

Exam Questions az-500

Microsoft Azure Security Technologies

<https://www.2passeasy.com/dumps/az-500/>



NEW QUESTION 1

- (Exam Topic 4)

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": {
      "workspaceId": "[variable('var1')]"
    },
    "protectedSettings": {
      "workspaceKey": "[variable('var2')]"
    }
  }
}
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 2

- (Exam Topic 4)

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: AB

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associ>

NEW QUESTION 3

- (Exam Topic 4)

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

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

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

- > An Azure Sentinel workspace
- > An Azure Event Grid instance

You need to ingest the CEF messages from the NVAs to Azure Sentinel.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application, email Description automatically generated

NEW QUESTION 4

- (Exam Topic 4)

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

NEW QUESTION 5

- (Exam Topic 4)

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 storage1.	<input type="radio"/>	<input type="radio"/>
From VM1, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input type="radio"/>
From VM2, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
From VM2, you can create a container in storage1.	<input type="radio"/>	<input checked="" type="radio"/>
From VM1, you can upload data to the blob storage of storage1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, you can upload data to the blob storage of storage1.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 6

- (Exam Topic 4)

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.

- A. Mastered
- B. Not Mastered

Answer: A

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.

NEW QUESTION 7

- (Exam Topic 4)

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>

NEW QUESTION 8

- (Exam Topic 4)

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>

NEW QUESTION 9

- (Exam Topic 4)

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NEW QUESTION 10

- (Exam Topic 4)

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.	<input type="radio"/>	<input type="radio"/>
Audit events for DB2 are written to storage1 and storage2.	<input type="radio"/>	<input type="radio"/>
Storage3 can be used as an audit log destination for DB3.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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>

NEW QUESTION 10

- (Exam Topic 4)

You have an Azure SQL Database server named SQL1.

You plan to turn on Advanced Threat Protection for SQL1 to detect all threat detection types. Which action will Advanced Threat Protection detect as a threat?

- A. A user updates more than 50 percent of the records in a table.
- B. A user attempts to sign as SELECT * from table1.

- C. A user is added to the db_owner database role.
- D. A user deletes more than 100 records from the same table.

Answer: B

Explanation:

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

References:

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

NEW QUESTION 15

- (Exam Topic 4)

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, application, table Description automatically generated

NEW QUESTION 16

- (Exam Topic 4)

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

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

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

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

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

- A. Yes
- B. No

Answer: B

NEW QUESTION 17

- (Exam Topic 4)

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

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

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

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

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

Which authentication method should you instruct the developers to use?

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

Answer: C

Explanation:

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

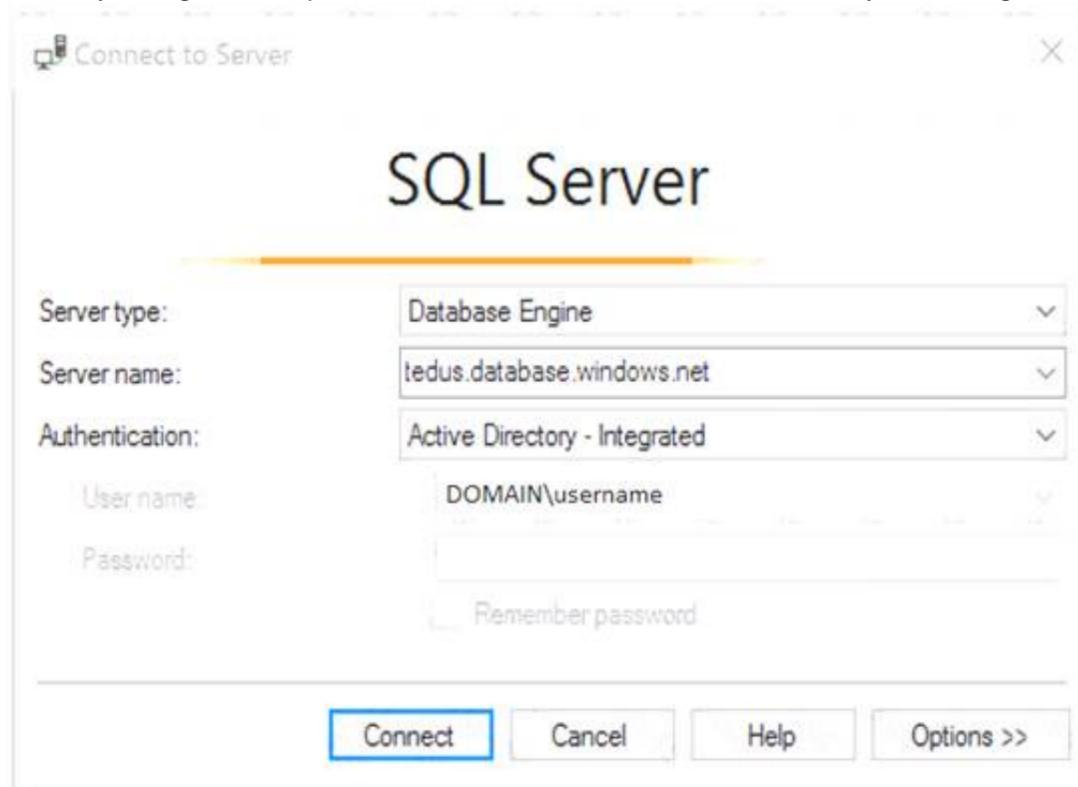
Using an Azure AD identity to connect using SSMS or SSDT

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

Active Directory integrated authentication

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

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



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

References:

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

NEW QUESTION 22

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

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

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

Azure Password: GpOAe4@IDg

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

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

Task 2

You need to add the network interface of a virtual machine named VM1 to an application security group named ASG1.

- A. Mastered
- B. Not Mastered

Answer: A

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.

NEW QUESTION 26

- (Exam Topic 4)

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

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

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

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

Answer: D

NEW QUESTION 27

- (Exam Topic 4)

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	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

The subnets of the virtual networks have the service endpoints shown in the following table.

Subnet	Service endpoint
VNET1/Subnet1	Microsoft.Storage
VNET1/Subnet2	Microsoft.KeyVault
VNET2/Subnet1	Microsoft.Storage, Microsoft.KeyVault

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.	<input type="radio"/>	<input type="radio"/>
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	<input type="radio"/>	<input type="radio"/>
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
Connections from VM1 to storage1 always use IP address 10.1.1.5.	<input checked="" type="radio"/>	<input type="radio"/>
Connections from VM2 to Vault1 always use IP address 20.224.219.230.	<input type="radio"/>	<input checked="" type="radio"/>
Authentication from VM3 to the tenant uses either IP address 10.11.1.5 or 40.122.155.212.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 29

- (Exam Topic 4)

You are troubleshooting a security issue for an Azure Storage account.

You enable the diagnostic logs for the storage account. What should you use to retrieve the diagnostics logs?

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

Answer: D

Explanation:

References:

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

NEW QUESTION 32

- (Exam Topic 4)

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

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

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

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

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

Name	Assignment type
User1	Active
User2	Eligible
user3	Eligible

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

YES (Already active)

YES (The user will be prompted for MFA regardless the MFA Status of the user) NO (Even the user is included in the group, a user can't approve itself)
<https://docs.microsoft.com/es-es/azure/active-directory/privileged-identity-management/pim-deployment-plan> (Require approval section)

NEW QUESTION 33

- (Exam Topic 4)

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

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

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

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

On which virtual machines is the 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>

NEW QUESTION 38

- (Exam Topic 4)

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>

NEW QUESTION 43

- (Exam Topic 4)

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

NEW QUESTION 45

- (Exam Topic 4)

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

Name	Type	Attached to	NSG
NSG1	Network security group (NSG)	VM5	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

VM5

+ Add Save Discard

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

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

You enable JIT VM access for VM5.

NSG1 has the inbound rules shown in the following exhibit.

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

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 46

- (Exam Topic 4)

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

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

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

- A. an event hub
- B. a storage account
- C. a Log Analytics workspace

Answer: C

Explanation:

Reference:

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

NEW QUESTION 48

- (Exam Topic 4)

You have an Azure subscription.

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

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

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

NOTE: Each correct selection is worth one point.

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

Answer: BF

Explanation:

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

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

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

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

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

NEW QUESTION 50

- (Exam Topic 4)

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>

NEW QUESTION 53

- (Exam Topic 4)

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-anaccou>

NEW QUESTION 55

- (Exam Topic 4)

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

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

You have an Azure Subscription. The subscription contains 50 virtual machines that run Windows Server 2012 R2 or Windows Server 2016.

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

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

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

References:

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

NEW QUESTION 59

- (Exam Topic 4)

You have a file named File1.yaml that contains the following contents.

```
apiVersion: 2018-10-01
location: eastus
name: containergroup1
properties:
  containers:
  - name: container1
    properties:
      environmentVariables:
      - name: 'Variable1'
        value: 'Value1'
      - name: 'Variable2'
        secureValue: 'Value2'
      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

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 64

- (Exam Topic 4)

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

Name	Member of	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.	<input type="radio"/>	<input type="radio"/>
If User2 signs in from an anonymous IP address, she must change her password.	<input type="radio"/>	<input type="radio"/>
If User3 signs in from a computer containing malware that is communicating with known bot servers, he must change his password.	<input type="radio"/>	<input type="radio"/>

A. Mastered
 B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 66

- (Exam Topic 4)

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>

NEW QUESTION 68

- (Exam Topic 4)

You have an Azure subscription that contains the storage accounts shown in the following, table.

Name	Performance	Account kind	Azure Data Lake Storage Gen2
storage1	Standard	BlobStorage	Enabled
storage2	Premium	BlockBlobStorage	Disabled
storage3	Standard	Storage	Disabled
storage4	Premium	FileStorage	Disabled
storage5	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 storage5 services:

Protected storage accounts:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Monitored storage5 services:

Protected storage accounts:

NEW QUESTION 73

- (Exam Topic 4)

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

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

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

NOTE: Each correct selection is worth one point.

Assign role to:

- A group account
- A system-assigned managed identity
- A user account
- A user-assigned managed identity

Role assignment to create:

- Built-in role assignment
- Classic administrator role assignment
- Custom role-based access control (RBAC) role assignment

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 75

- (Exam Topic 4)

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

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

Save Discard Add client IP

Deny public network access Yes No

Click here to create a new private endpoint.
[Create Private Endpoint](#)

Minimum TLS Version 1.0 1.1 1.2

Connection Policy Default Proxy Redirect

Allow Azure services and resources to access this server Yes No

Client IP address 89.212.25.106

Rule name	Start IP	End IP
<input type="text"/>	<input type="text"/>	<input type="text"/>

No firewall rules configured.

Virtual networks
[+ Add existing virtual network](#) [+ Create new virtual network](#)

Rule name	Virtual network	Subnet
No vnet rules for this server.		

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

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

Answer: C

NEW QUESTION 76

- (Exam Topic 4)

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

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

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

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 77

- (Exam Topic 4)

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

Name	Type	Region	Resource group
Sa1	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: B

Explanation:

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

NEW QUESTION 78

- (Exam Topic 4)

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.

