Azure fundamental assignment 5

1. **What is the Azure firewall? How to use the Azure firewall?**

   Azure Firewall is a cloud-native and intelligent network firewall security service that provides the best of breed threat protection for your cloud workloads running in Azure. It's a fully stateful, firewall as a service with built-in high availability and unrestricted cloud scalability.

   - Deploy the firewall into the VNet.
   - On the Azure portal menu or from the Home page, select Create a resource.
   - Type firewall in the search box and press Enter.
   - Select Firewall and then select Create.
   - On the Create a Firewall page, configure the firewall.
   - Accept the other default values, then select Review + create.
   - Review the summary, and then select Create to create the firewall.
   - This will take a few minutes to deploy.
   - After deployment completes, go to the Test-FW-RG resource group, and select the Test-FW01 firewall.

   - Note the firewall private and public IP addresses. You'll use these addresses later.

2. **Differentiate authentication and authorization?**

S.NO	Authentication	Authorization
1.	In authentication process, the identity of users are checked for providing the access to the system.	While in authorization process, person’s or user’s authorities are checked for accessing the resources.
2.	In authentication process, users or persons are verified.	While in this process, users or persons are validated.
3.	It is done before the authorization process.	While this process is done after the authentication process.
4.	It needs usually user’s login details.	While it needs user’s privilege or security levels.
5.	Authentication determines whether the person is user or not.	While it determines What permission do user have?

3. **What is Azure Active Directory?**

   Azure Active Directory (Azure AD) is a cloud-based identity and access management service. This service helps your employees access external resources, such as Microsoft 365, the Azure portal, and thousands of other SaaS applications. Azure AD also helps them access internal resources. These are resources like apps on your corporate network and intranet, along with any cloud apps developed by your own organization.

4. **What are multifactor authentication and conditional access available in Azure?**

   Multi-factor authentication is a process in which users are prompted during the sign-in process for an additional form of identification, such as a code on their cellphone or a fingerprint scan. If you only use a password to authenticate a user, it leaves an insecure vector for attack.

   Conditional Access brings signals together, to make decisions, and enforce organizational policies. Azure AD Conditional Access is at the heart of the new identity-driven control plane.

5. **What is resource lock? Describe why resource lock should be used?**

   As an administrator, you can lock a subscription, resource group, or resource to prevent other users in your organization from accidentally deleting or modifying critical resources. The lock overrides any permissions the user might have.

   As an additional layer of access control, we can use Azure Resource locking. Azure resource locks can be applied on individual resources or to resource groups. When applied to a resource group, all resource in that group, including any created after the lock has been put into place will be locked.

   A resource lock can be created with one of the following lock levels:

   CanNotDelete - the resource can be modified however not deleted.

   ReadOnly - the resource can neither be deleted or modified.

   Once a resource has been locked, the resource lock must first be removed before the resource can be modified or deleted.

6. **What is Azure policy? Write it Usage.**

   Azure Policy is a service in Azure which allows you create polices which enforce and control the properties of a resource. When these policies are used they enforce different rules and effects over your resources, so those resources stay compliant with your IT governance standards.

7. **What is the Azure government? What is Azure China 21Vianet?**

   Azure Government is the mission-critical cloud, delivering breakthrough innovation to US government customers and their partners. Only US federal, state, local and tribal governments and their partners have access to this dedicated instance, operated by screened US citizens.

   Microsoft Azure operated by 21Vianet (Azure China) is a physically separated instance of cloud services located in China. It's independently operated and transacted by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd..