

Microsoft

AZ-305 Exam

Designing Microsoft Azure Infrastructure Solutions

Thank you for Downloading AZ-305 exam PDF Demo

You can also try our AZ-305 practice exam software

Download Free Demo

https://prepbolt.com/AZ-305.html

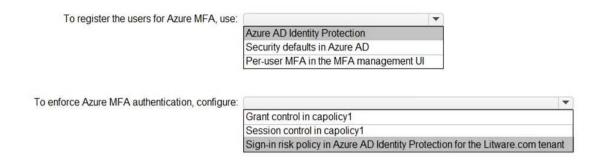
QUESTIONS & ANSWERS

DEMO VERSION

(LIMITED CONTENT)

Version: 20.2

Question: 1		
HOTSPOT		
потого		
You need to ensure that users manage	ging the production environment are registered for Azure I	MFA
and must authenticate by using Azur	e MFA when they sign in to the Azure portal. The solution	must
meet the authentication and authori		
meet the dathertication and dathor	zation requirements.	
What should you do? To answer, sele	ct the appropriate options in the answer area.	
NOTE: Each correct selection is worth	n one point.	
To register the users for Azure MFA, use:	Azure AD Identity Protection	
	Security defaults in Azure AD	
	Per-user MFA in the MFA management UI	
To enforce Azure MFA authentication, configure:	•	
,	Grant control in capolicy1	
	Session control in capolicy1	
	Sign-in risk policy in Azure AD Identity Protection for the Litware.com tenant	
	Answer:	
Explanation:		



Box 1: Azure AD Identity Protection

Azure AD Identity Protection helps you manage the roll-out of Azure AD Multi-Factor Authentication (MFA) registration by configuring a Conditional Access policy to require MFA registration no matter what modern authentication app you are signing in to.

Scenario: Users that manage the production environment by using the Azure portal must connect from a hybrid Azure AD-joined device and authenticate by using Azure Multi-Factor Authentication (MFA).

Box 2: Sign-in risk policy...

Scenario: The Litware.com tenant has a conditional access policy named capolicy1. Capolicy1 requires that when users manage the Azure subscription for a production environment by using the Azure portal, they must connect from a hybrid Azure AD-joined device.

Identity Protection policies we have two risk policies that we can enable in our directory.

Sign-in risk policy

User risk policy

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-protection-configure-mfa-policy

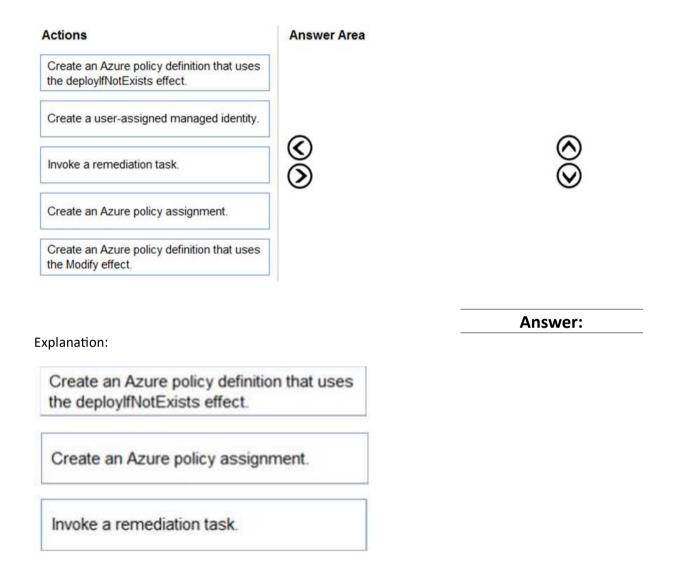
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/howto-identity-

protection-configure-risk-policies
Question: 2 You plan to migrate App1 to Azure.
You need to recommend a network connectivity solution for the Azure Storage account that will host the App1 dat
a. The solution must meet the security and compliance requirements.
What should you include in the recommendation?
A. a private endpoint
B. a service endpoint that has a service endpoint policy
C. Azure public peering for an ExpressRoute circuit
D. Microsoft peering for an ExpressRoute circuit
Explanation: Answer: A
Private Endpoint securely connect to storage accounts from on-premises networks that connect to the VNet using VPN or ExpressRoutes with private-peering.
Private Endpoint also secure your storage account by configuring the storage firewall to block all connections on the public endpoint for the storage service.
https://docs.microsoft.com/en-us/azure/expressroute/expressroute-faqs#microsoft-peering

Question: 3
You plan to migrate App1 to Azure. The solution must meet the authentication and authorization requirements.
Which type of endpoint should App1 use to obtain an access token?
A. Azure Instance Metadata Service (IMDS)
B. Azure AD
C. Azure Service Management
D. Microsoft identity platform
Answer: D
Explanation:
Scenario: To access the resources in Azure, App1 must use the managed identity of the virtual machines that will host the app.
Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication. Applications may use the managed identity to obtain Azure AD tokens.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-
<u>resources/overview</u>
Question: 4
DRAG DROP

You need to configure an Azure policy to ensure that the Azure SQL databases have TDE enabled. The solution must meet the security and compliance requirements.

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.



Scenario: All Azure SQL databases in the production environment must have Transparent Data Encryption (TDE) enabled.

Step 1: Create an Azure policy definition that uses the deployIfNotExists identity.

The first step is to define the roles that deployIfNotExists and modify needs in the policy definition to successfully deploy the content of your included template.

Step 2: Create an Azure policy assignment

When creating an assignment using the portal, Azure Policy both generates the managed identity and grants it the roles defined in roleDefinitionIds.

Step 3: Invoke a remediation task

Resources that are non-compliant to a deployIfNotExists or modify policy can be put into a compliant state through Remediation. Remediation is accomplished by instructing Azure Policy to run the deployIfNotExists effect or the modify operations of the assigned policy on your existing resources and subscriptions, whether that assignment is to a management group, a subscription, a resource group, or an individual resource.

During evaluation, the policy assignment with deploylfNotExists or modify effects determines if there are non-compliant resources or subscriptions. When non-compliant resources or subscriptions are found, the details are provided on the Remediation page.

Reference:

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

Question: 5
HOTSPOT

.....

You plan to migrate App1 to Azure.

You need to recommend a high-availability solution for App1. The solution must meet the resiliency requirements.

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

NOTE: Each correct selection is worth one point.

Number of host groups:		-	
	1		
	2		
	3		
	6		
Number of virtual machine scale sets:		-	
	0		
	1		
	3		
		•	
			Answ

Number of host groups:		-
	1	
	2	
	3	
	6	
Number of virtual machine scale sets:		-
	0	
	1	
	3	

Box 1: 3

Explanation:

Scenario: App1 must meet the following requirements:

Be hosted in an Azure region that supports availability zones.

Maintain availability if two availability zones in the local Azure region fail.

A host group is a resource that represents a collection of dedicated hosts. You create a host group in a region and an availability zone, and add hosts to it.

Use Availability Zones for fault isolation

Availability zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. A host group is created in a single availability zone. Once created, all hosts will be placed within that zone. To achieve high availability across zones, you need to create multiple host groups (one per zone) and spread your hosts accordingly.

Box 2: 1

Scenario: App1 must meet the following requirements:

Be hosted on Azure virtual machines that support automatic scaling.

An Azure virtual machine scale set can automatically increase or decrease the number of VM instances that run your application. This automated and elastic behavior reduces the management overhead to monitor and optimize the performance of your application.

Reference:

https://docs.microsoft.com/en-us/azure/virtual-machines/dedicated-hosts

https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-autoscale-overview

Thank You for trying AZ-305 PDF Demo

To try our AZ-305 practice exam software visit link below

https://prepbolt.com/AZ-305.html

Start Your AZ-305 Preparation

Use Coupon "SAVE50" for extra 50% discount on the purchase of Practice Test Software. Test your AZ-305 preparation with actual exam questions.