

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": {
      "[variable('var1')]"
      "AzureADApplicationID"
      "WorkspaceID"
      "WorkspaceName"
      "WorkspaceURL"
    },
    "protectedSettings": {
      "[variable('var2')]"
      "AzureADApplicationSecret"
      "StorageAccountKey"
      "WorkspaceID"
      "WorkspaceKey"
    }
  }
}
```

- 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)

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

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

You have a hybrid configuration of Azure Active Directory (Azure AD). You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.

Solution: You deploy an Azure AD Application Proxy.

Does this meet the goal?

- A. Yes
 B. No

Answer: B

Explanation:

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

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

- > Create Azure Virtual Network.
- > Create a custom DNS server in the Azure Virtual Network.
- > Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
- > Configure forwarding between the custom DNS server and your on-premises DNS server. Reference:

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

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 that contains the storage accounts shown in the following table.

| Name | Type |
|----------|---------------------|
| storage1 | Azure Blob storage |
| storage2 | Azure Files SMB |
| storage3 | Azure Table storage |

You need to configure authorization access.

Which authorization types can you use for each storage account? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

storage1:

Shared Key only

Shared access signature (SAS) only

Azure Active Directory (Azure AD) only

Shared Key and shared access signature (SAS) only

Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

storage2:

Shared Key only

Shared access signature (SAS) only

Shared Key and shared access signature (SAS)

storage3:

Shared Key only

Shared access signature (SAS) only

Azure Active Directory (Azure AD) only

Shared Key and shared access signature (SAS) only

Shared Key, shared access signature (SAS), and Azure Active Directory (Azure AD)

- A. Mastered

B. Not Mastered

Answer: A

Explanation:

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

Reference:

<https://docs.microsoft.com/en-us/azure/storage/common/authorize-data-access>

NEW QUESTION 5

- (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 6

- (Exam Topic 4)

You have an Azure Container Registry named Registry1.

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

| User | Role |
|-------|----------------|
| User1 | AcrPush |
| User2 | AcrPull |
| User3 | AcrImageSigner |
| User4 | Contributor |

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

NOTE: Each correct selection is worth one point.

Upload images:

▼

User1 only

User1 and User4 only

User1, User3, and User4

User1, User2, User3, and User4

Download images:

▼

User2 only

User1 and User2 only

User2 ad User4 only

User1, User2, and User4

User1, User2, User3, and User4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: User1 and User4 only

Owner, Contributor and AcrPush can push images. Box 2: User1, User2, and User4

All, except AcrImageSigner, can download/pull images.

| Role/Permission | Access Resource Manager | Create/delete registry | Push image | Pull image | Delete image data | Change policies | Sign images |
|-----------------|-------------------------|------------------------|------------|------------|-------------------|-----------------|-------------|
| Owner | X | X | X | X | X | X | |
| Contributor | X | X | X | X | X | X | |
| Reader | X | | | X | | | |
| AcrPush | | | X | X | | | |
| AcrPull | | | | X | | | |
| AcrDelete | | | | | X | | |
| AcrImageSigner | | | | | | | X |

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

NEW QUESTION 7

- (Exam Topic 4)
You have an Azure subscription that contains a user named User1. You need to ensure that User1 can create managed identities. The solution must use the principle of least privilege.
What should you do?

A. Create a resource group and assign User1 to the Managed Identity Contributor role.
B. Create a management group and assign User1 the Managed Identity Operator role.
C. Create an organizational unit (OU) and assign User1 the User administrator Azure AD role.
D. Create management group and assign User1 the Hybrid Identity Administrator Azure AD role.

Answer: A

NEW QUESTION 8

- (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.
SQ11 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 9

- (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 a hybrid configuration of Azure Active Directory (AzureAD). You have an Azure HDInsight cluster on a virtual network.
You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.
Solution: You deploy the On-premises data gateway to the on-premises network. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

Instead, you connect HDInsight to your on-premises network by using Azure Virtual Networks and a VPN gateway.
 Note: To allow HDInsight and resources in the joined network to communicate by name, you must perform the following actions:
 Create Azure Virtual Network.
 Create a custom DNS server in the Azure Virtual Network.
 Configure the virtual network to use the custom DNS server instead of the default Azure Recursive Resolver.
 Configure forwarding between the custom DNS server and your on-premises DNS server. References:
<https://docs.microsoft.com/en-us/azure/hdinsight/connect-on-premises-network>

NEW QUESTION 10

- (Exam Topic 4)

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

BASICS

| | |
|-------------------------|-----------------------------|
| Subscription | Microsoft Azure Sponsorship |
| Resource group | AzureBackupRG_eastus2_1 |
| Region | East US |
| Kubernetes cluster name | akscluster2 |
| Kubernetes version | 1.1 1.5 |
| DNS name prefix | akscluster2 |
| Node count | 3 |
| Node size | Standard_DS2_v2 |
| Virtual nodes (preview) | Disabled |

AUTHENTICATION

| | |
|-------------|----|
| Enable RBAC | No |
|-------------|----|

NETWORKING

| | |
|--------------------------|-------|
| HTTP application routing | Yes |
| Network configuration | Basic |

MONITORING

| | |
|-----------------------------|----|
| Enable container monitoring | No |
|-----------------------------|----|

TAGS

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

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

Answer: A

Explanation:

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

NEW QUESTION 10

- (Exam Topic 4)

You have an app that uses an Azure SQL database.
 You need to be notified if a SQL injection attack is launched against the database. What should you do?

- A. Modify the Diagnostics settings for the database.
- B. Deploy the SQL Health Check solution in Azure Monitor.
- C. Enable Azure Defender for SQL for the database.
- D. Enable server-level auditing for the database.

Answer: C

NEW QUESTION 11

- (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.

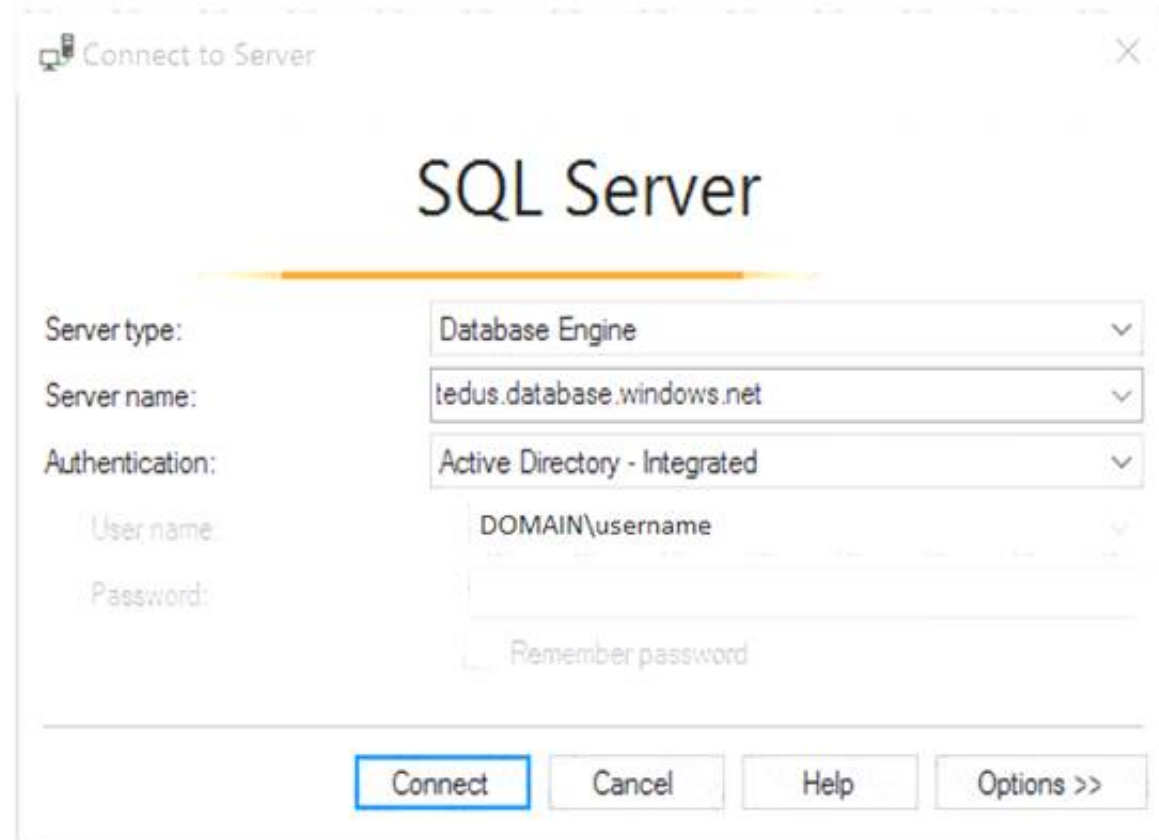
Using an Azure AD identity to connect using SSMS or SSDT

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 16

- (Exam Topic 4)

You have an Azure subscription that contains a resource group named RG1. RG1 contains a virtual machine named VM1 that uses Azure Active Directory (Azure AD) authentication.

You have two custom Azure roles named Role1 and Role2 that are scoped to RG1.

The permissions for Role1 are shown in the following JSON code.

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

The permissions for Role2 are shown in the following JSON code.

```
"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 | Role1, 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 sign in to VM1 by using Azure AD credentials. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

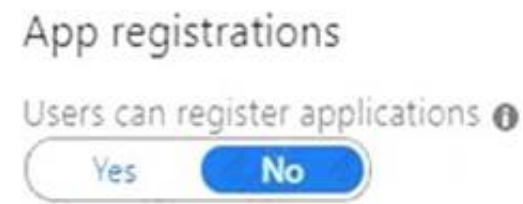
Answer Area

| Statements | Yes | No |
|---|----------------------------------|----------------------------------|
| User1 can delete VM1. | <input type="radio"/> | <input checked="" type="radio"/> |
| User2 can delete VM1. | <input checked="" type="radio"/> | <input type="radio"/> |
| User3 can sign in to VM1 by using Azure AD credentials. | <input checked="" type="radio"/> | <input type="radio"/> |

NEW QUESTION 21

- (Exam Topic 4)

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



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

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

Answer: D

Explanation:

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

NEW QUESTION 26

- (Exam Topic 4)

Lab Task
Task 6

You need to configure a Microsoft SQL server named Web3l 330471 only to accept connections from the Subnet0 subnet on the VNET01 virtual network.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Configure the firewall settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to add a firewall rule that allows inbound traffic from the IP address range of the Subnet0 subnet. You also need to disable the option to allow Azure services and resources to access this server.

Configure the network settings for the SQL server. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to enable service endpoints for SQL Server on the Subnet0 subnet. You also need to add a virtual network rule that links the SQL server to the Subnet0 subnet.

Configure the connection settings for the SQL server. You can use SQL Server Management Studio or Transact-SQL to do this. You need to enable remote server connections and specify a TCP port for listening. You also need to configure SQL Server Authentication or Azure Active Directory Authentication for connecting to the SQL server.

NEW QUESTION 31

- (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 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 36

- (Exam Topic 4)

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

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

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 39

- (Exam Topic 4)

You have an Azure subscription name Sub1 that contains an Azure Policy definition named Policy1. Policy1 has the following settings:

➤ Definition location: Tenant Root Group

➤ Category: Monitoring

You need to ensure that resources that are noncompliant with Policy1 are listed in the Azure Security Center dashboard.

What should you do first?

- A. Change the Category of Policy1 to Security Center.
- B. Add Policy1 to a custom initiative.
- C. Change the Definition location of Policy1 to Sub1.
- D. Assign Policy1 to Sub1.

Answer: D

Explanation:

Reference:

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

NEW QUESTION 44

- (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](https://www.contoso.com) 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 53

- (Exam Topic 4)

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

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

- A. TLS inspection only
- B. threat intelligence only
- C. TLS inspection and the IDPS only
- D. threat intelligence and the IDPS only
- E. TLS inspection, threat intelligence, and the IDPS

Answer: E

NEW QUESTION 56

- (Exam Topic 4)

You have 15 Azure virtual machines in a resource group named RG1. All virtual machines run identical applications.

You need to prevent unauthorized applications and malware from running on the virtual machines. What should you do?

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

Answer: B

Explanation:

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

Reference:

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

NEW QUESTION 60

- (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-anaccount>

NEW QUESTION 63

- (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 65

- (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 66

- (Exam Topic 4)

You have an Azure subscription that uses Azure Active Directory (Azure AD) Privileged Identity Management (PIM).

A PIM user that is assigned the User Access Administrator role reports receiving an authorization error when performing a role assignment or viewing the list of assignments.

You need to resolve the issue by ensuring that the PIM service principal has the correct permissions for the subscription. The solution must use the principle of least privilege.

Which role should you assign to the PIM service principle?

- A. Contributor
- B. User Access Administrator
- C. Managed Application Operator
- D. Resource Policy Contributor

Answer: B

NEW QUESTION 71

- (Exam Topic 4)

You have an Azure subscription that contains a resource group named RG1 and a security group named ServerAdmins. RG1 contains 10 virtual machines, a virtual network named VNET1, and a network security group (NSG) named NSG1. ServerAdmins can access the virtual machines by using RDP.

You need to ensure that NSG1 only allows RDP connections to the virtual machines for a maximum of 60 minutes when a member of ServerAdmins requests access.

What should you configure?

- A. an Azure policy assigned to RG1
- B. a just in time (JIT) VM access policy in Microsoft Defender for Cloud
- C. an Azure AD Privileged Identity Management (PiM) role assignment
- D. an Azure Bastion host on VNET1

Answer: B

NEW QUESTION 73

- (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 75

- (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 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 79

- (Exam Topic 4)

You have an Azure subscription.

You plan to implement Azure DDoS Protection. The solution must meet the following requirement:

* Provide access to DDoS rapid response support during active attacks.

* Project Basic SKU public IP addresses.

You need to recommend which type of DDoS projection to use for each requirement.

What should you recommend? To answer, drag the appropriate DDoS projection types to the correct requirements. Each DDoS Projection type may be used once, or not at all. You may need to drag the split bar between panes or scroll to view connect.

NOTE: Each correct selection is worth one point.

DDoS Protection types

DDoS infrastructure protection

DDoS IP Protection

DDoS Network Protection

Answer Area

Provide access to DDoS rapid response support during active attacks:

Protect Basic SKU public IP addresses:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

DDoS Protection types

DDoS infrastructure protection

DDoS IP Protection

DDoS Network Protection

Answer Area

Provide access to DDoS rapid response support during active attacks:

DDoS Network Protection

Protect Basic SKU public IP addresses:

DDoS IP Protection

NEW QUESTION 84

- (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 89

- (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 ContsosKey1.
- > 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 93

- (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 a hybrid configuration of Azure Active Directory (AzureAD). You have an Azure HDInsight cluster on a virtual network.

You plan to allow users to authenticate to the cluster by using their on-premises Active Directory credentials. You need to configure the environment to support the planned authentication.

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

- A. Yes
- B. No

Answer: A

Explanation:

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

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

Create Azure Virtual Network.

Create a custom DNS server in the Azure Virtual Network.

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

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

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

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

NEW QUESTION 95

- (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 | <i>Not applicable</i> |
| RG1 | Resource group | <i>Not applicable</i> |
| VM1 | Virtual machine | RG1 |
| VNET1 | Virtual network | RG1 |
| storage | Storage account | RG1 |
| User1 | User account | <i>Not applicable</i> |

You create an Azure role by using the following JSON file.

```
{
  "properties": {
    "roleName": "Role1",
    "description": "",
    "assignableScopes": [
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0",
      "/subscriptions/8372f433-2dcd-4361-b5ef-5b188fed87d0/resourceGroups/RG1"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Compute/*"
        ],
        "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 100

- (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 resource graph and an assignment that is scoped to a management group. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

References:

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

NEW QUESTION 104

- (Exam Topic 4)

You onboard Azure Sentinel. You connect Azure Sentinel to Azure Security Center.

You need to automate the mitigation of incidents in Azure Sentinel. The solution must minimize administrative effort.

What should you create?

- A. an alert rule
- B. a playbook
- C. a function app
- D. a runbook

Answer: B

NEW QUESTION 105

- (Exam Topic 4)

You have an Azure subscription that contains a Microsoft Defender External Attack Surface Management (Defender EASM) resource named EASM1. You review the Attack Surface Summary dashboard. You need to identify the following insights:

- Deprecated technologies that are no longer supported
- Infrastructure that will soon expire

Which section of the dashboard should you review?

- A. Securing the Cloud
- B. Sensitive Services
- C. attack surface composition
- D. Attack Surface Priorities

Answer: C

NEW QUESTION 109

- (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 118

- (Exam Topic 4)

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

- A. Azure Storage Explorer
- B. SQL query editor in Azure
- C. Azure Monitor
- D. Azure Cosmos DB explorer

Answer: A

NEW QUESTION 123

- (Exam Topic 4)

You have an Azure subscription that has a managed identity named identity and is linked to an Azure Active Directory (Azure AD) tenant. The tenant contains the resources shown in the following table.

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area.

| Name | Type | Assigned object |
|--------|---------------------|-----------------|
| AU1 | Administrative unit | User1, Group1 |
| AU2 | Administrative unit | None |
| User1 | User | Not applicable |
| Group1 | Security group | Not applicable |
| Group2 | Microsoft 365 group | Not applicable |

Which resources can be added to AU1 and AU2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

AU1:

AU2 only

Group2 only

Identity1 only

AU2 and Group2 only

Group2 and Identity1 only

AU2:

Identity1 only

AU1 and Identity1 only

Group1 and Group2 only

AU1, Group2 and Identity1 only

Group1, Group2 and User1 only

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

AU1:

AU2 only

Group2 only

Identity1 only

AU2 and Group2 only

Group2 and Identity1 only

AU2:

Identity1 only

AU1 and Identity1 only

Group1 and Group2 only

AU1, Group2 and Identity1 only

Group1, Group2 and User1 only

NEW QUESTION 124

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Data Lake Storage Gen2 account named storage1. You deploy an Azure Synapse Analytics workspace named synapsews1 to a managed virtual network. You need to enable access from synapsews1 to storage1. What should you configure?

- A. a virtual network gateway
- B. a network security group (NSG)
- C. a private endpoint
- D. peering

Answer: C

NEW QUESTION 127

- (Exam Topic 4)

You create an alert rule that has the following settings:

- > Resource: RG1
- > Condition: All Administrative operations
- > Actions: Action groups configured for this alert rule: ActionGroup1
- > Alert rule name: Alert1

You create an action rule that has the following settings:

- > Scope: VM1
- > Filter criteria: Resource Type = "Virtual Machines"
- > Define on this scope: Suppression
- > Suppression config: From now (always)
- > Name: ActionRule1

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

| Statements | Yes | No |
|---|-----------------------|-----------------------|
| If you start VM1, an alert is triggered. | <input type="radio"/> | <input type="radio"/> |
| If you start VM2, an alert is triggered. | <input type="radio"/> | <input type="radio"/> |
| If you add a tag to RG1, an alert is triggered. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1:
The scope for the action rule is set to VM1 and is set to suppress alerts indefinitely.
Box 2:
The scope for the action rule is not set to VM2. Box 3:
Adding a tag is not an administrative operation. References:
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-activity-log>
<https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-action-rules>

NEW QUESTION 128

- (Exam Topic 4)
DRAG DROP
You create an Azure subscription.
You need to ensure that you can use Azure Active Directory (Azure AD) Privileged Identity Management (PIM) to secure Azure AD roles.
Which three actions should you perform in sequence? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Actions

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

Consent to PIM.

Sign up PIM for Azure AD roles.

Discover privileged roles.

Discover resources.

Answer Area

⬅

➡

⬆

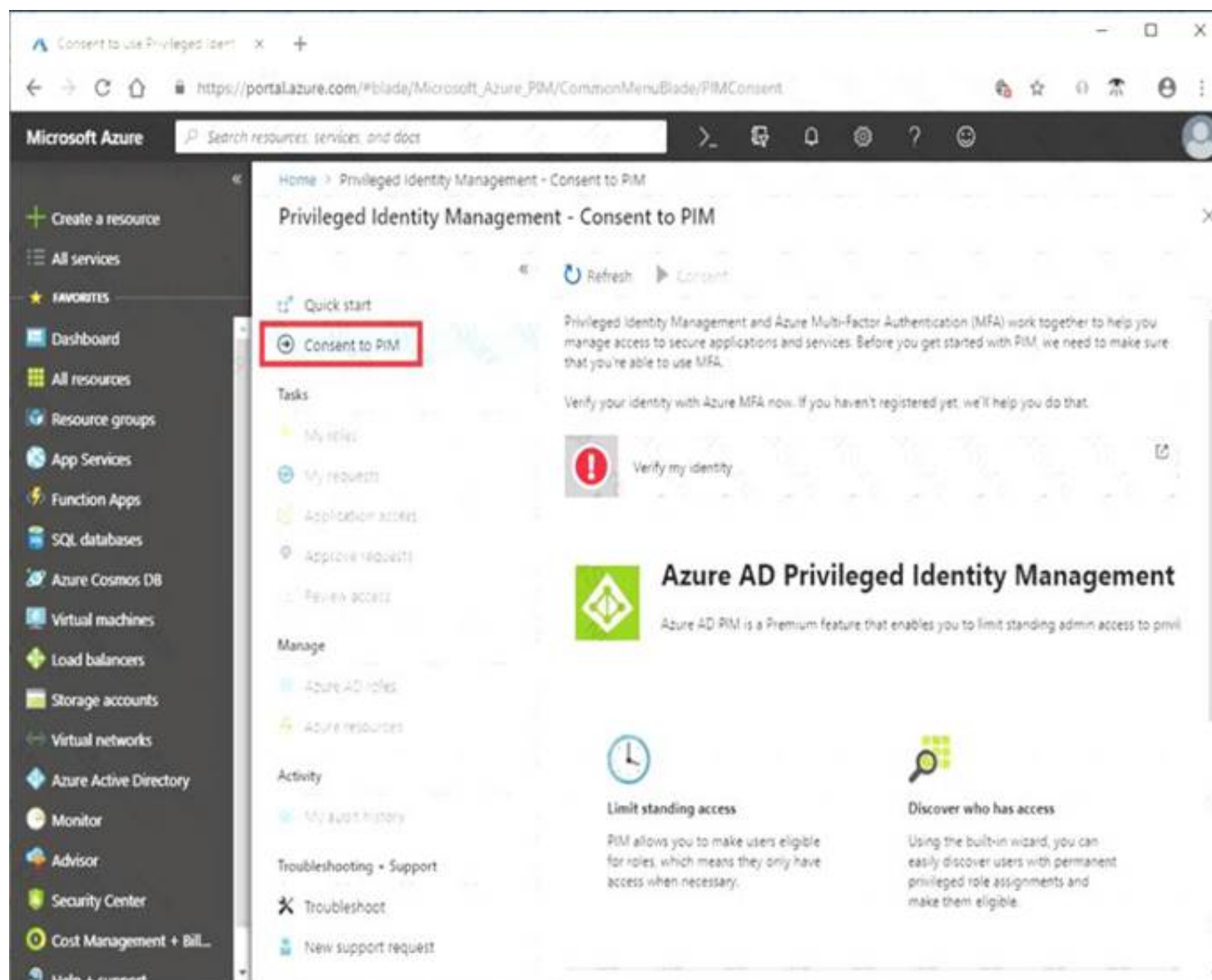
⬆

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Step 1: Consent to PIM



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

Click Verify my identity to verify your identity with Azure MFA. You'll be asked to pick an account. Step 3: Sign up PIM for Azure AD roles

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

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

NEW QUESTION 130

- (Exam Topic 4)

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

How should you complete the command? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

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

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

| | |
|--|---|
| <div>-EnabledForDeployment</div> <div>-EnablePurgeProtection</div> <div>-Tag</div> | <div>-Confirm</div> <div>-DefaultProfile</div> <div>-EnableSoftDelete</div> <div>-SKU</div> |
|--|---|

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: -EnablePurgeProtection

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

Box 2: -EnableSoftDelete

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

References:

<https://docs.microsoft.com/en-us/powershell/module/azurerm.keyvault/new-azurermkeyvault>

NEW QUESTION 131

- (Exam Topic 4)

You have an Azure subscription that uses Microsoft Defender for Cloud. You have accounts for the following cloud services:

- Alibaba Cloud
- Amazon Web Services (AWS)
- Google Cloud Platform (GCP)

What can you add to Defender for Cloud?

- A. AWS only
- B. Alibaba Cloud and AWS only

- C. Alibaba Good and GCP only
- D. AWS and GCP only
- E. Alibaba Cloud, AW
- F. and GCP

Answer: A

NEW QUESTION 132

- (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 133

- (Exam Topic 4)
You have a web app named WebApp1.
You create a web application firewall (WAF) policy named WAF1. You need to protect WebApp1 by using WAF1.
What should you do first?

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

Answer: A

Explanation:

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

NEW QUESTION 136

- (Exam Topic 4)
Your on-premises network contains a Hyper-V virtual machine named VM1. You need to use Azure Arc to onboard VM1 to Microsoft Defender for Cloud. What should you install first?

- A. the Azure Monitor agent
- B. the Azure Connected Machine agent
- C. the Log Analytics agent
- D. the guest configuration agent

Answer: B

NEW QUESTION 139

- (Exam Topic 4)

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

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

You have an Azure Subscription named Sub1.

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

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

You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to Sa1.

Solution: You generate new SASs. Does this meet the goal?

A. Yes

B. No

Answer: B

Explanation:

Instead you should create a new stored access policy.

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

References:

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

NEW QUESTION 142

- (Exam Topic 4)

You have an Azure Sentinel deployment.

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

A. a Transact-SQL statement

B. a JSON definition

C. GraphQL

D. a Kusto query

Answer: D

Explanation:

Reference:

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

NEW QUESTION 146

- (Exam Topic 4)

You have an Azure subscription.

You plan to map an online infrastructure and perform vulnerability scanning for the following:

- ASNs
 - Hostnames
 - IP addresses
 - SSL certificates
- What should you use?

A. Microsoft Defender for Cloud

B. Microsoft Defender for Identity

C. Microsoft Defender for Endpoint

D. Microsoft Defender External Attack Surface Management (Defender EASM)

Answer: A

NEW QUESTION 147

- (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 148

- (Exam Topic 4)

You have an Azure web app named webapp1.

You need to configure continuous deployment for webapp1 by using an Azure Repo. What should you create first?

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

Answer: B

Explanation:

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

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

NEW QUESTION 152

- (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 153

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant named contoso.onmicrosoft.com. The User administrator role is assigned to a user named Admin1.

An external partner has a Microsoft account that uses the user1@outlook.com sign in.

Admin1 attempts to invite the external partner to sign in to the Azure AD tenant and receives the following error message: "Unable to invite user user1@outlook.com Generic authorization exception."

You need to ensure that Admin1 can invite the external partner to sign in to the Azure AD tenant.

What should you do?

- A. From the Roles and administrators blade, assign the Security administrator role to Admin1.
- B. From the Organizational relationships blade, add an identity provider.
- C. From the Custom domain names blade, add a custom domain.
- D. From the Users blade, modify the External collaboration settings.

Answer: D

Explanation:

You need to allow guest invitations in the External collaboration settings.

NEW QUESTION 154

- (Exam Topic 4)

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

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

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

Which authentication method should you recommend?

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

Answer: D

Explanation:

References:

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

NEW QUESTION 157

- (Exam Topic 4)

You have the role assignments shown in the following exhibit.

