CANTON WEKE OTIENO

SECURITY ENGINEER TRACK

STUDENT TRACKING NUMBER; ADC-SE01-24010

CYBER SHUJAA

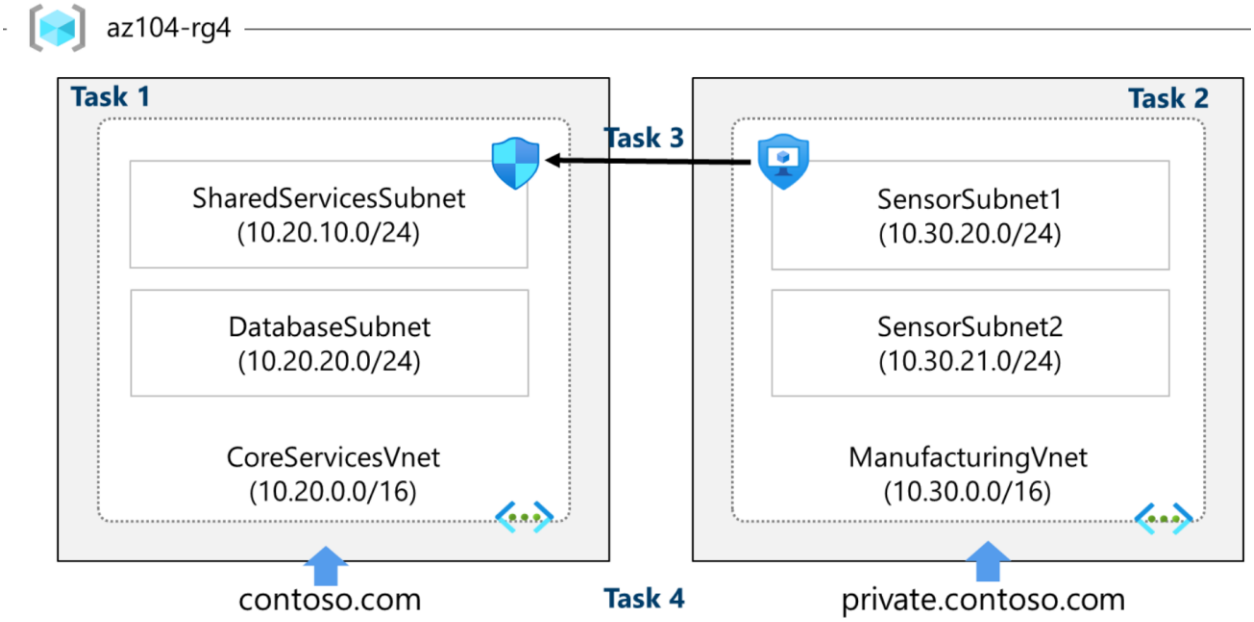
INSTRUCTOR: DR. PAULA

LAB 04 - IMPLEMENT VIRTUAL NETWORKING

This lab focuses on virtual networking. It covers the basics of virtual networking and subnetting. It provide practical guidance on how to protect your network with network security groups and application security group.

Azure Virtual Network (VNet) is a service that provides the fundamental building block for your private network in Azure. With Azure VNet, you can create a logically isolated network that is dedicated to your Azure account. An instance of the service, known as a virtual network, enables many types of Azure resources to securely communicate with each other, the internet, and on-premises networks. These Azure resources include virtual machines (VMs), Azure App Services, and Azure Kubernetes Service (AKS), among others. Each VNet you create can be customized to fit your needs, with options for configuring subnets, route tables, and security settings. With the capacity to create subnets, implement network security rules, and route traffic, a virtual network functions similarly to a conventional network that you may run in your own datacenter. On the other hand, it offers the further advantages of the Azure infrastructure.

Architecture diagram



This repport is dived into four section where each section describe how perticular task and configuration is done within the azure plartform, it contains how to create a virtual network with

subnets using the portal, how to create a virtual network and subnets using a template, how to create and configure communication between an Application Security Group and a Network Security Group and finally how to configure public and private Azure DNS zones.

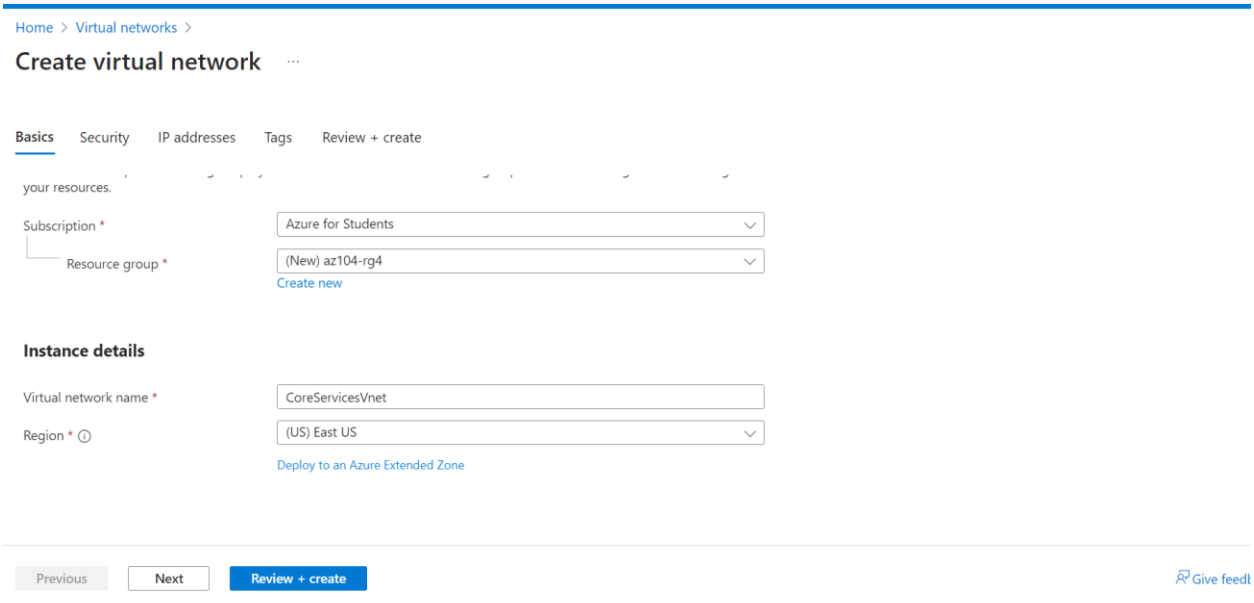
At the of the report everyone will be able to use the tools to efficiently manage and extend cloud infrastructure by laying out a complete path for establishing a secure and reliable Azure networking environment through these detailed activities.

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

This task illustrates how to create a basic network architecture that links different Azure resources, such as virtual machines and application services, so they can safely communicate inside a designated network area.

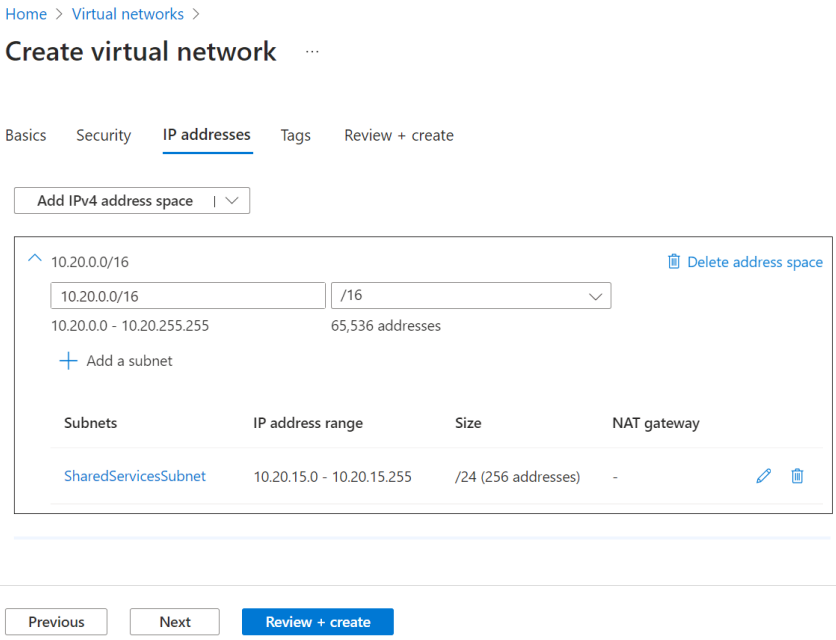
Instructions include;

- Sign in to the Azure portal - https://portal.azure.com.
- Search for and select Virtual Networks.
- Select Create on the Virtual networks page.
- Complete the Basics tab for the CoreServicesVnet

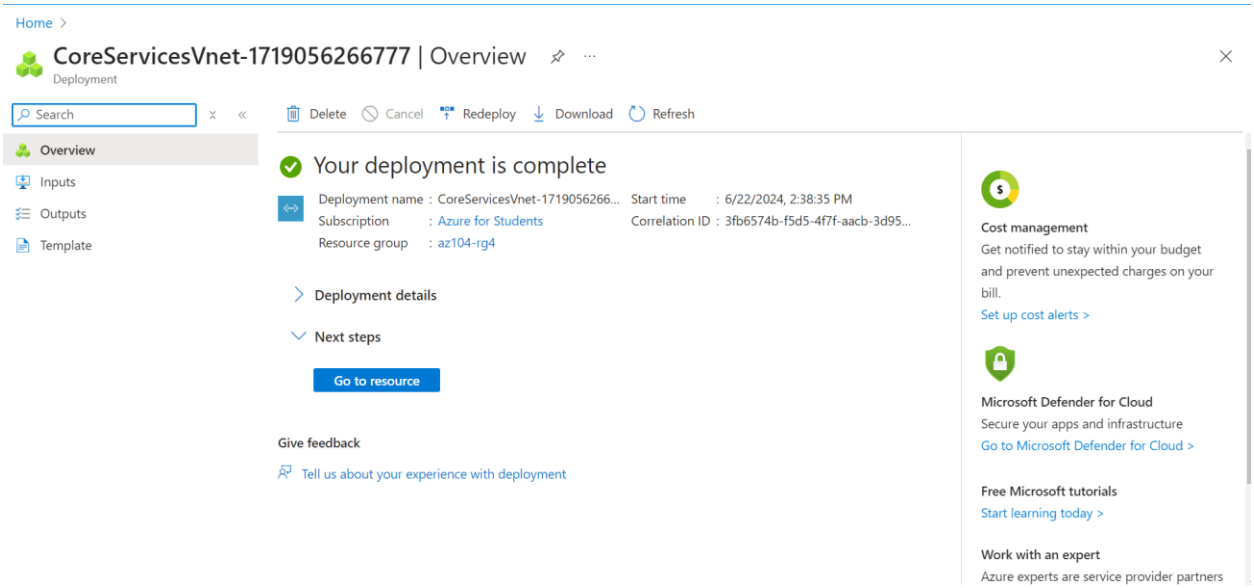


- Move to the IP Addresses tab.

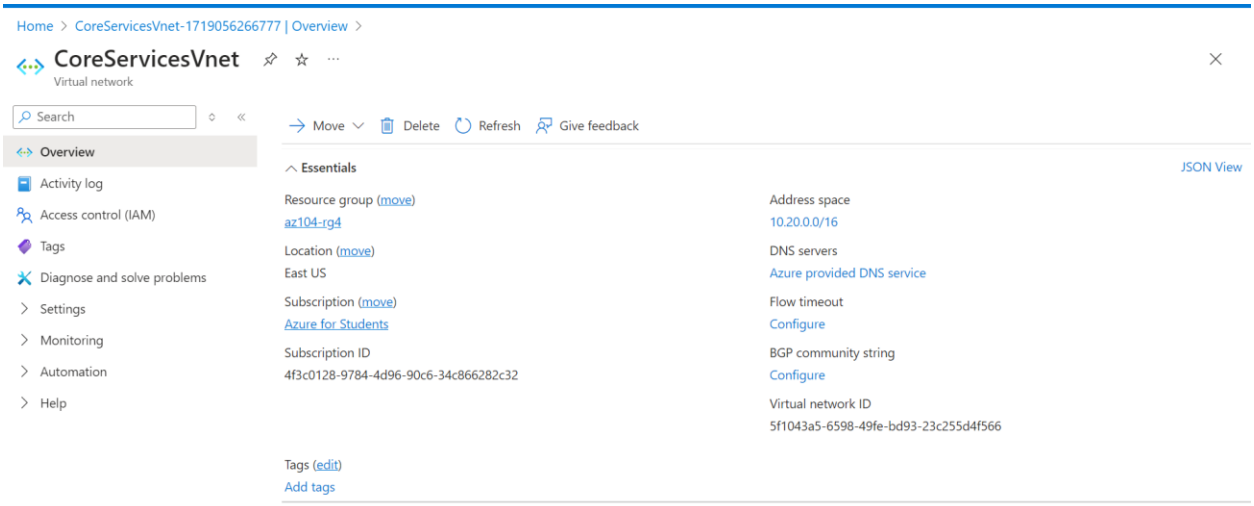
- **Option** **Value**
- **IPv4 address space** Replace the prepopulated IPv4 address space with 10.20.0.0/16 (separate the entries)
- Select + Add a subnet. Complete the name and address information for each subnet. Be sure to select Add for each new subnet. Be sure to delete the default subnet - either before or after creating the other subnets.

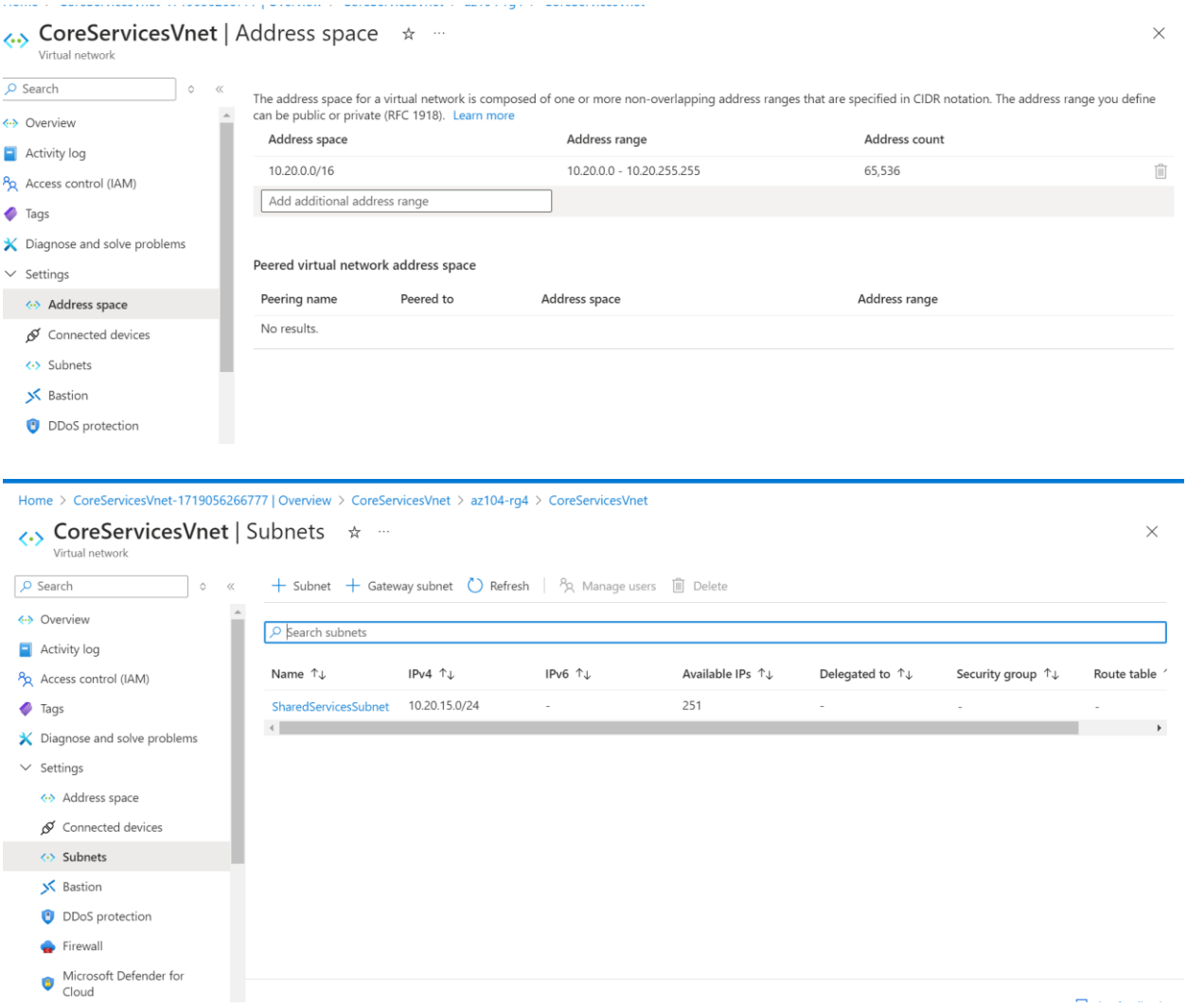


- To finish creating the CoreServicesVnet and its associated subnets, select **Review + create**.
- Verify your configuration passed validation, and then select **Create**.

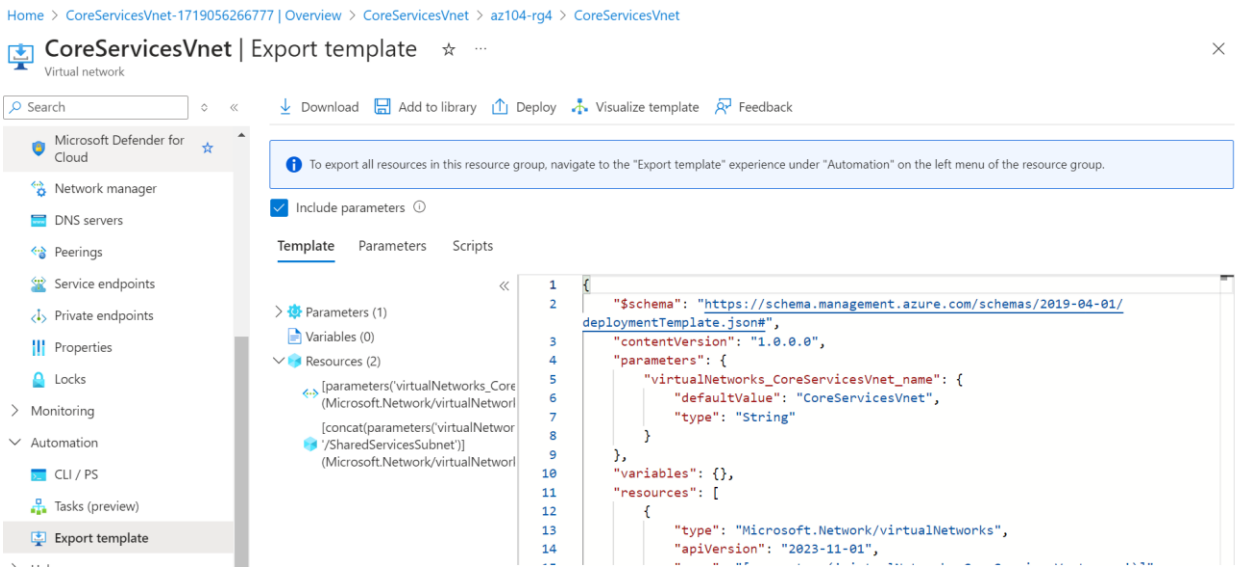


- Wait for the virtual network to deploy and then select **Go to resource**.
- Take a minute to verify the **Address space** and the **Subnets**. Notice your other choices in the **Settings** blade.





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



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

In Task 2, an Azure Resource Manager (ARM) template was used to create a virtual network and associated subnets. This technique demonstrates the benefits of infrastructure as code, enabling effective automation and replication of network setups across many contexts. It also demonstrates how templates may be used to swiftly deploy scalable and consistent network configurations that follow the guidelines and regulations of an organization, decreasing the possibility of manual errors and streamlining the deployment procedure.

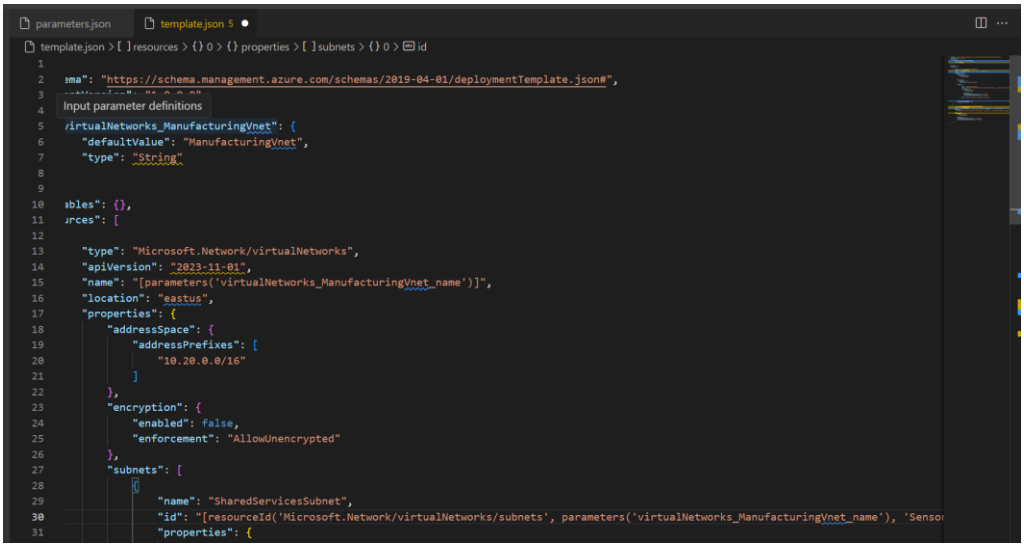
Instruction and screenshots

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

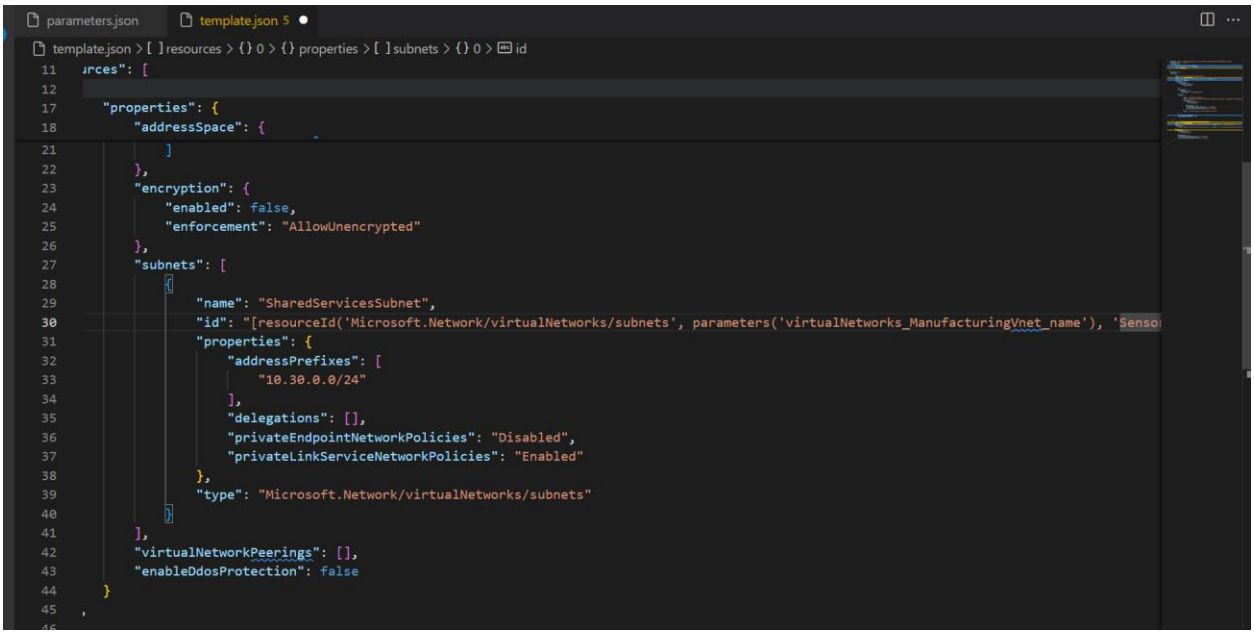
Make changes for the ManufacturingVnet virtual network

- Replace all occurrences of CoreServicesVnet with ManufacturingVnet.
- Replace all occurrences of 10.20.0.0 with 10.30.0.0.



Make changes for the ManufacturingVnet subnets

- Change all occurrences of SharedServicesSubnet to SensorSubnet1.
- Change all occurrences of 10.20.10.0/24 to 10.30.20.0/24.
- Change all occurrences of DatabaseSubnet to SensorSubnet2.
- Change all occurrences of 10.20.20.0/24 to 10.30.21.0/24.
- Read back through the file and ensure everything looks correct.
- Be sure to Save your changes

- 

Make changes to the parameters file

- Locate the parameters.json file exported in the previous task. It should be in your Downloads folder.
- Edit the file using the editor of your choice.
- Replace the one occurrence of CoreServicesVnet with ManufacturingVnet.
- Save your changes.

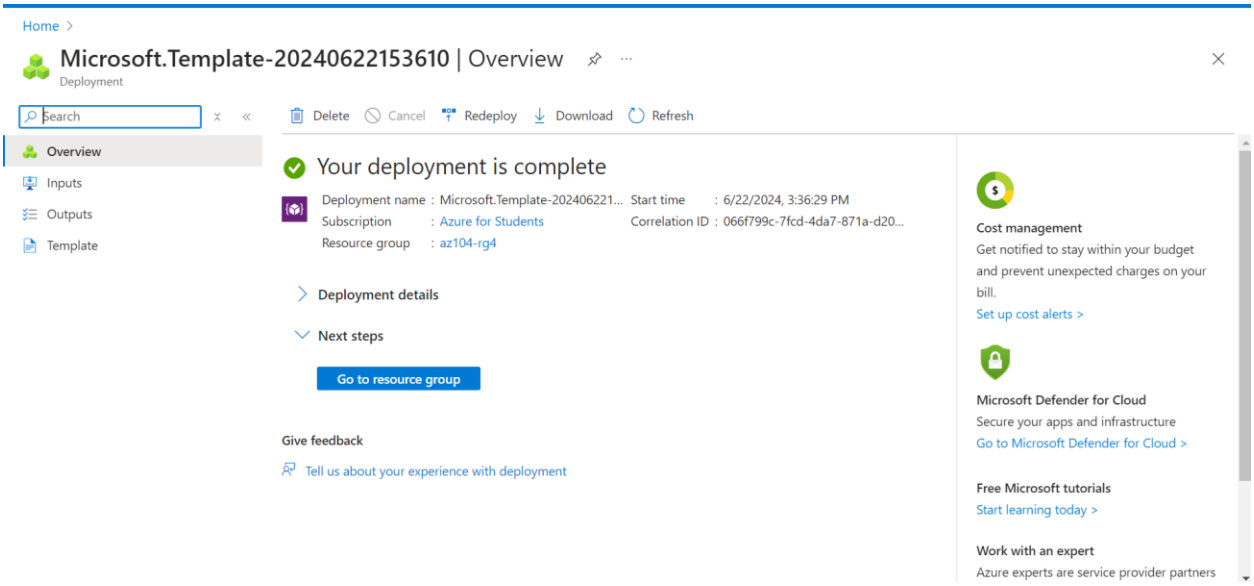
- parameters.json template.json 5

parameters.json > {} parameters > {} virtualNetworks_ManufacturingVnet

```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentParameters.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
        "virtualNetworks_ManufacturingVnet": {
            "value": null
        }
    }
}
```

Deploy the custom template

- In the portal, search for and select Deploy a custom template.
- Select Build your own template in the editor and then Load file.
- Select the templates.json file with your Manufacturing changes, then select Save.
- Select Review + create and then Create.
- Wait for the template to deploy, then confirm (in the portal) the Manufacturing virtual network and subnets were created.



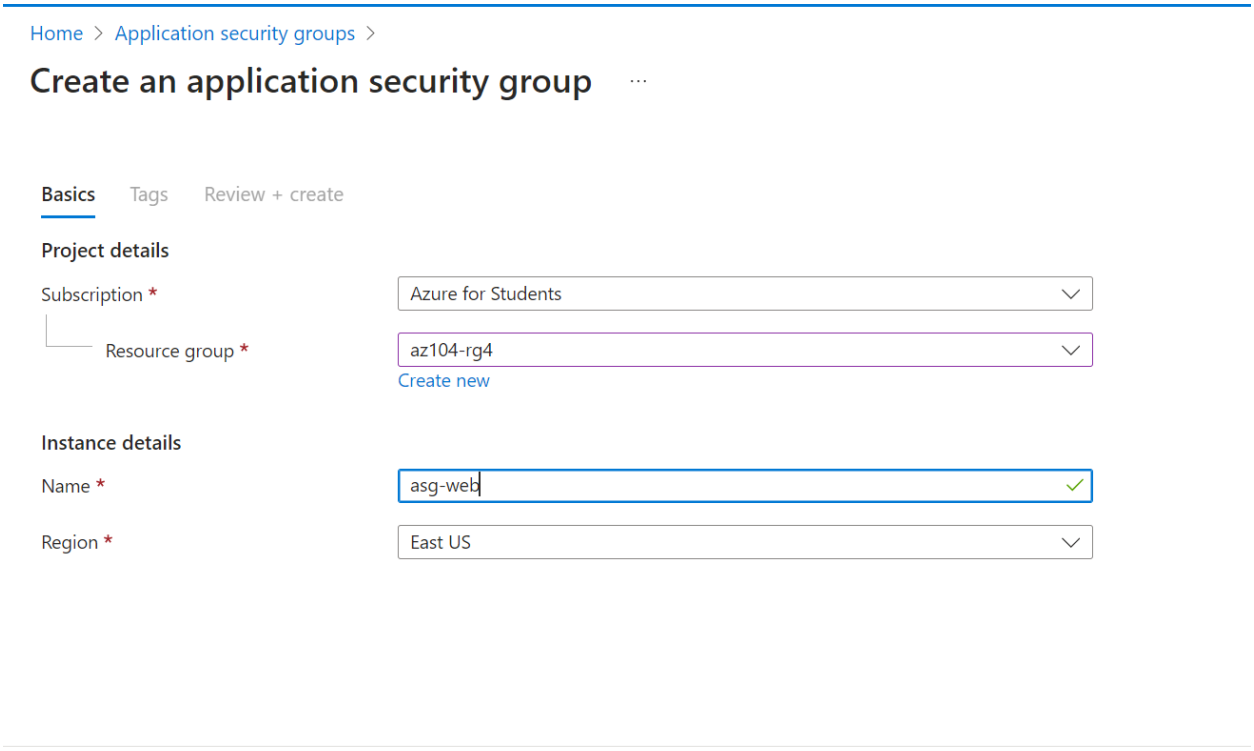
Task 3: Create and configure communication between an Application Security Group and a Network Security Group.

In this task, in involves creating an Application Security Group and a Network Security Group. The NSG has an inbound security rule that allows traffic from the ASG. The NSG will also

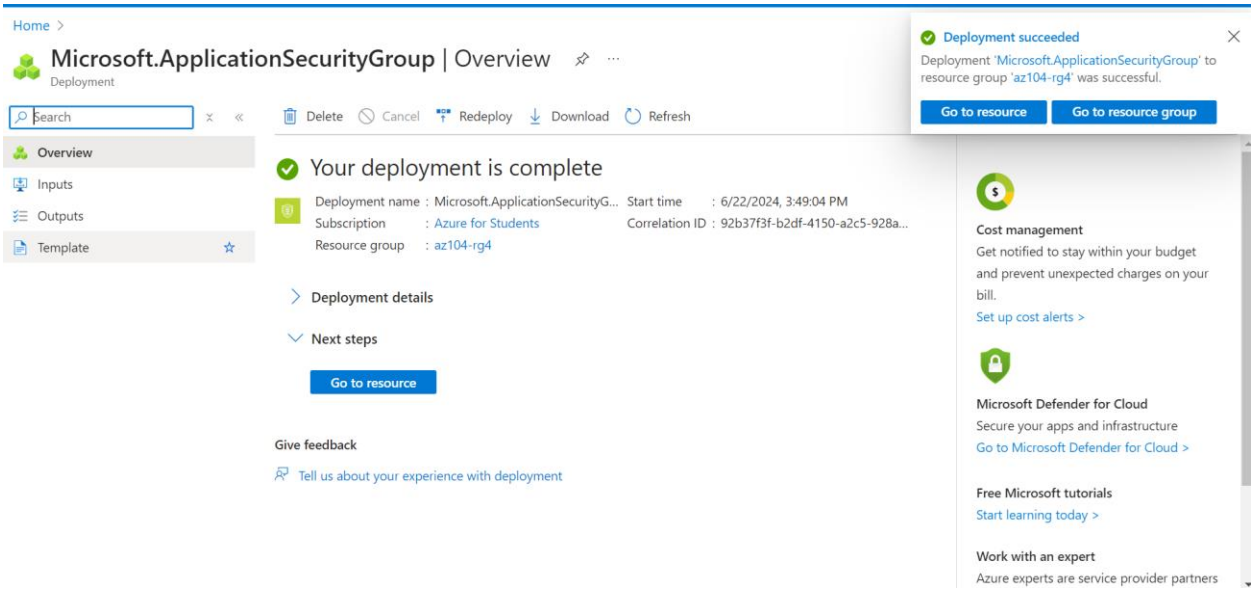
contain an outbound rule that denies access to the internet.it will also prevent your applications from illegal access and guarantee that your network is compliant and safe.

Instructions

- Create the Application Security Group (ASG)
- In the Azure portal, search for and select Application security groups.
- Click Create and provide the basic information.

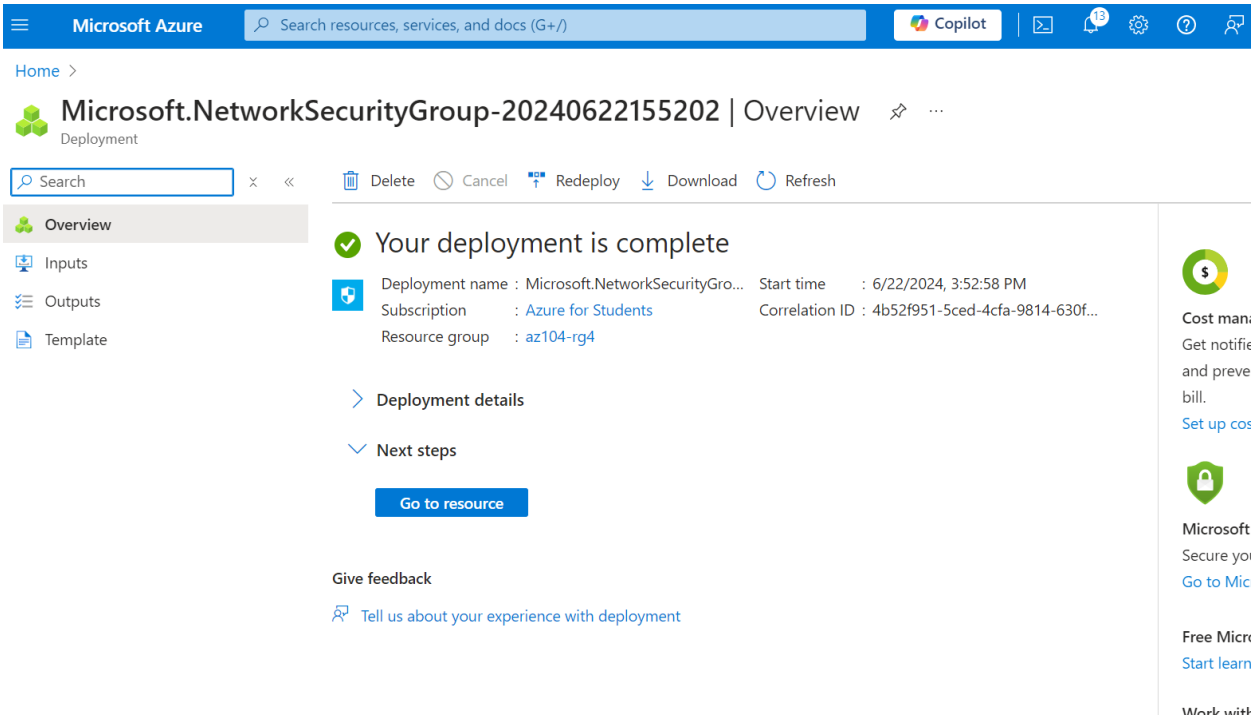


Click **Review + create** and then after the validation click **Create**.

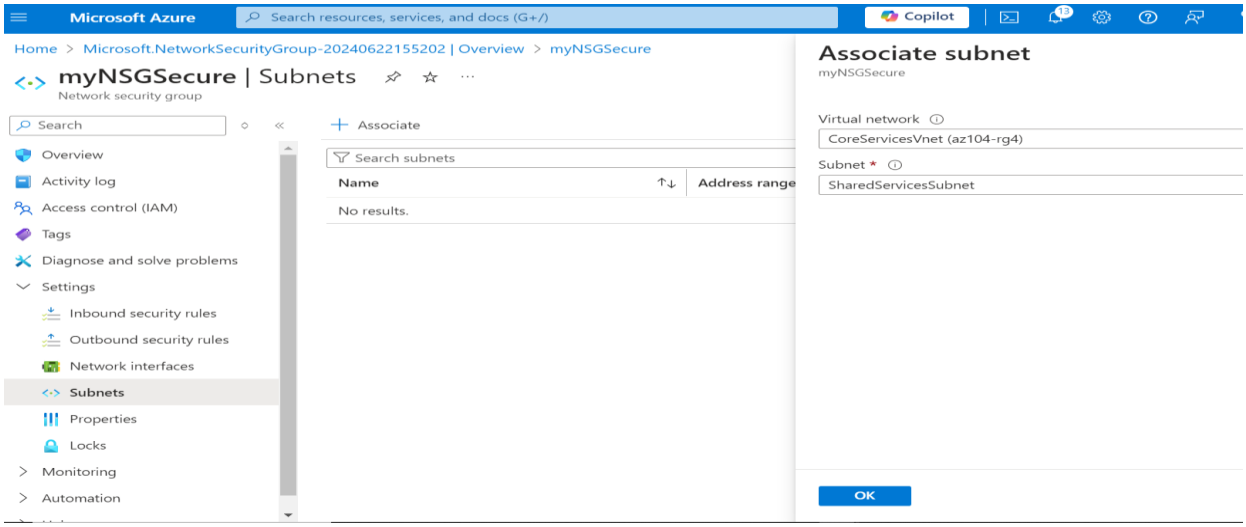


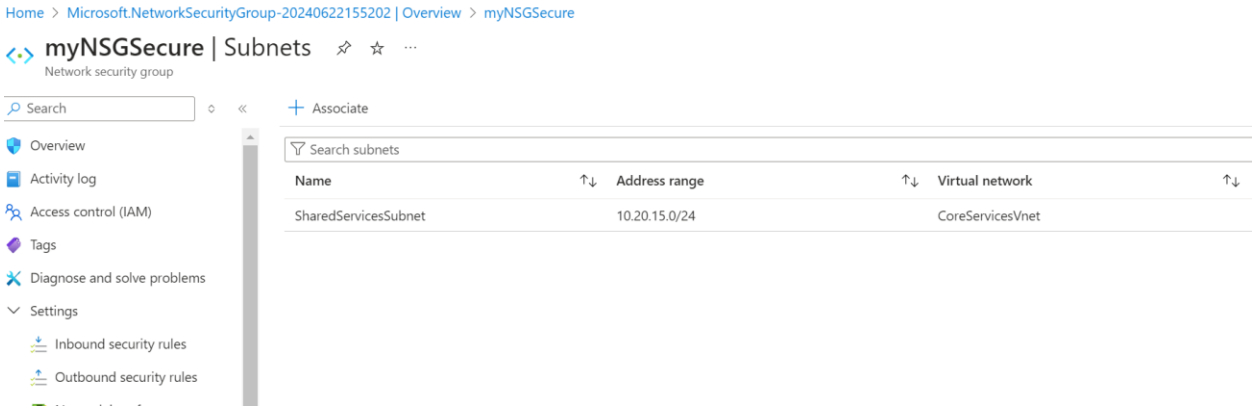
Create the Network Security Group and associate it with the ASG subnet

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



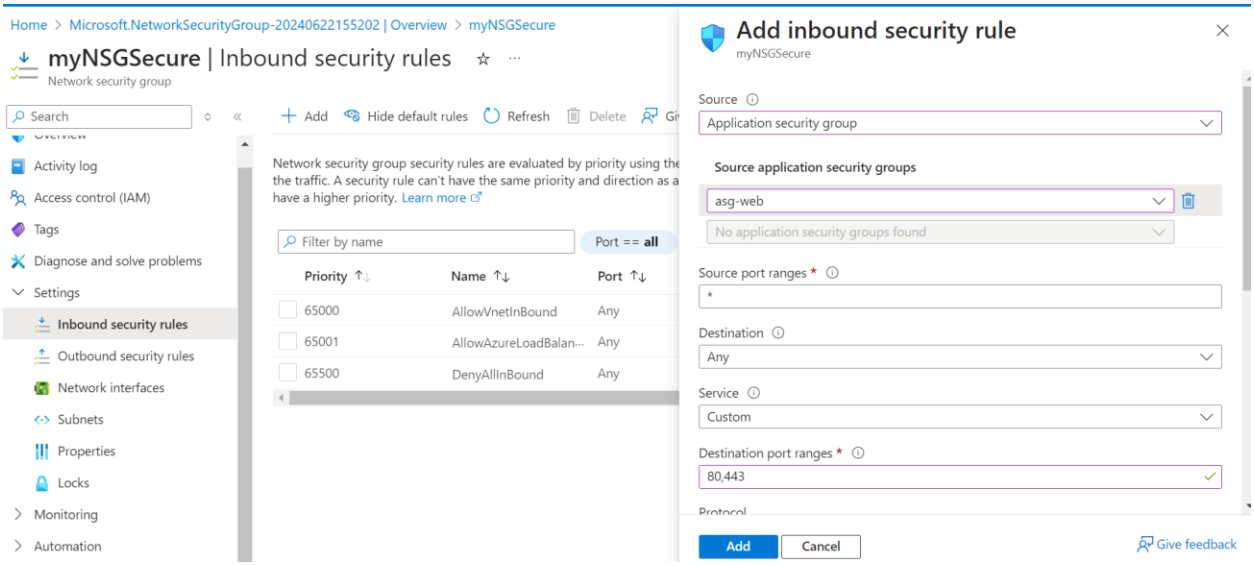
- After the NSG is deployed, click Go to resource.
- Under Settings click Subnets and then Associate.
- Click OK to save the association.



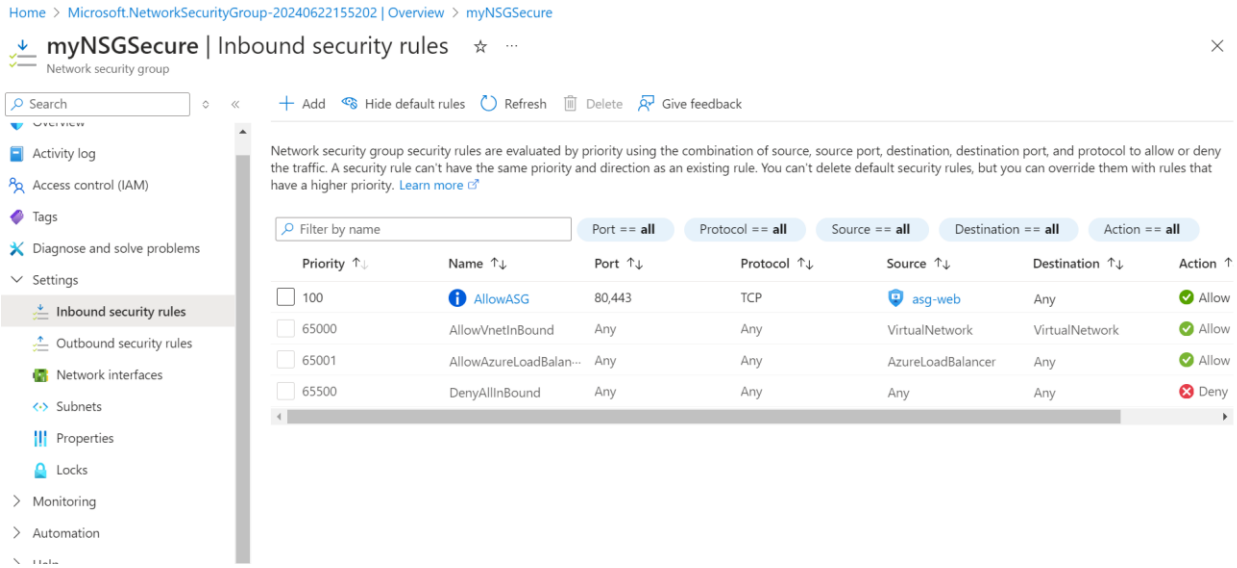


Configure an inbound security rule to allow ASG traffic

- Continue working with your NSG. In the Settings area, select Inbound security rules.
- Review the default inbound rules. Notice that only other virtual networks and load balancers are allowed access.

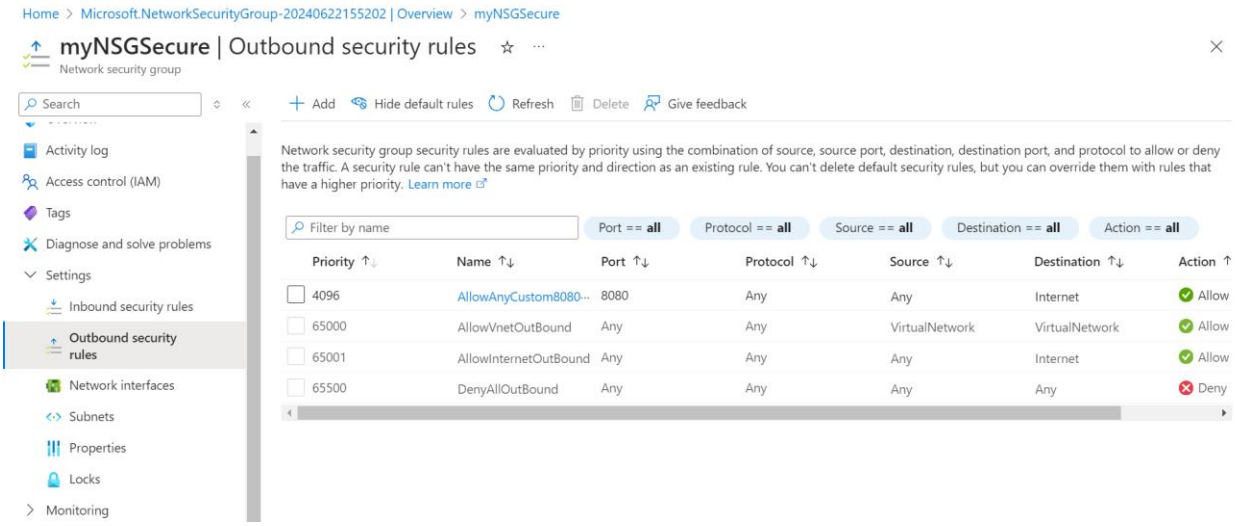


- Select + Add.
- On the Add inbound security rule blade, use the following information to add an inbound port rule. This rule allows ASG traffic. When you are finished, select Add.



Configure an outbound NSG rule that denies Internet access

- After creating your inbound NSG rule, select Outbound security rules.
- Notice the AllowInternetOutboundRule rule. Also notice the rule cannot be deleted and the priority is 65001.
- Select + Add and then configure an outbound rule that denies access to the internet. When you are finished, select Add

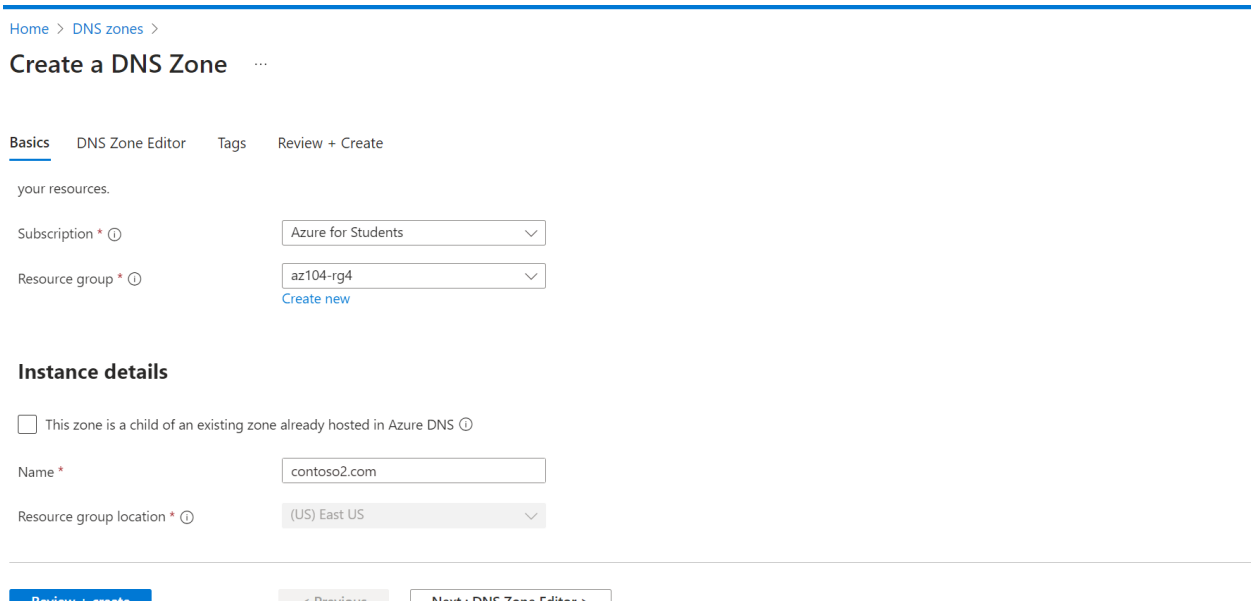


Task 4: Configure public and private Azure DNS zones

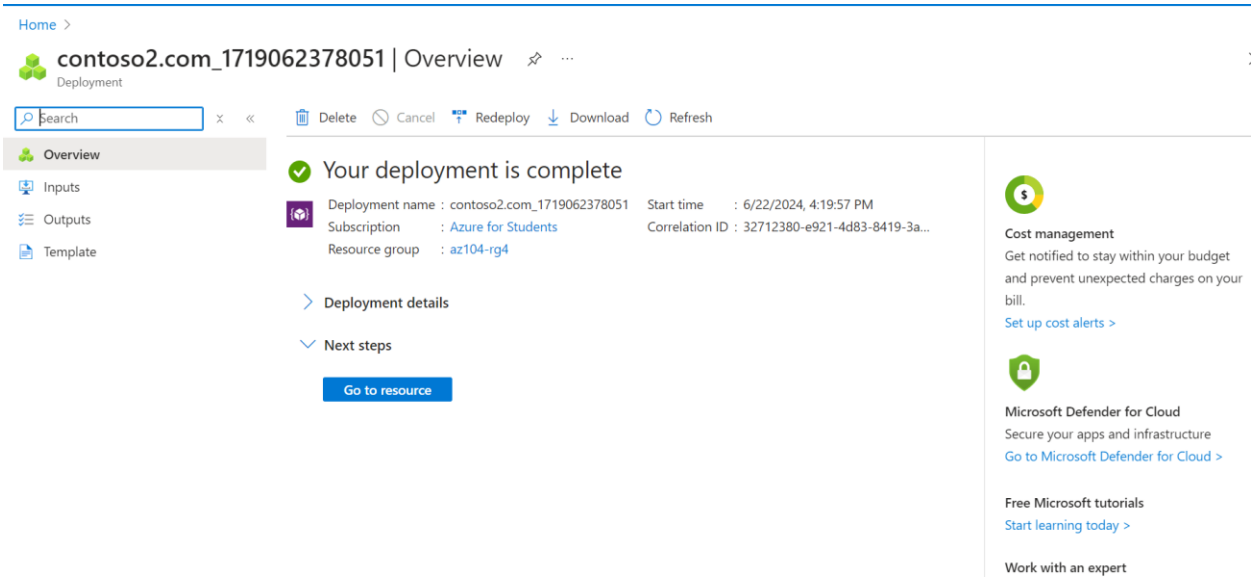
Azure Private DNS manages and resolves domain names in the virtual network without the need to configure a custom DNS solution. By using private DNS zones, you can use your own custom domain name instead of the Azure-provided names during deployment. In this task it involves configuring and maintaining domain name services to translate domain names to IP addresses and provide smooth access to the services and applications from inside avirtual network (VNet) as well as from outside the network.

Instructions

- In the portal, search for and select DNS zones.
- Select + Create.
- Configure the Basics tab.

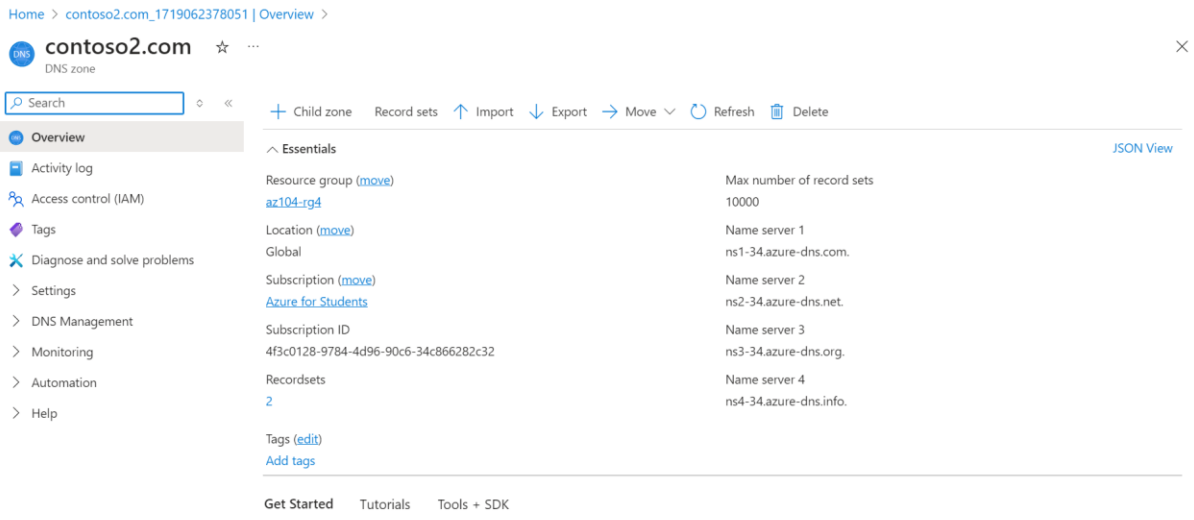


- Select Review create and then Create.

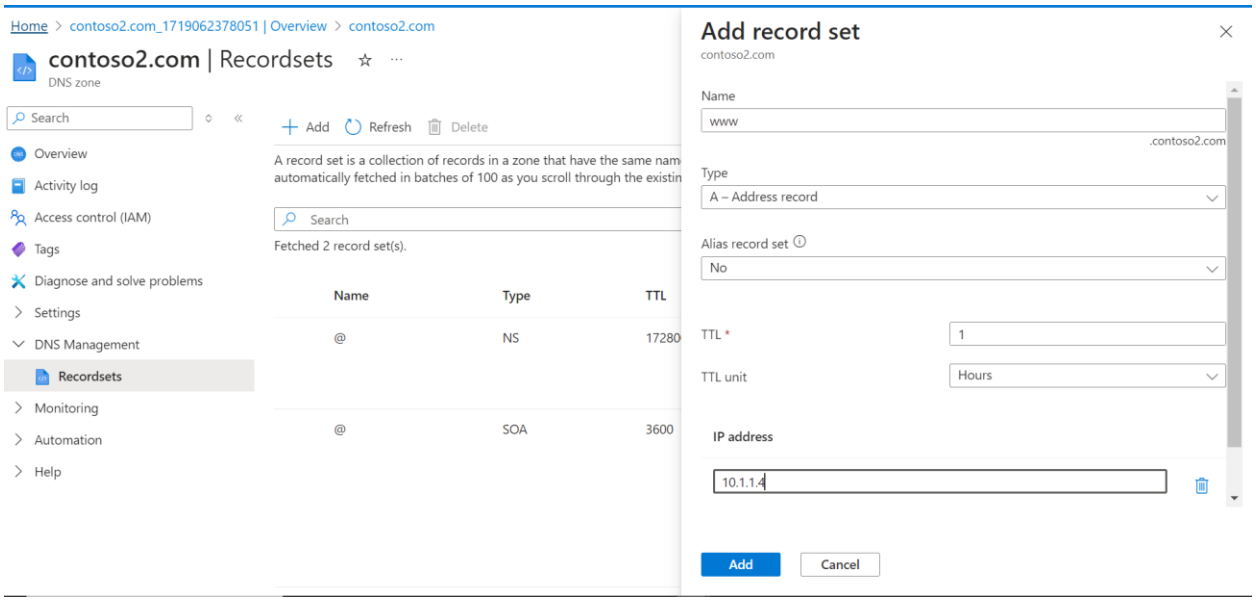


- Wait for the DNS zone to deploy and then select Go to resource.

- 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.



- Select + Record set. You add a virtual network link record for each virtual network that needs private name-resolution support



- Select OK and verify contoso.com has an A record set named www.
- Open a command prompt, and run the following command

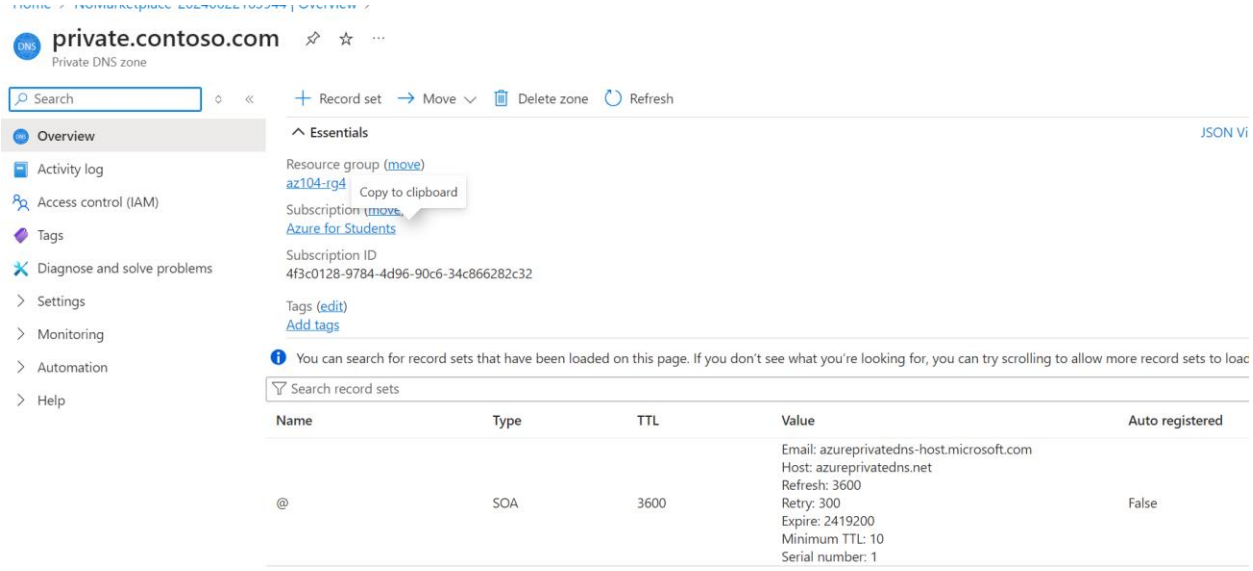
- Verify the host name www.contoso.com resolves to the IP address you provided. This confirms name resolution is working correctly.

Configuring a private DNS zone

A private DNS zone provides name resolution services within virtual networks. A private DNS zone is only accessible from the virtual networks that it is linked to and can't be accessed from the internet**.**

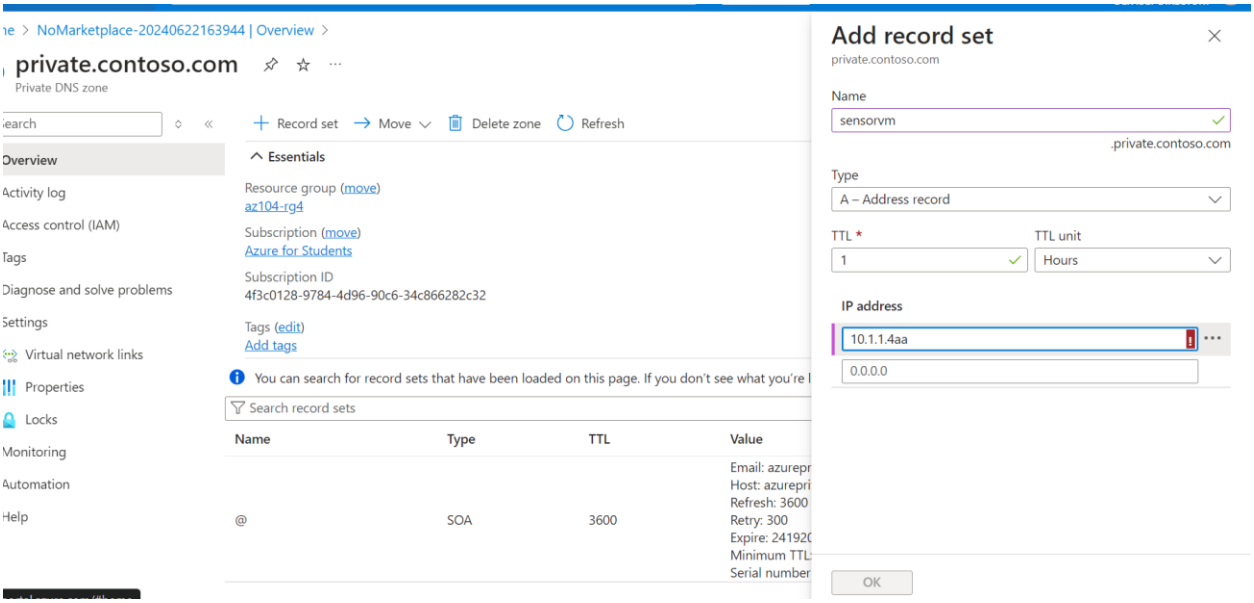
Steps

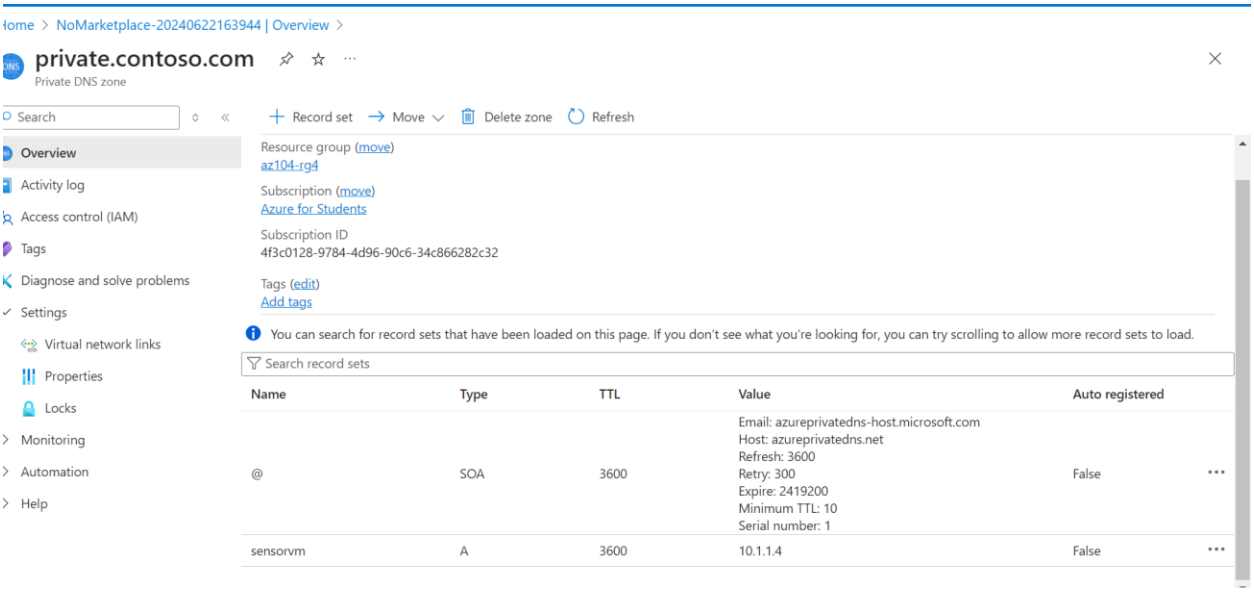
- In the portal, search for and select Private dns zones.
- Select + Create.
- On the Basics tab of Create private DNS zone, enter the information as listed in the table below:
- Select Review create and then Create.



- Select Review create and then Create.
- Wait for the DNS zone to deploy and then select Go to resource.
- Notice on the Overview blade there are no name server records.

- Select + Virtual network links and then select + Add
- Select OK and wait for the link to create.
- From the Overview blade select + Record set. You would now add a record for each virtual machine that needs private name-resolution support.





CONCLUTION

This report provides a detailed roadmap for setting up a robust and secure Azure networking environment, equipping cloud engineer with the skills to manage and scale cloud infrastructure effectively**.**