secure Score.
- D. From the Policy blade of the Azure Active Directory admin center, select Assignments.

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/get-compliance-data#portal>

Question: 206

You have an Azure subscription named Subscription1.

You need to view which security settings are assigned to Subscription1 by default.

Which Azure policy or initiative definition should you review?

- A. the Audit diagnostic setting policy definition
- B. the Enable Monitoring in Azure Security Center initiative definition
- C. the Enable Azure Monitor for VMs initiative definition

D. the Azure Monitor solution 'Security and Audit' must be deployed policy definition

Answer: B

Explanation:

Reference:

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

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

Question: 207

DRAG DROP

You have an Azure Sentinel workspace that has an Azure Active Directory (Azure AD) data connector.

You are threat hunting suspicious traffic from a specific IP address.

You need to annotate an intermediate event stored in the workspace and be able to reference the IP address when navigating through the investigation graph.

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

Add the query to Favorites.

From the Azure Sentinel workspace, run an Azure Log Analytics query.

In a Jupyter notebook, create a reference to the IP address

Add a bookmark and assign a tag

Add a bookmark and map an entity

From Azure Monitor, run an Azure Log Analytics query

Select a query result

Answer Area



Answer:

Explanation:

From the Azure Sentinel workspace, run an Azure Log Analytics query.

Select a query result.

Add a bookmark and map an entity.

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/bookmarks>

Question: 208

HOTSPOT

You have 20 Azure subscriptions and a security group named Group1. The subscriptions are children of the root management group.

Each subscription contains a resource group named RG1.

You need to ensure that for each subscription RG1 meets the following requirements:

The members of Group1 are assigned the Owner role.

The modification of permissions to RG1 is prevented.

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

NOTE: Each correct selection is worth one point.

Configure role-based access control (RBAC) role assignments by using:

	▼
Azure Blueprints	
Azure Policy	
Azure Security Center	

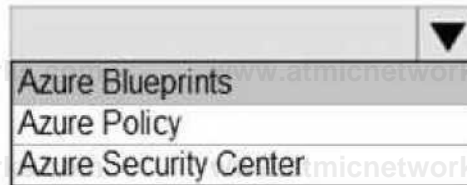
Prevent the modification of permissions to RG1 by using:

	▼
A resource lock	
A role-based access control (RBAC) role assignment at the resource group level	
Azure Blueprint assignments in locking mode	

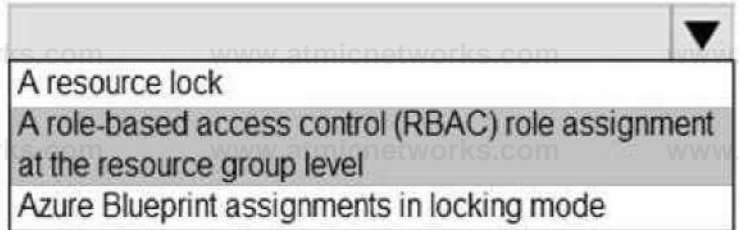
Answer:

Explanation:

Configure role-based access control (RBAC) role assignments by using:



Prevent the modification of permissions to RG1 by using:



Question: 209

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 an initiative and an assignment that is scoped to the Tenant Root Group management group.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

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

<https://4sysops.com/archives/apply-governance-policy-to-multiple-azure-subscriptions-with-management-groups/>

Question: 210

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001 standards. What should you use?

- A. Azure Sentinel
- B. Azure Active Directory (Azure AD) Identity Protection
- C. Azure Security Center
- D. Azure Advanced Threat Protection (ATP)

Answer: C

Explanation:

Reference:

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

Question: 211

HOTSPOT

You have an Azure Storage account that contains a blob container named container1 and a client application named App1.

You need to enable App1 access to container1 by using Azure Active Directory (Azure AD) authentication.

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

NOTE: Each correct selection is worth one point.

From Azure AD:

- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:

- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).

Answer:

Explanation:

From Azure AD:

- Register App1.
- Create an access package.
- Implement an application proxy.
- Modify the authentication methods.

From the storage account:

- Add a private endpoint.
- Regenerate the access key.
- Configure Access control (IAM).
- Generate a shared access signature (SAS).

Reference:

<https://azure.microsoft.com/en-in/blog/announcing-the-preview-of-aad-authentication-for-storage/>

<https://github.com/MicrosoftDocs/azure-docs/blob/master/articles/storage/common/storage-auth-aad-rbac-portal.md>

Question: 212

HOTSPOT

You have an Azure subscription that contains an Azure key vault named ContosoKey1.

You create users and assign them roles as shown in the following table.

Name	Subscription role assignment	ContosoKey1 role assignment
User1	Owner	None
User2	Security Admin	None
User3	None	User Access Administrator
User4	None	Key Vault Contributor

You need to identify which users can perform the following actions:

Delegate permissions for ContosoKey1.

Configure network access to ContosoKey1.

Which users should you identify? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Delegate permissions for ContosoKey: I _____

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Configure network access to ContosoKey: _____ 1

- User1 only
- User2 and User3 only
- User1 and User3 only
- User1 and User4 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

Answer:

Explanation:

Delegate permissions for ContosoKey

^
User1 only
User1 and User2 only
User1 and User3 only
User1 and User4 only
User1, User2, and User3 only
User1, User2, User3, and User4

Configure network access to ContosoKey

User1 only
User1 and User2 only
User1 and User3 only
User1 and User4 only
User1, User2, and User3 only
User1, User2, User3, and User4

Reference:

<https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide>

Question: 213

You have an Azure subscription that contains four Azure SQL managed instances.

You need to evaluate the vulnerability of the managed instances to SQL injection attacks. What should you do first?

- A. Create an Azure Sentinel workspace.
- B. Enable Advanced Data Security.
- C. Add the SQL Health Check solution to Azure Monitor.
- D. Create an Azure Advanced Threat Protection (ATP) instance.

Answer: B

Explanation:

Question: 214

HOTSPOT

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:

V

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

Answer:

Explanation:

Assign role to:

V

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

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-portal>

Question: 215

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>

Question: 216

HOTSPOT

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	<i>None</i>
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

V M1 can connect to storage.

V M2 can connect to storage.

V M3 can connect to storage.

Answer:

Explanation:

Statements

Yes

No

V M1 can connect to storage.

V M2 can connect to storage.

V M3 can connect to storage.

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.

Question: 217

You plan to create an Azure Kubernetes Service (AKS) cluster in an Azure subscription.

The manifest of the registered server application is shown in the following exhibit.

Save Discard Upload Download

The editor below allows you to update this application by directly modifying its JSON representation. For more details, see: [Understand how to update an Azure AD application manifest](#)

```
1 {
2   "id": "d6b00db3-7ef4-4f3c-ble7-8346f0a59546",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": null,
5   "addins": [],
6   "allowPublicClient": true,
7   "appId": "111374675-4c20-903a-f7b1-1ff7d494",
8   "appRoles": [],
9   "oauth2AllowUrlPathMatching": false,
10  "createdDateTime": "2019-07-15T21:00:00",
11  "groupMembershipClaims": null,
12  "identifierUris": [],
13  "informationalUrls": {
14    "termsOfService": null,
15    "support": null,
16    "privacy": null,
17    "marketing": null
18  },
19  "keyCredentials": [],
20  "knownClientApplications": [],
21  "logoUrl": null,
22  "logoutUrl": null,
23  "name": "AKI Anur-AD-rv*",
24  "oauth2AllowIdTokenImplicitFlow": true,
25  "oauth2AllowImplicitFlow": true,
26  "oauth2Permissions": [],
27  "oauth2RequirePostResponse": true,
28  "optionalClaims": null,
29  "orgRestrictions": [],
30  "parentalControlSettings": {
```

You need to ensure that the AKS cluster and Azure Active Directory (Azure AD) are integrated.

Which property should you modify in the manifest?

- A. accessTokenAcceptedVersion
- B. keyCredentials
- C. groupMembershipClaims
- D. acceptMappedClaims

Answer: C

Explanation:

Reference:

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

<https://www.codeproject.com/Articles/3211864/Operation-and-Maintenance-of-AKS-Applications>

Question: 218

HOTSPOT

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

Name	Location	Subnet	Peered network
VNET1	East US	Subnet1	VNET2
VNET2	West US	Subnet?, Subnets	VNET1
VNET4	East US	Subnet-4	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	Subnet?	No
VM3	ASG2	NSG1	SubnetB	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	<input type="radio"/> Allow -
130	Rule1	Any	Any	9 ASG1	Any	<input type="radio"/> Allow -
140	Rule2	Any	Any	9 ASG2	Any	<input checked="" type="radio"/> Allow -
150	Rule3	Any	Any	9 ASG4	Any	<input checked="" type="radio"/> Allow -
160	A Rule4	Any	Any	Any	Any	<input type="radio"/> Deny -
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	<input checked="" type="radio"/> Allow -
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	<input type="radio"/> Allow -
65500	DenyAllInBound	Any	Any	Any	Any	<input type="radio"/> Deny -

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	<input type="radio"/> Allow -
65001	AllowInternetOutBou...	Any	Any	Any	Internet	<input checked="" type="radio"/> Allow <input type="checkbox"/> <input type="checkbox"/>
65500	DenyAllOutBound	Any	Any	Any	Any	<input type="radio"/> 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
<input type="checkbox"/> M1 can ping VM3 successfully.	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> M2 can ping VM4 successfully.		
<input type="checkbox"/> M3 can be accessed by using Remote Desktop from the internet.		

Answer:

Explanation:

Statements	Yes	No
<input type="checkbox"/> M1 can ping VM3 successfully.	<input type="radio"/>	<input type="radio"/>
<input type="checkbox"/> M2 can ping VM4 successfully		
<input type="checkbox"/> M3 can be accessed by using Remote Desktop from the internet.		

Box 1: Yes

V M1 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

V M2 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

V M3 has a public IP address and the firewall allows traffic on port 3389.

Question: 219

HOTSPOT

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

Answer:

Explanation:

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

Reference:

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

Question: 220

DRAG DROP

Your network contains an on-premises Active Directory domain named contoso.com. The domain contains a user named User1.

You have an Azure subscription that is linked to an Azure Active Directory (Azure AD) tenant named contoso.com. The tenant contains an Azure Storage account named storage1. Storage1 contains an Azure file share named share1.

Currently, the domain and the tenant are not integrated.

You need to ensure that User1 can access share1 by using his domain credentials.

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 private link to storage1.

Enable Active Directory Domain Services (AD DS) authentication on storage1.

Implement Azure AD Connect.

Create a service endpoint to storage1.

Assign share-level permissions for share1.

Answer:

Explanation:

Implement Azure AD Connect.

Enable Active Directory Domain Services (AD DS) authentication on storage1.

Assign share-level permissions for share1.

Reference:

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

Question: 221

HOTSPOT

You have a management group named Group1 that contains an Azure subscription named sub1.

Sub1 has a subscription ID of 11111111-1234-1234-1234-1111111111.

You need to create a custom Azure role-based access control (RBAC) role that will delegate permissions to manage the tags on all the objects in Group1.

What should you include in the role definition of Role1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Resource provider:

Microsoft.Authorization _
Microsoft.Resources
Microsoft.Support |

*

Assignable scope:

/Group/
subscriptions/11111111-1234-1234-1234-1111111111

Answer:

Explanation:

Resource provider:

Microsoft.Authorization
Microsoft.Resources
Microsoft.Support

Assignable scope:

/Group/
subscriptions/11111111-1234-1234-1234-1111111111

Text, application Description automatically generated

Note: Assigning a custom RBAC role as the Management Group level is currently in preview only. So, for now the answer to the assignable scope is the subscription level.

Reference:

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

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal#step-5-assignable-scopes>

Question: 222
HOTSPOT

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

Name	Type
Role1	Azure Active Directory (Azure AD)
Role2	Azure subscription

In the Azure portal, you plan to create new custom roles by cloning existing roles. The new roles will be configured as shown in the following table.

Name	Type
Role3	Azure AD
Role4	Azure subscription

Which roles can you clone to create each new role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Role3:

- Role1 only
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only**
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:

- Role2 only
- Built-in Azure AD roles only
- Role2 and built-in Azure subscription roles only
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

Answer:

Explanation:

Role3:

- Role1 only
- Built-in Azure AD roles only
- Role1 and built-in Azure AD roles only
- Role1, built-in Azure AD roles, and built-in Azure subscription roles

Role4:

- Role2 only
- Built-in Azure AD roles only
- Role2 and built-in Azure subscription roles only
- Role2, built-in Azure subscription roles, and built-in Azure AD roles

Graphical user interface, text, application, email Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/roles/custom-create>

<https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles-portal>

Question: 223

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

Name	Type
VM1	Virtual machine
VNET1	Virtual network
storage 1	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>

Question: 224

DRAG DROP

You have an Azure subscription that contains the following resources:

- A network virtual appliance (NVA) that runs non-Microsoft firewall software and routes all outbound traffic from the virtual machines to the internet
- An Azure function that contains a script to manage the firewall rules of the NVA
- Azure Security Center standard tier enabled for all virtual machines
- An Azure Sentinel workspace
- 30 virtual machines

You need to ensure that when a high-priority alert is generated in Security Center for a virtual machine, an incident is created in Azure Sentinel and then a script is initiated to configure a firewall rule for the NVA.

How should you configure Azure Sentinel to meet the requirements? To answer, drag the appropriate components to the correct requirements. Each component 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.

Components	Answer Area
A data connector for Security Center	Enable alert notifications from Security Center: <input type="text" value="Component"/>
A data connector for the firewall software	Create an incident: <input type="text" value="Component"/>
A playbook	Initiate a script to configure the firewall rule: <input type="text" value="Component"/>
A rule	
A Security Events connector	
A workbook	

Answer:

Explanation:

Enable alert notifications from Security Center:

A data connector for Security Center

Create an incident:

A rule

Initiate a script to configure the firewall rule:

A playbook

Reference:

<https://docs.microsoft.com/en-us/azure/sentinel/create-incidents-from-alerts>

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

Question: 225

HOTSPOT

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.

What should you configure for each subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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

Answer:

Explanation:

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

Graphical user interface, text, application, email Description automatically generated

Question: 226

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>

Question: 227

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>

Question: 228

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>

Question: 229

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

Name	Location	Virtual network name
VM1	East US	VNET1
VM2	West US	VNET2
VM3	East US	VNET1
VM4	West US	VNET3

All the virtual networks are peered.

You deploy Azure Bastion to VNET2.

Which virtual machines can be protected by the bastion host?

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

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/bastion/vnet-peering>

Question: 230

HOTSPOT

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

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

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	SG1, 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.

NOTE: Each correct selection is worth one point.

Answer Area

Statements

Yet No

SQL1 will have TDE enabled automatically

The deployment of SQL1 will fail

SQL will be deployed and managed automatically.

Answer:

Explanation:

Statements

Y/N

SQL1 will be deployed automatically.

•

The deployment of SQL2 will fail.

•

SQL1 will be deployed and managed automatically.

Graphical user interface,

text, application Description automatically generated

Question: 231

HOTSPOT

You have an Azure subscription that contains three storage accounts, an Azure SQL managed instance named SQL and three Azure SQL databases. The storage accounts are configured as shown in the following table. SQL1 has the following settings:

- Auditing: On
- Audit log destination: storage1

The Azure SQL databases are configured as shown in the following table.

Answer Area

Statements

Yes

No

Audit events for DB1 are written to storage1

Audit events for DB2 are written to storage1 and storage2

Storage2 can be used as an audit log destination for DB3. (L)

Answer:

Explanation:

Answer Area

Audit events for DB1 are written to storage1. •

Audit events for DB2 are written to storage1 and storage2. •

Storage2 can be used as an audit log destination for DB3. •

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/managed-instance/auditing-configure>

<https://docs.microsoft.com/en-us/azure/azure-sql/database/auditing-overview>

Question: 232

You have an app that uses an Azure SQL database.

You need to be notified if a SQL injection attack is launched against the database.

What should you do?

- A. Modify the Diagnostics settings for the database.
- B. Deploy the SQL Health Check solution in Azure Monitor.
- C. Enable Azure Defender for SQL for the database.
- D. Enable server-level auditing for the database.

Answer: C

Explanation:

Question: 233

You plan to deploy an app that will modify the properties of Azure Active Directory (Azure AD) users by using Microsoft Graph. You need to ensure that the app can access Azure AD. What should you configure first?

- A. a custom role-based access control (RBAC) role
- B. an external identity
- C. an Azure AD Application Proxy
- D. an app registration

Answer: B

Explanation:

Reference:

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

Question: 234

You have an Azure Active Directory (Azure AD) tenant.

You need to prevent nonprivileged Azure AD users from creating service principals in Azure AD.

What should you do in the Azure Active Directory admin center of the tenant?

- A. From the Properties blade, set Enable Security defaults to Yes.
- B. From the Properties blade, set Access management for Azure resources to No
- C. From the User settings blade, set Users can register applications to No
- D. From the User settings blade, set Restrict access to Azure AD administration portal to Yes.

Answer: C

Explanation:

Question: 235

You have an Azure subscription.

You plan to create a workflow automation in Azure Security Center that will automatically remediate a security vulnerability.

What should you create first?

- A. a managed identity
- B. an automation account

- C. an Azure function app
- D. an alert rule
- E. an Azure logic app

Answer: E

Explanation:

Reference:

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

Question: 236

HOTSPOT

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
Appl	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	

Answer:

Explanation:

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

Graphical user interface, text, application Description automatically generated

Question: 237
HOTSPOT

You have an Azure Active Directory (Azure AD) tenant named contoso.com that contains three security groups named Group1, Group2, and Group3 and the users shown in the following table.

Name	Role	Member of
User1	Application administrator	Group1
User2	Application developer	Group2
User3	Cloud application administrator	Group3





Group3 is a member of Group2.

In contoso.com, you register an enterprise application named App1 that has the following settings:

Owners: User1

Users and groups: Group2


You configure the properties of App1 as shown in the following exhibit.


 Save  Discard  Delete  Got feedback


Enabled for users to sign-in? Yes No


Name *

Homepage URL

Logo 



Application ID 

Object ID 

User assignment required? Yes No

Visible to users Yes No

Notes

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 has Appl listed on his My Apps portal. User2 has Appl listed on her My Apps portal. User3 has Appl listed on her My Apps portal.

Answer:

Explanation:

Statements

Yes

No

User1 has Appl listed on his My Apps portal.

User2 has Appl listed on her My Apps portal.

User3 has Appl listed on her My Apps portal.

Text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/assign-user-or-group-access-portal>

Question: 238

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 machines in RG1 only.

Connect the virtual machines to the existing virtual networks 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. a custom RBAC role for RG2
- B. the Network Contributor role for RG2
- C. the Contributor role for the subscription
- D. a custom RBAC role for the subscription
- E. the Network Contributor role for RG1
- F. the Virtual Machine Contributor role for RG1

Answer: A,F

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

Question: 239

HOTSPOT

Your network contains an on-premises Active Directory domain named adatum.com that syncs to Azure Active Directory (Azure AD).

The Azure AD tenant contains the users shown in the following table.

Name	Source	Password
User1	Azure AD	Adatum123
User2	Azure AD	N3w3rT0Gue33
User3	On-premises Active Directory	ComplexPassword33

You configure the Authentication methods – Password Protection settings for adatum.com as shown in the following exhibit.

Custom smart lockout

Lockout threshold ⓘ

10

Lockout duration in seconds ⓘ

60

Custom banned passwords

Enforce custom list ⓘ

Yes

No

Adatum

Custom banned password list

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory ⓘ

Yes

No

Mode ⓘ

Enforced

Audit

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 will be prompted to change the password on the next sign-in.

User2 can change the password to @d@tum_C0mpleX123.

User3 can change the password to Adatum!23!.

Answer:

Explanation:

Statements

Yes No

User1 will be prompted to change the password on the next sign-in.

User2 can change the password to @d@tum_C0mpleX123.

UserS can change the password to Adatum!23!.

Text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>

Question: 240
HOTSPOT

Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes the users shown in the following table.

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

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	

Answer:

Explanation:

User:

	▼
User1	
User2	
User3	
User4	

Tool:

	▼
Azure Account Center	
Azure Cloud Shell	
Azure PowerShell	
Azure Security Center	

Table Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/billing-subscription-transfer>

Question: 241

HOTSPOT

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

Basics Artifacts

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

ARTIFACT TYPE

PARAMETERS

▼ 9 Subscription

4* Add artifact...

▼ 1 RG2

X User1 (U5er1@5k20062Scutlook.onmicrosoft.com): Tag Contributor

^ Add artifact...

Resource group

2 out of 2 parameters populated

Role assignment

1 out of 1 parameters populated

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.

User1 can add tags to RG2.

You can remove User1 from the Tag Contributor role for RG2.

Answer:

Explanation:

Statements

Yes

No

A locking mode of Read Only will be assigned to RG1.

User1 can add tags to RG2.

You can remove User1 from the Tag Contributor role for RG2.

Graphical user interface, text, application Description automatically generated

Reference:

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

Question: 242

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: C

Explanation:

Reference:

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

Question: 243

You have an Azure subscription named Subscription1 that contains a resource group named RG1 and the users shown in the following table.

Name	User principal name (UPN)	Type
User1	User1@outlook.com	Guest
User2	User2@outlook.com	Guest

You perform the following tasks:

Assign User1 the Network Contributor role for Subscription1.

Assign User2 the Contributor role for RG1.

To Subscription1 and RG1, you assign the following policy definition: External accounts with write permissions should be removed from your subscription.

What is the Compliance State of the policy assignments?

- A. The Compliance State of both policy assignments is Non-compliant.
- B. The Compliance State of the policy assignment to Subscription1 is Compliant, and the Compliance State of the policy assignment to RG1 is Non-compliant.
- C. The Compliance State of the policy assignment to Subscription1 is Non-compliant, and the Compliance State of the policy assignment to RG1 is Compliant.
- D. The Compliance State of both policy assignments is Compliant.

Answer: A

Explanation:

Question: 244

HOTSPOT

You have an Azure Sentinel workspace that has the following data connectors:

Azure Active Directory Identity Protection

Common Event Format (CEF)

Azure Firewall

You need to ensure that data is being ingested from each connector.

From the Logs query window, which table should you query for each connector? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Azure Active Directory Identity Protection:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

Azure Firewall:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

CEF:

- AzureDiagnostics
- CommonSecurityLog
- SecurityAlert
- SecurityEvent
- Syslog

Answer:

Explanation:

Azure Active Directory Identity Protection:

	▼
AzureDiagnostics	
CommonSecurityLog	
SecurityAlert	
SecurityEvent	
Syslog	

Azure Firewall:

	▼
AzureDiagnostics	
CommonSecurityLog	
SecurityAlert	
SecurityEvent	
Syslog	

CEF:

	▼
AzureDiagnostics	
CommonSecurityLog	
SecurityAlert	
SecurityEvent	
Syslog	

Graphical user interface, application, table Description automatically generated

Question: 245

DRAG DROP

You have an Azure subscription.

You plan to create a storage account.

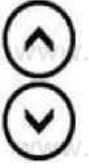
You need to use customer-managed keys to encrypt the tables in the storage account.

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

Answer Area

New-AzStorageAccountKey
 New-AzStorageTable
 Register-AzProviderFeature
 New-AzStorageAccount
 Register-AzResourceProvider



Answer:

Explanation:

New-AzStorageAccount

New-AzStorageAccountKey

New-AzStorageTable

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=powershell>

Question: 246

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>

Question: 247

DRAG DROP

You have three Azure subscriptions and a user named User1.

You need to provide User1 with the ability to manage and view costs for the resources across all three subscriptions.

The solution must use the principle of least privilege.

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.

NOTE: More than one order of answer choices is correct. You will receive credit for any of the correct orders you select.

Actions
Create a management group.
Add the three subscriptions to the management group.
Assign User1 the Global administrator role.
Assign User1 the Owner role for the management group.
Assign User1 the Cost Management Contributor role for the management group.

Answer:

Explanation:

Actions
Create a management group.
Assign User1 the Owner role for the management group.
Assign User1 the Cost Management Contributor role for the management group.

Answer Area

- 1 Assign User1 the Cost Management Reader role for the management group.
- 2 Assign User1 the Global administrator role.
- 3 Add the three subscriptions to the management group.



Question: 248

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

Explanation:

Question: 249

You have 10 on-premises servers that run Windows Server 2019.
You plan to implement Azure Security Center vulnerability scanning for the servers.

What should you install on the servers first?

- A. the Security Events data connector in Azure Sentinel
- B. the Microsoft Endpoint Configuration Manager client
- C. the Azure Arc enabled servers Connected Machine agent
- D. the Microsoft Defender for Endpoint agent

Answer: C

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/azure-arc/servers/agent-overview>

<https://docs.microsoft.com/en-us/azure/security-center/deploy-vulnerability-assessment-vm>

Question: 250

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

Which virtual machines should you use?

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

Answer: D

Explanation:

Question: 251

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>

Question: 252

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 pass-through authentication and seamless SSO with password hash synchronization.

Does the solution meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

Question: 253

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>

Question: 254

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 password hash synchronization and seamless SSO.

Does the solution meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Question: 255

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.

After syncing all on-premises identities to Azure AD, you are informed that users with a givenName attribute starting with LAB should not be allowed to sync to Azure AD.

Which of the following actions should you take?

- A. You should make use of the Synchronization Rules Editor to create an attribute-based filtering rule.
- B. You should configure a DNAT rule on the Firewall.
- C. B. You should configure a network traffic filtering rule on the Firewall.
- D. You should make use of Active Directory Users and Computers to create an attribute-based filtering rule.

Answer: A

Explanation:

Use the Synchronization Rules Editor and write attribute-based filtering rule.

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-change-the-configuration>

Question: 256

You have been tasked with applying conditional access policies for your company's current Azure Active Directory (Azure AD).

The process involves assessing the risk events and risk levels.

Which of the following is the risk level that should be configured for users that have leaked credentials?

- A. None

- B. Low
- C. Medium
- D. High

Answer: D

Explanation:

These six types of events are categorized in to 3 levels of risks – High, Medium & Low:

Sign-in Activity	Risk Level
Users with leaked credentials	High
Sign-ins from anonymous IP addresses	Medium
Impossible travel to atypical locations	Medium
Sign-ins from infected devices	Medium
Sign-ins from IP addresses with suspicious activity	Low
Sign-ins from unfamiliar locations	Medium

Table Description automatically generated

Reference:

<http://www.rebeladmin.com/2018/09/step-step-guide-configure-risk-based-azure-conditional-access-policies/>

Question: 257

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.

Reviewers

Group owners

Reviewers

Group owners Selected users Members (self) Link to program ¹

Graphical user interface, application Description automatically generated with medium confidence

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>

Question: 258

DRAG DROP

You have an Azure Storage account named storage1 and an Azure virtual machine named VM1. VM1 has a premium SSD managed disk.

You need to enable Azure Disk Encryption for VM1.

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

Run the `Set-AzVMDiskEncryptionExtension` cmdlet.

Set the Key Vault access policy to **Enable access to Azure Virtual Machines for deployment**.

Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.

Generate a key vault certificate.

Create an Azure key vault.

Configure storage1 to use a customer-managed key.

Answer Area

Answer:

Explanation:

Create an Azure key vault.

Set the Key Vault access policy to **Enable access to Azure Disk Encryption for volume encryption**.

Run the `Set-AzVMDiskEncryptionExtension` cmdlet.

Graphical user interface, text, application Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-key-vault>

Question: 259

HOTSPOT

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

Name	Type
storage1	Azure Blob storage
storage2	Azure Files SMB
storage3	Azure Table storage

You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

storage1:

- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2:

- Shared Key only
- Shared access signature (SAS) only
- Shared Key and shared access signature (SAS)

storage3:

- Shared Key only
- Shared access signature (SAS) only
- Azure Active Directory (Azure AD) only
- Shared Key and shared access signature (SAS) only
- Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

Answer:

Explanation:

storage1:

Shared Key only
Shared access signature (SAS) only
Azure Active Directory (Azure AD) only
Shared Key and shared access signature (SAS) only
Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2:

Shared Key only
Shared access signature (SAS) only
Shared Key and shared access signature (SAS)

storage3:

Shared Key only
Shared access signature (SAS) only
Azure Active Directory (Azure AD) only
Shared Key and shared access signature (SAS) only
Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

Graphical user interface, text, application, email Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/authorize-data-access>

Question: 260

You are troubleshooting a security issue for an Azure Storage account. You enable Azure Storage Analytics logs and archive them 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

Explanation:

Question: 261

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: A,C

Explanation:

Question: 262

HOTSPOT

You have an Azure subscription that contains the following resources:

- An Azure key vault
- An Azure SQL database named Database1
- Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1

You need to implement an encryption solution for Database1 that meets the following requirements:

- The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data.
- AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys.

How should you configure the encryption settings for Database1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

To configure the encryption of Database1:

- Always Encrypted by using Azure Key Vault.
- Always Encrypted by using the Windows Certificate Store.
- Transparent Data Encryption (TDE) by using Azure Key Vault integration.
- Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

- Create an access policy in Azure Key Vault.
- Generate a key on an HSM device.
- Import App Service certificates to AppSrv1 and AppSrv2.
- Register an enterprise application in Azure AD.

Answer:

Explanation:

To configure the encryption of Database1: 1 h

Always Encrypted by using Azure Key Vault

Always Encrypted by using the Windows Certificate Store.
Transparent Data Encryption (TDE) by using Azure Key Vault integration
Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK)

To obtain the cryptographic keys:

▼
Create an access policy in Azure Key Vault
Generate a key on an HSM device
Import App Service certificates to AppSvc and AppSvc2 Register an enterprise application in Azure AD.

Text Description automatically generated with medium confidence

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=azure-powershell>

Question: 263

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.

Question: 264

You have a Microsoft 365 tenant that uses an Azure Active Directory (Azure AD) tenant. The Azure AD tenant syncs to an on-premises Active Directory domain by using an instance of Azure AD Connect.

You create a new Azure subscription.

You discover that the synced on-premises user accounts cannot be assigned roles in the new subscription.

You need to ensure that you can assign Azure and Microsoft 365 roles to the synced Azure AD user accounts. What should you do first?

- A. Change the Azure AD tenant used by the new subscription.
- B. Configure the Azure AD tenant used by the new subscription to use pass-through authentication.
- C. Configure the Azure AD tenant used by the new subscription to use federated authentication.
- D. Configure a second instance of Azure AD Connect.

Answer: A

Explanation:

Question: 265

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains two users named User1 and User2 and a registered app named App1.

You create an app-specific role named Role1.

You need to assign Role1 to User1 and enable User2 to request access to App1.

Which two settings should you modify? To answer, select the appropriate settings in the answer area. NOTE: Each correct selection is worth one point.



Explanation:

Answer:



Graphical user interface, application Description automatically generated

Question: 266

You have the Azure resource shown in the following table.

Name	Type	town
Maimer* 1	'Alnj^erw -^cup	Tenant Root woe
Subiinncin'	Sijjnjptai	Miwgenwt!
f 61	"fscwce ."Li	^utsatplvi 1
^	Hesaragwif	5ub\$mpifiTI
VM1	Vrttir ntachne	RGi
VW	VfMi 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

Explanation:

Question: 267

You have multiple development teams that will create apps in Azure.

You plan to create a standard development environment that will be deployed for each team.

You need to recommend a solution that will enforce resource locks across the development environments and ensure that the locks are applied in a consistent manner.

What should you include in the recommendation?

- A. an Azure policy
- B. an Azure Resource Manager template
- C. a management group
- D. an Azure blueprint

Answer: D

Explanation:

Reference:

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

Question: 268

You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments.

You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege.

Which role should you assign to the PIM service principle?

- A. Contributor
- B. User Access Administrator
- C. Managed Application Operator
- D. Resource Policy Contributor

Answer: B

Explanation:

Question: 269

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

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

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

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

What should you do?

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

Answer: C

Explanation:

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

Reference:

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

Question: 270

HOTSPOT

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 Appl.	<input type="radio"/>	<input type="radio"/>
User1 can start and stop contl.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Statements	Yes	No
-------------------	------------	-----------

User1 can add VM1 to VNET1. 0 0

User1 can start and stop App1. 0 0

User1 can start and stop contl. 0 0

Text Description automatically generated

Reference:

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

Question: 271

HOTSPOT

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

Name	Type	Resource group	Location
RG1	Resource group	Not applicable	West US
ManagedI	Managed identity	RG1	West US

The subscription is linked to an Azure Active Directory (Azure AD) tenant that contains the users shown in the following table.

Name	Usage location
User1	United States
User2	Germany

You create the groups shown in the following table.

Name	Type	Membership type
Group1	Security	Dynamic User
Group2	Microsoft 365	Dynamic User

The membership rules for Group1 and Group2 are configured as shown in the following exhibit.



Dynamic membership rules

 Save  Discard |  Got feedback?

Configure Rules

Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value	
	accountEnabled	Equals	true	
Or	usageLocation	Equals	US	

[+ Add expression](#) [+ Get custom extension properties](#)

Rule syntax

 Edit

```
(user.accountEnabled -eq true) or (user.usageLocation - eq "US")
```

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 is a member of Group1 and Group2.

User2 is a member of Group2 only.

Managed1 is a member of Group1 and Group2.

Answer:

Explanation:

Statements

Yes

No

User1 is a member of Group1 and Group2.

User2 is a member of Group2 only.

Managed1 is a member of Group1 and Group2.

Text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/groups-dynamic-membership>

Question: 272

You have an Azure subscription name Sub1 that contains an Azure Policy definition named Policy1.

Policy1 has the following settings:

Definition location: Tenant Root Group

Category: Monitoring

You need to ensure that resources that are noncompliant with Policy1 are listed in the Azure Security Center dashboard.

What should you do first?

- A. Change the Category of Policy1 to Security Center.
- B. Add Policy1 to a custom initiative.
- C. Change the Definition location of Policy1 to Sub1.

D. Assign Policy1 to Sub1.

Answer: D

Explanation:

Reference:

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

Question: 273

HOTSPOT

You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table. Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.

Name	Type	Assigned object
AU1	Administrative unit	User1, Group1
AU2	Administrative unit	None
User1	User	Not applicable
Group1	Security group	Not applicable
Group2	Microsoft 365 group	Not applicable

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Are*

AU1: Group2 and Identity 1 only

AU2: Group1, Group2 and User1 only

Question: 274

HOTSPOT

You have an Azure Subscription that is linked to an Azure Active Directory (Azure AD). The tenant contains the users shown in the following table.

Name	Role	Member of
User1	Security administrator	Group1
User2	Network Contributor	Group2
User3	Key Vault Contributor	Group1, Group2

You have an Azure key vault named Vault1 that has Purge protection set to Disabled. Vault1 contains the access policies shown in the following table.

Name	Key permission	Secret permission	Certificate permission
Group1	Purge	Purge	Purge
Group2	Select all	Select all	Select all

You create role assignments for Vault1 as shown in the following table.

Name	Role
User1	None
User2	Key Vault Reader
User3	User Access Administrator

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

NOTE: Each correct selection is worth one point.

Answer Art*

Statement*	Yes*	No
User1 can set Purge protection to Enable for Vault 1	<input type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault1.	<input type="radio"/>	<input type="radio"/>
User3 can access secrets in Vault1	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Antwort Are*

Statement*	Yes*	No
User1 can set Purge protection to Enable for Vault1	<input type="radio"/>	<input type="radio"/>
User2 can configure firewalls and virtual networks for Vault 1.	<input type="radio"/>	<input type="radio"/>
User3 can add access policies to Vault1.	<input type="radio"/>	<input type="radio"/>

Question: 275

HOTSPOT

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	

Answer:

Explanation:

Account type:

Azure Active Directory User
Managed identity
Service Principal

Roles:

db_datawriter only
db_datareader and db_datawriter
db owner only

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%2Cdotnet>

Question: 276

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

Name	Type
storagel	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 storage Key Vault Reader for Vault
VM2	<ul style="list-style-type: none"> Storage Blob Data Reader for storage Key Vault Reader for Vault
VM3	<ul style="list-style-type: none"> Storage Blob Data Reader for storage Key Vault Reader for Vault Key Vault Reader for Vault?
VM4	<ul style="list-style-type: none"> Storage Blob Data Reader for storage Key Vault Reader for Vault Key Vault Reader for Vault?

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>

Question: 277
HOTSPOT

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 IDE enabled automatically.

The deployment of SQL2 will fail.

SQL3 will be deployed and marked as noncompliant.

Answer:

Explanation:

Statements

Yes

No

SQL1 will have TDE enabled automatically.

The deployment of SQL2 will fail.

SQL3 will be deployed and marked as noncompliant.

Graphical user interface, text, application Description automatically generated

Reference:

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

Question: 278

HOTSPOT

You have an Azure subscription that contains a resource group named RG1. RG1 contains a storage account named storage1.

You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.

The permissions for Role1 are shown in the following JSON code.

```
{
  "Name": "Role1",
  "Permissions": [
    {
      "Action": "Microsoft.Storage/*",
      "DataActions": [
        "Microsoft.Storage/storageAccounts/read"
      ],
      "NotDataActions": []
    }
  ]
}
```

The permissions for Role2 are shown in the following JSON code.

```
{
  "Name": "Role2",
  "Permissions": [
    {
      "Action": "Microsoft.Storage/*",
      "DataActions": [
        "Microsoft.Storage/storageAccounts/read",
        "Microsoft.Storage/storageAccounts/write"
      ],
      "NotDataActions": [
        "Microsoft.Storage/storageAccounts/delete"
      ]
    }
  ]
}
```

Answer Are* Statements

Yes

User1 can read data in storage1.

No

0

User2 can read data in storage1.

User3 can restore storage1 from a backup in Azure Backup.

Answer:

Explanation:

Answer Area Statements

Yes

No

User1 can read data in storage.

User? can read data in storage!

User? can restore storage from a backup in Azure Backup

E

Question: 279

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant that contains two administrative units named AU1 and AU2.

Users are assigned to the administrative units as shown in the following table.

User name	Member of
Admin1	AU1
Admin2	AU1
Admin3	AU2
Admin4	AU2
User1	AU1

Answer Area

Statements

Yes

No

Admin1 can reset the password of User1.

Admin2 can reset the password of User?.

Admin3 can reset the password of Admin4.

Answer:

Explanation:

Answer Area

Statements

Yes

No

Admin1 can reset the password of User1.

Admin? can reset the password of User?.

Admin? can reset the password of AdminA

Question: 280

You have an Azure subscription that uses Microsoft Sentinel.

You need to create a Microsoft Sentinel notebook that will use the Guided Investigation - Anomaly

Lookup template.

What should you create first?

- A. an analytics rule
- B. a Log Analytics workspace
- C. an Azure Machine Learning workspace
- D. a hunting query

Answer: A

Explanation:

Question: 281

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

You need to ensure that User1 can create and manage administrative units. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Privileged role administrator
- B. Helpdesk administrator
- C. Global administrator
- D. Security administrator

Answer: A

Explanation:

Question: 282

DRAG DROP

You have an Azure subscription that contains an Azure SQL database named SQLDB1. SQLDB1 contains the columns shown in the following table.

Name	Data type	Sample value
Email	Varchar	admin@contoso.com
Birthday	Date	2010-07-07

For the Email and Birthday columns, you implement dynamic data masking by using the default masking function.

Which value will the users see in each column? To answer, drag the appropriate values to the correct columns. Each value 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.

Values

- 1900-01-01
- 1900-01-01 00:00:00.0000
- 2010-XX-XX
- XXXX

Answer Area

Answer:

Explanation:

Answer Area

Email: 11900-0^1

i

Sirihday: | 2010-M

~

Question: 283

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

Name	Type
wr	Virtual machine
VNET1	Virtual network
storage1	Storage account
Vault1	Ke/vault

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

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

Answer: C

Explanation:

Question: 284

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:

Answer: See the answer below at

Explanation.

Explanation:

Answer is as image below.

Answer Area

Azure files share: AD DS only

Folders in the file share: AD DS and Azure AD

0

Question: 285

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.



Deny public network access 0

C Ws No J

0 [Click here to create a new private endpoint](#) **Create Private Endpoint**

Minimum TLS Version Q (1.0 1.1

Connection Policy 0

Proxy Redirect

Allow Azure services and resources to access this server (^ **ABB**

Client IP address 8.9.21225.106

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

Explanation:

Question: 286

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

```
{  
  "RoleAssignmentId": "333Sfcbf-3MS-.Sc8a.85b6-dBedd9<s4^
```

```

"Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
"DisplayName": "User1",
"SignInName": "User1@contoso.com",
"RoleId": "Owner",
},
{
  "RoleAssignmentId": "9d080d4-246e-4580-8b8b-077bfe22f7c1",
  "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault", "DisplayName": "User1",
  "SignInName": "User1@contoso.com",
  "RoleId": "KeyVault Crypto Officer",
  "RoleDefinitionName": "(
1 "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault/keys/Key", "DisplayName": "User3",
  "SignInName": "User3@contoso.com",
  "RoleDefinitionName": "Key Vault Secrets Officer",

  "RoleId": "Key Vault Administrator",
  "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa/resourceGroups/RG1/providers/Microsoft.KeyVault/vaults/KeyVault/keys/Key", "DisplayName": "User4",
  "SignInName": "User4@contoso.com",
  "RoleDefinitionName": "Key Vault Administrator",

```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

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

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

Answer: See the answer below at

Explanation.

Explanation:

Answer is as image below.

Answer Area

[Answer choice] can create keys in the key vault. Only User2 and User4

[Answer choice] can create secrets in the key vault. Only User1 and User3

Question: 287

HOTSPOT

You have an Azure subscription that contains a resource group named RG1. RG1 contains a virtual machine named VM1 that uses Azure Active Directory (Azure AD) authentication. You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.

The permissions for Role1 are shown in the following JSON code.

```

"permissions": (
{

```

```

"actions": [
  "Microsoft.Compute/virtualMachines/*"
]
"notActions": [
  "Microsoft-Compute/virtualMachines/delete"
]
"dotaActions": [ ]
"notDataActions": [ ]

```

The permissions for Role2 are shown in the following JSON code:

```

"permissions": [
  "Microsoft.Compute/virtualMachines/*"
]
"actions": [
  "Microsoft.Compute/virtualMachines/delete"
]
"notActions": [ ],
"dataActions": [ ], "notDataActions": [ ]

```

You assign the roles to the users shown in the following table.

Name	Role
User1	Role1
User!	Role2
User?	Role2

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 delete VM1.	<input type="radio"/>	<input type="radio"/>
User? can delete VM1.	<input type="radio"/>	<input type="radio"/>
User3 can sign in to VM1 by using Azure AD credentials.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Answer Area

Question: 288

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

Basic
s

Scope

Azure Pass - Sponsorship/RG1

Exclusions

Azure Pass - Sponsorship/RG1/NSG1

Policy definition

Flow logs should be enabled for every network security

Assignment name

group flow logs should be enabled for every network

Description

security group Description 1

Policy
enforcement

Enabled

Assigned by

Adminl

Parameters

effect

Audit

Remediation

Create managed identity

Yes

Managed identity
location

westeurop
e

Create a remediation
task

No

Non-compliance messages

Default non-compliance
message

Message
1

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

Explanation:

Question: 289

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:

Answer: See the answer below at

Explanation.

Explanation:

Answer is as image below.

Answer Area

Deploy: A Windows server and a Windows Event Forwarding subscription

Forward events to Microsoft Sentinel by using: An Azure Log Analytics agent

Question: 290

You have an Azure subscription that contains an Azure SQL database named SQL1 and an Azure key vault named KeyVault1. KeyVault1 stores the keys shown in the following table.

Name	Type	RS A key me	Elliptic one name
Key1	RSA	2048	Curve25519
Key2	RSA*	3072	Curve25519
Key3	RSA	4396	NistP256
Key4	EC	Curve25519	NistP256

You need to configure Transparent Data Encryption (TDE). TDE will use a customer-managed key for SQL1?

- A. Key1, Key2, Key3, and Key4
- B. Key1 only
- C. Key2 only
- D. Key1 and key2 only
- E. Key2 and Key3 only

Answer: E

Explanation:

Question: 291

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

Name	Performance	Account kind	Microsoft Defender for Storage
storage1	Standard	BlobStorage	Enabled
storageZ	Premium	BlockBlobStorage	Disabled
storage?	Standard	Storage	Disabled
storage-!	premium	Filestorage	Disabled
storages	Standard	StorageV2	Enabled

You enable Microsoft Defender for Storage.

Which storage services of storages are monitored by Microsoft Defender for Storage, and which storage accounts are protected by Microsoft Defender for Storage? To answer, select the appropriate options in the answer area.

Answer Area

Monitored storages services:

Protected storage accounts:

Answer: see the answer below in explanation.

Explanation:

Answer as below.

Answer Area

Monitored storages services: File services and table services only

Protected storage accounts: storage1, storage4, and storages only

Question: 292

HOTSPOT

You have a management group named MG1 that contains an Azure subscription and a resource group named RG1. RG1 contains a virtual machine named VM1. You have the custom Azure roles shown in the following table.

Name	Scoped to
Role1	MG1
Role2	RG1

The permissions for Role1 are shown in the following role definition file.

permissions: [c

"Microsoft.Compute/virtualMachines/*"

"notActions": [

"Microsoft.Compute/virtualMachines/delete" K "dateActions": (J

The pen > *)> * « » > « Ji "rtovtcrarc^ n n^s. i't r3>c »umswi**y ssme MCTiim*uvi me works.com

"permissions": (

"actions": ("Microsoft.Compute/virtualMachines/*"

h/"notActions": [], "dotActions": [], "notOataAetions": [] works.com

You assign the roles to the users shown in the following table.

Name	Role
User1	Role1
User2	Role1, Role2
User3	Role2

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
User 1 can delete VM1.	<input type="radio"/>
User? can delete VM1.	<input type="radio"/>
User3 can delete VM1.	<input type="radio"/>

Answer:

Explanation:

Answer Area

Statements	Yaa	Ne
Uteri can delete VM1	<input type="radio"/>	<input type="radio"/>
user? can deme VMI	<input type="radio"/>	<input type="radio"/>
Ute«3 can delete VM»	<input type="radio"/>	<input type="radio"/>

Question: 293

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 /Subnet?	NSG2
VM3	Central US	VNE ~2/Subnet1	NSG3
VM4	West US	VNET 3/Subnet 1	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:

Answer: see the answer below in explanation.

Explanation:

Answer as below.
Answer Area

ASG1: VM2, VM 3, and VM4 only

ASG2: VM 1, VM2, and VM4 only

Question: 294

You have 15 Azure virtual machines in a resource group named RG1.

All virtual machines run identical applications.

You need to prevent unauthorized applications and malware from running on the virtual machines.

What should you do?

- A. Configure Azure Active Directory (Azure AD) Identity Protection.
- B. From Microsoft Defender for Cloud, configure adaptive application controls.
- C. Apply an Azure policy to RG1.
- D. Apply a resource lock to RG1.

Answer: B

Explanation:

Microsoft Defender for Cloud helps you prevent, detect, and respond to threats. Defender for Cloud gives you increased visibility into, and control over, the security of your Azure resources. It provides

integrated security monitoring and policy management across your Azure subscriptions. It helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.

Defender for Cloud helps you optimize and monitor the security of your virtual machines by: Providing security recommendations for the virtual machines. Example recommendations include: apply system updates, configure ACLs endpoints, enable antimalware, enable network security groups, and apply disk encryption.

Monitoring the state of your virtual machines.

<https://learn.microsoft.com/en-us/azure/security/fundamentals/virtual-machines-overview>

Question: 295

HOTSPOT

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

Name	Days to retain deleted vaults	Purge protection	Permission model
KeyVault1	10	Enabled	Azure role-based access control (Azure RSAQ)
KeyVault2	15	Disabled	Azure role-based access control (Azure RBAQ)

The subscription contains the users shown in the following table.

Name	Role	Assigned to
Admin;	Key Vault Contributor	KeyVault1
Ad mm2	Key Vault Secrets Officer	Key Vault?
Admin3	Key Vault Administrator	KeyVault1

On June 1, you perform the following actions:

- Delete a key named key1 from KeyVault1.
- Delete a secret named secret 1 from KeyVault2.

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

Statements

Yes

No

Admin1 can recover key! on June 5.

Admin2 can purge secret! on June 12.

Admin3 can recover key 1 on June 17.

Answer:

Explanation:

Yes

Yes

No

Question: 296

HOTSPOT

You have an Azure subscription that contains a blob container named cont1. Cont1 has the access policies shown in the following exhibit.

Ss™

Stored access policies

Identifier Start time

Expiry time Permissions

Pohcyl

T Add policy

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

The maximum number of additional stored access policies that you can add to a container is [answer choice].



The maximum number of additional immutable blob storage policies that you can add to a container is [answer choice].

- 2
- 4
- 7

Answer:

Explanation:

The maximum number of additional stored access policies that you can add to a container is [answer choice].

The maximum number of additional immutable blob storage policies that you can add to a container is [answer choice].

Question: 297

You have an Azure environment.

You need to identify any Azure configurations and workloads that are non-compliant with ISO 27001:2013 standards.

What should you use?

- A. Azure Active Directory (Azure AD) Identity Protection
- B. Microsoft Defender for Cloud
- C. Microsoft Defender for Identity

D. Microsoft Sentinel

Answer: B

Explanation:

Question: 298

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

Explanation:

Question: 299

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 2.0
- 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->

enable?tabs=azure-portal

Question: 300

You have an Azure Active Directory (Azure AD) tenant. The tenant contains users that are assigned Azure AD Premium Plan 2 licenses.

You have a partner company that has a domain named The fabrikam.com domain contains a user named user1. User1 has an email address of user1@fabrikam.com.

You need to provide User1 with access to the resources in the tenant. The solution must meet the following requirements:

- user1 must be able to sign in by using the user1@fabrikam.com credentials
 - You must be able to grant User1 access to the resources in the tenant
 - Administrative effort must be minimized.
- What should you do?

- A. Create a user account for user1.
- B. Create an invite for User1.
- C. To the tenant add fabrikam.com as a custom domain
- D. Set Enable guest self-service sign up via user flows to Yes for the tenant.

Answer: B

Explanation:

Question: 301

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

Explanation:

Question: 302

HOTSPOT

You have an Azure subscription that contains a user named User1 and a storage account named storage1. The storage1 account contains the resources shown in the following table:

Name	Type
container1	Container
folder1	File share

table!	Table
--------	-------

User1 is assigned the following roles for storage1:

- Storage Blob Data Reader
- Storage Table Data Contributor
- Storage File Data SMB Share Reader

Statements

Yes

No

On October 1, 2022, if User1 accesses folder! by using SAS1 he can delete the files in folder!.

On October 1, 2022, if User1 maps folder! as a network drive by using his Azure Active Directory 'Azure AD' credentials he can delete the files in folder!.

On October 1, 2022, User! can delete the rows in table! by using SAS!.

Answer:

Explanation:

No, Yes, No

Question: 303

You have an Azure subscription that contains a web app named App1.

Users must be able to select between a Google identity or a Microsoft identity when authenticating to App1.

You need to add Google as an identity provider in Azure AD.

Which two pieces of information should you configure? Each correct answer presents part of the solution.

Each correct selection is worth one point

- A. a tenant name
- B. a tenant ID
- C. the endpoint URL Of an application
- D. a client ID
- E. a client secret

Answer: D,E

Explanation:

<https://learn.microsoft.com/en-us/azure/app-service/configure-authentication-provider-google>

Question: 304

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

Name	Type
Kfy1	Key
Secret 1	Secret
Cen1	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

Explanation:

Question: 305

You have an Azure subscription that contains a

You need to grant user1 access to blob1. The solution must ensure that the access expires after six days.

What should you use?

- A. a shared access policy
- B. a shared access signature (SAS)
- C. role-based access control (RBAC)
- D. a managed identity

Answer: B

Explanation:

Depending on how you want to authorize access to blob data in the Azure portal, you'll need specific

permissions. In most cases, these permissions are provided via Azure role-based access control (Azure RBAC). For more information about Azure RBAC, see [What is Azure role-based access control \(Azure RBAC\)?](#).

<https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal>

Question: 306

HOTSPOT

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

Name	Connected to	Private IP address	Public IP address
------	--------------	--------------------	-------------------

VM1	VNET1/Subnet1 I	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.12.5.	20.224.2192.30
VM3 j	VNET2/Subneti	10.11.1.5	40.122.155212

You have an Azure Cosmos DB account named cosmos1 configured as shown in the following exhibit.

AUcHA access from

f) AI networks • Selected networks

Statements

Yes

No

VM1 can access cosmos 1 over the internet

VM2 can access cosmosl over the internet.

VMS can access cosmosl over the internet.

Answer:

Explanation:

Yes, Yes, No

Question: 307
HOTSPOT

You have an Azure AD tenant named contoso.com that has Azure AD Premium P1 licenses.

You need to create a group named Group1 that will be assigned the Global reader role.

Which portal should you use to create Group1 and which type of group should you create? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

Portal:

The Azure Active Directory admin center only

The Microsoft 365 admin center only

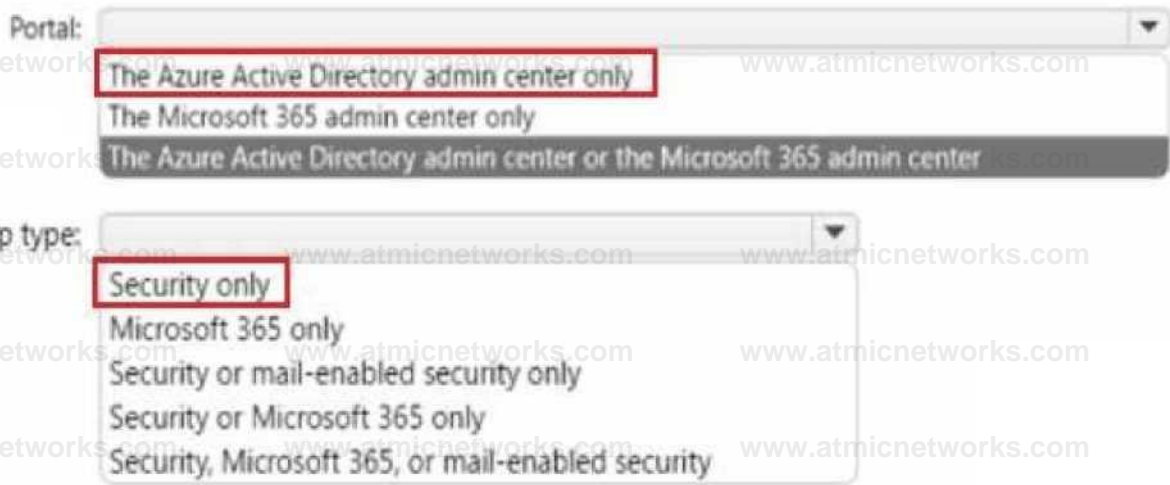
The Azure Active Directory admin center or the Microsoft 365 admin center

Group type:

- Security only
- Microsoft 365 only
- Security or mail-enabled security only
- Security or Microsoft 365 only
- Security, Microsoft 365, or mail-enabled security

Answer:

Explanation:



<https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible>

Question: 308

HOTSPOT

Your on-premises network contains the servers shown in the following table.

Name	Operating system	Description
Server1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server2	Windows Server 2019	File server that has the Azure Arc agent installed
Server3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent installed

You have an Azure subscription That contains multiple virtual machines that run either Windows Server 2019 Of SLES.

Operating systems: [_____]

SLES only

Windows Server only SLES and Windows Server

Platforms:

Azure virtual machines only

Azure virtual machines and Hyper-V virtual machines only

Azure Arc-enabled servers and Azure virtual machines only

Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled server

Answer:

Explanation:

Operating systems: [_____]

SLES only

Windows Server only | SLES and Windows Server |

Platforms:

Azure virtual machines only

Azure virtual machines and Hyper-V virtual machines only

Azure Arc-enabled servers and Azure virtual machines only

Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

Question: 309

You have an Azure subscription that contains an Azure key vault.

You need to configure maximum number of days for Which new keys are valid. The solution must minimize administrative effort.

What should you use?

- A. Key Vault properties
- B. Azure Policy
- C. Azure Purview
- D. Azure Blueprints

Answer: B

Explanation:

Question: 310

HOTSPOT

You have the role assignments shown in the following exhibit.

```

"RoleDefinitionId": "13e6e22-W31412f4c1c5-fc82b1726Me",
"Scope": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/resourceGroups/RGI",
"DisplayName": "Admin",
"SignInName": "Admin@contoso.co",
"RoleDefinitionName": "Owner",
"RoleDefinitionId": "/subscriptions/8abaf97-8be4-424a-92fa-873c5a45fbbc/provider/

```

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

NOTE: Each correct selection is worth one point.

(answer choice) can delete VM1. (_____)

- Only Admin 1
- Only Admin 1 and Admin 2
- Only Admin 1 and Admin 3
- Only Admin 1 and Admin 4
- Admin 1, Admin 2, Admin 3, and Admin 4

[answer choice] can create new resource groups. (_____)

- Admin 1 only
- Admin 2 only
- Admin 3 only
- Admin 1 and Admin 3 only
- Admin 1, Admin 2, Admin 3, and Admin 4

Answer:

Explanation:

Only Admin1 and Admin2

Admin3 only

Question: 311

HOTSPOT

Your on-premises network contains the servers shown in the following table.

Name	Operating system	Description
Server 1	Windows Server 2019	Hyper-V host hosting four virtual machines that run Windows Server 2022
Server 2	Windows Server 2019	File server that has the Azure Arc agent installed
Server 3	SUSE Linux Enterprise Server (SLES)	Database server that has the Azure Arc agent installed

You have an Azure subscription that contains multiple virtual machines that run either Windows Server 2019 or SLES. You plan to implement adaptive application controls in Microsoft Defender for Cloud. Which operating systems and platforms can you monitor? To answer, select the appropriate options in the answer area.

Operating systems:

SLES only

Windows Server only

SLES and Windows Server



Platforms:

Azure virtual machines only

Azure virtual machines and Hyper-V virtual machines only

Azure Arc-enabled servers and Azure virtual machines only

Azure virtual machines, Hyper-V virtual machines, and Azure Arc-enabled servers

ibw we the lelettniw foe Pletfanni.

Answer:

Explanation:

Windows Server only

Azure virtual machines only

Question: 312

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

Name	Type
Key1	Key
Secret1	Secret
CM1	Certificate

Which resources support the creation of a rotation policy?

- A. Key 1 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: A

Explanation:

Question: 313

You have an Azure subscription that contains an Azure SQL server named SQL1. SQL1 contains. You need to use Microsoft Defender for Cloud to complete a vulnerability assessment for DB1. What should you do first?

- A. From Advanced Threat Protection types, select SQL injection vulnerability.
- B. Configure the Send scan report to setting.
- C. Set Periodic recurring scans to ON.
- D. Enable the Microsoft Defender for SQL plan.

Answer: A

Explanation:

Question: 314

You have an Azure AD tenant that contains 500 users and an administrative unit named AU1.

From the Azure Active Directory admin center, you plan to add the users to AU1 by using Bulk add members.

You need to create and upload a file for the bulk add.

What should you include in the file?

- A. only the display name of each user
- B. only the user principal name (UPN) of each user
- C. only the object identifier of each user
- D. only the user principal name (UPN) and object identifier of each user
- E. Only the user principal name (UPN) and display name of each user

Answer: E

Explanation:

Question: 315

You have an Azure subscription that contains a user named User1. You need to ensure that User1 can create managed identities. The solution must use the principle of least privilege.

What should you do?

- A. Create a resource group and assign User1 to the Managed Identity Contributor role.
- B. Create a management group and assign User1 the Managed Identity Operator role.
- C. Create an organizational unit (OU) and assign User1 the User administrator Azure AD role.
- D. Create management group and assign User1 the Hybrid Identity Administrator Azure AD role.

Answer: A

Explanation:

Question: 316

HOTSPOT

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

Name	Type
RG1	Resource group
VM1	Virtual machine

You perform the following tasks:

Create a managed identity named Managed1.

Create a Microsoft 365 group named Group1.

You need to identify which service principals were created and which identities can be assigned the Reader role for RG1.

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

Answer Area

Service Principals:

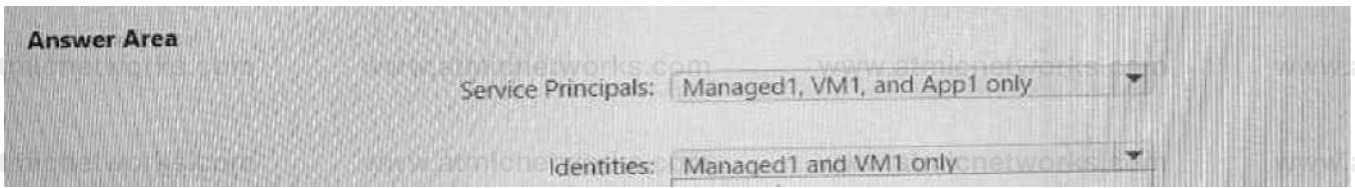
- Managed1, VM1, and App1 only
- App1 only
- Managed1 and VM1 only
- Managed1, VM1, and App1 only**
- Managed1, VM1, App1, and Group1

Identities:

- Managed1 and VM1 only
- App1 only
- Managed1 and VM1 only**
- Managed1, VM1, and App1 only
- Managed1, VM1, App1, and Group1

Answer:

Explanation:



Question: 317

DRAG DROP

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

Name	User device
User1	Android mobile device with facial recognition
User2	Windows device with Windows Hello for Business-compatible hardware

You enable passwordless authentication for the tenant.

Which authentication method can each user use for passwordless authentication? To answer, drag the appropriate authentication methods to the correct users. Each authentication method 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.

The screenshot shows an 'Authentication methods' pane on the left and an 'Answer Area' on the right. The 'Authentication methods' pane contains six options:

- FIDO2 security key only
- Microsoft Authenticator app only
- Windows Hello for Business only
- Microsoft Authenticator app and Windows Hello for Business only
- Windows Hello for Business and FIDO2 security key only
- Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key

The 'Answer Area' has two empty boxes for 'User1:' and 'User2:'.

Answer:

Explanation:

Authentication methods	Answer Area
FIDO2 security key only	User1: Microsoft Authenticator app only
Microsoft Authenticator app only	User2: Windows Hello for Business only
Windows Hello for Business only	
Microsoft Authenticator app and Windows Hello for Business only	
Windows Hello for Business and FIDO2 security key only	
Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key	

Question: 318

HOTSPOT

You have an Azure subscription named Sub1 that contains the resource groups shown in the following table.

Name	Location
RG1	West US
RG2	East US

You create the Azure Policy definition shown in the following exhibit.

Code: "ill policyBul*F
I*! {

"anyOf": {
(

field! "locrtipn * "no t f q ^ a 15 " : *{res6uf<eGrQup().lateticmj

"fi<ld"i -^(W, "notCent•ins": "odj"

L
Rthen: { "tY-tcf"; "cen-*

Mr«*et«rB*t O

You assign the policy to Sub1.

You plan to create the resources shown in the following table.

Name	Type	Location	Resource group
iPobject 1	Public IP address	East US	RG2
obj1	Resource group	West US	wof 0V0Aco6te
OBB	Virtual network	west us	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.

Answer Area

Statement*

Yes

No

You can create iPobject1

You can create obj1

You can create OBB.

Answer:

Explanation:

Answer Area

Statements

Yes

No

you can create iPobject

YOU can create obj 1.

*ou can create OBJ3

Question: 319

HOTSPOT

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

Name	Type
SQL1	Azure SQL Database server
DB1	Azure SQL database on SQL1
DB2	Azure SQL database on SQL1
storage1	Storage account
storage2	Storage account
Workspace1	Log Analytics workspace

SQL1 has the following configurations:

- Auditing: Enabled
- Audit log destination: storage1, Workspace1

DB1 has the following configurations:

- Auditing: Enabled
- Audit log destination: storage2

DB2 has auditing disabled.

Where are the audit logs for DB1 and DB2 stored? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point.

Answer Area

DB1: storage1, storage2, and Workspace1
 storage2 only
 storage1 and Workspace1 only
 storage2 and Workspace1 only
 storage1, storage2, and Workspace1

DB2: Workspace1 only
 No audit logs created
 storage1 only
 Workspace1 only
 storage1 and Workspace1

Answer:

Explanation:

Answer Area

OBI: storage1 storage? and Workspace!

Question: 320

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 sql4 only
- D. sql1, sql2, sql3, and sql4

Answer: D

Explanation:

Question: 321

You have an Azure subscription that contains an Azure Data Lake Storage Gen2 account named storage1. You deploy an Azure Synapse Analytics workspace named synapsews1 to a managed virtual network. You need to enable access from synapsews1 to storage1. What should you configure?

- A. a virtual network gateway
- B. a network security group (NSG)
- C. a private endpoint
- D. peering

Answer: C

Explanation:

Question: 322**HOTSPOT**

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

Subnet1 and Subnet2 have a network security group (NSG). The NSG has an outbound rule that has the following configurations:

- Port: Any
- Source: Any
- Priority: 100
- Action: Deny
- Protocol: Any
- Destination: Storage

The subscription contains a storage account named storage1.

You create a private endpoint named Private1 that has the following settings:

- Resource type: Microsoft.Storage/storageAccounts
- Resource: storage1
- Target sub-resource: blob
- Virtual network: VNet1
- Subnet: Subnet1

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 VM2, you can create a container in storage!		
From VM1, you can upload data to the blob storage of storage!	0	0
From VM2, you can upload data to the blob storage of storage!	0	0

Answer:

Explanation:

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage!		<input checked="" type="radio"/>
From VM1, you can upload data to the blob storage of storage!	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can upload data to the blob storage of storage!	<input type="radio"/>	<input checked="" type="radio"/>

Question: 323

You have an Azure subscription.

You create a new virtual network named VNet1.

You plan to deploy an Azure web app named App1 that will use VNet1 and will be reachable by using private IP addresses.

The solution must support inbound and outbound network traffic.

What should you do?

- A. Create an Azure App Service Hybrid Connection.
- B. Configure regional virtual network integration.
- C. Create an App Service Environment
- D. Create an Azure application gateway.

Answer: C

Explanation:

Question: 324

HOTSPOT

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

Name	Type	Location	In resource group
RG1	Resource group	East US	Not applicable
RG2	Resource group	West US	Not applicable
RG3	Resource group	Central US	Not applicable
VNet1	Virtual network	Central US	RG2

VNet1 contains the subnets shown in the following table.

Name	Description
AzureFireAdil	Contains no resources
AzureFirewallSubnet	Contains no resources
Subnet 1	Contains a virtual machine
Subnet?	Contains no resources

You plan to use the Azure portal to deploy an Azure firewall named AzFW1 to VNet1.

Which resource group and subnet can you use to deploy AzFW1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Resource group:



Subnet: AzureFirewallSubnet or?

AzureFirewall only

AzureFirewallSubnet only

AzureFirewall or AzureFirewallSubnet only AzureFirewall.

AzureFirewallSubnet, or Subnet? only AzureFirewall.

AzureFirewallSubnet, Subnet!, or Subnet?

Answer:

Explanation:

Answer Area

Resource group: RG2

Subnet: AzureFirewallSubnet only

Question: 325

DRAG DROP

You have an Azure subscription that contains an Azure web app named Appl.

You plan to configure a Conditional Access policy for Appl. The solution must meet the following requirements:

- Only allow access to App1 from Windows devices.
- Only allow devices that are marked as compliant to access Appl.

Which Conditional Access policy settings should you configure? To answer, drag the appropriate settings to the correct requirements. Each setting may be used once, more than once, or not at all.

You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Poiky sett ings

Answer Area

Cloud apps or actions
Conditions
Grant
Session

Only allow access to App1 from Windows devices:

Only allow devices that are marked as compliant to access Appt:

Answer:

Explanation:

Policy

Answer Area

Cloud apps or actions
Conditions
Grant
Session

Only allow access to Appt from Windows devices: Conditions

Only allow devices that are marked as compliant to access App 1: Conditions

Question: 326

You have an Azure subscription that contains an instance of Azure Firewall Standard named AzFW1

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: A

Explanation:

Question: 327

You have an Azure subscription that contains a storage account named storage1 and a virtual machine named VM1. VM1 is connected to a virtual network named VNet1 that contains one subnet and uses Azure DNS. You need to ensure that VM1 connects to storage1 by using a private IP address. The solution must minimize administrative effort.

What should you do?

- A. For storage1, disable public network access.
- B. Create an Azure Private DNS zone.
- C. On VNet1, create a new subnet.
- D. For storage1, create a new private endpoint.

Answer: D

Explanation:

Question: 328

HOTSPOT

You have an Azure subscription that is linked to an Azure AD tenant and contains the virtual machines shown in the following table.

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.11.5	20224.219.170
VM2	VNET1/Subnet2	10.1.25	20224.219.230
VMS	VNET2/Subnet1	10.11.15	40.122.155212

The subnets of the virtual networks have the service endpoints shown in the following table.

Subnet	Service endpoint
VNET1/Subnet1	MicrosoftStorage
VNET1/Subnet2	Microsoft KeyVault
VNET2/Subnet1	MicrosoftStorage, MicrosoftKeyVault

You create the resources shown in the following table.

Name	Type
storage1	Azure Storage account
Vault1	Azure Key Vault

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

Connections from VM1 to storage1 always use IP address 10.1.1.5.

Connections from VM2 to Vault1 always use IP address 20.224.219.230.

Authentication from VMS to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.

Answer:

Explanation:

Answer Area Statements

Yes

No

Connection! from VM1 to storage1 always use IP address 10.1.1.5,

To which resources can User1 write on July 1, 2022 by using SAS1 and key 1? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

SAS1: container and folder1 only

Key1: container1, folder1, and table1

Question: 330

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

Explanation:

Question: 331

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
Served	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: D

Explanation:

Question: 332

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. GDPR Compliance
- C. Security Posture
- D. OWASP Top 10

Answer: D

Explanation:

Question: 333

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: B

Explanation:

Question: 334

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: B

Explanation:

Question: 335

HOTSPOT

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		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:



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



Answer

Explanation:

Answer Area

Total number of Microsoft Defender for Cloud email notifications about an RDP brute force attack 4 on Tuesday;

Total number of Microsoft Defender for Cloud email notifications on Tuesday: 7

Question: 336
SIMULATION

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 1

You need to configure Azure to allow RDP connections from the Internet to a virtual machine named VM1. The solution must minimize the attack surface of VM1.

