AZ-104 Q&As

Microsoft Azure Administrator

Pass Microsoft AZ-104 Exam with 100% Guarantee

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

https://www.pass2lead.com/az-104.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

HOTSPOT

You have an Azure Active Directory (Azure AD) tenant.

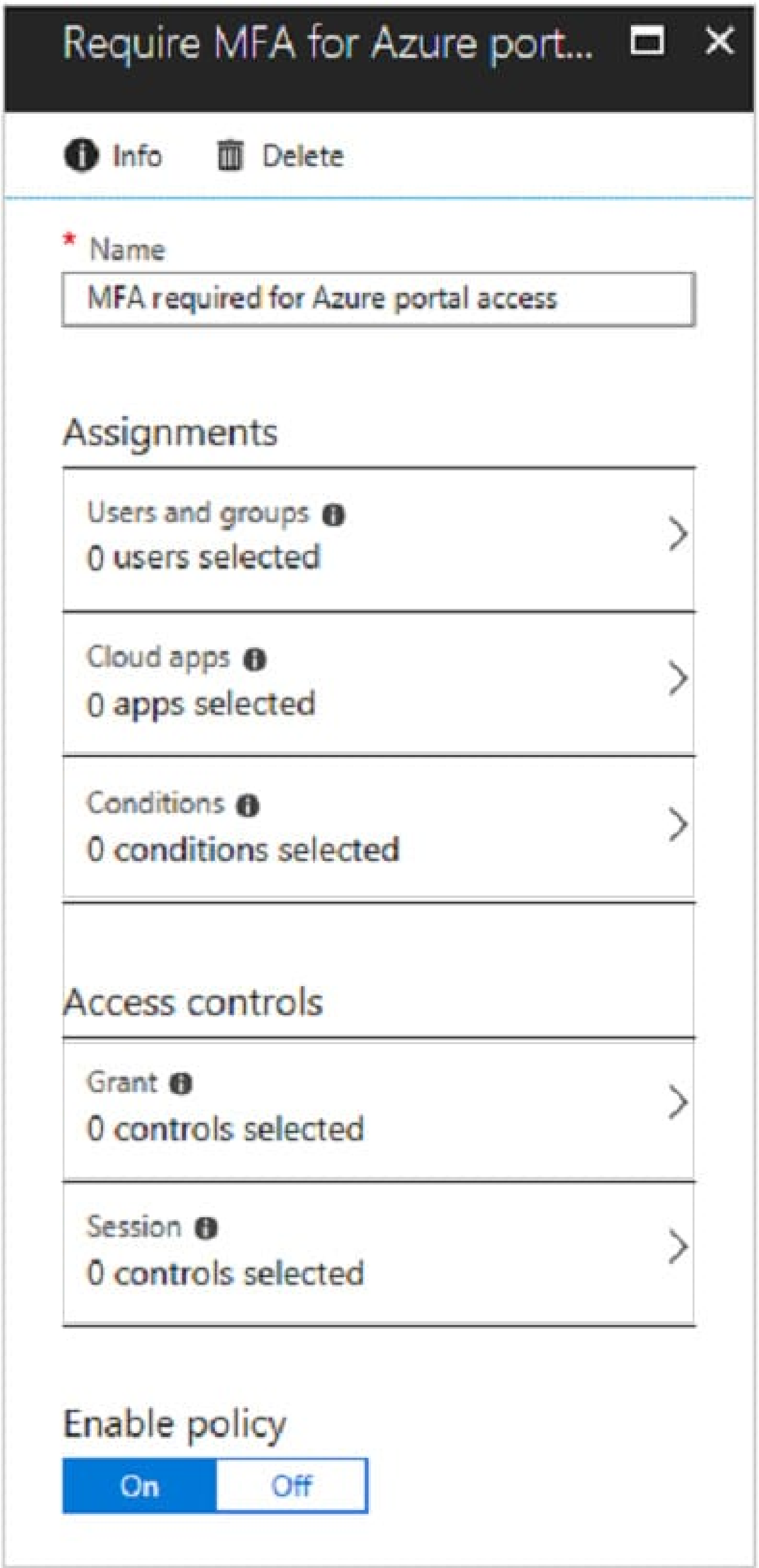
You want to implement Multi-Factor Authentication by making use of a conditional access policy. The conditional access policy must be applied to all users when they access the Azure portal.

Which three settings should you configure? To answer, select the appropriate settings to the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area



Require MFA for Azure port...