```

Name : DenyStorageAccess
Description :
Protocol : *
SourcePortRange : (*)
DestinationPortRange : (*)
SourceAddressPrefix : (*)
DestinationAddressPrefix : (Storage)
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Deny
Priority : 105
Direction : Outbound

Name : StorageEA2Allow
ProvisioningState : Succeeded
Description :
Protocol : *
SourcePortRange : (*)
DestinationPortRange : (443)
SourceAddressPrefix : (*)
DestinationAddressPrefix : (Storage/EastUS2)
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Allow
Priority : 104
Direction : Outbound

Name : Contoso_FTP
Description :
Protocol : TCP
SourcePortRange : (*)
DestinationPortRange : (21)
SourceAddressPrefix : (1.2.3.4/32)
DestinationAddressPrefix : (10.0.0.5/32)
SourceApplicationSecurityGroups : []
DestinationApplicationSecurityGroups : []
Access : Allow
Priority : 504
Direction : Inbound
    
```

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.

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

- A. Mastered
- B. Not Mastered

Answer: A

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>

NEW QUESTION 81

- (Exam Topic 4)

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

NEW QUESTION 82

- (Exam Topic 4)

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
table1	Table

In storage1, you create a shared access signature (SAS) named SAS1 as shown in the following exhibit.

Allowed services ⓘ

Blob File Queue Table

Allowed resource types ⓘ

Service Container Object

Allowed permissions ⓘ

Read Write Delete List Add Create Update Process Immutable storage

Allowed blob index permissions ⓘ

Read/Write Filter

Start and expiry date/time ⓘ

Start: 01/01/2022 12:00:00 AM

End: 01/01/2023 12:00:00 AM

(UTC+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague

Allowed IP addresses ⓘ

For example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ

HTTPS only HTTPS and HTTP

Preferred routing tier ⓘ

Basic (default) Microsoft network routing Internet routing

i Some routing options are disabled because the endpoints are not published.

Signing key ⓘ

key1

Generate SAS and connection string

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

SAS1:

Key1:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area



NEW QUESTION 87

- (Exam Topic 4)

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: C

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).
<https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal>

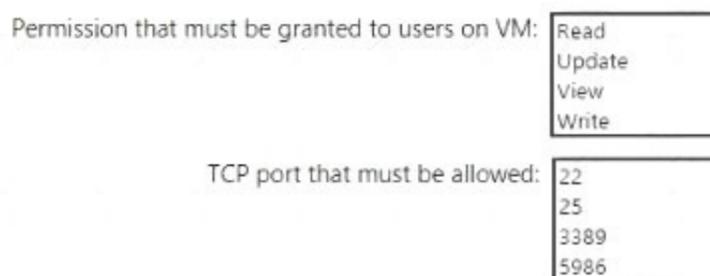
NEW QUESTION 91

- (Exam Topic 4)

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

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

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

- * 1. Read permission
- * 2. 5986

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

NEW QUESTION 93

- (Exam Topic 4)

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

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

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

D. Cloud Application Administrate

Answer: C

NEW QUESTION 95

- (Exam Topic 4)

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>

NEW QUESTION 97

- (Exam Topic 4)

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 ContosoKey1:

▼

- 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 ContosoKey1:

▼

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

<https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-guide>

NEW QUESTION 98

- (Exam Topic 4)

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 user'. User' has an email address of userl@fabrikam.com.

You to provide User1 with to the resources in the tenant The solution must meet the following requirements: > user1 must be able to sign in by using the userl@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 fabrikamcom as a custom domain
- D. Set Enable guest self-service sign up via user flows to Yes for the tenant.

Answer: B

NEW QUESTION 100

- (Exam Topic 4)

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	Not applicable
RG1	Resource group	Not applicable
VM1	Virtual machine	RG1
VNET1	Virtual network	RG1
storage	Storage account	RG1
User1	User account	Not applicable

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/*"
        ],
        "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
User1 can create a new virtual machine in RG1.	<input type="radio"/>	<input type="radio"/>
User can modify the properties of storage1.	<input type="radio"/>	<input type="radio"/>
User1 can attach the network interface of VM1 to VNET1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NO NO NO

Reference:

<https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#compute>

NEW QUESTION 103

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

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

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

Azure Password: GpOAe4@IDg

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

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

Task 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.

- A. Mastered
- B. Not Mastered

Answer: A

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.

NEW QUESTION 106

- (Exam Topic 4)

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

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

Which of the following should you set Reviewers to?

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

Answer: C

Explanation:

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

Graphical user interface, application Description automatically generated with medium confidence



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/governance/create-access-review>

<https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-programs-controls>

NEW QUESTION 110

- (Exam Topic 4)

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

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

Answer: A

NEW QUESTION 113

- (Exam Topic 4)

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>

NEW QUESTION 116

- (Exam Topic 4)

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

Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

User2 is the owner of Group2.

The user and group settings for App1 are configured as shown in the following exhibit.

You enable self-service application access for App1 as shown in the following exhibit.

User3 is configured to approve access to App1.

You need to identify the owners of Group2 and the users of App1.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/manage-self-service-access>

NEW QUESTION 117

- (Exam Topic 4)

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

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

You create the Azure policies shown in the following table.

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

You create the resource locks shown in the following table.

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

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

Answer Area

Statements	Yes	No
You can start VM1.	<input type="radio"/>	<input type="radio"/>
You can start VM2.	<input type="radio"/>	<input type="radio"/>
You can create a virtual machine in RG2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 120

- (Exam Topic 4)

You have the Azure resource shown in the following table.

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

You need to meet the following requirements:

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

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

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

Answer: D

NEW QUESTION 122

- (Exam Topic 4)

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

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 Area

⬅
➡

⬆
⬇

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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
}
```