```
{
  "RoleAssignmentId": "13ae6e22-b93a-412f-9dc5-fc82b1726bde",
  "Scope": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/resourceGroups/RG1",
  "DisplayName": "Admin1",
  "SignInName": "Admin1@contoso.com",
  "RoleDefinitionName": "Owner",
  "RoleDefinitionId": "/subscriptions/0a1baf97-0be4-424a-92fa-873c5a45fbbc/providers/
```

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.
NOTE: Each correct selection is worth one point.

[answer choice] can delete VM1.

- Only Admin1
- Only Admin1 and Admin2
- Only Admin1 and Admin3
- Only Admin1 and Admin4
- Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

- Admin1 only
- Admin2 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

[answer choice] can delete VM1.

- Only Admin1
- Only Admin1 and Admin2
- Only Admin1 and Admin3
- Only Admin1 and Admin4
- Admin1, Admin2, Admin3, and Admin4

[answer choice] can create new resource groups.

- Admin1 only
- Admin2 only
- Admin3 only
- Admin1 and Admin3 only
- Admin1, Admin2, Admin3, and Admin4

NEW QUESTION 160

- (Exam Topic 4)

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

| Name | Pattern | Case sensitivity |
|------------|---------|------------------|
| Condition1 | White | On |
| Condition2 | Black | Off |

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

| Name | Applies to | Use label | Set the default label |
|---------|----------------|-----------|-----------------------|
| Global | Not applicable | None | None |
| Policy1 | User1 | Label1 | None |
| Policy2 | User1 | Label2 | None |

You need to identify how Azure Information Protection will label files.

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

If User1 creates a Microsoft Word file that includes the text "Black and White", the file will be assigned:

▼

| |
|-------------------|
| No label |
| Label1 only |
| Label2 only |
| Label1 and Label2 |

If User1 creates a Microsoft Notepad file that includes the text "Black or white", the file will be assigned:

▼

| |
|-------------------|
| No label |
| Label1 only |
| Label2 only |
| Label1 and Label2 |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: Label 2 only

How multiple conditions are evaluated when they apply to more than one label

- The labels are ordered for evaluation, according to their position that you specify in the policy: The label positioned first has the lowest position (least sensitive) and the label positioned last has the highest position (most sensitive).
- The most sensitive label is applied.
- The last sublabel is applied.

Box 2: No Label

Automatic classification applies to Word, Excel, and PowerPoint when documents are saved, and apply to Outlook when emails are sent. Automatic classification does not apply to Microsoft Notepad.

References:

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

NEW QUESTION 162

- (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 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 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: | <div><input type="checkbox"/> User1 only</div> <div><input type="checkbox"/> User1 and User2 only</div> <div><input type="checkbox"/> User1, User 2, and User3 only</div> <div><input type="checkbox"/> User1, User 2, User3, and User 4 only</div> |
| Users who can remediate users and configure policies: | <div><input type="checkbox"/> User1 and User2 only</div> <div><input type="checkbox"/> User1 and User3 only</div> <div><input type="checkbox"/> User1, User 2, and User3 only</div> <div><input type="checkbox"/> User1, User 2, User3, and User 4</div> |

- 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 170

- (Exam Topic 4)

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

| Name | Type |
|------------|----------------|
| Container1 | Blob container |
| Share1 | File share |

You generate a shared access signature (SAS) to connect to the blob service and the file service.
Which tool can you use to access the contents in Container1 and Share1 by using the SAS? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Answer Area

Tools for Container1:

Robocopy.exe

Azure Storage Explorer

File Explorer

Tools for Share1:

Robocopy.exe

Azure Storage Explorer

File Explorer

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Tools for Container1:

Robocopy.exe

Azure Storage Explorer

File Explorer

Tools for Share1:

Robocopy.exe

Azure Storage Explorer

File Explorer

NEW QUESTION 171

- (Exam Topic 4)

You have an Azure subscription.

You need to deploy an Azure virtual WAN to meet the following requirements:

- Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.
- Ensure that security rules sync between the regions. What should you use?

- A. Azure Firewall Manager
- B. Azure Virtual Network Manager
- C. Azure Network Function Manager
- D. Azure Front Door

Answer: A

NEW QUESTION 173

- (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 178

- (Exam Topic 4)

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

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

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic. NOTE: Each correct selection is worth one point.

Answer Area

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

Only User1 and User4

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

Only User1 and User3

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: GpOAe4@IDg

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

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

Task 9

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

- 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)

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

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

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

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

Solution: You recommend the use of pass-through authentication and seamless SSO with password hash synchronization.

Does the solution meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/choose-ad-authn>

NEW QUESTION 186

- (Exam Topic 4)

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

You need to identify a method to dynamically construct a resource ID that will designate the key vault containing the appropriate secret during each deployment.

The name of the key vault and the name of the secret will be provided as inline parameters.

What should you use to construct the resource ID?

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

Answer: C

Explanation:

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

NEW QUESTION 187

- (Exam Topic 4)

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

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

You have an Azure Subscription named Sub1.

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

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

You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to Sa1.

Solution: You create a new stored access policy. Does this meet the goal?

- A. Yes

B. No

Answer: B

Explanation:

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

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

NEW QUESTION 192

- (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 194

- (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 195

- (Exam Topic 4)

You have an Azure subscription that contains an Azure Sentinel workspace.

Azure Sentinel is configured to ingest logs from several Azure workloads. A third-party service management platform is used to manage incidents.

You need to identify which Azure Sentinel components to configure to meet the following requirements:

- > When Azure Sentinel identifies a threat, an incident must be created.
 - > A ticket must be logged in the service management platform when an incident is created in Azure Sentinel.
- Which component should you identify for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

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

| | |
|-----------------|---|
| | ▼ |
| Analytics | |
| Data connectors | |
| Playbooks | |
| Workbooks | |

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

| | |
|-----------------|---|
| | ▼ |
| Analytics | |
| Data connectors | |
| Playbooks | |
| Workbooks | |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Reference:

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

NEW QUESTION 199

- (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 an initiative and an assignment that is scoped to the Tenant Root Group management group.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

Reference:

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

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

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 204

- (Exam Topic 4)

You have an Azure Active Directory (Azure AD) tenant that contains a user named User1.

You need to ensure that User1 can create and manage administrative units. The solution must use the principle of least privilege.

Which role should you assign to User1?

- A. Privileged role administrator
- B. Helpdesk administrator
- C. Global administrator
- D. Security administrator

Answer: A

NEW QUESTION 209

- (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 213

- (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.

Values

Get-AzPolicyRemediation

Set-AzContext

Set-AzResourceGroup

Start-AzPolicyComplianceScan

Start-AzPolicyRemediation

Answer Area

```
$policyAssignmentId = "/subscriptions/f0710c27-9663-4c05-19f8-1b4be01e86a5/providers/Microsoft.Authorization/
```

Value -Subscription "Sub1"

Value -PolicyAssignmentId \$policyAssignmentId -Name "policy1" -ResourceDiscovery

- 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 214

- (Exam Topic 4)

Your company has an Azure subscription named Subscription1. Subscription1 is associated with the Azure Active Directory tenant that includes the users shown in the following table.

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

The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

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

NOTE: Each correct selection is worth one point.

User:

Tool:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Table Description automatically generated

Reference:

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

NEW QUESTION 217

- (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 5

You need to ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

To ensure that only devices connected to a 131-107.0.0/16 subnet can access data in the rg1lod28681041 Azure Storage account, you can follow these steps:

- > In the Azure portal, search for and select the storage account named rg1lod28681041.
- > In the left pane, select Firewalls and virtual networks.
- > In the Firewalls and virtual networks pane, select Selected networks.
- > In the Selected networks pane, select Add existing virtual network.
- > In the Add existing virtual network pane, select the virtual network that contains the 131-107.0.0/16 subnet.
- > Select Add.

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

NEW QUESTION 220

- (Exam Topic 4)

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

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

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

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

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

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

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

Answer Area

Statements

Yes

No

User1 can access App1 from an IP address of 154.12.18.10.

☐

☐

User2 can access App1 from an IP address of 193.77.10.15.

☐

☐

User2 can access App1 from an IP address of 154.12.18.34.

☐

☐

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements

Yes

No

User1 can access App1 from an IP address of 154.12.18.10.

☐

☒

User2 can access App1 from an IP address of 193.77.10.15.

☒

☐

User2 can access App1 from an IP address of 154.12.18.34.

☐

☒

NEW QUESTION 221

- (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 224

- (Exam Topic 4)

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

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

You have an Azure Subscription named Sub1. Sub1 contains an Azure virtual machine named VM1 that runs Windows Server 2016.

You need to encrypt VM1 disks by using Azure Disk Encryption.

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

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

References:

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

NEW QUESTION 229

- (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 233

- (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 237

- (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

Explanation:

Instead use a management group.

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

Reference:

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

NEW QUESTION 241

- (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 246

- (Exam Topic 4)

You have an Azure subscription that contains a user named User1. User1 is assigned the Reader role for the subscription.

You plan to create a custom role named Role1 and assign Role1 to User1.

You need to ensure that User1 can create and manage application security groups by using the Azure portal. Which two permissions should you add to Role1? To answer, select the appropriate permission in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

Add permissions

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

A. Mastered

B. Not Mastered

Answer: A

Explanation:

* 1. Microsoft Portal 2. Microsoft Network

<https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/azure-services-resource-providers>

NEW QUESTION 247

- (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.

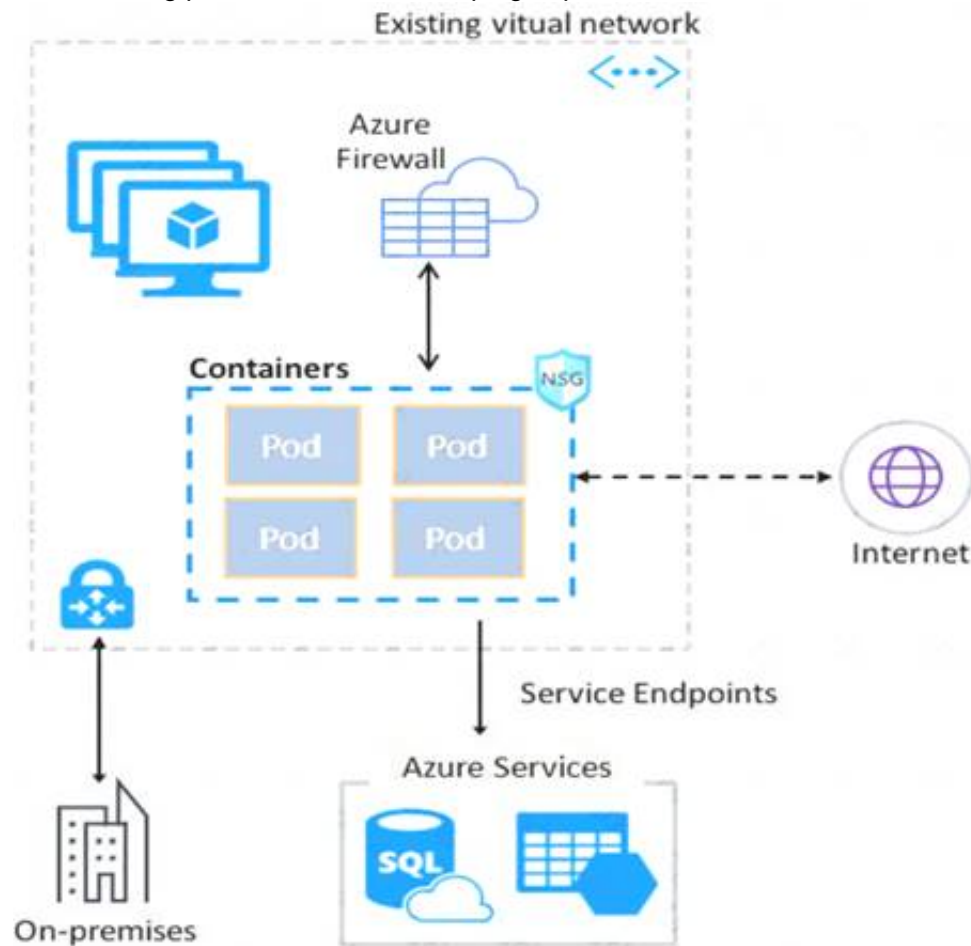
Answer: C

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 252

- (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 253

- (Exam Topic 4)

You have an Azure Kubernetes Service (AKS) cluster that will connect to an Azure Container Registry. You need to use automatically generated service principal for the AKS cluster to authenticate to the Azure Container Registry.

What should you create?

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

Answer: B

Explanation:

References:

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

NEW QUESTION 256

- (Exam Topic 4)

You have an Azure Sentinel workspace that contains an Azure Active Directory (Azure AD) connector, an Azure Log Analytics query named Query1 and a playbook named Playbook1.

Query1 returns a subset of security events generated by Azure AD.

You plan to create an Azure Sentinel analytic rule based on Query1 that will trigger Playbook1. You need to ensure that you can add Playbook1 to the new rule. What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Create the rule and set the type to:

| |
|--------------------------------------|
| Fusion |
| Microsoft Security incident creation |
| Scheduled |

Configure the playbook to include:

| |
|------------------------------------|
| A managed connector |
| A system-assigned managed identity |
| A trigger |
| Diagnostic settings |

- 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 258

- (Exam Topic 4)

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

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

Answer: B

Explanation:

References:

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

NEW QUESTION 263

- (Exam Topic 4)

You have an Azure subscription that contains the following resources:

- > A virtual network named VNET1 that contains two subnets named Subnet1 and Subnet2.
- > A virtual machine named VM1 that has only a private IP address and connects to Subnet1.

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

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

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 264

- (Exam Topic 4)

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

All Alerts

[+ New alert rule](#)
[Edit columns](#)
[Manage alert rules](#)
[View classic alerts](#)
[Refresh](#)
[Change state](#)

Don't see a subscription? [Open Directory](#) • [Subscription settings](#)

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

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

All Alerts Alerts By Smart Group (Preview)

| NAME | SEVERITY | MONITOR C... | ALERT STATE | AFFECT... | MONITOR SERV... | SIGNAL TYPE | FIRE 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 268
- (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 | Answer Area |
|--|--|
| <div>FIDO2 security key only</div> | |
| <div>Microsoft Authenticator app only</div> | |
| <div>Windows Hello for Business only</div> | |
| <div>Microsoft Authenticator app and Windows Hello for Business only</div> | User1: <div>Microsoft Authenticator app only</div> |
| <div>Windows Hello for Business and FIDO2 security key only</div> | User2: <div>Windows Hello for Business only</div> |
| <div>Microsoft Authenticator app, Windows Hello for Business, and FIDO2 security key</div> | |

NEW QUESTION 270

- (Exam Topic 4)

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

| Name | Type |
|---------|---------------|
| Item1 | Key |
| Item2 | Secret |
| Policy1 | Access policy |

In KeyVault1 the following events occur in sequence:

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

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

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

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 273

- (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 275

- (Exam Topic 4)

You have an Azure subscription that contains the following resources:

- An Azure key vault
- An Azure SQL database named Database1
- Two Azure App Service web apps named AppSrv1 and AppSrv2 that are configured to use system-assigned managed identities and access Database1

You need to implement an encryption solution for Database1 that meets the following requirements:

- The data in a column named Discount in Database1 must be encrypted so that only AppSrv1 can decrypt the data.
- AppSrv1 and AppSrv2 must be authorized by using managed identities to obtain cryptographic keys. How should you configure the encryption settings for Database1 To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point

To configure the encryption of Database1:

Always Encrypted by using Azure Key Vault.

Always Encrypted by using the Windows Certificate Store.

Transparent Data Encryption (TDE) by using Azure Key Vault integration.

Transparent Data Encryption (TDE) by using Bring Your Own Key (BYOK).

To obtain the cryptographic keys:

Create an access policy in Azure Key Vault.

Generate a key on an HSM device.

Import App Service certificates to AppSrv1 and AppSrv2.

Register an enterprise application in Azure AD.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated with medium confidence

Reference:

<https://docs.microsoft.com/en-us/azure/azure-sql/database/always-encrypted-azure-key-vault-configure?tabs=az>

NEW QUESTION 276

- (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.

Dynamic membership rules



Save Discard Got feedback?

Configure Rules Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

| And/Or | Property | Operator | Value | |
|--------|----------------|----------|-------|--|
| | accountEnabled | Equals | true | |
| Or | usageLocation | Equals | US | |

+ Add expression + Get custom extension properties

Rule syntax

Edit

