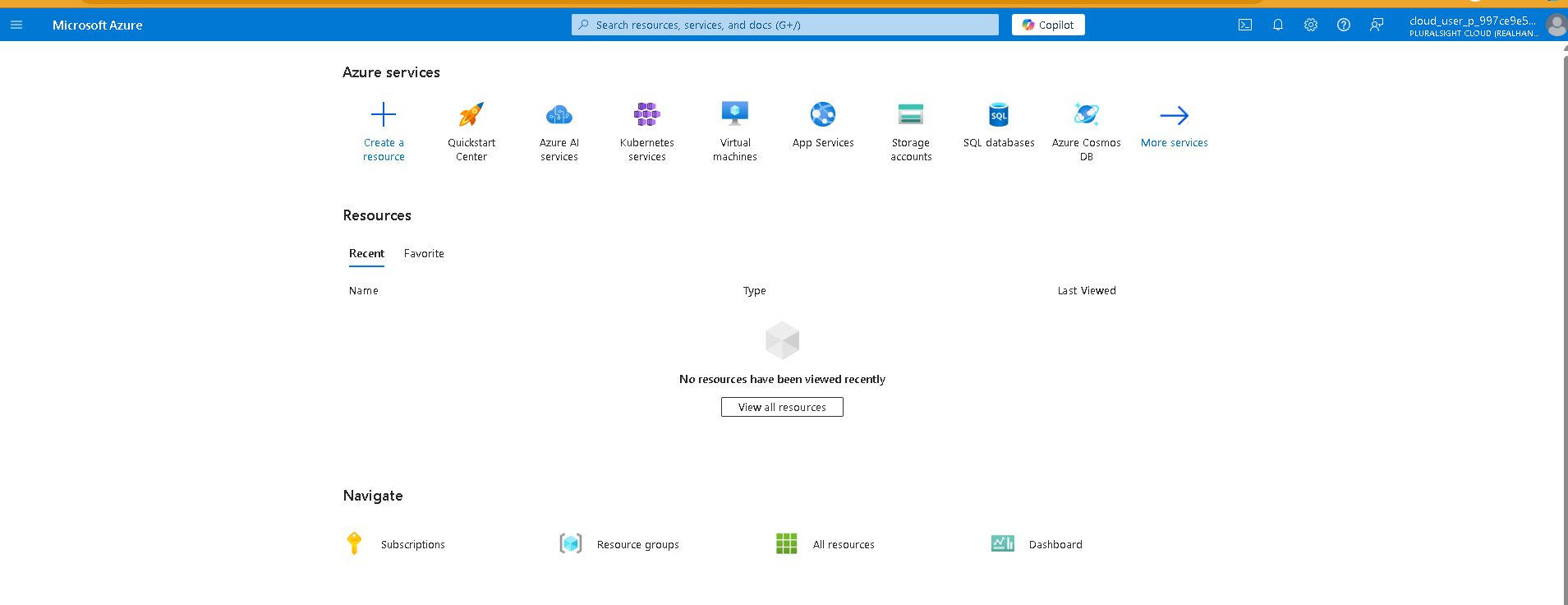
# Lab 04 - Implement Virtual Networking

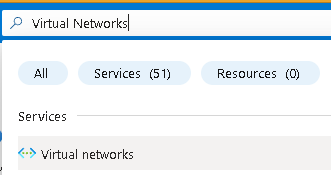
Made by Valeriy Manuilyk <3

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

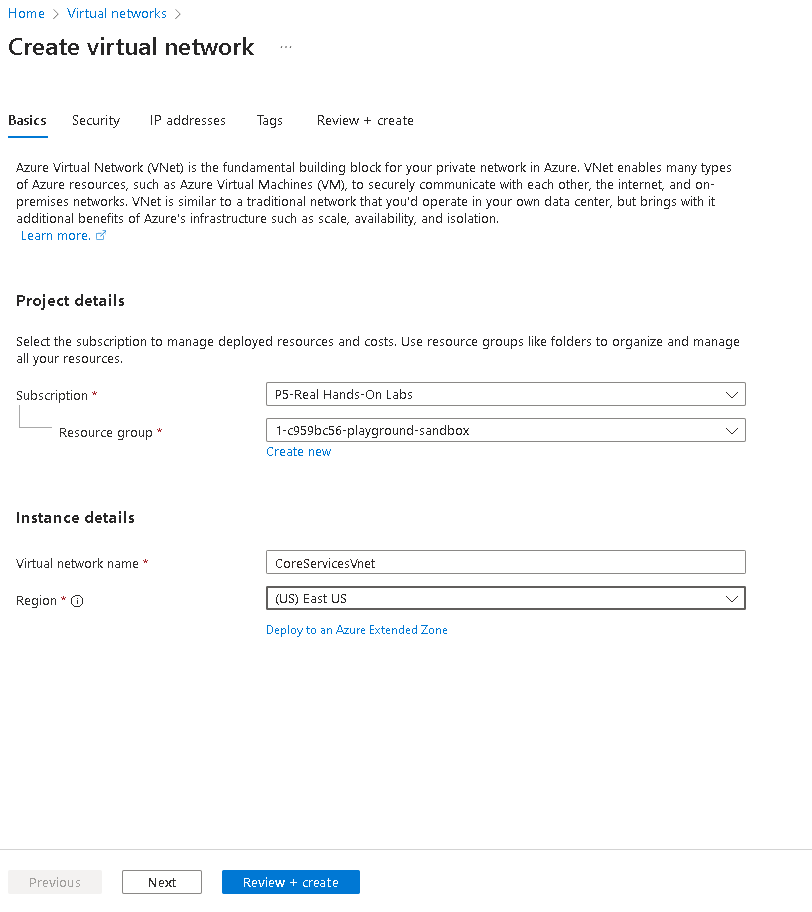
1.Sign in to the ****Azure portal**** - https://portal.azure.com.



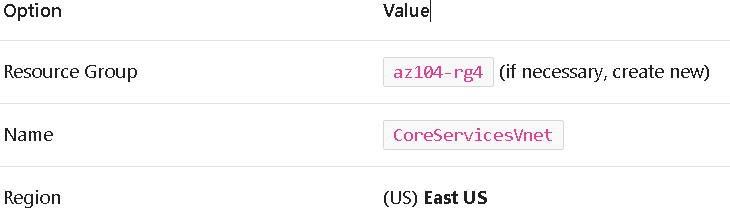
2.Search for and select Virtual Networks



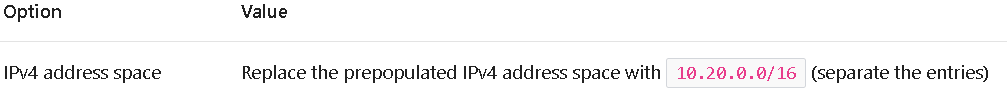
3.Select ****Create**** on the Virtual networks page.

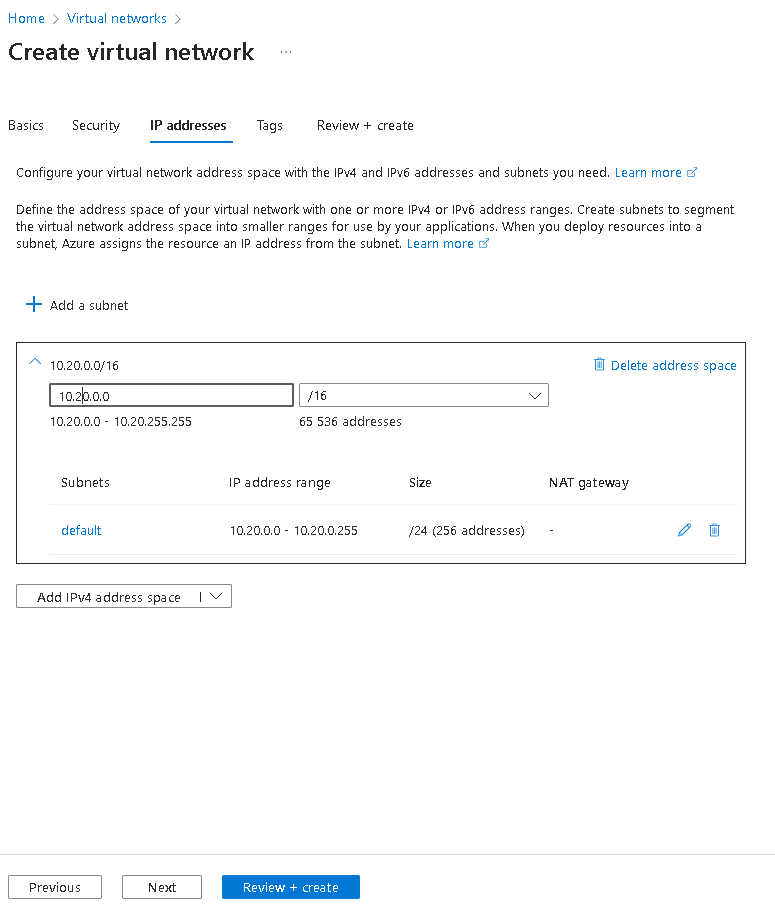


4.Complete the ****Basics**** tab for the CoreServicesVnet.

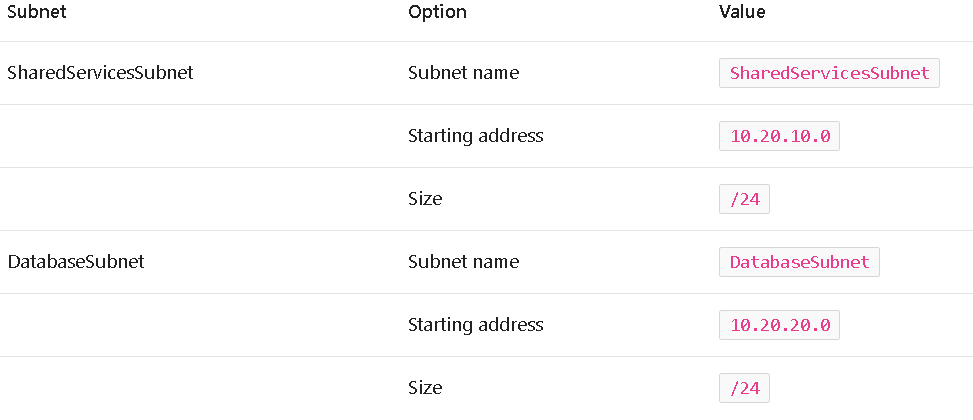


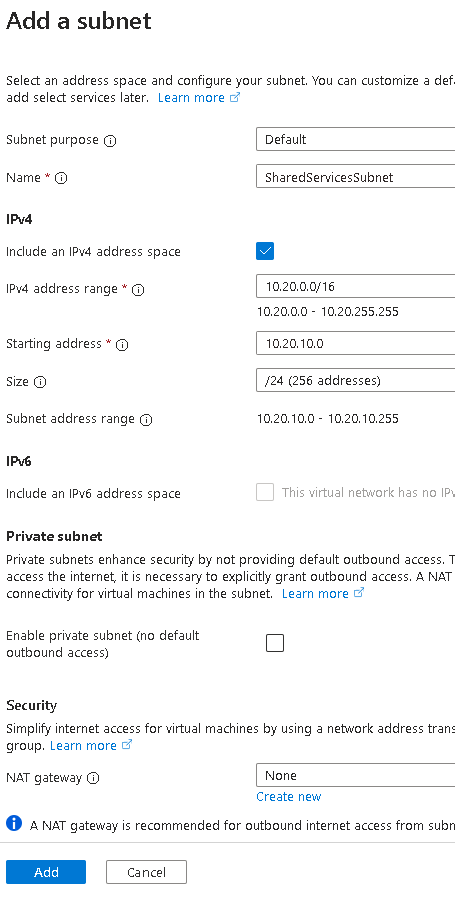
5.Move to the ****IP Addresses**** tab.

