1. **Types of instances offered by Azure:**

Azure offers various types of virtual machine instances including General Purpose, Compute Optimized, Memory Optimized, Storage Optimized, GPU, and High-Performance Compute.

1. **How to set up an Azure VM:**

To set up an Azure VM, you can follow these steps:

• Sign in to the Azure portal.

• Click on "Create a resource" and search for "Virtual Machine".

• Click on "Virtual Machine" and then click "Create".

• Follow the wizard to configure the VM, including choosing a subscription, resource group, VM size, authentication type, networking settings, and other configurations.

1. **Difference between Scale Set and Availability Set:**

• Availability Set ensures that your VMs are distributed across multiple fault domains and update domains to ensure high availability and reliability.

• Scale Set allows you to create and manage a group of identical, load-balanced VMs. It automatically scales the number of VM instances in response to demand or a defined schedule.

1. **IaaS, PaaS, SaaS:**

• IaaS (Infrastructure as a Service) provides virtualized computing resources over the internet.

• PaaS (Platform as a Service) provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure.

• SaaS (Software as a Service) delivers software applications over the internet, on a subscription basis.

1. **Public, private, and hybrid cloud:**

• Public cloud: Services are delivered over the public internet and are available to anyone who wants to purchase them.

• Private cloud: Services and infrastructure are maintained on a private network, usually within a company's firewall.

• Hybrid cloud: A combination of public and private clouds, allowing data and applications to be shared between them.

1. **Connectivity between VMs in different subscriptions:**

• To connect VMs in different subscriptions, you can use Virtual Network Peering or VPN Gateway.

1. **Why use Application Gateway as an entry point:**

• Application Gateway provides application-level routing and load balancing services that let you build a scalable and highly available web front end in Azure.

1. **Load Balancers and LB rules:**

• Load Balancers distribute incoming network traffic across multiple VM instances. Load Balancer rules define how the traffic is distributed.

1. **/16 and /28, which will have more usable IPs:**

• /16 will have more usable IPs.

1. **Address prefixes:**

• Address prefixes are the range of IP addresses available to your Azure virtual network.

1. **Access control (IAM) in Azure:**

• IAM (Identity and Access Management) in Azure allows you to manage access to Azure resources.

1. **Different types of Storage in Azure:**

• Azure offers Blob Storage, File Storage, Queue Storage, Table Storage, Disk Storage, and Premium Storage.

1. **Managed identity, service connection, and principal:**

• Managed identity allows you to authenticate to services that support Azure AD authentication without needing to insert credentials into your code.

• Service connection is a connection to an external service endpoint that's stored in Azure DevOps.

• Principal refers to an identity that is used to define access policy and to grant access to resources.

1. **Methods to create VM:**

• You can create a VM in Azure using the Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, or Azure SDKs.

1. **Controlling traffic on VM:**

• Traffic to and from a VM can be controlled using Network Security Groups (NSGs) and Azure Firewall.

1. **Types of different storages in Azure:**

• Blob Storage, File Storage, Queue Storage, Table Storage, Disk Storage, and Premium Storage.

1. **Increasing disk size after deploying VM:**

• Yes, it is possible to increase the disk size after deploying a VM. You can do this by resizing the disk in the Azure portal or using Azure CLI.

1. **Logging into VM without sharing username and password:**

• You can use SSH keys or Azure Active Directory for authentication to log in to a VM without sharing a username and password.

1. **Connecting On-Prem VM and Virtual VM:**

• You can establish a VPN connection between your on-premises network and Azure Virtual Network.

1. **Sending script files to a VM:**

• You can use tools like Azure Storage Explorer, Azure PowerShell, or Azure CLI to copy files to a VM.

1. **Fault domain and Update domain:**

• Fault domain is a group of hardware in the datacenter that share a common power source and network switch.

• Update domain is a group of VMs that can be rebooted at the same time for maintenance and updates.

1. **Bastion:**

• Azure Bastion is a fully managed PaaS service that provides secure and seamless RDP and SSH access to your virtual machines directly through the Azure Portal.

1. **Replacing Bastion with a firewall:**

• No, Bastion cannot be replaced with a firewall. They serve different purposes. Bastion provides secure RDP/SSH access to VMs, while a firewall controls network traffic.

1. **NGS and ASG:**

• NSG (Network Security Group) is a firewall that filters network traffic to and from Azure resources.

• ASG (Application Security Group) is a collection of VMs that allows you to apply network security policies to all VMs in the group.

1. **Use of virtual network in Azure:**

• Virtual Network in Azure allows you to create private networks in the cloud, enabling Azure resources to communicate with each other, the internet, and on-premises networks.

1. **Resources I've worked on in Azure:**

• Virtual Machines, Virtual Networks, Azure Storage (Blob, File, Table, Queue), Azure Active Directory, Azure DevOps, Azure Functions, Azure App Service, Azure SQL Database, Azure Cognitive Services, Azure Monitor, Azure Kubernetes Service, Azure Logic Apps, etc.

1. **Ensuring high availability for frontend and backend applications:**

• For the frontend application, you can use Azure App Service with multiple instances and Azure Traffic Manager for load balancing. For the backend, you can use Azure SQL Database with Geo-replication for high availability.

1. **Applying security patches to a VM:**

• You can apply security patches to a VM by enabling Automatic OS patching in Azure Update Management. Alternatively, you can manually install patches using Windows Update or Linux package manager.