**Question: 232**

You are implementing authentication for applications in your company. You plan to implement self-service password reset (SSPR) and multifactor authentication (MFA) in Azure Active Directory (Azure AD).

You need to select authentication mechanisms that can be used for both MFA and SSPR.

Which two authentication methods should you use? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. **Short Message Service (SMS) messages**
B. **Authentication app**
C. **Email addresses**
D. **Security questions**
E. **App passwords**

**Answer: AB**

**Explanation:**

The following authentication mechanisms can be used for both MFA and SSPR:

- Short Message Service (SMS) messages
- Azure AD passwords
- Microsoft Authenticator app
- Voice call

Incorrect Answers:

C, D:

The following authentication mechanisms are used for SSPR only:

- Email addresses
- Security questions

E: App passwords authentication mechanisms can be used for MFA only, but only in certain cases.

Reference:


**Question: 233**

You have an Azure subscription.

You have 100 Azure virtual machines.

You need to quickly identify underutilized virtual machines that can have their service tier changed to a less expensive offering.

Which blade should you use?

A. **Customer insights**
B. **Monitor**
C. **Advisor**
D. **Metrics**
Explanation:
Advisor helps you optimize and reduce your overall Azure spend by identifying idle and underutilized resources. You can get cost recommendations from the Cost tab on the Advisor dashboard. 
Reference:
https://docs.microsoft.com/en-us/azure/advisor/advisor-cost-recommendations

Question: 234

An app uses a virtual network with two subnets. One subnet is used for the application server. The other subnet is used for a database server. A network virtual appliance (NVA) is used as a firewall. Traffic destined for one specific address prefix is routed to the NVA and then to an on-premises database server that stores sensitive data. A Border Gateway Protocol (BGP) route is used for the traffic to the on-premises database server.

You need to recommend a method for creating the user-defined route.
Which two options should you recommend? Each correct answer presents a complete solution.

A. For the virtual network configuration, use a VPN.
B. For the next hop type, use a virtual network peering.
C. For the virtual network configuration, use Azure ExpressRoute.
D. For the next hop type, use a virtual network gateway.

Answer: AD

Explanation:
You can create custom, or user-defined, routes in Azure to override Azure’s default system routes, or to add additional routes to a subnet’s route table. You can specify the following next hop types when creating a user-defined route:

Virtual appliance: A virtual appliance is a virtual machine that typically runs a network application, such as a firewall.
Virtual network gateway: Specify when you want traffic destined for specific address prefixes routed to a virtual network gateway. The virtual network gateway must be created with type VPN. You cannot specify a virtual network gateway created as type ExpressRoute in a user-defined route because with ExpressRoute, you must use BGP for custom routes.
None: Specify when you want to drop traffic to an address prefix, rather than forwarding the traffic to a destination.
Virtual network: Specify when you want to override the default routing within a virtual network.
Internet: Specify when you want to explicitly route traffic destined to an address prefix to the Internet, or if you want traffic destined for Azure services with public IP addresses kept within the Azure backbone network.

Incorrect Answers:
B: You cannot specify VNet peering or VirtualNetworkServiceEndpoint as the next hop type in user-defined routes. Routes with the VNet peering or VirtualNetworkServiceEndpoint next hop types are only created by Azure, when you configure a virtual network peering, or a service endpoint.
C: You cannot specify a virtual network gateway created as type ExpressRoute in a user-defined route because with ExpressRoute, you must use BGP for custom routes.

Reference:

Question: 235

You plan to automate the deployment of a virtual machine scale set that uses the Windows Server 2016 Datacenter image. You need to ensure that when the scale set virtual machines are provisioned, they have web server components installed. Which two actions should you perform? Each correct answer presents part of the solution.

A. Upload a configuration script.
B. Create an automation account.
C. Create a new virtual machine scale set in the Azure portal.
D. Create an Azure policy.
E. Modify the extensionProfile section of the Azure Resource Manager template.

Answer: CE

References:
Question: 236
You have an Azure subscription that contains 10 virtual machines.
You need to ensure that you receive an email message when any virtual machines are powered off, restarted, or deallocated.
What is the minimum number of rules and action groups that you require?
A. three rules and three action groups
B. one rule and one action group
C. three rules and one action group
D. one rule and three action groups

Answer: C

We need a separate rule for each condition. We also need a separate action group for each action type that we want to fire when the rule is met. In this scenario we have three conditions (when any virtual machines are powered off, restarted, or deallocated) and one action type (you are sent an email message).

References:
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-metric-overview
https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups

Question: 237
You have an Azure subscription that contains 100 virtual machines.
You regularly create and delete virtual machines.
You need to identify unattached disks that can be deleted.
What should you do?
A. From Microsoft Azure Storage Explorer, view the Account Management properties.
C. From the Azure portal, configure the Advisor recommendations.
D. From Azure Cost Management, open the Optimizer tab and create a report.

Answer: D

Explanation:
You can find unused disks in the Azure Storage Explorer console. Once you drill down to the Blob containers under a storage account, you can see the lease state of the residing VHD (the lease state determines if the VHD is being used by any resource) and the VM to which it is leased out. If you find that the lease state and the VM fields are blank, it means that the VHD in question is unused.

Note: The ManagedBy property stores the Id of the VM to which Managed Disk is attached to. If the ManagedBy property is $null then it means that the Managed Disk is not attached to a VM.

Reference:
https://cloud.netapp.com/blog/reduce-azure-storage-costs

Question: 238
You have an Active Directory forest named contoso.com.
You install and configure Azure AD Connect to use password hash synchronization as the single sign-on (SSO) method. Staging mode is enabled.
You review the synchronization results and discover that the Synchronization Service Manager does not display any sync jobs.
You need to ensure that the synchronization completes successfully.
What should you do?
A. From Azure PowerShell, run Start-AdSyncSyncCycle -PolicyType Initial.
B. Run Azure AD Connect and set the SSO method to Pass-through Authentication.
C. From Synchronization Service Manager, run a full import.
D. Run Azure AD Connect and disable staging mode.

Answer: D

Explanation:
You have an Active Directory forest named contoso.com.
You install and configure Azure AD Connect to use password hash synchronization as the single sign-on (SSO) method. Staging mode is enabled.
You review the synchronization results and discover that the Synchronization Service Manager does not display any sync jobs.
You need to ensure that the synchronization completes successfully.
What should you do?
A. From Azure PowerShell, run Start-AdSyncSyncCycle -PolicyType Initial.
B. Run Azure AD Connect and set the SSO method to Pass-through Authentication.
C. From Synchronization Service Manager, run a full import.
D. Run Azure AD Connect and disable staging mode.

Answer: D

Explanation:
In staging mode, the server is active for import and synchronization, but it does not run any exports. A server in staging mode is not running password sync or password writeback, even if you selected these features during installation.

When you disable staging mode, the server starts exporting, enables password sync, and enables password writeback.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-staging-server
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sync-operations

Question: 239

You have an Azure subscription named Subscription1 that contains an Azure virtual machine named VM1. VM1 is in a resource group named RG1.

VM1 runs services that will be used to deploy resources to RG1.

You need to ensure that a service running on VM1 can manage the resources in RG1 by using the identity of VM1.

What should you do first?
A. From the Azure portal, modify the Access control (IAM) settings of RG1.
B. From the Azure portal, modify the Policies settings of RG1.
C. From the Azure portal, modify the Access control (IAM) settings of VM1.
D. From the Azure portal, modify the value of the Managed Service Identity option for VM1.

Answer: D

Through a create process, Azure creates an identity in the Azure AD tenant that's trusted by the subscription in use. After the identity is created, the identity can be assigned to one or more Azure service instances.

Reference: https://docs.microsoft.com/en-us/azure/app-service/overview-managed-identity

References: https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

Question: 240

You configure Azure AD Connect for Azure Active Directory Seamless Single Sign-On (Azure AD Seamless SSO) for an on-premises network.

Users report that when they attempt to access myapps.microsoft.com, they are prompted multiple times to sign in and are forced to use an account name that ends with onmicrosoft.com.

You discover that there is a UPN mismatch between Azure AD and the on-premises Active Directory.

You need to ensure that the users can use single-sign on (SSO) to access Azure resources.

What should you do first?
A. From on-premises network, deploy Active Directory Federation Services (AD FS).
B. From Azure AD, add and verify a custom domain name.
C. From on-premises network, request a new certificate that contains the Active Directory domain name.
D. From the server that runs Azure AD Connect, modify the filtering options.

Answer: B

Explanation:
The UPN is used by Azure AD to allow users to sign-in. The UPN that a user can use, depends on whether or not the domain has been verified. If the domain has been verified, then a user with that suffix will be allowed to sign-in to Azure AD.

To do so, you need to add and verify a custom domain in Azure AD before you can start syncing the users.

Reference:
https://docs.microsoft.com/en-us/azure/active-directory/hybrid/plan-connect-design-concepts#azure-ad-sign-in


Question: 241

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

You have an existing Azure AD conditional access policy named Policy1. Policy1 enforces the use of Azure AD-joined devices when members of the Global Administrators group authenticate to Azure AD from untrusted locations.

You need to ensure that members of the Global Administrators group will also be forced to use multi-factor authentication when authenticating from untrusted locations.

What should you do?
A. From the Azure portal, modify session control of Policy1.
B. From multi-factor authentication page, modify the user settings.

Answer: A
C. From multi-factor authentication page, modify the service settings.
D. From the Azure portal, modify grant control of Policy1.

Answer: C

Explanation:
We need to modify the grant control of Policy1.
The grant control can trigger enforcement of one or more controls.
Require multi-factor authentication (Azure Multi-Factor Authentication)
Require device to be marked as compliant (Intune)
Require Hybrid Azure AD joined device
Require approved client app
Require app protection policy
Note: It is now possible to explicitly apply the Require MFA for admins rule.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/untrusted-networks
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-baseline-protection

Question: 242

You have an Azure subscription named Subscription1 that is used by several departments at your company. Subscription1 contains the resources in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage1</td>
<td>Storage account</td>
</tr>
<tr>
<td>RG1</td>
<td>Resource group</td>
</tr>
<tr>
<td>Container1</td>
<td>Blob container</td>
</tr>
<tr>
<td>Share1</td>
<td>File share</td>
</tr>
</tbody>
</table>

Another administrator deploys a virtual machine named VM1 and an Azure Storage account named Storage2 by using a single Azure Resource Manager template. You need to view the template used for the deployment.
From the Azure Portal, for which blade can you view the template that was used for the deployment?
A. Container1
B. VM1
C. Storage2
D. RG1

Answer: D

Explanation:
You can verify the deployment by exploring the resource group from the Azure portal
Reference:

Question: 243

You have two subscriptions named Subscription1 and Subscription2. Each subscription is associated to a different Azure AD tenant.
Subscription1 contains a virtual network named VNet1. VNet1 contains an Azure virtual machine named VM1 and has an IP address space of 10.0.0.0/16.
Subscription2 contains a virtual network named VNet2. VNet2 contains an Azure virtual machine named VM2 and has an IP address space of 10.10.0.0/24.
You need to connect VNet1 to VNet2. What should you do first?
A. Modify the IP address space of VNet2.
B. Move VM1 to Subscription2.
C. Provision virtual network gateways.
D. Move VNet1 to Subscription2.

Answer: D
For More exams visit https://killexams.com/vendors-exam-list

Kill your exam at First Attempt....Guaranteed!