**Answer: Check below
steps in explanation
for Task.**

Explanation:

To configure Azure to allow RDP connections from the Internet to a virtual machine named VM1, you can follow the steps below:

Create a new inbound security rule in the network security group (NSG) that is associated with the virtual network subnet that contains VM1. The rule should allow RDP traffic from the Internet to the virtual network subnet. You can use the Azure portal, Azure PowerShell, or Azure CLI to create the rule.

Configure the network security group (NSG) to associate it with the virtual network subnet that contains VM1.

Configure the virtual machine to allow RDP traffic. You can use the Azure portal, Azure PowerShell, or Azure CLI to configure the virtual machine.

To minimize the attack surface of VM1, you can use the following best practices:

Use a strong password for the local administrator account on the virtual machine.

Use Network Security Groups (NSGs) to restrict traffic to only the necessary ports and protocols.

Use Azure Security Center to monitor and protect your virtual machines.

Question: 337

SIMULATION

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 2

You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.

Answer: Check below steps in explanation for Task.

Explanation:

To add the network interface of a virtual machine named VM1 to an application security group named ASG1, you can follow these steps:

In the Azure portal, search for and select the virtual machine named VM1.

In the left pane, select Networking.

In the Networking pane, select the network interface that you want to add to the application security group named ASG1.

In the network interface pane, select Application security groups.

In the Application security groups pane, select Add.

In the Add application security group pane, select the application security group named ASG1.

Select Save.

You can find more information on this topic in the following Microsoft documentation: [Add a network interface to an application security group using the Azure portal.](#)

Question: 338

SIMULATION

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 3

The developers at your company plan to create a web app named App28681041 and to publish the app to <https://www.contoso.com>. You need to perform the following tasks:

- Ensure that App28681041 is registered to Azure AD.
- Generate a password for App28681041.

**Answer: Check below
steps in explanation
for Task.**

Explanation:

To register App28681041 to Azure AD and generate a password for it, you can follow these steps:

In the Azure portal, search for and select Azure Active Directory.

In the left pane, select App registrations.

Select New registration.

In the Register an application pane, enter the following information:

Name: App28681041

Supported account types: Select the appropriate account types for your scenario.

Redirect URI: Leave this field blank.

Select Register.

In the App registrations pane, select the newly created App28681041 application.

In the left pane, select Certificates & secrets.

Select New client secret.

In the Add a client secret pane, enter the following information:

Description: Enter a description for the client secret.

Expires: Select an appropriate expiration date for the client secret.

Select Add.

In the Certificates & secrets pane, copy the value of the newly created client secret.

You can find more information on this topic in the following Microsoft documentation: [Quickstart: Register an application with the Microsoft identity platform](#).

Question: 339

SIMULATION

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 4

You need to ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group. The solution must use the principle of least privilege.

**Answer: Check below
steps in explanation
for Task.**

Explanation:

To ensure that a user named user2-28681041 can manage the properties of the virtual machines in the RG1lod28681041 resource group using the principle of least privilege, you can follow these steps: In the Azure portal, search for and select the resource group named RG1lod28681041.

In the left pane, select Access control (IAM).

Select Add.

In the Add role assignment pane, enter the following information:

Role: Select the appropriate role for your scenario. For example, Virtual Machine Contributor.

Assign access to: Select User, group, or service principal.

Select: Enter the name of the user you want to assign the role to. For example, user2-28681041. Select Save.

<https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal>

Question: 340

SIMULATION

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 5

You need to ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account.

Answer: Check below
steps in explanation
for Task.

Explanation:

To ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account, you can follow these steps:

In the Azure portal, search for and select the storage account named rg1lod28681041.

In the left pane, select Firewalls and virtual networks.

In the Firewalls and virtual networks pane, select Selected networks.

In the Selected networks pane, select Add existing virtual network.

In the Add existing virtual network pane, select the virtual network that contains the 131-107.0.0/16 subnet.

Select Add.

<https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>

Question: 341

SIMULATION

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: GpO Ae4@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.

Answer: Check below
steps in explanation
for Task.

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.

Question: 342

SIMULATION

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 7

You need to collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account. To complete this task, sign in to the Azure portal.

Answer: Check below
steps in explanation
for Task.

Explanation:

To collect all the audit failure data from the security log of a virtual machine named VM1 to an Azure Storage account, you can follow these steps:

In the Azure portal, search for and select the virtual machine named VM1.

In the left pane, select Diagnostic settings.

Select Add diagnostic setting.

In the Add diagnostic setting pane, enter the following information:

Name: Enter a name for the diagnostic setting.

Destination: Select Storage account.

Storage account: Select the storage account you want to use.

Logs: Select Windows Event Logs.

Categories: Select Security.

Event types: Select Audit Failure.

Select Save.

Question: 343

SIMULATION

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 8

You need to prevent HTTP connections to the rg1lod28681041n1 Azure Storage account.

Answer: Check below
steps in explanation
for Task.

Explanation:

To prevent HTTP connections to the rg1lod28681041n1 Azure Storage account, you can follow these steps:

In the Azure portal, search for and select the storage account named rg1lod28681041n1.

In the left pane, select Firewalls and virtual networks.

In the Firewalls and virtual networks pane, select Selected networks.

In the Selected networks pane, select Add existing virtual network.

In the Add existing virtual network pane, select the virtual network that does not allow HTTP connections.

Select Add.

Question: 344

SIMULATION

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 9

You need to ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault.

**Answer: Check below
steps in explanation
for Task.**

Explanation:

To ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault, you can follow these steps:

In the Azure portal, search for and select the storage account named rg1lod28681041n1.

In the left pane, select Encryption.

In the Encryption pane, select Customer-managed key.

In the Customer-managed key pane, select Select from Key Vault.

In the Select from Key Vault pane, enter the following information:

Key vault: Select the KeyVault28681041 Azure key vault.

Key: Select the key you want to use.

Select Save.

Question: 345

SIMULATION

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 10

You need to create a new Azure AD directory named 28681041.onmicrosoft.com. The new directory must contain a new user named user1@28681041.onmicrosoft.com.

**Answer: Check below
steps in explanation
for Task.**

Explanation:

To create a new Azure AD directory named 28681041.onmicrosoft.com that contains a new user named user1@28681041.onmicrosoft.com, you can follow these steps:

In the Azure portal, search for and select Azure Active Directory.

In the left pane, select Domains.

Select Add domain.

In the Add a custom domain pane, enter the following information:

Domain name: Enter the domain name you want to use. For example, 28681041.onmicrosoft.com.

Add domain: Select Add domain.

In the left pane, select Users.

Select New user.

In the New user pane, enter the following information:

User name: Enter the user name you want to use. For example, user1@28681041.onmicrosoft.com.

Name: Enter the name of the user.

Password: Enter a password for the user.

Groups: Select the groups you want the user to be a member of.

Select Create.

You can find more information on these topics in the following Microsoft documentation:

Add a custom domain name to Azure Active Directory

Create a new user in your organization - Azure Active Directory

Question: 346

Your on-premises network contains a Hyper-V virtual machine named VM1. You need to use Azure Arc to onboard VM1 to Microsoft Defender for Cloud. What should you install first?

- A. the Azure Monitor agent
- B. the Azure Connected Machine agent
- C. the Log Analytics agent
- D. the guest configuration agent

Answer: C

Explanation:

Question: 347

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

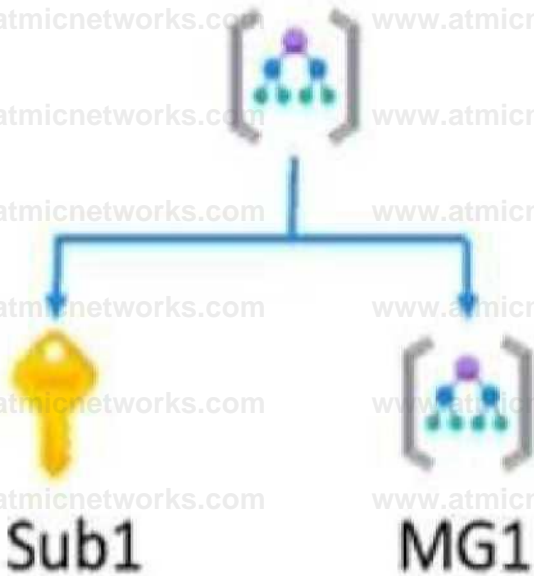
Answer: D

Explanation:

Question: 348

You have an Azure subscription named Sub1 that uses Microsoft Defender for Cloud. You have the management group hierarchy shown in the following exhibit.

Tenant Root Group



You create the definitions shown in the following table.

Name	Location	Type
Policy1	Sub1	Policy
Initiative1	Tenant Root Group	Initiative
Initiative2	Sub1	Initiative
Initiative3	MG1	Initiative

You need to use Defender for Cloud to add a security policy. Which definitions can you use as a security policy?

- A. Policy1 only
- B. Policy1 and Initiative1 only
- C. Initiative1 and Initiative2 only
- D. Initiative1, Initiative2, and Initiatives only
- E. Policy1, Initiative1, Initiative2, and Initiative3

Answer: B

Explanation:

Question: 349

You have an Azure subscription that uses Azure AD Privileged Identity Management (PIM).

A user named User1 is eligible for the Billing administrator role.

You need to ensure that the role can only be used for a maximum of two hours.

What should you do?

- A. Create a new access review.
- B. Edit the role assignment settings.
- C. Update the end date of the user assignment
- D. Edit the role activation settings.

Answer: B

Explanation:

Question: 350

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

Name	
storage 1	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:StorageAccountmanagementPolicyAction
- C. Set-A:StorageAccountmanagementPolicy
- D. Add-AsKeyVaultmanageStorageAccount

Answer: D

Explanation:

Question: 351

You have an Azure subscription that contains a web app named Appl. App1 provides users with product images and videos. Users access App1 by using a URL of HTTPS://appl.contoso.com. You deploy two server pools named Pool1 and Pool2. Pool1 hosts product images. Pool2 hosts product videos. You need to optimize The performance of Appl. The solution must meet the following requirements:

- Minimize the performance impact of TLS connections on Pool1 and Pool2.
- Route user requests to the server pools based on the requested URL path.

What should you include in the solution?

- A. Azure Traffic Manager
- B. Azure Bastion
- C. Azure Application Gateway
- D. Azure Front Door

Answer: C

Explanation:

Question: 352

HOTSPOT

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	VneB
Vnet2	East US	10.2.0.0/16	Vnet1, VneB
VneB	West US	10.3.0.0/16	VneB,

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
AzureFirewallSubne	Vnet1	10.1.3.0/24
Subnet/-1	Vne-2	10.2.1.0/24
SubneB-1	VneB	103.1.0/24

The subscription contains the routes shown in the following table.

Name	Subnet	IP address prefix	Next hop type	Next hop IP address
Rt1	Subnet1-	0.0.0.0/0	Virtual appliance	10.13.4
Rt2	Subnet 1-2	10.1.1.0/24	Virtual appliance	10.13.4
Rt3	Subnet2-1	10.1.1.0/24	Virtual appliance	10.13.4
Rt4	SubneB-1	10.2.1.0/24	Virtual appliance	10.13.4

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 Subnet 1-1 to Subnet 1-3 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 Subnets-1 to the internet is routed through Fw1.	<input checked="" type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Answer Area

Statements	Yes	No
Traffic from Subnet1-1 to Subnet 1-3 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 SubnetJ-1 to the internet is routed through Fw1.	<input checked="" type="radio"/>	<input type="radio"/>

Question: 353

DRAG DROP

You have an Azure subscription.

You plan to create two custom roles named Role1 and Role2.

The custom roles will be used to perform the following tasks:

- Members of Role1 will manage application security groups.
- Members of Role2 will manage Azure Bastion.

You need to add permissions to the custom roles.

Which resource provider should you use for each role? To answer, drag the appropriate resource providers to the correct roles. Each resource provider 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

Resource Providers

Microsoft.Compute

Microsoft.Network

Microsoft.Security

Microsoft.Solutions

Answer Area

Answer:

Explanation:

Resource Providers

Microsoft.Compute

Microsoft.Network

Microsoft.Security

Microsoft.Solutions

Answer Area

Role1: | Microsoft Network
 Role2: | Microsoft-Network

Question: 354

You have an Azure subscription that contains a resource group named RG1 and a security group named ServerAdmins. RG1 contains 10 virtual machines, a virtual network named VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.

You need to ensure that NSG1 only allows RDP connections to the virtual machines for a maximum of 60 minutes when a member of ServerAdmins requests access.

What should you configure?

- A. an Azure policy assigned to RG1
- B. a just in time (JIT) VM access policy in Microsoft Defender for Cloud
- C. an Azure AD Privileged Identity Management (PiM) role assignment
- D. an Azure Bastion host on VNET1

Answer: B

Explanation:

Question: 355

DRAG DROP

You have two Azure subscriptions named Sub1 and Sub2. Sub1 contains a resource group named RG1 and an Azure policy named Policy1.

You need to remediate the non-compliant resources in Sub1 based on Policy1.

How should you complete the PowerShell script? To answer, drag the appropriate values to the correct targets.

Each value 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.

Values

Get-AzPolicyRemediation

Set-AzContext

Set-AzResourceGroup

Start-AzPolicyComplianceScan

Start-AzPolicyRemediation

Answer Area

\$policyAssignmentId - "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization?f

Value

-Subscription "Sub1"

Value

-PolicyAssignmentId \$policyAssignmentId -Name "policy1" -ResourceDiscovery

Answer:

Explanation:

For the first blank, use Set-AzContext to set the current subscription context.

For the second blank, use Start-AzPolicyRemediation to create and start a policy remediation for a policy assignment.

The final script should look like this:

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-1978-
```

```
1b4be01e86a5/providers/Microsoft.Authorization/f Value Set-AzContext -Subscription "Sub1"
```

```
Value Start-AzPolicyRemediation -PolicyAssignmentId $policyAssignmentId -Name "policy1" - ResourceDiscovery
```

Question: 356

HOTSPOT

You plan to deploy a custom policy initiative for Microsoft Defender for Cloud.

You need to identify all the resource groups that have a Delete lock.

How should you complete the policy definition? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

••«

```
"policyRule": {
  "if": {
    "field": "type",
    "equals": "Microsoft.Resources/subscriptions/
      Microsoft.Resources/subscriptions/
      Microsoft.Resources/subscriptions/resourceGroups"
    *
  }
  "effect": "auditIfBotchists",
  "details": (
    "type": "Microsoft.Authorization/locks",
    "existenceCondition": [
      "existenceCondition"
    ]
    "operations": [
      "value"
    ]
    "field": "Microsoft.Authorization/locks/level",
    "equals": "CanHotDelete"
  )
}
```

Answer:

Explanation:

Answer Area

```
"policyRule": {
```

```
  "if": (
```

```
    "field": "type",
```

```
    "equals":
```

```
      "MicrosoftResources^subscription<^^^^^^^^^^"
```

```

"then": {
  "resourceGroups":
    "effect": "auditIfNotExists", "details": {
      "type": "Microsoft.Authorization/locks",
        "operations": "value"
          "field":
            "Microsoft.Authorization/locks/level",
              "equals": "CannotDelete"

```

A screenshot of a computer Description automatically generated

Question: 357

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

Name	Description
Used	Uses app password authentication for the Mail and Calendar app in Windows 10
USCT2	Uses Outlook on the web

You need to ensure that the users cannot create app passwords. The solution must ensure that User1 can continue to use the Mail and Calendar app.

What should you do?

- A. Assign User1 the Authentication Policy Administrator role.
- B. Enable Azure AD Password Protection.
- C. Configure a multi-factor authentication (MFA) registration policy.
- D. Create a new app registration.

Answer: C

Explanation:

Question: 358

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

Explanation:

Question: 359

You have an Azure subscription.

You plan to map an online infrastructure and perform vulnerability scanning for the following:

- ASNs
- Hostnames
- IP addresses
- SSL certificates

What should you use?

- A. Microsoft Defender for Cloud
- B. Microsoft Defender for Identity
- C. Microsoft Defender for Endpoint
- D. Microsoft Defender External Attack Surface Management (Defender EASM)

Answer: D

Explanation:

Question: 360

You have an Azure subscription that uses Microsoft Defender for Cloud. You have accounts for the following cloud services:

- Alibaba Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

What can you add to Defender for Cloud?

- A. AWS only
- B. Alibaba Cloud and AWS only
- C. Alibaba Cloud and GCP only
- D. AWS and GCP only
- E. Alibaba Cloud, AWS, and GCP

Answer: D

Explanation:

Question: 361

HOTSPOT

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

Name	Type
Item1	Key
Item2	Secret
Policy 1	Access policy

In KeyVault1 the following events occur in sequence:

- item 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. ui

Answer Area

Statements	Yes	No
You can recover Policy!	0	0
You can add a new key named Hem! Q		
You can recover ItemZ.	0	

Answer:

Explanation:

Answer Area

Statements	Yes	No
You can recover Poky 1,	0	•
You can add a new key named item)		
You can recover ttem2		

Question: 362

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. You review the Attack Surface Summary dashboard. You need to identify the following insights:

- Deprecated technologies that are no longer supported
- Infrastructure that will soon expire

Which section of the dashboard should you review?

- A. Securing the Cloud
- B. Sensitive Services
- C. attack surface composition
- D. Attack Surface Priorities

Answer: C

Explanation:

Question: 363

HOTSPOT

You have an Azure subscription that contains a Microsoft Sentinel workspace.

Microsoft 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 Microsoft Sentinel components to configure to meet the following requirements:

- When Microsoft 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 Microsoft 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.

Answer Area

When Microsoft Sentinel identifies a threat an incident must be created: | Analytics

- Analytics
- Data connectors
- Playbooks
- Workbooks

A ticket must be logged in the service management platform when an incident is created in Microsoft | Playbooks

- Senenel: Analytics
- Data connectors
- Playbooks
- Workbooks

Answer:

Explanation:

Answer Area

When Microsoft Sentinel identifies a threat an incident must be created: Analytics

A ticket must be logged in the service management platform when an incident is created in Microsoft Playbooks

Question: 364

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

Name	Type
LSI	Azure Standard Load Balancer
W1	Virtual machine
5QL1	Azure SQL Database
VMSS1	Virtual machine scale set

You plan to deploy an Azure Private Link service named APL1.

Which resource must you reference during the creation of APL1?

- A. VMSS1
- B. VM1
- C. SQL

D. LB1

Answer: D

Explanation:

Question: 365

You have an Azure subscription.

You need to deploy an Azure virtual WAN to meet the following requirements:

- Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.
- Ensure that security rules sync between the regions.

What should you use?

- A. Azure Firewall Manager
- B. Azure Virtual Network Manager
- C. Azure Network Function Manager
- D. Azure Front Door

Answer: A

Explanation:

Question: 366

SIMULATION

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.

Answer: see the task
answer with step by
step below:

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.

Question: 367

SIMULATION

Lab Task

Task 2

You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-Subnet0-NSG network security group (NSG) are stored in the logs31330471 Azure Storage account for 30 days.

Answer: see the task answer with step by step below:

Explanation:

Enable diagnostic resource logging for the NSG. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the Rule counter category under Logs and choose the logs31330471 storage account as the destination.

Configure the retention policy for the storage account to keep the logs for 30 days. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify the days parameter as 30 for the Set-AzStorageServiceProperty cmdlet or the az storage logging update command.

View and analyze the logs in the storage account. You can use any tool that can read JSON files, such as Azure Storage Explorer or Visual Studio Code. You can also export the logs to any visualization tool, SIEM solution, or IDS of your choice.

Question: 368

SIMULATION

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.

Answer: see the task answer with step by step below:

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.

Question: 369

SIMULATION

Lab Task

Task 4

You need to ensure that when administrators deploy resources by using an Azure Resource Manager template, the deployment can access secrets in an Azure key vault named KV31330471.

**Answer: see the task
answer with step by
step below:**

Explanation:

Grant permission to the application that is used to deploy the resources to access the secrets in the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Key Vault Secrets User role to the application at the scope of the key vault or individual secrets.

Enable template deployment for the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to set the `enabledForTemplateDeployment` property of the key vault to `true`.

Reference the secrets in the template by using their resource ID. You can use the `listSecrets` function to get the resource ID of a secret in the key vault. You need to specify the name of the key vault and the name of the secret as parameters.

Deploy the template by using Azure PowerShell, Azure CLI, or REST API. You can use the `New-AzResourceGroupDeployment` cmdlet, the `az deployment group create` command, or the `Deployments - Create Or Update` REST API to do this. You need to provide the template file or URI and any required parameters.

Question: 370

SIMULATION

Lab Task

Task 5

A user named Debbie has the Azure app installed on her mobile device.

You need to ensure that `debbie@contoso.com` is alerted when a resource lock is deleted.

Answer: see the task

answer with step by
step below:

Explanation:

Create an Azure Resource Manager service principal. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify a name and a role for the service principal, such as Contributor. Grant permission to the service principal to access the secrets in the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Key Vault Secrets User role to the service principal at the scope of the key vault or individual secrets.

Enable template deployment for the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to set the `enabledForTemplateDeployment` property of the key vault to `true`.

Reference the secrets in the template by using their resource ID. You can use the `listSecrets` function to get the resource ID of a secret in the key vault. You need to specify the name of the key vault and the name of the secret as parameters.

Deploy the template by using Azure PowerShell, Azure CLI, or REST API. You can use the `New-AzResourceGroupDeployment` cmdlet, the `az deployment group create` command, or the Deployments - Create Or Update REST API to do this. You need to provide the template file or URI and any required parameters. You also need to provide the credentials of the service principal.

Question: 371

SIMULATION

Lab Task

Task 6

You need to configure a Microsoft SQL server named Web3I 330471 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.

Answer: see the task
answer with step by
step below:

Explanation:

Configure the firewall settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to add a firewall rule that allows inbound traffic from the IP address range of the Subnet0 subnet. You also need to disable the option to allow Azure services and resources to access this server.

Configure the network settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to enable service endpoints for SQL Server on the Subnet0 subnet. You also need to add a virtual network rule that links the SQL server to the Subnet0 subnet.

Configure the connection settings for the SQL server. You can use SQL Server Management Studio or Transact-SQL to do this. You need to enable remote server connections and specify a TCP port for listening. You also need to configure SQL Server Authentication or Azure Active Directory Authentication for connecting to the SQL server.

Question: 372

SIMULATION

Lab Task

Task 7

You need to ensure that connections through an Azure Application Gateway named Homepage-AGW are inspected for malicious requests.

Answer: see the task answer with step by step below:

Explanation:

Enable Web Application Firewall (WAF) for the application gateway. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select a WAF policy and a WAF mode for the application gateway. You can choose a predefined policy or create a custom policy with your own rules and exclusions. Configure WAF policy settings. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the managed rulesets and rule groups that you want to enable or disable for the WAF policy. You can also configure custom rules to match specific patterns or conditions and take actions such as blocking or logging requests.

Monitor WAF logs. You can use different types of logs in Azure to manage and troubleshoot the application gateway and the WAF policy. You can access some of these logs through the portal, such as metrics and health probes. You can also export the logs to Azure Storage, Event Hubs, or Log Analytics and view them in different tools, such as Azure Monitor, Excel, or Power BI.

Question: 373

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

Explanation:

Question: 374

You have an Azure subscription that contains an Azure Blob storage account blob1.

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: B

Explanation:

Question: 375

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

Name	Type
DB1	Azure Cosmos DB KCI
VM1	Virtual Machine
VM2	Virtual Machine
VNET1	Virtual Network
NSG1	Network Security Group

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

Explanation:

Question: 376

DRAG DROP

You have an Azure subscription.

You plan to implement Azure DDoS Protection. The solution must meet the following requirement:

- * Provide access to DDoS rapid response support during active attacks.
- * Project Basic SKU public IP addresses.

You need to recommend which type of DDoS protection to use for each requirement.

What should you recommend? To answer, drag the appropriate DDoS protection types to the correct requirements. Each DDoS Protection type may be used once, or not at all. You may need to drag the split bar between panes or scroll to view connect.

NOTE: Each correct selection is worth one point.

DDoS Protection types

DDoS Network Protector

Answer Area

Provide access to DDoS rapid response support during active attacks: [

Protect Basic SKU public IP addresses: [

Answer:

Explanation:

DDoS Protection types

Answer Area

ppDoS - r* sstr-ucture protecton

device access to DDoS upto response _____
support c jf fflf Kl. * sokw: | Doos Neave* Protect or

pjCcTtpPretelon [DDoS Newer* Protector

Protect Basic s-su pub e³ Moteses: [:DcsTpPrD'eclcr

Question: 377

HOTSPOT

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 Dynamics 365 telemetry	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 MicrosoftPurview	Microsoft Resource Graph Powerful tool to query, explore, and analyze your cloud resources at scale.

Answer:

Explanation:

Answer Area

Add permissions



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

Question: 378

You have an Azure subscription that contains an Azure web app named 1 and a virtual machine named VM1. VM1 runs Microsoft SQL Server and is connected to a virtual network named VNet1. App1, VM1, and VNet1 are in the US Central Azure region.

You need to ensure that App1 can connect to VM1. The solution must minimize costs.

- A. NAT gateway integration
- B. Azure Front Door
- C. regional virtual network integration
- D. gateway-required virtual network integration
- E. Azure Application Gateway integration

Answer: C

Explanation:

Question: 379

You have an Azure subscription that contains a storage account and an Azure web app named App1.

App1 connects to an Azure Cosmos DB database named Cosmos1 that uses a private endpoint named Endpoint1.

Endpoint1 has the default settings.

You need to validate the name resolution to Cosmos1.

Which DNS zone should you use?

- A. Endpoint1. Privatelink, blob, core, windows, net
- B. Endpoint1. Privatelink, database, azure, com
- C. Endpoint1. Privatelink, azurewebsites, net
- D. Endpoint1. Privatelink, documents, azure, com

Answer: D

Explanation:

Question: 380

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

Name	Virtual network	Location
Sundem	VM?	Wen J 5
	Ar"	We# /
Sut-^i	VNetZ	

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

Explanation:

Question: 381

You have an Azure AD turned 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 Administrate

Answer: C

Explanation:

Question: 382

DRAG DROP

You have an Azure subscription named Sub1 that contains the storage accounts shown in the

following table

Name	Resource group
storage1	RG1
storage2	RG1
storage3	RG2

The storage3 storage account is encrypted by using customer-managed keys.

YOU need to enable Microsoft Defender for storage to meet the following requirements.

- * The storage1 and storage2 account must be include in the defender for storage requirement.
- * The storage3 account must be exclude from the Defender for Storage protections.

Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and them in the correct order.

Actions

For storage, enable the Customer-managed keys.

Disable Defender for Storage for storage3.

Enable the Defender for Storage plan for Sub1.

For storage, assign the AzDefenderPlanAutoEnable tag and set the value to off.

Enable the Defender for Storage plan for Sub1.

Answer Area



Answer:

Explanation:

Actions

For storage, enable the customer-managed keys.

Disable Defender for Storage for storage3.

Answer Area

1 Enable the Defender for Storage plan for Sub1.

2 For storage, assign the AzDefenderPlanAutoEnable tag and set the value to off.

3 Enable the Defender for Storage plan for Sub1.

Question: 383

HOTSPOT

You have an Azure subscription named Sub 1 that is associated to an Azure AD Tenant named contoso.com. The tenant contains the users shown in the following table.

Name	Role
User1	Global administrator
UserZ	Security administrator
User3	Security reader
Userf	License administrator

Each user is assigned an Azure AD Premium P2 license.

You plan to onboard and configure Azure AD Identity Protection.

Which users can onboard Azure AD Identity Protection, remediate users, and configure policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

- Users who can onboard Azure AD Identity Protection: User1 only User1 only User1 and User2 only User1, User 2, and User3 only User1, User 2, User3, and User 4 only
- Users who can remediate users and configure policies: User1 and User2 only User1 and User2 only User1 and User3 only User1, User 2, and User3 only User1, User 2, User3, and User 4

Answer:

Explanation:

Answer Area

- Users who can onboard Azure AD Identity Protection: User 1 only
- Users who can remediate users and configure policies: User1 and User2 only

Question: 384

HOTSPOT

You are implementing an Azure Application Gateway web application firewall (WAF) named WAF1. You have the following Bicep code snippet.

