AZURE CLOUD

# **Aim: - Azure cloud scenario based questions and answers:**

# **Q1. Assume that the development team in your company consults you as an Azure administrator to suggest an Azure solution that can be used to manage, scale, and orchestrate the deployment of the container-based application that they have developed. Which Azure solution will you suggest?**

# **Ans:-**

# As an Azure administrator, I would suggest the **Azure Kubernetes Service (AKS)** as an ideal solution to manage, scale, and orchestrate the deployment of the container-based application developed by the team.

# AKS is a fully managed Kubernetes service provided by Azure, which simplifies the deployment, scaling, and management of containerized applications. With AKS, the team can deploy and manage containerized applications with the power of Kubernetes without worrying about the underlying infrastructure.

# Some of the key features of AKS are:

# Automatic scaling, Integration with Azure services, Security, High availability, Easy deployment.

# AKS provides a highly available, secure, and scalable Kubernetes service that can effectively manage, scale, and orchestrate the deployment of containerized applications.

# **Q2. You are planning to deploy several Azure Virtual machines to host your applications. During the cost calculation phase, what are the two main factors that you will consider while deploying your virtual machines to Azure with the least possible cost?**

# **Ans:-**

# I can suggest that when deploying virtual machines to Azure with the least possible cost, the two main factors to consider are:

# **VM Size**: The size of the virtual machine is one of the most significant factors that affect the cost of deploying and running a virtual machine on Azure. You should choose the smallest VM size that is capable of running your application workloads effectively to reduce the cost of deploying virtual machines.

# **Reserved Instance**: Azure provides an option to reserve virtual machines for a 1-year or 3-year term. This option offers significant discounts on the cost of running virtual machines, particularly for long-term deployments. Therefore, it is essential to check the cost of reserved instances and compare them to the cost of on-demand instances before making a decision.

# **Q3. You are planning to build a policy to ensure that only the related team can deploy the Virtual machines and configure them. Which Azure tool will you use to achieve that?**

# **Ans:-**

# To ensure that only the related team can deploy Virtual Machines (VMs) and configure them in Azure, you can use **Role-Based Access Control (RBAC**). RBAC is an Azure tool that enables you to manage access to resources based on the roles of users in your organization.

# You can create custom RBAC roles that specify the exact permissions required for the related team to deploy and configure VMs. You can then assign those roles to the members of the team who require access to those resources.

# To implement RBAC in Azure, follow these general steps:

# Identify the Azure resources that you want to control access to, such as Virtual Machines, Virtual Networks, or Storage Accounts.

# Define the roles that you need for your organization, such as "Virtual Machine Contributor" or "Network Contributor".

# Assign users or groups to the roles that you defined.

# Test and refine your access control policies as necessary.

# By using RBAC, you can ensure that only the related team members have access to deploy and configure Virtual Machines in Azure, while also providing them with the appropriate level of access required to do their jobs.

# **Q4. Working as an Azure administrator, assume that you have deployed your applications to Azure Virtual machines. How could you restrict the traffic into these Azure virtual machines to be accepted only from specific sources?**

# **Ans:-**

# As an Azure administrator, you can restrict traffic to Azure virtual machines by using **Network Security Groups (NSGs) or Azure Firewall**.

# Here's how you can restrict traffic to Azure virtual machines using NSGs:

# Identify the virtual machines that need to be restricted.

# Create a new NSG or use an existing NSG.

# Associate the NSG with the virtual machines by assigning the NSG to the virtual network subnet containing the virtual machines.

# Configure inbound and outbound security rules on the NSG to allow traffic from specific sources and deny traffic from all other sources.

# For example, to restrict traffic to a virtual machine to only allow traffic from a specific IP address, you would create an inbound security rule on the NSG that allows traffic from that specific IP address and deny all other traffic.

# Here's how you can restrict traffic to Azure virtual machines using Azure Firewall:

# Create an Azure Firewall instance.

# Associate the Azure Firewall with the virtual network containing the virtual machines.

# Configure network rules to allow traffic from specific sources and deny traffic from all other sources.

# For example, to restrict traffic to a virtual machine to only allow traffic from a specific IP address, you would create a network rule on the Azure Firewall that allows traffic from that specific IP address and deny all other traffic.

# Both NSGs and Azure Firewall can provide granular control over network traffic, and the choice between the two options will depend on the specific requirements of your application and network architecture.

# **Q5. If you plan to deploy one of your Azure virtual machines in a separate network segment. How could you achieve that?**

# **Ans:-**

# To deploy an Azure virtual machine in a separate network segment, you can follow these steps:

# **Create a new virtual network**: First, create a new virtual network that will host the virtual machine. You can create a virtual network using the Azure portal, Azure CLI, or Azure PowerShell. Make sure that the new virtual network is in a different subnet than the virtual network that currently hosts the virtual machine.

# **Create a network security group**: Next, create a new network security group that will control the traffic to and from the virtual machine. You can create a network security group using the Azure portal, Azure CLI, or Azure PowerShell.

# **Configure network security group rules**: Once you have created the network security group, configure inbound and outbound rules to allow the traffic you need. For example, you may need to allow traffic for Remote Desktop Protocol (RDP) or HTTP traffic.

# **Assign the network security group to the virtual network:** After you have created and configured the network security group, assign it to the new virtual network that you created in step 1.

# **Move the virtual machine to the new virtual network**: Finally, move the virtual machine to the new virtual network by updating its network settings. You can do this using the Azure portal, Azure CLI, or Azure PowerShell. Once the virtual machine is in the new virtual network, it will be isolated from the other virtual machines in the original virtual network.

# By following these steps, you can deploy an Azure virtual machine in a separate network segment and control its traffic using a network security group.

# **Q6. A client wants the front end of his/ her application to be hosted on Azure, but wants the database to be hosted on-premises.**

# **Ans:-**

# Yes, it is possible to host the front end of an application on Azure while hosting the database on-premises. This setup is commonly known as a **hybrid cloud architecture**, which combines on-premises infrastructure with cloud-based resources.

# To implement this setup, you can use **Azure's Virtual Network service** to create a secure and reliable connection between the on-premises network and Azure. This allows the front end application to communicate with the on-premises database securely through the virtual network.

# One possible approach is to use **Azure App Service** to host the front-end application, which provides an easy way to deploy and manage web apps in Azure. You can also use **Azure Virtual Machines** to host the application if you need more control over the infrastructure.

# For the on-premises database, you can use a database management system like **Microsoft SQL Server** and configure it to allow access from the Azure virtual network. You can use **Azure ExpressRoute or VPN Gateway** to establish a secure connection between the on-premises network and Azure.

# Overall, hosting the front end of an application on Azure while hosting the database on-premises can provide a flexible and cost-effective solution for businesses that want to take advantage of cloud resources while maintaining control over their data.

# **Q7. You need to ensure that every time a user logs in, they are not asked to re-enter their passwords as part of the authentication.**

# **A. To enable Microsoft Account authentication**

# **B. Deploy Express Route**

# **C. set up a VPN between premises and datacentre. Set up an AD domain controller in VM and implement integrated Windows Authentication**

# **D. Configure Azure AD Sync to use single sign-on.**

# **Ans:-**

# The correct answer to ensure that users are not asked to re-enter their passwords as part of authentication when logging in is option

# **D. Configure Azure AD Sync to use single sign-on.**

# **Single sign-on (SSO)** is a feature that allows users to log in once using their credentials, after which they can access multiple systems or applications without having to provide their credentials again.

# When you **configure Azure AD Sync to use SSO**, users can use their Active Directory (AD) domain credentials to sign in to both on-premises and cloud-based applications, including Microsoft 365.

# Option A, enabling Microsoft Account authentication, would not prevent users from having to re-enter their password every time they log in, as it only applies to authentication using Microsoft Accounts, not AD domain credentials.

# Option B, deploying ExpressRoute, is a method for establishing a private, high-speed connection between your on-premises infrastructure and Azure datacenters. While this can improve network performance and security, it does not provide a mechanism for SSO.

# Option C, setting up a VPN between premises and datacenter and implementing integrated Windows Authentication, would allow users to use their AD domain credentials to authenticate when accessing resources in the datacenter. However, it would not provide SSO for cloud-based applications.

# In summary, to enable SSO for users logging in, you should configure Azure AD Sync to use SSO.

# **Q8. Your standard tier application is used across the world and uses the Azure website standard tier. It uses a large number of image files. However, this causes the application to load slowly**

# **A. Configure Azure blob storage with a custom domain**

# **B. Configure Azure website Autoscaling to increase instances at high loads**

# **C. Configure Azure CDN to cache all responses from the application’s web endpoint**

# **D. Configure Azure CDN to cache site images and content stored in Azure blob storage.**

# **Ans:-**

# The best approach to improve the performance of the application and reduce load times for image files would be **to configure Azure CDN to cache site images and content stored in Azure blob storage**. This will enable the CDN to serve the images and content from its cache rather than having to retrieve them from the website server every time they are requested, which will significantly reduce load times.

# Option (A) of configuring Azure blob storage with a custom domain would improve the performance of the application, but it would not directly address the issue of slow image file loading times.

# Option (B) of configuring Azure website autoscaling would help to manage high traffic loads, but it would not directly address the issue of slow image file loading times.

# Option (C) of configuring Azure CDN to cache all responses from the application’s web endpoint could help to improve performance by caching all responses, but it would also cache non-image files and increase cache misses, which can cause latency.

# Therefore, option (D) of configuring Azure CDN to cache site images and content stored in Azure blob storage is the best solution to improve the performance of the application and reduce load times for image files.