References:

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

NEW QUESTION 126

- (Exam Topic 4)

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 ⓘ ✓

Lockout duration in seconds ⓘ ✓

Custom banned passwords

Enforce custom list ⓘ Yes No

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.	<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"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-de> <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>

NEW QUESTION 127

- (Exam Topic 4)

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.	<input type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input type="radio"/>	<input type="radio"/>
Admin3 can reset the password of Admin4.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
 Answer Area

Statements	Yes	No
Admin1 can reset the password of User1.	<input checked="" type="radio"/>	<input type="radio"/>
Admin2 can reset the password of User3.	<input checked="" type="radio"/>	<input type="radio"/>
Admin3 can reset the password of Admin4.	<input type="radio"/>	<input checked="" type="radio"/>

NEW QUESTION 131

- (Exam Topic 4)

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

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

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

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

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

NOTE: Each correct selection is worth one point.

CosmosDB1:

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

WebApp1:

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

- A. Mastered
- B. Not Mastered

Answer: A

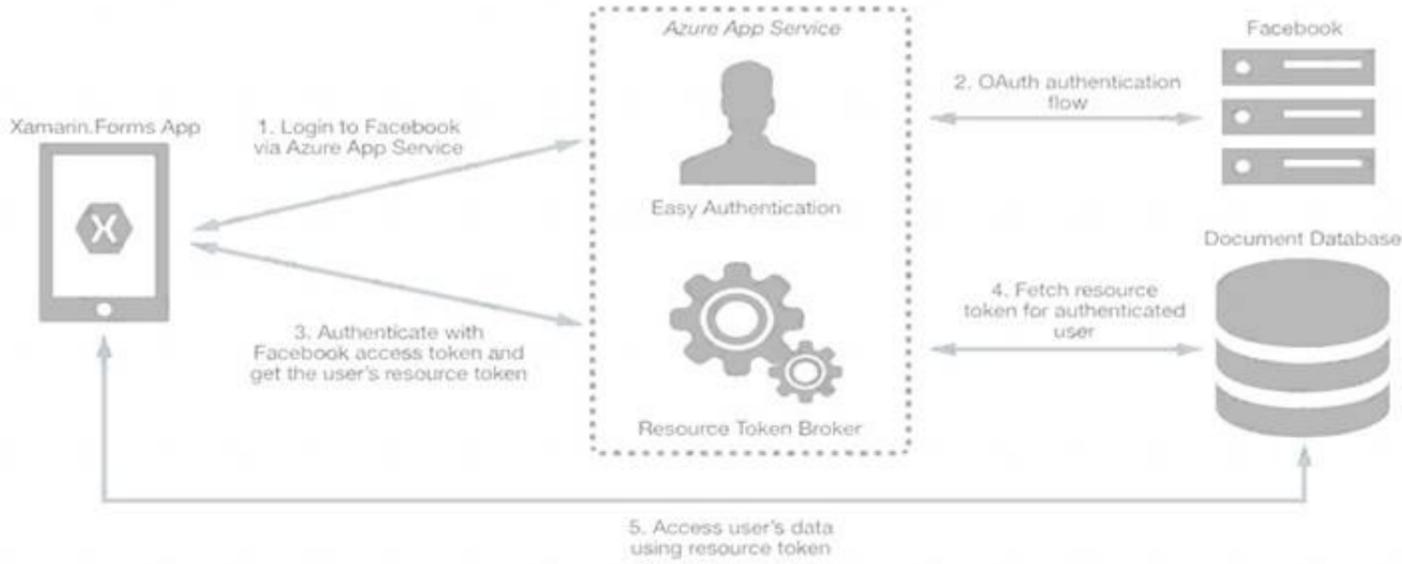
Explanation:

CosmosDB1: Create database users and generate resource tokens.

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

WebApp1: Authenticate Azure AD users and relay resource tokens

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



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

NEW QUESTION 133

- (Exam Topic 4)

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 storage3, disable the customer-managed keys.
- Disable Defender for Storage for storage3.
- Enable the Defender for Storage plan for Sub1.
- For storage3, assign the AzDefenderPlanAutoEnable tag and set the value to off.
- Enable the Defender for Storage plan for RG1.

Answer Area

- 1
- 2
- 3

Navigation icons: right arrow, left arrow, and a set of right and left arrows.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

- For storage3, disable the customer-managed keys.
- Disable Defender for Storage for storage3.
- Enable the Defender for Storage plan for Sub1.
- For storage3, assign the AzDefenderPlanAutoEnable tag and set the value to off.
- Enable the Defender for Storage plan for RG1.

Answer Area

- 1
- 2
- 3

Navigation icons: right arrow, left arrow, and a set of right and left arrows.

NEW QUESTION 135

- (Exam Topic 4)

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>

NEW QUESTION 136

- (Exam Topic 4)
 You have an Azure subscription that contains 100 virtual machines and has Azure Security Cent,-. 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: AC

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-arc/servers/onboard-service-principal>

NEW QUESTION 139

- (Exam Topic 4)
 You have an Azure subscription and the computers shown in the following table.

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

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

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

Answer: A

NEW QUESTION 143

- (Exam Topic 4)
 You have an Azure subscription that contains the resources shown in the following table.

Name	Type
storage1	Storage account
KeyVault1	Azure key vault

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

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

Answer: D

NEW QUESTION 148

- (Exam Topic 4)
 You have an Azure subscription that contains 100 virtual machines and has Azure Security Center Standard tier enabled. You plan to perform a vulnerability scan of each virtual machine. You need to deploy the vulnerability scanner extension to the virtual machines by using an Azure Resource Manager template. Which two values should you specify in the code to automate the deployment of the extension to the virtual machines? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

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

Answer: AC

NEW QUESTION 149

- (Exam Topic 4)

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

NEW QUESTION 150

- (Exam Topic 4)

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

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

You need to ensure that Update1 meets the following requirements:

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

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

Answer: D

NEW QUESTION 155

- (Exam Topic 4)

You create an Azure subscription with Azure AD Premium P2.

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

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

Actions

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

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 160

- (Exam Topic 4)

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 161

- (Exam Topic 4)
 You have an Azure subscription that contains the virtual machines shown in the following table.

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

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

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

On which virtual machines is the Microsoft Monitoring agent installed?

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

Answer: D

Explanation:

When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created.
 Supported Operating systems include: Ubuntu 14.04 LTS (x86/x64), 16.04 LTS (x86/x64), and 18.04 LTS (x64) and Windows Server 2008 R2, 2012, 2012 R2, 2016, version 1709 and 1803.
 References:
<https://docs.microsoft.com/en-us/azure/security-center/security-center-faq>

NEW QUESTION 163

- (Exam Topic 4)
 You have an Azure subscription that contains a user named UseR1. You need to ensure that UseR1 can perform the following tasks:

- Create groups.
- Create access reviews for role-assignable groups.

• Assign Azure AD roles to groups.
 The solution must use the principle of least privilege. Which role should you assign to User1?

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

Answer: C

NEW QUESTION 165

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1 and a storage account named storage 1. The storage1 account contains the resources shown in the following table:

Name	Type
container1	Container
folder1	File share
table1	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 folder1 by using SAS1, he can delete the files in folder1.	<input type="radio"/>	<input type="radio"/>
On October 1, 2022, if User1 maps folder1 as a network drive by using his Azure Active Directory (Azure AD) credentials, he can delete the files in folder1.	<input type="radio"/>	<input type="radio"/>
On October 1, 2022, User1 can delete the rows in table1 by using SAS1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

No, Yes, No

NEW QUESTION 167

- (Exam Topic 4)

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

NEW QUESTION 168

- (Exam Topic 4)

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, User3, and User 4 only

Users who can remediate users and configure policies:

- User1 and User2 only
- User1 and User3 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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, User3, and User 4 only

Users who can remediate users and configure policies:

- User1 and User2 only
- User1 and User3 only
- User1, User 2, and User3 only
- User1, User 2, User3, and User 4

NEW QUESTION 169

- (Exam Topic 4)

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

Name	Type
LB1	Azure Standard Load Balancer
VM1	Virtual machine
SQL1	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

NEW QUESTION 174

- (Exam Topic 4)

Lab Task

Task 7

You need to ensure that connections through an Azure Application Gateway named Homepage-AGW are inspected for malicious requests.

- A. Mastered
- B. Not Mastered

Answer: A

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.

NEW QUESTION 177

- (Exam Topic 4)

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

You have an Amazon Web Services (AWS) account.

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

What should you configure first?

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

Answer: A

NEW QUESTION 179

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

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

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

Azure Password: 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 9

You need to ensure that the rg1lod28681041n1 Azure Storage account is encrypted by using a key stored in the KeyVault28681041 Azure key vault.

- A. Mastered
- B. Not Mastered

Answer: A

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.

NEW QUESTION 182

- (Exam Topic 4)

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

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

You deploy and configure an Azure Key vault.

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

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

NOTE: Each correct selection is worth one point.

VM1: ▼

The operating system version

The tier

The type

VM2: ▼

The operating system version

The tier

The type

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

VM1: The Tier

The Tier needs to be upgraded to standard.

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

VM2: the operating system

References:

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

NEW QUESTION 184

- (Exam Topic 4)

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>

NEW QUESTION 186

- (Exam Topic 4)

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

You enable content trust for ConReg1.

You need to ensure that User1 can create trusted images in ConReg1. The solution must use the principle of least privilege.

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

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

Answer: CD

Explanation:

References:

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

NEW QUESTION 189

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

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

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

Azure Password: GpOAe4@IDg

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

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

Task 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.

- A. Mastered
- B. Not Mastered

Answer: A

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.

NEW QUESTION 190

- (Exam Topic 4)

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

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

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

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

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

- A. Yes
- B. No

Answer: B

NEW QUESTION 193

- (Exam Topic 4)

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

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

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

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 196

- (Exam Topic 4)

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

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

Transparent Data Encryption (TDE) is disabled on SQL1.

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

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

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

Name	Resource group	TDE
SQL2	RG2	Disabled
SQL3	RG1	Disabled

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

NOTE: Each correct selection is worth one point.

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated
 Reference:

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

NEW QUESTION 199

- (Exam Topic 4)

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

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

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

Name	Role
VM1	<ul style="list-style-type: none"> • Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM2	<ul style="list-style-type: none"> • Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1
VM3	<ul style="list-style-type: none"> • Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2
VM4	<ul style="list-style-type: none"> • Storage Blob Data Reader for storage1 • Key Vault Reader for Vault1 • Key Vault Reader for Vault2

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

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

What is the minimum number of managed identities required?

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

Answer: B

Explanation:

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

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

Reference:

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

NEW QUESTION 201

- (Exam Topic 4)

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

NEW QUESTION 203

- (Exam Topic 4) You have an Azure subscription. You plan to create a storage account.

You need to use customer-managed keys to encrypt the tables in the storage account.

From Azure Cloud Shell, which three cmdlets should you run in sequence? To answer, move the appropriate cmdlets from the list of cmdlets to the answer area and arrange them in the correct order.

Cmdlets

Answer Area

New-AzStorageAccountKey		
New-AzStorageTable	➤	⬆
Register-AzProviderFeature		⬇
New-AzStorageAccount	⬅	
Register-AzResourceProvider		

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text, table Description automatically generated with medium confidence

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-configure-key-vault?tabs=pow>

NEW QUESTION 205

- (Exam Topic 4)

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.

<p>Values</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Get-AzPolicyRemediation</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Set-AzContext</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Set-AzResourceGroup</div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;">Start-AzPolicyComplianceScan</div> <div style="border: 1px solid #ccc; padding: 5px;">Start-AzPolicyRemediation</div>	<p>Answer Area</p> <pre>\$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization/policyAssignments/Policy1" Value -Subscription "Sub1" Value -PolicyAssignmentId \$policyAssignmentId -Name "policy1" -ResourceDiscovery</pre>
--	--

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

➤ For the first blank, use Set-AzContext

to set the current subscription context.

> For the second blank, use Start-AzPolicyRemediation policy assignment.

to create and start a policy remediation for a

The final script should look like this:

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-1978-1bdbedle86as/providers/Microsoft.Authorization/f Value Set-AzContext
-Subscription "Sub1" ValuSetart-AzPolicyRemediation
-PolicyAssignmentId $policyAssignmentId -Name "policy1" -ResourceDiscovery
```

NEW QUESTION 206

- (Exam Topic 4)

You have an Azure subscription named Sub1.

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

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

Currently, you have not provisioned any network security groups (NSGs). You need to implement network security to meet the following requirements:

- > Allow traffic to VM4 from VM3 only.
- > Allow traffic from the Internet to VM1 and VM2 only.
- > Minimize the number of NSGs and network security rules.

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

NOTE: Each correct selection is worth one point.

NSGs: ▼

1
2
3
4

Network security rules: ▼

1
2
3
4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NSGs: 1
 Network security rules: 3
 Not 2: You cannot specify multiple service tags or application groups) in a security rule. References:
<https://docs.microsoft.com/en-us/azure/virtual-network/security-overview>

NEW QUESTION 210

- (Exam Topic 4)

From Azure Security Center, you enable Azure Container Registry vulnerability scanning of the images in Registry1.

You perform the following actions:

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

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

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

Answer: BC

NEW QUESTION 211

- (Exam Topic 4)

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

Answer Area

- 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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 216

- (Exam Topic 4)

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:

Assignable scope:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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>

NEW QUESTION 221

- (Exam Topic 4)

You have a Azure subscription.

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

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

* The accounts must use multi-factor authentication (MFA).

* The account must use 20-character complex passwords.

* The passwords must be changed every 180 days.

* The account must be managed by using PIM.

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

Which PIM alert should you modify?

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

Answer: D

Explanation:

Reference:

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

NEW QUESTION 222

- (Exam Topic 4)

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>

NEW QUESTION 225

- (Exam Topic 4)

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: AC

Explanation:

<https://docs.microsoft.com/en-us/azure/storage/common/account-encryption-key-create?tabs=portal>

NEW QUESTION 227

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named Contoso.com and an Azure Service (AKS) cluster AKS1.

You discover that AKS1 cannot be accessed by using accounts from Contoso.com

You need to ensure AKS1 can be accessed by using accounts from Contoso.com The solution must minimize administrative effort.

What should you do first?

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

Answer: A

Explanation:

Reference:

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

NEW QUESTION 232

- (Exam Topic 4)

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.

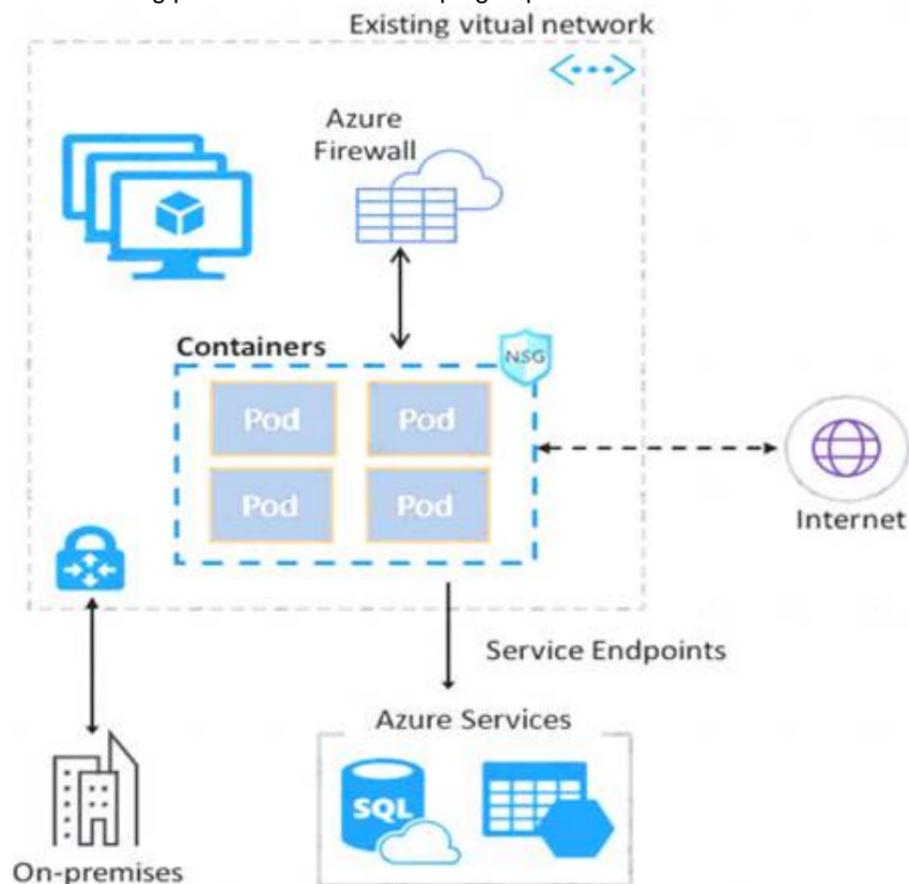
Answer: C

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:



References:

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

NEW QUESTION 235

- (Exam Topic 4)

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",  
    },  
    "then": {  
      "effect": "auditIfNotExists",  
      "details": {  
        "type": "Microsoft.Authorization/locks",  
        "existenceCondition": {  
          "field": "Microsoft.Authorization/locks/level",  
          "equals": "CanNotDelete"  
        }  
      }  
    }  
  }  
}
```

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

```
...  
  "policyRule": {  
    "if": {  
      "field": "type",  
      "equals": "Microsoft.Resources/subscriptions",  
    },  
    "then": {  
      "effect": "auditIfNotExists",  
      "details": {  
        "type": "Microsoft.Authorization/locks",  
        "existenceCondition": {  
          "field": "Microsoft.Authorization/locks/level",  
          "equals": "CanNotDelete"  
        }  
      }  
    }  
  }  
}
```

NEW QUESTION 236

- (Exam Topic 4)

You have Azure Resource Manager templates that you use to deploy Azure virtual machines. You need to disable unused Windows features automatically as instances of the virtual machines are provisioned. What should you use?

- A. device compliance policies in Microsoft Intune
- B. Azure Automation State Configuration
- C. application security groups
- D. Azure Advisor

Answer: B

Explanation:

You can use Azure Automation State Configuration to manage Azure VMs (both Classic and Resource Manager), on-premises VMs, Linux machines, AWS VMs, and on-premises physical machines.

Note: Azure Automation State Configuration provides a DSC pull server similar to the Windows Feature DSCService so that target nodes automatically receive configurations, conform to the desired state, and report back on their compliance. The built-in pull server in Azure Automation eliminates the need to set up and maintain your own pull server. Azure Automation can target virtual or physical Windows or Linux machines, in the cloud or on-premises.

References:

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

NEW QUESTION 241

- (Exam Topic 4)

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>

NEW QUESTION 242

- (Exam Topic 4)

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

Name	Type
Key1	Key
Secret1	Secret
Cert1	Certificate

Which resources support the creation of a rotation policy?

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

Answer: C

NEW QUESTION 246

- (Exam Topic 4)

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:
<https://docs.microsoft.com/en-us/azure/governance/policy/how-to/remediate-resources>

NEW QUESTION 247

- (Exam Topic 4)
 You have the Azure virtual machines shown in the following table.

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

Each virtual machine has a single network interface.
 You add the network interface of VM1 to an application security group named ASG1.
 You need to identify the network interfaces of which virtual machines you can add to ASG1. What should you identify?

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

Answer: D

Explanation:

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

NEW QUESTION 248

- (Exam Topic 4)
 You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. EASM1 has discovery enabled and contains several inventory assets.
 You need to identify which inventory assets are vulnerable to the most critical web app security risks. Which Defender EASM dashboard should you use?

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

Answer: D

NEW QUESTION 251

- (Exam Topic 4)
 You are configuring an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry.
 You need to use the auto-generated service principal to authenticate to the Azure Container Registry. What should you create?

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

Answer: B

Explanation:

When you create an AKS cluster, Azure also creates a service principal to support cluster operability with other Azure resources. You can use this auto-generated service principal for authentication with an ACR registry. To do so, you need to create an Azure AD role assignment that grants the cluster's service principal access to the container registry.

References:

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

NEW QUESTION 255

- (Exam Topic 4)

Lab Task

use the following login credentials as needed:

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

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

Azure Password: GpOAe4@IDg

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

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

Task 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.

A. Mastered

B. Not Mastered

Answer: A

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>

NEW QUESTION 257

- (Exam Topic 4)

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: [Understanding the Azure Active Directory application manifest](#).

```

1 {
2   "id": "d6b00db3-7ef4-4f3c-ble7-8346f0a59546",
3   "acceptMappedClaims": null,
4   "accessTokenAcceptedVersion": null,
5   "addIns": [],
6   "allowPublicClient": null,
7   "appId": "88137405-6a75-4c20-903a-f7b18ff7d496",
8   "appRoles": [],
9   "oauth2AllowUrlPathMatching": false,
10  "createdDateTime": "2019-07-15T21:09:20Z",
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": "AKSAzureADServer",
24  "oauth2AllowIdTokenImplicitFlow": false,
25  "oauth2AllowImplicitFlow": false,
26  "oauth2Permissions": [],
27  "oauth2RequirePostResponse": false,
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>

NEW QUESTION 260

- (Exam Topic 4)

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

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

Answer: C

NEW QUESTION 262

- (Exam Topic 4)

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

Name	Role
Admin1	Global administrator
Admin2	Group administrator
Admin3	User administrator

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

Users who can create a security group named Contoso Sales:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 264

- (Exam Topic 4)

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>

NEW QUESTION 265

- (Exam Topic 4)

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

Name	Type
Item1	Key
Item2	Secret
Policy1	Access policy

In 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.	<input type="radio"/>	<input type="radio"/>
You can add a new key named Item1.	<input type="radio"/>	<input type="radio"/>
You can add a new secret named Item2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

NO. Policies cannot be recovered YES, Item1 is permanently deleted
 NO, You cannot use the same name cause Item2 is in Soft-deleted status <https://docs.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview>

NEW QUESTION 268

- (Exam Topic 4)

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

NAME	SEVERITY	MONITOR C...	ALERT STATE	AFFECT...	MONITOR SERV...	SIGNAL TYPE	FIRED TIME	SU...
Alert1	Sev4	Fired	New		ActivityLog Ad...	Log	6/6/2019, 11:23:53 ...	Azure ...
Alert1	Sev4	Fired	Acknowledged		ActivityLog Ad...	Log	6/6/2019, 11:23:52 ...	Azure ...
Alert2	Sev4	Fired	Acknowledged		ActivityLog Ad...	Log	6/6/2019, 11:23:25 ...	Azure ...
Alert2	Sev4	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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 273

- (Exam Topic 4)

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.

Authentication methods

- 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

Answer Area

User1: [Authentication method]

User2: [Authentication method]

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Authentication methods

- 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

Answer Area

User1: [Microsoft Authenticator app only]

User2: [Windows Hello for Business only]

NEW QUESTION 275

- (Exam Topic 4)

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

SKUs

Answer Area

Basic	VpnGw1	VpnGw2	VpnGw3
-------	--------	--------	--------

VNET1:	SKU
VNET2:	SKU

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 278

- (Exam Topic 4)

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:

<input type="checkbox"/> A Kusto query language query
<input type="checkbox"/> A Transact-SQL query
<input type="checkbox"/> An Azure PowerShell query
<input type="checkbox"/> An Azure Sentinel playbook

Automate responses:

<input type="checkbox"/> An Azure Functions app
<input type="checkbox"/> An Azure PowerShell script
<input type="checkbox"/> An Azure Sentinel playbook
<input type="checkbox"/> An Azure Sentinel workbook

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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>

NEW QUESTION 279

- (Exam Topic 4)

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



You create the Azure Blueprints definitions shown in the following table.

Name	Published at
Blueprint1	Tenant Root Group
Blueprint2	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.

Blueprint1:

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

Blueprint2:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Blueprints can only be assigned to subscriptions.

NEW QUESTION 281

- (Exam Topic 4)

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

NEW QUESTION 286

- (Exam Topic 4)

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
Managed1	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.

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.	<input type="radio"/>	<input type="radio"/>
User2 is a member of Group2 only.	<input type="radio"/>	<input type="radio"/>
Managed1 is a member of Group1 and Group2.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated

Reference:

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

NEW QUESTION 289

- (Exam Topic 4)

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

Name	Subscription role	Azure Active Directory (Azure AD) user role	Multi-factor authentication (MFA) status
User1	Owner	Authentication administrator	Enabled
User2	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>

NEW QUESTION 291

- (Exam Topic 4)

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.

Save Discard

Allow access from: All networks Selected networks

[Configure network access control for your key vault. Learn More](#)

Virtual networks: [+ Add existing virtual networks](#) [+ Add new virtual network](#)

VIRTUAL NETWORK	SUBNET	RESOURCE GROUP	SUBSCRIPTION
VNET1	default	RG1	...

Firewall: [i](#)

IPv4 ADDRESS OR CIDR

...

Exception:

Allow trusted Microsoft services to bypass this firewall? Yes No

[i](#) 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.	<input type="radio"/>	<input type="radio"/>
From VM2, users can manage the keys and secrets stored in KeyVault1.	<input type="radio"/>	<input type="radio"/>
VM2 can use KeyVault for Azure Disk Encryption	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Statements	Yes	No
From VM1, users can manage the keys and secrets stored in KeyVault1.	<input checked="" type="radio"/>	<input type="radio"/>
From VM2, users can manage the keys and secrets stored in KeyVault1.	<input checked="" type="radio"/>	<input type="radio"/>
VM2 can use KeyVault for Azure Disk Encryption	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 293

- (Exam Topic 4)

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

NEW QUESTION 298

- (Exam Topic 4)

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:

References:

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

NEW QUESTION 303

- (Exam Topic 4)

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

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

- A. From Azure CLI run the Get-AzOperationalInsightsworkspace cmdlet.
- B. From the Azure SQL Database query editor, create a Transact-SQL query.
- C. From the Azure Sentinel workspace, create a Kusto Query Language query.
- D. From Microsoft SQL Server Management Studio (SSMS), create a Transact-SQL query.

Answer: C

NEW QUESTION 308

- (Exam Topic 4)

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": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [
      "Microsoft.Compute/virtualMachines/delete"
    ],
    "dataActions": [],
  }
]
```

The permissions for Role2 are shown in the following role definition file.

```
"permissions": [
  {
    "actions": [
      "Microsoft.Compute/virtualMachines/*"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }
]
```

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
User1 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input type="radio"/>
User3 can delete VM1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
User1 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>
User2 can delete VM1.	<input type="radio"/>	<input checked="" type="radio"/>
User3 can delete VM1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 309

- (Exam Topic 4)

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

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

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

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

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

- A. Yes
- B. No

Answer: B

Explanation:

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

Reference:

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

NEW QUESTION 313

- (Exam Topic 4)

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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

<https://learn.microsoft.com/en-us/azure/active-directory/roles/groups-create-eligible>

NEW QUESTION 318

- (Exam Topic 4)

You have an Azure subscription that contains an Azure key vault named Vault1. In Vault1, you create a secret named Secret1.

An application developer registers an application in Azure Active Directory (Azure AD). You need to ensure that the application can use Secret1.

What should you do?

- A. In Azure AD, create a role.
- B. In Azure Key Vault, create a key.
- C. In Azure Key Vault, create an access policy.
- D. In Azure AD, enable Azure AD Application Proxy.

Answer: C

Explanation:

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

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

NEW QUESTION 322

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual az-500 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the az-500 Product From:

<https://www.2passeasy.com/dumps/az-500/>

Money Back Guarantee

az-500 Practice Exam Features:

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