```

resource AppCW_AppFW_Pol 'Microsoft.Network/ApplicationGatewayWebApplicationFirewallPolicies^2021-08-01' • {
  name: AppGW_AppFW_Pol_name
  location: Location
  properties: {
    customRules: [
      {
        name: *CustRule01*
        priority: 100
        ruleType: 'HatchRule'
        action: 'Block'
       matchConditions: [
          {
            matchVariables: [
              {
                variableName: 'RemoteAddr'
              }
            ]
            operator: 'IPHatch'
            negateCondition: true
            matchValues: [
              '10.10.10.0/24'
            ]
          }
        ]
      }
    ]
    policySettings: {
      requestBodyCheck: true
      maxRequestBodySizeInKb: 128
      state: 'Enabled'
      mode: 'Detection'
    }
    managedRules: {
      managedRuleSets: [
        {
          ruleSetType: 'OWASP'
          ruleSetVersion: '3.2'
        }
      ]
    }
  }
}

```

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

A request to the backend pool from IP address 10.1.1.5 is allowed.

Incoming requests attempting file path attacks are blocked.

WAF1 allows a 50-MB file to be uploaded.

Answer:

Explanation:

Answer Area

Statements

Yes

No

A request to the backend pool from IP address 10.1.1.5 is allowed.

Incoming requests attempting file path attacks are blocked.

0

0

WAF1 allows a 50-MB file to be uploaded.

0

0

Question: 385

HOTSPOT

You have an Azure SQL database named DB1 that contains a table named Table.

You need to configure DB1 to meet the following requirements;

- Sensitive data in Table1 must be identified automatically.
- Only the first character and last character of the sensitive data must be displayed in query results.

Which two features should you configure? To answer, select the features in the answer area.

NOTE: Each correct selection is worth one point.



DB1

SQL database

 Search (Ctrl+/)


 Auditing

 Ledger

 Data Discovery & Classification


 Dynamic Data Masking


 Microsoft Defender for Cloud

 Transparent data encryption

Intelligent Performance

 Performance overview

 Performance recommendations

 Query Performance Insight

 Automatic tuning

Monitoring

 Alerts

 Metrics

 Diagnostic settings

 Logs

Answer:

Explanation:

1. Data Discovery & Classification
2. Dynamic Data Masking

<https://learn.microsoft.com/en-us/azure/sql/database/data-discovery-and-classification-overview?view=azuresql>
Data Discovery & Classification is built into Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics. It provides basic capabilities for discovering, classifying, labeling, and reporting the sensitive data in your databases.

Question: 386

DRAG DROP

You have an Azure AD Tenant and an application named App1.

You need to ensure that App1 can use Microsoft Entra Verified ID to verify credentials.

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

- Add an identity provider.
- Configure an authentication methods policy.
- Create an Azure key vault.
- Configure the Verified ID service.
- Register App1 in Azure AD and grant permissions.

Answer Area

^y
^^



Answer:

Explanation:

Actions

- Add an identity provider.
- Configure an authentication methods policy.

Answer Area



<https://learn.microsoft.com/en-us/azure/active-directory/verifiable-credentials/verifiable-credentials-configure-tenant>

Question: 387

You have an Azure AD tenant.

You plan to implement an authentication solution to meet the following requirements:

- Require number matching.
- Display the geographical location when signing in.

Which authentication method should you include in the solution?

- A. SMS
- B. Temporary Access Pass
- C. Microsoft Authenticator
- D. FIDO2 security key

Answer: B

Explanation:

Question: 388

HOTSPOT

You have an Azure Subscription that is connected to an on-premises datacenter and contains the resources shown in the following table.

Name	Description
storage1	A storage account
storage2	A storage account
KeyVault1	An Azure key vault
VNet1	A virtual network containing a single subnet that has five virtual machines connected
VNet2	A virtual network containing a single subnet that has three virtual machines connected

You need to configure virtual network service endpoints for VNet1 and VNet2. The solution must meet the following requirements:

- The virtual machines that connect to the subnet of VNet1 must access storage1, storage2, and Azure AD by using the Microsoft backbone network.
- The virtual machines that connect to the subnet of VNet2 must access storage1 and KeyVault1 by using the Microsoft backbone network.
- The virtual machines must use the Microsoft backbone network to communicate between VNet1 and VNet2.

How many service endpoints should you configure for each virtual network? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

VNet1: 1

A dropdown menu for VNet1 with a blue highlight on the number 1. The visible options are 1, 2, 3, 5, and 10.

A dropdown menu for VNet2 with a blue highlight on the number 2. The visible options are 1, 2, 3, 6, and 15.

Answer:

Explanation:

Answer Area

VNet1: 1

VNet2: 2

Question: 389

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

User1	User	<i>Not applicable</i>
Group1	Microsoft 365 group	Yes
Group2	Security group	No
Group3	Security group	Yes
Group4	Security group	Yes

You assign Group4 the Contributor role for RG1.

Which identities can you add to Group4 as members?

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

Answer: E

Explanation:

Question: 390

You have an Azure subscription that contains an Azure Key Vault Standard key vault named Vault1.

Vault1 hosts a 2048-bit RSA key named key1.

You need to ensure that key1 is rotated every 90 days.

What should you do first?

- A. Create a key rotation policy.
- B. Modify the Access policies settings of Vault1.
- C. Upgrade Vault1 to Key Vault Premium.
- D. Recreate key1 as an EC key.

Answer: A

Explanation:

Question: 391

HOTSPOT

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

Name	Subnet	Subnet-associated network security group (NSG)	Peered with
VNet1	Subnet1	NSG1	VNet2
VNet2	Subnet2	NSG2	VNet1

NSG1 and NSG2 both have default rules only.

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

Name	Connected to
VM1	Subnet1
VM2	Subnet2

The subscription contains the web apps shown in the following table.

Name	Description
WebApp1	Uses an App Service plan in the Premium pricing tier and has virtual network integration with VNet1
WebApp2	Uses an App Service plan in the Isolated pricing tier and is deployed to Subnet2

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
WebApp1 can connect to VM2.	<input type="radio"/>	<input type="radio"/>
NSG1 controls inbound traffic to WebApp1.	<input type="radio"/>	<input type="radio"/>
WebApp2 can connect to VM1.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Answer Area

Statements	Yes	No
WebAppl can connect to VM2.	<input checked="" type="radio"/>	<input type="radio"/>
NSG1 controls inbound traffic to WebAppl.	<input type="radio"/>	<input checked="" type="radio"/>
WebApp2 can connect to VM1.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 392

DRAG DROP

You have an Azure subscription.

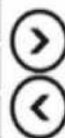
You create an Azure Firewall policy that has the rules shown in the following table:

Name	Type	Priority
Rule1	Application rule collection	100
Rule2	NAT rule collection	200
Rule3	Network rule collection	300
Rule4	NAT rule collection	400
Rule5	Network rule collection	500

In which order should the rules be processed? To answer, move all rules from the list of rules to the answer area and arrange them in the correct order.

Rules

- Rule5
- Rule4
- Rule3
- Rule2
- Rule1



Answer Area

Answer:

Explanation:

The rules should be processed in the following order:

Rule1: This is a network rule collection with the lowest priority (100). It allows any protocol and port from any source to any destination.

Rule2: This is a NAT rule collection with the second lowest priority (200). It translates the source IP address of VM1 to a public IP address when it accesses the internet.

Rule3: This is an application rule collection with the third lowest priority (300). It allows HTTP and HTTPS traffic from any source to any destination.

Rule4: This is an application rule collection with the fourth lowest priority (400). It blocks HTTP and HTTPS traffic from any source to www.contoso.com.

Rule5: This is a network rule collection with the highest priority (500). It blocks ICMP traffic from any source to any destination.

The rules are processed from the lowest priority to the highest priority. If a rule matches the traffic, it is applied and no further rules are evaluated. If no rule matches the traffic, it is denied by default.

Question: 393

You have an Azure subscription that contains an Azure Data Lake Storage account named sa1.

You plan to deploy an app named App1 that will access sa1 and perform operations, including Read, List, Create Directory, and Delete Directory.

You need to ensure that App1 can connect securely to sa1 by using a private endpoint

What is the minimum number of private endpoints required for sa1?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

Answer: A

Explanation:

A private endpoint is a network interface that connects you privately and securely to a service that's powered by Azure Private Link. By enabling a private endpoint, you're bringing the service into your virtual network. You only need one private endpoint for each service that you want to access privately, such as Azure Data Lake Storage. You can create a private endpoint for your Azure Data Lake Storage account named sa1 by following the steps in this article.

Reference:

What is a private endpoint? - Azure Private Link

Private Endpoints for Azure Storage are now Generally Available

Step-by-Step: How to Configure a Private Endpoint to Secure Azure ...

Question: 394

HOTSPOT

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

Name	Type
storage1	Storage account
storage2	Storage account
VM1	Virtual machine
VM2	Virtual machine
Analytics1	Log Analytics workspace

You need to enable Microsoft Defender for Cloud for storage accounts and virtual machines.

At which levels can you enable Defender for Cloud for the storage accounts and the virtual machines? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point

Storage accounts:

Subscription only

Workspace only

Storage account only

Subscription or storage account only

Subscription, workspace, or storage account

Virtual machines:

Subscription only

Workspace only

Virtual machine only

Subscription or virtual machine only

Subscription, workspace, or virtual machine

Answer:

Explanation:

Storage accounts:

- Subscription only
- Workspace only
- Storage account only
- Subscription or storage account only**
- Subscription, workspace, or storage account

Virtual machines:

- Subscription only
- Workspace only
- Virtual machine only
- Subscription or virtual machine only
- Subscription, workspace, or virtual machine**

Question: 395

HOTSPOT

You have an Azure AD tenant that contains the groups shown in the following table.

Name	Type	Contains members
Group1	Security	Yes
Group2	Microsoft 365	No

You assign licenses to the groups as shown in the following table.

Group	License
Group1	Azure Active Directory Premium P2
Group?	Office 365 E5
Group3	Azure Active Directory Premium P2

On May1, you delete Group1. Group2, and Group3.

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
On May 3, you can restore Group1.	0	0
On May 15, you can restore Group?.	0	0
On June 3. you can restore Group3.	0	0

Answer:

Explanation:

Answer Area

Statements	Yes	No
On May 3, you can restore Group1		0
On May 15, you can restore Group?.		
On June 3. you can restore Group3.	<input checked="" type="radio"/>	

Question: 396

You have an Azure subscription that is linked to an Azure AD tenant and contains the resources shown in the following table.

Name	Location	Description
Group1	<i>Not applicable</i>	Dynamic device security group in Azure AD
Managed1	East US	Managed identity
VM1	West US	Virtual machine that has a system-assigned managed identity
VM2	Central US	Virtual machine
App1	<i>Not applicable</i>	Enterprise application in Azure AD

Which resources can be assigned the Contributor role for VM1?

- A. Managed1 and App1 only
- B. Group1 and Managed1 only
- C. Group1, Managed1, and VM2only
- D. Group1, Managed1, VM1. and App1 only

Answer: A

Explanation:

Question: 397

DRAG DROP

You have an on-premises datacenter.

You have an Azure subscription that contains a virtual machine named VM1. VM1 is connected to a virtual network named VNet1. VNet1 is connected to the on-premises datacenter by using a Site-to-Site (S2S) VPN.

You plan to create an Azure storage account named storage1 and App1.

You need to ensure that network communication to each resource meets the following requirements:

- Connections to App1 must be allowed only from corporate network NAT addresses.
- Connections from VNet1 to storage1 must use the Microsoft backbone network.
- The solution must minimize costs.

What should you configure for each resource? To answer, drag the appropriate components to the correct resources. Each component 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.

Components

A private endpoint

A service endpoint

An access restriction rule

Azure Private Link

Answer Area

storage1:

App1:

Answer:

Explanation:

Components

A private endpoint

A service endpoint

An access restriction rule

Azure Private Link

Answer Area

storage1: A private endpoint

App1: Azure Private Link

Question: 398

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.

You need to use the automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.

What should you create?

- A. an Azure AD user
- B. a secret in Azure Key Vault
- C. an Azure AD group
- D. a role assignment

Answer: D

Explanation:

Question: 399

You have an Azure subscription named Sub1. Sub1 contains a virtual network named VNet1 that contains one subnet named

Subnet1.

Subnet1 contains an Azure virtual machine named VM1 that runs Ubuntu Server 20.04.

You create a service endpoint for Microsoft Storage in Subnet1.

You need to ensure that when you deploy Docker containers to VM1, the containers can access Azure Storage resources by using the service endpoint.

What should you do on VM1 before you deploy the container?

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

Answer: B

Explanation:

Question: 400

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

You have an Amazon Web Services (AWS) account.

You need to add the AWS account to Defender for Cloud.

What should you do first?

- A. From the Azure portal, add the AWS enterprise application.
- B. From the AWS account, enable a security hub.
- C. From Defender for Cloud, configure the Security solutions settings.
- D. From Defender for Cloud, configure the Environment settings.

Answer: D

Explanation:

Question: 401

HOTSPOT

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of	Role
Admin1	Group1	Global Administrator
Admin2	Group1	Privileged Authentication Administrator
User1	None	None

You configure the Temporary Access Pass settings as shown in the following exhibit.

Temporary Access Pass settings •

X

Temporary Access Pass, or TAP, is a time-limited or limited-use passcode that can be used by users for bootstrapping new accounts, account recovery, or when other auth methods are unavailable. Learn more. TAP is issuable only by administrators, and is seen by the system as strong authentication. It is not usable for Self Service Password Reset.

Enable and Target Configure

Enable ^^

Include Exclude

Target () All users • Select groups

Add groups

Name	Type	Registration
Group	Group	Optional

You add the Temporary Access Pass authentication method to Admin2.

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
Admin1 can view the Temporary Access Pass of Admin?.	<input type="radio"/>	<input type="radio"/>
Admin? can add the Temporary Access Pass authentication method to User!.	<input type="radio"/>	<input type="radio"/>
Admin? can add the Temporary Access Pass authentication method to Admin!.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Answer Area

Statements	Ves	No
Admin1 can view the Temporary Access Pass of Admin?.	<input type="radio"/>	<input checked="" type="radio"/>
Admin? can add the Temporary Access Pass authentication method to User!.	<input checked="" type="radio"/>	<input type="radio"/>
Admin? can add the Temporary Access Pass authentication method to Admin!.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 402

HOTSPOT

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

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

You have a storage account named contoso2024 that contains the following resources:

- A container named Contained that contains a file named File1
- A file share named Share1 that contains a file named File2

You create a private endpoint for contoso2024 as shown in the following exhibit.

Create a private endpoint

Q Validation passed

>Z Basics 'Z Resource x Z Virtual Network xZ DNS xZ Tags 0 Review create

Basics

Subscription	Azure Pass - Sponsorship
Resource group	RG1
Region	East US
niame	PE1
Network Interface Name	PE1-nic

Resource

Subscription ID	a45b7def-alc-4700-afeb-80f3dfIS85fd (Azure Pass - Sponsorship)
Resource	Microsoft-Storage/storageAccounts
Resource	contoso2024
Target sub-resource	blob

Virtual Network

Virtual network resource group	RG1
Virtual network	VNet2
Subnet	Subnet2I
Network Policies	Disabled
Application security groups	None

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 access File! by using a private IP address. Yes No

From VM2, you can access Filei by using a private IP address. Yes No

From VM2, you can access File? by using a private IP address. Yes No

Answer:

Explanation:

Answer Area

Statement*

Yes*

No

From VM1, you can access File 1 by using a private IP address.

From VM2, you can access File1 by using a private IP address.

0

From VM2, you can access File2 by using a private IP address.

Question: 403

HOTSPOT

You have a Microsoft Entra 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

You create and enforce a Microsoft Entra Identity Protection sign-in risk policy that has the following settings:

- Assignments: Include Group1, exclude Group2
- Conditions: Sign-in risk level: Low and above
- Access: Allow access, Require multi-factor authentication

You need to identify what occurs when the users sign in to Microsoft Entra ID.

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.

Answer Area

When User1 signs in from an anonymous IP address, the user will: Be prompted for MFA 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 blocked

Be prompted for MFA

Sign in by using a username and password only

Answer:

Explanation:

Answer Area

When User1 signs in from an anonymous IP address, the user will: Be prompted for MFA

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

Question: 404

You have a Microsoft Entra tenant that contains a user named User1.

You plan to enable passwordless authentication for the tenant.

You need to ensure that User1 can enable the combined registration experience. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Security Administrator
- B. Global Administrator
- C. Privileged Role Administrator
- D. Authentication Administrator

Answer: D

Explanation:

Question: 405

You have an Azure subscription.

You plan to deploy a new Conditional Access policy named CAPolicy1.

You need to use the What If tool to evaluate how CAPolicy1 will affect user1. The solution must minimize the impact of CAPolicy1 on the users.

To what should you set the Enable policy setting for CAPolicy1?

- A. Off
- B. On
- C. Report only

Answer: C

Explanation:

Question: 406

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains a single subnet. The subscription contains a virtual machine named VM1 that is connected to VNet1.

You plan to deploy an Azure SQL managed instance named SQL1.

You need to ensure that VM1 can access SQL1.

Which three components should you create? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. a virtual network gateway
- B. a network security group (NSG)
- C. a route table
- D. a subnet
- E. a network security perimeter

Answer: B,C,D

Explanation:

Question: 407

DRAG DROP

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

Name	Type	Location
VM1	Virtual machine	East US
VNet1	Virtual network	East US
NSG1	Network security group (NSG)	East US
storage1	Storage account	West US

You need to configure network connectivity to meet the following requirements:

- Communication from VM1 to storage1 must traverse an optimized Microsoft backbone network.
- All the outbound traffic from VM1 to the internet must be denied.
- The solution must minimize costs and administrative effort

What should you configure for VNet1 and NSG1? To answer, drag the appropriate components to the correct resources. Each component 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.

Components

- A private endpoint
- A route table
- A service endpoint
- A service tag

Resources

VNet1

NSG1

Answer:

Explanation:

Components

Answer Area

A private endpoint

Virtual Network service tag

A route table

NSG1: A private endpoint

A service endpoint

A service tag

Question: 408

HOTSPOT

You have an Azure subscription that contains a storage account named contoso2023. You need to perform the following tasks:

- Verify that identity-based authentication over SMB is enabled.
- Only grant users access to contoso2023 in the year 2023.

Which two settings should you use? To answer, select the appropriate settings in the answer area

NOTE: Each correct selection is worth one point.

Answer Area

— contoso2023 ^

£ Seieh iOrt-fl
^ Dugfi&w d¹ : a! -^ ptc^bin;
■ V Awe^ Ortnc JAM

g' nit. " ., ilcr*
* E .cn^
■ Sirr.i:]-.tjJ^<r

DJ1J ikrw?

— COrr***! ii

4 Hk 1MH\$
&>>fV«

I>xuitY * <i«hMMtrM]

A Nc^-rj

* Aiuer CM

¹ A (HI k>"VJ

J Shy»d KC*IJ liqnthn

U fi&crfljtiQn

(^ MKrnKjft Dr'Ktidff, « r^jj

D1U mirMQifnsHit

® ■*t>>F':-li llrf.'il

^ t T ■ S'Jle " s':

Answer:

Explanation:

Answer Area

■ contaso2023 —

p Watch ! ??!■;

^ Apcm ConhnUIAM

if" t)aij ■"JJ ii <n

■ {tTpU

BL Swrag ■ bU'Mitf

PaU |I?rw»

S CwtUmtfn

J RIFih ■ w

3 tatuH

E hb^

purity k IWhMWtHQ

' - t)NO ■ J

* Aju<t CDh

Y. Atm* kry^

Qfj Shartd icaui^naiun

Q {ncrftitidii

* Doti pttWccta

A screenshot of a computer Description automatically

generated

Requirement: Verify that identity-based authentication over SMB is enabled

Go there to configure Identity-based authentication (Active Directory) for Azure file shares.

Ref: <https://learn.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-overview>

HOTSPOT

You have an Azure subscription that contains an Azure key vault and an Azure SQL database named SQL1.

You generate a key named Key1.

You need to enable Transparent Data Encryption (TDE) for SQL1 by using Key1.

Which two settings should you modify for Key1? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

2. Share access signature

Requirement: Only grant users access to contoso2023 in the year 2023

Question: 409

HOTSPOT

You have an Azure Storage account that contains a blob container named container1 and a client application named App1. You need to enable App1 access to container1 by using Microsoft Entra authentication. What should you do?

To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one

Answer Area



point.

Explanation:

Answer Arts



Answer:

From Microsoft Entra: Register App1

From the storage account: Configure Access control (IAM).

Question: 410

Answer Area

81cb93e71e7e401095f37bb5841417dd  

key version

Save Discard changes Download public key

Key type	RSA
RSA key size	2048
Created	4/24/2023, 7:39:34 PM
Updated	4/24/2023, 7:39:34 PM

Key identifier: <https://16230424.vault.azure.net/keys/Key2/81cb93e71e7e401095f37bb5841417dd>

Set expiration date

Expiration date: 01/01/2030 6:49:08 PM
(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Enabled: Yes No

Tags: 0 tags

Permitted operations:

- Encrypt
- Decrypt
- Sign
- Verify
- Wrap Key
- Unwrap Key

Answer:

Explanation:

Bkb93e71e7e4010 9 5f3 7bb564!417dd

J#M X O*wd cMnjj 4 OoM4»d tvbR l'y

UFT>p«

KA^tae*

UM.

UptM

5

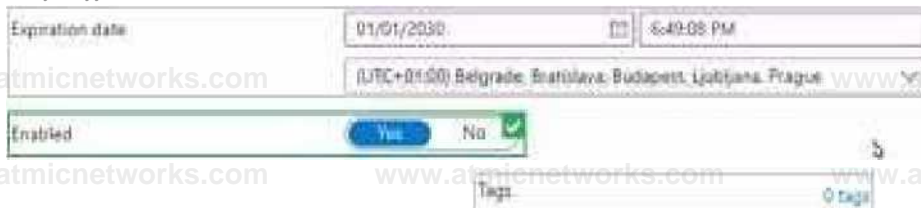
aw

tftf&nilKlrt

4M«IOB • J? H w

tft lint h.r

httpRjllh^TIUdL^k.^ir.ntLIR^&^nrrt^



Question: 411

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

Name	Operating system
VM1	Windows Server 2019
VM2	Windows Server 2022
VM3	Server Core installation of Windows Server 2022
VM4	Windows Server 2022 configured with an AppLocker policy

You are configuring Microsoft Defender for Servers.

You plan to enable adaptive application controls to create an allowlist of known-safe apps on the virtual machines. Which virtual machines support the use of adaptive application controls?

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

Answer: D

Explanation:

Question: 412

You have an Azure subscription named Sub1 that has Security defaults disabled. The subscription contains the following users:

- Five users that have owner permissions for Sub1.
- Ten users that have owner permissions for Azure resources.

None of the users have multi-factor authentication (MFA) enabled.

Sub1 has the secure score as shown in the Secure Score exhibit. (Click the Secure Score tab.)

You plan to enable MFA for the following users:

- Five users that have owner permissions for Sub1.
- Five users that have owner permissions for Azure resources.

By how many points will the secure score increase after you perform the planned changes?

- A. 0
- B. 5
- C. 7.5
- D. 10
- E. 14

Answer: C

Explanation:

Question: 413

HOTSPOT

You have a Microsoft Entra tenant named contoso.com.

You collaborate with a partner organization that has a Microsoft Entra tenant named fabrikam.com.

Fabrikam.com has multi-factor authentication (MFA) enabled for all users.

Contoso.com has the Cross-tenant access settings configured as shown in the Cross-tenant access settings exhibit. (Click the Cross-tenant access settings:

Inbound access settings

& Edit inbound defaults

Type

Applies to

Status

B2B collaboration

External users and groups

All allowed

B2B collaboration

Applications

All allowed

B2B direct connect

External users and groups

All blocked

B2B direct connect

Applications

All blocked

Trust settings

N/A

Disabled

Outbound access settings

^ Edit outbound defaults

Type

Applies to

Status

B2B collaboration

Users and groups

All allowed

B2B collaboration

External applications

All allowed

B2B direct connect

Users and groups

All blocked

B2B direct connect

External applications

All blocked

Contoso.com has the External collaboration settings configured as shown in the External collaboration settings exhibit. (Click the External collaboration settings tab.)

Guest user access

Guest user access restrictions 0

[Learn more](#)

0 Guest users have the same access as members (most inclusive)

Q Guest users have limited access to properties and memberships of directory objects

Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

You create a Conditional Access policy that has the following settings:

- Name: CAPolicy1

■ Assignments

- o Guest or external users: B2B collaboration guest users
- o Target resources

- Include: All cloud apps
- o Access controls
- Grant access
- Require device to be marked as compliant
- Require multi-factor authentication
- Enable policy: On

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

NOTE: Each correct section is worth one point.

Answer Area

Statements	Yes	No
Users with devices that have a compliant device claim from fabrikam.com will be granted access to the cloud apps in contoso.com.	<input type="radio"/>	<input type="radio"/>
To minimize the number of MFA authentication prompts for the users in fabrikam.com, you must configure the Trust settings.	<input type="radio"/>	<input type="radio"/>
Users with devices that have a compliant device claim from fabrikam.com can review the user properties of the users in contoso.com.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Answer Area

Statements	Yes	No
Users with devices that have a compliant device claim from fabrikam.com will be granted <input checked="" type="radio"/> access to the cloud apps in contoso.com.	<input checked="" type="radio"/>	<input type="radio"/>
To minimize the number of MFA authentication prompts for the users in fabrikam.com, you must configure the Trust settings.	<input type="radio"/>	<input checked="" type="radio"/>
Users with devices that have a compliant device claim from fabrikam.com can review the user properties of the users in contoso.com.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 414

HOTSPOT

Your network contains an on-premises Active Directory domain named adatum.com that syncs to a Microsoft Entra tenant.

The Microsoft Entra tenant contains the users shown in the following table.

Name	On premises sync enabled	Password
User	No	Adatumt23
User?	No	N3w3rT0GueB
User}	Yes	Complex Pass word3.3

You configure the Microsoft Entra Password Protection settings for adatum.com as shown in the

following exhibit.

Custom smart lockout

Lockout threshold 10

Lockout duration in seconds 60

Custom banned passwords

Enforce custom list Yes No

Adatum

Custom banned password list

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory Yes No

Mode Enforced Audit

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 will be prompted to change the password on the next sign-in.	<input type="radio"/>	<input type="radio"/>
User2 can change the password to @d@tum C0mpleX123	<input type="radio"/>	<input type="radio"/>
User3 can change the password to Adatum123!	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Answer Area Statements

Yes

No

User1 will be prompted to change the password on the next sign-in.

User2 can change the password to @d@tum_C0mpleX123.

User3 can change the password to Adatum123I.

Question: 415

You have a Microsoft Entra tenant that contains three users named User1, User2, and User3.

You configure Microsoft Entra Password Protection as shown in the following exhibit.

0 Save X Discard

Custom smart lockout

Lockout threshold 0

10

lockout duration in seconds 0

60

Custom banned passwords

Enforce custom list 0

Yes

No

Custom banned password W C

Contoso

Product

PatnUm

Password protection for Windows Server Active Directory

Enable password protection on Windows ' VM

NO

Server Active Directory Q

M0dt 0

The users perform the following tasks:

- User1 attempts to reset her password to C0nt0s0
- User2 attempts to reset her password to F@brikamHQ
- User3 attempts to reset her password to Pr0duct123.

Which password reset attempts fail?

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

Answer: E

Explanation:

Question: 416

You have an Azure subscription that contains an Azure key vault named Vault1 and a virtual machine named VM1. VM1 has the Key Vault VM extension installed.

For Vault1, you rotate the keys, secrets, and certificates.

What will be updated automatically on VM1?

- A. the keys only
- B. the secrets only
- C. the certificates only
- D. the keys and secrets only
- E. the secrets and certificates only
- F. the keys, secrets, and certificates

Answer: C

Explanation:

Question: 417

HOTSPOT

You have an Azure subscription.

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

Name	Size	Operating system
VM1	DC4ads_v5	Windows Server 2022 Datacenter. Azure Edition
VM2	D2ads_v5	Windows Server 2022 Standard
VM3	EC4ads_v5	Windows Server 2019 Datacenter
VM4	D2ads_v5	Debian
VM5	EC4ad\$ v5	Ubuntu Server
VM6	DC4ads v5	SUSE Linux Enterprise Server

You need to identify the virtual machines and operating systems that can be deployed as confidential virtual machines?

Which Windows virtual machines and which Linux virtual machines should you identify?

Answer
Area

Windows : VMI only
VM1 only
VM3 only
VM1 and VM2 only
VM1 and VM3 only
VM1, VM2 and VM3

Linux : VM<VMSandVM6
VM5 only
VM6 only
VM4 and VM6 only
VM5 and VM6 only

VM4 VMS and VM6

Answer:

Explanation:

Windows: VM1 only

Linux: VM4, VM5 and VM6

Answer
Area

Question: 418

You have a Microsoft Entra tenant that uses Microsoft Entra Permissions Management and contains the accounts shown in the following table:

Name	Role
Admin1	Global Administrator
Admin2	Privileged Role Administrator
Admin3	Privileged Authentication Administrator
Admin4	Exchange Administrator

Which accounts will be listed as assigned to highly privileged roles on the Azure AD insights tab in the Entra Permissions Management portal?

- A. Admin1 only
- B. Admin2 and Admin3 only
- C. Admin2 and Admin4 only
- D. Admin1, Admin2, and Admin3 only
- E. Admin2, Admin3, and Admin4 only
- F. Admin1, Admin2, Admin3, and Admin4

Answer: D

Explanation:

Question: 419

HOTSPOT

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of
Used	Group i
Useri	Group' Group2
User Ei	Groups

You configure a Conditional Access policy that has the following settings:

- Name: CAPolicy1
- Assignments
 - o Users or workload identities: Group1
 - o Target resources: All cloud apps
- Access controls
 - o Grant access: Require multifactor authentication

From Microsoft Authenticator settings for the tenant, the Enable and Target settings are configured as shown in the Enable and Target exhibit. (Click the Enable and Target tab.)

Enable and Target Configure

Enable

Include Exclude

Target (J All users

- i Select groups

Registration

Authentication mode

Add groups

i Passwordless V X

Name Type

Groupl Group

From Microsoft Authenticator settings for the tenant, the Configure settings are configured as shown in the Configure exhibit. (Click the Configure tab.)

Enable and Target Configure

Note: Users must be included as part of the Microsoft Authenticator targeted groups under the Enable and Target tab.

GENERAL

Allow use of Microsoft Authenticator OTP (Yes

Require number matching for push notifications

Note: If the feature status is set to Microsoft-managed, it will be enabled by Microsoft at an appropriate time after the preview. Learn more

Status | Enabled

Target Include Exclude

Q All users

(+) Select group

Add selected group

Include target

Group?

X

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 is required to use number matching during sign-in, 0

User? is required to use number matching curing sign-in.

User? is required to use number matching during sign-in.

Answer:

Explanation:

Answer Area

Statements

Yes

No

User) is required to use number matching during sign-in.

0

User? is required to use number matching during sign-in.

User3 is required to use number matching during sign-in.

Question: 420

You have an Azure subscription. The subscription contains a virtual network named VNet1 that contains the subnets shown in the following table.

Name	Associated network security group(NSG)
Subnet1	NSG1
Subnet2	NSG1
Subnet3	NSG1
Subnet4	NSG1

The subscription contains the function apps shown in the following table.

Name	Description
App1	Uses the Azure Functions Premium plan and has virtual network integration with VNet1/Subnet1
App2	Uses an App Service plan in the Basic pricing tier and has virtual network integration with VNet1/Subnet2
App3	Uses an App Service plan in the Premium pricing tier and has virtual network integration with VNet1/Subnet3
App4	Uses an App Service plan in the Isolated pricing tier and is deployed to VNet1/Subnet4

The outbound traffic of which app is controlled by using NSG1?

- A. App4 only
- B. App3 and App4 only
- C. App2, App3, and App4 only
- D. App1, App2, App3, and App4

Answer: D

Explanation:

Question: 421

You have an Azure subscription that contains an Azure Kubernetes Service (AKS) cluster named AKS1. You have an Azure container registry that stores container images that were deployed by using Azure DevOps Microsoft-hosted agents.

You need to ensure that administrators can access AKS1 only from specific networks. The solution must minimize administrative effort.

What should you configure for AKS1?

- A. an Application Gateway Ingress Controller (AGIC)
- B. a private cluster
- C. authorized IP address ranges
- D. a private endpoint

Answer: C

Explanation:

Question: 422

HOTSPOT

You have an Azure subscription that contains an Azure key vault named KeyVault1 and the virtual machines shown in the following table.

Name	Private IP address	Public IP address	Connected to
VM1	10.7,04	51.144.245.152	VNET1/Default
VM2	10.8,0.4	104.45.9.227	VNET2/Default

You enable the Azure Disk Encryption for volume encryption KeyVault1 setting. KeyVault1 is configured as shown in the following exhibit.

Allow access from:

All networks • Selected networks

0 Configure network access control for your key vault, earn More

Virtual networks: 0

Add existing virtual networks

Add new virtual network

VIRTUAL NETWORK

SUBNET

RESOURCE GROUP

SUBSCRIPTION

VNET1

default

RG1

Firewall: 0

IPV4 ADDRESS OR ODR

| IPv4 address or CIDR

Exception:

Allow trusted Microsoft services to bypass Yes No

this firewall? 0 This setting is related to firewall only. In order to access this key vault, the trusted service must also be given explicit permissions in the Access policies section.

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, users can manage the keys and secrets stored in KeyVaultL ?

From VM2. users can manage the keys and secrets stored in KeyVaultL

VM2 can use KeyVaultl for Azure Disk Encryption. L

Answer:

Explanation:

Answer Area

Statements

Yes

No

From VM1, users can manage the keys and secrets stored in KeyVault 1.

From VM2, users can manage the keys and secrets stored in KeyVault1,

VM2 can use KeyVault1 for Azure Disk Encryption.

Question: 423

HOTSPOT

You have an Azure subscription.

You plan to deploy a virtual machine named VM1.

You need to use confidential disk encryption on VM1.

Which virtual machine series should you use for VM1, and which type of disks can be encrypted by using confidential disk encryption? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

Virtual machine series: ECasvS



Disks: The OS disk and data disks

Data disks only The OS disk only

The OS disk and data disks

Answer:

Explanation:

Answer Area

Virtual machine series: ECasv5

Disks: The OS disk and data disks

Question: 424

You have an Azure subscription that contains a virtual network named VNet1. The subscription contains an Azure App Service web app named App1.

You have an Azure Front Door profile named AFD1 that has an Azure Web Application Firewall (WAF) policy.

You need to ensure that all inbound traffic to App1 is filtered through AFD1.

What should you do?

- A. For VNet1, configure network security group (NSG) rules.
- B. For App1, configure the HTTP headers filter settings.
- C. For App1, enable virtual network integration.
- D. Configure Microsoft Entra application proxy.

Answer: B

Explanation:

Question: 425

You have an Azure subscription that contains a managed identity named Identity1 and the Azure key vaults shown in the following table.

Name	Permissions model
KeyVault1	Access control
KeyVault2	Azure RBAC

Key Vault1 contains an access policy that grants Identity1 the following key permissions:

- Get
- List
- Wrap
- Unwrap

You need to provide Identity1 with the same permissions for KeyVault2. The solution must use the principle of least privilege.

Which role should you assign to Identity1?

- A. Key Vault Crypto Service Encryption User
- B. Key Vault Crypto User
- C. Key Vault Reader
- D. Key Vault Crypto Officer

Answer: D

Explanation:

Question: 426

You have an Azure subscription named Subscription1 that is linked to a Microsoft Entra tenant named contoso.com and a resource group named RG1.

You create a custom role named Role1 in contoso.com.

Where can you use Role1 for permission delegation?

- A. contoso.com only
- B. contoso.com and RG1 only

- C. contoso.com and Subscription 1 only
- D. contoso.com, RG1, and Subscription1

Answer: D

Explanation:

Question: 427

You have an Azure subscription that contains a SQL Server on Azure Virtual Machines instance named E. t1 and a Microsoft Sentinel workspace named Sentinel1.

You need to monitor security incidents on SQL1 by using Sentinel1.

What should you do first?

- A. On SQL1, enable SQL1 Server audit.
- B. On SQL1, install the Connected Machine agent for Azure Arc-enabled servers.
- C. From the Azure portal, create a Log Analytics workspace.
- D. From Sentinel1, enable VM insights.

Answer: A

Explanation:

Question: 428

You have an Azure subscription that contains an Azure App Service app named App1, an Azure container instance named AC1, and a storage account named storage1. AC1 hosts an app named App2.

Users send requests to App1 by using a URL of `https://app1.contoso.com/echo/resource-cache? param1 =sample`.

App1 calls App2, which retrieves data from storage1.

You need to ensure that a security alert will be generated when connections are detected from anomalous IP addresses. Which Microsoft Defender for Cloud service should you use?

- A. Microsoft Defender for App Service
- B. Microsoft Defender for APIs
- C. Microsoft Defender for Storage
- D. Microsoft Defender for Containers

Answer: B

Explanation:

Question: 429

HOTSPOT

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

Name	Location	Peered with
VNet1	East US	VNet2
VNet2	West US	VNet1

The subscription contains the subnets shown in the following table.

Name	IP address space	Virtual network	Description
Subnet1	10.11.0/24	VNet1	Contains a virtual machine named VM1
Subnet2	172.16.1.0/27	VNet1	Contains n * resources
Subnet3	192.168.100/24	VNet2	Contains an integrated Azure web app named WebApp1

You plan to create an Azure web app named WebApp2 that will have the following configurations:

- Region: East US
- VNet integration: Enabled
- Scale out; Autoscale to up to 10 instances

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

WebApp2 can be integrated with Subnet1.

WebApp2 can be integrated with Subnet2.

WebApp2 can be integrated with Subnet3.

Answer:

Explanation:

Answer Area

Statements

WebApp2 can be integrated with Subnet1.

WebApp2 can be integrated with Subnet2.

WebApp2 can be integrated with Subnet3.

Question: 430

HOTSPOT

Your on-premises network contains an Active Directory Domain Services (AD DS) domain and the devices shown in the following table.

You have a hybrid Microsoft Entra tenant that contains a synced user named User1.

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

Used is assigned the Storage File Data SMB Share Contributor role for storage1 and storage2.
The Security settings for Share! are configured as shown in the following exhibit.

Security

X

Azure expose wtlngj that id you logz^ to 5ME protocol t: &■ nwre wmprttf» .■ more secure depending on yu-m wgarcatiani rKuirenwnts. Rsstnoug tost lettngs m*y prwrt some chtnb fromtwng able to corwvct L»>n"■-·*.

Previl

Cuitrm

SMB protocol v>'liwn

EM3 tonnd tncryptm

Nona

■ AEV12&CCM

^ AES 12B GCM

■ AES-256GCM

KerterM MiM encryption

Q - .< . !■-■ ■ .r

g SMS 3 11

A..toMiatkcr mechtwfw

Q VTLM v2 Q Kettles

Q Fat-THjrt "irti^!^*1 pntuppartfhi p>dta£^i^H- gi^>•^ L J-smi ut L2 " Mid iUftjCfLUojM.

