AZ-500 Q&As

Microsoft Azure Security Technologies

Pass Microsoft AZ-500 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/az-500.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

You have an Azure subscription that contains a resource group named RG1 and a security group serverless RG1 contains 10 virtual machine, a virtual network VNET1, and a network security group (NSG) named NSG1. ServerAdmins can

access the virtual machines by using RDP.

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

What should you configure?

A. an Azure Active Directory (Azure AD) Privileged identity Management (PIM) role assignment.

B. a just in time (JIT) VM access policy in Microsoft Defender for Cloud

C. an azure policy assigned to RG1.

D. an Azure Bastion host on VNET1.

Correct Answer: B

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

QUESTION 2

HOTSPOT

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": "3336fcbf-33d8-4c8a-85b6-d8edd964762b",
        "Scope": "/subscriptions/76c42af2-b40d-48fd-bf3b-de37baaa7ffa",
        "DisplayName": "User1",
        "SignInName": "User1@contoso.com",
        "RoleDefinitionName": "Owner",
        …
    },
    {
        "RoleAssignment": "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": "0d61eae6-4612-4ee2-88f3-fb6dab84eb10",
        "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.

Hot Area:

Answer Area

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

- Only User1
- Only User2
- Only User1 and User4
- Only User1, User2, and User4
- User1, User2, User3, and User4

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

- Only User3
- Only User1 and User3
- Only User3 and User4
- Only User1, User3, and User4
- User1, User2, User3, and User4

Correct Answer:

Answer Area

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

- Only User1
- **Only User2**
- Only User1 and User4
- Only User1, User2, and User4
- User1, User2, User3, and User4

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

- **Only User3**
- Only User1 and User3
- Only User3 and User4
- Only User1, User3, and User4
- User1, User2, User3, and User4

User1 - has ownership at subscription level therefore has access to the control plane of the key vault but not to the data plane. therefore User1 can manage RBAC permissions but cannot create/access keys or secrets (unless bthey can grant themself \\'Key Administrator\\' access and do this, which again does not show up in this RBACs listed so we cannot assume that)

-Therefore User1 has not access to the keys or secrets in this vault

User2 - Is a Key VAult Crypto officer for the KeyVault1. so according to this:https://learn.microsoft.com/en-us/azure/key-vault/general/rbac-guide?tabs=azure-cli#azure-built-in-roles-for-key-vault-data-plane-operations , they can manage keys

(but not access secrets or manage permissions)

User3 - Is a Secrets officer for the KeyVault1 scope. they can access secrets data in this key vault

User4 - Here\\'s a tricky one. while they are indeed given \\'Key Vault Administrator\\', notice the scope is set to "../KeyVault1/Keys/Key1". So they should only be able to work with that key.

QUESTION 3

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

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 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	None	Disabled
User2	Group1	Disabled
user3	Group1	Enforced

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

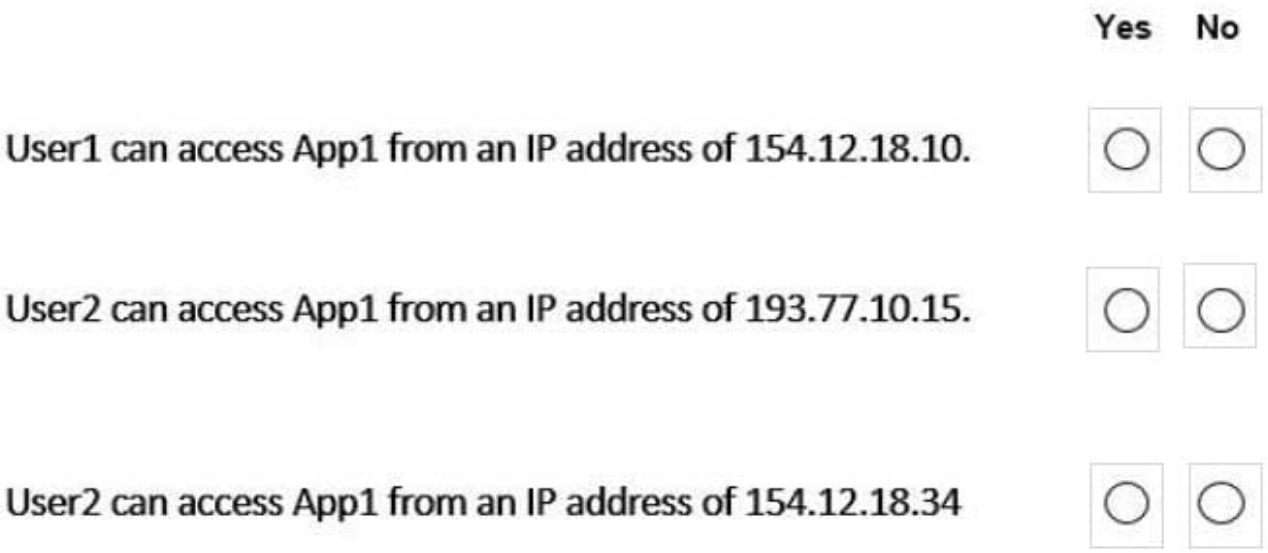
Name	Type	Trusted location
Seattle	193.77.10.0/24	YES
Boston	154.12.18.0/24	NO

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

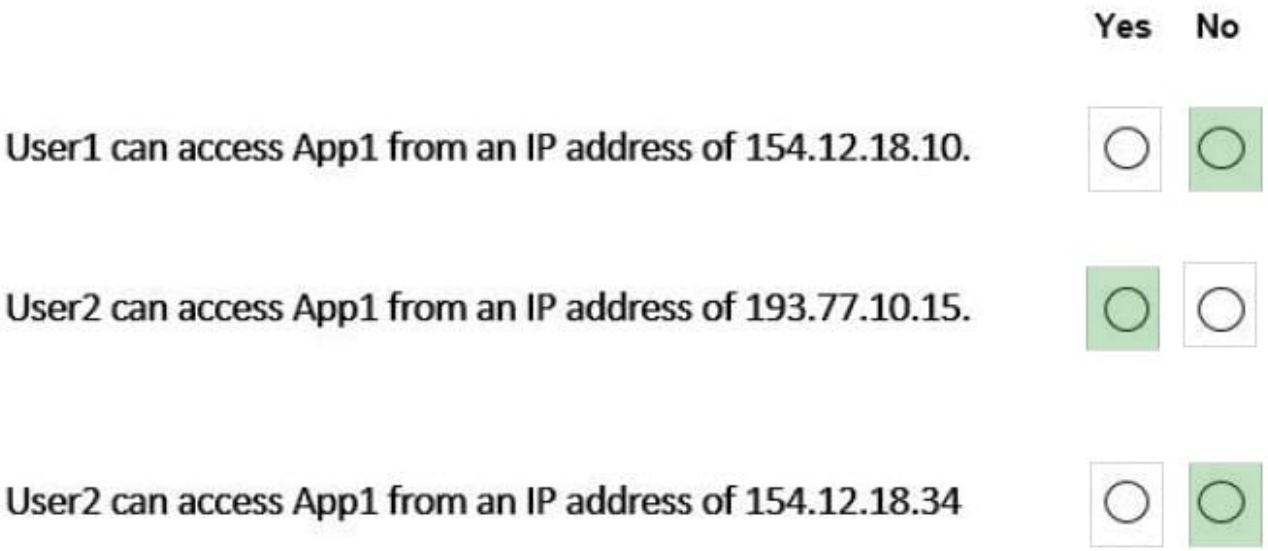
Name	Type	Exclude	Trusted location	Grant
Policy1	Group1	Group2	Locations: Boston	Block access
Policy2	Group1	None	Locations: Any location	Grant access, Require multi-factor authentication
Policy3	Group2	Group1	Locations: Boston	Block access
Policy4	Group2	None	Locations: Any location	Grant access, Require 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.

Hot Area:



Correct Answer:



QUESTION 5

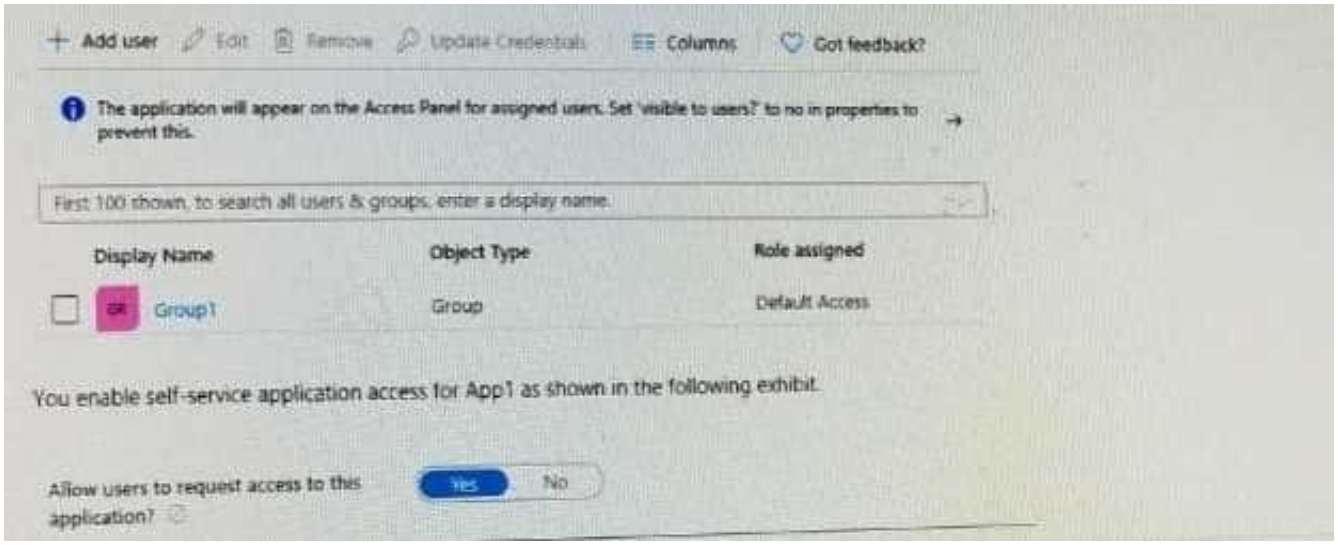
HOTSPOT

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

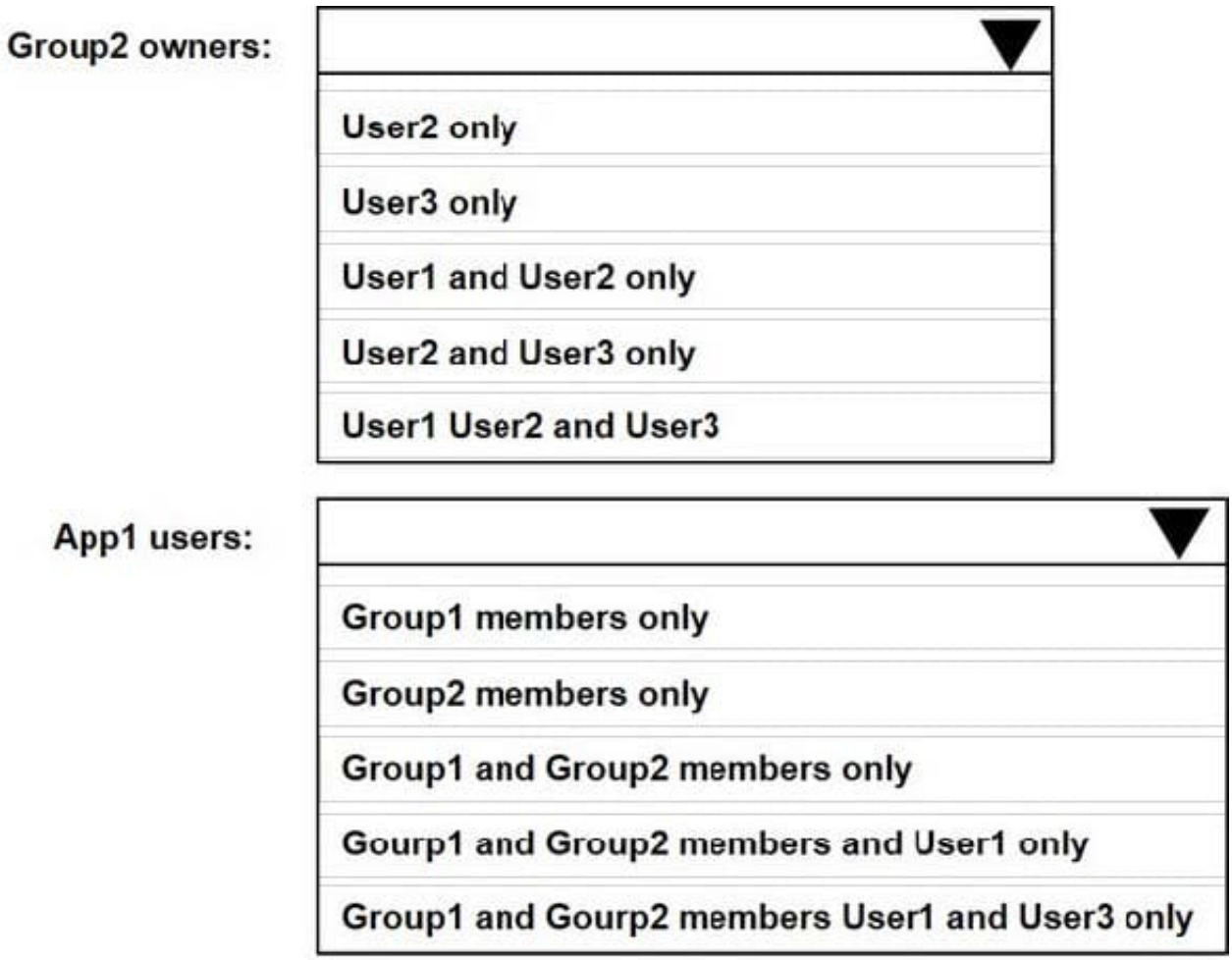
Name	Type
User1	User
User2	User
User3	User
Group1	Security group
Group2	Security group
App1	Enterprise application

User2 is the owner of Group2.

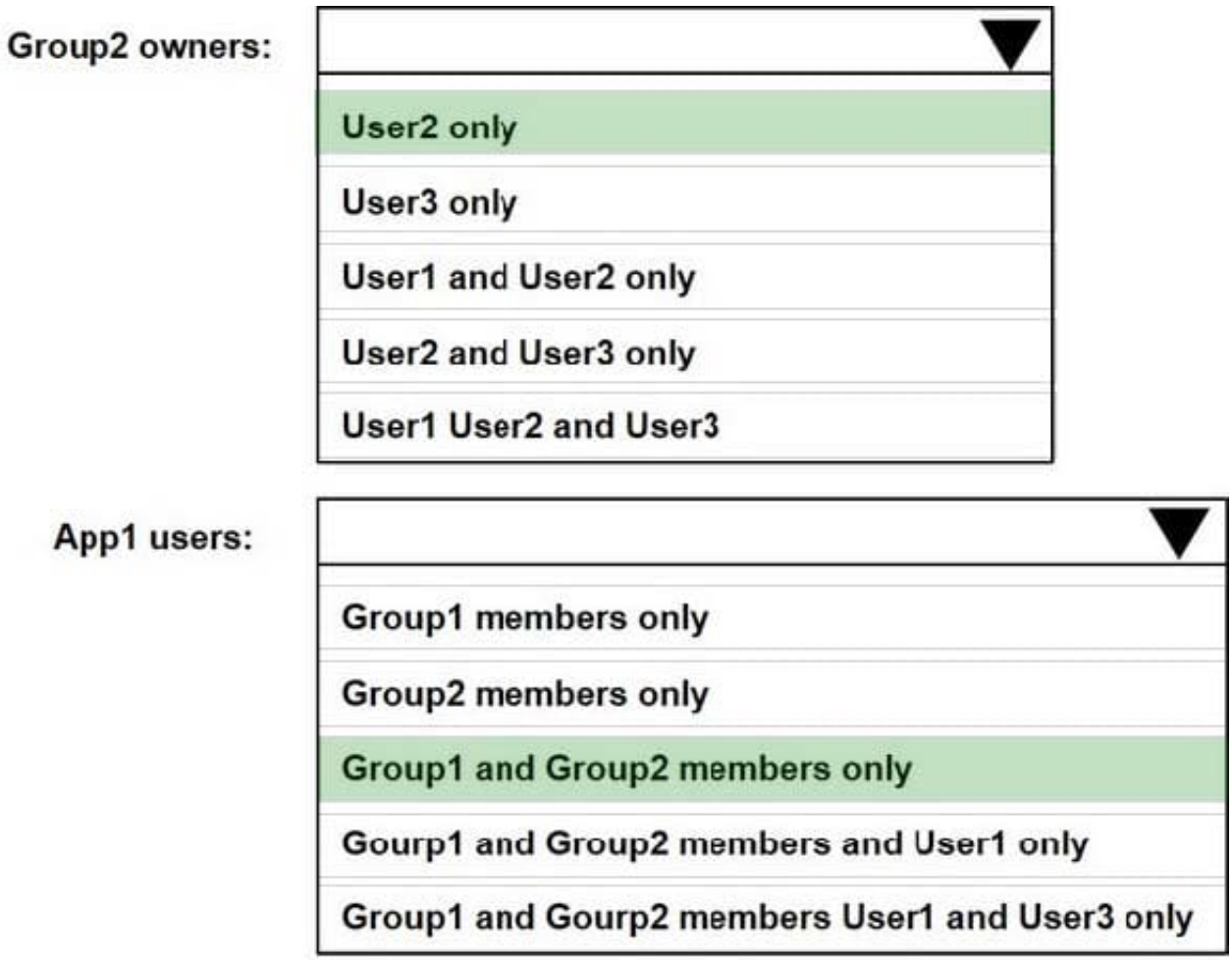
The user and group settings for App1 are configured as shown in the following exhibit.



Hot Area:



Correct Answer:



QUESTION 6

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

You enable the diagnostic logs for the storage account.

What should you use to retrieve the diagnostics logs?

A. Azure Security Center

B. Azure Monitor

C. the Security admin center

D. Azure Storage Explorer

Correct Answer: D

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

QUESTION 7

HOTSPOT

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

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

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

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

The firewalls on all the virtual machines allow ping traffic.

NSG1 is configured as shown in the following exhibit. Inbound security rules

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

Outbound security rules

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

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

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Statements	Yes	No
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

Correct Answer:

Answer Area

Statements	Yes	No
VM1 can ping VM3 successfully.	○	○
VM2 can ping VM4 successfully.	○	○
VM3 can be accessed by using Remote Desktop from the internet.	○	○

Box 1: Yes

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

Box 2: No

VM2 and VM4 are on separate VNets and the VNets are not peered. Therefore, the pings would have to go over the Internet. VM4 does have a public IP and the firewall allows pings. However, for VM2 to be able to ping VM4, VM2 would

also need a public IP address. In Azure, pings don\\'t go out through the default gateway as they would in a physical network. For an Azure VM to ping external IPs, the VM must have a public IP address assigned to it.

Box 3: Yes

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

QUESTION 8

HOTSPOT

You have the Azure key vaults shown in the following table.

Name	Location	Azure subscription name
KV1	West US	Subscription1
KV2	West US	Subscription1
KV3	East US	Subscription1
KV4	West US	Subscription2
KV5	East US	Subscription2

KV1 stores a secret named Secret1 and a key for a managed storage account named Key1.

You back up Secret1 and Key1.

To which key vaults can you restore each backup? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

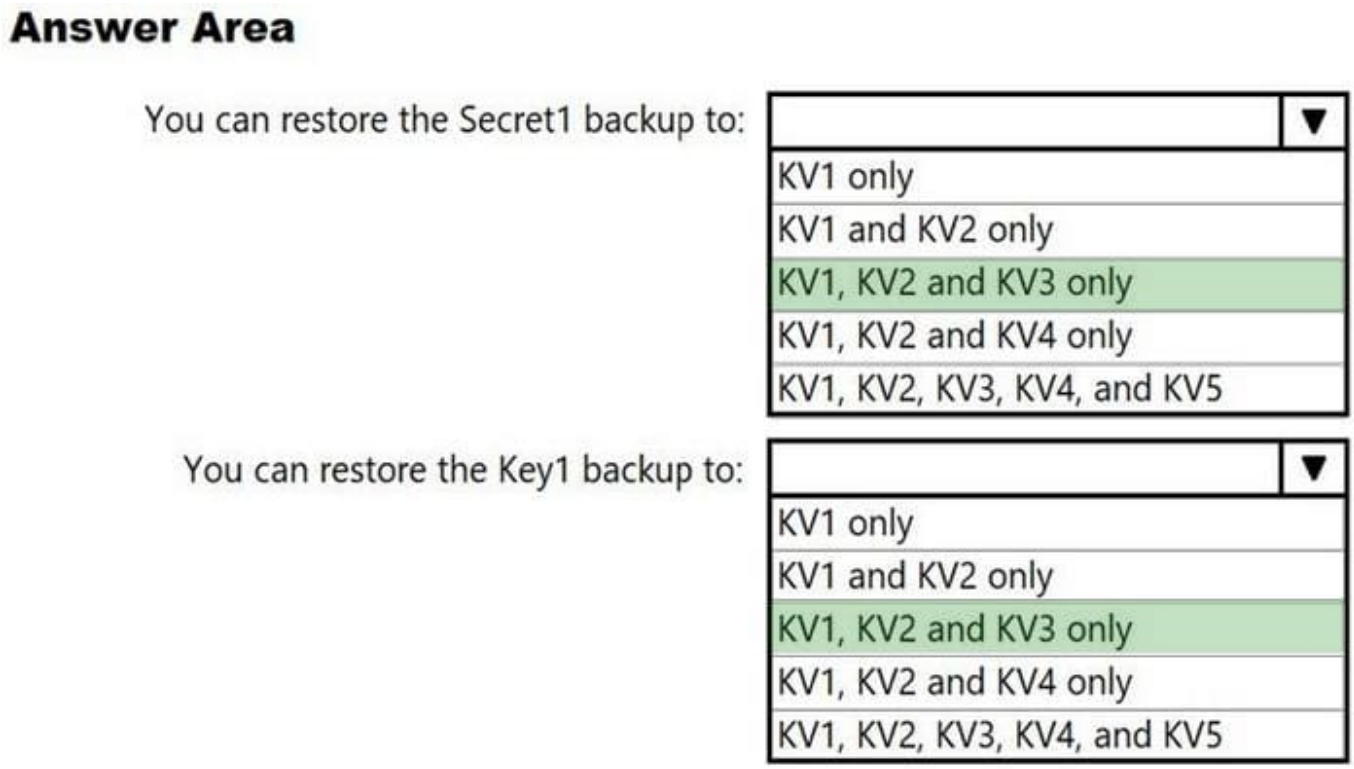
You can restore the Secret1 backup to:

- KV1 only
- KV1 and KV2 only
- KV1, KV2 and KV3 only
- KV1, KV2 and KV4 only
- KV1, KV2, KV3, KV4, and KV5

You can restore the Key1 backup to:

- KV1 only
- KV1 and KV2 only
- KV1, KV2 and KV3 only
- KV1, KV2 and KV4 only
- KV1, KV2, KV3, KV4, and KV5

Correct Answer:



The backups can only be restored to key vaults in the same subscription and same geography. You can restore to a different region in the same geography.

QUESTION 9

SIMULATION

A user named Debbie has the Azure app installed on her mobile device.

You need to ensure that debbie@contoso.com is alerted when a resource lock is deleted.

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

A. See the explanation below.

Correct Answer: A

You need to configure an alert rule in Azure Monitor.

1.

Type Monitor into the search box and select Monitor from the search results.

2.

Click on Alerts.

3.

Click on +New Alert Rule.

4.

In the Scope section, click on the Select resource link.

5.

In the Filter by resource type box, type locks and select Management locks (locks) from the filtered results.

6.

Select the subscription then click the Done button.

7.

In the Condition section, click on the Select condition link.

8.