```
(user.accountEnabled -eq true) or (user.usageLocation - eq "US")
```

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

Statements

Yes

No

User1 is a member of Group1 and Group2.

☐
☐

User2 is a member of Group2 only.

☐
☐

Managed1 is a member of Group1 and Group2.

☐
☐

- 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 278

- (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 280

- (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:

IPv4 ADDRESS OR CIDR

...

Exception:

Allow trusted Microsoft services to bypass this firewall?
☒ Yes
 ☐ No

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 282

- (Exam Topic 4)

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

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

You have an Azure subscription named Sub1.

You have an Azure Storage account named sa1 in a resource group named RG1.

Users and applications access the blob service and the file service in sa1 by using several shared access signatures (SASs) and stored access policies.

You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to sa1.

Solution: You regenerate the Azure storage account access keys. Does this meet the goal?

A. Yes

B. No

Answer: A

Explanation:

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

NEW QUESTION 287

- (Exam Topic 4)

You have a Microsoft 365 tenant that uses an Azure Active Directory (Azure AD) tenant. The Azure AD tenant syncs to an on-premises Active Directory domain by using an instance of Azure AD Connect.

You create a new Azure subscription.

You discover that the synced on-premises user accounts cannot be assigned roles in the new subscription. You need to ensure that you can assign Azure and Microsoft 365 roles to the synced Azure AD user accounts. What should you do first?

A. Change the Azure AD tenant used by the new subscription.

B. Configure the Azure AD tenant used by the new subscription to use pass-through authentication.

C. Configure the Azure AD tenant used by the new subscription to use federated authentication.

D. Configure a second instance of Azure AD Connect.

Answer: A

NEW QUESTION 292

- (Exam Topic 4)

You have a Microsoft Sentinel deployment.

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

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

Answer Area

Deploy:

Forward events to Microsoft Sentinel by using:

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area

Deploy:

Forward events to Microsoft Sentinel by using:

NEW QUESTION 295

- (Exam Topic 4)

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

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

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

A. VM1, VNET1, and storage1 only

B. VM1, storage1, and Vault1 only

C. VM1, VNET1, storage1, and Vault1

D. VM1 and storage1 only

E. VM1 and VNET only

Answer: C

NEW QUESTION 296

- (Exam Topic 4)

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

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

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

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

You plan to enable Azure Disk Encryption on VM1.

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

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

Answer: A

Explanation:

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

Reference:

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

NEW QUESTION 300

- (Exam Topic 4)

HOTSPOT

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

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

The company is sold to a new owner.

The company needs to transfer ownership of Subscription1.

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

NOTE: Each correct selection is worth one point.

User:

▼

User1
 User2
 User3
 User4

Tool:

▼

Azure Account Center
 Azure Cloud Shell
 Azure PowerShell
 Azure Security Center

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1; User2

Billing Administrator

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

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

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

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

NEW QUESTION 301

- (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 306

- (Exam Topic 4)

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

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

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

Create an access review

Access reviews enable reviewers to attest to users access.

Review name Review1

Description

Start date 2019-03-01

Frequency One time

End date 2019-03-20

Users

Scope Everyone

Review role membership Password administrator

Reviewers Members(self)

Sign completion settings

Sign completion settings: (empty)

Sign completion settings: (empty)

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

NOTE: Each correct selection is worth one point.

User3 can perform Review1 for

▼

User3 only

User1 and User2 only

User1, User2, and User3

If User2 fails to complete Review1 by March 20, 2019

▼

The Password administrator role will be revoked from User2

User2 will retain the Password administrator role

User3 will receive a confirmation request

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Box 1: User3 only

Use the Members (self) option to have the users review their own role assignments. Box 2: User3 will receive a confirmation request

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

No change - Leave user's access unchanged Remove access - Remove user's access Approve access - Approve user's access

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

References:

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

NEW QUESTION 307

- (Exam Topic 4)

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

| Name | Location | Performance | Premium account type |
|----------|-----------|-------------|-----------------------|
| storage1 | East US | Standard | <i>Not applicable</i> |
| storage2 | East US | Premium | Block blobs |
| storage3 | East US | Premium | File shares |
| storage4 | East US 2 | Standard | <i>Not applicable</i> |

You plan to enable auditing for DB1.

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

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

Answer: C

NEW QUESTION 309

- (Exam Topic 4)

You have an Azure subscription that contains a web app named Appl. App1 provides users with product images and videos. Users access App1 by using a URL of HTTPS://appl.contoso.com. You deploy two server pools named Pool1 and Pool2. Pool1 hosts product images. Pool2 hosts product videos. You need to optimize

The performance of Appl. The solution must meet the following requirements:

- Minimize the performance impact of TLS connections on Pool1 and Pool2.
- Route user requests to the server pools based on the requested URL path. What should you include in the solution?

- A. Azure Traffic Manager
B. Azure Bastion
C. Azure Application Gateway
D. Azure Front Door

Answer: C

NEW QUESTION 312

- (Exam Topic 4)

Lab Task

Task 4

You need to ensure that when administrators deploy resources by using an Azure Resource Manager template, the deployment can access secrets in an Azure key vault named KV31330471.

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Grant permission to the application that is used to deploy the resources to access the secrets in the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to assign the Key Vault Secrets User role to the application at the scope of the key vault or individual secrets. Enable template deployment for the key vault. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to set the `enabledForTemplateDeployment` property of the key vault to `true`. Reference the secrets in the template by using their resource ID. You can use the `listSecrets` function to get the resource ID of a secret in the key vault. You need to specify the name of the key vault and the name of the secret as parameters. Deploy the template by using Azure PowerShell, Azure CLI, or REST API. You can use the `New-AzResourceGroupDeployment` cmdlet, the `az deployment group create` command, or the Deployments - Create Or Update REST API to do this. You need to provide the template file or URI and any required parameters.

NEW QUESTION 316

- (Exam Topic 4)

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

You are planning the monitoring of Azure services in the subscription. You need to retrieve the following details:

- > Identify the user who deleted a virtual machine three weeks ago.
- > Query the security events of a virtual machine that runs Windows Server 2016.

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

NOTE: Each correct selection is worth one point.

| Settings | Answer Area |
|----------------|--|
| Activity log | |
| Logs | Identify the user who deleted a virtual machine three weeks ago: <input type="text"/> |
| Metrics | Query the security events of a virtual machine that runs Windows Server 2016: <input type="text"/> |
| Service Health | |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box1: Activity log

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

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

Box 2: Logs

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

References:

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