Th- i^Ful, setlmns +nr ' "i -■ IFF cr.nfiq'irei ■* ■.^n^ n (HF ^, J -.wing -xi. brt

Security

x

Arure =des Op^es ^: tot W yOU togglt to SMB ptOkccl to M mOhe CtmpWifcde « **more secure** depending on yOyr or jartssaiitri s rHQdiremenft. Relffflng these svttinoi may p^etfj me chITO lrcm b^rg at^to ronnac* j-n m.-rs

Profile

CurtCMTI

SMB protocol versions

J SMB 2 t

tME „■ .rr-T 7- . ■ l Nana

M..7. ■-7.-.-1/

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 mount share to Server1 by providing a storage access key.	0	0
User1 can mount share to Device1 by using their Microsoft Entra identity.		
User1 can mount share to Server2 by using their AD DS identity.	0	0

Answer:

Explanation:

Answer Area

Statements	Yes	No
User1 can mount share to Server1 by providing a storage access key.	<input checked="" type="radio"/>	0
User1 can mount share to Device1 by using their Microsoft Entra identity.	<input checked="" type="radio"/>	
User1 can mount share to Server2 by using their AD DS identity.	<input checked="" type="radio"/>	

Question: 431

HOTSPOT

You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Member of
User1	Group1
User2	Group2
User3	Group1, Group2

All the users have devices that contain certificates issued by a certification authority (CA) named ContosoCA. You create a Conditional Access policy that has the following settings:

- Name: CAPolty1
- Assignments
 - o Users and groups: Group1
 - o Target resources
- Include: All cloud apps
- o Access controls
 - * Grant access: Require multi-factor authentication
- o Enable policy: On

You enable and target certificate-based authentication as shown in the Enable and Target exhibit. (Click the Enable and Target tab.)

Enable and Target Configure

Enable

Include Exclude

Target <) All users • Select groups

Add groups

Name

Type

Registration

Group

Group



You configure certificate-based authentication as shown in the Configure exhibit. (Click the Configure tab.)

Enable and Target Configure

Authentication binding

Select the default protection level for all certificate bindings. To override the default create special rules.

Protection Level 3

Multi-factor authentication

Add rule

Rule type

Identifier

Protection Level

Certificate issuer

CN=ContosoCA DC=contoso.DC=com Single-factor authentication

Username binding

Select user attribute to create binding. The first certificate field has the highest priority in the username binding.

Certificate field

User attribute

PrincipalName

| userPrincipalName

xz ...

RFC822Name

userPrincipalName xz ...

SubjectKeyIdentifier

certificateUserids _____ v | «» •

'SHA1PublicKey

Select user attribute

v ...

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

User1 can sign in without providing a password

User2 can choose to use a certificate or a smart card to sign in.

User 3 must use a certificate during sign in

Yes

No

Answer:

Explanation:

Answer Area

Statements

User1 can sign in without providing a password

User2 can choose to use a certificate or a smart card to sign in.

User3 must use a certificate during sign in

Yes

No

Question: 432

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

Name	Type
VM1	Virtual machine
VNet1	Virtual network
AFW1	Azure firewall

You need to configure AFW1 to only allow traffic from VM1 to storage accounts in the West US Azure region. The solution must minimize administrative effort.

What should you configure?

- A. a DNAT rule
- B. a network rule
- C. an SNAT private IP address range
- D. an application rule

Answer: B

Explanation:

Question: 433

HOTSPOT

You have a Microsoft Entra tenant named contoso.com. The tenant contains the users shown in the

following table.

Name	Role	Sign in frequency
User I	Password Administrator	Signs in every work day
User?	Password Administrator	Signs in bi-weekly
User!	Global Administrator, Password Administrator	Signs in every month

You configure an access review named Review1 as shown in the following exhibit Dates in the exhibit are in the MM/DD/YYYY format.

Review name

Review1 ✓

Description i.

Start date

11/12/2020

Frequency

One time ✓

End date *

12/12/2020

Users

Scope

* E

Review role membership (permanent and eligible)

Password Admmis

Reviewers

/en

Members (self) ✓

Upon completion settings

Auto apply results to resource 0 Enable **C2E3p**

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

NOTE: Each correct selection is worth one point.

Answer Area

User3 can perform Review1 for [answer choice]

User 3 only

User 3 only

User2 and User3 only

User1, User2, and User3

If User2 fails to complete Review1 by December 12, 2020, [answer choice]

User3 will receive a confirmation request
the Password administrator role will be revoked from User2
User2 will retain the Password administrator role

User3 will receive a confirmation request

Answer:

Explanation:

Answer Area

User3 can perform Review1 for [answer choice].

User3 only

If User2 fails to complete Review1 by December 12, 2020, [answer choice].

User3 will receive a confirmation request

Question: 434

You have an Azure subscription that contains an Azure App Services web app named WebApp1 and an Azure key vault named Vault1. Vault1 has the certificates shown in the following table.

Name	Content type	Key type	Key size
Cert1	PKCSS12	RSA	2048
Cert2	PKTS #12	RSA	4096
Cert3	PEM	RSA	2048
Cert4	PEM	RSA	4096

You plan to implement TLS for WebApp1.

You need to add a certificate to WebApp1.

Which certificates from Vault1 can you add to WebApp1?

- A. Cert1 and Cert2 only
- B. Cert1 and Cert3 only
- C. Cert3 and Cert4 only
- D. Cert1, Cert2, Cert3, and Cert4

Answer: A

Explanation:

Question: 435

You have an on-premises datacenter that contains multiple servers.

You have an Azure subscription.

You plan to onboard the on-premises servers to Microsoft Defender for Cloud by using a script.

You need to create an identity to enable the script to run without prompting for Microsoft Entra credentials.

Which type of identity should you create?

- A. user account
- B. user-assigned managed identity
- C. system-assigned managed identity
- D. group account
- E. service principal

Answer: E

Explanation:

Question: 436

You have an Azure subscription.

You need to ensure that you receive notifications regarding suspicious Azure DNS activity. Which Microsoft Defender plan for Cloud Workload Protection (CWP) should you enable? A. Storage

- B. Servers
- C. App Service
- D. APIs
- E. Resource Manager

Answer: B

Explanation:

Question: 437

HOTSPOT

You have an Azure subscription.

You configure Microsoft Sentinel to use multiple data sources.

You need to create analytic rules that meet the following requirements:

* Rule 1: Automatically match Common Event Format (CEF) logs and syslog data with domain, IP address, and URL indicators.

* Rule 2: Use Microsoft proprietary algorithms.

Which type of detection should you use for each rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Rule1: Threat intelligence

Fusion

Machine learning (ML) behavioral analytics

Microsoft Security

Threat intelligence

Rule2: Machine learning (ML) behavioral analytics Fusion

Machine learning (ML) behavioral analytics

Microsoft Security

Threat intelligence

Answer:

Explanation:

Answer Area

Rule! Threat intelligence

Rule2: Machine learning (ML) behavioral analytics

Question: 438

You have an Azure subscription.

You plan to deploy an Azure SQL managed instance named AzSQL1.

You need to recommend an encryption solution for AzSQL1.

The solution must meet the following requirements:

* The database engine must be prevented from performing key provisioning, data encryption, and decryption operations.

* Database administrators must be prevented from viewing the encrypted data in plain text.

What should you include in the recommendation?

- A. Azure Disk Encryption
- B. TLS
- C. Transparent Data Encryption (TDE) with customer-managed keys
- D. Always Encrypted
- E. Transparent Data Encryption (TDE) with Microsoft-managed keys

Answer: D

Explanation:

Question: 439

HOTSPOT

You have an Azure subscription that contains an Azure firewall named AzFW1. AzFW1 has a firewall policy named FWPolicy1. You need to add rule collections to FWPolicy1 to meet the following requirements:

- Allow traffic based on the FQDN of the destination.
- Allow TCP traffic.

Which types of rule collections should you add for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Allow traffic based on the destination FQDN: Application only

Network only

Application only

Network or DNAT only Application or

DNAT only Network or application only

Network, application, or DNAT

Allow TCP traffic Network only

Network only Application only

Network or DNAT only

Application or DNAT only

Network or application only

Network, application, or DNAT

Answer:

Explanation:

Answer Area

Allow traffic based on the destination FQDN: Application only

Allow TCP traffic: Network only

Question: 440

HOTSPOT

You have two Azure subscriptions named Sub1 and Sub2 that contain the virtual networks shown in the following table.

Name	Subscription	Location	Subnet
VNet1	Sub1	East US	Subnet1
VNetZ	Sub2	East US	Subnet2
VNet1	Sub1	West US	Subnet1

You have an Azure Virtual Network Manager instance that has the following settings:

- Name: NetMgr1
- Region: East US
- Features: Connectivity
- Management scope: Sub1

For NetMgr1, you create the target network groups shown in the following table.

Name	Member type	Group member
Group1	Virtual network	VNet1
Group2	Virtual network	None
Group3	Subnet	None

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 add VNet1 to Group2.

0

You can add VNet2 to Group1.

0

You can add Subnets to Group3.

0

Answer:

Explanation:

Answer Area

Statements

Yes

No

You can add VNet1 to Group?

0

0

You can add VNet? to Group1.

0

#

You can add Subnets to Groups.

9

0

Question: 441

HOTSPOT

You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant uses Microsoft Entra ID Protection.

You have 2,000 users that are each assigned a Microsoft Entra ID P2 license.

You plan to use Azure Monitor to generate an alert when a workload identity that is using leaked credentials is detected.

You need to configure the Diagnostic setting to support the planned alert. The solution must minimize administrative effort.

Which log category should you collect, and to

which destination should you send the logs? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Log category: ServicePrincipalRiskEvents
RiskyServicePrincipals Ri
skyUsers

ServicePrincipalRiskEvents

UserRiskEvents

Destination: IA Log Analytics workspace An
Azure event hub
A Log Analytics workspace
A storage account

Explanation:

Answer:

Answer Area

Log category: ServicePrincipalRiskEvents

Destination: A Log Analytics workspace

Question: 442

HOTSPOT

You have an Azure App Service web app named App1 as shown in the following exhibit.

z.s Virtual Network Integration

*SP d»moappa789577SS7336group 84c7

App Service Plan

ASP-demoapp87895775«7336group84d2

App Service Plan location

East US

Regional VNet integrations

1/2

Gateway required VNet integrations

0/5

VNet NAME T

GATEWAY STATUS U

vnet/subnet?

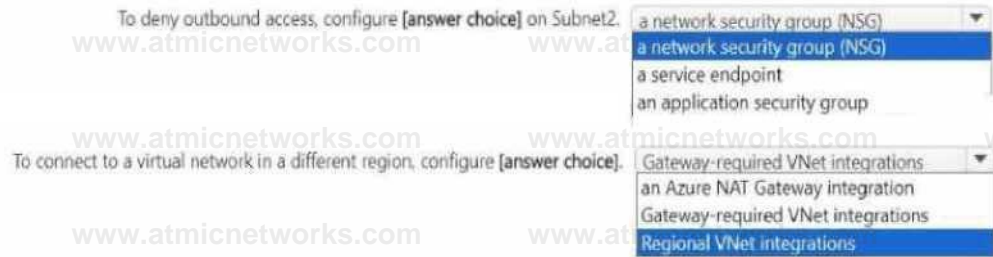
N/A

Subnet 2 contains a virtual machine named VM1.

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

NOTE: Each correct selection is worth one point.

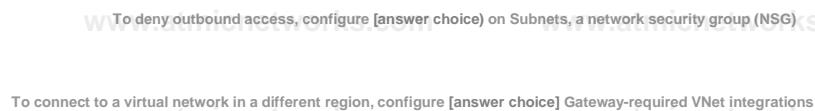
Answer Area



Answer:

Explanation:

Answer Area



Question: 443

You have an Azure subscription that contains an Azure App Services web app named WebApp1.

WebApp1 is accessed by users in multiple Azure regions.

You need to secure access to WebApp1. The solution must meet the following requirements:

- * Protect against common web vulnerabilities.
- * Optimize the routing of traffic from different regions.

What should you use?

- A. Azure Application Gateway
- B. Azure Content Delivery Network (CDN)
- C. Azure Firewall
- D. Azure Front Door Premium

Answer: D

Explanation:

Question: 444

You have an Azure subscription that contains a key vault and an Azure SQL server.

You need to deploy an Azure SQL database that uses Transparent Data Encryption (TDE) and a customer-managed key.

What should you create before you deploy the database?

- A. An app registration
- B. A standard general-purpose v2 storage account
- C. A user-assigned managed identity
- D. A user account that is assigned the SQL Security Manager role

Answer: C

Explanation:

Question: 445

HOTSPOT

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

Name	Type
	Standard
Polini	Premium

The subscription contains the firewalls shown in the following table.

Name	Tier	Hfcy
rwi	Premium	Palsy?
FW2	Premium	Policy 1

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

Name	Firewall
VNet1	
VNet2	FW2
VNet3	Mase

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 use URL filtering on the network rules for VNet1

You can use an intrusion detection and prevention system (IDPS) to monitor malicious activity on VNet2

If you configure peering between VNet1 and VNet1, encrypted outbound traffic from VNet1 will be inspected.

Answer:

Explanation:

Answer Area

Statements

Yes No

You can use URL filtering on the network rules for VNet1

0 IF

You can use an intrusion detection and prevention system (IDPS) to monitor malicious activity on VNet1

•

If you configure peering between VNet1 and VNet1, encrypted outbound traffic from VNet1 will be inspected.

Question: 446

You have an Azure subscription that contains an Azure key vault named Vault1 and a virtual machine named VM1. VM1 is connected to a virtual network named VNet1.

You need to allow access to Vault1 only from VM1.

What should you do in the Networking settings of Vault1?

- A. From the Firewalls and virtual networks tab, set Allow trusted Microsoft services to bypass this firewall to Yes for Vault1.
- B. From the Firewalls and virtual networks tab, add the IP address of VM1.
- C. From the Firewalls and virtual networks tab, add VNet1.
- D. From the Private endpoint connections tab, create a private endpoint for VM1.

Answer: D

Explanation:

Question: 447

You have two Azure subscriptions named Sub1 and Sub2 that contain the virtual networks shown in the following table.

Name	Subscription	Tag
VNet1	Sub1	Blue
VNet2	Sub1	Red

You have an Azure Virtual Network Manager instance named AVNM1 that has the following configurations:

- * Management scope: Sub1
- * Network groups:
 - * NetGrp1: Static membership that includes VNet1
 - * NetGrp2: Dynamic membership that has the following criteria: Tags that contain Red
- * Security admin rule collection: SARule1
- * Deployed to all Azure regions

Name	Subscription	Tag
VNet3	Sub1	Red
VNet4	Sub2	Red

You create two new virtual networks as shown in the following table. Which virtual networks will have SARule1 applied?

- A. VNet1 and VNet2 only
- B. VNet2 and VNet3 only
- C. VNet1, VNet2, and VNet3 only
- D. VNet2, VNet3, and VNet4 only
- E. VNet1, VNet2, VNet3, and VNet4

Answer: C

Explanation:

Question: 448

You have an Azure subscription.

You plan to create a workflow automation in Microsoft Defender for Cloud that will automatically remediate a security vulnerability.

What should you create first?

- A. an Azure function app
- B. an automation account
- C. a managed identity
- D. an alert rule
- E. an Azure logic app

Answer: E

Explanation:

Question: 449

HOTSPOT

You have a Microsoft Entra tenant named contoso.com that contains the users shown in the following table.

KB iti4	Role
User1	^?i'c: cn Adm initiator
L5EF2	Apphcottoi Developef
UMfJ	A;u:t Pw?ih torr initial. l
UserM	SKwity Operator

You add enterprise applications to contoso.com as shown in the following table.

Name	Owner	U\$ws and groups.
top'	User1	U5ET4
*PP2	User4	Lti3

You need to Identify which users can grant admin consent for App1 and App2.

Answer Area

App1:

- User1 only
- User1 and User2 only
- User1 and User3 only
- User1, User2, and User3 only
- User1, User2, User3, and User4

App2:

- User1 only
- User1 and User2 only
- User1 and User4 only
- User1, User2, and User4 only
- User1, User2, User3, and User4

Answer:

Explanation:

Answer Area

App 1: User 1 and User3 only

App2: User 1 and User4 only

Question: 450

HOTSPOT

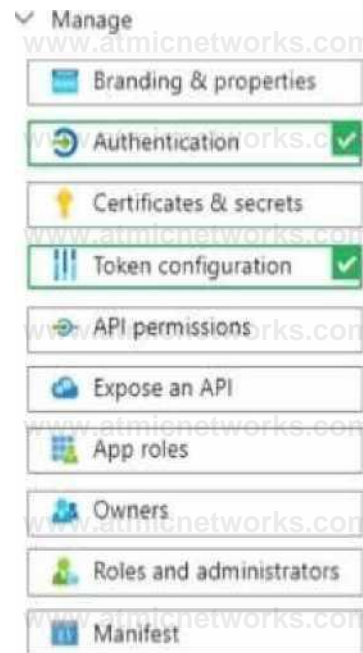
You have an Azure subscription that is linked to a Microsoft Entra tenant named contoso.com. In contoso.com, you register an app named App1. You need to perform the following tasks for App1:

- Add and configure the Mobile and desktop applications platform.
- Add the ipaddr optional claim.

Which two settings should you select for App1? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

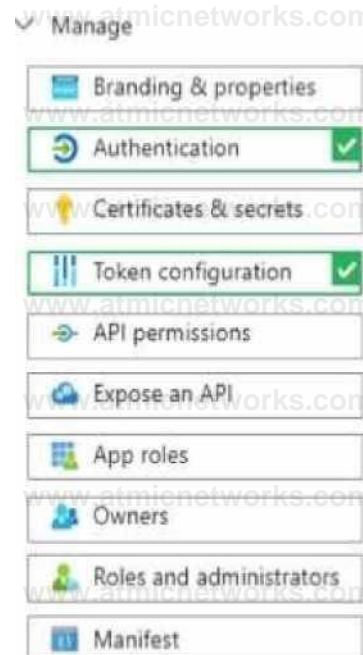
Answer Area



Answer:

Explanation:

Answer Area



Question: 451

You have a Microsoft Entra tenant that contains a user named User1.

You have an app registration named App1.

For App1, you create an app role named Role1.

You need to assign User1 to Role1.

What should you use in the Azure portal?

- A. Roles and administrators for App1 from Enterprise applications
- B. App roles for App1 from App registrations
- C. Users and groups for App1 from Enterprise applications
- D. API permissions for App1 from App registrations
- E. Roles and administrators from the Microsoft Entra admin center

Answer: C

Explanation:

Question: 452

HOTSPOT

You have an on-premises server named Server1.

You have an Azure subscription that contains a Microsoft Sentinel workspace named Sentinel 1.

You install the Windows Firewall solution in Sentinel1.

You need to use Microsoft Sentinel to monitor Windows Defender Firewall on Server1.

What should you install on Server1, and what should you create in the Azure subscription? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

- Server!:
- The Azure Connected Machine agent
 - An Azure Pipelines agent
 - An on premises data gateway
 - The Azure Connected Machine agent
 - The Microsoft Inta provisioning agent

- Subscription:
- A data collection rule (DCR)
 - A data collection endpoint (DCE)
 - A data collection rule (DCR)
 - A private endpoint
 - An Azure Private Link service

Answer:

Explanation:

Answer Area

Server!: The Azure Connected Machine agent

Subscription: A data collection rule (DCR)

Question: 453

HOTSPOT

You have an Azure key vault named sk2311 configured as shown in the following exhibit.

sk2311 | Properties ☆



Key vault

Refresh

sk2311

Name

Standard

Sku (Pricing tier)

eastus

Location

https://sk2311.vaultaiufe.net/ ©

Vault URI

/subscriptions/7fefd66e-8694-4bS4-beae-... ©

Resource ID

7fefd66e-8694-4bS4-beae-17fd819d4873 S

Subscription ID

Visual Studio Enterprise Subscription

Subscription Name

5 864e7 3 5-7190-4 615>b2aO-Ob2O6l5b7 5de S

Directory ID

Default Directory lb

Directory Name

Soft delete has been enabled on this key vault

Soft-delete

[W ']

Days to retain deleted vaults

(•) Disable purge protection (allow key vault and objects to be purged during retention period)

Purge protection

Q Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)

Sk2311 contains the items shown in the following table.

Name	Type
Item1	Key
Item 2	Secret
Policy1	Access policy

In sk2311, 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.

Answer Area

Statements	Yes	No
You can recover Policy 1.	<input type="radio"/>	<input type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input type="radio"/>
You can recover ItemZ.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Answer Area

Statements	Yes	No
You can recover Policy 1.	<input type="radio"/>	<input checked="" type="radio"/>
You can add a new key named Item 1.	<input checked="" type="radio"/>	<input type="radio"/>
You can recover ItemZ.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 454

You have an Azure subscription.

You plan to use Microsoft Defender for Cloud to provide AI security posture management capabilities.

You need to recommend a Defender for Cloud plan that supports the deployment requirements. The solution must minimize costs.

What should you recommend?

- A. Microsoft Defender for App Service
- B. Microsoft Defender for APIs
- C. Foundational Cloud Security Posture Management (CSPM)
- D. Defender Cloud Security Posture Management (CSPM)

Answer: C

Explanation:

Question: 455

HOTSPOT

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

Defender for Cloud has the security alerts shown in the following exhibit.

0 3

Open alerts

v3

Active alerts

Oo

In progress alerts

*1

Affected resources

Ip Search by ID, IP, name, or affecte...

Subscription xs All Status ■■ Active, Resolved, In Progress -

Answer Area

If you change the status of the alert that was triggered at 05:11 PM to Dismissed, [answer choice].

- the alert will no longer be visible
- the alert activity start time will change
- the alert severity will change to Low
- the alert will no longer be visible
- the status of all four alerts will change

The status of the alert that was triggered at 12:44 PM [answer choice].

- can be changed to Active, In Progress, or Dismissed
- can be changed to Active only
- can be changed to Active or Dismissed only
- can be changed to Active, In Progress, or Dismissed
- can be changed to In Progress or Dismissed only
- cannot be changed

Severity = Low, Medium, High X *y Add filter

Severity	Alert name	Affected resource	Activity start time	MITRE ATT&...	Status
Medium	Suspicious authentication activity	VM-4	01/29/24,05:11 PM	Pre-attack	Active
Medium	Suspicious authentication activity	VM-4	12/02/23,11:39 PM	Pre-attack	Active
Medium	Suspicious authentication activity	VM-4	12/02/23,11:18 PM	Pre-attack	Active
Medium	Suspicious authentication activity	VM-4	12/01/23,12:44 PM	Pre-attack	Resolved

Answer:

Explanation:

Answer Area

If you change the status of the alert that was triggered at 05:11 PM to Dismissed (answer choice).

the alert will no longer be visible

The status of the alert that was triggered at 12:44 PM (answer choice)

can be changed to Active, In Progress, or Dismissed

Question: 456

HOTSPOT

You have an Azure subscription named Sub1 and use Microsoft Defender for Cloud. Sub1 contains a user named User1 and a resource group named RG1. RG1 contains a Log Analytics workspace named Workspace1. You need to ensure that User1 can modify Azure Logic Apps workflows triggered in response to security incidents. The solution must follow the principle of least privilege.

Which role should you assign to User1, and to which resource should you assign the role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Role:

- Contributor
- Logic App Contributor
- Logic App Operator
- Microsoft Sentinel Automation Contributor
- Microsoft Sentinel Contributor

Resource:

- RG1
- Sub1
- Workspace1

Answer:

Explanation:

Answer Area

Role:

Resource:

Question: 457

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

Name	Description
App1	Azure App Service app in a Premium plan
SQL1	Azure SQL managed instance
storage1	Azure Storage account
Function1	Azure functions function in a Consumption plan

App1 uses Function 1, SQL1, and storage 1.

You need to secure the traffic between App1, Function1, SQL1, and storage1, by using private endpoints. With which resources can App1 communicate by using a private endpoint?

- A. SQL1 only
- B. storage1 only
- C. Function1 only
- D. SQL1 and storage1 only

- E. storage1 and Function1 only
- F. storage1, SQL1, and Function1

Answer: F

Explanation:

Question: 458

You have an Azure subscription that contains the Azure App Service apps shown in the following table.

Name	App Service plan
App1	Free
App2	Shared
App3	Basic
App4	Standard

You purchase custom SSL certificates from a trusted third-party authority. To which apps can you assign the custom SSL certificates?

- A. App4 only
- B. App3 and App4 only
- C. App2, App3, and App4 only
- D. App1, App2, App3, and App4

Answer: B

Explanation:

Question: 459

You have an Azure subscription that contains an Azure SQL server named sqlsrv1 and an Azure SQL database named DB1. sqlsrv1 is configured for Microsoft Entra authentication only.

You have the Microsoft Entra identities shown in the following table.

Name	Type	Description	Role for DB1
User1	User	Atone	db_owner
User2	User	Member of Group1	Atone
User3	User	Member of Group2	Atone
Group1	Group	User2 and Group2 are members	db_owner
Group2	Group	Member of Group1	Atone

Which users can create scoped credentials for DB1?

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

Answer: C

Explanation:

Question: 460

HOTSPOT

Your company uses cloud-based resources from the following platforms:

- Azure
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

You plan to implement Microsoft Defender for Cloud.

On which platforms can you use Defender for Cloud to protect containers and storage? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Containers: Azure, AWS, and GCP

Azure only

Azure and AWS only

Azure and GCP only

Storage: Azure only

Azure only

Azure and AWS only

Azure and GCP only

Answer:

Explanation:

Answer Area

Containers: **Azure, AWS, and GCP**

Storage: **Azure only**

Question: 461

HOTSPOT

You have an Azure subscription that contains a virtual network named VNet1. VNet1 contains the subnets shown in the following table.

Name	IP address space
Subnet1	10.10.0.0/24
Subnet?	172.6.0.0/24
Subnet^	192.168.10.0/24

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

Name	Connected to
VM1	Subnet1
VM?	Subnet?
VM3	Subnet 5

VM3 contains a service that listens for connections on port 8080.

For VM1, you configure just-in-time (JIT) VM access as shown in the following exhibit.

Home > Just-in-time VM access >

JIT VM access configuration

VM1

Add 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	CIDR	10.10.0.0/24 192.168.10.0/24	3 hours
8080	Any	Per request	N/A	5 hours

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 establish a Remote Desktop connection from VM1 to VMS for a maximum of three hours.	<input type="radio"/>	<input type="radio"/>
You can establish a Remote Desktop connection from VM2 to VM1 after requesting access.	<input type="radio"/>	<input type="radio"/>
You can establish a Remote Desktop connection from VMS to VM1 without requesting access.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Answer Area

Statements	Yes	No
You can establish a Remote Desktop connection from VM1 to VM3 for a maximum of three hours.	<input type="radio"/>	<input type="radio"/>
You can establish a Remote Desktop connection from VM2 to VM1 after requesting access.	<input type="radio"/>	<input type="radio"/>

Question: 462

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 that contains an Azure Kubernetes Service (AKS) cluster named AKS1 and an Azure container registry named AZCR1.

You need to ensure that AKS1 can deploy container images stored in AZCR1.

Solution: You assign the AcrPush role-based access control (RBAC) role to the system-assigned managed identity of AKS1.

Does this meet the requirement?

- A. Yes
- B. No

Answer: B

Explanation:

Question: 463

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 that contains an Azure Kubernetes Service (AKS) cluster named AKS1 and an Azure container registry named AZCR1.

You need to ensure that AKS1 can deploy container images stored in AZCR1.

Solution: You assign the Kubernetes Agentless Operator role to the system-assigned managed identity of the agent pool for AKS1.

Does this meet the requirement?

- A. Yes
- B. No

Answer: B

Explanation:

Question: 464

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 that contains an Azure Kubernetes Service (AKS) cluster named AKS1 and an Azure container registry named AZCR1.

You need to ensure that AKS1 can deploy container images stored in AZCR1.

Solution: You configure AKS1 to use a user-assigned managed identity and assign the Azure Kubernetes Service Cluster Admin Role to the managed identity.

Does this meet the requirement?

- A. Yes
- B. No

Answer: A

Explanation:

Question: 465

You have a Microsoft Entra tenant named contoso.com that contains a user named User1.

You register an app named App1 in contoso.com and create an app role named Role1.

You need to assign Role1 to User1.

What should you configure on the Enterprise applications blade of App1 in the Microsoft Entra admin center?

- A. API permissions
- B. App roles
- C. Users and groups
- D. Roles and administrators

Answer: C

Explanation:

Question: 466

You have an Azure subscription that uses Microsoft Defender.

You enable the CIS Microsoft Azure Foundations Benchmark v2.0.0 built-in to the subscription.

You need to ensure that when users attempt to assign custom role-based access control (RBAC) roles, they receive a custom error message that includes a link to an internal website. The solution must minimize the impact on other policies.

What should you configure?

- A. the effect of the policy
- B. the remediation task of the policy
- C. a policy-specific non-compliance message
- D. the default non-compliance message of the built-in

Answer: C

Explanation:

Question: 467

HOTSPOT

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

You plan to use the Secure Score Over Time workbook.

You need to configure the Continuous export settings for the Defender for Cloud data.

Which two settings should you configure? To answer, select the appropriate settings in the answer area.

NOTE: Each correct selection is worth one point.

Settings | Continuous export

Visual Studio Enterprise Subscription

Save

Continuous export

Configure streaming export setting of Defender for Cloud data to multiple export targets.

Exporting Defender for Cloud's data also enables you to use experiences such as integration with 3rd-party SIEM and Azure Data Explorer.

[Learn More >](#)

Event hub **Log Analytics workspace**

Export enabled: On Off

Exported data types

<input type="checkbox"/> Security recommendations	No selected recommendation
<input checked="" type="checkbox"/> Secure score ⓘ	Overall score, Control score
Controls	All controls selected
<input type="checkbox"/> Security alerts	No selected severities
<input type="checkbox"/> Regulatory compliance	No selected standards

Export frequency

<input checked="" type="checkbox"/> Streaming updates ⓘ
<input type="checkbox"/> Snapshots (Preview) ⓘ

Answer:

Explanation:

Answer Area

Settings | Continuous export

Save



Continuous export

Export frequency

<input type="checkbox"/> Security alerts	No selected severities
<input type="checkbox"/> Regulatory compliance	No selected standards

Exported data types

<input type="checkbox"/> Security recommendations	No selected recommendation
<input checked="" type="checkbox"/> Secure score ⓘ	Overall score, Control score

Export frequency

<input checked="" type="checkbox"/> Streaming updates ⓘ
<input type="checkbox"/> Snapshots (Preview) ⓘ

Question: 468

You need to implement the planned change for storage2. The solution must meet the technical requirements for storage encryption.

- A. Create an encryption scope in storage2.
- B. Configure storage2 to use an account encryption key.
- C. Assign an Azure role-based access control (Azure RBAC) role to storage2.
- D. Enable purge protection for storage2.

Answer: A

Explanation:

Question: 469

You need to implement the function apps to meet the technical requirements. Which apps should you include in the implementation?

- A. Fa1 and Fa2 only
- B. Fa2 and Fa3 only
- C. Fa1 and Fa3 only
- D. Fa1, Fa2, and Fa3

Answer: D

Explanation:

Question: 470
HOTSPOT

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

Name	Location	Peered with
VNet1	East US	vNuL
VNet?	West US	VNet1

The virtual networks contain the subnets shown in the following table.

Answer Area

Statements

Yes

No

You can associate RT1 with SubnetO.

You can delete RT1,

When you attempt to ping VM2 from VM1, traffic is routed to 172.16.10.10.

Answer:

Explanation:

Answer Area

Statements

Yes

No

You can associate RT1 with Subnet?.

You can delete RT1

When you attempt to ping VM2 from VM1, traffic is routed to 172.16.10.10.

UHM

Question: 471

You have a Microsoft Entra tenant.

You need to prevent nonprivileged Microsoft Entra users from creating service principals in Microsoft Entra ID.

- A. From the Properties blade, set Enable Security defaults to Yes.
- B. From the Properties blade, set Access management for Azure resources to No.
- C. From the User settings blade, set Restrict access to Microsoft Entra ID administration portal to Yes.
- D. From the User settings blade, set Users can register applications to No.

Answer: D

Explanation:

Question: 472

You have a Microsoft 365 E5 subscription.

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

You have an on-premises datacenter that contains the servers shown in the following table.

You enable direct onboarding to Microsoft Defender for Cloud.

Which servers will be onboarded to Defender for Cloud?

- A. Server1 only
- B. Server2 only
- C. Server3 only
- D. Server1 and Server3
- E. Server2 and Server3
- F. Server1, Server2, and Server3

Answer: C

Explanation:

Question: 473

HOTSPOT

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 contains the inventory assets shown in the following table.

Name	Type	State
VM1	Host	Approved Inventory
VM2	Host	Dependency
VM3	Host	Monitor Only
VM4	Host	Candidate

Which assets are scanned daily, and which assets will display in the default dashboard charts? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer
Area

Scanned daily VM1, VM2, and VM3 only

VM1 only

VM1 and VM2 only

VM1, VM2, and VM3 only

VM1, VM2, VM3, and VM4

Display in the default dashboard charts: VM1 only

VM1 only

VM1 and VM2 only

VM1, VM2, and VM3 only

VM1, VM2, VM3, and VM4

Answer:

Explanation:

Answer Area

Scanned daily VM1, VM2, and VM3 only

Display in the default dashboard charts

VM1 only

Question: 474

You have an Azure subscription that uses Microsoft Defender for Cloud. The subscription contains an instance of Azure Database for PostgreSQL.

You need to ensure that an email alert is triggered when a suspected brute force attack on the database is detected. The solution must minimize administrative effort.

What should you configure?

- A. an Azure Monitor alert rule
- B. Microsoft Defender for open-source relational databases
- C. the Azure Monitor activity log
- D. the PostgreSQL Audit extension (pgAudit)

Answer: B

Explanation:

Question: 475

HOTSPOT

You have an Azure subscription that contains three storage accounts named storage1, storage2, and storage3, three Log Analytics workspaces named Analytics1, Analytics2, Analytics3, and three Azure event hubs named EventHub1, EventHub2, and EventHub3.

For Microsoft Entra ID, you create the diagnostic settings shown in the following table.

Name	tog	Storage account	Log Analytics workspace	Event hub
Setting!	AuditLogs	storage!	Analytics!	None
Setting?	ServkePiincipalSignInLogs. ManagedIdentitySignInLogs	None	Analytics?	None
Settings	SignInLogs	storage?	None	EventHub!
Setting-l	AuditLogs, PiovmoningLogs	None	Analytrcs3	EventHub?
Settings	NonInteractiveUserSignInLogs	Storages	None	Event Hub3

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 create additional Microsoft Entra diagnostic settings.	<input type="radio"/>	<input type="radio"/>
You can configure retention for locations where Settmg4 stores logs.	<input type="radio"/>	<input type="radio"/>
You can configure Setting? to have Analytics! and Analytics? as destinations.	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Answer Area

Statements	Yes	No
You can create additional Microsoft Entra diagnostic settings.	<input checked="" type="radio"/>	<input type="radio"/>
You can configure retention for locations where Settmg4 stores logs.	<input type="radio"/>	<input type="radio"/>
You can configure Setting? to have Analytics! and Analytics? as destinations.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 476

HOTSPOT

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

Name	Tier
GW1	Basic
GW?	Standard V2
GW3	WAF V2

You need to configure settings to implement URL rewrite and prevent SQL injection attacks.

Which application gateways support each requirement? To answer, select the appropriate options in the answer area

NOTE: Each correct selection is worth one point.

Answer Area



Answer:

Explanation:

Answer Area

Implement URL rewrite GW2 and GW3 only

Prevent SQL injection attacks | GW3 only

Question: 477

HOTSPOT

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

Name	Type	Resource provider
VM1	Virtual machine	Microsoft Compute
storage1	Storage account	Microsoft.Storage
WebApp1	Azure App Service web app	Microsoft.Web

You plan to use service endpoints and service endpoint policies.

Which resources can be accessed by using a service endpoint, and which resources support service endpoint policies? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Can be accessed by using a service endpoint storage1 and WebApp1 only

storage1 and WebApp1 only

- VM1 and storage1 only
- VM1 and WebApp1 only
- VM1, storage1, and WebApp1 only

Support service endpoint policies:

- storage1 only
- storage1 only
- VM1 only
- WebApp1 only
- VM1 and storage1 only
- Storage1 and WebApp1 only

Answer

Explanation:

Answer Area

Can be accessed by using a service endpoint [[Storage! and WebApp! only](#)]

Support service endpoint policies storage! only

Question: 478

You have an Azure subscription that contains an Azure API Management instance named ContosoAPI1.

You need to configure SSL 3.0 support for ContosoAPI1.

What should you do first in the Azure portal?

- A. From Certificates, add a certificate.
- B. From Protocols + ciphers, select a backend protocol.
- C. From APIs, add an API tag.
- D. From Pricing tier, change the pricing tier.

Answer: B

Explanation:

Question: 479

HOTSPOT

You have an Azure subscription that is linked to a Microsoft Entra tenant. The tenant contains the groups shown in the following table.

Name	Member of
Group1	None
Group?	Group1

The tenant contains the users shown in the following table.

Name	Member of J
User1	Group1
User?	Group?

The subscription contains the Azure SQL servers shown in the following table.

Name	Assigned server admin	Database
sqlsvr 1	User1	DB1
sqlsvr2	Group1	DB2

The servers are configured for Microsoft Entra-only authentication. For each of the following statements, select

Answer Area

Statements

Yes

No

User1 can alter the schema of DB1.

User1 can alter the schema of DB2

User? can alter the schema of DB2

Answer

Explanation:

Answer Area

Statements

Yes

No

User1 can alter the schema of DB1.

User1 can alter the schema of DB?

\$

User? can alter the schema of DB?

Question: 480

HOTSPOT

You have a hybrid Microsoft Entra tenant named contoso.com that contains a user named User1 and the servers shown in the following table.

Name	Operating system	Configuration
Server1	Windows Server 2016	Domain-joined
Server2	Windows Server: 2022	Domain-joined

The tenant is linked to an Azure subscription that contains a storage account named storage1. The storage1 account contains a file share named shares1.

User1 is assigned the Storage File Data SMB Share Contributor role for storage1.

The Security protocol settings for the file shares of storage1 are configured as shown in the following exhibit.

Security

Protocol settings

Azure Files exposes settings that let you toggle the SMB protocol to be more compatible or more secure depending on your organization's requirements. Restricting these settings may prevent some clients from being able to connect to team drives.

Profile
Custom

SMB protocol versions

SMB 2.1

SMB 3.0

SMB 3.1.1

Authentication mechanisms

NTLM v2

Kerberos

SMB channel encryption

None

AES-128-CCM

AES-128-GCM

AES-256-GCM

Kerberos ticket encryption

RC4-HMAC

AES-256

For more information on support for protocol settings in SMB 3.0 see SMB 3.0 on Windows and SMB 3.0 on Unix.

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 map share to Server1 by using the access key of storage1.		
User1 can map share to Server1 by using the user's credentials.		
User1 can map share to Server2 by using the access key of storage1.		

Answer:

Explanation:

Answer Area Statements

Statements	Yes	No
User1 can map share to Server1 by using the access key of storage1.		<input type="radio"/>
User1 can map share to Server1 by using the user's credentials.	<input checked="" type="radio"/>	

Question: 481

You have an Azure subscription that contains an Azure SQL database named SQL1. SQL1 contains the columns shown in the following table.

Name	Contains
Column1	Comments from a confidential investigation
Column2	Government ID numbers
Column3	Images
Column4	Videos

You configure SQL1 to use Always Encrypted.

You need to configure deterministic encryption. Which column supports deterministic encryption? A. Column1

- B. Column2
- C. Column3
- D. Column4

Answer: B

Explanation:

Question: 482

HOTSPOT

You have a management group named MG1 that contains an Azure subscription named Sub1. Sub1 contains the resources shown in the following table.

Name	Description
VM1	A virtual machine that has a public IP address.
VNet1	A virtual network that contains a subnet named Subnet1.
NSG1	A network security group (NSG) that is associated to Subnet1 and has a custom inbound security rule named NSGRule1 with the following settings: <ul style="list-style-type: none"> • Source: Any • Source port ranges: * • Destination: Any • Destination port ranges: * • Action: Allow • Priority: 500

You create an Azure Virtual Network Manager instance named AVNM1 that has the following configurations:

- Management scope: MG1
- Network groups:
 - o Name: Group1
 - Group members: VNet1
- Security admin configuration:
 - o Name: SAT
 - o Rule collections:
 - Name: SACollection1

- Target network groups: Group1
- Security admin rules:
 - Name: SARule1
 - Priority: 500
 - Action: Deny
 - Direction: Inbound
 - Source type: Any
 - Source port *
- A1 is deployed to all Azure regions.

You create a Virtual Network Manager instance named AVNM2 that has the following configurations:

- Management scope: Sub1
- Network groups:
 - o Name: Group2
 - Group members: VNet1
- Security admin configuration:
 - o Name: SA2
 - o Rule collections:
 - Name: SACollection2
 - Target network groups: Group2
 - Security admin rules:
 - Name: SARule2
 - Priority: 500
 - Action: Always allow
 - Direction: Inbound
 - Source type: Any
 - Source port: *
 - A2 is deployed to all Azure regions.

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

If you change Priority for NSGRule1 to 100 NSG1 will be processed before SA1 and SA2

Internet traffic is blocked to the public IP address of VM1

If you change Action for SARule1 to Allow internet traffic to the public IP address of VM1 will be enabled automatically

Answer:

Explanation:

Answer Area

Statements	Yes	No
If you change Priority for NSGRule1 to 100 NSG1 will be processed before SA1 and SA2	<input type="radio"/>	<input type="radio"/>
Internet traffic is blocked to the public IP address of VM1	<input type="radio"/>	<input type="radio"/>
If you change Action for SARule1 to Allow internet traffic to the public IP address of VM1 will be enabled automatically	<input type="radio"/>	<input type="radio"/>

Question: 483

HOTSPOT

You have an Azure subscription.

You have the following custom role-based access control (RBAC) role definition. {

```
"properties": {  
  "roleName": "custoRole",  
  "assignableScopes": [  
    "/subscriptions/<subid>"  
  ],  
  "permissions": {  
    "actions": [  
      "Microsoft.Authorization/*/*/*",  
      "Microsoft.Authorization/write",  
      "Microsoft.Authorization/elevateAccess/Action",  
      "Microsoft.Sql/servers/administrators/write",  
      "Microsoft.Sql/servers/administrators/delete"  
    ],  
    "notActions": [  
      "Microsoft.Authorization/*/*/*",  
      "Microsoft.Authorization/write",  
      "Microsoft.Authorization/elevateAccess/Action",  
      "Microsoft.Sql/servers/administrators/write",  
      "Microsoft.Sql/servers/administrators/delete"  
    ],  
    "dataActions": [],  
    "notDataActions": []  
  }  
}
```

1

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
The custom role grants a user permission to delete Azure SQL Database resources.	<input type="radio"/>	<input type="radio"/>
The custom role grants a user permission to manage the Microsoft Entra admin settings for an Azure SQL Database server	<input type="radio"/>	<input type="radio"/>
The custom role grants a user permission to reset the administrator password for instances of Azure Database for MariaDB	<input type="radio"/>	<input type="radio"/>

Answer:

Explanation:

Answer Area

Statements	Yes	No
The custom role grants a user permission to delete Azure SQL Database resources.	<input type="radio"/>	<input checked="" type="radio"/>

Question: 484
HOTSPOT

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

Name	Performance	Premium account type	Redundancy	Sub-resource
storage 1	Standard	<i>Not applicable</i>	Locally-redundant storage (LRS)	Two Azure Files shares
storage2	Premium	Page blobs	Local ly-redundant storage (LRS)	Three containers

You need to create private endpoints for the target sub-resources of the storage accounts. The solution must ensure that all the target sub-resources can be accessed by using a private endpoint. What is the minimum number of private endpoints you should create for each storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

storage1: 1

- 1
- 2
- 3
- 6

storage2: 1

- 1
- 2
- 3
- 6
- 8

S

Answer:

Explanation:

Answer Area

storage1

storage^1

Question: 485

You have an Azure subscription that contains a virtual machine named VM1.

You are creating a data collection rule (DCR) named DCR1 that will collect events from VM1.

You need to ensure that only events that have an ID of 4798 are collected.

What should you use in DCR1?

- A. a PowerShell script
- B. a T-SQL query
- C. an XPath query
- D. a KQL query

Answer: C

Explanation:

Question: 486

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals.

More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

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

Name	Type
Group1	Security group
Group2	Microsoft 365 group
Appl	App registration
Mil	User-assigned managed identity

You have The users shown in the following table.

Name	Description
User1	<ul style="list-style-type: none"> Member of Group1 and Group2 Assigned Owner role for Appl and Mil
User2	<ul style="list-style-type: none"> Member of Group1 and Group2 Assigned Owner role for Appl and MI1

You create an Azure SQL managed instance named SQL1 and enable Microsoft Entra-only authentication. You need to ensure that both User1 and User2 are set as the Microsoft Entra admin for SQL1.

Solution: You set MM as the Microsoft Entra admin for SQL1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Question: 487

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals. More than one solution in the set might solve the problem. It is also possible that none of the solutions in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

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

Name	Type
Group1	Security group
Group2	Microsoft 365 group
Appl	App registration
Mil	User-assigned managed identity

You have The users shown in the following table.

Name	Description
User1	<ul style="list-style-type: none"> Member of Group1 and Group2 Assigned Owner role for Appl and Mil
User2	<ul style="list-style-type: none"> Member of Group1 and Group2 Assigned Owner role for Appl and MI1

You create an Azure SQL managed instance named SQL1 and enable Microsoft Entra-only authentication. You need to ensure that both User1 and User2 are set as the Microsoft Entra admin for SQL1.

Solution: You set App1 as the Microsoft Entra admin for SQL1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Question: 488

Note: This section contains one or more sets of questions with the same scenario and problem. Each question presents a unique solution to the problem. You must determine whether the solution meets the stated goals.

More than one solution in the set might solve the problem. It is also possible that **none of the solutions** in the set solve the problem.

After you answer a question in this section, you will NOT be able to return. As a result, these questions do not appear on the Review Screen.

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

Name	Type
Group1	Security group
Group2	Microsoft 365 group
Appl	App registration
Mil	User-assigned managed identity

You have The users shown in the following table.

Name	Description
User1	<ul style="list-style-type: none">• Member of Group1 and Group2• Assigned Owner role for Appl and Mil
User2	<ul style="list-style-type: none">• Member of Group1 and Group2• Assigned Owner role for Appl and MI1

You create an Azure SQL managed instance named SQL1 and enable Microsoft Entra-only authentication. You need to ensure that both User1 and User2 are set as the Microsoft Entra admin for SQL1.

Solution: You set Group1 as the Microsoft Entra admin for SQL1.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Question: 489

DRAG DROP

You have an Azure subscription that contains a resource group named RG1 and an Azure policy named Policy1.

You need to assign Policy1 to RG1.

How should you complete the script? To answer, drag the appropriate values to the correct targets. Each value 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.

Values

Answer Area

- Get-AzPolicyAssignment
- Get-AzPolicyDefinition
- Get-AzPolicySetDefinition
- New-AzPolicyAssignment
- New-AzPolicyDefinition
- New-AzPolicySetDefinition
- Set-AzPolicySetDefinition
- Set-AzPolicyAssignment
- Set-AzPolicyDefinition

```
lff = Get-AzResourceGroup -Name 'RG1'  
{Policy * [ _____ ] -Name 'Policy1'  
-Name 'AuditStorageAccounts' -PolicyDefinition  
{Policy -Scope {rg.ResourceId
```

Answer:

Explanation:

Values

Answer Area

- Get-AzPolicyAssignment
- Get-AzPolicyDefinition
- Get-AzPolicySetDefinition
- New-AzPolicyAssignment
- New-AzPolicyDefinition
- New-AzPolicySetDefinition
- Set-AzPolicySetDefinition
- Set-AzPolicyAssignment
- Set-AzPolicyDefinition

```
Srg = Get-AzResourceGroup -Name '%r'  
$policy = Get-AzPolicyDefinition [ _____ ] -Name 'MicyT'  
*e^ATsGII^ATT^* -Name 'AuditStorageAccounts' -PolicyDefinition  
(Policy -Scope Srg.ResourceId
```

Question: 490

You have an Azure subscription that contains an Azure key vault.

You create a storage account named storage1.

You plan to store data in the following storage services:

- Azure Files
- Azure Blob storage
- Azure Table storage
- Azure Queue storage

For which two services can you configure data encryption by using the keys stored in the key vault?

Each correct answer presents a complete solution.

NOTE Each correct selection is worth one point.

- A. Azure Files
- B. Table storage
- C. Queue storage
- D. Blob storage

Answer: A, D

Explanation:

Question: 491

You have an Azure subscription that contains a route table named RT1. RT1 includes a route that has the following configurations:

- Name: RouteA
- IP address prefix: 192.168.0.0/24
- Next hop IP address: 172.16.10.10

You are evaluating whether to add the routes shown in the following table.

Name	IP address prefix	Next hop IP address
Route 1	192.168.0.0/16	172.16.10.20
Route2	192.168.0.0/24	172.16.10.30
RouteS	192.168.0.0/28	172.16.10.40

Which routes can you add to RT1?

- A. Route1 only
- B. Route2 only
- C. Route3 only
- D. Route1 and Route2 only
- E. Route1 and Route3 only
- F. Route2 and Route3 only

Answer: E

Explanation:

Question: 492

You have an Azure 480zsubscription that contains the resources shown in the following table.
You have the users shown in the following table.

Name	Description
User1	<ul style="list-style-type: none">Member of Group1 and Group2Assigned Owner role for App1 and MI1
User2	<ul style="list-style-type: none">Member of Group1 and Group2Assigned Owner role for App1 and MI1

Name	Type
Group1	Security group
Group2	Microsoft 365 group
App1	App registration
MI1	User-assigned managed identity

You create an Azure SQL managed instance named SQL1 and enable Microsoft Entra-only authentication. You need to ensure that both User1 and User2 are set as the Microsoft Entra admin for SQL1.

Solution: You set Group2 as the Microsoft Entra admin for SQL1.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation: