**Azure**

* Azure provides a variety of scalable, on-demand computing resources, among them being virtual machines (VMs). A virtual machine is usually your best option if you require greater control over the computing environment than the other options provide.

**Network Security Groups**

* In an Azure virtual network, you can filter network traffic between Azure services by using an Azure network security group. Security rules that permit or prohibit network traffic entering or leaving certain kinds of Azure resources are contained in a network security group. You can set the protocol, port, and source and destination for each rule.

**Methods of connection**

* Remote desktop protocol, or RDP  
  RDP is widely used for Windows virtual machines connections.  
  Functionality: RDP enables remote user interface (GUI) interaction with Windows virtual machines (VMs), offering a desktop experience that is identical to being physically present on the system.
* Secure Shell Protocol, or SSH  
  Although it can connect to Windows VMs if SSH is enabled, SSH is mostly used to connect to Linux virtual machines.  
  Functionality: SSH offers a command-line interface for connecting to a virtual machine remotely. It is a safe method for carrying out system upgrades, configuration, and software installation.  
  SSH is the command. For VM connection, use the -i command.

**SCP – secure copy**

This command is used to move files from your workstation up to an Azure VM, or from an Azure VM down to your workstation.

* **Upload a file to the VM:** scp file azureuser@azurehost:directory/targetfile
* **Download a file from the VM:** scp azureuser@azurehost:directory/file targetfile

**Commands for configuring VM to host a website**

First connect to your VM

1. **Update the system packages**: sudo apt update
2. **Install Nginx**: sudo apt install nginx -y
3. **Start and Enable Nginx**:
   1. sudo systemctl start nginx
   2. sudo systemctl enable nginx
4. **From your workstation upload files to VM:** scp -r /path/to/your/website/files <your-username>@<your-vm-ip>:/var/www/html/
5. **Set Permissions**:
   1. sudo chown -R www-data:www-data /var/www/html/
   2. sudo chmod -R 755 /var/www/html/
6. **Configure Nginx Virtual Host**: sudo nano /etc/nginx/sites-available/default
7. Modify the file to look something like this:

server {

  listen 80;

  server\_name <your-domain-or-vm-ip>;

  root /var/www/html;

  index index.html;

  location / {

      try\_files $uri $uri/ =404;

  }

}

1. **Restart Nginx**: sudo systemctl restart nginx

**Configure inbound and outbound rules**

We make use Network security group to create a rule that only allows access to specified IP

*Create/Identify the NSG:*

* Go to your Azure Portal.
* Find the Network Security Group (NSG) associated with your VM's network interface or subnet.

*Restrict Inbound Access by IP Address:*

* In the NSG settings, navigate to Inbound security rules.
* Remove any rule that allows open access, such as Allow All on port 22 (for SSH) or 3389 (for RDP).
* Add a new rule:
  + Source: Specify IP Addresses.
  + Source IP address range: Enter your public IP address.
  + Destination: The IP address of your VM or leave it as "Any" if you only have one VM.
  + Port: Specify the port used for VM access (22 for SSH, 3389 for RDP, etc.).
  + Action: Allow.

This will allow only your IP address to access the VM.

**Azure VM custom data:**

Azure VM Custom Data allows you to pass user-defined data into the VM during its creation. It is typically used to initialize the VM with specific configurations, install software, or run scripts as part of the VM's provisioning process. Custom data is usually a base64-encoded string containing configuration scripts or text, which the VM processes during its first boot.

Example cloud-init.yml script:

*#cloud-config*

*package\_update: true*

*package\_upgrade: true*

*packages:*

*- nginx*

*runcmd:*

*- systemctl enable nginx*

*- systemctl start ngin*

**Commands used by me:**

**>> ssh -I azureuser@<public-ip> vineet-ubuntu\_key.pem**

**>> sudo apt update**

**>> sudo apt install nginx**

**>> scp -i vineet-ubuntu\_key.pem -r C:\Users\vineet.sawant\Downloads\energym-html** [**azureuser@@<public-ip>:/var/www/html**](mailto:azureuser@52.169.211.244:/var/www/html)

**>> sudo mv /tmp/energym-html /var/www/html**

**>> ls /var/www/html/energym-html**

**>> sudo chown -R www-data:www-data /var/www/html/**

**>> sudo chmod -R 755 /var/www/html/**

**>> sudo systemctl reload nginx**