Select the Delete management locks condition the click the Done button.

9.

In the Action group section, click on the Select action group link.

10.Click the Create action group button to create a new action group.

11.Give the group a name such as Debbie Mobile App (it doesn\\'t matter what name you enter for the exam) then click the Next: Notifications > button.

12.In the Notification type box, select the Email/SMS message/Push/Voice option.

13.In the Email/SMS message/Push/Voice window, tick the Azure app Push Notifications checkbox and enter and enter debbie@contoso.com in the Azure account email field.

14.Click the OK button to close the window.

15.Enter a name such as Debbie Mobile App in the notification name box.

16.Click the Review and Create button then click the Create button to create the action group.

17.Back in the Create alert rule window, in the Alert rule details section, enter a name such as Management lock deletion in the Alert rule name field.

18.Click the Create alert rule button to create the alert rule.

QUESTION 10

You have an Azure subscription.

You plan to create a custom role-based access control (RBAC) role that will provide permission to read the Azure Storage account.

Which property of the RBAC role definition should you configure?

A. NotActions []

B. DataActions []

C. AssignableScopes []

D. Actions []

Correct Answer: D

To `Read a storage account\\', ie. list the blobs in the storage account, you need an `Action\\' permission. To read the data in a storage account, ie. open a blob, you need a `DataAction\\' permission.

Reference: https://docs.microsoft.com/en-us/azure/role-based-access-control/role-definitions

QUESTION 11

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

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

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

You need to deploy Microsoft Antimalware to the virtual machines.

Solution: You connect to each virtual machine and add a Windows feature.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

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

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

QUESTION 12

SIMULATION

You need to create a new Azure Active Directory (Azure AD) directory named 11641655.onmicrosoft.com and a user named User1 in the new directory. The solution must ensure that User1 is enabled for Azure Multi-Factor Authentication (MFA).

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

A. See the explanation below.

Correct Answer: A

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 is created.

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.

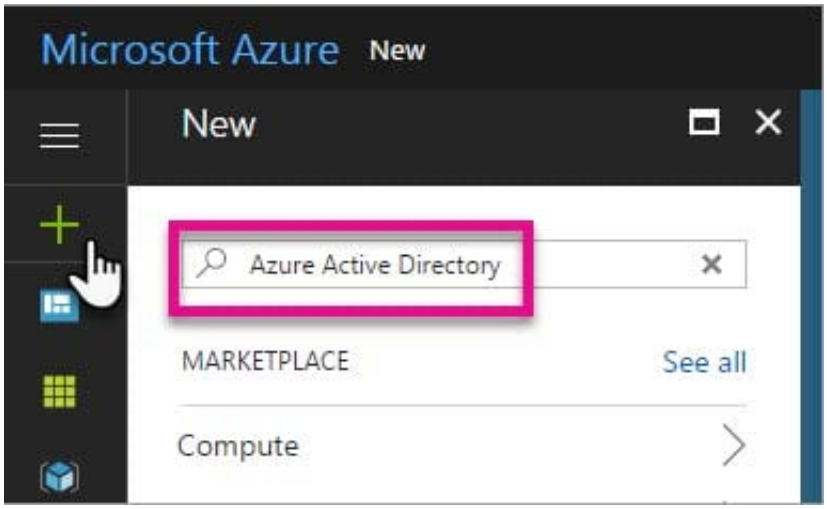
Under Manage, select Users.

9.

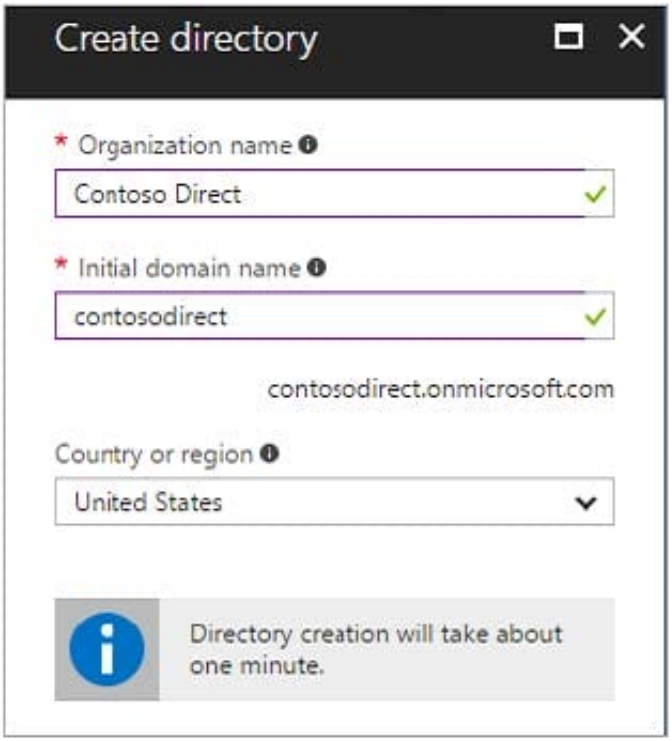
Select All users and then select + New user.

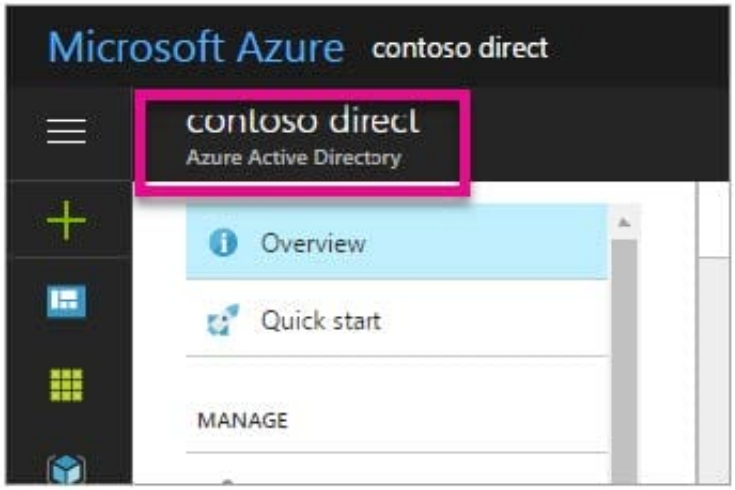
10.

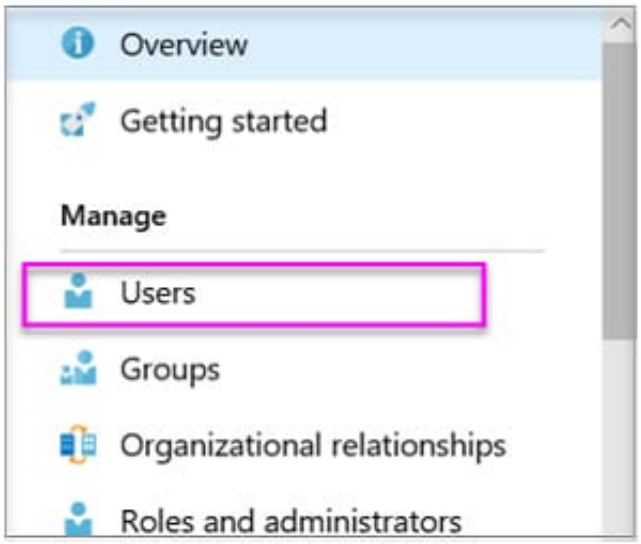
Provide a Name and User name (user1) for the regular user tenant You can also show the temporary password. When you\\'re done, select Create.


Microsoft Azure New
New
Azure Active Directory
MARKETPLACE
See all
Compute

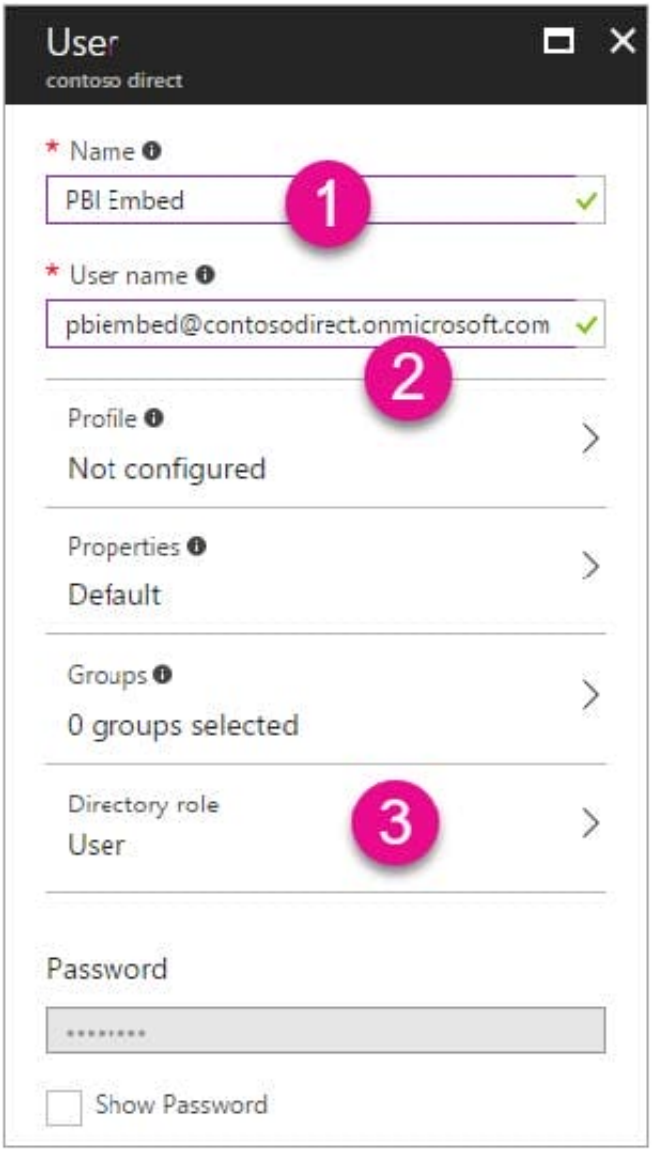

Azure Active Directory
Results
NAME
PUBLISHER
Azure Active Directory
Microsoft


Create directory
* Organization name
Contoso Direct
* Initial domain name
contosodirect
contosodirect.onmicrosoft.com
Country or region
United States
Directory creation will take about one minute.





Name: user1 User name: user1@10598168.onmicrosoft.com



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

QUESTION 13

HOTSPOT

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

Name	Type	Location	In resource group
RG1	Resource group	East US	*Not applicable*
RG2	Resource group	West US	*Not applicable*
RG3	Resource group	Central US	*Not applicable*
VNet1	Virtual network	Central US	RG2

VNet1 contains the subnets shown in the following table.

Name	Description
AzureFirewall	Contains no resources
AzureFirewallSubnet	Contains no resources
Subnet1	Contains a virtual machine
Subnet2	Contains no resources

You plan to use the Azure portal to deploy an Azure firewall named AzFW1 to VNet1.

Which resource group and subnet can you use to deploy AzFW1? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

DB1:

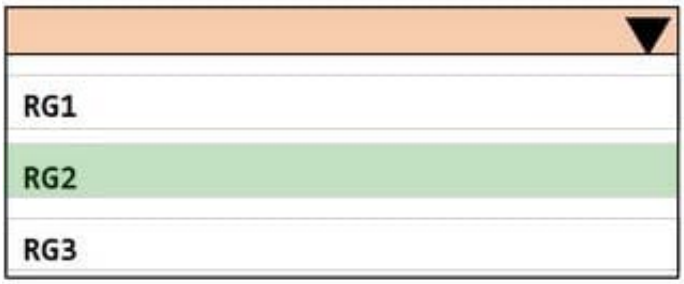
- RG1
- RG2
- RG3

Subnet:

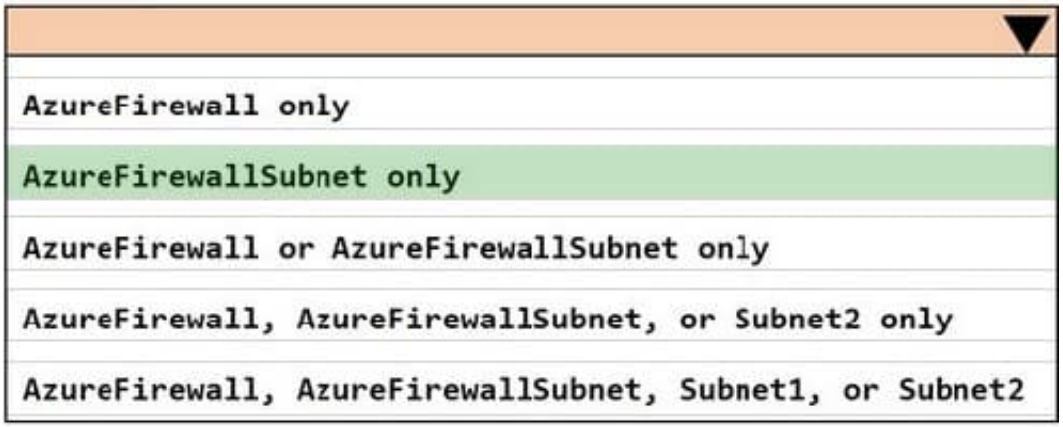
- AzureFirewall only
- AzureFirewallSubnet only
- AzureFirewall or AzureFirewallSubnet only
- AzureFirewall, AzureFirewallSubnet, or Subnet2 only
- AzureFirewall, AzureFirewallSubnet, Subnet1, or Subnet2

Correct Answer:

DB1:



Subnet:



QUESTION 14

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

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

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

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

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

A. VM4 only

B. VM1 and VM3 only

C. VM1, VM3 and VM4 only

D. VM1, VM2, VM3, and VM4

Correct Answer: C

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

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

QUESTION 15

HOTSPOT

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

Name	Connected to	Private IP address	Public IP address
VM1	VNET1/Subnet1	10.1.1.5	20.224.219.170
VM2	VNET1/Subnet2	10.1.2.5.	20.224.219.230
VM3	VNET2/Subnet1	10.11.1.5	40.122.155.212

You have an Azure Cosmos DB account named cosmos1 configured as shown in the following exhibit.

Hot Area:

Statements	Yes	No
VM1 can access cosmos1 over the internet.	○	○
VM2 can access cosmos1 over the internet.	○	○
VM3 can access cosmos1 over the internet.	○	○

Correct Answer:

Statements	Yes	No
VM1 can access cosmos1 over the internet.	○	○
VM2 can access cosmos1 over the internet.	○	○
VM3 can access cosmos1 over the internet.	○	○