# Azure Virtual Networks

## **Tutorial**

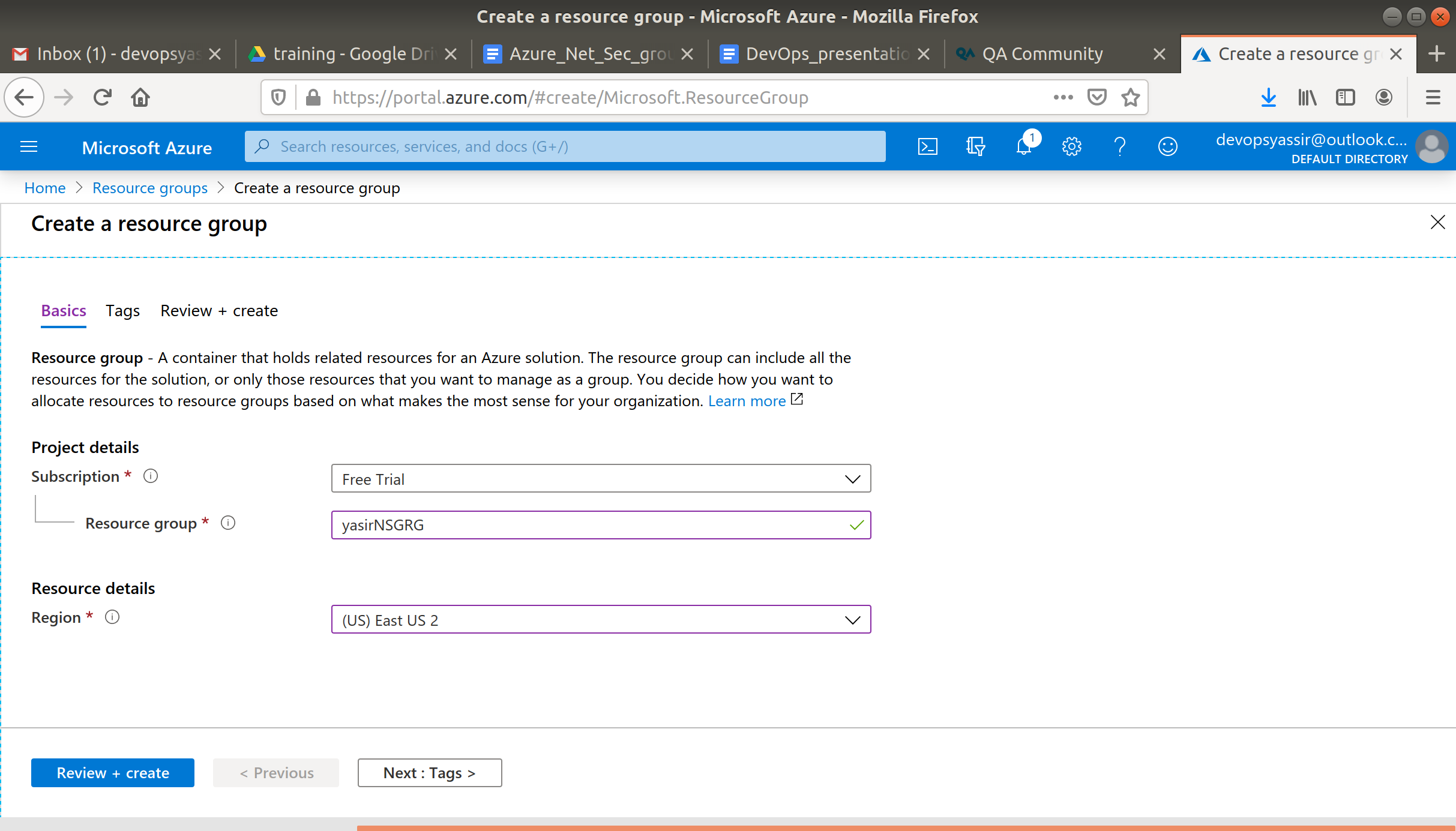
In this tutorial we will create and modify rules with an NSG that is associated with a virtual machine..

### **New Resource Group**

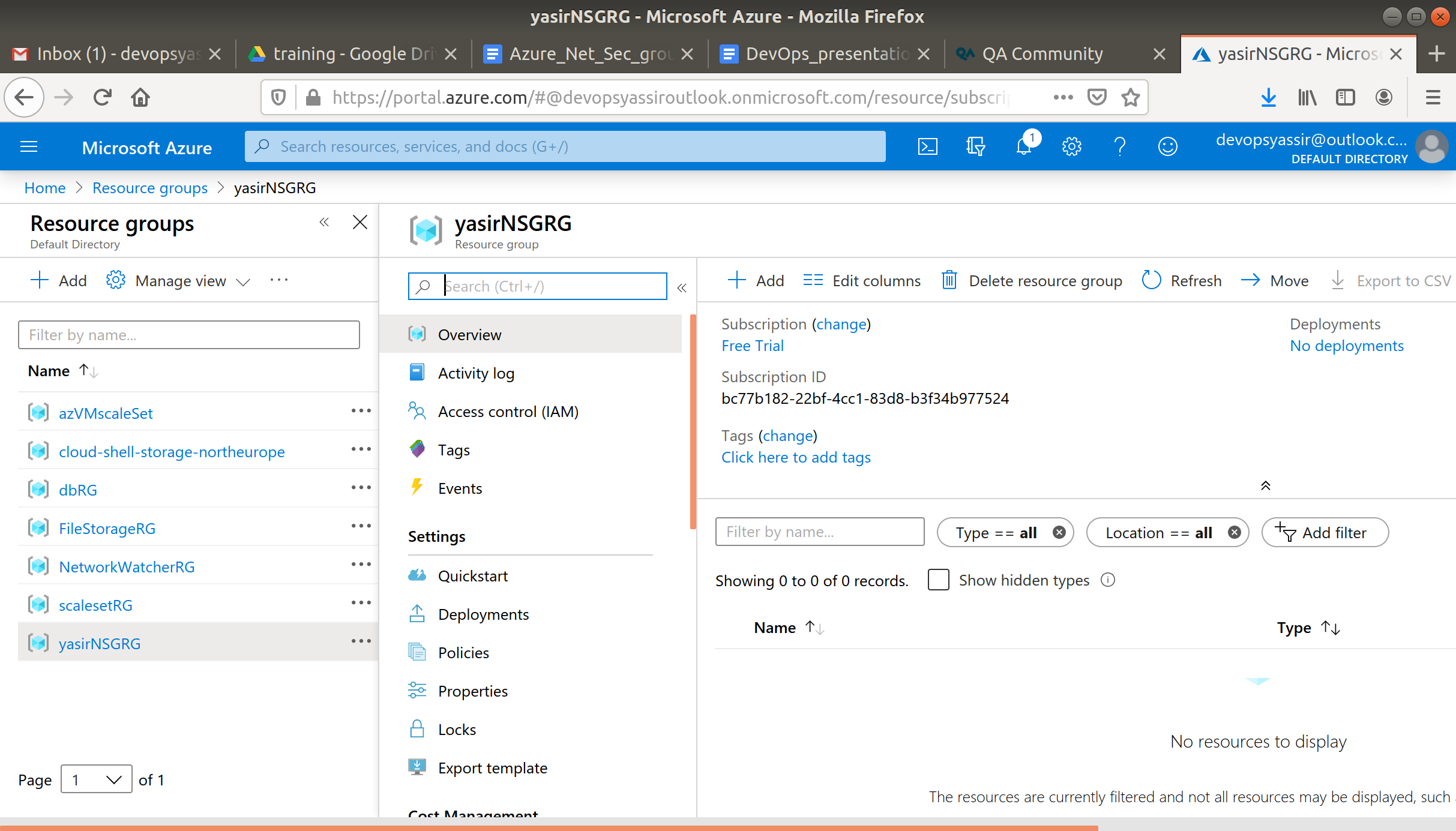
The first thing is to create a new resource group, which we can do by clicking the burger bar in the top left corner and choosing Resource groups:

Then, we can click +Add:

Here, we can name the resource group and pick a location to have it in:



Lastly, we will click Review & Create and then Create to create the resource group:



### **New Virtual Machine**

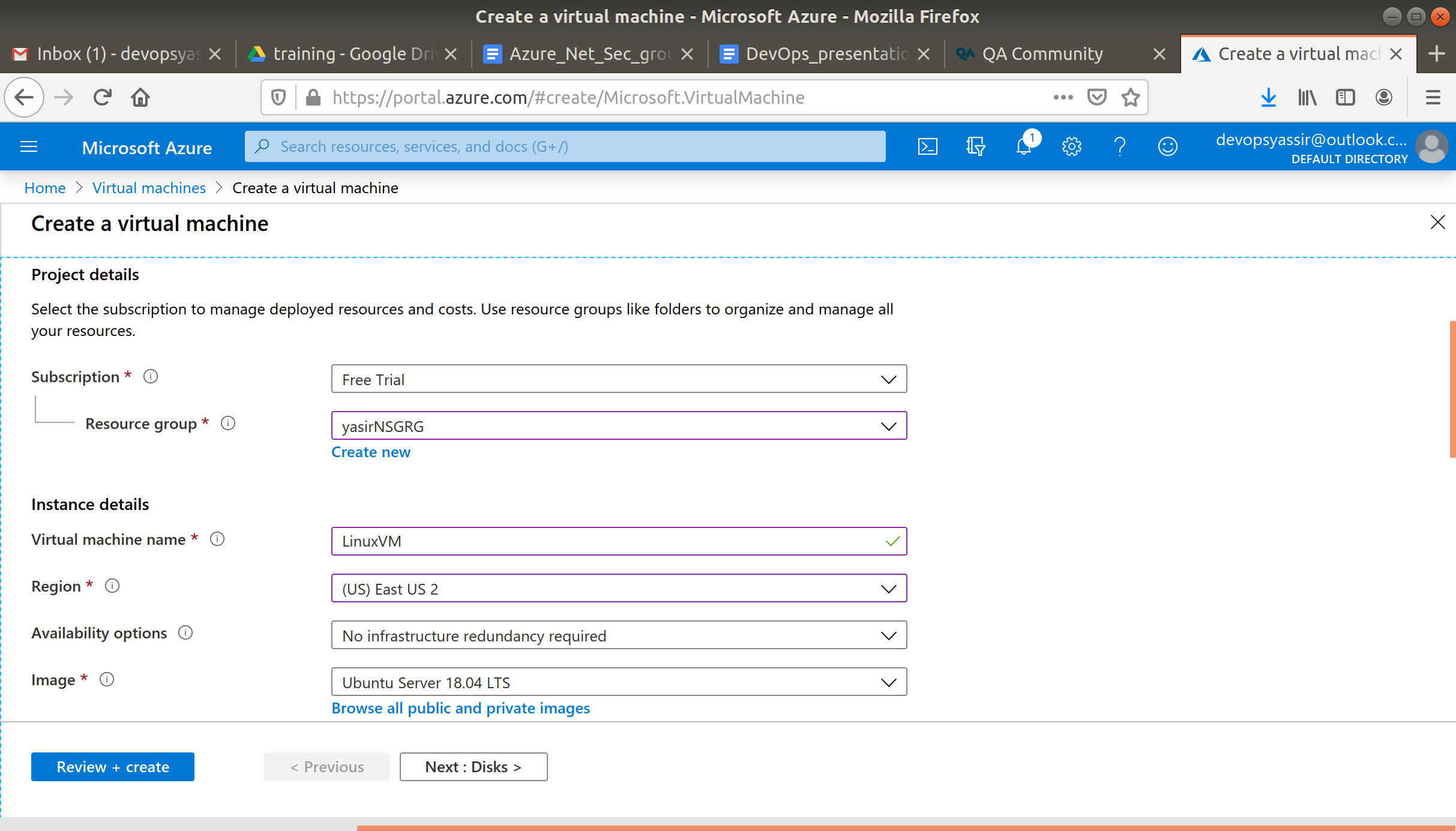
For this, we need to first go to the hamburger menu again, but this time click Virtual machines:

Then, we click + Add:

We will need to choose our new resource group from the drop down menu, give the machine a name and pick a region for it to be deployed into.

The image can be Ubuntu Server 18.04 LTS, and the Size can be Standard D2s v3:

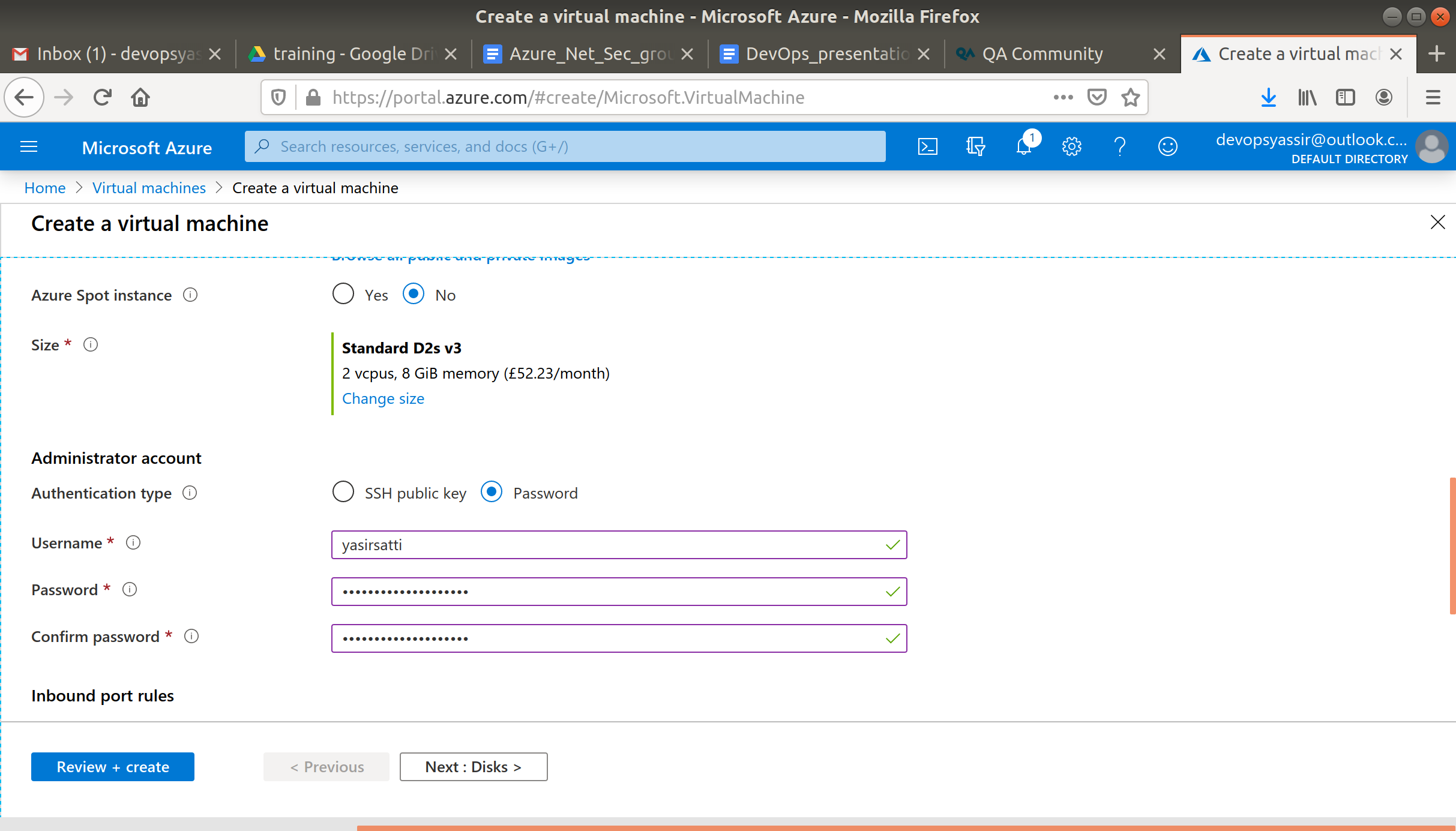
We need to choose password for authentication type, and create a username and password.

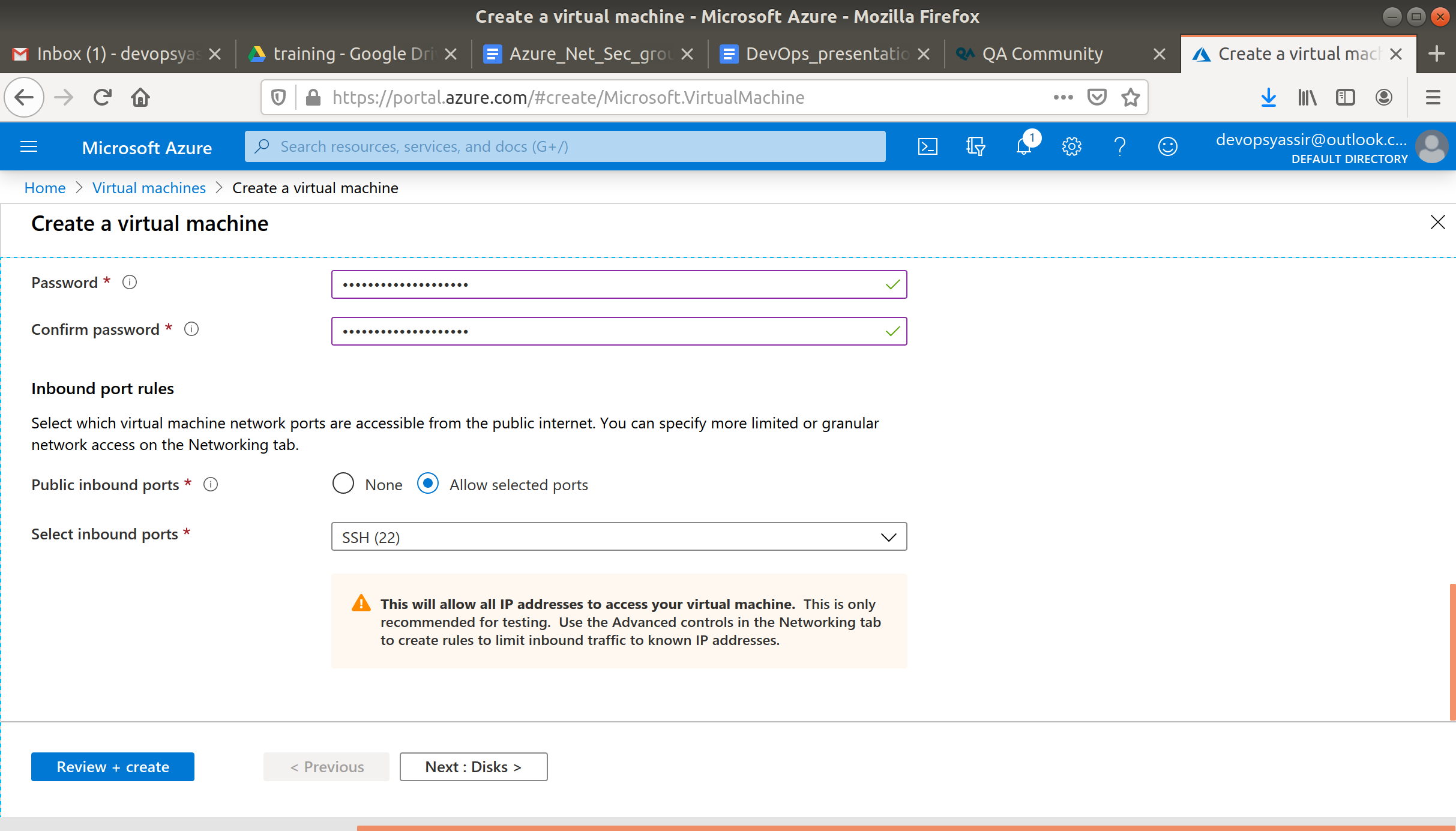


Under the Allow Selected Ports section. You should be able to see a dropdown menu.

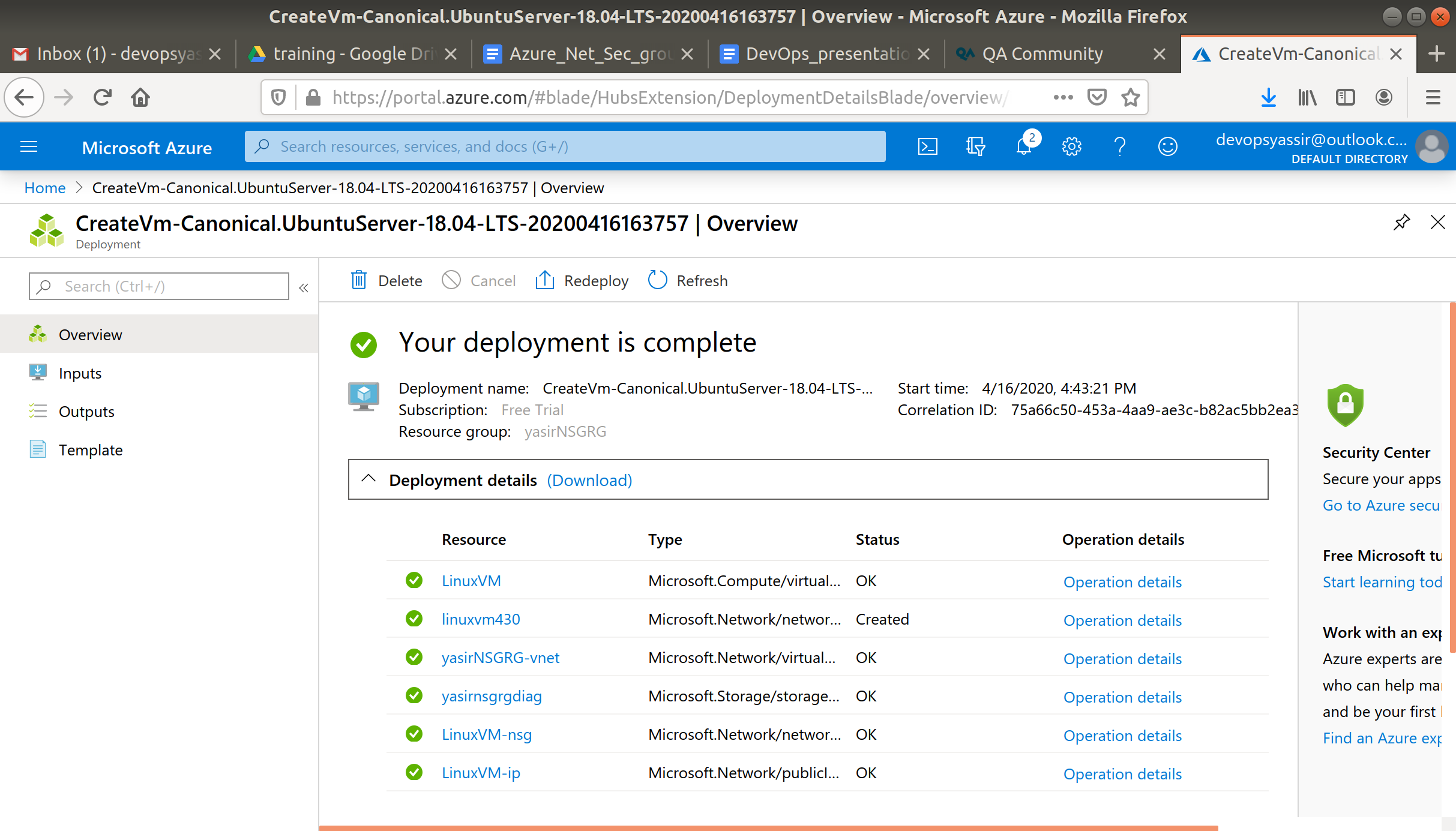
In that dropdown menu you should be able to see the predefined inbound rules for SSH, HTTP and HTTPS.

We also need to ensure that Port 22 is open, so we can SSH into the machine later (this should be checked by default):





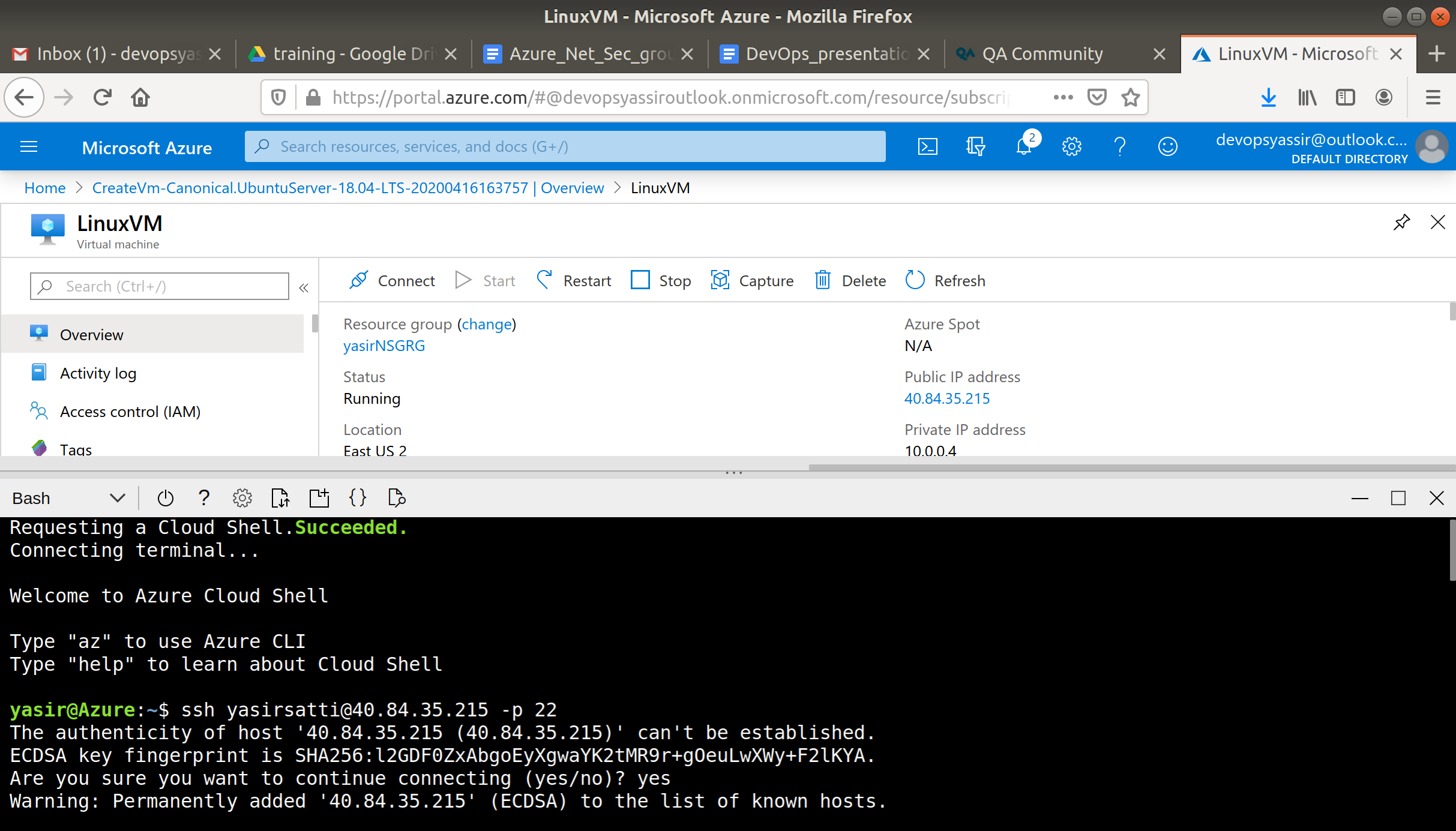
After clicking Create, our Linux VM is created!

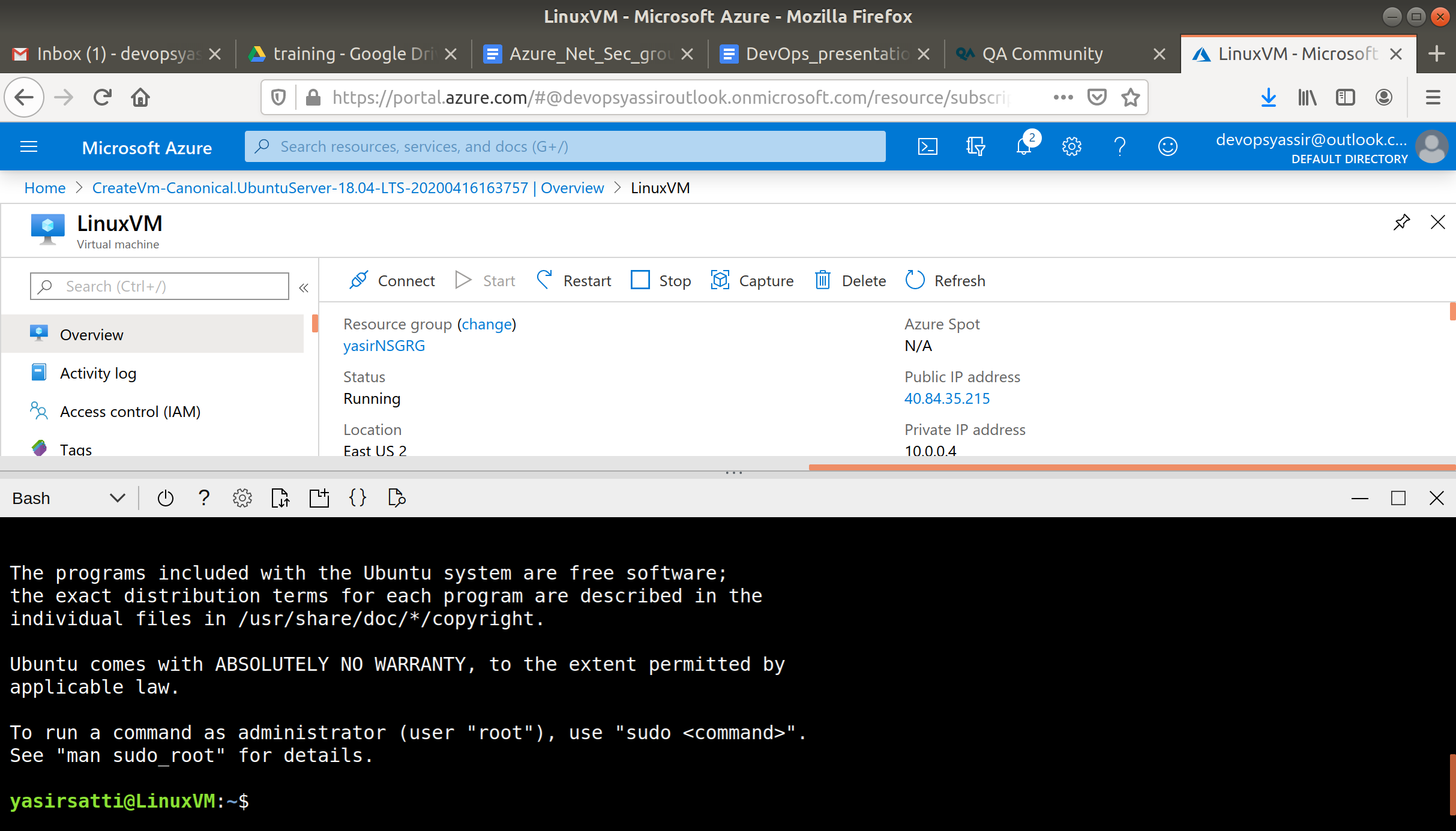


### **NSG**

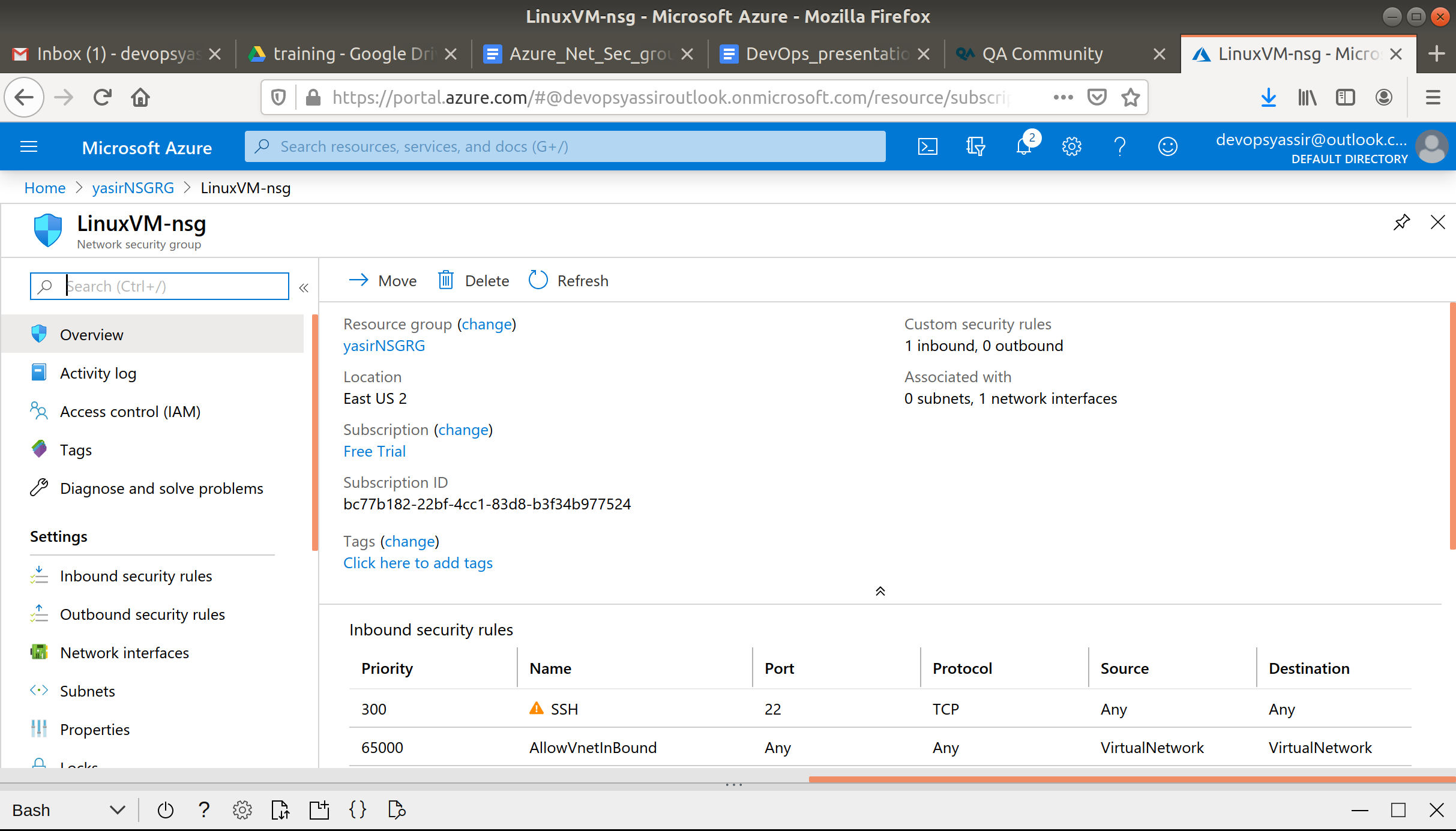
SSH into your machine from your local machine, to show that it works, with a command like

ssh student@[IP Address] -p 22

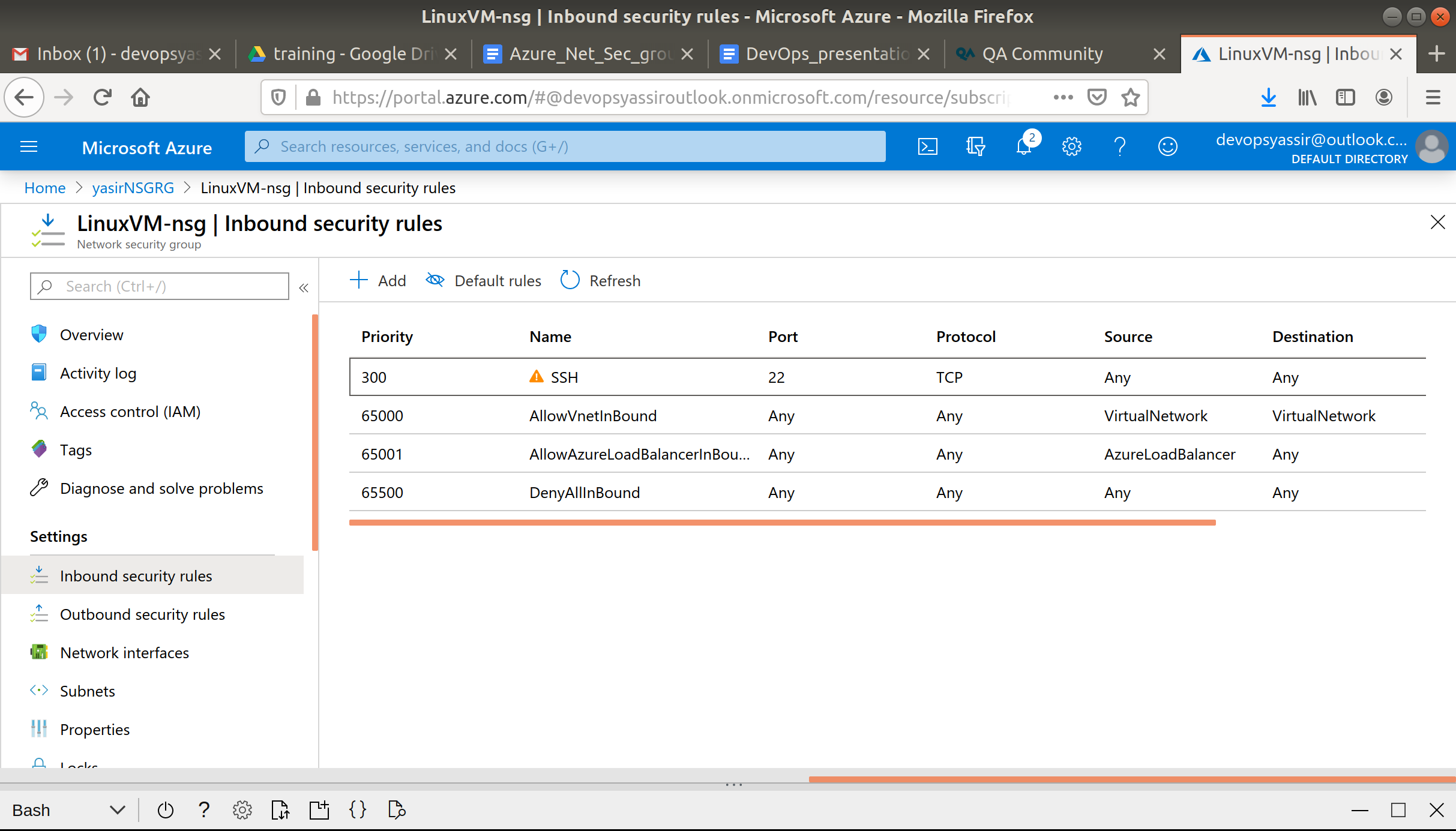




Now navigate to your vms NSG it will be called VM-nsg



Now on your NSGs page, select Inbound Security Rules.



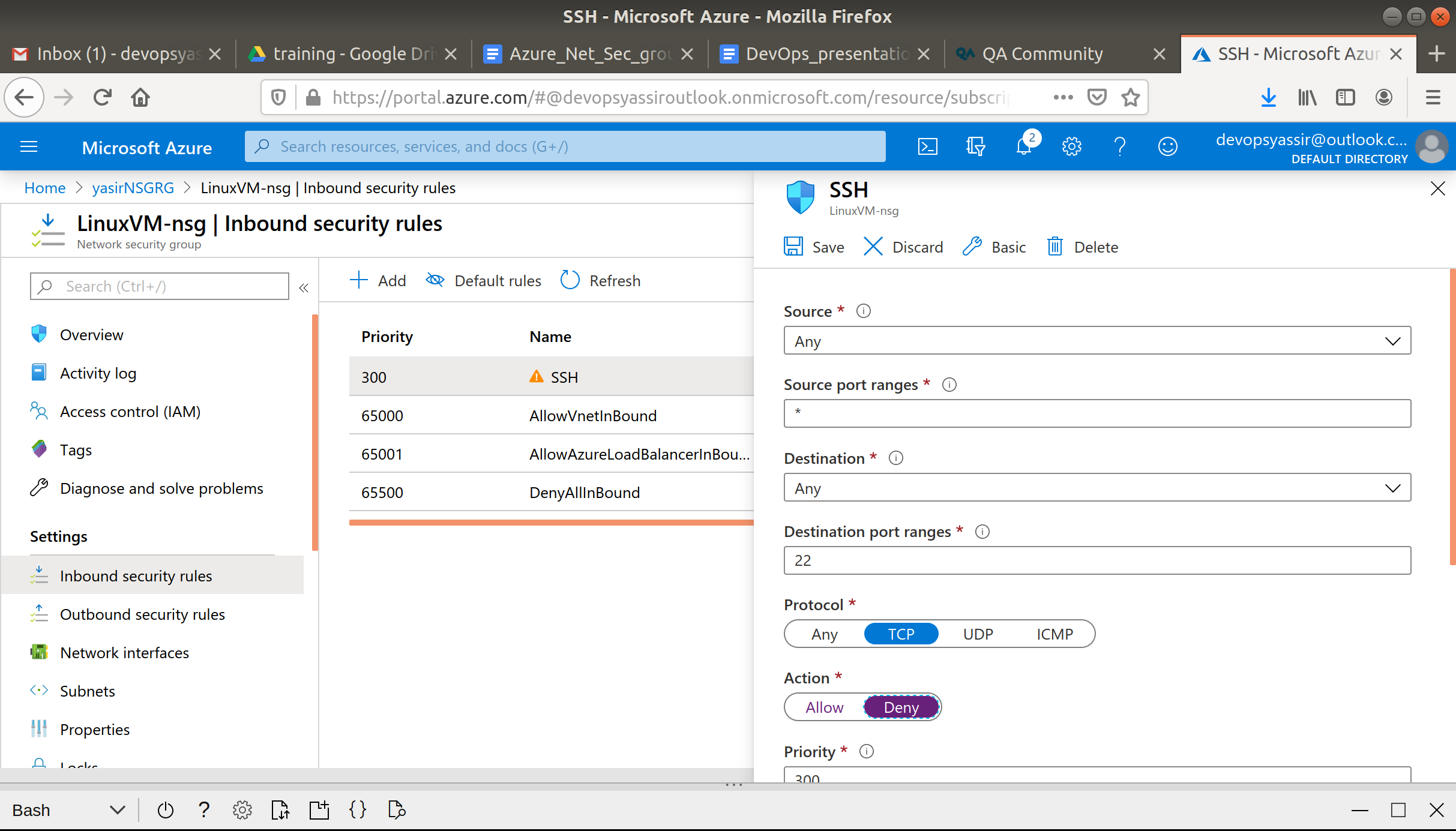
You should be able to see the SSH inbound rule.

Select the rule. And change the Source to Service Tag.

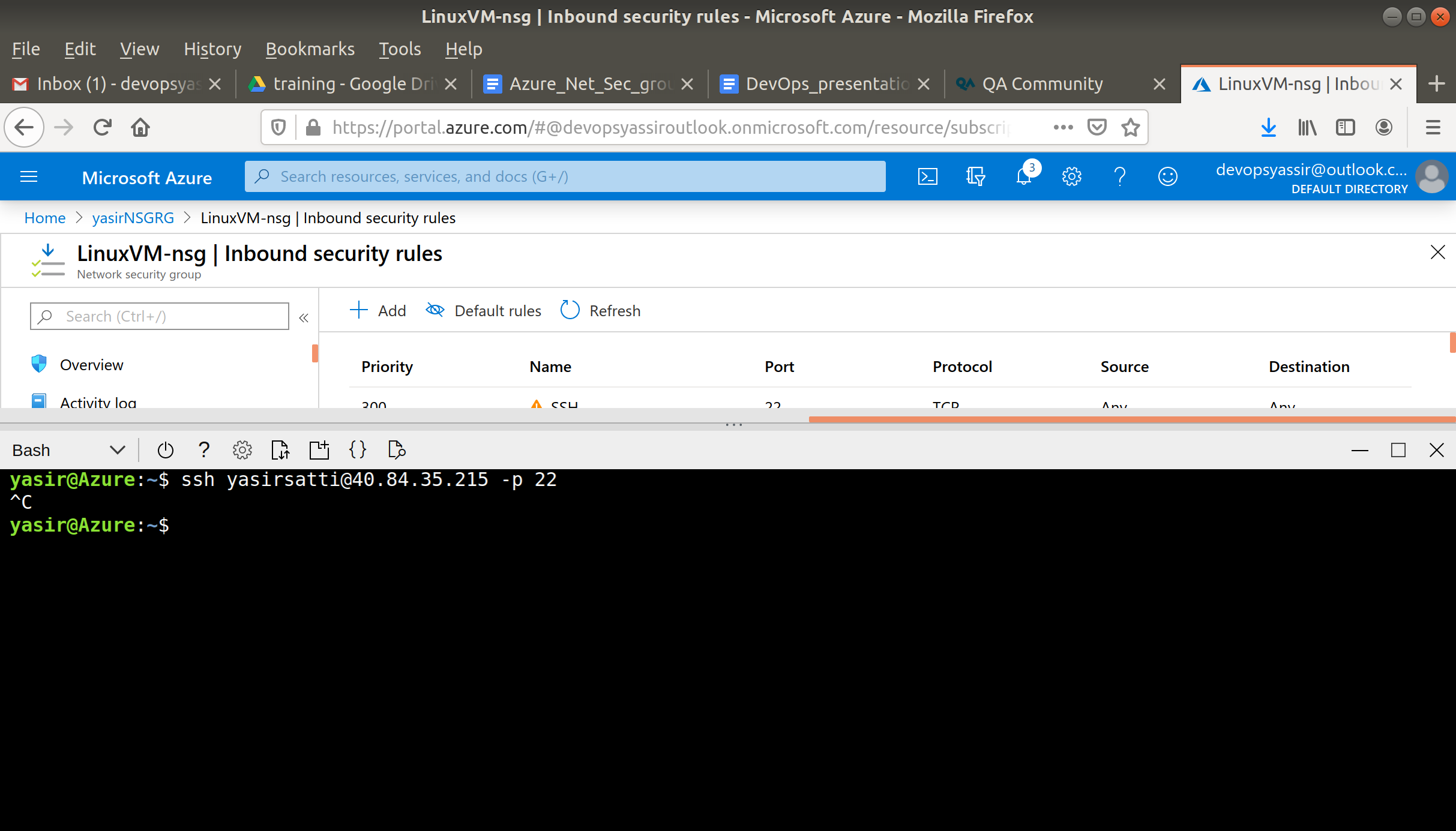
Now take a look at the drop down Source Service Tag you can see all the different options with Azure services so that you can allow traffic from them without much configuration.

Now click the X in the top right and select the rule again, to make sure you don't save changes.

Now select Deny rather than Allow.



Click Save and try now to SSH into your machine again. You should see that you will not be able to and port 22 is now closed.



### **Clean Up**

To clean up, go back to the Resource Group page, click your resource group you used for this module, and then choose Delete.

Once you type the name of the resource group to confirm deletion, this will be deleted along with everything inside of it.