NEW QUESTION 319

- (Exam Topic 4)

Your company recently created an Azure subscription.

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

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

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

Answer: A

Explanation:

To start using PIM in your directory, you must first enable PIM.

* 1. Sign in to the Azure portal as a Global Administrator of your directory.

You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.

Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com

Reference:

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

NEW QUESTION 320

- (Exam Topic 4)

You have an Azure subscription.

You create a new virtual network named VNet1.

You plan to deploy an Azure web app named App1 that will use VNet1 and will be reachable by using private IP addresses. The solution must support inbound and

outbound network traffic.
What should you do?

- A. Create an Azure App Service Hybrid Connection.
- B. Configure regional virtual network integration.
- C. Create an App Service Environment
- D. Create an Azure application gateway.

Answer: D

NEW QUESTION 321

- (Exam Topic 4)

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

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

You have an Azure subscription named Sub1.

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

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

You discover that unauthorized users accessed both the file service and the blob service. You need to revoke all access to Sa1.

Solution: You create a lock on Sa1. Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

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

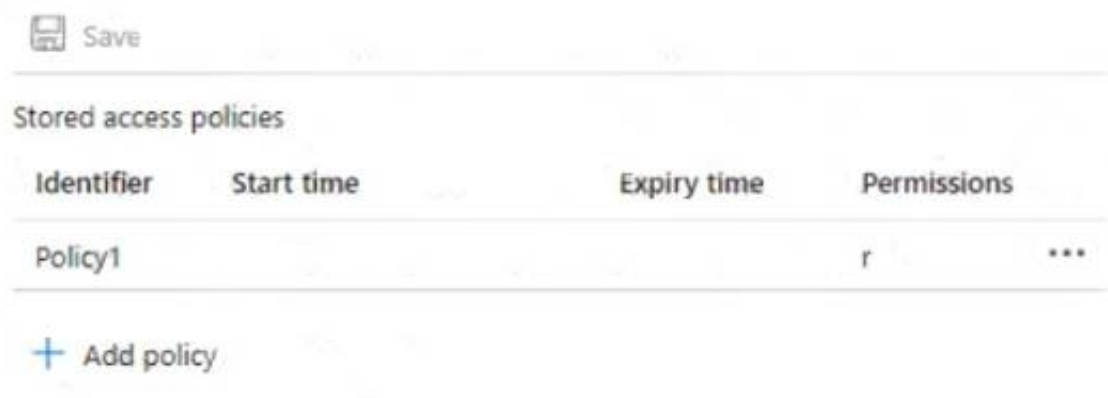
References:

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

NEW QUESTION 324

- (Exam Topic 4)

You have an Azure subscription that contains a blob container named cont1. Cont1 has the access policies shown in the following exhibit.



| Identifier | Start time | Expiry time | Permissions |
|------------|------------|-------------|-------------|
| Policy1 | | | r |

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

The maximum number of additional stored access policies that you can add to cont1 is [answer choice].

▼

1

2

4

7

15

The maximum number of additional immutable blob storage policies that you can add to cont1 is [answer choice].

▼

1

2

4

7

15

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

The maximum number of additional stored access policies that you can add to cont1 is [answer choice].

- 1
- 2
- 4
- 7
- 15

The maximum number of additional immutable blob storage policies that you can add to cont1 is [answer choice].

- 1
- 2
- 4
- 7
- 15

NEW QUESTION 328

- (Exam Topic 4)

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

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

Admin1 performs the following actions on RG1:

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

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

NOTE: Each correct selection is worth one point.

Adding VNET1:

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

Adding Lock1:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Adding VNET1:

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

Adding Lock1:

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

NEW QUESTION 332

- (Exam Topic 4)

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

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

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

* Create two application security groups named ASG1 and ASG2 in the West US region.

* Add the network interface of VM1 to ASG1.

Answer Area

ASG1:

ASG2:

- A. Mastered
B. Not Mastered

Answer: A

Explanation:

Answer Area

ASG1:

ASG2:

NEW QUESTION 335

- (Exam Topic 4)

You have an Azure Subscription that is linked to an Azure Active Directory (Azure AD). The tenant contains the users shown in the following table.

| Name | Role | Member of |
|-------|------------------------|----------------|
| User1 | Security administrator | Group1 |
| User2 | Network Contributor | Group2 |
| User3 | Key Vault Contributor | Group1, Group2 |

You have an Azure key vault named Vault1 that has Purge protection set to Disabled. Vault1 contains the access policies shown in the following table.

| Name | Key permission | Secret permission | Certificate permission |
|--------|----------------|-------------------|------------------------|
| Group1 | Purge | Purge | Purge |
| Group2 | Select all | Select all | Select all |

You create role assignments for Vault1 as shown in the following table.

| Name | Role |
|-------|---------------------------|
| User1 | None |
| User2 | Key Vault Reader |
| User3 | User Access Administrator |

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

NOTE: Each correct selection is worth one point.

Answer Area

| Statements | Yes | No |
|--|-----------------------|-----------------------|
| User1 can set Purge protection to Enable for Vault1. | <input type="radio"/> | <input type="radio"/> |
| User2 can configure firewalls and virtual networks for Vault1. | <input type="radio"/> | <input type="radio"/> |
| User3 can add access policies to Vault1. | <input type="radio"/> | <input type="radio"/> |

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

| Statements | Yes | No |
|--|----------------------------------|----------------------------------|
| User1 can set Purge protection to Enable for Vault1. | <input checked="" type="radio"/> | <input type="radio"/> |
| User2 can configure firewalls and virtual networks for Vault1. | <input type="radio"/> | <input checked="" type="radio"/> |
| User3 can add access policies to Vault1. | <input type="radio"/> | <input checked="" type="radio"/> |

NEW QUESTION 336

- (Exam Topic 4)
Lab Task
Task 2

You need to ensure that the events in the NetworkSecurityGroupRuleCounter log of the VNET01-Subnet0-NSG network security group (NSG) are stored in the logs31330471 Azure Storage account for 30 days.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Enable diagnostic resource logging for the NSG. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to select the Rule counter category under Logs and choose the logs31330471 storage account as the destination. Configure the retention policy for the storage account to keep the logs for 30 days. You can use the Azure portal, Azure PowerShell, or the Azure CLI to do this. You need to specify the days parameter as 30 for the Set-AzStorageServiceProperty cmdlet or the az storage logging update command. View and analyze the logs in the storage account. You can use any tool that can read JSON files, such as Azure Storage Explorer or Visual Studio Code. You can also export the logs to any visualization tool, SIEM solution, or IDS of your choice

NEW QUESTION 339

- (Exam Topic 3)

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

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

Answer: D

Explanation:

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

NEW QUESTION 341

- (Exam Topic 3)

You need to encrypt storage1 to meet the technical requirements. Which key vaults can you use?

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

Answer: B

Explanation:

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

NEW QUESTION 346

- (Exam Topic 2)
You need to ensure that User2 can implement PIM. What should you do first?

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

Answer: D

Explanation:

To start using PIM in your directory, you must first enable PIM.
* 1. Sign in to the Azure portal as a Global Administrator of your directory.
You must be a Global Administrator with an organizational account (for example, @yourdomain.com), not a Microsoft account (for example, @outlook.com), to enable PIM for a directory.
Scenario: Technical requirements include: Enable Azure AD Privileged Identity Management (PIM) for contoso.com
References:
<https://docs.microsoft.com/bs-latn-ba/azure/active-directory/privileged-identity-management/pim-getting-started>

NEW QUESTION 349

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

Answer Area

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

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

NEW QUESTION 350

- (Exam Topic 2)
You need to meet the technical requirements for VNetwork1. What should you do first?

- A. Create a new subnet on VNetwork1.

- B. Remove the NSGs from Subnet11 and Subnet13.
- C. Associate an NSG to Subnet12.
- D. Configure DDoS protection for VNetwork1.

Answer: A

Explanation:

From scenario: Deploy Azure Firewall to VNetwork1 in Sub2.

Azure firewall needs a dedicated subnet named AzureFirewallSubnet. References:

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

NEW QUESTION 352

- (Exam Topic 2)

What is the membership of Group1 and Group2? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Group1:

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

Group2:

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

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: User1, User2, User3, User4

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

Box 2: User1, User2, User3, User4 References:

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

NEW QUESTION 356

.....

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