* Name

MFA required for Azure portal access

Assignments

Users and groups
0 users selected

Cloud apps
0 apps selected

Conditions
0 conditions selected

Access controls

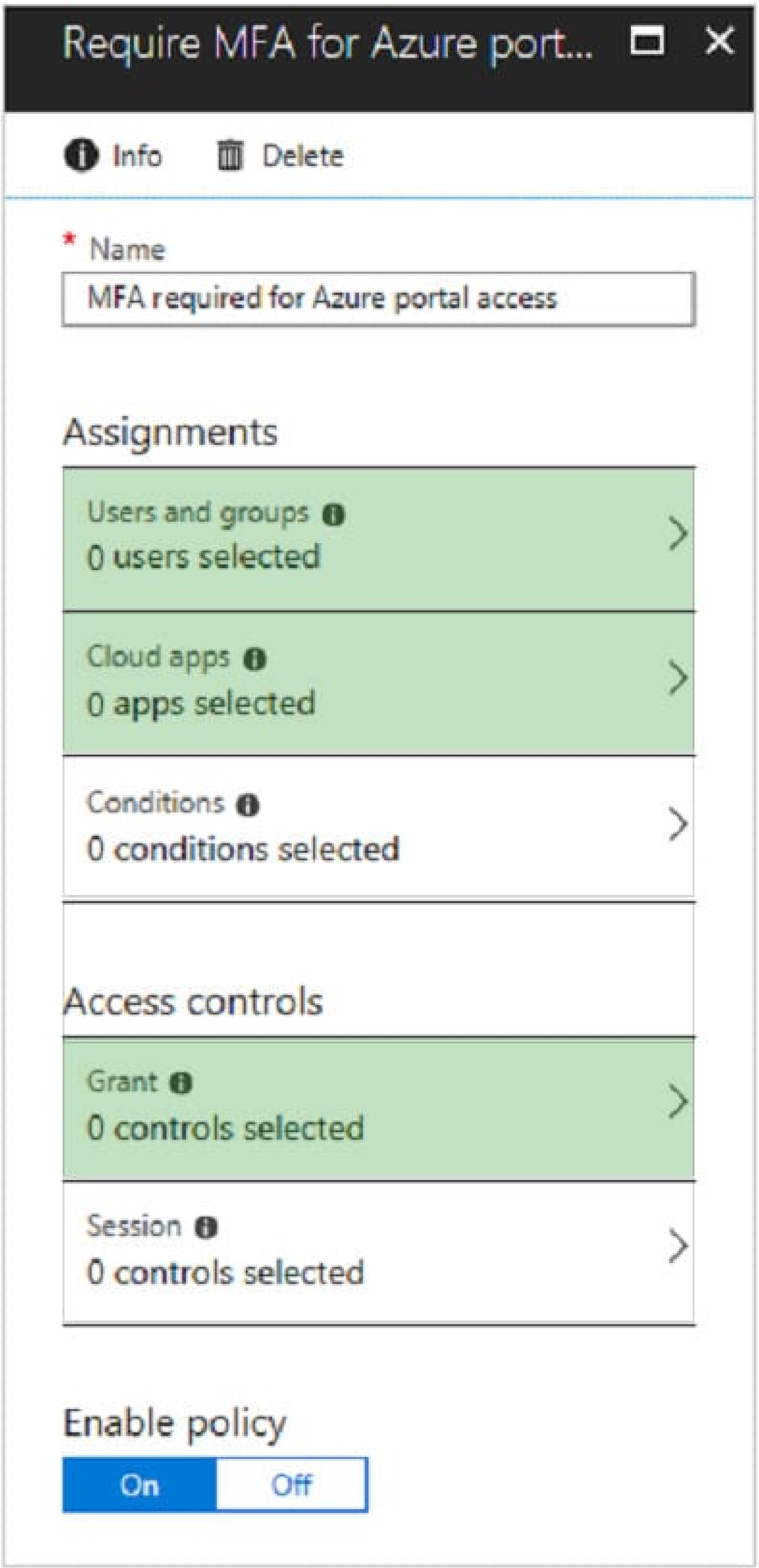
Grant
0 controls selected

Session
0 controls selected

Enable policy

Correct Answer:

Answer Area



Require MFA for Azure port...

* Name

MFA required for Azure portal access

Assignments

Users and groups
0 users selected

Cloud apps
0 apps selected

Conditions
0 conditions selected

Access controls

Grant
0 controls selected

Session
0 controls selected

Enable policy

Box 1:

The conditional access policy must be applied or assigned to Users and Groups.

Box 2:

The conditional access policy must be applied when users access the Azure portal, which is a cloud app.

That is: Microsoft Azure Management

Box 3:

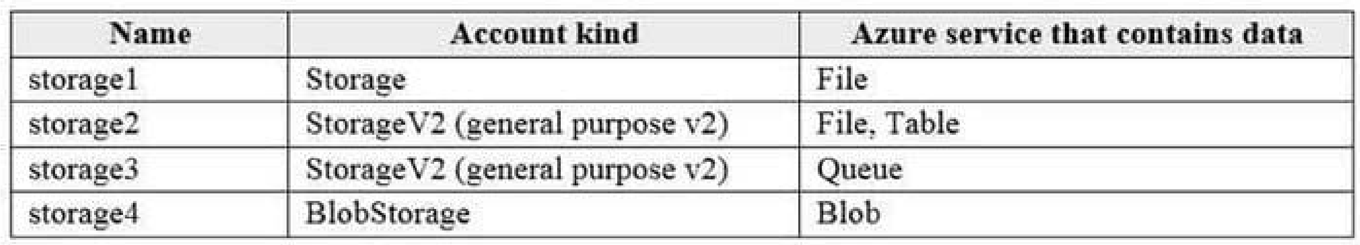
Access control must require multi-factor authentication when granting access.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/app-based-mfa

QUESTION 2

You have an Azure subscription named Subscription1 that contains the storage accounts shown in the following table:



Name	Account kind	Azure service that contains data
storage1	Storage	File
storage2	StorageV2 (general purpose v2)	File, Table
storage3	StorageV2 (general purpose v2)	Queue
storage4	BlobStorage	Blob

You plan to use the Azure Import/Export service to export data from Subscription1.

You need to identify which storage account can be used to export the data.

What should you identify?

A. storage1

B. storage2

C. storage3

D. storage4

Correct Answer: D

Azure Import/Export service supports the following of storage accounts:

1.

Standard General Purpose v2 storage accounts (recommended for most scenarios)

2.

Blob Storage accounts

3.

General Purpose v1 storage accounts (both Classic or Azure Resource Manager deployments), Azure Import/Export service supports the following storage types:

1.

Import supports Azure Blob storage and Azure File storage

2.

Export supports Azure Blob storage

Reference: https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-requirements

QUESTION 3

You have a service deployed to a Kubernetes cluster.

Another application needs to access the service via the private IP address of the pod.

Which of the following would you define as the networking type for the cluster to meet this requirement?

A. Kubenet

B. Azure container networking plugin

C. Service Endpoints

D. Network security groups

Correct Answer: B

Azure container networking plugin : Correct Choice

With the Azure container networking plugin , every pod gets an IP address allocated.

With Azure CNI, every pod gets an IP address from the subnet and can be accessed directly. These IP addresses must be unique across your network space, and must be planned in advance. Each node has a configuration parameter for the

maximum number of pods that it supports. The equivalent number of IP addresses per node are then reserved up front for that node. This approach requires more planning, as can otherwise lead to IP address exhaustion or the need to

rebuild clusters in a larger subnet as your application demands grow.

Nodes use the Azure Container Networking Interface (CNI) Kubernetes plugin.

Kubenet : Incorrect Choice

The kubenet networking option is the default configuration for AKS cluster creation. With kubenet, nodes get an IP address from the Azure virtual network subnet. Pods receive an IP address from a logically different address space to the

Azure virtual network subnet of the nodes.

Service Endpoints : Incorrect Choice

Capabilities like service endpoints or UDRs are supported with both kubenet and Azure CNI, the support policies for AKS define what changes you can make. For example:

If you manually create the virtual network resources for an AKS cluster, you\\'re supported when configuring your own UDRs or service endpoints. If the Azure platform automatically creates the virtual network resources for your AKS cluster, it

isn\\'t supported to manually change those AKS-managed resources to configure your own UDRs or service endpoints.

Network security groups : Incorrect Choice

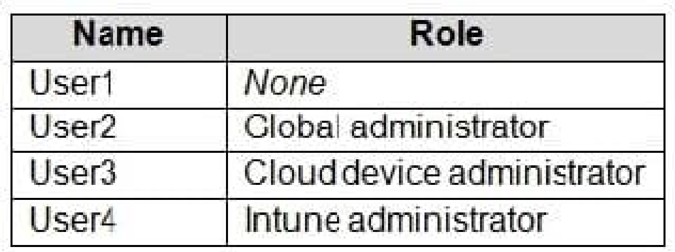
A network security group filters traffic for VMs, such as the AKS nodes. As you create Services, such as a LoadBalancer, the Azure platform automatically configures any network security group rules that are needed.

Reference:

https://docs.microsoft.com/en-us/azure/aks/concepts-network

QUESTION 4

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



Name	Role
User1	*None*
User2	Global administrator
User3	Cloud device administrator
User4	Intune administrator

Adatum.com has the following configurations:

1.

Users may join devices to Azure AD is set to User1.

2.

Additional local administrators on Azure AD joined devices is set to None.

You deploy Windows 10 to a computer named Computer1. User1 joins Computer1 to adatum.com.

You need to identify the local Administrator group membership on Computer1.

Which users are members of the local Administrators group?

A. User1 only

B. User1, User2, and User3 only

C. User1 and User2 only

D. User1, User2, User3, and User4

E. User2 only

Correct Answer: C

Users may join devices to Azure AD - This setting enables you to select the users who can register their devices as Azure AD joined devices. The default is All. Additional local administrators on Azure AD joined devices - You can select the users that are granted local administrator rights on a device. Users added here are added to the Device Administrators role in Azure AD. Global administrators, here User2, in Azure AD and device owners are granted local administrator rights by default.

References: https://docs.microsoft.com/en-us/azure/active-directory/devices/device-management-azure-portal

QUESTION 5

HOTSPOT

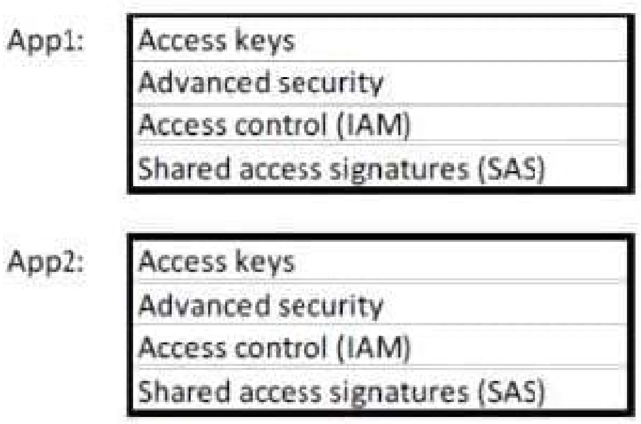
You have an Azure Storage account named storage1.

You have an Azure App Service app named app1 and an app named App2 that runs in an Azure container instance. Each app uses a managed identity.

You need to ensure that App1 and App2 can read blobs from storage1 for the next 30 days.

What should you configure in storage1 for each app?

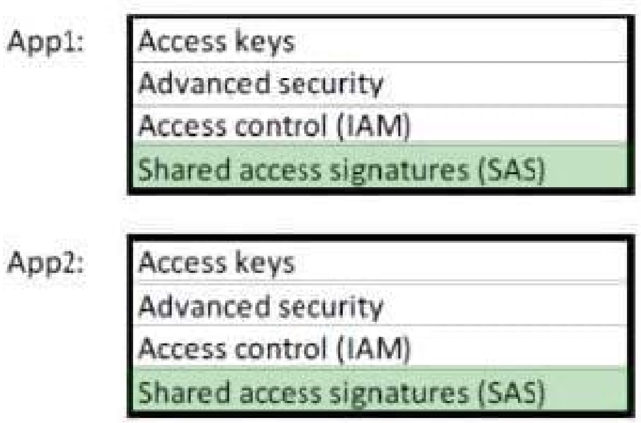
Hot Area:



App1:
- Access keys
- Advanced security
- Access control (IAM)
- Shared access signatures (SAS)

App2:
- Access keys
- Advanced security
- Access control (IAM)
- Shared access signatures (SAS)

Correct Answer:



App1:

- Access keys
- Advanced security
- Access control (IAM)
- [✓ Shared access signatures (SAS)]

App2:

- Access keys
- Advanced security
- Access control (IAM)
- [✓ Shared access signatures (SAS)]

With Shared access signature you can limit the resources for access and at the same time can control the duration of the access.

A shared access signature (SAS) provides secure delegated access to resources in your storage account without compromising the security of your data. With a SAS, you have granular control over how a client can access your data. You can

control what resources the client may access, what permissions they have on those resources, and how long the SAS is valid, among other parameters.

Reference:

https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview