

# Assignment Practical

*by* Gareth Williams

---

**Submission date:** 04-Jan-2023 02:32PM (UTC+0000)

**Submission ID:** 193594305

**File name:** 17790\_Gareth\_Williams\_Assignment\_Practical\_460444\_2144883969.docx (6.1M)

**Word count:** 5478

**Character count:** 29696

# Cloud Computing Architecture

## Assignment 2: Practical

Gareth Williams 1910285  
9<sup>th</sup> January 2023

## Table of Contents

|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| <b>1. Introduction .....</b>                                            | <b>4</b>  |
| <b>2. Virtual Machine Resources.....</b>                                | <b>4</b>  |
| 2.1 Disk Usage .....                                                    | 4         |
| 2.2 Disk Hardware .....                                                 | 5         |
| 2.3 Memory & CPU .....                                                  | 5         |
| 2.4 NIC (Network Interface).....                                        | 6         |
| 2.5 Location .....                                                      | 6         |
| 2.6 Azure VM Sizes .....                                                | 6         |
| <b>3. Creating a Virtual Machine .....</b>                              | <b>7</b>  |
| 3.1 VM Images .....                                                     | 7         |
| 3.1.1 Finding an Image.....                                             | 8         |
| 3.2 Creating a VM – az vm create .....                                  | 9         |
| 3.3 Verifying Virtual Machine Creation .....                            | 10        |
| 3.4 Default Network Settings .....                                      | 11        |
| <b>4. Virtual Machine Maintenance.....</b>                              | <b>12</b> |
| 4.1 Maintenance Access – Bastion & Jump-box .....                       | 12        |
| 4.2 Shutdown .....                                                      | 12        |
| 4.3 Changing Component Specification.....                               | 13        |
| <b>5. Networking &amp; Network Security Groups .....</b>                | <b>14</b> |
| 5.1 Virtual Network (VNet).....                                         | 14        |
| 5.2 Subnet.....                                                         | 15        |
| 5.3 Network Interface (NIC).....                                        | 15        |
| 5.4 Network Security Groups.....                                        | 16        |
| <b>6. Additional Exercise – Simple 2 Tier IaaS Implementation .....</b> | <b>19</b> |
| 6.1 Deployment Design .....                                             | 19        |
| 6.2 Step 1. Create vNet and Subnets.....                                | 20        |
| 6.3 Step 2. Create Jump Box VM with Public IP address .....             | 20        |
| 6.4 Step 3. Create Network Interfaces for Application Servers .....     | 21        |
| 6.5 Step 4. Create Web Server VM (nginx) .....                          | 22        |
| 6.6 Step 5. Create Database VM .....                                    | 23        |
| 6.7 Step 5. Create NSGs and Rules Using subnets.....                    | 25        |
| 6.8 Testing Implementation .....                                        | 26        |

|             |                                           |           |
|-------------|-------------------------------------------|-----------|
| 6.8.1       | HTTP Connectivity.....                    | 26        |
| 6.8.2       | SSH to App server Public IP address ..... | 27        |
| 6.8.3       | Connect From nginxVM to PostgreSQL.....   | 27        |
| <b>7.</b>   | <b>Works Cited .....</b>                  | <b>28</b> |
| <b>8.</b>   | <b>Appendix A – Full Script.....</b>      | <b>29</b> |
|             |                                           |           |
| Figure 1 -  | Azure Disk Type Comparison [2].....       | 5         |
| Figure 2 -  | Azure VM Sizes.....                       | 6         |
| Figure 3 -  | Azure Resource Manager.....               | 7         |
| Figure 4 -  | Market Place Attributes.....              | 8         |
| Figure 5 -  | VM Image List .....                       | 9         |
| Figure 6 -  | VM image list parameters.....             | 9         |
| Figure 7 -  | VM Create .....                           | 10        |
| Figure 8 -  | Linux Commands.....                       | 11        |
| Figure 9 -  | Shutting Down Operating System.....       | 12        |
| Figure 10 - | Stopped State .....                       | 13        |
| Figure 11 - | Powerstate.....                           | 13        |
| Figure 12 - | VM Resize.....                            | 13        |
| Figure 13 - | az network vnet create .....              | 15        |
| Figure 14 - | Subnet Example .....                      | 15        |
| Figure 15 - | Subnet List.....                          | 15        |
| Figure 16 - | Simple Network Topology.....              | 15        |
| Figure 17 - | NSGs.....                                 | 17        |
| Figure 18 - | NSG Rules Example .....                   | 17        |
| Figure 19 - | Azure Portal NSG Rules View .....         | 18        |
| Figure 20 - | Deployment Design.....                    | 19        |

## 1. Introduction

This report explains the resources associated with an Azure Virtual Machine and a demonstrates creating a simple virtual machine. The examples given are based on Microsoft Azure cloud, however there are other suppliers such as Amazon Web Services (AWS), Google, IBM and so on. Each cloud service provider will work in a similar fashion.

The second part of this report discusses the networking elements within a cloud environment and the use of network security groups.

The third part of the report provides an example of how a simple web server service could be established within Azure using Infrastructure-as-a-Service (IaaS).

A supporting Video for this report can be found at the following Youtube link:

<https://youtu.be/oji9kRLHmFw>

## 2. Virtual Machine Resources

In the book Cloud Computing: Concepts, Technology, & Architecture, T. Erl et al state:

“A virtual server is a form of virtualization software that emulates a physical server. Virtual servers are used by cloud providers to share the same physical server with multiple cloud consumers by providing cloud consumers with individual virtual server instances.” [1]

Cloud service providers charge for storage and compute, therefore the cost of running a virtual machine depends on the amount of processing power (CPU, memory) and storage a VM is configured to use.

As a minimum, the main components that need to be configured are virtual machine Memory, CPU, network and operating system disk.

### 2.1 Disk Usage

There are three disk usage categories, Operating System Disk, Resource Disk and Data Disk.

As the name suggests, the Operating System Disk is where the guest OS is installed in a single VHD file which is stored in Azure Storage (and is therefore charged), this will be permanent storage and is essentially the “boot disk”. Services and applications can also be installed on this disk. The Azure default size for OS disks is approx. 30GB, although the specification allows up to 1000 Gigabytes (1 Terabyte).

The Microsoft Azure Learn website states:

“Cost is based on the capacity of the provisioned disk. IOPS and throughput (that is, data transfer rate) also depend on disk size, so when you provision a disk, consider all three factors (capacity, IOPS, and throughput).” [2]

*Data Disks* are for permanent storage of data and can be attached and mounted to the vm image. The disks are separate *resources* from the VM and so the costs, specification and configuration are separate. A VM does not need a data storage disk to run.

A *Resource Disk* is fast temporary storage and is normally SSD. This is used as temporary space by the OS or applications to store working or process files. Anything stored on the *resource* disk will be lost on reboot.

## 2.2 Disk Hardware

Azure offers both solid state and standard hard disk drives. *Figure 1* shows a table provided by Microsoft Azure [2] showing a comparison of disk type. Azure offers a choice of Hard Disk Drives (lower costs), or Solid State Drive, with the solid state drive having a number of choices regarding capacity and throughput.

| Disk type comparison                                                                              |                                                                                                                                |                                                                                                                   |                                                |                                                                |                                         |
|---------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|------------------------------------------------|----------------------------------------------------------------|-----------------------------------------|
| The following table provides a comparison of the five disk types to help you decide which to use. |                                                                                                                                |                                                                                                                   |                                                |                                                                |                                         |
|                                                                                                   | Ultra disk                                                                                                                     | Premium SSD v2                                                                                                    | Premium SSD                                    | Standard SSD                                                   | Standard HDD                            |
| Disk type                                                                                         | SSD                                                                                                                            | SSD                                                                                                               | SSD                                            | SSD                                                            | HDD                                     |
| Scenario                                                                                          | IO-intensive workloads such as SAP HANA, top tier databases (for example, SQL, Oracle), and other transaction-heavy workloads. | Production and performance-sensitive workloads that consistently require low latency and high IOPS and throughput | Production and performance sensitive workloads | Web servers, lightly used enterprise applications and dev/test | Backup, non-critical, infrequent access |
| Max disk size                                                                                     | 65,536 gibibyte (GiB)                                                                                                          | 65,536 GiB                                                                                                        | 32,767 GiB                                     | 32,767 GiB                                                     | 32,767 GiB                              |
| Max throughput                                                                                    | 4,000 MB/s                                                                                                                     | 1,200 MB/s                                                                                                        | 900 MB/s                                       | 750 MB/s                                                       | 500 MB/s                                |
| Max IOPS                                                                                          | 160,000                                                                                                                        | 80,000                                                                                                            | 20,000                                         | 6,000                                                          | 2,000                                   |
| Usable as OS Disk?                                                                                | No                                                                                                                             | No                                                                                                                | Yes                                            | Yes                                                            | Yes                                     |

Figure 1 - Azure Disk Type Comparison [2]

## 2.3 Memory & CPU

In the Article, *Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey*, Manvi and Shyam state:

“The increased number of cores in cloud servers combined with the rapid adoption of virtualization technologies also creates huge demand for memory.” [3]

Memory size will depend on OS and the number and type of processes the VM will serve.

## 2.4 NIC (Network Interface)

The Network Interface (NIC), must be assigned to a VM. When creating a VM if no network details are specified, Azure will try to create a Virtual Network (if one doesn't exist), and single NIC using default values. As a minimum a single public and single private IP address will be assigned to the NIC. The NIC will present itself as a Network Card to the VM Operating System.

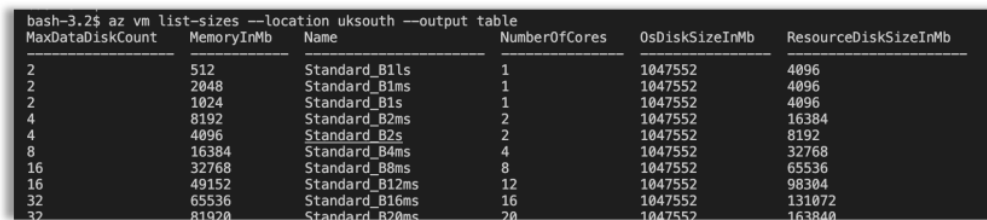
## 2.5 Location

An important design consideration is where a virtual machine is created. Cloud service providers have many datacentres both in countries around the world and then have zones (datacentres), within a country. As well as making sense to host services near main user base, a combination of these locations can be used when designing in business continuity or resilience. In addition, countries may have Data Protection Laws that prohibit the storing or processing of data outside of their jurisdiction.

Another consideration is that not all datacentres are the same and that some will have limitations on hardware or provide specialist features. This can be seen when attempting to install from images i.e., not all images are available in all datacentres.

## 2.6 Azure VM Sizes

The following table in Figure 2 shows sample output from the `az vm list-sizes` command. The table shows the key elements of Memory, CPU cores, OS and Resource Disk size that are available in the particular *zone*.



| bash-3.2\$ az vm list-sizes --location uksouth --output table |            |                |               |                |                      |
|---------------------------------------------------------------|------------|----------------|---------------|----------------|----------------------|
| MaxDataDiskCount                                              | MemoryInMb | Name           | NumberOfCores | OsDiskSizeInMb | ResourceDiskSizeInMb |
| 2                                                             | 512        | Standard_B1ls  | 1             | 1047552        | 4096                 |
| 2                                                             | 2048       | Standard_B1ms  | 1             | 1047552        | 4096                 |
| 2                                                             | 1024       | Standard_B1s   | 1             | 1047552        | 4096                 |
| 4                                                             | 8192       | Standard_B2ms  | 2             | 1047552        | 16384                |
| 4                                                             | 4096       | Standard_B2s   | 2             | 1047552        | 8192                 |
| 8                                                             | 16384      | Standard_B4ms  | 4             | 1047552        | 32768                |
| 16                                                            | 32768      | Standard_B8ms  | 8             | 1047552        | 65536                |
| 16                                                            | 49152      | Standard_B12ms | 12            | 1047552        | 98304                |
| 32                                                            | 65536      | Standard_B16ms | 16            | 1047552        | 131072               |
| 32                                                            | 81920      | Standard_B20ms | 20            | 1047552        | 163840               |

Figure 2 - Azure VM Sizes

In *Figure 2*, the Memory and CPU cores columns are self-explanatory. Note that the `OsDiskSizeInMB` denotes the permanent *managed* storage for the OS, Azure allows up to 1 Terabyte - this space can also be used to install applications.

The **Resource Disk** is essentially temporary fast storage of SSD type – this disk tends to hold OS page or swap files and can be used by applications as fast storage of temporary or working files. Any data saved to this disk will be lost on reboot of the machine.

**MaxDataDiskCount** – is the number of permanent storage devices that can be attached e.g., cloud storage that can be attached as devices then mounted as disks.

The **Name** column gives us the `--size` parameter value of the `az vm create` command.

### 3. Creating a Virtual Machine

Azure resources such as VM machines are created and maintained using cloud web services that provide secure access to the Azure Resource Manager (ARM), for convenience and flexibility these services are wrapped with a number of utilities such as REST APIs and Software Development Kits (SDKs). PowerShell and Azure CLI also encapsulate these services and allows for resource manipulation from scripting tools. In addition, the Azure Portal is a web application that provides a graphical interface.

The diagram in *Figure 3* provided by Microsoft Learn [4], shows how these tools are connected to the ARM control plane.

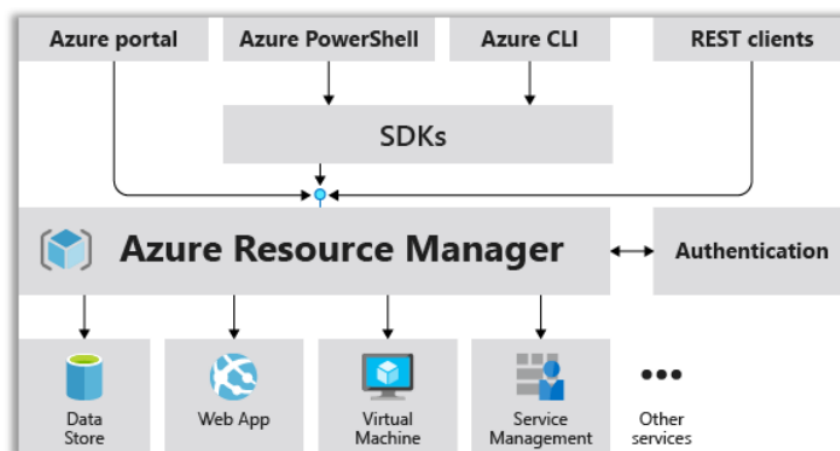


Figure 3 - Azure Resource Manager

In day-to-day production a mix of these tools maybe used. In this report the Azure CLI will be used as the main tooling.

#### 3.1 VM Images

In her blog “VM Image”, Christine Avaneessians describes a virtual machine image as “a VM Image is a collection of metadata and pointers to a set of VHDs (one VHD per disk) stored as page blobs in Azure Storage”. [5]

The VM image is essentially a used as “a ‘model’ to quickly stamp out similar virtual machines, such as scaling out a front-end to your application in production or spinning up and tearing down similar development and test environments quickly”. [5]

Microsoft provides a public Market place of ready to use VM Images. As with other resources, the Market place listings can be searched using the Azure Portal or command lines tools.

The image can be a simple empty operating system or an operating with software preinstalled e.g., a PostgreSQL database engine.

Some of the benefits of using Images are

- The suppliers of images have done the work of ensuring the OS and installed software are optimized, tested, and patched saving a lot of time when provisioning machines
- Security hardened images are available such as CIS Hardened Images [6]
- Confidence that the image will work out-of-the-box
- Only fine tuning and configuration is required

Care must take when choosing an image as some come with a licensing element and may incur additional charges or restrict use as “for personal use only” or “try before you buy”.

As well as the public images, cloud service providers will allow customers to create their own VM images with specific OS and application configurations and store in a private “gallery”. These custom images can then be used for quickly scaling out services.

### 3.1.1 Finding an Image

Figure 4 shows the Azure Marketplace image attributes.

A Marketplace image in Azure has the following attributes:

- **Publisher:** The organization that created the image. Examples: Canonical, MicrosoftWindowsServer
- **Offer:** The name of a group of related images created by a publisher. Examples: UbuntuServer, WindowsServer
- **SKU:** An instance of an offer, such as a major release of a distribution. Examples: 18.04-LTS, 2019-Datacenter
- **Version:** The version number of an image SKU.

*Figure 4 - Market Place Attributes*

Figure 5 shows the output of the `az vm image list`. This is essentially a list of the most commonly used public images. A full list is available with the `--all` parameter.

```
AzureCLI$ az vm image list --output table
You are viewing an offline list of images. use --all to retrieve an up-to-date list
```

| Architecture                                         | Offer                        | Publisher              | Skus                               | Version   | Urn                        |
|------------------------------------------------------|------------------------------|------------------------|------------------------------------|-----------|----------------------------|
| x64                                                  | CentOS                       | OpenLogic              | CentOS                             | 7.5       | OpenLogic:CentOS:7.5:lates |
| t                                                    | debian-10                    | Debian                 | 10                                 | latest    | Debian:debian-10:10:latest |
| x64                                                  | flatcar-container-linux-free | kinvolk                | Flatcar                            | stable    | kinvolk:flatcar-container- |
| linux-free:stable:latest                             |                              |                        |                                    | latest    |                            |
| x64                                                  | opensuse-leap-15-3           | SUSE                   | Flatcar                            | gen2      | SUSE:opensuse-leap-15-3:ge |
| n2:latest                                            |                              |                        |                                    | latest    |                            |
| x64                                                  | RHEL                         | RedHat                 | openSUSE-Leap                      | 7-LVM     | RedHat:RHEL:7-LVM:latest   |
| x64                                                  | sles-15-sp3                  | SUSE                   | RHEL                               | gen2      | SUSE:sles-15-sp3:gen2:late |
| st                                                   |                              |                        |                                    | latest    |                            |
| x64                                                  | UbuntuServer                 | Canonical              | SLES                               | 18.04-LTS | Canonical:UbuntuServer:18. |
| 04-LTS:latest                                        |                              |                        |                                    | latest    |                            |
| x64                                                  | WindowsServer                | MicrosoftWindowsServer | 2022-Datacenter                    | latest    | MicrosoftWindowsServer:Win |
| dowsServer:2022-Datacenter:latest                    |                              |                        |                                    | latest    |                            |
| x64                                                  | WindowsServer                | MicrosoftWindowsServer | 2022-datacenter-azure-edition-core | latest    | MicrosoftWindowsServer:Win |
| dowsServer:2022-datacenter-azure-edition-core:latest |                              |                        |                                    | latest    |                            |
| x64                                                  | WindowsServer                | MicrosoftWindowsServer | 2019-Datacenter                    | latest    | MicrosoftWindowsServer:Win |
| dowsServer:2019-Datacenter:latest                    |                              |                        |                                    | latest    |                            |
| x64                                                  | WindowsServer                | MicrosoftWindowsServer | 2016-Datacenter                    | latest    | MicrosoftWindowsServer:Win |
| dowsServer:2016-Datacenter:latest                    |                              |                        |                                    | latest    |                            |
| x64                                                  | WindowsServer                | MicrosoftWindowsServer | 2012-R2-Datacenter                 | latest    | MicrosoftWindowsServer:Win |
| dowsServer:2012-R2-Datacenter:latest                 |                              |                        |                                    | latest    |                            |
| x64                                                  | WindowsServer                | MicrosoftWindowsServer | 2012-Datacenter                    | latest    | MicrosoftWindowsServer:Win |
| dowsServer:2012-Datacenter:latest                    |                              |                        |                                    | latest    |                            |
| x64                                                  | WindowsServer                | MicrosoftWindowsServer | 2008-R2-SP1                        | latest    | MicrosoftWindowsServer:Win |
| dowsServer:2008-R2-SP1:latest                        |                              |                        |                                    | latest    |                            |

Figure 5 - VM Image List

The az vm image list command can take several search parameters as shown in Figure 6.

```
AzureCLI$ az vm image list --location ukwest --publisher Canonical --offer UbuntuServer --sku 18.04-LTS --all --output table
```

| Architecture | Offer        | Publisher | Skus      | Urn                                              | Version         |
|--------------|--------------|-----------|-----------|--------------------------------------------------|-----------------|
| x64          | UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201804262 | 18.04.201804262 |
| x64          | UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201805170 | 18.04.201805170 |
| x64          | UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201805220 | 18.04.201805220 |
| x64          | UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201806130 | 18.04.201806130 |
| x64          | UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201806170 | 18.04.201806170 |
| x64          | UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201807240 | 18.04.201807240 |
| x64          | UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201808060 | 18.04.201808060 |
| x64          | UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201808080 | 18.04.201808080 |
| x64          | UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201808140 | 18.04.201808140 |
| x64          | UbuntuServer | Canonical | 18.04-LTS | Canonical:UbuntuServer:18.04-LTS:18.04.201809210 | 18.04.201809210 |

Figure 6 - VM image list parameters

This list gives shows us the Urn (Unique Reference Name), of a VM Images which will allow us to create a VM from the image that has a very specific version of Ubuntu Server that maybe required for compatibility or certification reasons.

If only the latest certified image is required, then we can use the SKUALias as the value of the vm create *name* parameter e.g., RHEL for RedHat linux.

### 3.2 Creating a VM – az vm create

By putting together the *size* and the vm *image* parameters we can create a virtual machine with the Azure CLI command az vm create:

```
AzureCLI$ az vm create --resource-group myvm-resource-gp --name myVM --size Standard_B1ls
--image UbuntuLTS --admin-username azureuser --generate-ssh-keys
```

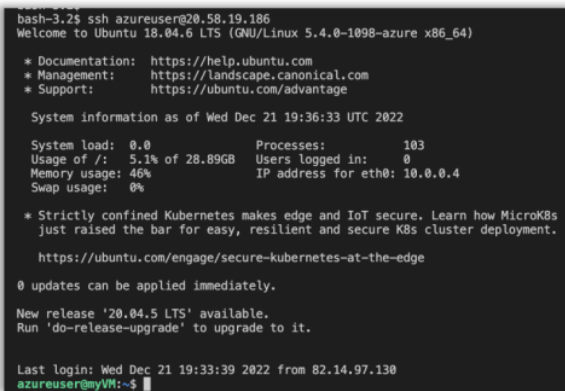
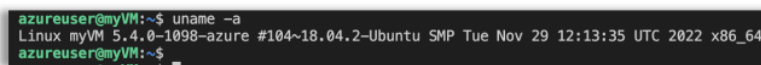
```
{
  "fqdns": "",
  "id": "/subscriptions/84ffd6a3-07a3-41e4-9797-fa31b78319c3/resourceGroups/myvm-resource-
gp/providers/Microsoft.Compute/virtualMachines/myVM",
  "location": "uksouth",
  "macAddress": "60-45-BD-D0-EB-43",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "20.254.118.10",
  "resourceGroup": "myvm-resource-gp",
  "zones": ""
}
AzureCLI$
```

Figure 7 - VM Create

The output from the create command shows the public and private IP address. The *generate-ssh-keys* parameter was provided, which disables the default password and produces keys to allow access to the virtual machine using SSH (Secure Shell) with the public IP address – the private IP address is only accessible from within the *virtual network*.

### 3.3 Verifying Virtual Machine Creation

Now the server has been created we can simply SSH login using this public IP address. The following table shows some unix commands to show how the components match the specification of the *az vm create* statement.

| Command                         | Output                                                                               |
|---------------------------------|--------------------------------------------------------------------------------------|
| Ssh<br>azureuser@[pu<br>blicip] |  |
| uname -a                        |  |

| lscpu                                                                                                                                                                                                                                                                                                                                                          | <pre>azureuser@myVM:~\$ lscpu Architecture:          x86_64 CPU op-mode(s):        32-bit, 64-bit Byte Order:             Little Endian CPU(s):                 1 On-line CPU(s) list:   0 Thread(s) per core:    1 Core(s) per socket:    1 Socket(s):              1 NUMA node(s):          1 Vendor ID:              GenuineIntel CPU family:              6 Model:                  85 Model name:             Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz Stepping:               7 CPU MHz:                2593.908 BogoMIPS:               5187.81 Hypervisor vendor:      Microsoft Virtualization type:    full L1d cache:              32K L1i cache:              32K L2 cache:               1024K L3 cache:               36608K</pre>                                                                                                                                                                                                                                                                               |            |           |        |                |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|-----------|--------|----------------|-----------|------------|-----------|--------|------|--------|-----|------|-------|-------|-------|-------|----|------|-----------|----------|---------|----------|----|---|-------|--------|---|--------|----|----------|-------|------|---|------|----|-----------|-------|--------|---|--------|----|----------------|------------|--------|------|--------|----|-----------|-----------|---------|----|---------|----|------|-------|-------|---|-------|----|----------------|
| The following screen grab from Azure shows the matching CPU type 8272CL.                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |           |        |                |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| <p>provided. B-series run on the 3rd Generation Intel® Xeon® Platinum 8370C (Ice Lake), the Intel® Xeon® Platinum 8272CL (Cascade Lake), the Intel® Xeon® 8171M 2.1 GHz (Skylake), the Intel® Xeon® E5-2673 v4 2.3 GHz (Broadwell), or the Intel® Xeon® E5-2673 v3 2.4 GHz (Haswell) processors. B-series VMs are ideal for workloads that do not need the</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |            |           |        |                |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| free -h --si<br>0.5Gb                                                                                                                                                                                                                                                                                                                                          | <pre>azureuser@myVM:~\$ free -h --si</pre> <table><tr><th></th><th>total</th><th>used</th><th>free</th><th>shared</th><th>buff/cache</th><th>available</th></tr><tr><td>Mem:</td><td>419M</td><td>144M</td><td>27M</td><td>712K</td><td>247M</td><td>262M</td></tr><tr><td>Swap:</td><td>0B</td><td>0B</td><td>0B</td><td></td><td></td><td></td></tr></table>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |            | total     | used   | free           | shared    | buff/cache | available | Mem:   | 419M | 144M   | 27M | 712K | 247M  | 262M  | Swap: | 0B    | 0B | 0B   |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
|                                                                                                                                                                                                                                                                                                                                                                | total                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | used       | free      | shared | buff/cache     | available |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| Mem:                                                                                                                                                                                                                                                                                                                                                           | 419M                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 144M       | 27M       | 712K   | 247M           | 262M      |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| Swap:                                                                                                                                                                                                                                                                                                                                                          | 0B                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | 0B         | 0B        |        |                |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| df -k                                                                                                                                                                                                                                                                                                                                                          | <pre>azureuser@myVM:~\$ df -k</pre> <table><tr><th>Filesystem</th><th>1K-blocks</th><th>Used</th><th>Available</th><th>Use%</th><th>Mounted on</th></tr><tr><td>udev</td><td>190972</td><td>0</td><td>190972</td><td>0%</td><td>/dev</td></tr><tr><td>tmpfs</td><td>41948</td><td>684</td><td>41264</td><td>2%</td><td>/run</td></tr><tr><td>/dev/sda1</td><td>30298176</td><td>1552832</td><td>28728960</td><td>6%</td><td>/</td></tr><tr><td>tmpfs</td><td>209740</td><td>0</td><td>209740</td><td>0%</td><td>/dev/shm</td></tr><tr><td>tmpfs</td><td>5120</td><td>0</td><td>5120</td><td>0%</td><td>/run/lock</td></tr><tr><td>tmpfs</td><td>209740</td><td>0</td><td>209740</td><td>0%</td><td>/sys/fs/cgroup</td></tr><tr><td>/dev/sda15</td><td>106858</td><td>4477</td><td>102382</td><td>5%</td><td>/boot/efi</td></tr><tr><td>/dev/sdb1</td><td>4044512</td><td>28</td><td>3818488</td><td>1%</td><td>/mnt</td></tr><tr><td>tmpfs</td><td>41948</td><td>0</td><td>41948</td><td>0%</td><td>/run/user/1000</td></tr></table> | Filesystem | 1K-blocks | Used   | Available      | Use%      | Mounted on | udev      | 190972 | 0    | 190972 | 0%  | /dev | tmpfs | 41948 | 684   | 41264 | 2% | /run | /dev/sda1 | 30298176 | 1552832 | 28728960 | 6% | / | tmpfs | 209740 | 0 | 209740 | 0% | /dev/shm | tmpfs | 5120 | 0 | 5120 | 0% | /run/lock | tmpfs | 209740 | 0 | 209740 | 0% | /sys/fs/cgroup | /dev/sda15 | 106858 | 4477 | 102382 | 5% | /boot/efi | /dev/sdb1 | 4044512 | 28 | 3818488 | 1% | /mnt | tmpfs | 41948 | 0 | 41948 | 0% | /run/user/1000 |
| Filesystem                                                                                                                                                                                                                                                                                                                                                     | 1K-blocks                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Used       | Available | Use%   | Mounted on     |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| udev                                                                                                                                                                                                                                                                                                                                                           | 190972                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 0          | 190972    | 0%     | /dev           |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| tmpfs                                                                                                                                                                                                                                                                                                                                                          | 41948                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 684        | 41264     | 2%     | /run           |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| /dev/sda1                                                                                                                                                                                                                                                                                                                                                      | 30298176                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | 1552832    | 28728960  | 6%     | /              |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| tmpfs                                                                                                                                                                                                                                                                                                                                                          | 209740                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 0          | 209740    | 0%     | /dev/shm       |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| tmpfs                                                                                                                                                                                                                                                                                                                                                          | 5120                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 0          | 5120      | 0%     | /run/lock      |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| tmpfs                                                                                                                                                                                                                                                                                                                                                          | 209740                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 0          | 209740    | 0%     | /sys/fs/cgroup |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| /dev/sda15                                                                                                                                                                                                                                                                                                                                                     | 106858                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | 4477       | 102382    | 5%     | /boot/efi      |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| /dev/sdb1                                                                                                                                                                                                                                                                                                                                                      | 4044512                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | 28         | 3818488   | 1%     | /mnt           |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| tmpfs                                                                                                                                                                                                                                                                                                                                                          | 41948                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 0          | 41948     | 0%     | /run/user/1000 |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| cat /etc/fstab                                                                                                                                                                                                                                                                                                                                                 | <pre>azureuser@myVM:~\$ cat /etc/fstab # CLOUD_IMG: This file was created/modified by the Cloud Image build process UUID=c88d12c3-41c9-4695-b552-e0f40acc7dfe / ext4 defaults,discard 0 1 UUID=9CD8-F43F /boot/efi vfat umask=0077 0 1 /dev/disk/cloud/azure_resource-part1 /mnt auto defaults,nofail,x-systemd.requires=clo</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |            |           |        |                |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |
| ifconfig                                                                                                                                                                                                                                                                                                                                                       | <pre>azureuser@myVM:~\$ ifconfig eth0: flags=4163&lt;UP,BROADCAST,RUNNING,MULTICAST&gt; mtu 1500 inet 10.0.0.4 netmask 255.255.255.0 broadcast 10.0.0.255 inet6 fe80::20d:3aff:fe0b:a99a prefixlen 64 scopeid 0x20&lt;link&gt; ether 00:0d:3a:0b:a9:9a txqueuelen 1000 (Ethernet) RX packets 313767 bytes 71809034 (71.8 MB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 386103 bytes 99532166 (99.5 MB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0</pre>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |            |           |        |                |           |            |           |        |      |        |     |      |       |       |       |       |    |      |           |          |         |          |    |   |       |        |   |        |    |          |       |      |   |      |    |           |       |        |   |        |    |                |            |        |      |        |    |           |           |         |    |         |    |      |       |       |   |       |    |                |

Figure 8 - Linux Commands

### 3.4 Default Network Settings

When creating a VM, if no network details are specified, Azure will create a default virtual network. The command `az network vnet list` shows the default network private address space.

```

bash-3.2$ az network vnet list
[
  {
    "addressSpace": {
      "addressPrefixes": [
        "10.0.0.0/16"
      ]
    },
    "bgpCommunities": null,
    "ddosProtectionPlan": null,
  }
]

```

| VNet     | Subnet     | SubnetAddr  |
|----------|------------|-------------|
| myVMVNET | myVMSubnet | 10.0.0.0/24 |

## 4. Virtual Machine Maintenance

Section 3 showed using SSH to connect. This service is provided automatically and is the only way to access the virtual machines operating system when first created.

### 4.1 Maintenance Access – Bastion & Jump-box

A Bastion server or “jumpbox” is essentially a single security hardened gateway into backend services. In the examples provided in this report, the jumpbox is just for SSH access to backend services. Security is based on keys which can either be manually maintained or automatically maintained by Azure.

### 4.2 Shutdown

As cloud providers charge for compute and RAM, it is essential to shut-down the virtual machine correctly. Simply stopping the operating system using “shutdown” from within the OS does not stop the vm resource and therefore will generate a charge. *Figure 9* and *Figure 10* demonstrate this.

```

azureuser@myVM:~$ sudo shutdown
Shutdown scheduled for Thu 2022-12-22 18:24:23 UTC, use 'shutdown -c' to cancel.
azureuser@myVM:~$
azureuser@myVM:~$ time
real    0m0.000s
user    0m0.000s
sys     0m0.000s
azureuser@myVM:~$ date
Thu Dec 22 18:24:01 UTC 2022
azureuser@myVM:~$ Connection to 20.108.8.47 closed by remote host.
Connection to 20.108.8.47 closed.

```

Figure 9 - Shutting Down Operating System

```
bash-3.2$ az vm list -d -o table
Name      ResourceGroup  PowerState  PublicIps      Fqdns      Location  Zones
-----
myVM      MYVM-RESOURCE-GP  VM stopped  20.108.8.47    uksouth
myVM1     MYVM-RESOURCE-GP  VM running  20.117.161.159 uksouth
```

Figure 10 - Stopped State

The azure command `az vm deallocate` – signals and waits for the VM operating system to shut down, then tells the control plane to release the CPU and RAM resources.

Figure 11 shows the vm *PowerState* before and after the running of the deallocate command

```
bash-3.2$ az vm list -d -o table
Name      ResourceGroup  PowerState  PublicIps      Fqdns      Location  Zones
-----
myVM      MYVM-RESOURCE-GP  VM running  20.108.8.47    uksouth
myVM1     MYVM-RESOURCE-GP  VM running  20.117.161.159 uksouth

bash-3.2$ az vm list -d -o table
Name      ResourceGroup  PowerState  PublicIps      Fqdns      Location  Zones
-----
myVM      MYVM-RESOURCE-GP  VM deallocated
myVM1     MYVM-RESOURCE-GP  VM running  20.117.161.159 uksouth
```

Figure 11 - Powerstate

Deallocate also releases any non-static public ip addresses. Note that charges will still be incurred for the storage for the OS disk!

#### 4.3 Changing Component Specification

Commonly known as *vertical scaling*, as with physical hardware the virtual machines processing ability by upgrade/downgrade the VM machine spec by utilising the `vm resize` command. This uses the azure standard specs parameter to set the CPU, Memory and Disk size. T. Erl, R. Puttini, and Z. Mahmood in the book *Cloud computing : concepts, technology, & architecture*, describe this scaling as:

“... the replacing of an IT resource with another that has a higher capacity is referred to as scaling up and the replacing an IT resource with another that has a lower capacity is considered scaling down.” [1]

In this example, the machine is resized from standard\_B1ls to Standard\_B1s to increase the VM *memory* to 1Gigabyte.

```
bash-3.2$ az vm resize -g myvm-resource-gp -n myVM --size Standard_B1s
```

Figure 12 - VM Resize

The change can be validated by logging in to virtual machine OS command line and running the *free* utility. The output confirms the memory total has increased. The

```
azureuser@myVM:~$ free -h --si
```

|       | total | used | free |
|-------|-------|------|------|
| Mem:  | 934M  | 145M | 560M |
| Swap: | 0B    | 0B   | 0B   |

The same `azure resize` command can be used to *scale down* the VM.

```
bash-3.2$ az vm resize -g myvm-resource-gp -n myVM --size Standard_B1ls
```

```
azureuser@myVM:~$ free -m --si
```

|       | total | used | free |
|-------|-------|------|------|
| Mem:  | 419   | 138  | 59   |
| Swap: | 0     | 0    | 0    |

In summary, the use of the virtual machine provides the flexibility to quickly scale the virtual machine in-line with changing requirements.

## 5. Networking & Network Security Groups

Microsoft Learn describes the networking features as:

“Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.” [7]

Not specifying networking details as part of the `vm image create` command will mean a new NIC is created with a private IP (internal to Azure), and an internet facing public IP address (if available). If no Virtual Network network exists, Azure will also create a default virtual subnet for the NIC to reside in.

### 5.1 Virtual Network (VNet)

The Azure VNet is a virtual network within a region that allows resources to communicate with each other. As with a physical network, a subscriptions VNet can be configured into subnets to suit business needs. VNets created in separate regions can be linked using *peering*.

Figure 13 shows example syntax for creating a network.

```
AzureCLI$ az network vnet create --name myVNet --resource-group myvm-resource-gp --subnet-name mySubnet --address-prefix 10.1.0.0/16 --subnet-prefix 10.1.1.0/24
```

Figure 13 - az network vnet create

## 5.2 Subnet

Subnets are defined using the `az network vnet create` command. *Figure 14* shows the create with the subnet address ranges, *Figure 15* shows the user of the list command to show a summary of Subnets within a resource group.

```
AzureCLI$ az network vnet create --name myVNet --resource-group myvm-resource-gp --subnet-name mySubnet --address-prefix 10.1.0.0/16 --subnet-prefix 10.1.1.0/24
```

Figure 14 - Subnet Example

```
AzureCLI$ az network vnet list --resource-group myvm-resource-gp --query "[{vNet:name,Subnet:subnets[0].name,SubnetAddr:subnets[0].addressPrefix}]" --output table
```

| VNet    | Subnet   | SubnetAddr  |
|---------|----------|-------------|
| myVNet  | mySubnet | 10.1.1.0/24 |
| myVNet2 | default  | 10.0.0.0/24 |

Figure 15 - Subnet List

## 5.3 Network Interface (NIC)

NICs are created inside a network subnet, then are assigned to virtual machines.

At least one NIC is assigned to a virtual machine (primary NIC). If required additional NICs can be added to a VM. From the VM operating system perspective each NIC will be presented as a network card and so VM operating system commands such as `ifconfig` will display the card details.

The sketch in *Figure 15* shows a simple multi-tier application. It demonstrates:

- A Virtual Machine can have more than one NIC, each NIC can be on different Subnets
- A NIC can have a private and public IP address (the VM OS is not aware of the public IP)

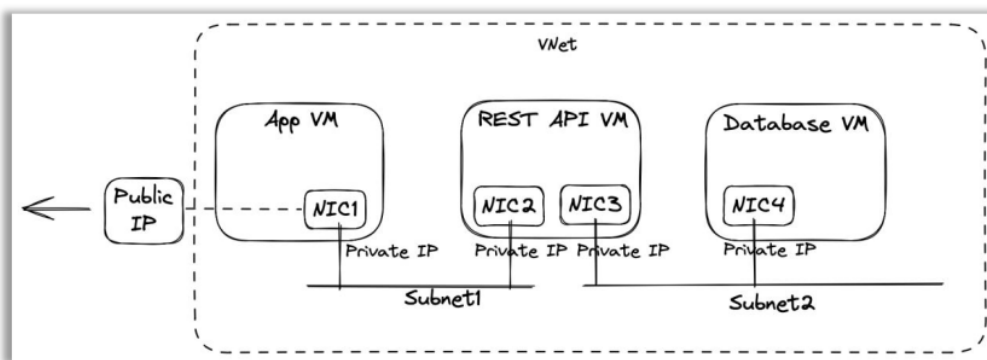


Figure 16 - Simple Network Topology

Although a static IP address can be assigned to a NIC, to maintain flexibility it is good practice to allow Azure DHCP to manage the private IP of NICs, resources can then use DNS to access servers by hostname.

```
AzureCLI$ az network nic list --resource-group myvm-resource-gp --query "[].(Name:name, MAC:macAddress, IP:ipConfigurations[0].privateIpAddress, IPub:ipConfigurations[0].publicIpAddress.id)" --output table
Name      IP      IPub
-----
myNic1    10.0.0.4 /subscriptions/84ffd6a3-07a3-41e4-9797-fa31b78319c3/resourceGroups/myvm-resource-gp/providers/Microsoft.Network/publicIPAddresses/myPublicIP
myNic2    10.0.0.5
myNic3    10.0.0.6
myNic4    10.0.0.7
```

As with physical networks and servers, which inbound and outbound ports are opened still need to be considered.

## 5.4 Network Security Groups

In the book *Zen of cloud*, H. Bai says of NSGs that:

“NSGs are your first line of defense. By designing your NSGs, you can block any unwanted traffic while ensuring accessibility to your services” [8]

Microsoft Learn provides an overview of the main NSG capabilities:

“You can use an Azure network security group to filter network traffic between Azure resources in an Azure virtual network. A network security group contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.” [7]

Opening a port on a public IP address will automatically create an NSG and a rule for the given port.

The following sketch in *Figure 17* shows how NSGs can be implemented for the same multi-tier application shown in *Figure 15*. The two NSG will separate the front-end server from the database server and only allow traffic for administration (SSH), and database access for the application backend (PostgreSQL port).

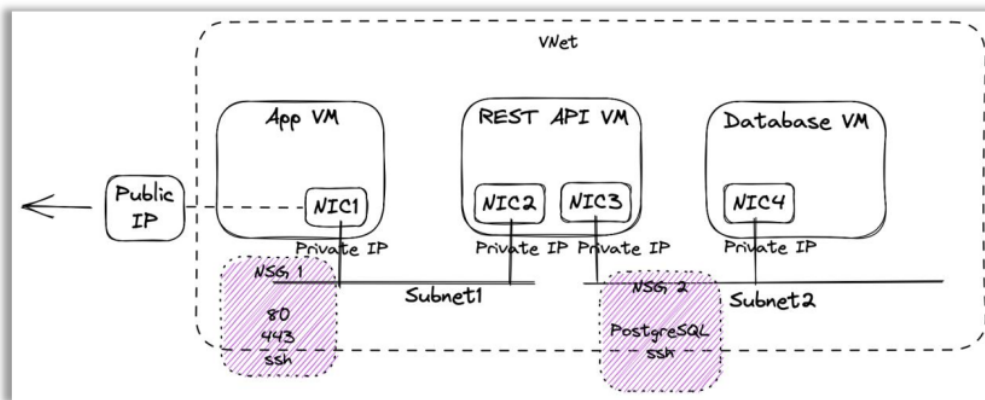


Figure 17 - NSGs

The `nsg rule create` command is used to build up the NSG. Several rules are put together to meet requirements. In this case, only allow TCP traffic from 10.0.1.0/24 to access the PostgreSQL port 5432:

```
az network nsg rule create -g $rg --nsg-name nsgDB --name
Allow-PostgreSQL --access Allow --protocol Tcp --
direction Inbound --priority 100 --source-address-prefix
10.0.1.0/24 --source-port-range "*" --destination-
address-prefix "*" --destination-port-range 5432
```

The `nsg rule --priority` property value dictates which order the rules are applied. The `list` command to see rules within a NSG:

```
Azure CLI$ az network nsg rule list -g $rg --nsg-name nsgDB -o table
```

| Name              | ResourceGroup | Priority | SourcePortRanges | SourceAddressPrefixes | SourceASG | Access | Protocol | Direction |
|-------------------|---------------|----------|------------------|-----------------------|-----------|--------|----------|-----------|
| Deny-All-TCP      | appResourceGP | 1000     | *                | 10.0.1.0/24           | None      | Deny   | Tcp      | Inbound   |
| Allow-SSH-Jumpbox | appResourceGP | 300      | *                | 10.0.1.0/24           | None      | Allow  | Tcp      | Inbound   |
| Allow-PostgreSQL  | appResourceGP | 100      | *                | 10.0.1.0/24           | None      | Allow  | Tcp      | Inbound   |

```
Azure CLI$ az network nsg rule list -g $rg --nsg-name nsgApp -o table
```

| Name            | ResourceGroup | Priority | SourcePortRanges | SourceAddressPrefixes | SourceASG | Access | Protocol | Direction |
|-----------------|---------------|----------|------------------|-----------------------|-----------|--------|----------|-----------|
| Allow-HTTP-All  | appResourceGP | 1000     | *                | Internet              | None      | Allow  | Tcp      | Inbound   |
| Allow-HTTPS-All | appResourceGP | 1200     | *                | Internet              | None      | Allow  | Tcp      | Inbound   |
| Allow-SSH-All   | appResourceGP | 300      | *                | Internet              | None      | Allow  | Tcp      | Inbound   |

Figure 18 - NSG Rules Example

The same details can be viewed from the Azure Portal, in this case the database server rules:

| Priority ↑↓             | Name ↑↓                 | Port ↑↓ | Protocol ↑↓ | Source ↑↓         | Destination ↑↓ | Action ↑↓ |  |
|-------------------------|-------------------------|---------|-------------|-------------------|----------------|-----------|--|
| Inbound Security Rules  |                         |         |             |                   |                |           |  |
| 100                     | Allow-PostgreSQL        | 5432    | Tcp         | 10.0.1.0/24       | Any            | Allow     |  |
| 300                     | Allow-SSH-Jumpbox       | 22      | Tcp         | 10.0.1.0/24       | Any            | Allow     |  |
| 1000                    | Deny-All-TCP            | Any     | Tcp         | 10.0.1.0/24       | Any            | Deny      |  |
| 65000                   | AllowVnetInBound        | Any     | Any         | VirtualNetwork    | VirtualNetwork | Allow     |  |
| 65001                   | AllowAzureLoadBalancer- | Any     | Any         | AzureLoadBalancer | Any            | Allow     |  |
| 65500                   | DenyAllInBound          | Any     | Any         | Any               | Any            | Deny      |  |
| Outbound Security Rules |                         |         |             |                   |                |           |  |
| 65000                   | AllowVnetOutBound       | Any     | Any         | VirtualNetwork    | VirtualNetwork | Allow     |  |
| 65001                   | AllowInternetOutBound   | Any     | Any         | Any               | Internet       | Allow     |  |
| 65500                   | DenyAllOutBound         | Any     | Any         | Any               | Any            | Deny      |  |

Figure 19 - Azure Portal NSG Rules View

The NSG examples here are for illustration, ideally in production environments, a more detailed design would be required meeting the *principle of least privilege*.

## 6. Additional Exercise – Simple 2 Tier IaaS Implementation

This section describes steps to create a 2 Tier IaaS Implementation of a simple Web server and PostgreSQL Database. In addition, a dedicated administration machine will be used as a jumpbox to allow administration tasks.

The full Azure and Linux commands can be found in Appendix A.

### 6.1 Deployment Design

Figure 20 shows the key aspects of the deployment. Two public IP addresses will be used, one for the web application front end (port 80), the second to gain access to a VM that will act as the jump-box (port 22). This jumpbox will be set up on its own administration subnet. Two Network Security Groups will be set up one for each subnet to control which ports are accessible within the network.

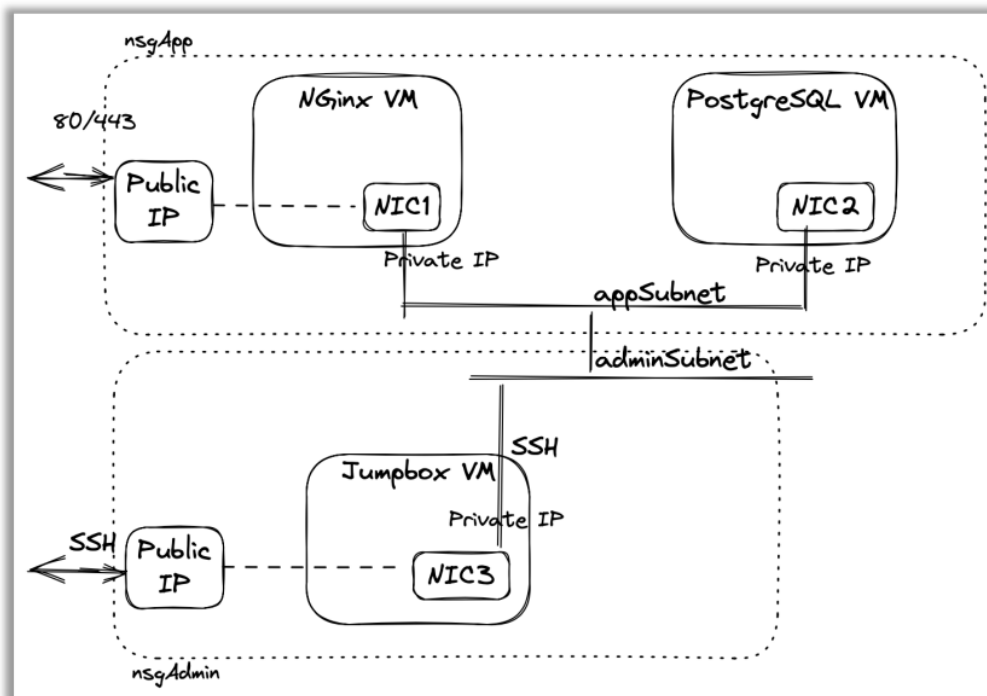
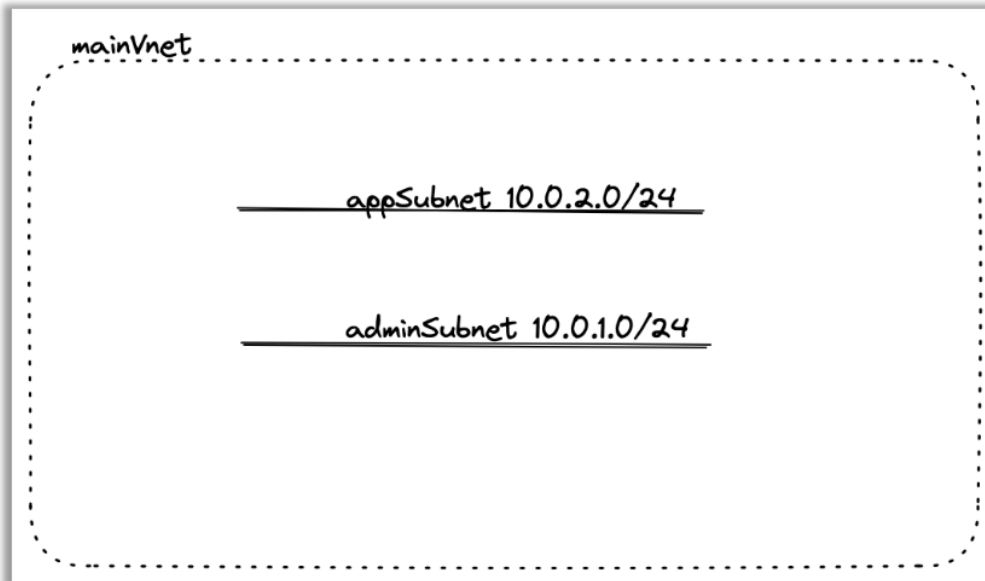


Figure 20 - Deployment Design

### 6.2 Step 1. Create vNet and Subnets

This step creates a single virtual network (mainVnet) and two subnets. The first subnet will contain the jumpbox virtual machine only, the second subnet will contain the Nginx VM (web server) and the PostgreSQL VM (database server)



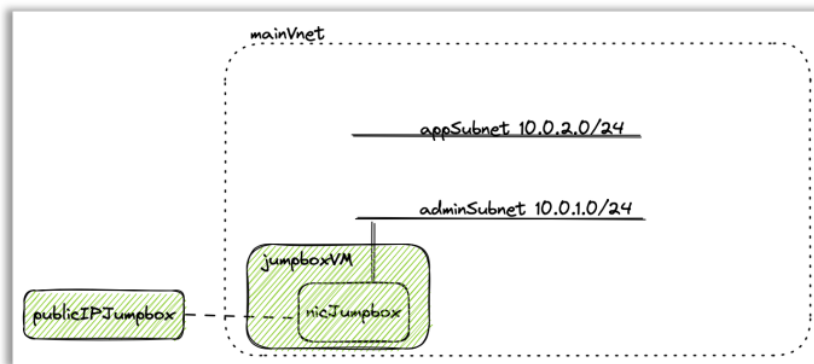
```
az network vnet create -n $vn1 -g $rg --address-prefix 10.0.0.0/16

# Create admin subnet and app subnet
az network vnet subnet create -n $s1 --vnet-name $vn1 -g $rg --address-prefixes 10.0.1.0/24
az network vnet subnet create -n $s2 --vnet-name $vn1 -g $rg --address-prefixes 10.0.2.0/24

# Show the created vnet and subnets
az network vnet list --output table
az network vnet subnet list -g $rg --vnet-name $vn1 -o table
```

### 6.3 Step 2. Create Jump Box VM with Public IP address

A public IP address is needed to gain access to the jumpboxVM from the internet



The following commands create a Network Interface (NIC), and public-IP resources. The two are then associated by updating the ip configuration of the jumpbox NIC.

```
# Create jumpboxnic in the adminsubnet
az network nic create -g $rg --subnet $s1 --vnet-name $vn1 -n jumpboxNic

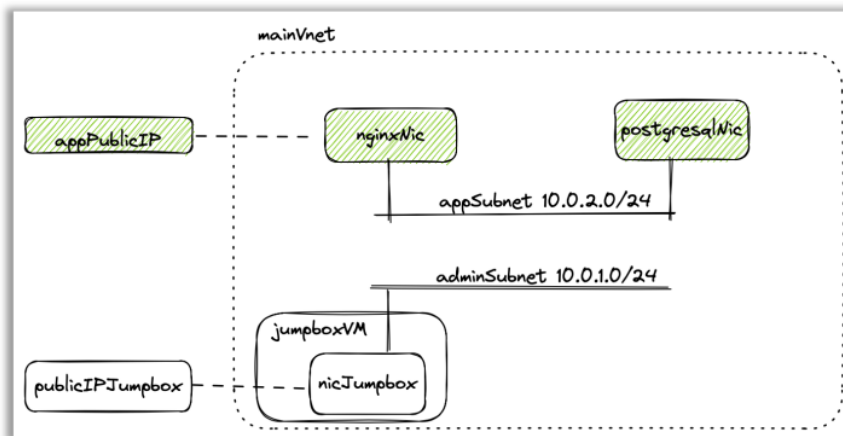
# Create a static public ip address and assign to nic
az network public-ip create -g $rg --name jumpboxPublicIP --allocation-method Static
az network nic ip-config update --name ipconfig1 --nic-name jumpboxNic -g $rg --public-ip-address jumpboxPublicIP
```

The following `vm create` shows how the `jumpboxNic` with its public IP address is assigned to the VM.

```
# Create vm with Nic using the Ubuntu image
az vm create -g $rg --name jumpboxVM --nics jumpboxNic --size Standard_B1ls --image UbuntuLTS --admin-username azureuser --generate-ssh-keys
```

### 6.4 Step 3. Create Network Interfaces for Application Servers

This step creates a public IP for the application server and two Nics.



The two NICs are the application NICs and are created on the same subnet

```
# 3.1 Create nics for app VMs
az network nic create -g $rg --subnet $s2 --vnet-name $vn1 -n nginxNic
az network nic create -g $rg --subnet $s2 --vnet-name $vn1 -n postgresqlNic
```

The second public IP is created and assigned to the internet facing nginxNic

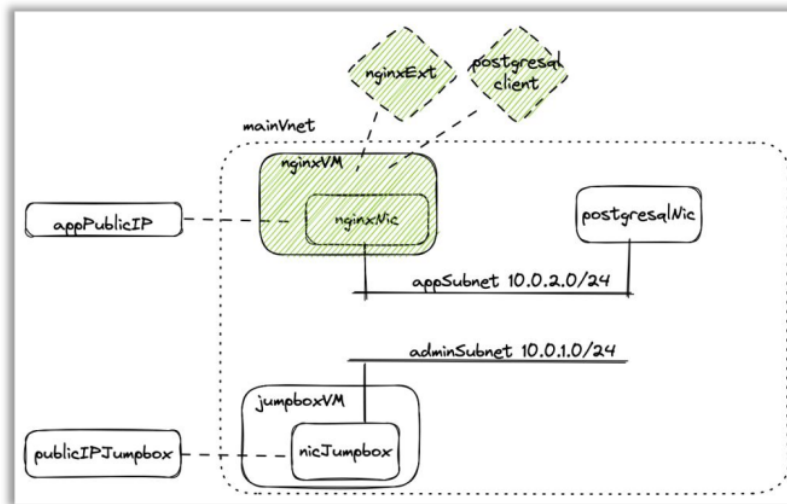
```
# 3.3 Create a static app public ip address
az network public-ip create -g $rg --name appPublicIP --allocation-method Static
```

Associate the public-ip to the configuration of the web server NIC (nginxNic):

```
# 3.4 Assign the public ip address to the NginxNic
az network nic ip-config update --name ipconfig1 --nic-name nginxNic -g $rg --public-ip-address appPublicIP
```

#### 6.5 Step 4. Create Web Server VM (nginx)

The web server VM will use Nginx service. This will be installed using an Azure Extension.



Create the VM and then execute the extension script:

```
# 4.1 A plain Ubuntu install for the nginx server.
az vm create -g $rg --name nginxVM --nics nginxNic --size Standard_B1ls --image UbuntuLTS --admin-username azureuser --ssh-key-value ~/.ssh/id_rsa.pub

# 4.2 Using a CustomScript extension to deploy nginx on to the web app server
az vm extension set -g $rg --vm-name nginxVM --publisher Microsoft.Azure.Extensions --name CustomScript --version 2.0 --settings '{"fileUris":["https://raw.githubusercontent.com/Azure-Samples/compute-automation-configurations/master/automate_nginx.sh"], "commandToExecute":"./automate_nginx.sh"}'
```

The postgresql-client package is installed on this VM to allow the nginx server to connect to the PostgreSQL database.

```
ssh azureuser@10.0.2.4

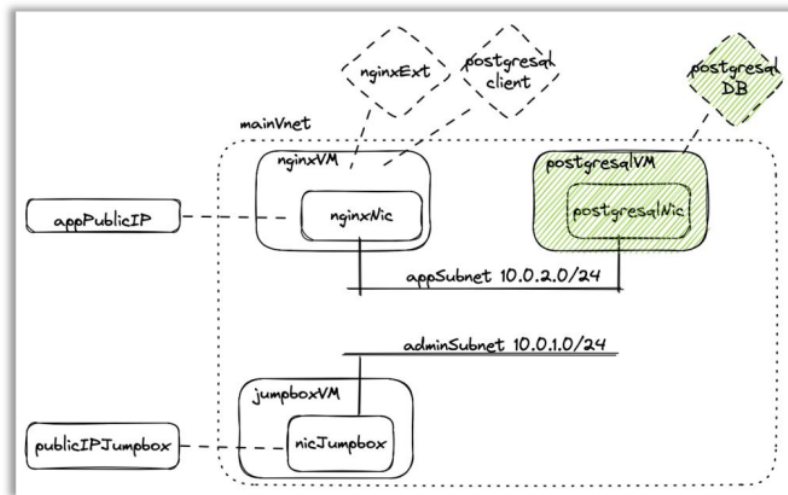
sudo apt-get install postgresql-client
```

## 6.6 Step 5. Create Database VM

In this step we would normally use a virtual machine Image with PostgreSQL pre-installed, for example:

```
az vm create -g $rg --name myDBVM1 --nics postgresqlNic --image cloud-  
infrastructure-services:postgresql-ubuntu:postgresql-ubuntu:0.0.1 --admin-  
username azureuser --ssh-key-value ~/.ssh/id_rsa.pub --size Standard_B2s
```

Due to limitations with the azure subscription PostgreSQL element will be installed manually.



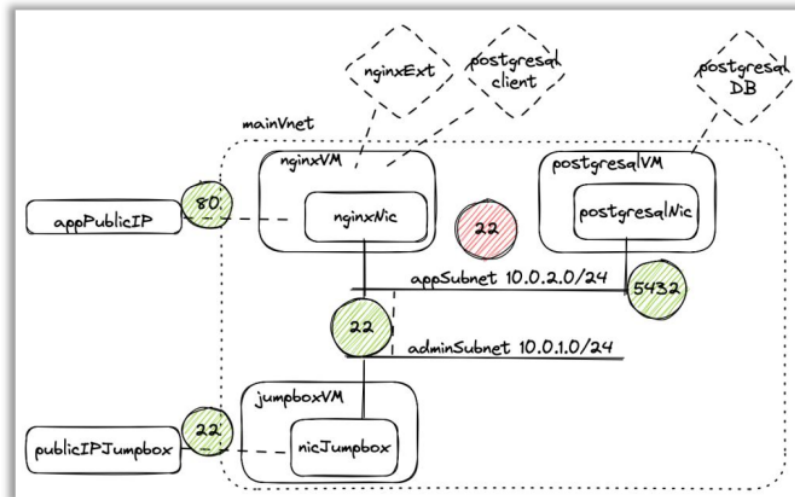
The existing public key for SSH is reused to save time, this is done by providing the `--ssh-key-value` parameter:

```
# 5.1 Create vm using plain Ubuntu image
az vm create -g $rg --name postgresqlVM --nics postgresqlNic --image UbuntuLTS --admin-username azureuser
--ssh-key-value ~/.ssh/id_rsa.pub --size Standard_B1ls
```

### 6.7 Step 5. Create NSGs and Rules Using subnets

As the private IP address are not static (managed by Azure), the nsg rules are based on the subnet ranges.

In the following sketch the ports effected are highlighted as circles.



Once the empty NSGs are created and assigned to subnets the default rules will now block access to ports:

```
# 6.1 Create admin and app nsgs
az network nsg create -g $rg --name nsgAdmin
az network nsg create -g $rg --name nsgApp

# 6.1.2 Associate nsgs with subnets - note this will block traffic as deny rules applied by default!!!
az network vnet subnet update --vnet-name $vn1 --name $s1 -g $rg --network-security-group nsgAdmin
az network vnet subnet update --vnet-name $vn1 --name $s2 -g $rg --network-security-group nsgApp
```

To allow access the Rules are created:

```
# 6.3 Create port 80 rule for nginx
# Can't browse yet until ...
az network nsg rule create -g $rg --nsg-name nsgApp --name appHTTP --access Allow --direction Inbound --protocol tcp --priority 300 --source-port-ranges '*' --destination-port-ranges 80
# show we can browse, but can't connect via ssh 22
ssh azureuser@20.254.112.115 22

# 6.4 Allow postgres - but only from it's own subnet
# Allow postgres port
az network nsg rule create -g $rg --nsg-name nsgApp --name Deny-PostgreSQL --access Deny --direction Inbound --protocol '*' --priority 550 --source-port-ranges '*' --destination-address-prefix "10.0.2.0/24" --destination-port-ranges 5432
az network nsg rule create -g $rg --nsg-name nsgApp --name Allow-PostgreSQL --access Allow --direction Inbound --protocol tcp --priority 500 --source-port-ranges '*' --source-address-prefix 10.0.2.0/24 --destination-port-ranges 5432

# 6.5 for demonstration, block SSH except from admin subnet i.e. we can't ssh from nginx to postgres
az network nsg rule create -g $rg --nsg-name nsgApp --name Deny-SSH --access Deny --direction Inbound --protocol '*' --priority 650 --source-port-ranges '*' --destination-address-prefix "10.0.2.0/24" --destination-port-ranges 22
# test - this rule take time to kick in
ssh azureuser@10.0.2.5
az network nsg rule create -g $rg --nsg-name nsgApp --name Allow-SSH-AdminSubnet --access Allow --direction Inbound --protocol '*' --priority 600 --source-address-prefix "10.0.1.0/24" --source-port-ranges '*' --destination-address-prefix "10.0.2.0/24" --destination-port-ranges 22
```

The following shows a screen grab of the rules in Azure Portal. It shows the mix of allow and deny rules that meet the requirements.

| Priority ↑↓             | Name ↑↓                | Port ↑↓ | Protocol ↑↓ | Source ↑↓         | Destination ↑↓ | Action ↑↓ |  |
|-------------------------|------------------------|---------|-------------|-------------------|----------------|-----------|--|
| Inbound Security Rules  |                        |         |             |                   |                |           |  |
| 300                     | appHTTP                | 80      | Tcp         | Any               | Any            | Allow     |  |
| 450                     | Allow-PostgreSQL       | 5432    | Tcp         | 10.0.2.0/24       | Any            | Allow     |  |
| 500                     | Deny-PostgreSQL        | 5432    | Any         | Any               | 10.0.2.0/24    | Deny      |  |
| 600                     | Allow-SSH-AdminSubnet  | 22      | Any         | 10.0.1.0/24       | 10.0.2.0/24    | Allow     |  |
| 650                     | Deny-SSH               | 22      | Any         | Any               | 10.0.2.0/24    | Deny      |  |
| 65000                   | AllowVnetInBound       | Any     | Any         | VirtualNetwork    | VirtualNetwork | Allow     |  |
| 65001                   | AllowAzureLoadBalancer | Any     | Any         | AzureLoadBalancer | Any            | Allow     |  |
| 65500                   | DenyAllInBound         | Any     | Any         | Any               | Any            | Deny      |  |
| Outbound Security Rules |                        |         |             |                   |                |           |  |
| 65000                   | AllowVnetOutBound      | Any     | Any         | VirtualNetwork    | VirtualNetwork | Allow     |  |
| 65001                   | AllowInternetOutBound  | Any     | Any         | Any               | Internet       | Allow     |  |
| 65500                   | DenyAllOutBound        | Any     | Any         | Any               | Any            | Deny      |  |

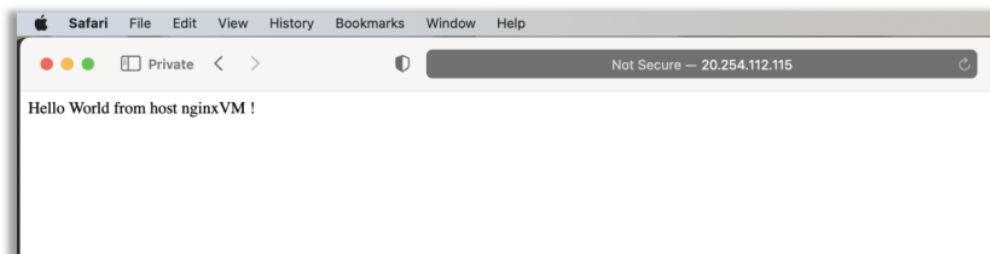
The rules here are intended to demonstrate the NSG capabilities.

## 6.8 Testing Implementation

This section shows some basic tests to validate the implementation.

### 6.8.1 HTTP Connectivity

Browsing to the public IP of the nginxVM shows that nginx, NSGs and Rules to be configured correctly:



### 6.8.2 SSH to App server Public IP address

This correctly fails to connect as we have denied port 22 in the appNSG for this public IP:

```
Azure CLI$ echo $appPublicIP
20.254.112.115
Azure CLI$ ssh azureuser@$appPublicIP
ssh: connect to host 20.254.112.115 port 22: Operation timed out
Azure CLI$ █
```

### 6.8.3 Connect From nginxVM to PostgreSQL

This screen shot shows logging in to the nginxVM from the jumpbox, then executing psql to the postgres host, then running "select date();" sql.

```
azureuser@jumpboxVM:~$ ssh azureuser@10.0.2.4 -q
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1098-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Tue Jan  3 17:46:02 UTC 2023

System load:  0.0               Processes:    105
Usage of /:   5.2% of 28.89GB   Users logged in:  0
Memory usage: 48%              IP address for eth0: 10.0.2.4
Swap usage:   0%

0 updates can be applied immediately.

New release '20.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Tue Jan  3 17:45:11 2023 from 10.0.1.4
azureuser@nginxVM:~$ psql -h 10.0.2.5 -U postgres
psql (10.22 (Ubuntu 10.22-0ubuntu0.18.04.1))
SSL connection (protocol: TLSv1.3, cipher: TLS_AES_256_GCM_SHA384, bits: 256, compression: off)
Type "help" for help.

postgres=# select now();
          now
-----
2023-01-03 17:47:51.040798+00
(1 row)

postgres=# █
```

~ End ~

## 7. Works Cited

- [1] R. P. a. Z. M. T. Erl, Cloud computing : concepts, technology, & architecture., Upper Saddle River, NJ: Prentice Hall, 2013.
- [2] M. Azure, "linux-vm," Microsoft, 2022. [Online]. Available: <https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/linux-vm>. [Accessed 23 12 2022].
- [3] Microsoft, "Azure managed disk types," Microsoft, 2022 12 10. [Online]. Available: <https://learn.microsoft.com/en-us/azure/virtual-machines/disks-types>. [Accessed 2022 12 16].
- [4] S. S. M. a. G. K. Shyam, "Resource management for Infrastructure as a Service (IaaS) in cloud computing: A survey," *Journal of network and computer applications*, vol. 41, p. 424–440, 2014.
- [5] Microsoft, "Azure Resource Manager Overview," Microsoft, 2022. [Online]. Available: <https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview>. [Accessed 27 12 2022].
- [6] C. Avanesians, "VM Image," 14 April 2014. [Online]. Available: <https://azure.microsoft.com/en-gb/blog/vm-image-blog-post/>. [Accessed 27 12 2022].
- [7] C. f. I. Security, "CIS Hardened Images," Center for Internet Security, 2022. [Online]. Available: <https://www.cisecurity.org/cis-hardened-images>. [Accessed 28 12 2022].
- [8] Microsoft Azure, "Virtual Networks Overview," Microsoft, 2022. [Online]. Available: <https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>. [Accessed 28 12 2022].
- [9] H. Bai, Zen of cloud : learning cloud computing by examples, Second edition. Boca Raton: CRC Press, Taylor & Francis Group, 2019. "NSGs are your first line of defense. By designing your NSGs, you can block any unwanted traf- fic while ensuring acce, Boca Ranton: CRC Press, 2019.
- [10] Microsoft, "Azure network security groups overview," Microsoft, 2022. [Online]. Available: <https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview>. [Accessed 28 12 2022].

## 8. Appendix A – Full Script

Note: this script is not designed to run as a single bash script as there are manual steps included for testing.

```
#!/usr/bin/env bash
export PS1="Azure CLI$ "
# bash command to exit on non 0 returns i.e. stop script on error.
set -e

# useful bash variables
l=uksouth
rg=appResourceGP
vn1=mainVNet
s1=adminSubnet
s2=appSubnet
adminIPConfigName=nothing
jumpbox=

# Create app resource group
az group create -n $rg -l $l

#####
#
# Step 1. Create vnet and subnets
#
#####

az network vnet create -n $vn1 -g $rg --address-prefix 10.0.0.0/16

# Create admin subnet and app subnet
az network vnet subnet create -n $s1 --vnet-name $vn1 -g $rg --address-prefixes 10.0.1.0/24
az network vnet subnet create -n $s2 --vnet-name $vn1 -g $rg --address-prefixes 10.0.2.0/24

# Show the created vnet and subnets
az network vnet list --output table
az network vnet subnet list -g $rg --vnet-name $vn1 -o table

#####
#
# Step 2. Create Jump Box with Public IP address
#
#####

# Create jumpboxnic in the adminsubnet
az network nic create -g $rg --subnet $s1 --vnet-name $vn1 -n jumpboxNic
```

```

# Create a static public ip address and assign to nic
az network public-ip create -g $rg --name jumpboxPublicIP --allocation-method Static
az network nic ip-config update --name ipconfig1 --nic-name jumpboxNic -g $rg --public-ip-address
jumpboxPublicIP

# store in handy variable
jumpboxPublicIP=$(az network public-ip show -g $rg -n jumpboxPublicIP --query "{address: ipAddress}" -o tsv)
echo $jumpboxPublicIP

# confirm publicip is linked to nic
az network public-ip show -g $rg -n jumpboxPublicIP --query "{address: ipAddress}" -o tsv
az network nic list -g $rg --query "[{Name:name, MAC:macAddress, IP:ipConfigurations[0].privateIpAddress,
IPub:ipConfigurations[0].publicIpAddress.id}]" --output table

# Create vm with Nic using the Ubuntu image
az vm create -g $rg --name jumpboxVM --nics jumpboxNic --size Standard_B1ls --image UbuntuLTS --admin-
username azureuser --generate-ssh-keys

# Check ports
nc -vz $jumpboxPublicIP 22
ssh azureuser@$jumpboxPublicIP

# Pause the machine while we build others
az vm deallocate -g $rg -n jumpboxVM

#####
#
# Step 3. Create Network Interfaces for application servers
#
#####

# 3.1 Create nics for app VMs
az network nic create -g $rg --subnet $s2 --vnet-name $vn1 -n nginxNic
az network nic create -g $rg --subnet $s2 --vnet-name $vn1 -n postgresqlNic

# 3.2 list the NICs
az network nic list -g $rg --query "[{Name:name, MAC:macAddress, IP:ipConfigurations[0].privateIpAddress,
IPub:ipConfigurations[0].publicIpAddress.id}]" --output table

# 3.3 Create a static app public ip address
az network public-ip create -g $rg --name appPublicIP --allocation-method Static

appPublicIP=$(az network public-ip show -g $rg -n appPublicIP --query "{address: ipAddress}" -o tsv)
echo $appPublicIP

# 3.4 Assign the public ip address to the NginxNic
az network nic ip-config update --name ipconfig1 --nic-name nginxNic -g $rg --public-ip-address appPublicIP

#####
#

```

```

# Step 4. Create web server - nginxVM
#
#####

# 4.1 A plain Ubuntu install for the nginx server.
az vm create -g $rg --name nginxVM --nics nginxNic --size Standard_B1ls --image UbuntuLTS --admin-username
azureuser --ssh-key-value ~/.ssh/id_rsa.pub

# 4.2 Using a CustomScript extension to deploy nginx on to the web app server
az vm extension set -g $rg --vm-name nginxVM --publisher Microsoft.Azure.Extensions --name CustomScript --
version 2.0 --settings '{"fileUris":["https://raw.githubusercontent.com/Azure-Samples/compute-automation-
configurations/master/automate_nginx.sh"],"commandToExecute":"./automate_nginx.sh"}'

# 4.3 Check port 80 is open - we can also browse to web page from a private browser
az network public-ip list -o table
nc -vz $appPublicIP 80

# 4.3.1 copy private key
cd .ssh
scp id_rsa azureuser@$jumpboxPublicIP:/home/azureuser/.ssh

# 4.4 Install Postgres Client on nginx web VM
PS1="jumpboxVM$ "
nginxPrivateIP=$(az vm show -g $rg -n nginxVM -d --query privateIps -otsv)
echo $nginxPrivateIP

ssh azureuser@$jumpboxPublicIP

ssh azureuser@10.0.2.4

sudo apt-get install postgresql-client

# 4.6 Stop web server
az vm deallocate -g $rg -n nginxVM

#####
#
#
# Step 5. Create Database VM
#
#####
#
# As we can't use the postgres market place images with our subscription we'll manually install postgres.
#az vm create -g $rg --name myDBVM1 --nics postgresqlNic --image cloud-infrastructure-services:postgresql-
ubuntu:postgresql-ubuntu:0.0.1 --admin-username azureuser --ssh-key-value ~/.ssh/id_rsa.pub --size
Standard_B2s
#az vm image list --publisher jetware-srl --offer postgresql --output table --all
#az vm image terms accept --urn jetware-srl:postgresql:postgresql95-ubuntu-1604:1.0.170503
#az vm create -g $rg --name myDBVM1 --nics myNic4 --size Standard_B1ls --image UbuntuLTS --admin-
username azureuser --ssh-key-value ~/.ssh/id_rsa.pub

```

```

#az vm image terms accept --urn jetware-srl:mysql:mysql56-ubuntu-1604:1.0.170503
#az vm create -g $rg --name myDBVM1 --nics postgresqlNic --image jetware-srl:mysql:mysql56-ubuntu-
1604:1.0.170503 --admin-username azureuser --ssh-key-value ~/.ssh/id_rsa.pub --size Standard_B2s

# 5.1 Create vm using plain Ubuntu image
az vm create -g $rg --name postgresqlVM --nics postgresqlNic --image UbuntuLTS --admin-username azureuser
--ssh-key-value ~/.ssh/id_rsa.pub --size Standard_B1ls

# Get the private ip
postgresPrivateIP=$(az vm show -g $rg -n postgresqlVM -d --query privateIps -otsv)
echo $postgresPrivateIP

# 5.2 Not good practice, but to save time, copy private key to jump box via public ip - for future use with app
machines
az vm start -g $rg -n jumpboxVM
scp id_rsa azureuser@$jumpboxPublicIP:/home/azureuser/.ssh

# Goto jumpboxVM
ssh azureuser@$adminPublicIP

# Jump to PostgreSQL VM
ssh azureuser@$postgresPrivateIP

# copy to jumpbox
# scp dvdrental.zip azureuser@20.68.182.87:/home/azureuser

# 3.2 install postgresSQL on postgresqlVM
sudo apt update
sudo apt install postgresql postgresql-contrib

# Update PostgreSQL config to allow remote connections
sudo vi /etc/postgresql/10/main/postgresql.conf
# listen_addresses = '*'
sudo vi /etc/postgresql/10/main/pg_hba.conf
# host all all 0.0.0.0/0 trust

# restart postgresql
sudo systemctl restart postgresql.service

# try to connect locally
sudo -i -u postgres
psql
select now();

# Check connectivity from nginxVM
ssh azureuser@$adminPublicIP
ssh azureuser@$appPrivateIP

# Check we can connect to postgres from nginx server
psql -h 10.0.2.5 -U postgres
select now();

```

```
#####
#
# Step 6. Create NSGs and rules using subnets - !!not specific IPs!!
#
#####

# 6.1 Create admin and app nsgs
az network nsg create -g $rg --name nsgAdmin
az network nsg create -g $rg --name nsgApp

# 6.1.2 Associate nsgs with subnets - note this will block traffic as deny rules applied by default!!!
az network vnet subnet update --vnet-name $vn1 --name $s1 -g $rg --network-security-group nsgAdmin
az network vnet subnet update --vnet-name $vn1 --name $s2 -g $rg --network-security-group nsgApp

# 6.2 Allow SSH only from internet to jumpbox
az network nsg rule create -g $rg --nsg-name nsgAdmin --name Allow-SSH-adminVM --access Allow --protocol
Tcp --direction Inbound --priority 300 --source-address-prefix Internet --source-port-range "*" --destination-
address-prefix "10.0.1.0/24" --destination-port-range 22
# 6.2.1 this should now work - note it can take a while for the rule to be applied
ssh azureuser@$adminPublicIP

# 6.3 Create port 80 rule for nginx
# Can't browse yet until ...
az network nsg rule create -g $rg --nsg-name nsgApp --name appHTTP --access Allow --direction Inbound --
protocol tcp --priority 300 --source-port-ranges "*" --destination-port-ranges 80
# show we can browse, but can't connect via ssh 22
ssh azureuser@20.254.112.115 22

# 6.4 Allow postgres - but only from it's own subnet
# Allow postgresql port
az network nsg rule create -g $rg --nsg-name nsgApp --name Deny-PostgreSQL --access Deny --direction
Inbound --protocol "*" --priority 550 --source-port-ranges "*" --destination-address-prefix "10.0.2.0/24" --destination-
port-ranges 5432
az network nsg rule create -g $rg --nsg-name nsgApp --name Allow-PostgreSQL --access Allow --direction
Inbound --protocol tcp --priority 500 --source-port-ranges "*" --source-address-prefix 10.0.2.0/24 --destination-port-
ranges 5432

# 6.5 for demonstration, block SSH except from admin subnet i.e. we can't ssh from nginx to postgres
az network nsg rule create -g $rg --nsg-name nsgApp --name Deny-SSH --access Deny --direction Inbound --
protocol "*" --priority 650 --source-port-ranges "*" --destination-address-prefix "10.0.2.0/24" --destination-port-
ranges 22
# test - this rule take time to kick in
ssh azureuser@10.0.2.5
az network nsg rule create -g $rg --nsg-name nsgApp --name Allow-SSH-AdminSubnet --access Allow --direction
Inbound --protocol "*" --priority 600 --source-address-prefix "10.0.1.0/24" --source-port-ranges "*" --destination-
address-prefix "10.0.2.0/24" --destination-port-ranges 22

ssh azureuser@10.0.2.5
```

```
# 5.7 Test NSGs
# try to ssh from nginx to postgresVM
ssh azureuser@postgresPrivateIP

# try to psql from nxginxVM to postgresVM
psql -h 10.0.2.5 -U postgres

#####
#
# 7. Clean up
#
#####

az group delete -n $rg -y
```

# Assignment Practical

---

## GRADEMARK REPORT

---

FINAL GRADE

90/100

GENERAL COMMENTS

### Instructor

VM Resources (40): 39

VM Images (35): 28

Config Exercise (20): 18

Demo (5):5

Feedback:

=====

Excellent discussion of VMs and components, could have provided a little more explanation of some concepts e.g. what is a NIC?

You discussed and demonstrated the use of images in your applicaiton and video.

Excellent configurattion demo with good explanation that meets all the criteria Interesting you used a jumpbox VM instead of a Bastion. In Azure a Bastion is considered a more secure and better approach.

---

PAGE 1

---

PAGE 2

---

PAGE 3

---

PAGE 4

---

PAGE 5

---

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

PAGE 14

PAGE 15

PAGE 16

PAGE 17

PAGE 18

PAGE 19

PAGE 20

PAGE 21

PAGE 22

PAGE 23

PAGE 24

PAGE 25

PAGE 26

PAGE 27

PAGE 28

PAGE 29

PAGE 30

PAGE 31