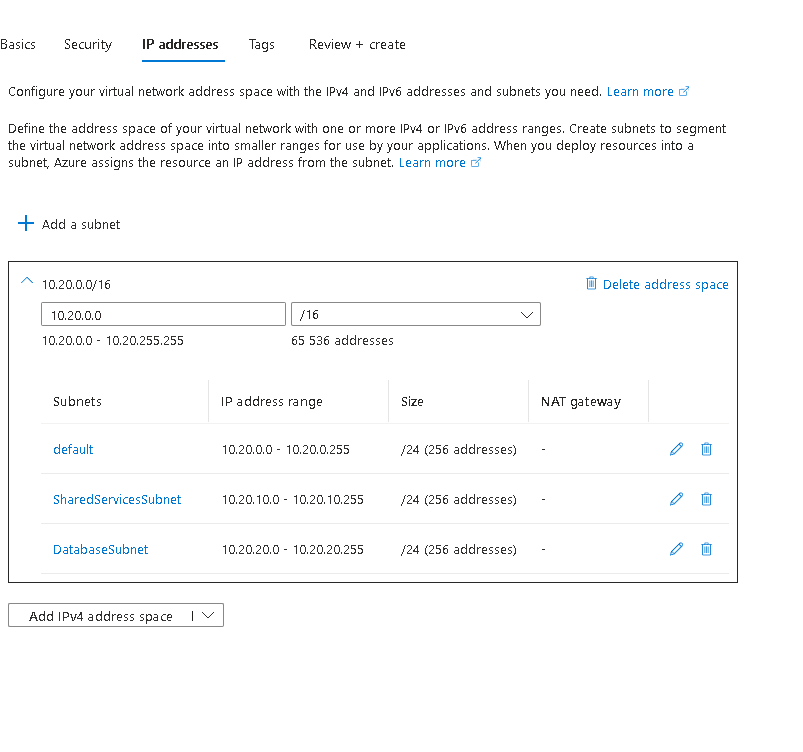




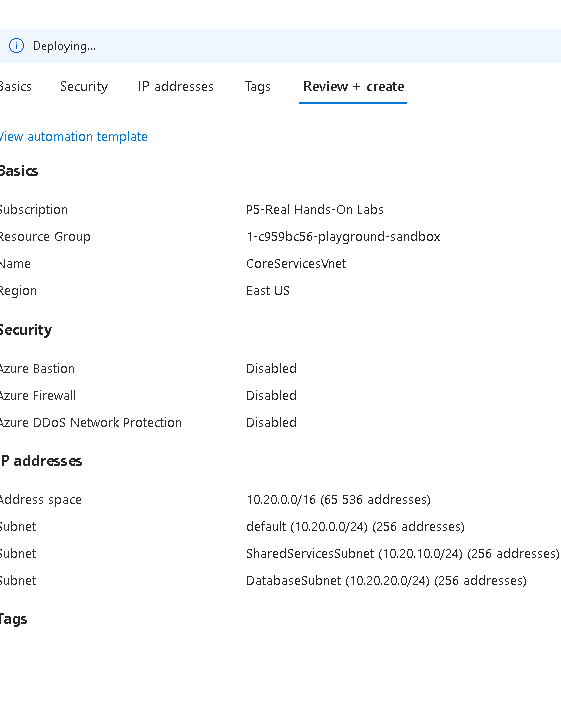
6.Select ****+ Add a subnet****. Complete the name and address information for each subnet. Be sure to select ****Add**** for each new subnet. Be sure to delete the default subnet - either before or after creating the other subnets.



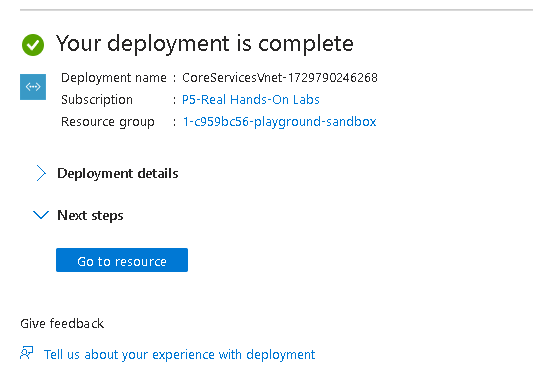




1. To finish creating the CoreServicesVnet and its associated subnets, select ****Review + create****.

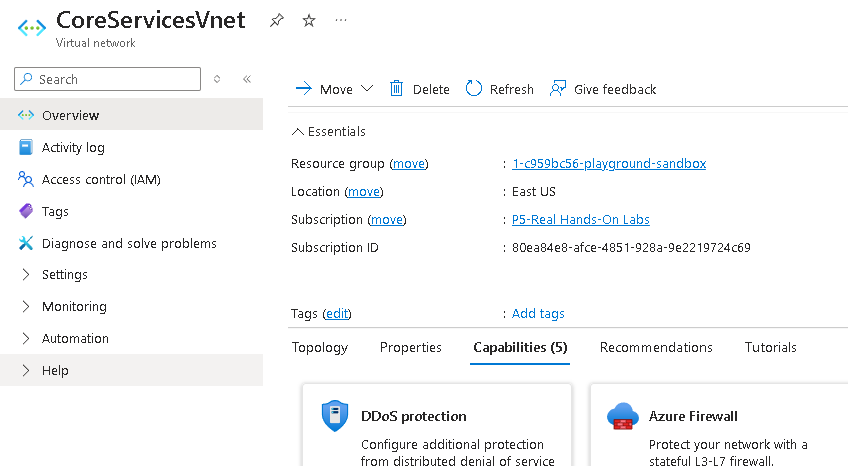


8.Verify your configuration passed validation, and then select ****Create****.

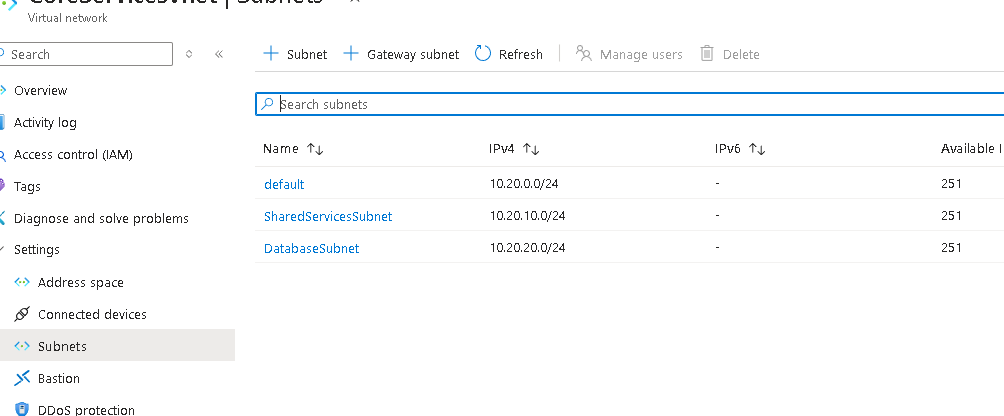


9.Wait for the virtual network to deploy and then select ****Go to resource****.

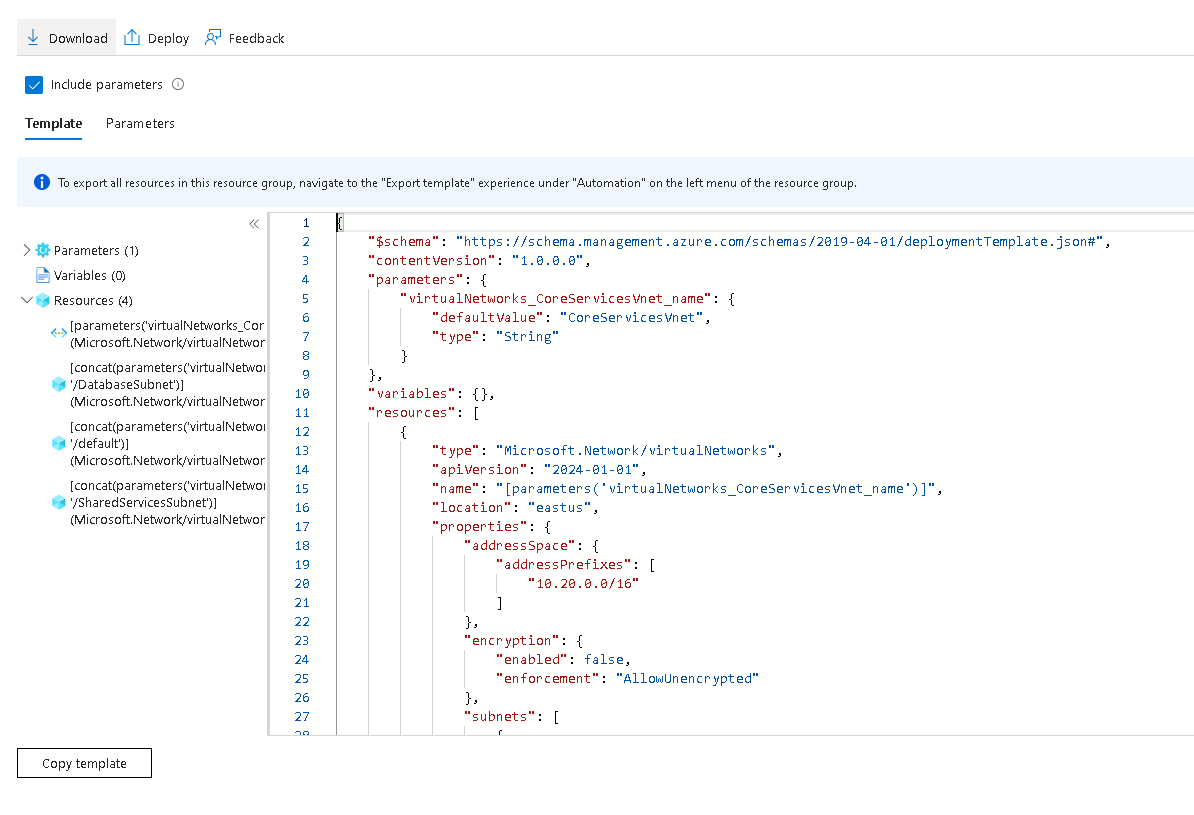




10.Take a minute to verify the ****Address space**** and the ****Subnets****. Notice your other choices in the ****Settings**** blade.



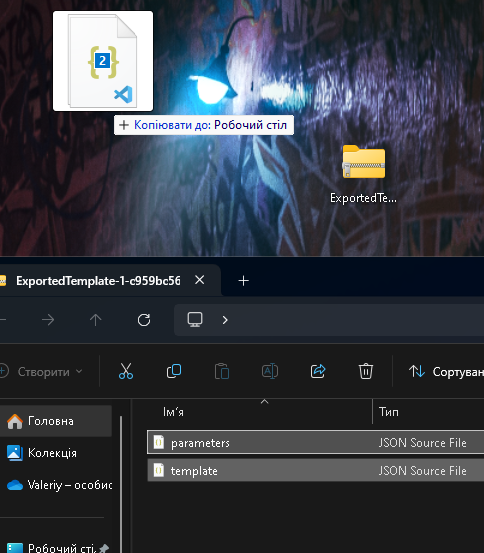
1. In the ****Automation**** section, select ****Export template****, and then wait for the template to be generated.



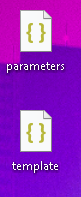
**12.**Download**** the template.



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



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

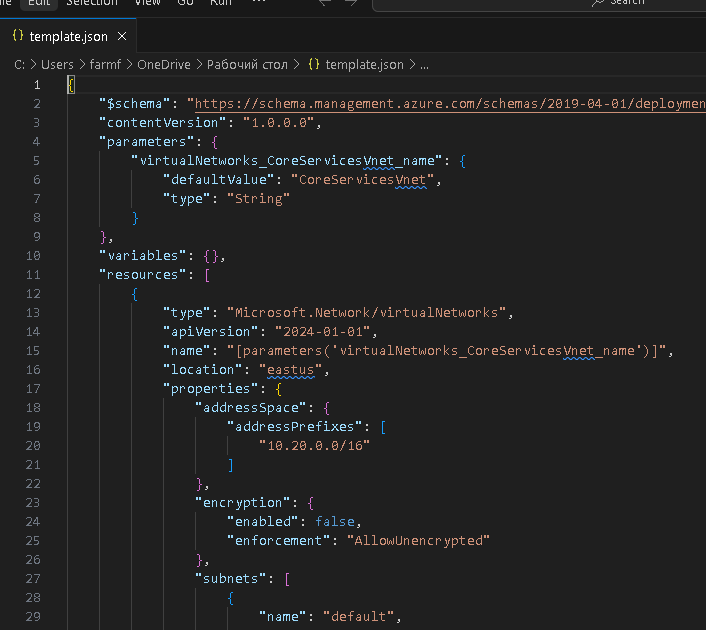


## Task 2: Create a virtual network and subnets using a template

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.



### Make changes for the ManufacturingVnet virtual network

3.Replace all occurrences of ****CoreServicesVnet**** with ManufacturingVnet.

4.Replace all occurrences of ****10.20.0.0**** with 10.30.0.0.

### Make changes for the ManufacturingVnet subnets

5.Change all occurrences of ****SharedServicesSubnet**** to SensorSubnet1.

