Shaheed Zulfikar Ali Bhutto Institute of Science and Technology

Department of Software Engineering

Bisma Saeed – 2280108

BSSE – 7A

Lab: 04

Implement Virtual Networking

In this lab, you learn the basics of virtual networking and subnetting. You learn how to protect your network with **network security groups** and **application security groups**. You also learn about DNS zones and records.

The **CoreServicesVnet** virtual network has the largest number of resources. A large amount of growth is anticipated, so a large address space is necessary for this virtual network. The **ManufacturingVnet** virtual network contains systems for the operations of the manufacturing facilities.

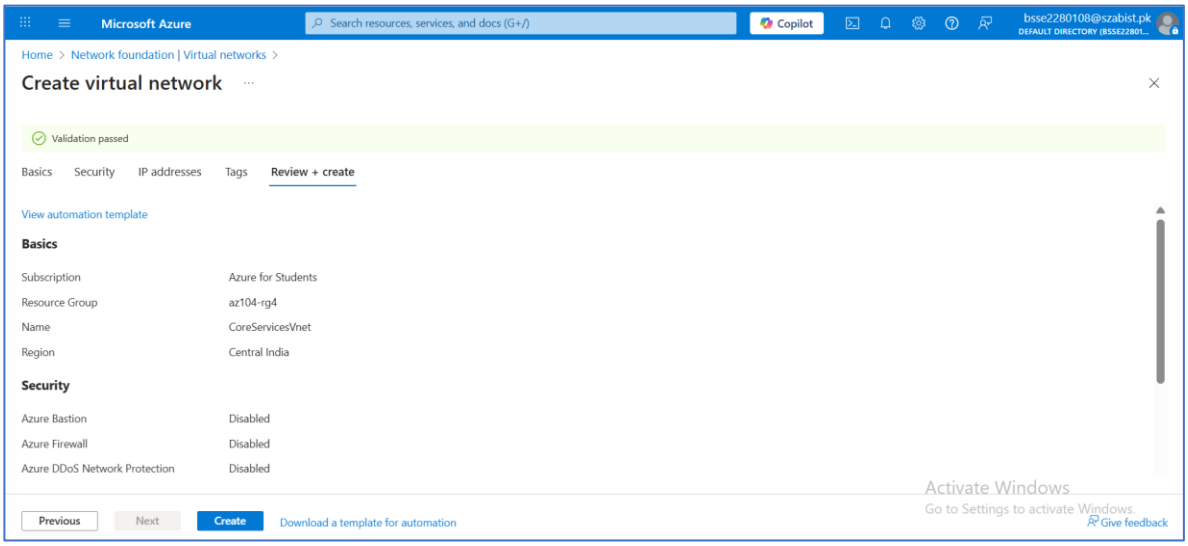
Task 1: Create a virtual network with subnets using the portal

The organization plans a large amount of growth for core services. In this task, you create the virtual network and the associated subnets to accommodate the existing resources and planned growth. In this task, you will use the Azure portal.

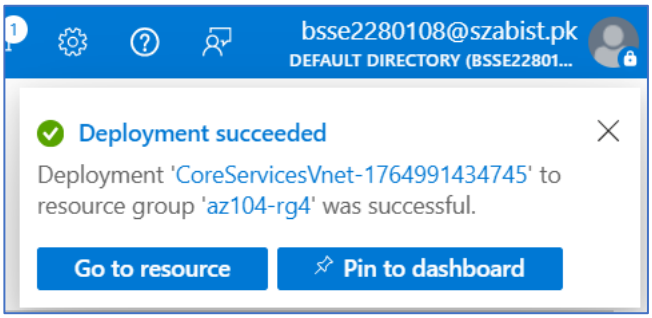
1. Sign in to the **Azure portal** - `https://portal.azure.com`. Search for and select `Virtual Networks`.

2. Select **Create** on the Virtual networks page. Complete the **Basics** tab for the CoreServicesVnet.

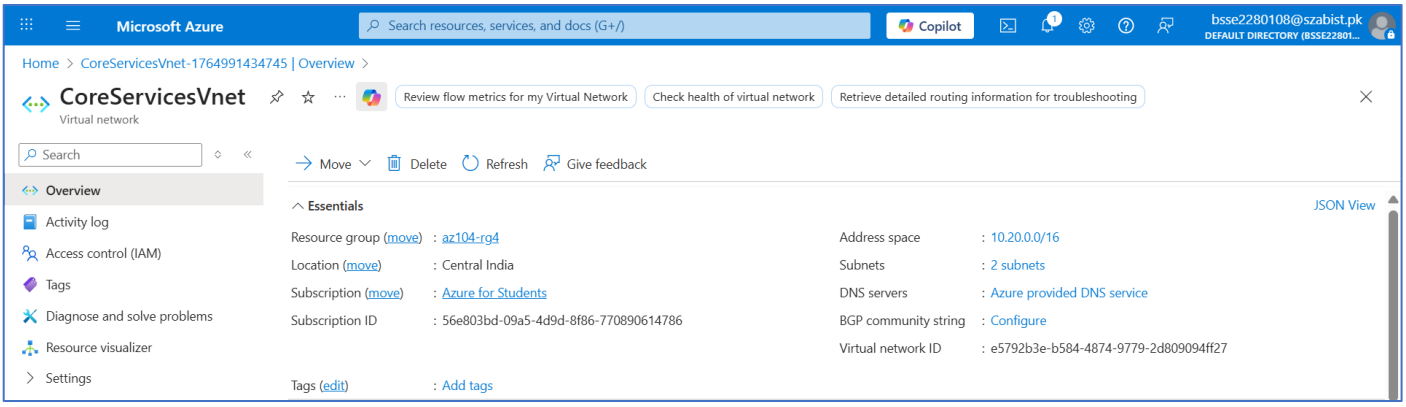
3. To finish creating the CoreServicesVnet and its associated subnets, select **Review + create**. Verify your configuration passed validation, and then select **Create**.



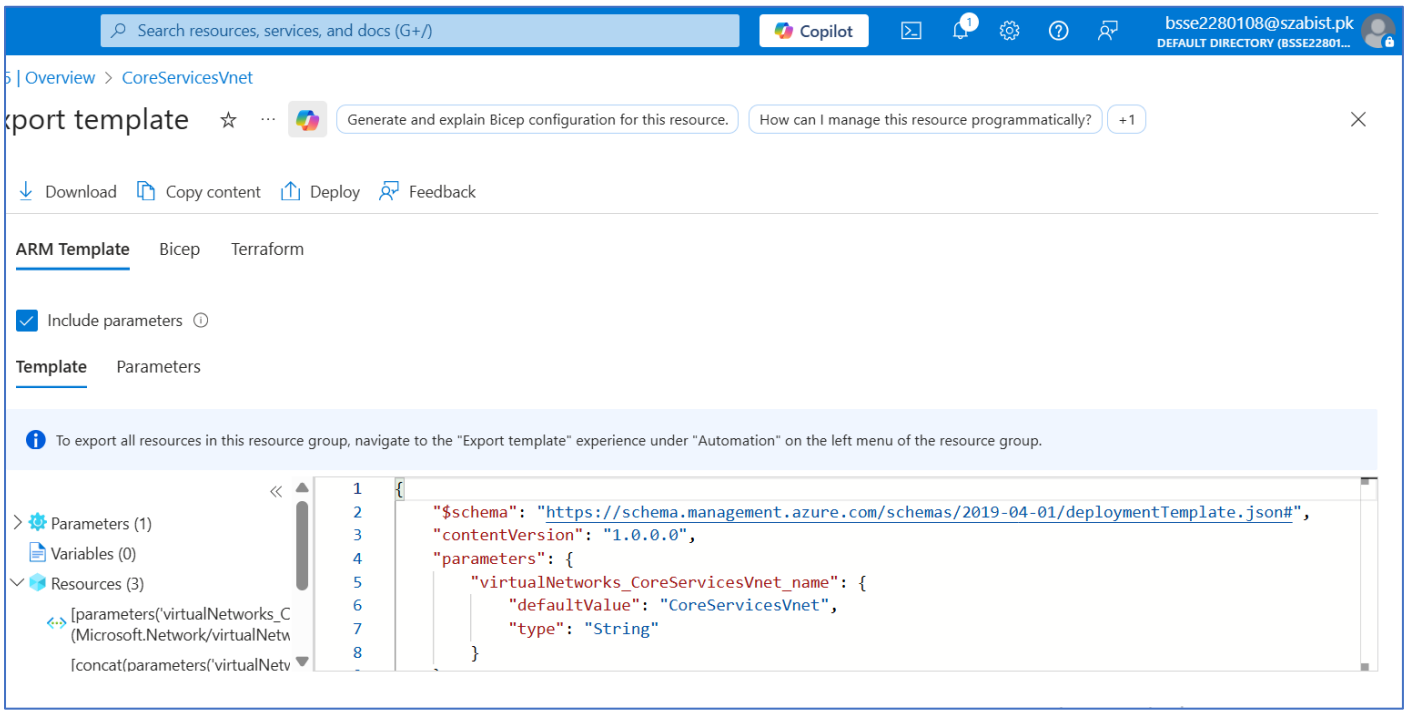
4. Wait for the virtual network to deploy and then select **Go to resource**.



5. Take a minute to verify the **Address space** and the **Subnets**. Notice your other choices in the **Settings** blade.

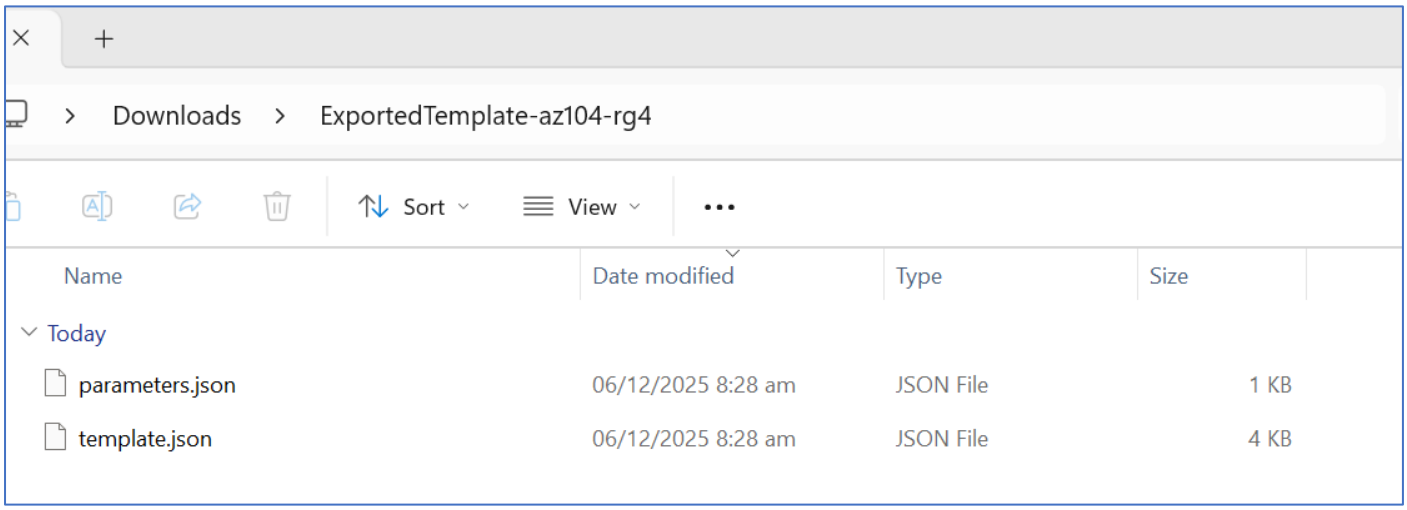


6. In the **Automation** section, select **Export template**, and then wait for the template to be generated. **Download** the template.



7. Navigate on the local machine to the **Downloads** folder and **Extract all** the files in the downloaded zip file.

8. Before proceeding, ensure you have the **template.json** file. You will use this template to create the ManufacturingVnet in the next task.



Task 2: Create a virtual network and subnets using a template

1. Locate the **template.json** file exported in the previous task. It should be in your **Downloads** folder.

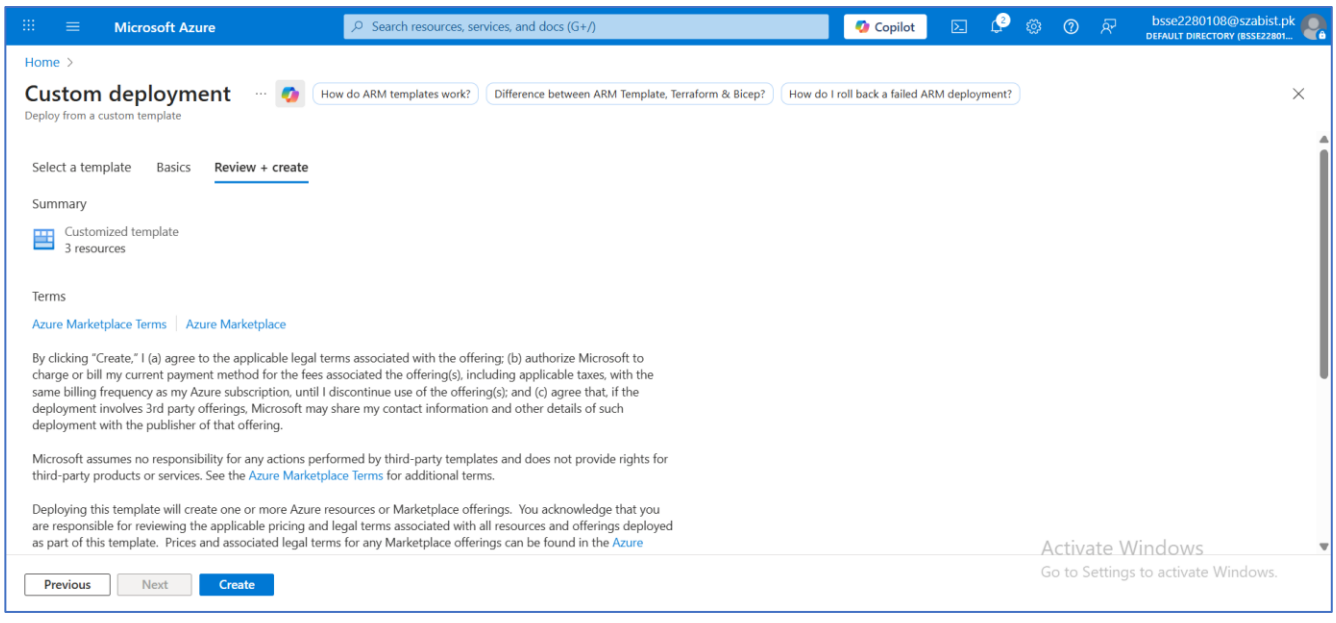
2. Edit the file using the editor of your choice. Many editors have a *change all occurrences* feature. If you are using Visual Studio Code be sure you are working in a **trusted window** and not in the **restricted mode**. Consult the architecture diagram to verify the details.

3. Replaced all the required things in both the json files.

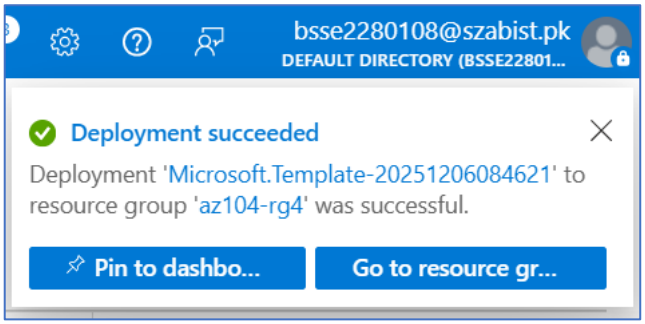
4. ### Deploy the custom template in the portal, search for and select `Deploy a custom template`.

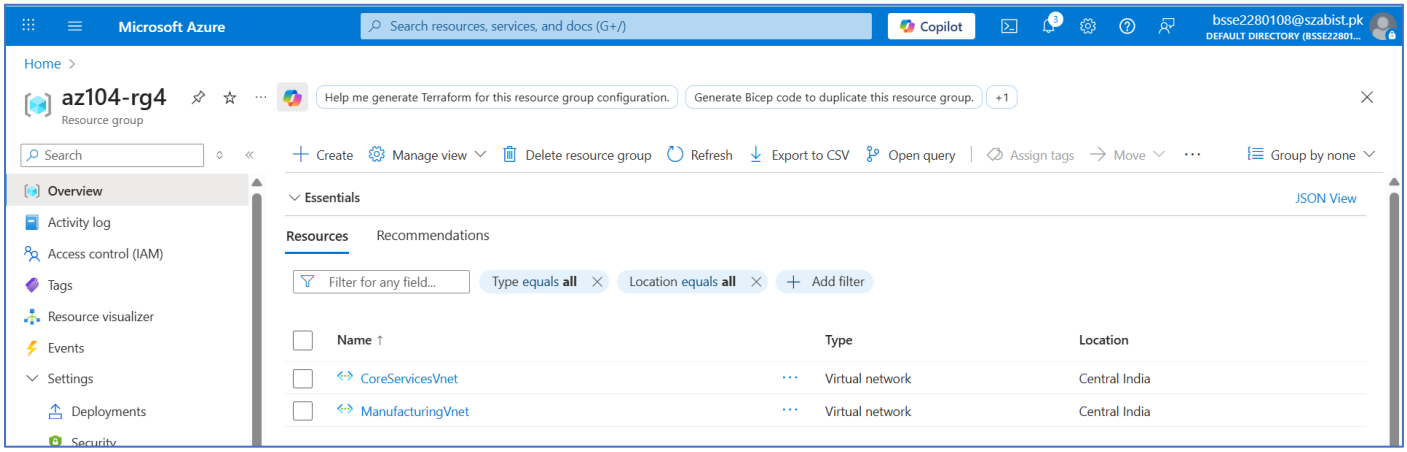
5. Select **Build your own template in the editor** and then **Load file**, Select the **template.json** file with your Manufacturing changes, then select **Save**, Select **Edit parameters**, and then **Load file**, Select the **parameters.json** file with your Manufacturing changes, then select **Save**, Ensure your resource group, **az104-rg4** is selected.

6. Select **Review + create** and then **Create**.



7. Wait for the template to deploy, then confirm (in the portal) the Manufacturing virtual network and subnets were created.

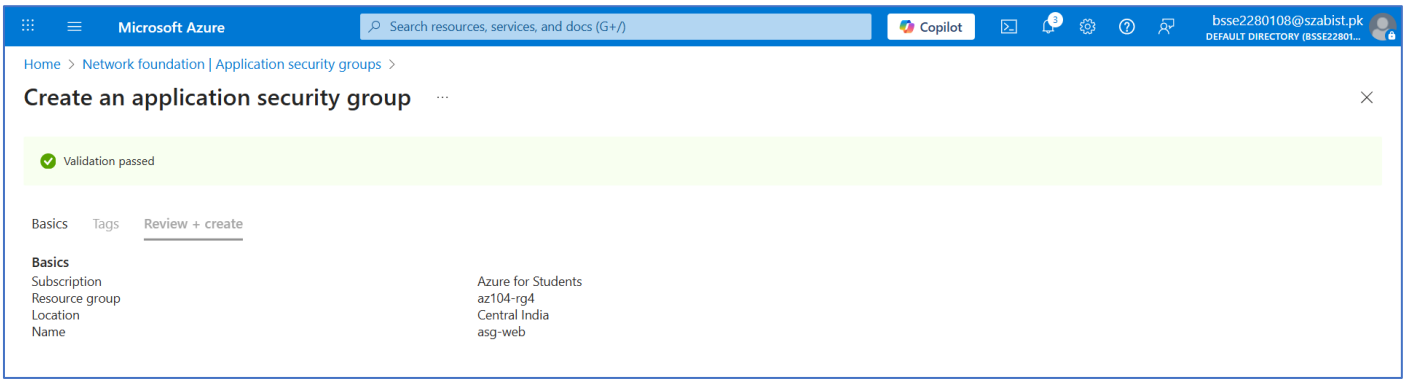


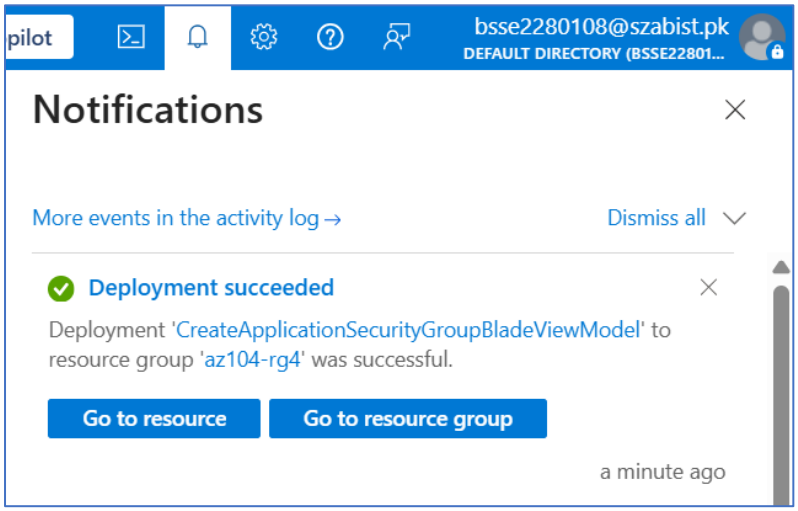


Task 3: Create and configure communication between an Application Security Group and a Network Security Group

In this task, we create an Application Security Group and a Network Security Group. The NSG will have an inbound security rule that allows traffic from the ASG. The NSG will also have an outbound rule that denies access to the internet.

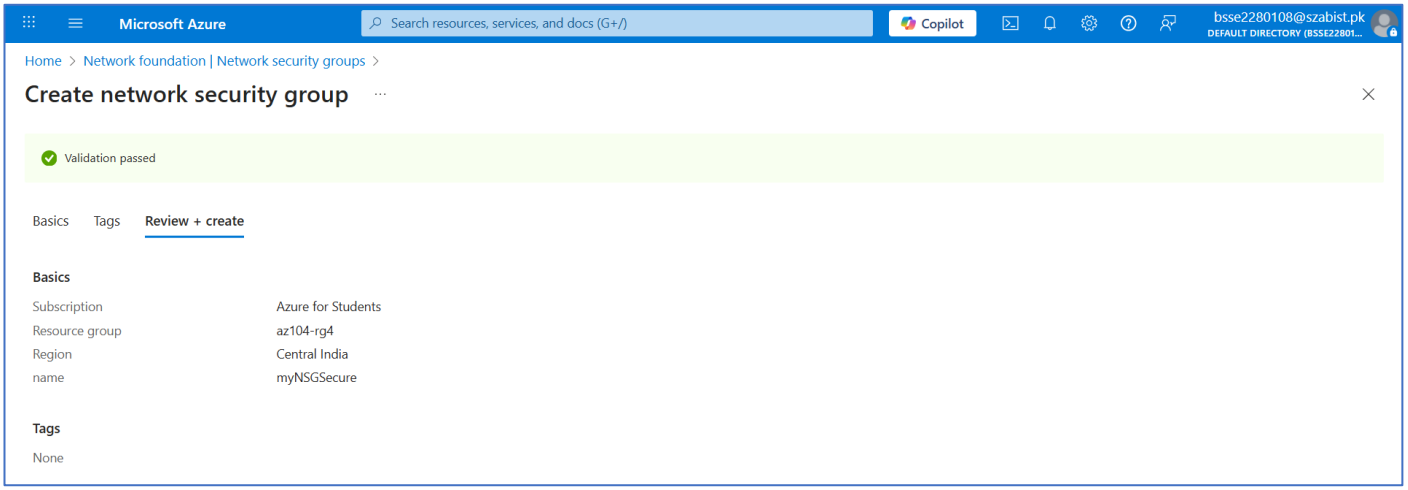
1. In the Azure portal, search for and select `Application security groups`.
2. Click **Create** and provide the basic information.
3. Click **Review + create** and then after the validation click **Create**.



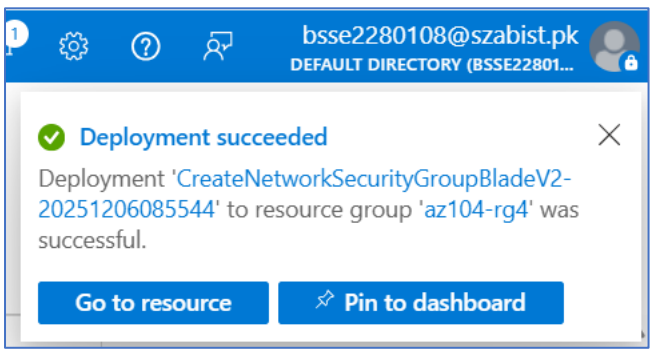


Create the Network Security Group and associate it with CoreServicesVnet

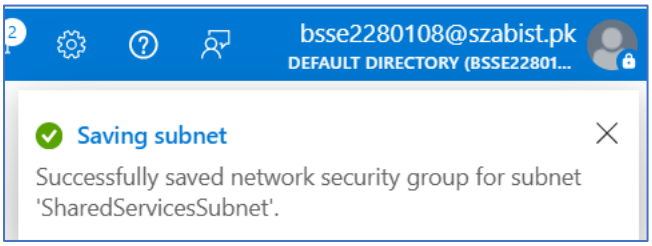
4. In the Azure portal, search for and select `Network security groups`.
5. Select **+ Create** and provide information on the **Basics** tab.
6. Click **Review + create** and then after the validation click **Create**.



7. After the NSG is deployed, click **Go to resource**.



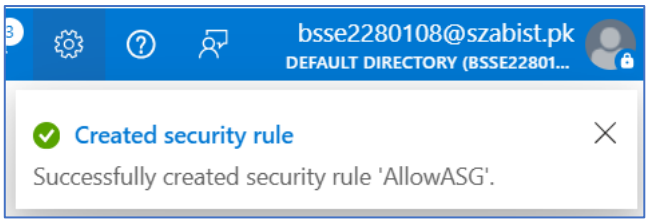
8. Under **Settings** click **Subnets** and then **Associate**. Click **OK** to save the association.



Configure an inbound security rule to allow ASG traffic

9. Continue working with your NSG. In the **Settings** area, select **Inbound security rules**.

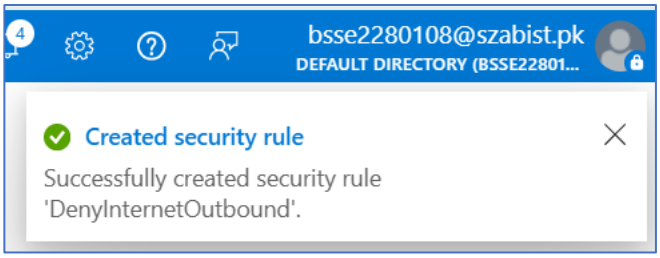
10. Select **+ Add**. On the **Add inbound security rule** blade, use the following information to add an inbound port rule. This rule allows ASG traffic. When you are finished, select **Add**.



Configure an outbound NSG rule that denies Internet access

11. After creating your inbound NSG rule, select **Outbound security rules**.

12. Select **+ Add** and then configure an outbound rule that denies access to the internet. When you are finished, select **Add**.

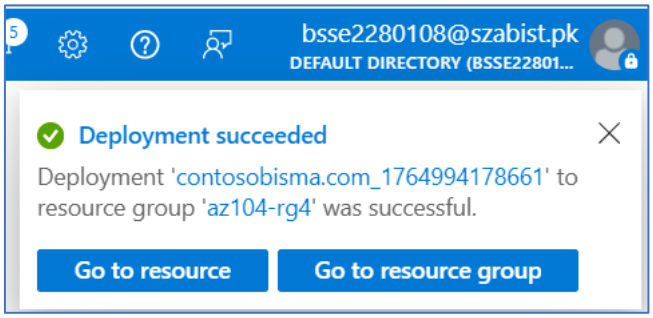


Task 4: Configure public and private Azure DNS zones

In this task, you will create and configure public and private DNS zones.

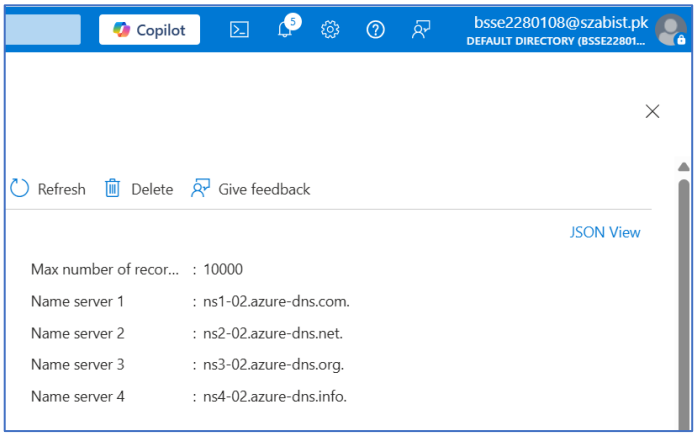
Configure a public DNS zone

1. In the portal, search for and select `DNS zones`. Select **+ Create**. Configure the **Basics** tab. Select **Review + create** and then **Create**.



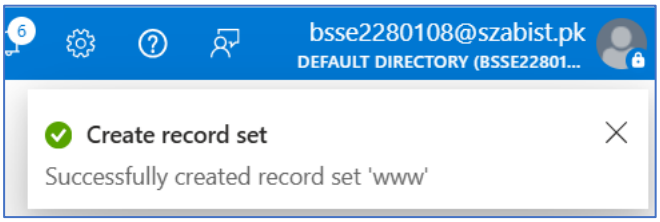
2. Wait for the DNS zone to deploy and then select **Go to resource**.

1. On the **Overview** blade notice the names of the four Azure DNS name servers assigned to the zone. **Copy** one of the name server addresses. You will need it in a future step.



2. Expand the **DNS Management** blade and select **Recordsets**. Click **+Add**.

3. Select **Add** and verify your domain has an A record set named **www**.



4. Open a command prompt, and run the following command. If you have changed the domain name, make an adjustment. nslookup www.contoso.com <name server name>

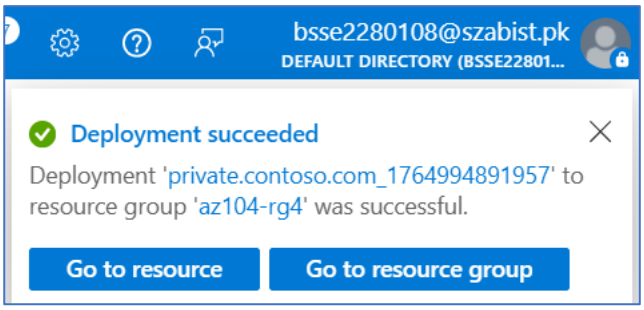
5. Verify the host name www.contoso.com resolves to the IP address you provided. This confirms name resolution is working correctly.

```
C:\Users\ZA>nslookup www.contosobisma.com ns1-02.azure-dns.com
Server:  UnKnown
Address:  13.107.236.2

Name:    www.contosobisma.com
Address:  10.1.1.4


C:\Users\ZA>
```

Configure a private DNS zone

6. In the portal, search for and select `Private dns zones`. Select **+ Create**. On the **Basics** tab of Create private DNS zone, enter the information as listed in the table below:

7. Select **Review + create** and then **Create**.

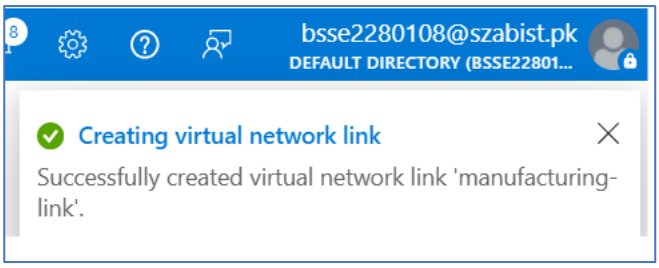


8. Wait for the DNS zone to deploy and then select **Go to resource**.

9. Notice on the **Overview** blade there are no name server records.

10. Expand the **DNS Management** blade and then select **Virtual network links**. Configure the link.

11. Select **Create** and wait for the link to create.



12. From the **DNS Management** blade select **+ Recordsets**. You would now add a record for each virtual machine that needs private name-resolution support.

Key takeaways

Congratulations on completing the lab. Here are the main takeaways for this lab.

+ A virtual network is a representation of your own network in the cloud.
+ When designing virtual networks it is a good practice to avoid overlapping IP address ranges. This will reduce issues and simplify troubleshooting.
+ A subnet is a range of IP addresses in the virtual network. You can divide a virtual network into multiple subnets for organization and security.
+ A network security group contains security rules that allow or deny network traffic. There are default incoming and outgoing rules which you can customize to your needs.
+ Application security groups are used to protect groups of servers with a common function, such as web servers or database servers.
+ Azure DNS is a hosting service for DNS domains that provides name resolution. You can configure Azure DNS to resolve host names in your public domain. You can also use private DNS zones to assign DNS names to virtual machines (VMs) in your Azure virtual networks.