

 **CERT** *Ya!*

Microsoft

AZ-500

Microsoft Azure Security Technologies

QUESTION & ANSWERS

QUESTION 1

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

What should you do?

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

Correct Answer: D

Explanation/Reference:

Explanation:

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

Scenario:

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

The tenant currently contain this group:

Name	Type	Description
Group1	Security group	A group that has the Dynamic User membership type, contains all the San Francisco users, and provides access to many Azure AD applications and Azure resources.

References:

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

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

QUESTION 2

HOTSPOT

You have an Azure Container Registry named Registry1.

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

User	Role
User1	AcrPush
User2	AcrPull
User3	AcrImageSigner
User4	Contributor

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

NOTE: Each correct selection is worth one point.

Upload images:

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

Download images:

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

Correct Answer:

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	

Explanation/Reference:

Explanation:

Box 1: User1 and User4 only

Owner, Contributor and AcrPush can push images.

Box 2: User1, User2, and User4

All, except AcrImagineSigner, 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>

QUESTION 3

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

You plan to assign policies that use the DeployIfNotExist, AuditIfNotExist, Append, and Deny effects. Which effect requires a managed identity for the assignment?

A. AuditIfNotExist

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

Correct Answer: C

Explanation/Reference:

Explanation:

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

References:

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

QUESTION 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

Correct Answer: A

QUESTION 5

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

Correct Answer: B

Explanation/Reference:

Explanation:

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

Reference:

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

QUESTION 6

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.

Correct Answer: C

Explanation/Reference:

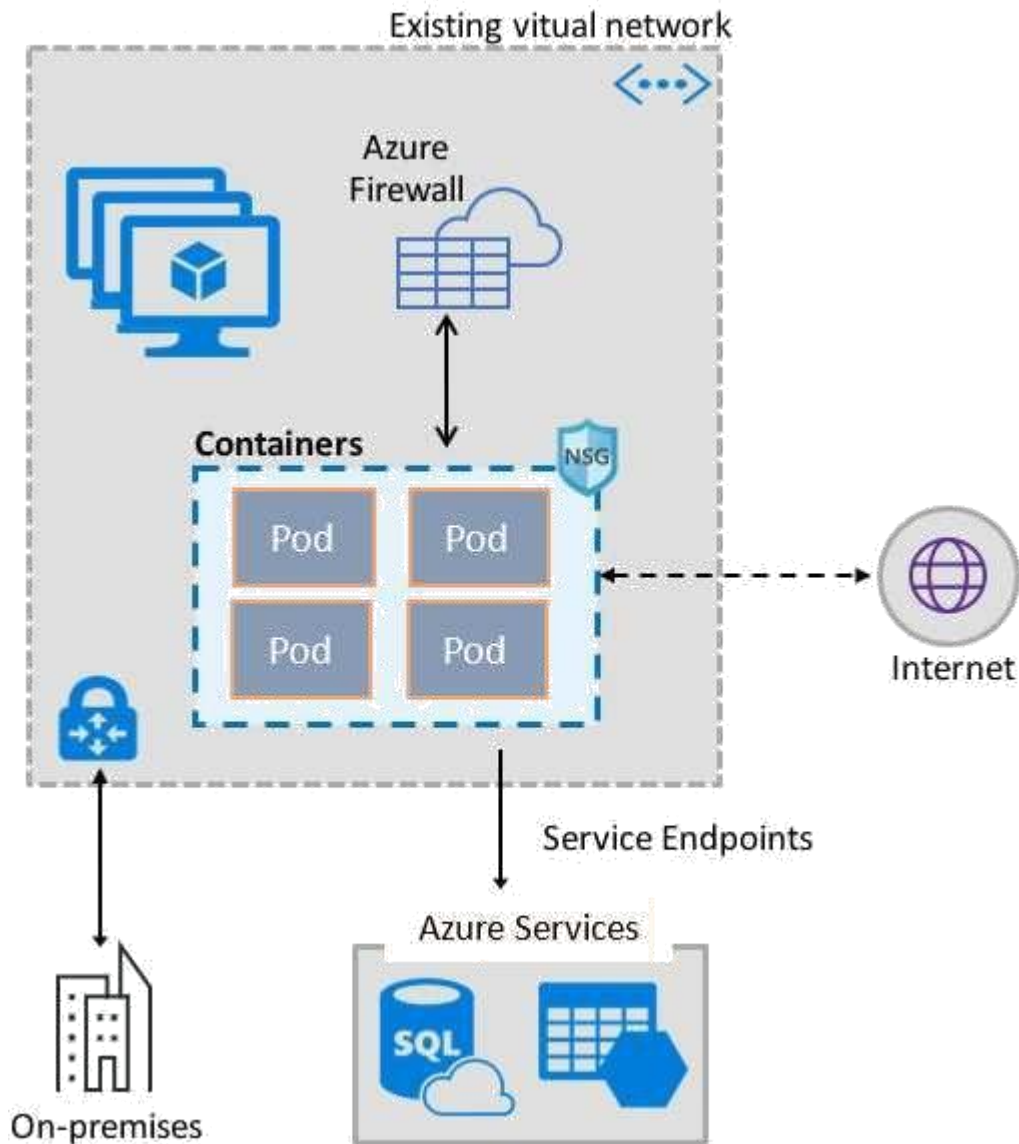
Explanation:

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>

QUESTION 7

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.

Correct Answer: A

Explanation/Reference:

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>

QUESTION 8

Question: 50

You have an Azure subscription named Sub1 that contains an Azure Log Analytics workspace named LAW1.

You have 100 on-premises servers that run Windows Server 2012 R2 and Windows Server 2016. The servers connect to LAW1. LAW1 is configured to collect security-related performance counters from the connected servers.

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

requirements:

- Alert rules must support dimensions.
- The time it takes to generate an alert must be minimized.
- Alert notifications must be generated only once when the alert is generated and once when the alert is
- resolved.

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

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

Correct Answer: C

Explanation/Reference:

Explanation:

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

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

References:

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

QUESTION 9

SIMULATION

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: User1-10598168@ExamUsers.com

Azure Password: Ag1Bh9!#Bd

The following information is for technical support purposes only:

Lab Instance: 10598168

Microsoft Azure




Sign in

to continue to Microsoft Azure

[No account? Create one!](#)

[Can't access your account?](#)

[Next](#)

 [Sign in with GitHub](#)

Azure services

- [Create a resource](#)
- [Virtual machines](#)
- [App Services](#)
- [Storage accounts](#)
- [SQL databases](#)
- [Azure Database for PostgreSQL](#)
- [Azure Cosmos DB](#)
- [Kubernetes services](#)
- [Function App](#)
- [More services](#)

Navigate

- [Subscriptions](#)
- [Resource groups](#)
- [All resources](#)
- [Dashboard](#)

Tools

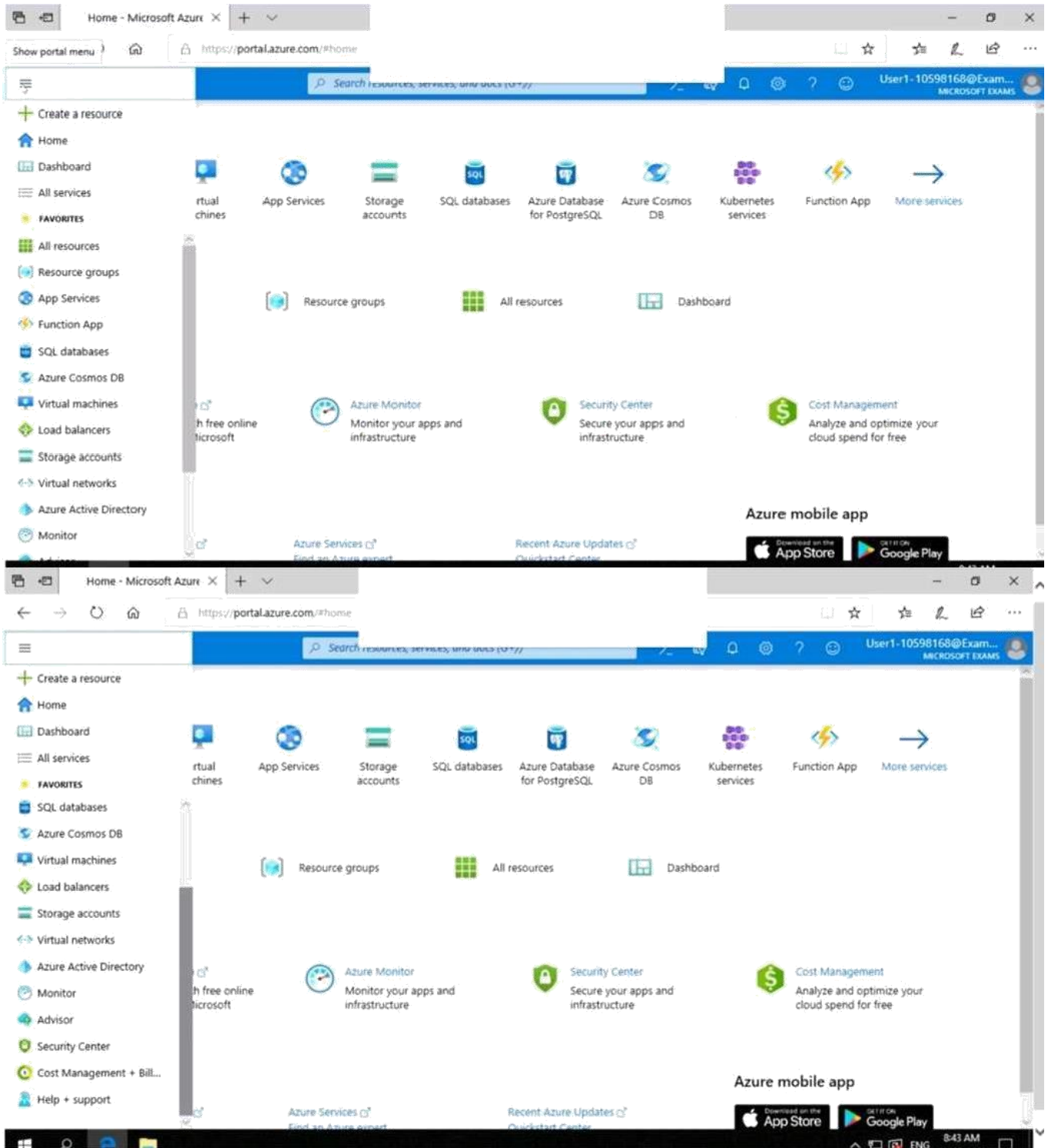
- [Microsoft Learn](#)
Learn Azure with free online training from Microsoft
- [Azure Monitor](#)
Monitor your apps and infrastructure
- [Security Center](#)
Secure your apps and infrastructure
- [Cost Management](#)
Analyze and optimize your cloud spend for free

Useful links

- [Technical Documentation](#)
- [Azure Services](#)
- [Recent Azure Updates](#)

Azure mobile app

Download on the [App Store](#) | [GET IT ON Google Play](#)



You need to create a new Azure Active Directory (Azure AD) directory named 10598168.onmicrosoft.com. The new directory must contain a user named user1@10598168.onmicrosoft.com who is configured to sign in by using Azure Multi-Factor Authentication (MFA).

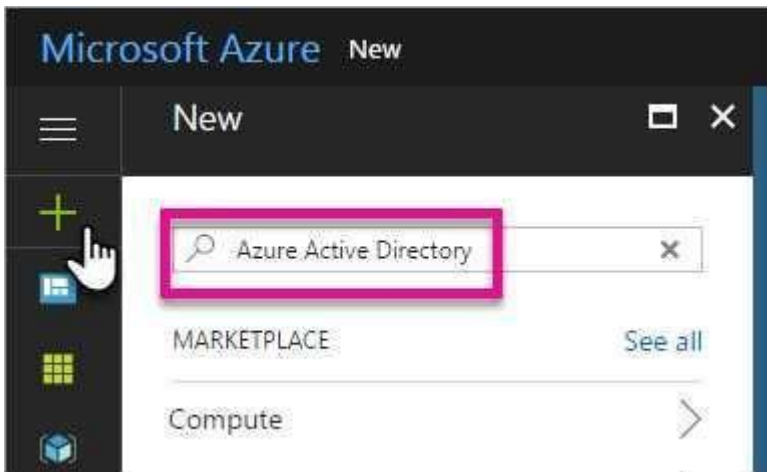
To complete this task, sign in to the Azure portal.

Correct Answer: see explanation below

Explanation/Reference:

Step 1: Create an Azure Active Directory tenant

1. Browse to the Azure portal and sign in with an account that has an Azure subscription.
2. Select the plus icon (+) and search for Azure Active Directory.

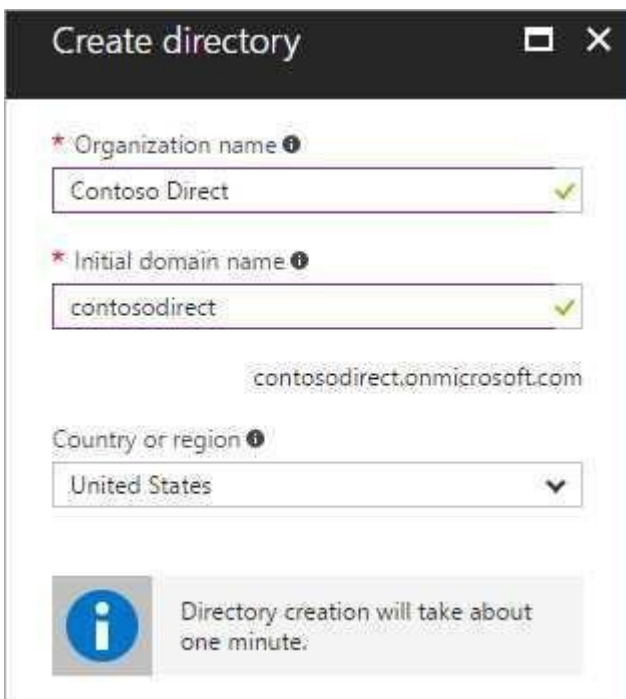


3. Select Azure Active Directory in the search results.



4. Select Create.

5. Provide an Organization name and an Initial domain name (10598168). Then select Create. Your directory

A screenshot of the 'Create directory' form in the Azure portal. The form has three main input fields: 'Organization name' with the value 'Contoso Direct', 'Initial domain name' with the value 'contosodirect', and 'Country or region' with a dropdown menu set to 'United States'. Below these fields, the domain 'contosodirect.onmicrosoft.com' is displayed. At the bottom of the form, there is a blue information icon and a message that says 'Directory creation will take about one minute.'

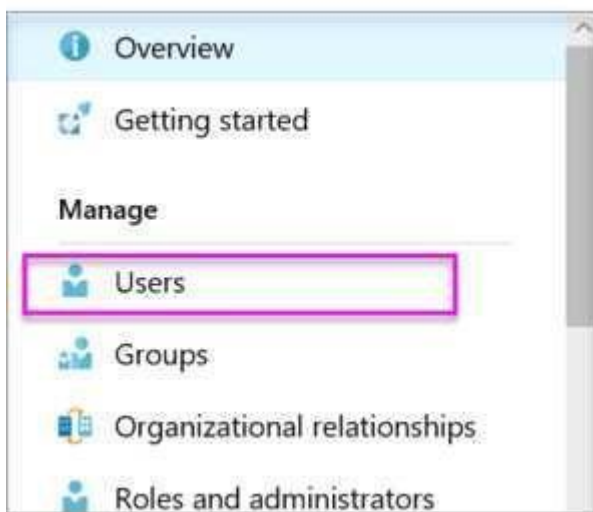
6. After directory creation is complete, select the information box to manage your new directory.
Next, you're going to add tenant users.

Step 2: Create an Azure Active Directory tenant user

7. In the Azure portal, make sure you are on the Azure Active Directory fly out.



8. Under Manage, select Users.



9. Select All users and then select + New user.

10. Provide a Name and User name (user1) for the regular user tenant You can also show the temporary password. When you're done, select Create.

Name: user1

User name: user1@10598168.onmicrosoft.com

User
contoso direct

* Name ⓘ
PBI Embed ✓ 1

* User name ⓘ
pbiembed@contosodirect.onmicrosoft.com ✓ 2

Profile ⓘ
Not configured >

Properties ⓘ
Default >

Groups ⓘ
0 groups selected >

Directory role ⓘ
User 3

Password
[Masked] [Show Password]

Reference:

<https://docs.microsoft.com/en-us/power-bi/developer/create-an-azure-active-directory-tenant>

QUESTION 10

SIMULATION

You need to deploy an Azure firewall to a virtual network named VNET3.

To complete this task, sign in to the Azure portal and modify the Azure resources.

This task might take several minutes to complete. You can perform other tasks while the task completes.

Correct Answer: see explanation below

Explanation/Reference:

To add an Azure firewall to a VNET, the VNET must first be configured with a subnet named AzureFirewallSubnet (if it doesn't already exist).

Configure VNET3.

- In the Azure portal, type Virtual Networks in the search box, select Virtual Networks from the

search results then select VNET3. Alternatively, browse to Virtual Networks in the left navigation pane.

- In the Overview section, note the Location (region) and Resource Group of the virtual network. We'll need these when we add the firewall.

- Click on Subnets.
- Click on + Subnet to add a new subnet.
- Enter AzureFirewallSubnet in the Name box. The subnet must be named AzureFirewallSubnet.
- Enter an appropriate IP range for the subnet in the Address range box.
- Click the OK button to create the subnet.

- In the settings of VNET3 click on Firewall.
- Click the Click here to add a new firewall link.
- The Resource group will default to the VNET3 resource group. Leave this default.
- Enter a name for the firewall in the Name box.
- In the Region box, select the same region as VNET3.
- In the Public IP address box, select an available public IP address if one exists, or click Add new to add a new public IP address.
- Click the Review + create button.
- Review the settings and click the Create button to create the firewall.

Reference:

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

QUESTION 11

HOTSPOT

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

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

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

NOTE: Each correct selection is worth one point


```

{
  "if" : {
    "allOf" : [
      {
        "field" : "type",
        "equals" : "Microsoft.Compute/virtualMachines"
      }
      {
        "field" : "Microsoft.Compute/imageSKU",
        "equals" : "2016-Datacenter",
      }
    ]
  },
  "then" : {
    "effect" : " ",
  },
  "details" : {
    "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
    "roleDefinitionsIds" : [
      "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
    ],
    "name" : "customExtension",
    "deployment" : {
      "properties" : {
        "mode" : "incremental",
        "parameters" : {
          " ",
        }
      }
    }
  }
}
}
)

```

	▼
Append	
Deny	
DeployIfNotExists	

	▼
existenceCondition	
resources	
template	

Correct Answer:

```
},
  "then" : {
    "effect" : "DeployIfNotExists",
    "details" : {
      "type" : "Microsoft.GuestConfiguration/guestConfigurationAssignments",
      "roleDefinitionsIds" : [
        "/providers/microsoft.authorization/roleDefinitions/12345678-1234-5678-abcd-012345678910"
      ],
      "name" : "customExtension",
      "deployment" : {
        "properties" : {
          "mode": "incremental",
          "parameters" : {
            "existenceCondition": {
              "resources": {
                "template": {

```

Explanation/Reference:

Explanation:

Box 1: DeployIfNotExists

DeployIfNotExists executes a template deployment when the condition is met.

Box 2: Template

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

Deployment [required]

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

References:

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

QUESTION 12

HOTSPOT

You plan to use Azure Sentinel to create an analytic rule that will detect suspicious Threats and automate responses. Which components are required for the rule? To answer, select the appropriate options in the answer area.

NOTE Each correct selection is worth one point.

Answer Area

Detect suspicious threats: A Kusto query language query A Transact-SQL query An Azure PowerShell script An Azure Sentinel playbook

Automate responses: An Azure Functions app

Correct Answer:



QUESTION 13

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.

Correct Answer: B

QUESTION 14

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

Correct Answer: B

Explanation/Reference:

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-withmanagementgroups/>

QUESTION 15

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

Name	Operating system	Region	Resource group
VM1	Windows Server 2012	East US	RG1
VM2	Windows Server 2012 R2	West Europe	RG1
VM3	Windows Server 2016	West Europe	RG2
VM4	Red Hat Enterprise Linux 7.4	East US	RG2

You create an Azure Log Analytics workspace named Analytics1 in RG1 in the East US region.

Which virtual machines can be enrolled in Analytics1?

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

Correct Answer: C

Explanation/Reference:

Explanation:

Note: Create a workspace

In the Azure portal, click All services. In the list of resources, type Log Analytics. As you begin typing, the list filters based on your input. Select Log Analytics.

Click Create, and then select choices for the following items:

Provide a name for the new Log Analytics workspace, such as DefaultLAWorkspace. OMS workspaces are now referred to as Log Analytics workspaces.

Select a Subscription to link to by selecting from the drop-down list if the default selected is not appropriate.

For Resource Group, select an existing resource group that contains one or more Azure virtual machines.

Select the Location your VMs are deployed to. For additional information, see which regions Log Analytics is available in.

Incorrect Answers:

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

D: VM4 is a different resource group. References:

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

QUESTION 16

HOTSPOT

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

Name	Type	Region
RG1	Resource group	West Europe
VNET1	Azure virtual network	West Europe
Contoso1901	Azure Storage account	West Europe

VNET1 contains two subnets named Subnet1 and Subnet2. Subnet1 has a network ID of 10.0.0.0/24. Subnet2 has a network ID of 10.1.1.0/24.

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

```
PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet
ByPass          : Logging, Metrics
DefaultAction   : Deny
IpRules         : [193.77.0.0/16,...]
VirtualNetworkRules : [/subscriptions/a90c8c8f-d8bc-4112-abfb-
                        dac4906573dd/resourceGroups/RG1/providers/Microsoft.Network/
                        virtualNetworks/VNET1/subnets/Subnet1,...]

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRuleSet.
                                                    IpRules
Action IPAddressOrRange
-----
Allow  193.77.0.0/16

PS C:\> (Get-AzStorageAccount -ResourceGroupName RG1 -Name contoso1901).NetworkRules
Action VirtualNetworkResourceId                               State
-----
Allow  /subscriptions/a90c8c8f-d8bc-4112-abfb dac4906573dd/resourceGroups/
      RG1/providers/Microsoft.Network/virtualNetworks/VNET1/subnets/Subnet1 Succeeded

PS C:\> _
```

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

NOTE: Each correct selection is worth one point.

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
An Azure virtual machine on Subnet2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	<input type="radio"/>	<input type="radio"/>

Correct Answer:

Statements	Yes	No
An Azure virtual machine on Subnet1 can access data in Contoso1901.	<input checked="" type="radio"/>	<input type="radio"/>
An Azure virtual machine on Subnet2 can access data in Contoso1901.	<input type="radio"/>	<input checked="" type="radio"/>
A computer on the Internet that has an IP address of 193.77.10.2 can access data in Contoso1901.	<input checked="" type="radio"/>	<input type="radio"/>

Explanation/Reference:

Explanation:

Box 1: Yes

Access from Subnet1 is allowed.

Box 2: No

No access from Subnet2 is allowed.

Box 3: Yes

Access from IP address 193.77.10.2 is allowed

QUESTION 17

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



Consent to PIM.

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

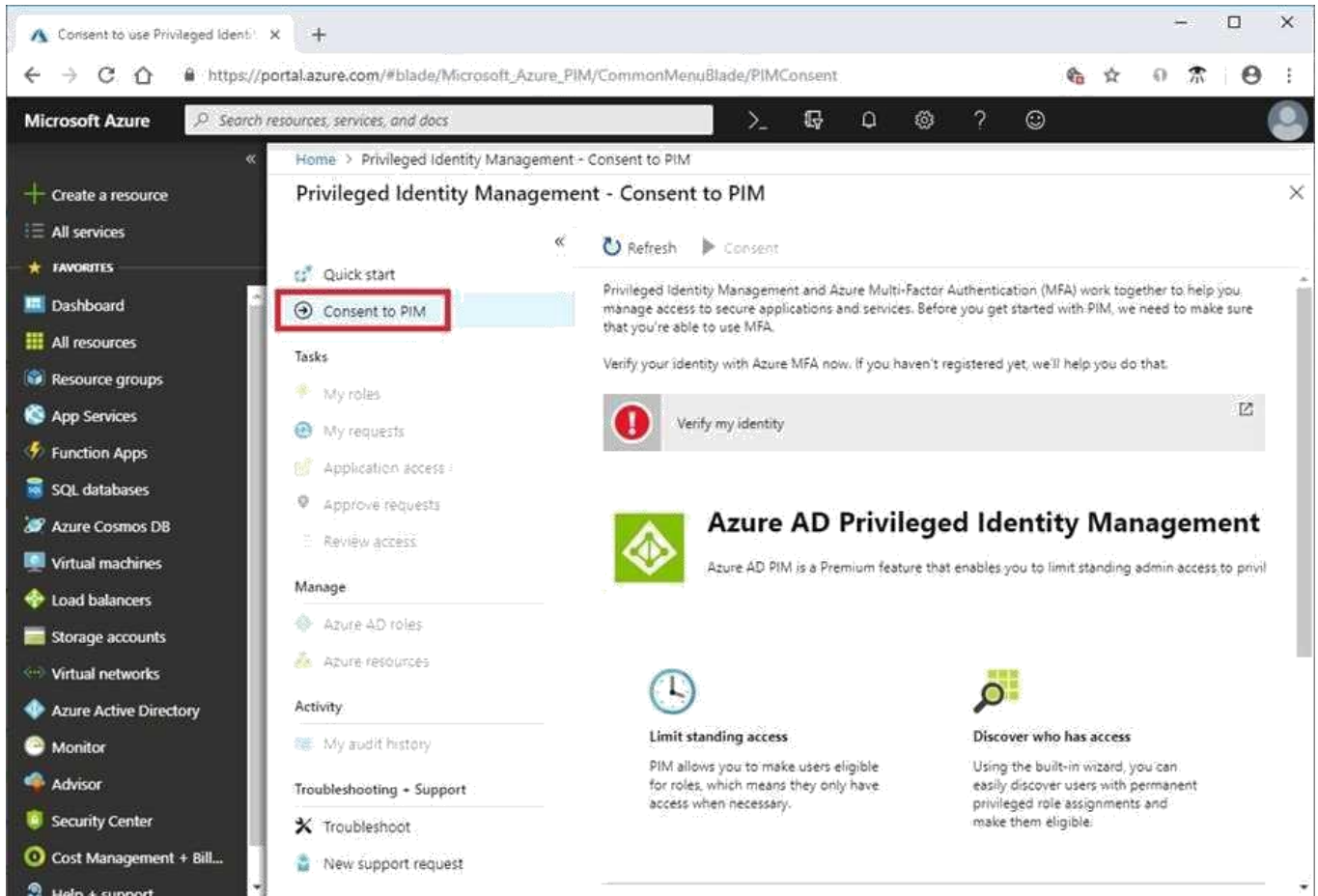
Sign up PIM for Azure AD roles.

Correct Answer:

Explanation/Reference:

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 MF

A. 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/pimgetting-started>

QUESTION 18

HOTSPOT

You have an Azure subscription named Subcription1 that contains the resources shown in the following table.

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

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

- An Azure Sentinel workspace
- An Azure Event Grid instance

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

NOTE: Each correct selection is worth one point.



Correct Answer:



QUESTION 19

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

Name	Resource group
VM1	RG1
VM2	RG2
VM3	RG1
VM4	RG2

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

What should you configure?

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

Correct Answer: D

Explanation/Reference:

Explanation:

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

Note: When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by

creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down.

These ports are controlled by the just-in-time solution.

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

Reference:

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

QUESTION 20

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

Correct Answer: C

Explanation/Reference:

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.

Connect to Server

SQL Server

Server type: Database Engine

Server name: tedus.database.windows.net

Authentication: Active Directory - Integrated

User name: DOMAIN\username

Password:

Remember password

Connect Cancel Help Options >>

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-aadauthentication-configure.md>