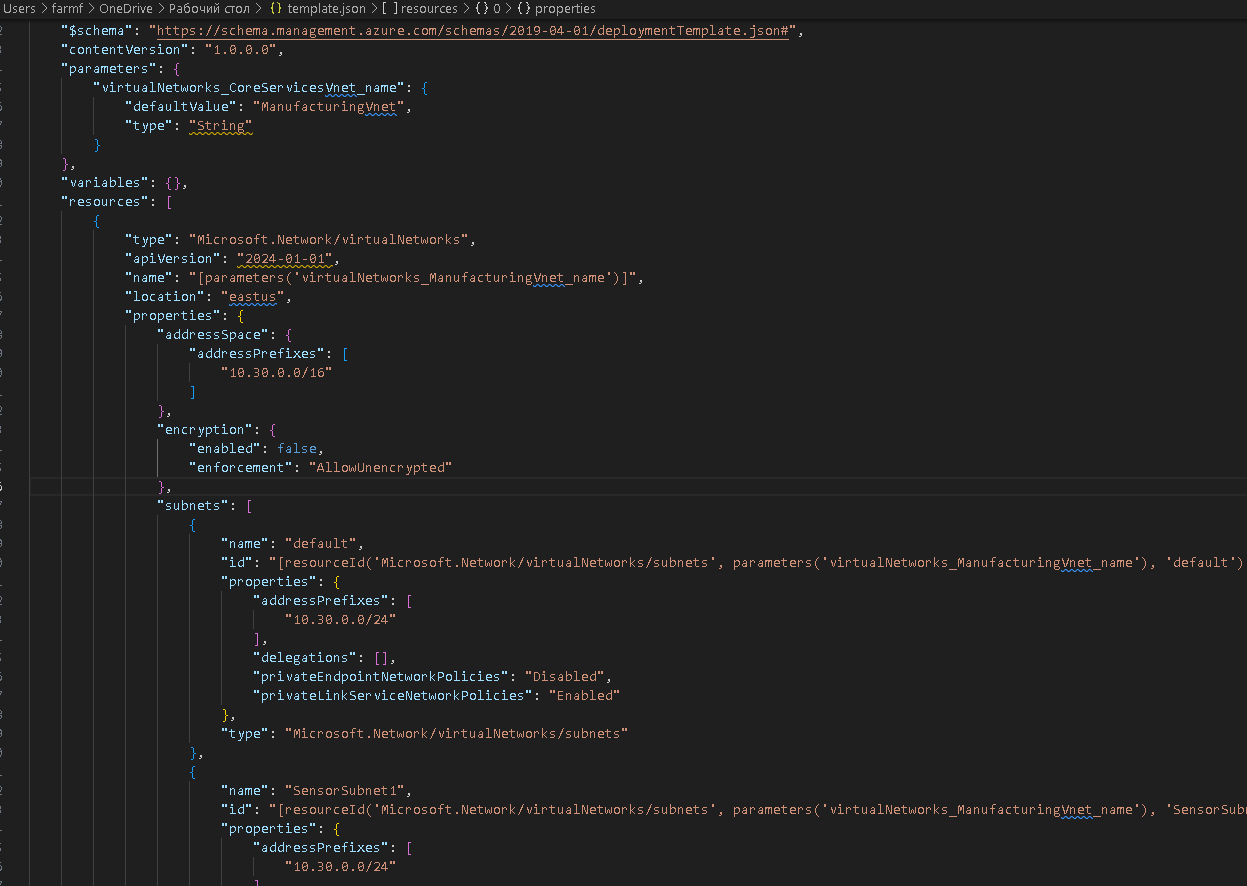
6.Change all occurrences of ****10.20.10.0/24**** to 10.30.20.0/24

7.Change all occurrences of ****DatabaseSubnet**** to SensorSubnet2.

8.Change all occurrences of ****10.20.20.0/24**** to 10.30.21.0/24.

9.Read back through the file and ensure everything looks correct.

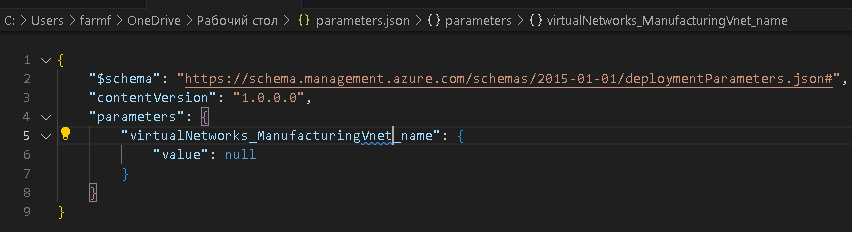
10.Be sure to ****Save**** your changes.



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

12.Edit the file using the editor of your choice.

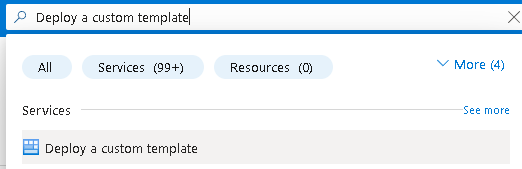
13.Replace the one occurrence of ****CoreServicesVnet**** with ManufacturingVnet.



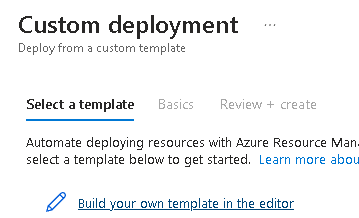
**14.**Save**** your changes.

### Deploy the custom template

1. In the portal, search for and select ****Deploy a custom template****.



16.Select ****Build your own template in the editor**** and then ****Load file****.



17.Select the ****templates.json**** file with your Manufacturing changes, then select ****Save****.



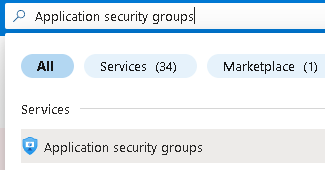
18.Select ****Review + create**** and then ****Create****.

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

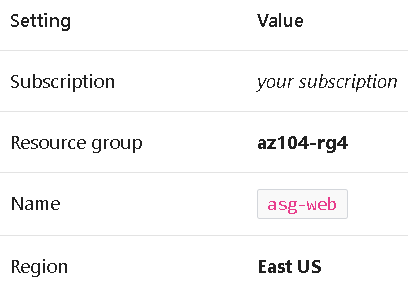


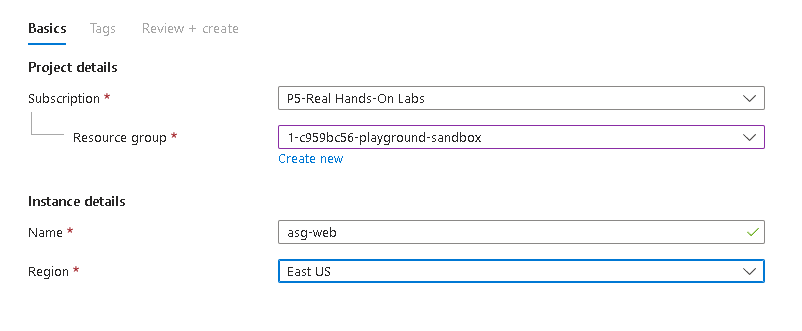
## Task 3: Create and configure communication between an Application Security Group and a Network Security Group

1.In the Azure portal, search for and select Application security groups.

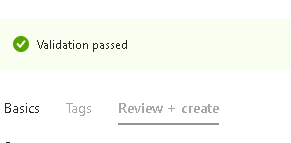


2.Click ****Create**** and provide the basic information.





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

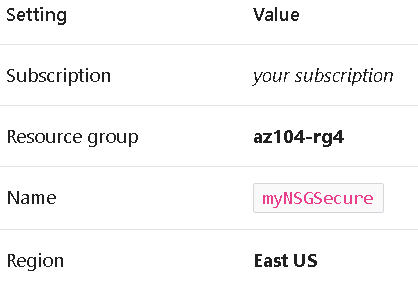


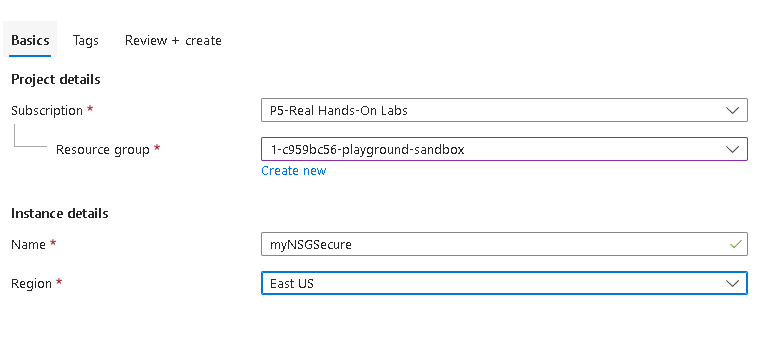
### Create the Network Security Group and associate it with the ASG subnet

4.In the Azure portal, search for and select Network security groups.

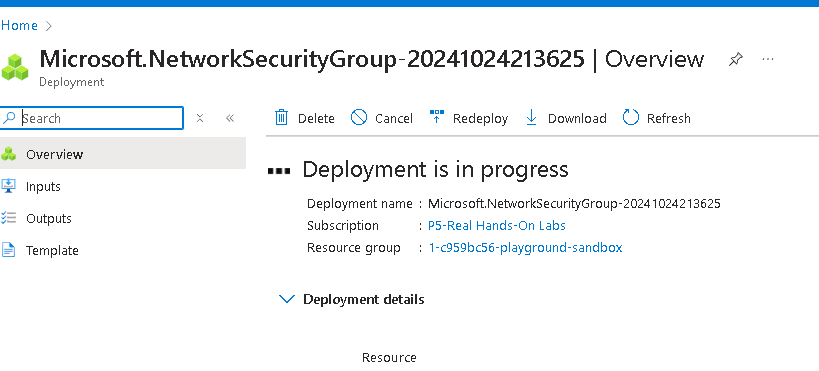


5.Select ****+ Create**** and provide information on the ****Basics**** tab

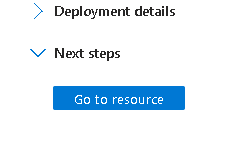




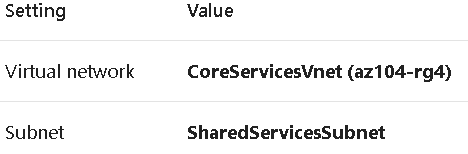
6.Click ****Review + create**** and then after the validation click ****Create****.

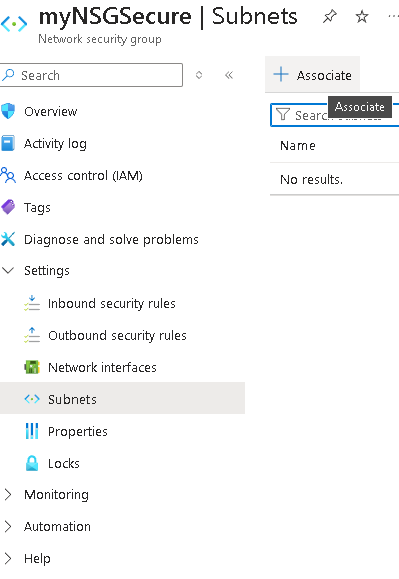


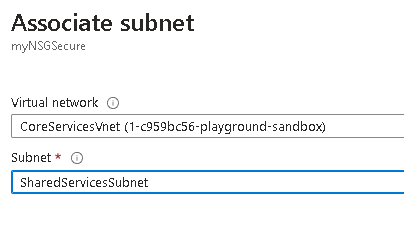
7.After the NSG is deployed, click ****Go to resource****.



8.Under ****Settings**** click ****Subnets**** and then ****Associate****.



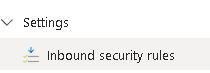




9.Click ****OK**** to save the association.

### Configure an inbound security rule to allow ASG traffic

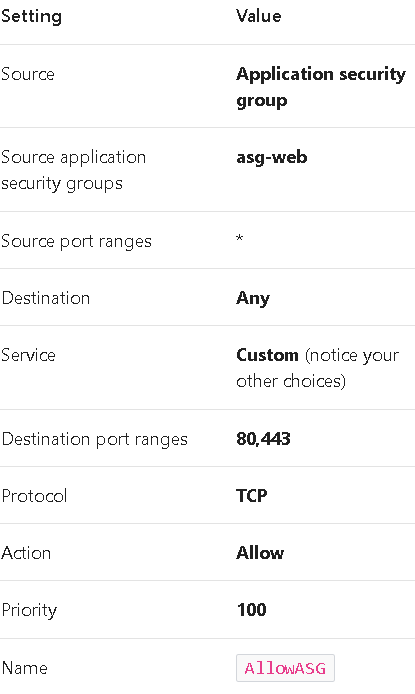
10.Continue working with your NSG. In the ****Settings**** area, select ****Inbound security rules****.

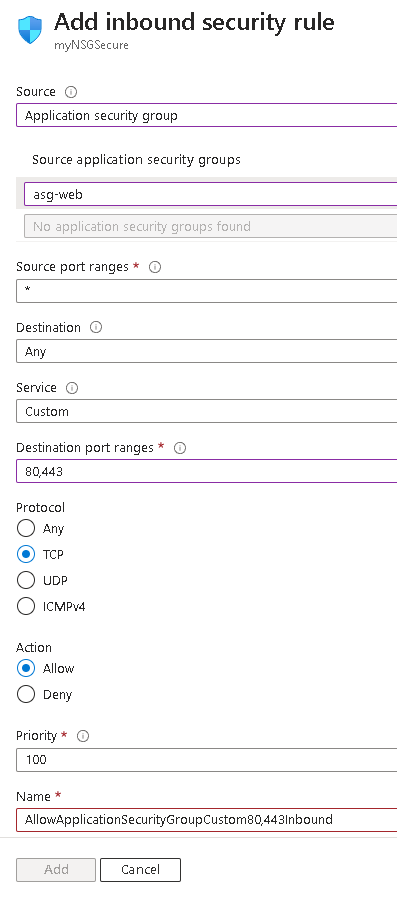


11.Review the default inbound rules. Notice that only other virtual networks and load balancers are allowed access.

12.Select ****+ Add****.

13.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

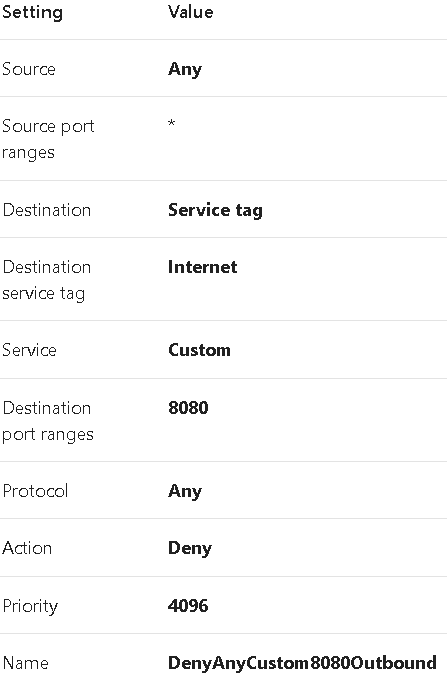
1. After creating your inbound NSG rule, select ****Outbound security rules****.

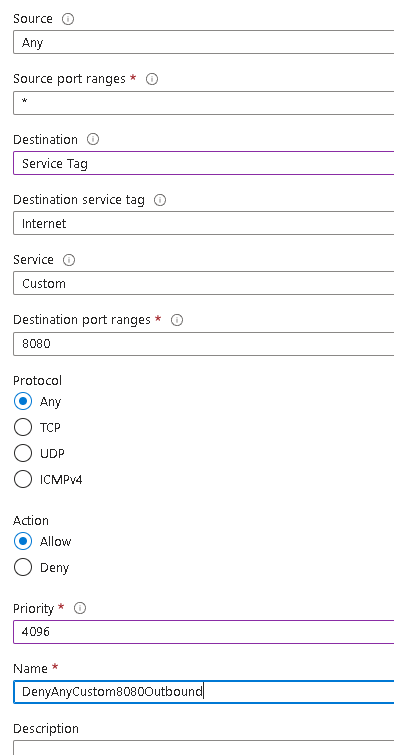


15.Notice the ****AllowInternetOutboundRule**** rule. Also notice the rule cannot be deleted and the priority is 65001.



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

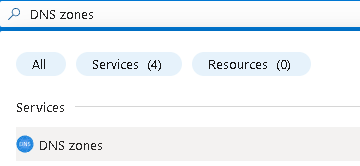






## Task 4: Configure public and private Azure DNS zones

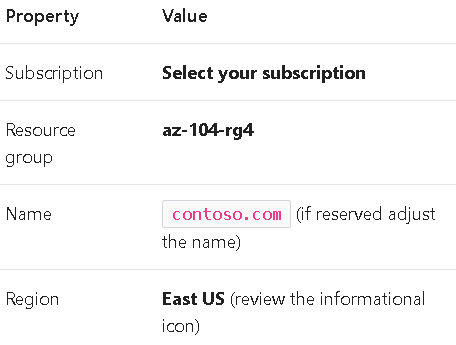
1.In the portal, search for and select DNS zones.

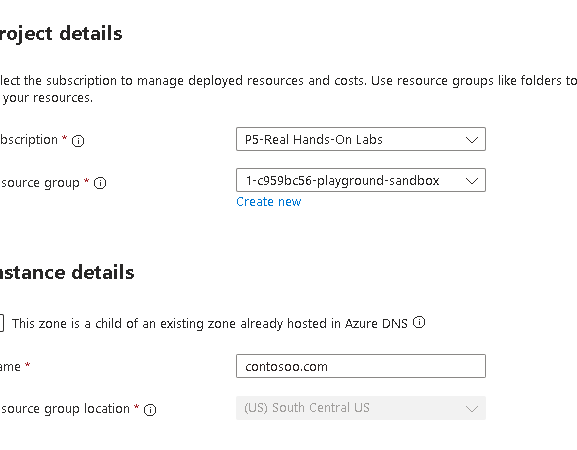


2.Select ****+ Create****.

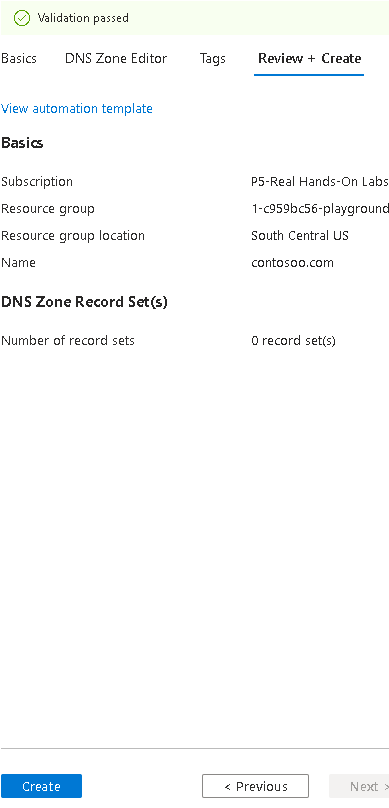


3.Configure the ****Basics**** tab.

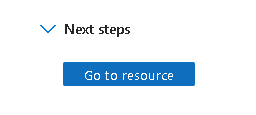




4.Select ****Review create**** and then ****Create****.

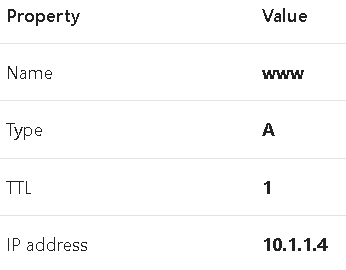


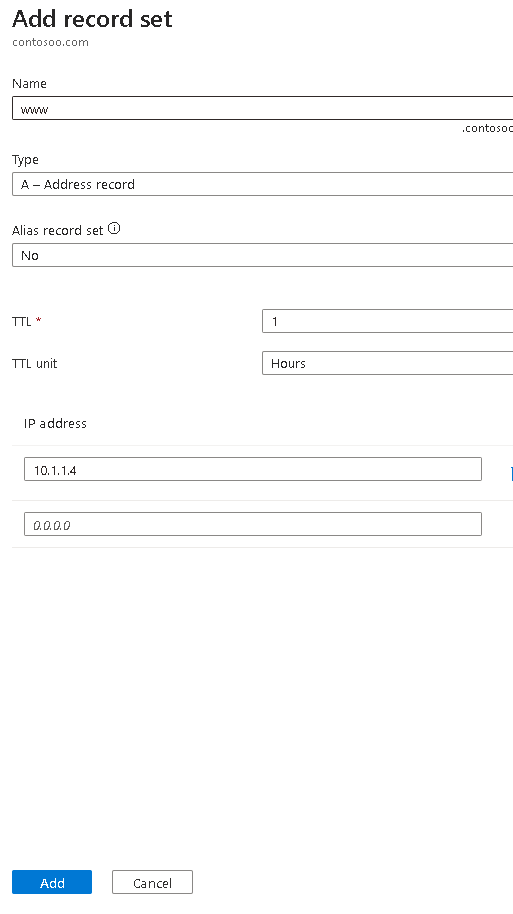
5.Wait for the DNS zone to deploy and then select ****Go to resource****



6.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.

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





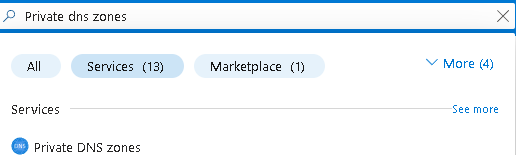
8.Select ****OK**** and verify ****contoso.com**** has an A record set named ****www****.

9.Open a command prompt, and run the following command:

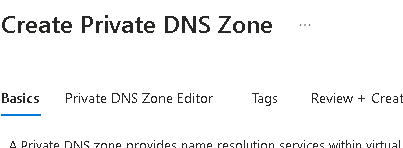
10.Verify the host name www.contoso.com resolves to the IP address you provided. This confirms name resolution is working correctly.

### Configure a private DNS zone

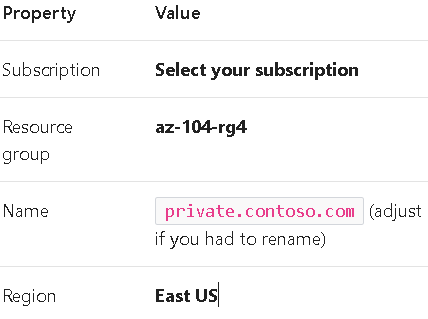
1.In the portal, search for and select Private dns zones.

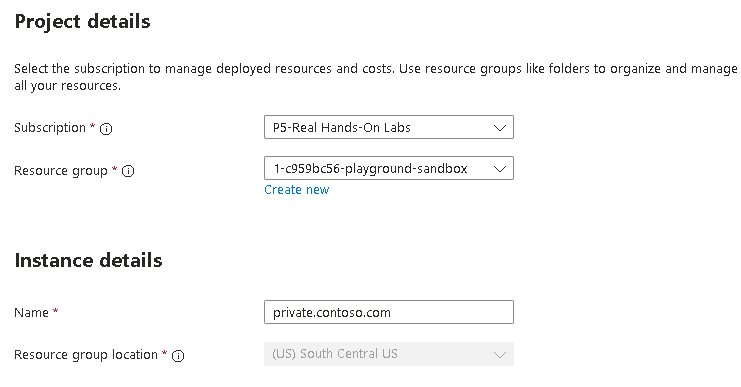


2.Select ****+ Create****.

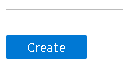


3.On the ****Basics**** tab of Create private DNS zone, enter the information as listed in the table below:

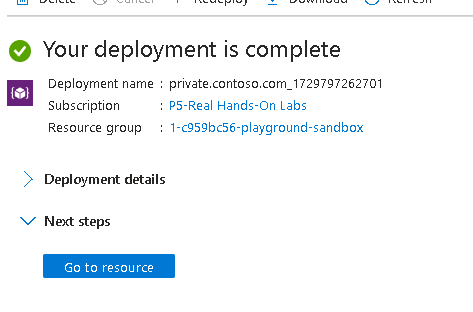




4.Select ****Review create**** and then ****Create****.

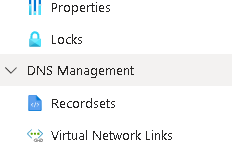


5.Wait for the DNS zone to deploy and then select ****Go to resource****



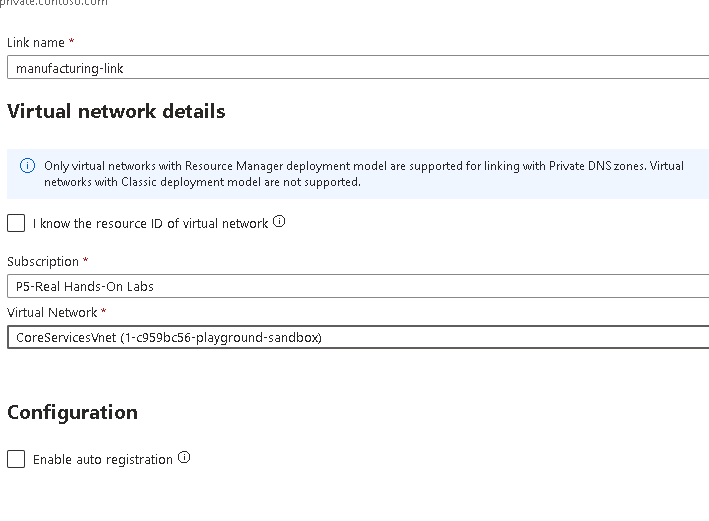
6.Notice on the ****Overview**** blade there are no name server records.

7.Select ****Settings**** and then ****DNS Management****.



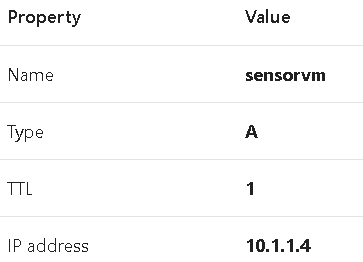
8.Select ****Virtual network links**** and configure the link.

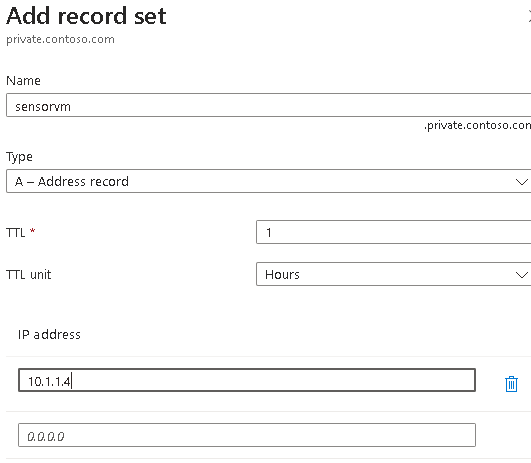




9.Select ****Create**** and wait for the link to create.

10.From the ****Overview**** blade select ****+ Record set****. You would now add a record for each virtual machine that needs private name-resolution support.





**Сonclusion:**

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.