3. osTicket Live-Deployment

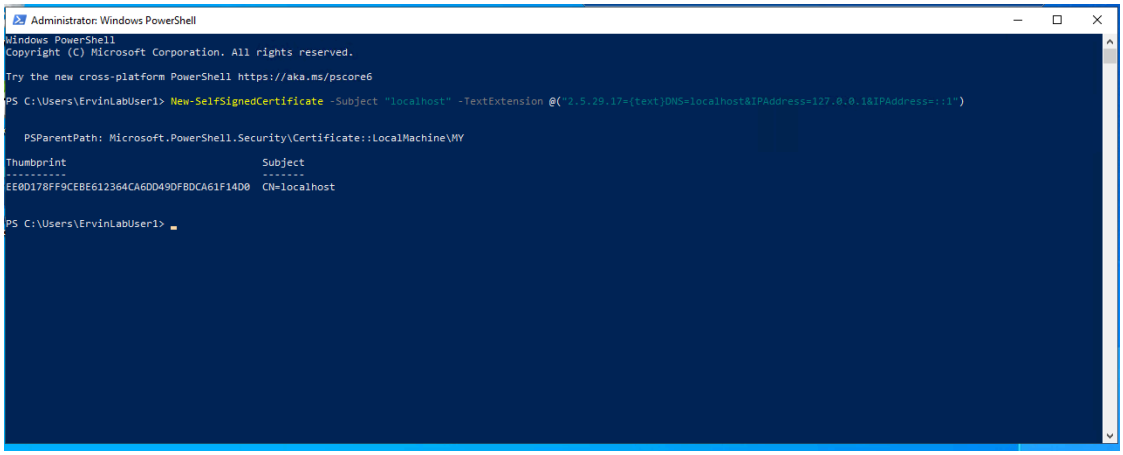
Deployment of a Cloud-Based osTicket System on Microsoft Azure for Home Network Support on Windows 10

1. Hosting the Azure Windows 10 Virtual Machine

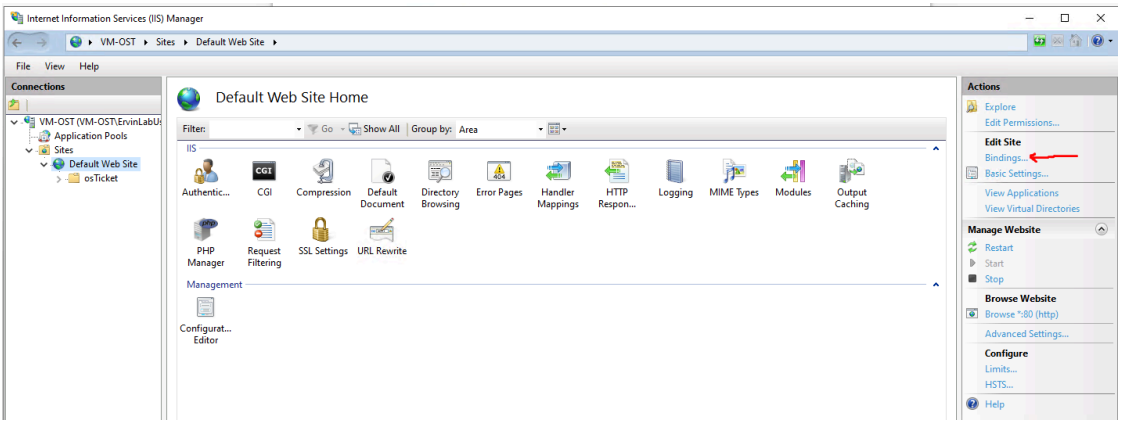
1.1. Setting up a HTTPS

As this is for testing and personal project purposes, we'll create our own self-signed SLL/TLS certificate for our "localhost".

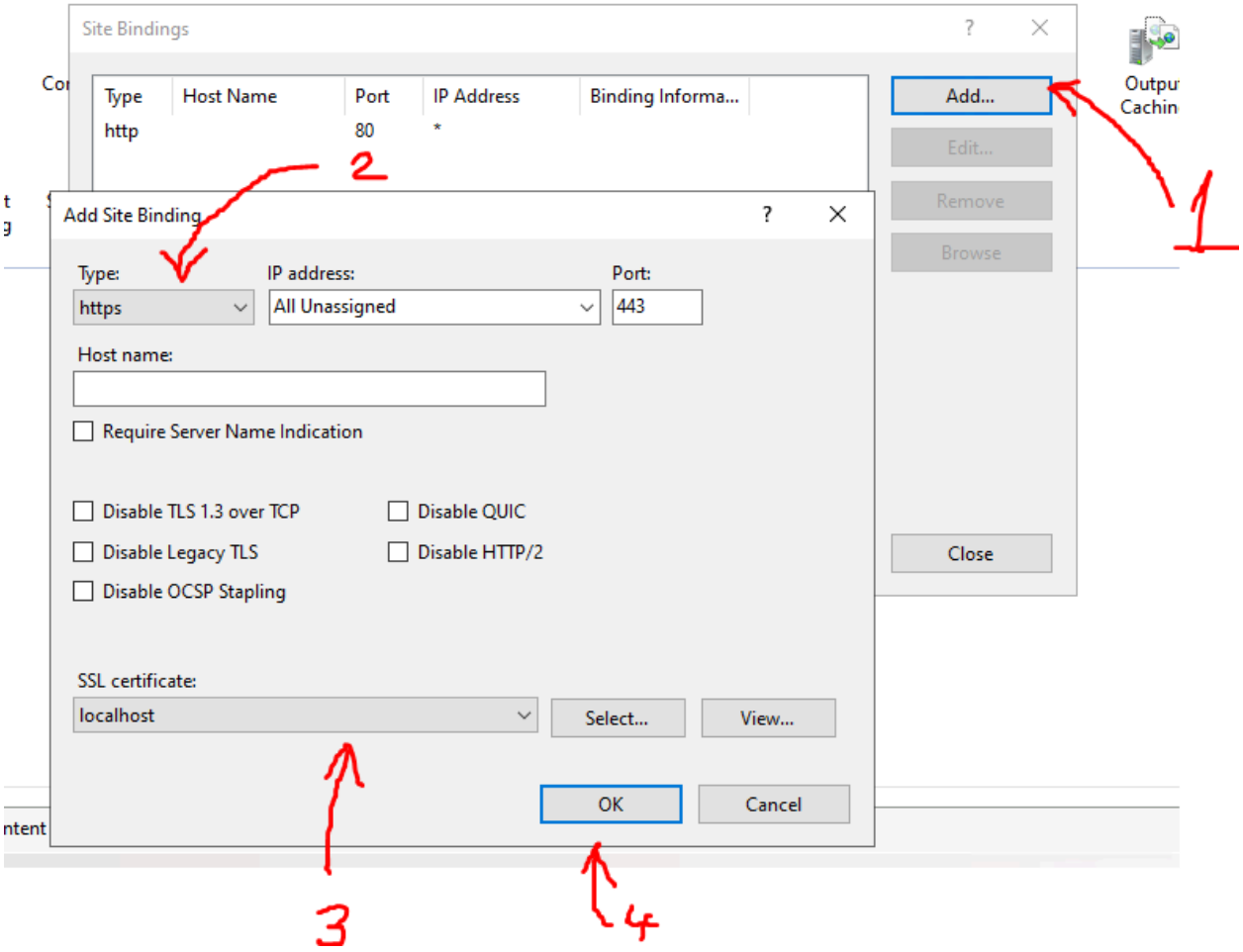
We'll have to Remote Desktop Access to our Windows 10 Virtual Machine.



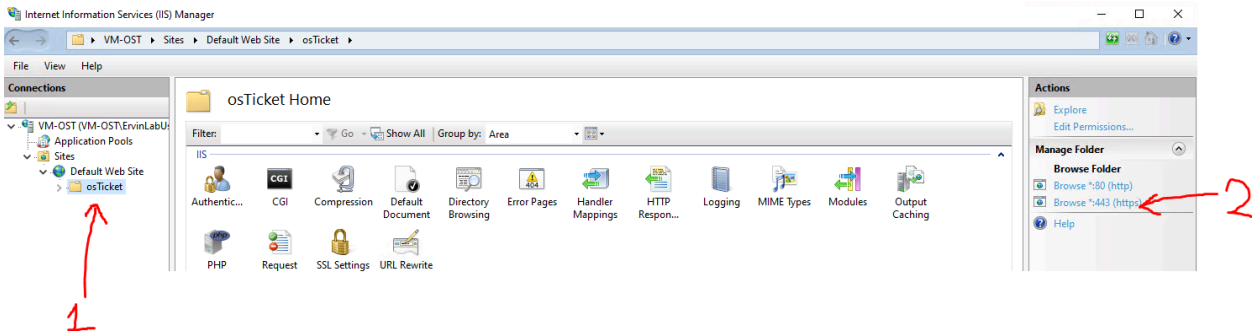
- Open Windows Powershell with administrator
- Paste this line of code: "New-SelfSignedCertificate -Subject "localhost" -TextExtension @("2.5.29.17={text}DNS=localhost&IPAddress=127.0.0.1&IPAddress=::1")"
    - This command creates a self-signed certificate with "localhost" as the subject. The certificate is valid for the DNS name "localhost," the IPv4 address `127.0.0.1`, and the IPv6 address `::1`. This allows the certificate to be used securely with connections to `https://localhost`, `https://127.0.0.1`, or `https://[::1]` on the machine where it is installed.



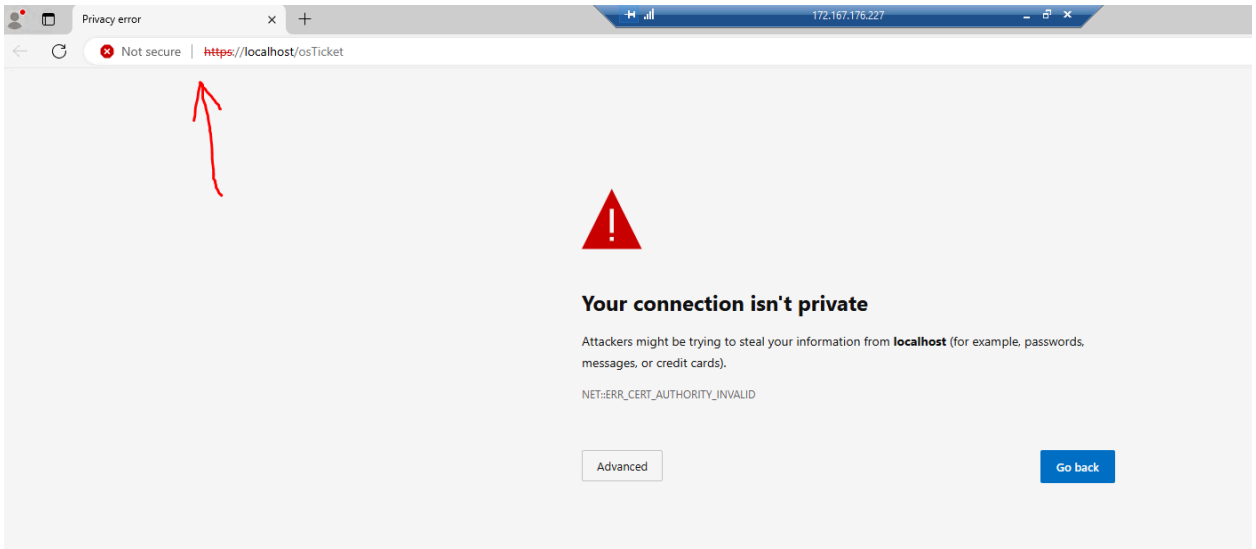
- You then select "Bindings…"



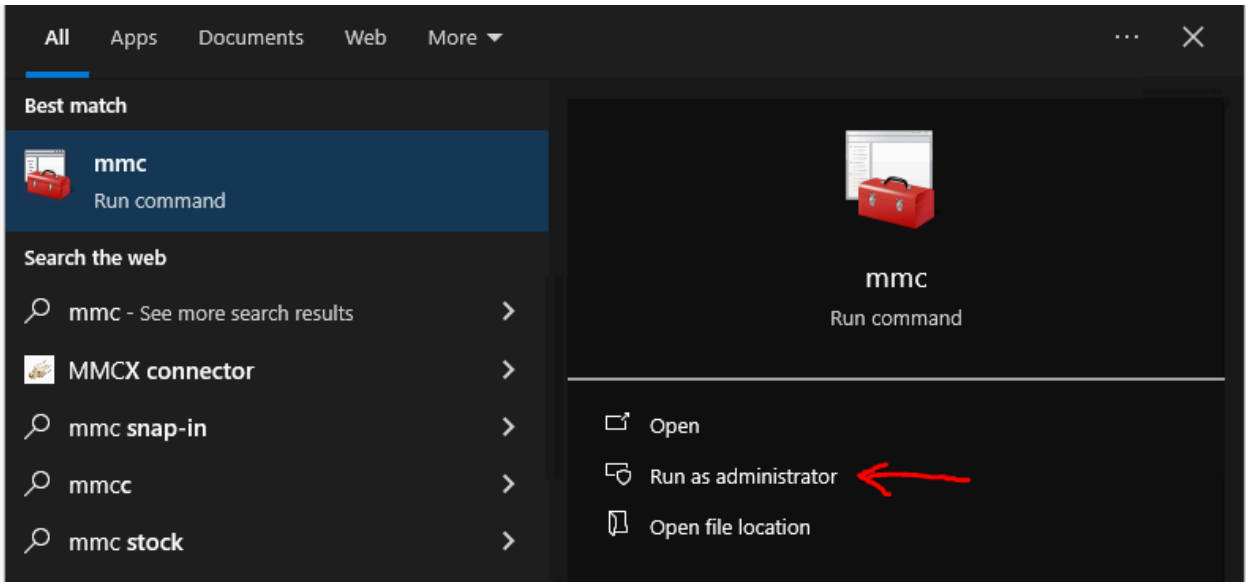
- Select Add
- Change Type to https
- Select localhost under SSL certificate
- Click OK



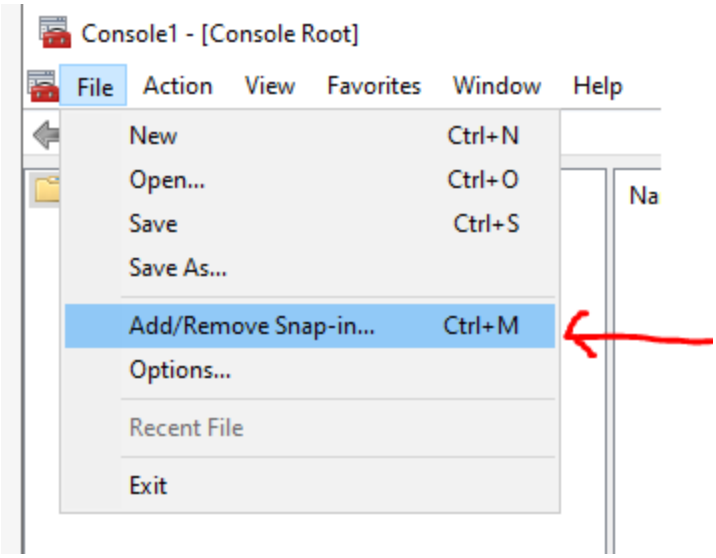
- First select osTicket
- Second select Browse *:443 (https)



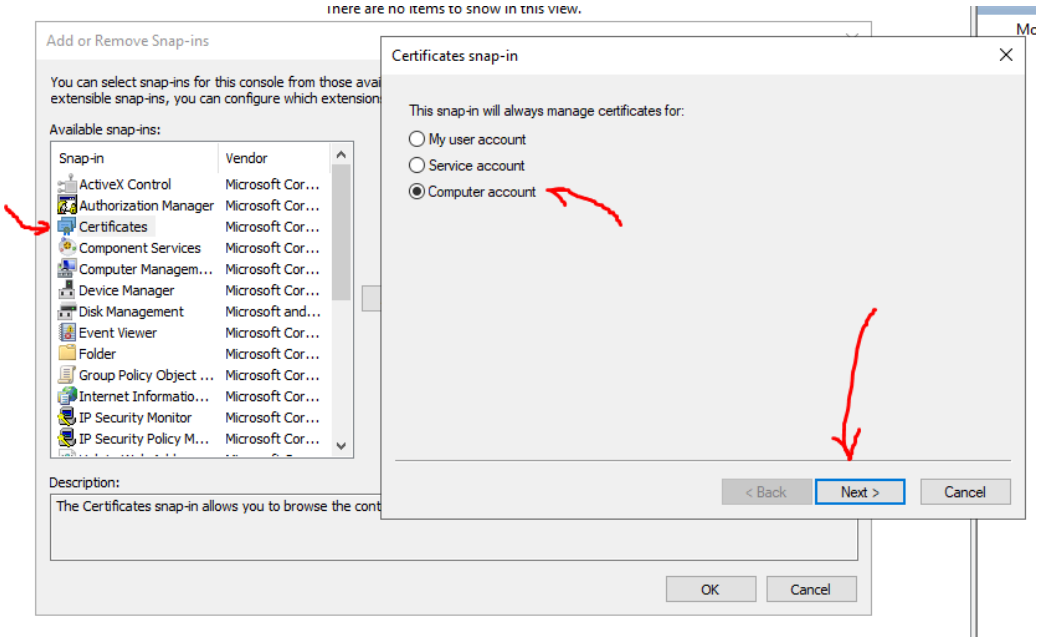
- What you'll see is that the connection isn't secure. Let's fix this.



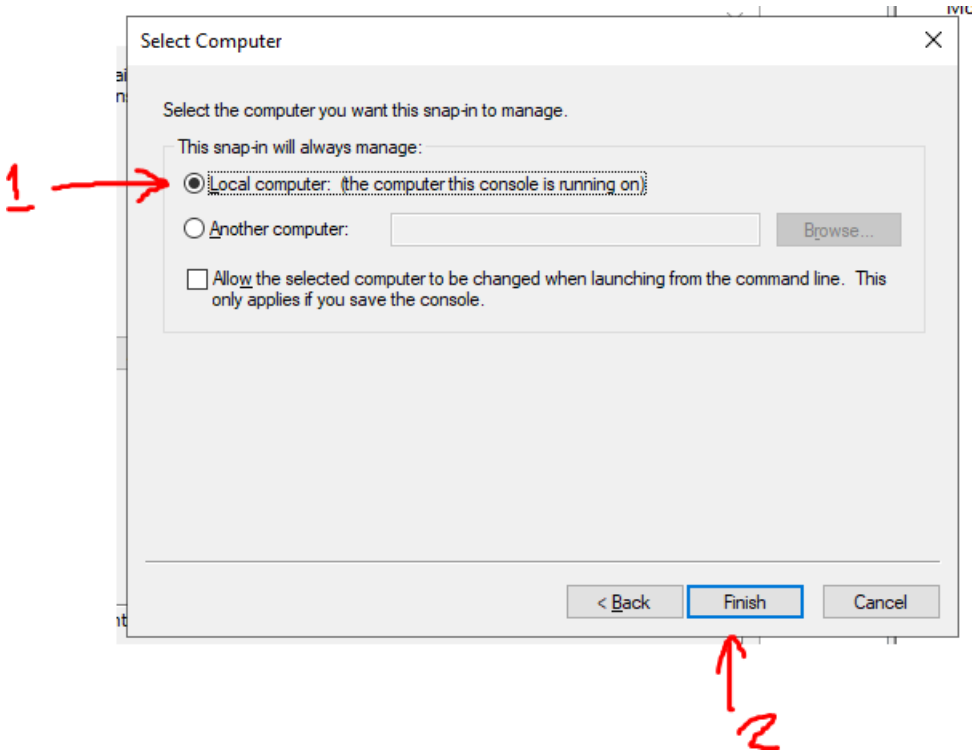
- Search for MMC
- Run as administrator



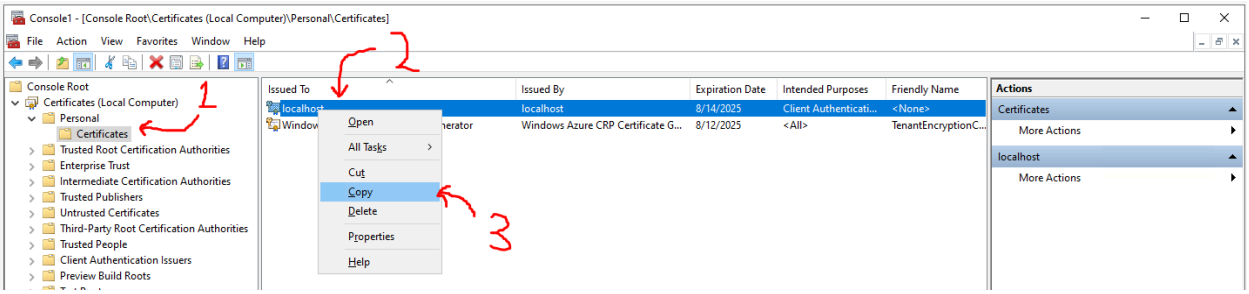
- We want to Add/Remove Snap-in…



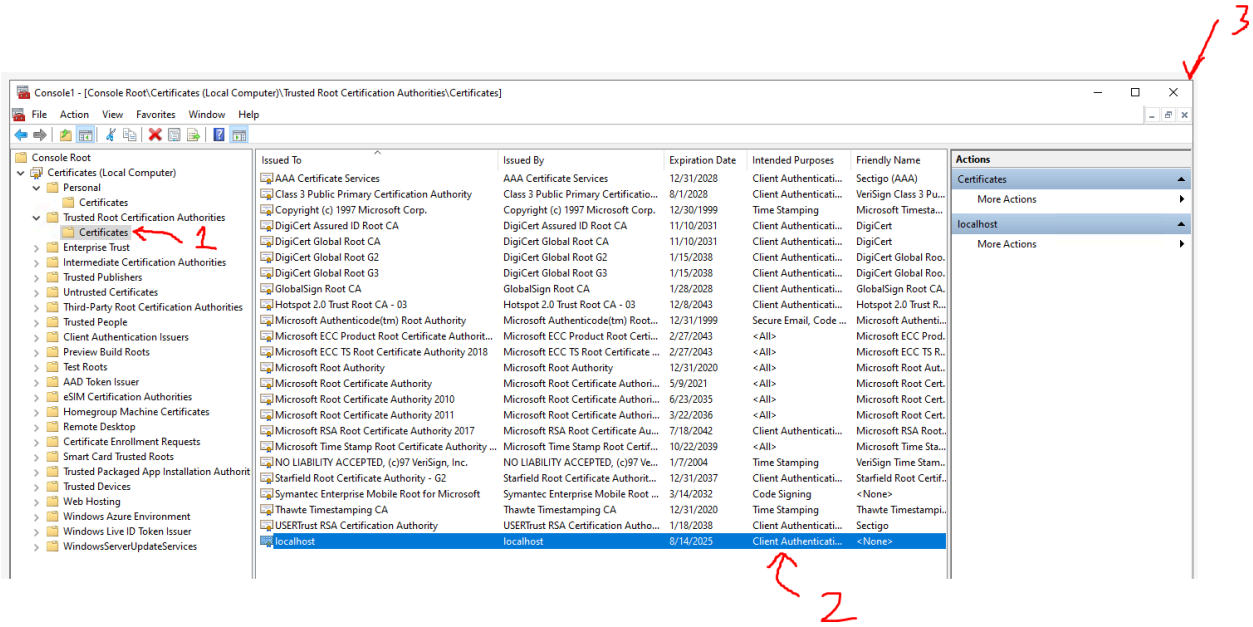
- Select Certificates
- Select “Computer account”
- Go to Next



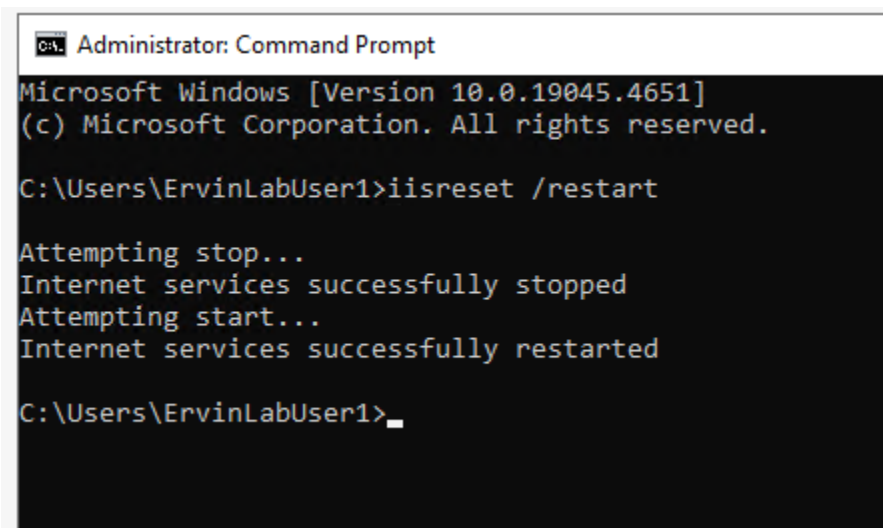
- Select Local Computer
- Click “Finish”
- Then click OK to close out of the Add or Remove Snap-ins



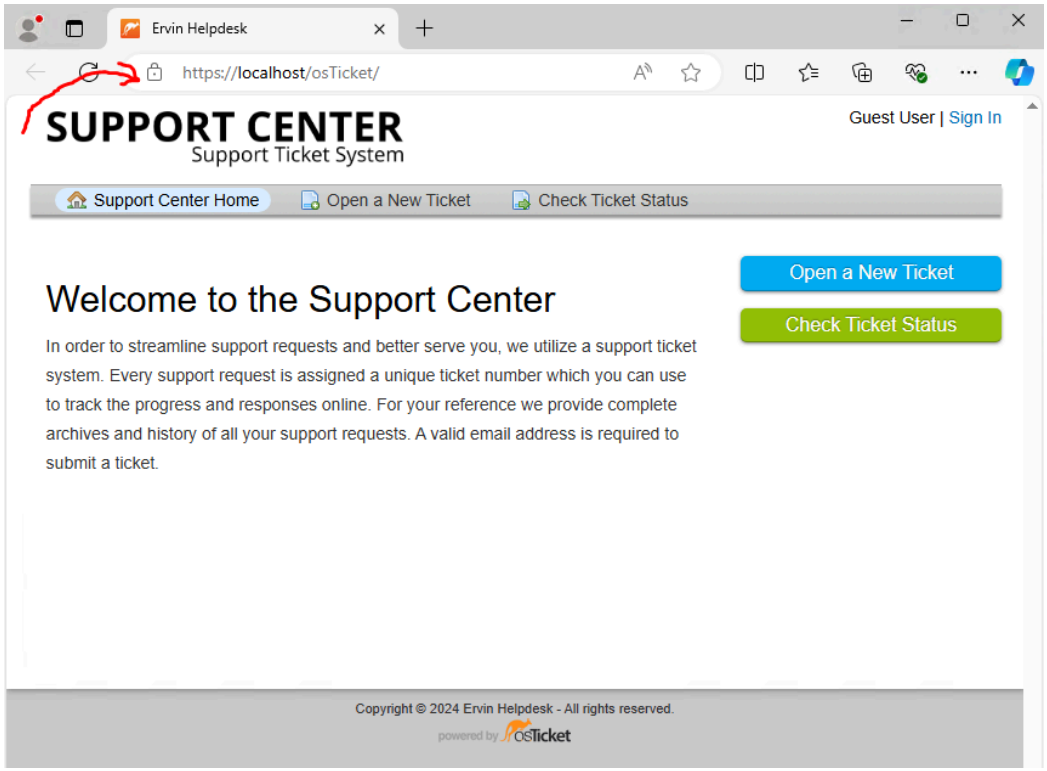
- Select “Certificates” under Certificates>Personal>Certificates
- Go to “localhost”
- Then select “Copy”



- Select “Certificates” from Certificates>Trusted Root Certification Authorities>Certificates
- Paste it into there
- Close it. You don’t need to save anything.



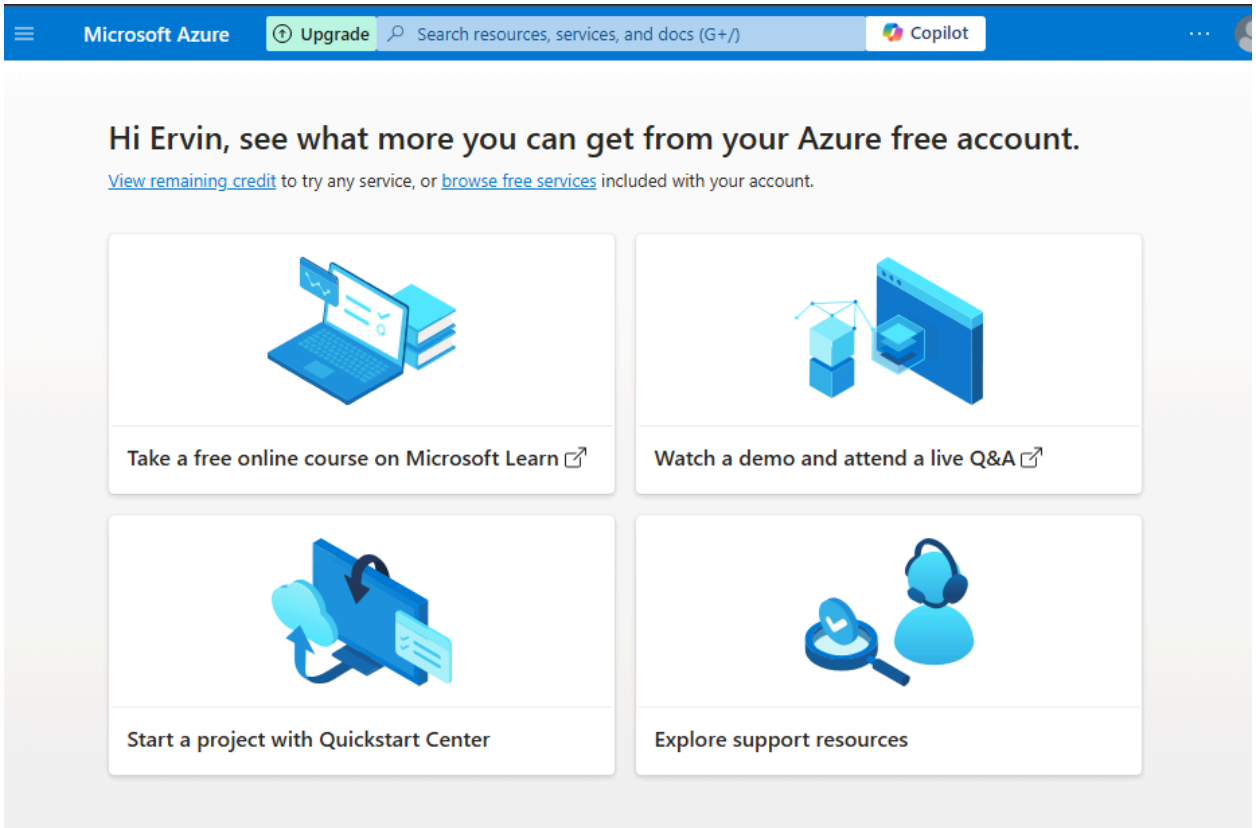
- Open CMD as an Administrator
- Type: “iisreset / restart”
    - This will reset the IIS

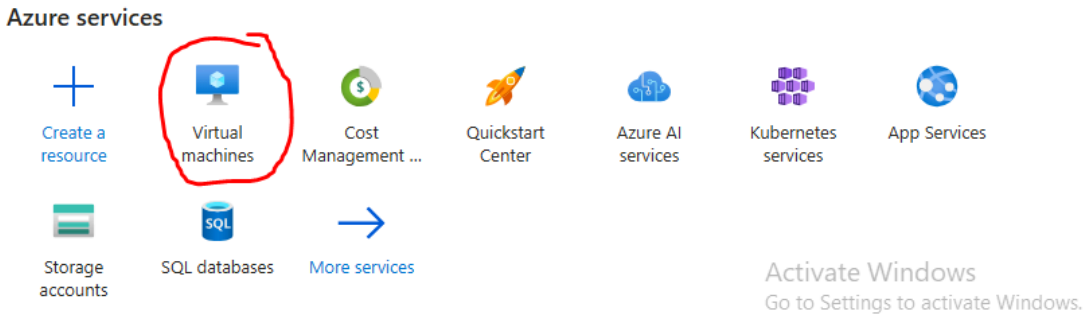


- From here you can now see that the HTTPS has been set up.

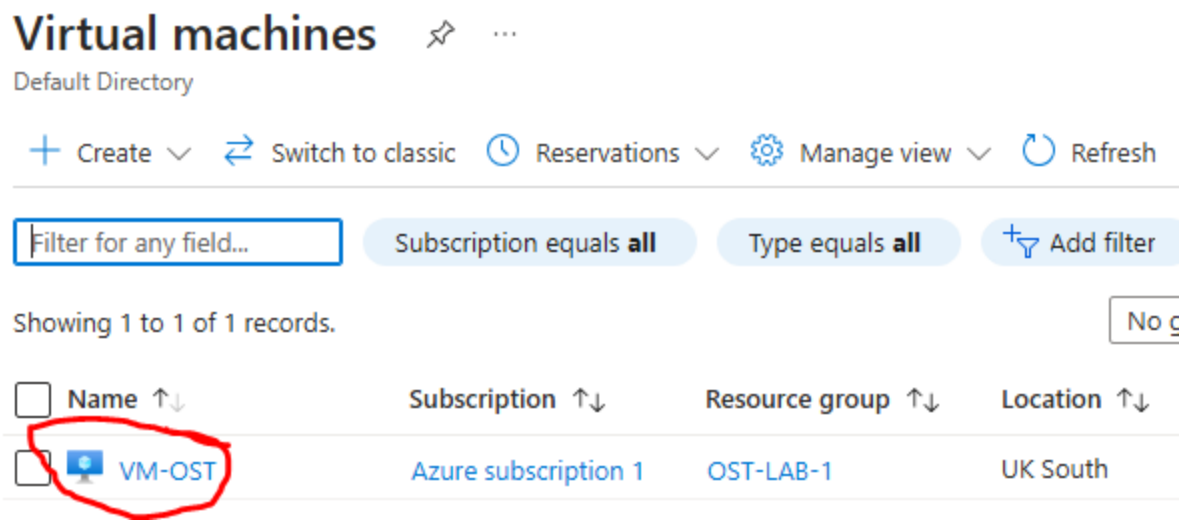
1.2. Configuring Network Security Group (NSG) Rules

Here we're going to configure the network security rules to allow for inbound HTTPS traffic. This will help get our virtual machine in Azure into a live environment.

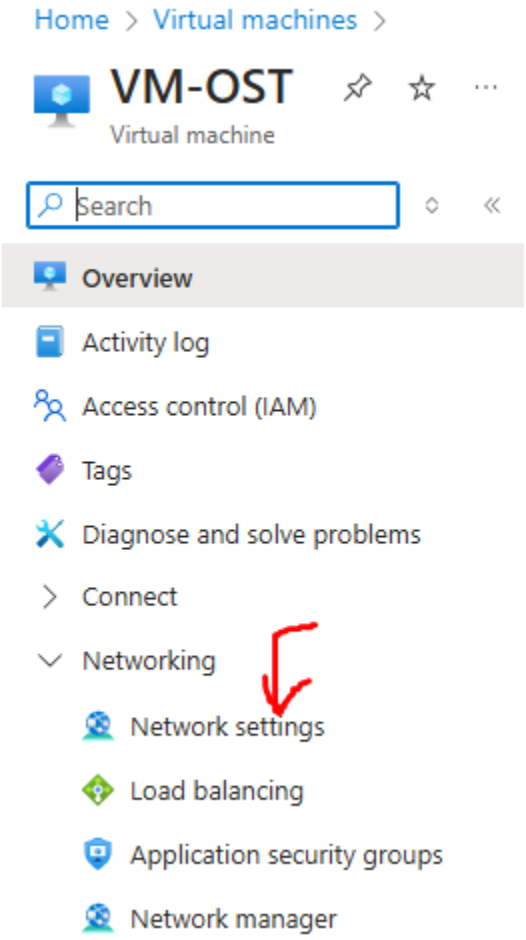




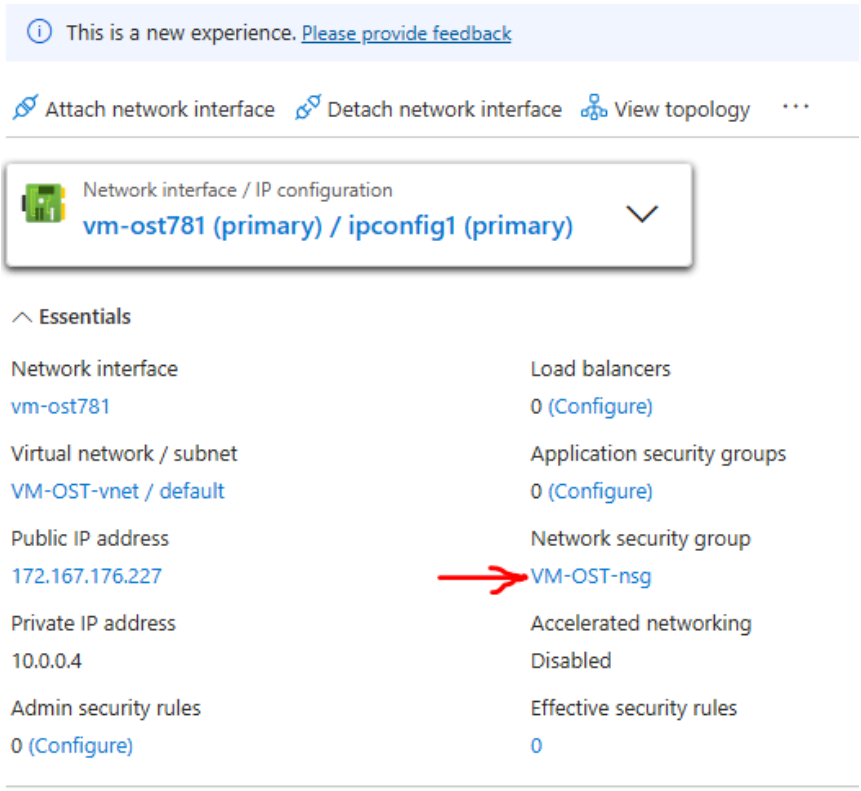
- Select Virtual Machines
- Ignore the "Active Windows" on the bottom left 🙂



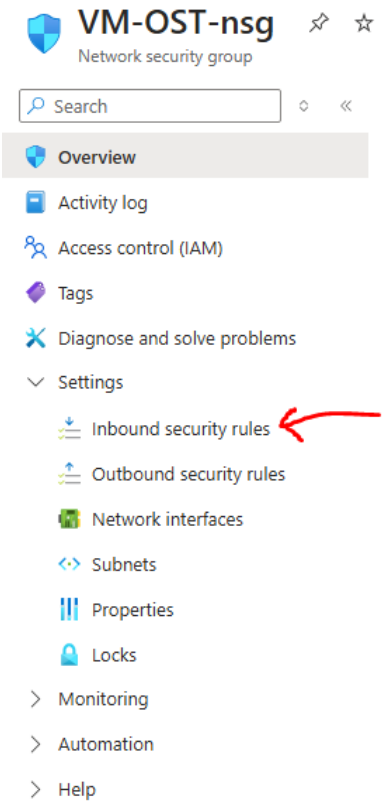
- Select your VM. In this case, it's our VM-OST



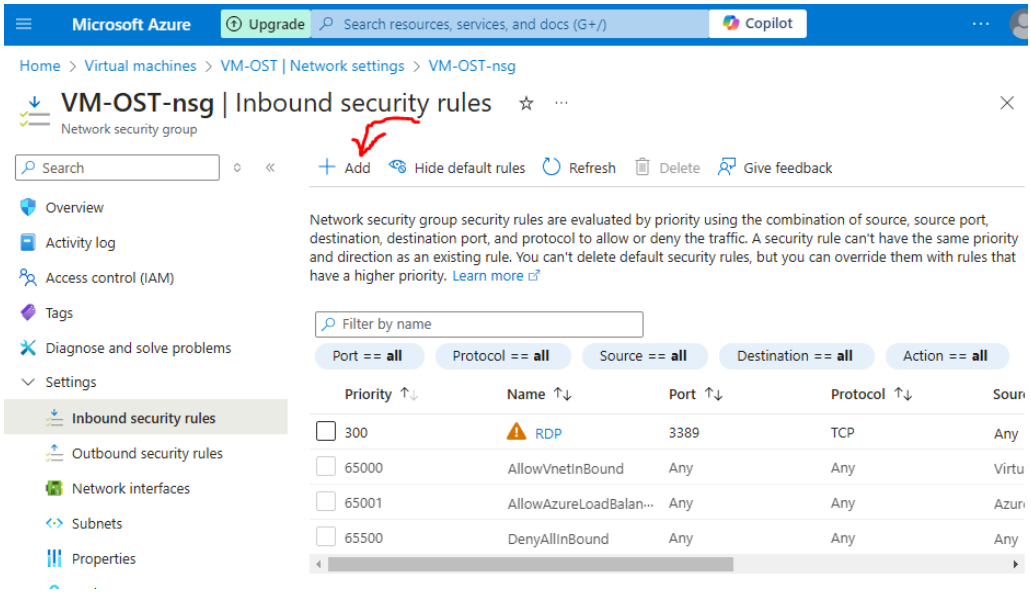
- Select Network Settings



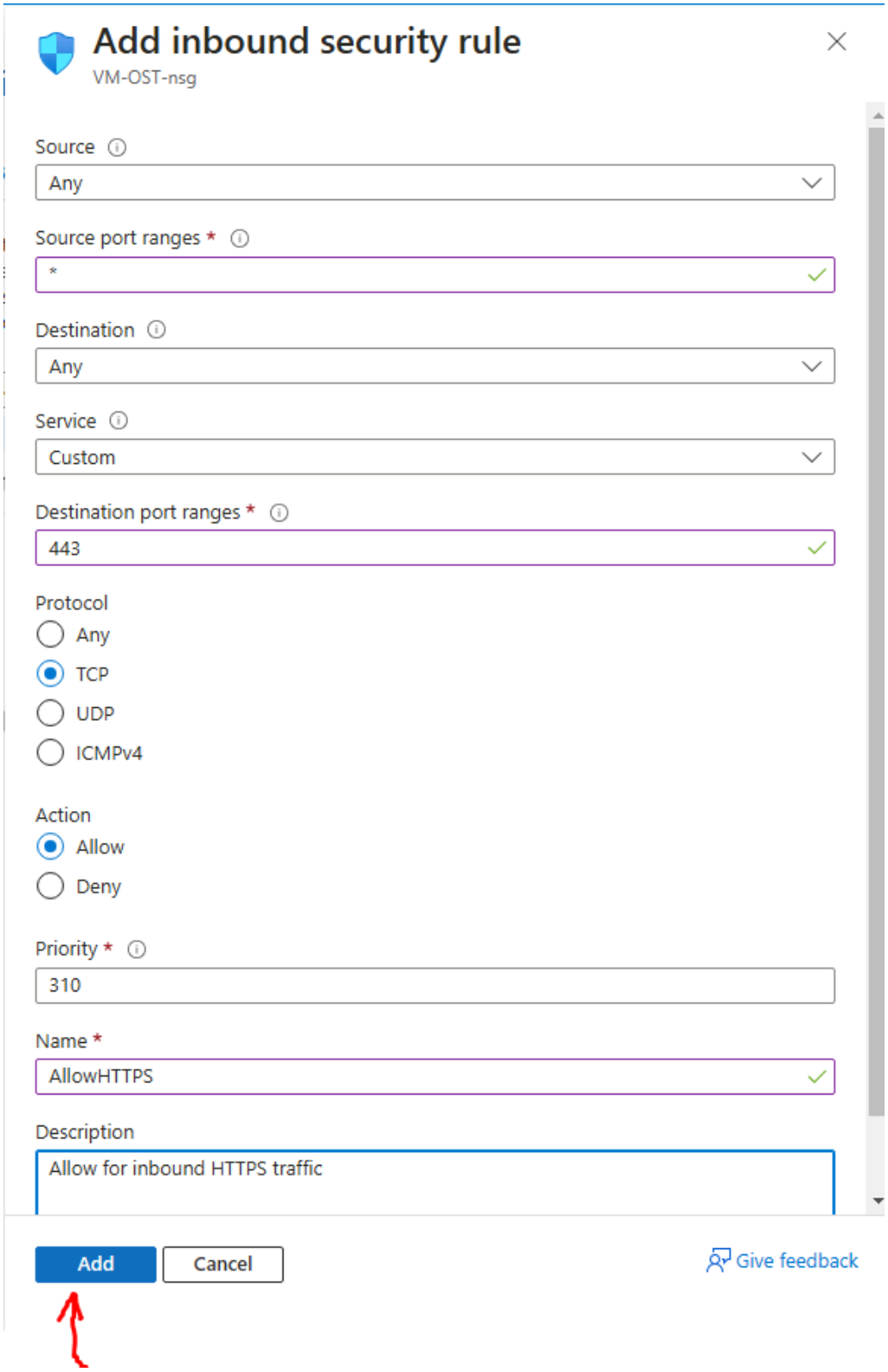
- Select VM-OST-nsg



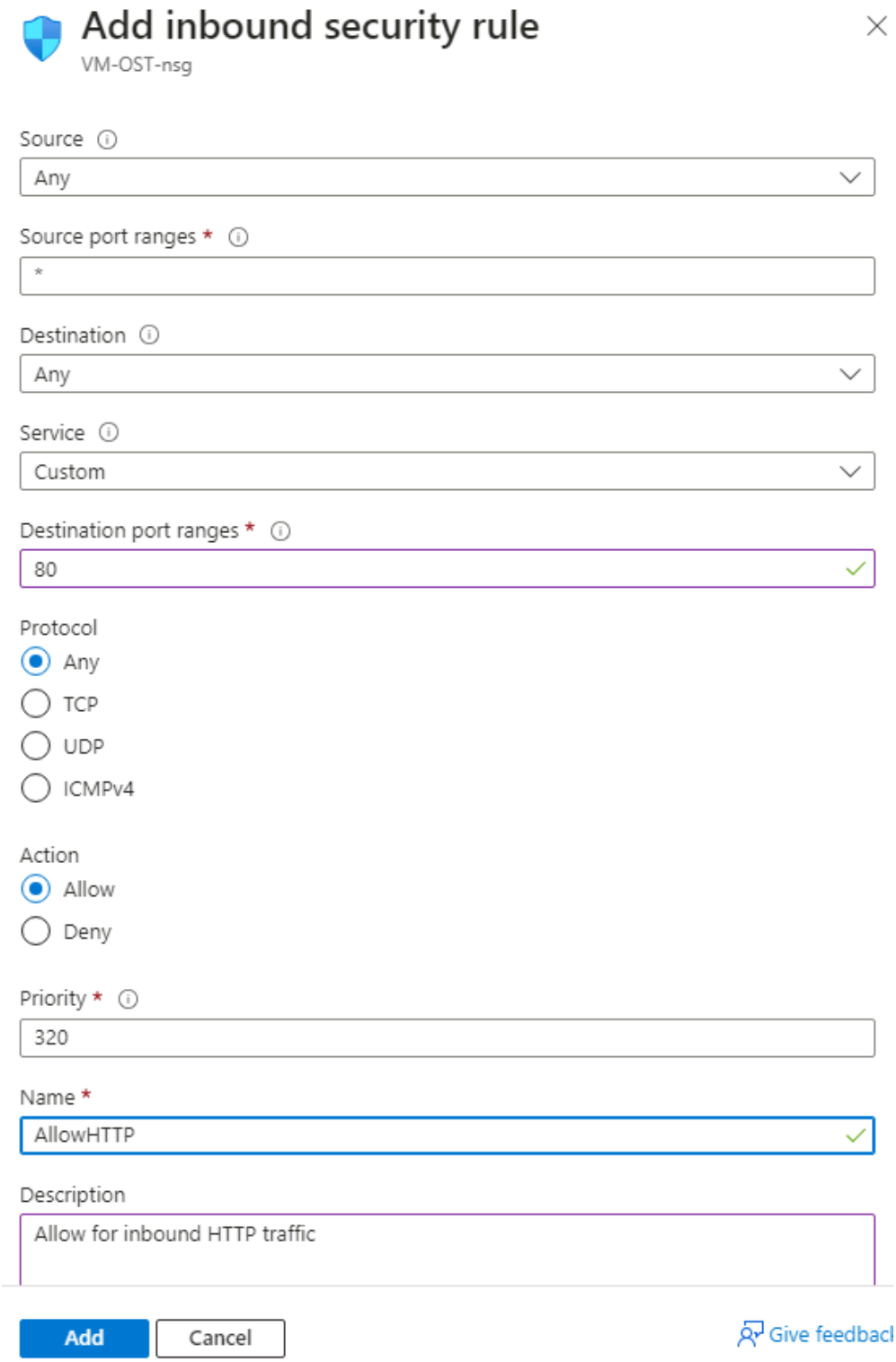
- Select “Inbound Security Rules”



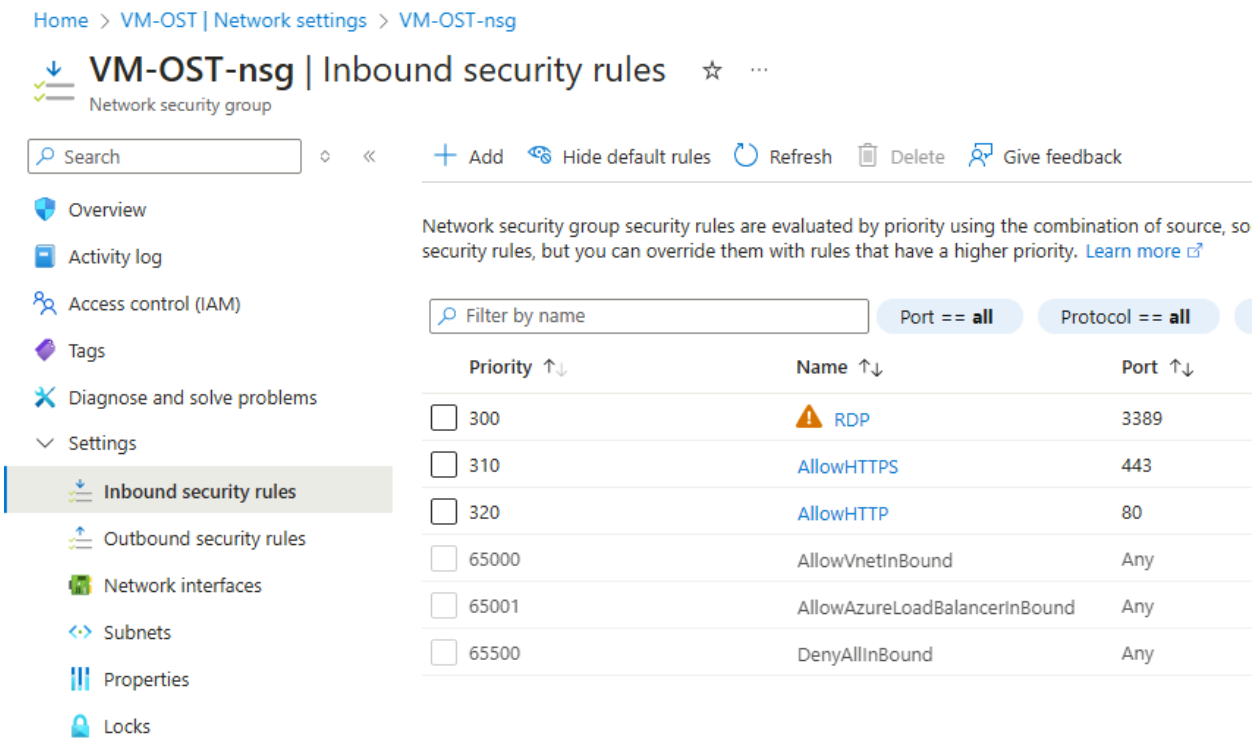
- Select “Add”



- Fill out all the details as shown above. We want to go for Port 443 as we have now set up a HTTPS. Protocol will be TCP for secure connection - since it's HTTPS as well.



- Add another inbound security rule. This time for Allowing HTTP - under port 80.

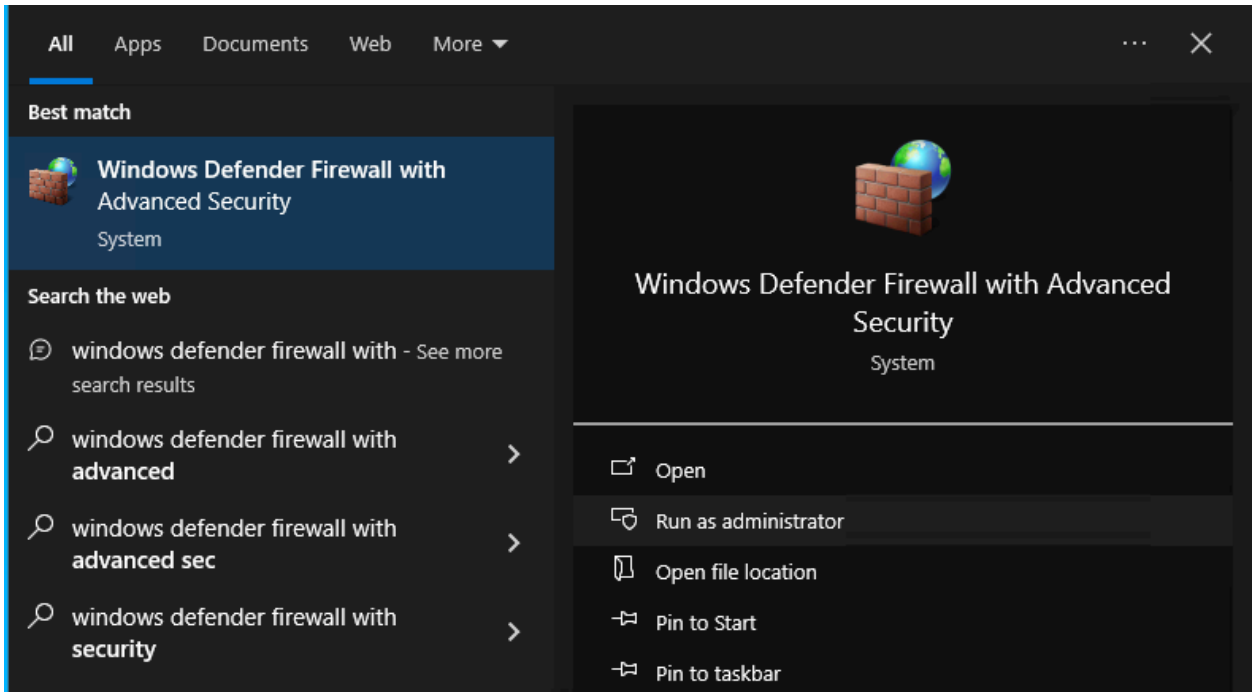


- This should now be set.

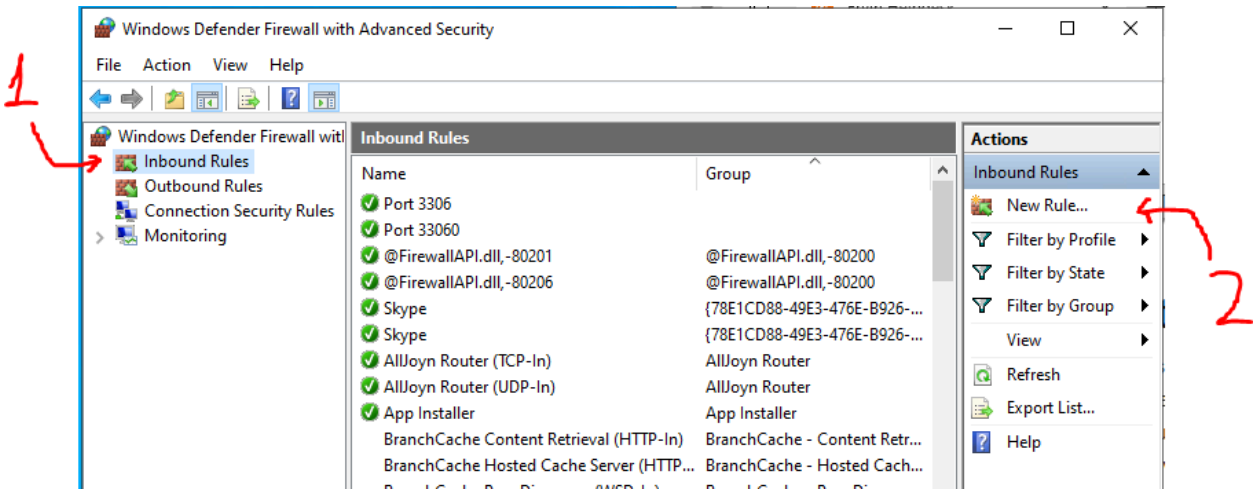
1.3. Configure VM's Firewall

Now it's time to configure the Windows 10 Virtual Machine firewall to allow for inbound connections within the VM.

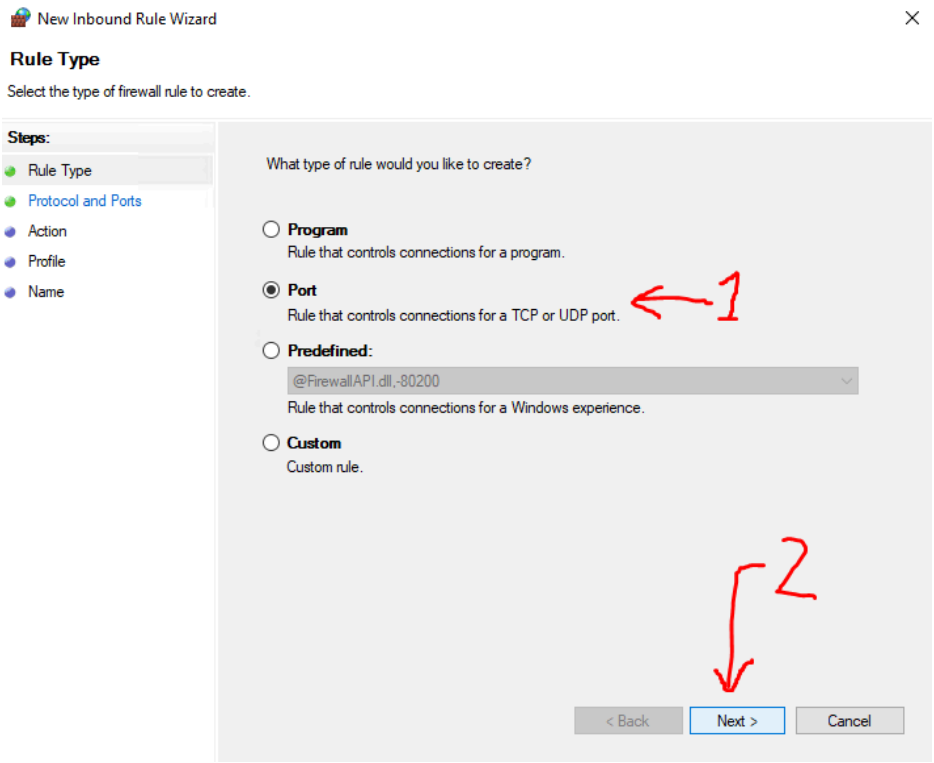
We'll have to Remote Desktop Access to our Windows 10 Virtual Machine if you closed it prior.



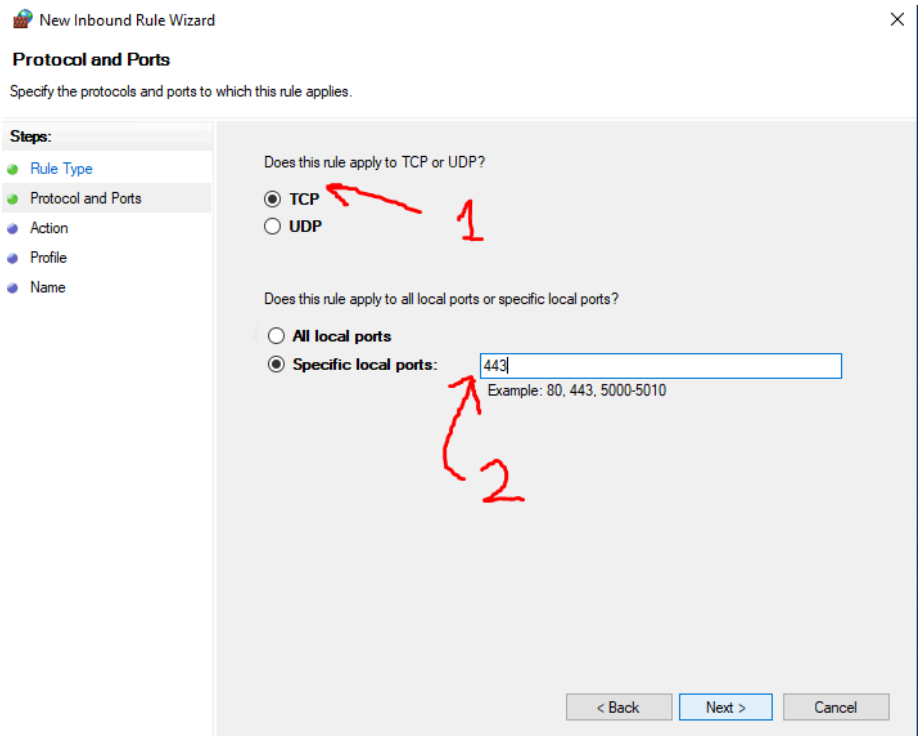
- Run Windows Defender Firewall with Advanced Security as Administrator



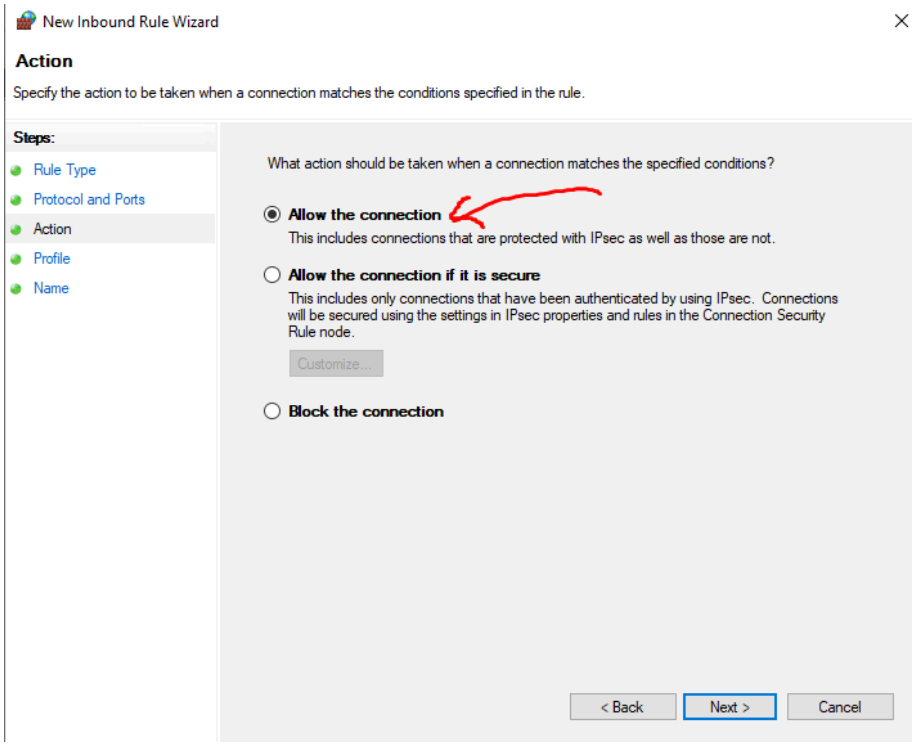
- Select Inbound Rules
- Select New Rule…



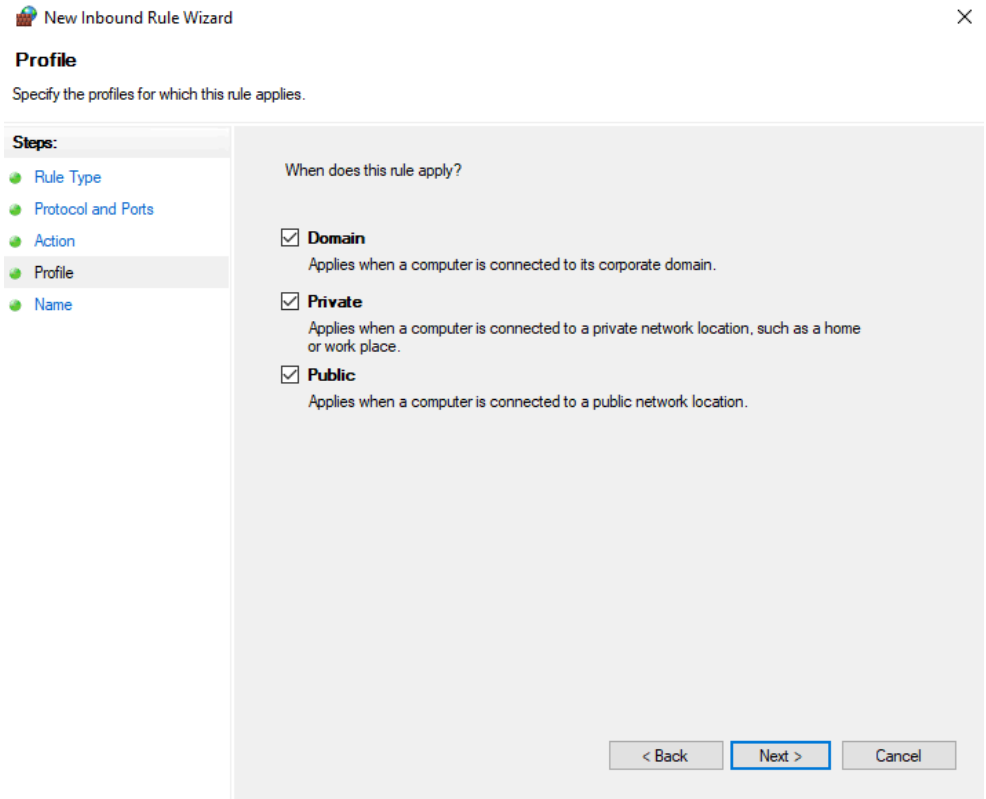
- Select Port
- Then click “Next”



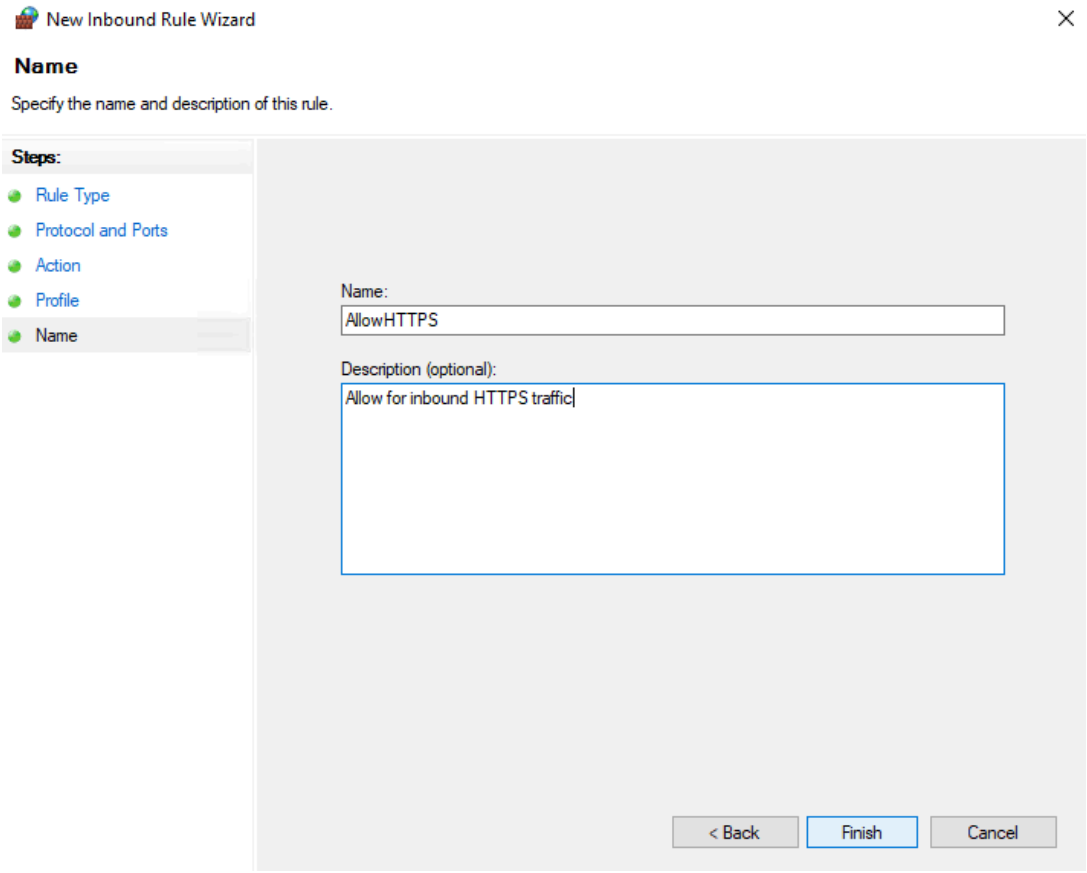
- Select TCP
- Select the specific local port: 443
- Click on Next



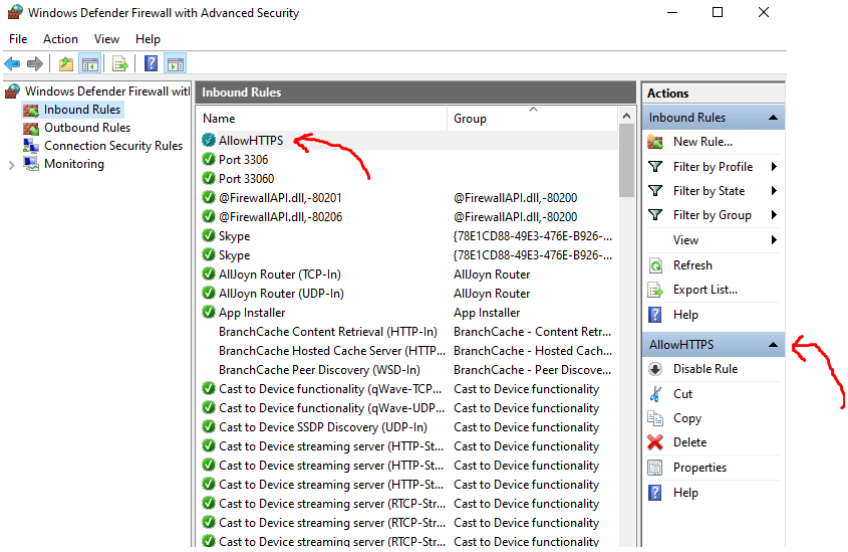
- Select “Allow the connection”
- Press “Next”



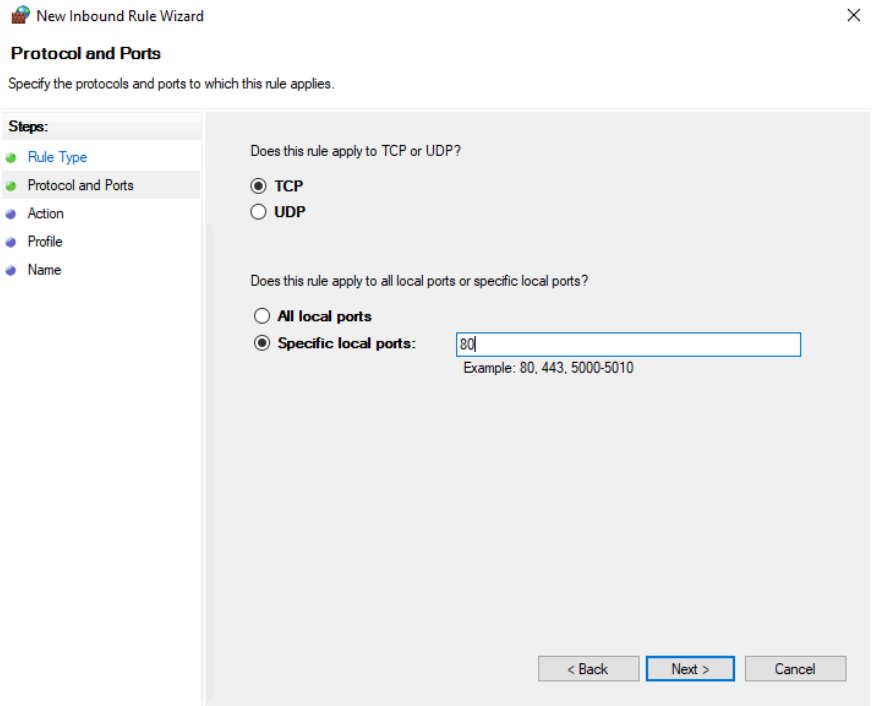
- Keep everything as shown above
- Click “Next”



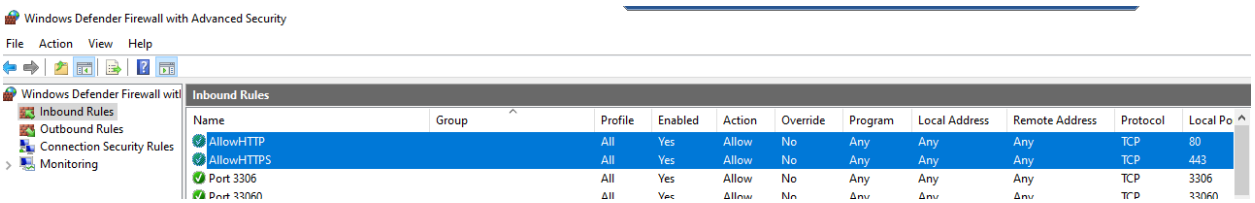
- We then set the name and description
- Name can be: AllowHTTPS
- Description is whatever you feel works well.
- Press Finish



- We can now see that it's setup



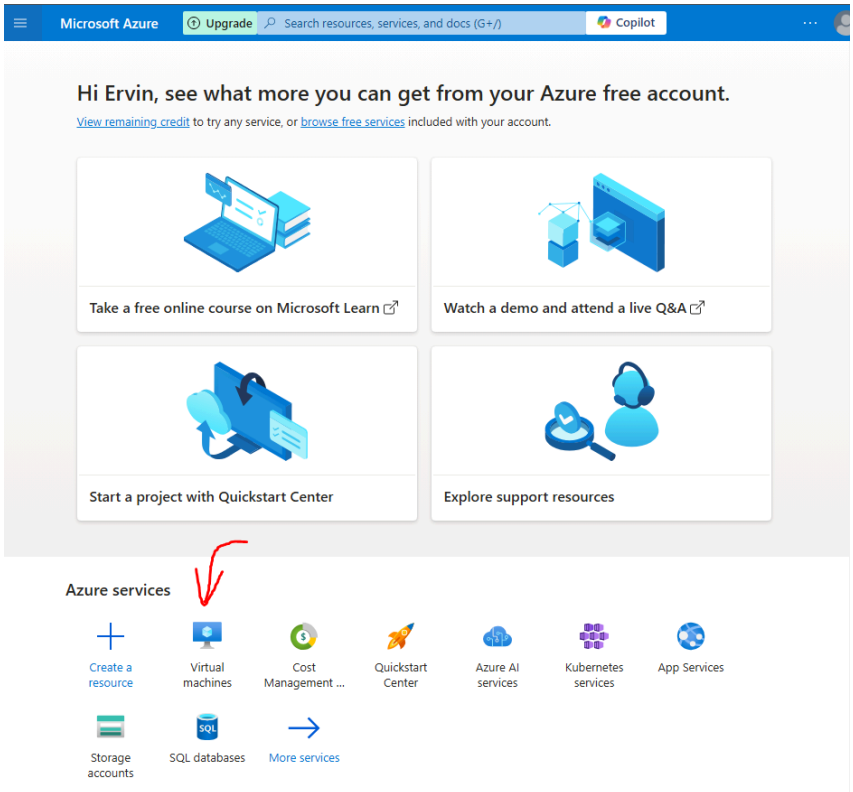
- We'll do the same as before but with port 80 this time to allow for HTTP



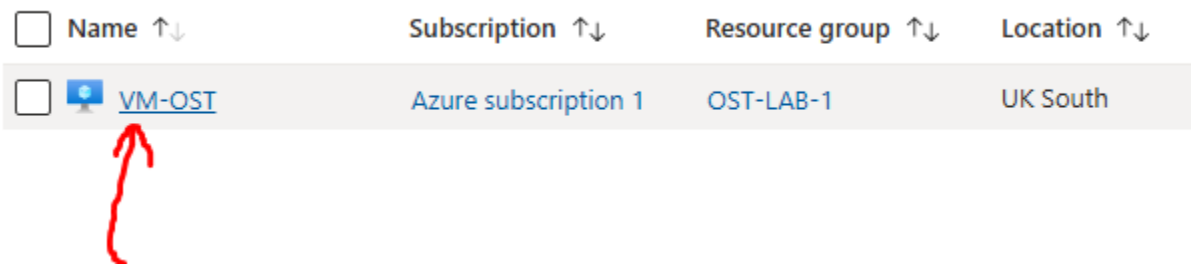
Now we have allowed for both HTTP and HTTPS

1.4. Verify Web Server Configuration

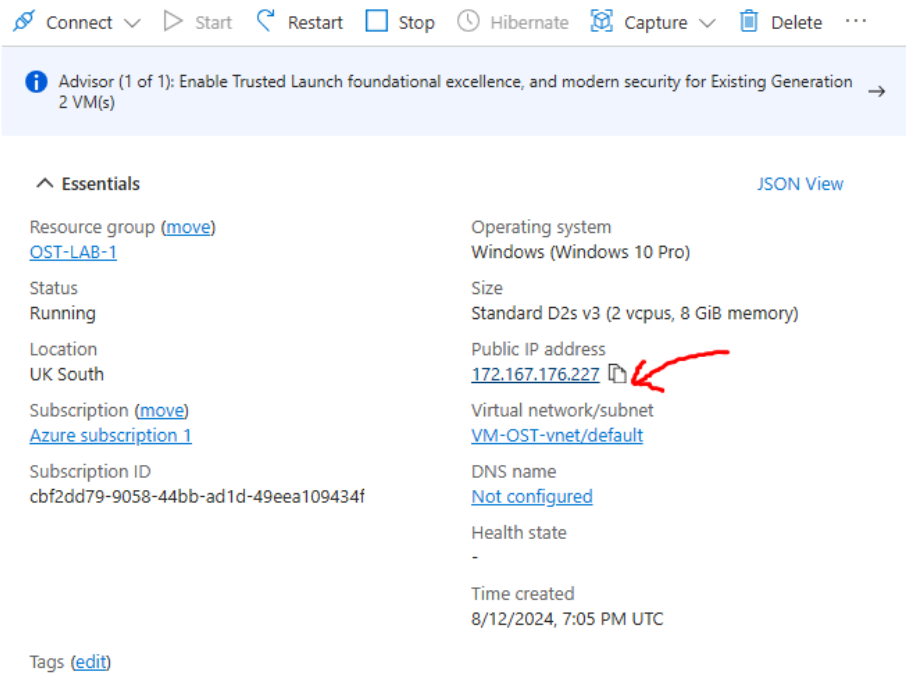
Time to verify the webpage! First we'll need to get our Public IP Address given for our Virtual Machine.



- Select Virtual Machines

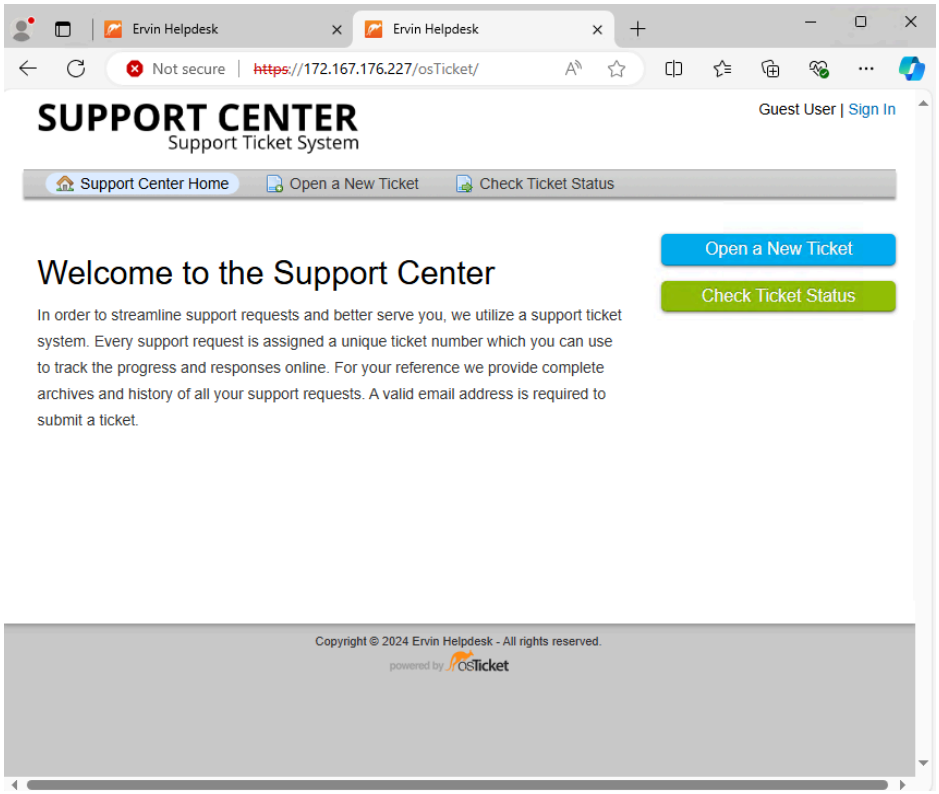


- Select your Virtual Machine



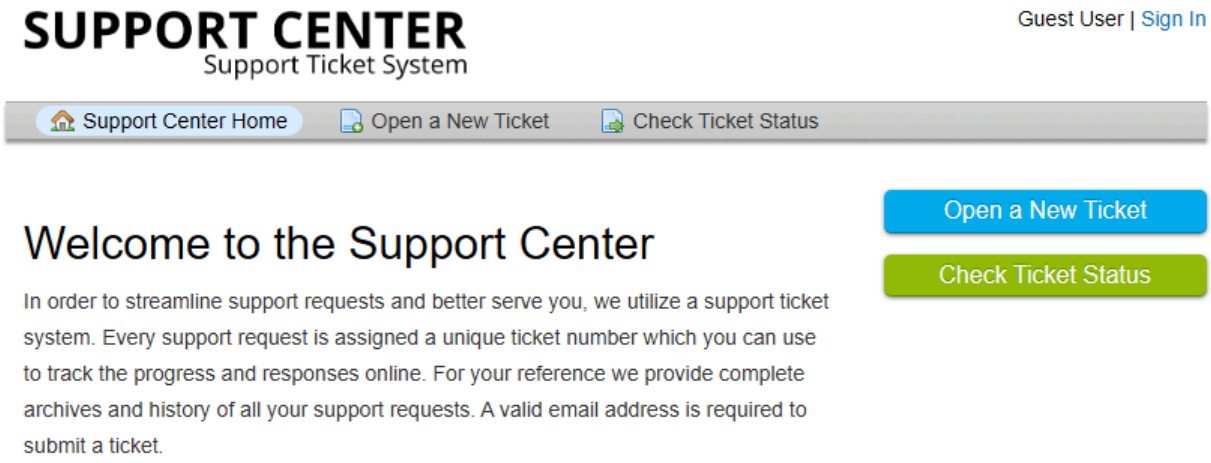
- Copy your Public IP Address

Next go back to your Virtual Machine by Remote Accessing it.



- Type “https://”yourIPaddresshere”/osTicket/ and see if the page opens up!
- If it doesn’t work, add :443 at the then to access port 443

Try it out on your own system. To double confirm.



You may get a warning, but just visit the link anyways and it should work!

1.4. Getting your own Domain and SSL Certificate

1.4.1. Domain Setup

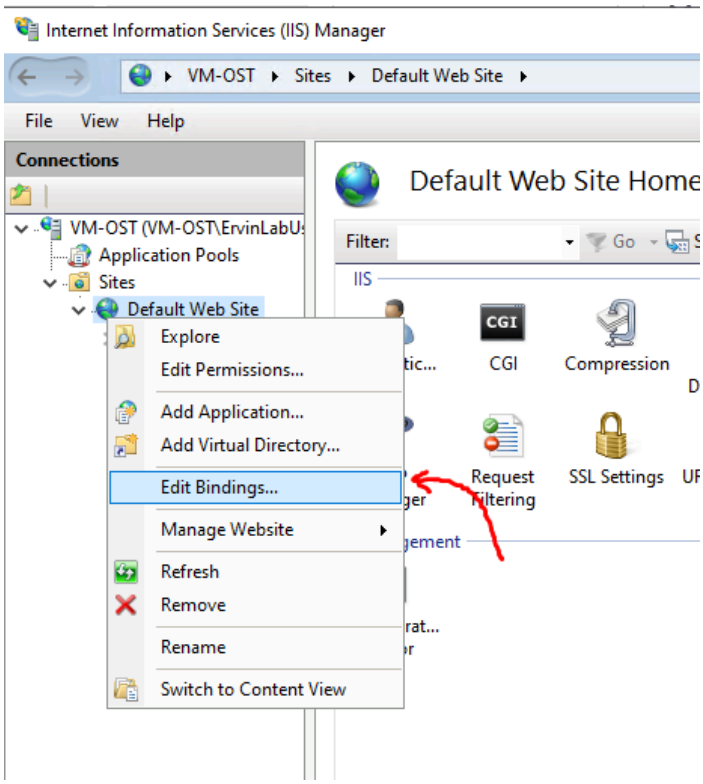
For this, I won't be going through the step by step guide on getting your own domain and setting it up, but I'll provide YouTube video links to help guide you.

I use namecheap.com for purchasing my own domain for pretty cheap. You can then use this YouTube video to setup your domain:
https://www.youtube.com/watch?v=851IbWp7aEw

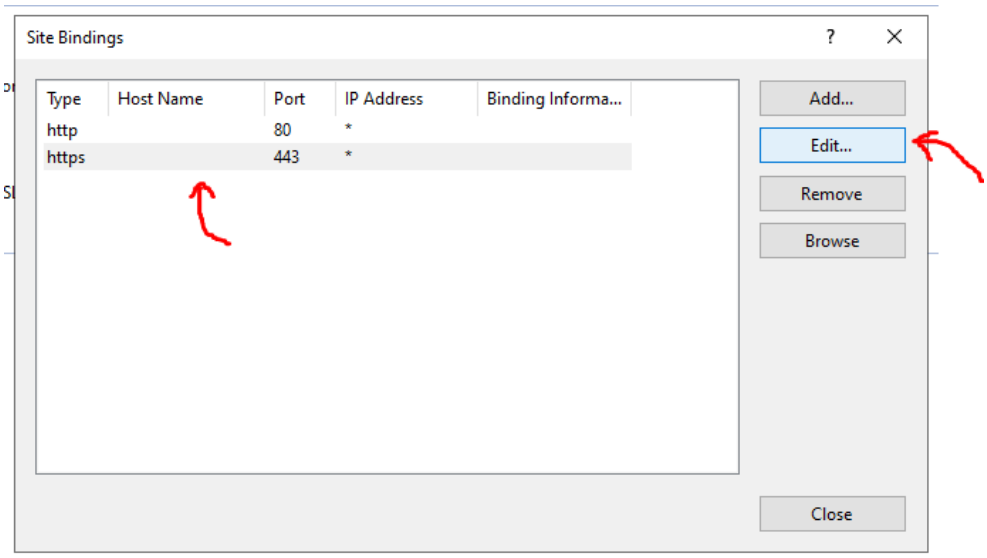
1.4.2. SSL Certificate Setup

1.4.2.1. Configure Host Bindings in IIS

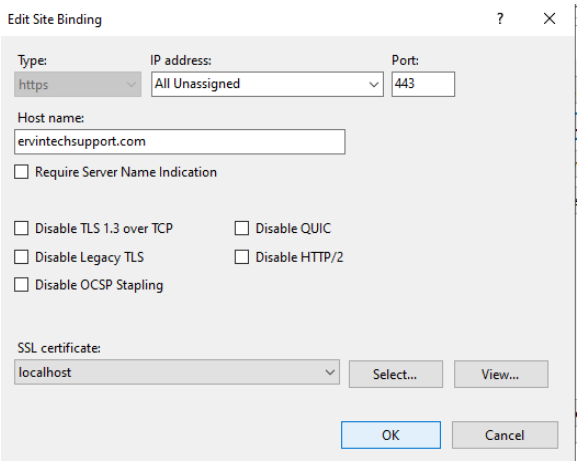
To set up an SSL, it does take a number of steps to do it for free.
First we'll have to set up our IIS to have the current bindings to work with win-ACME. Remote Access your Virtual Machine and search for IIS Manager there.



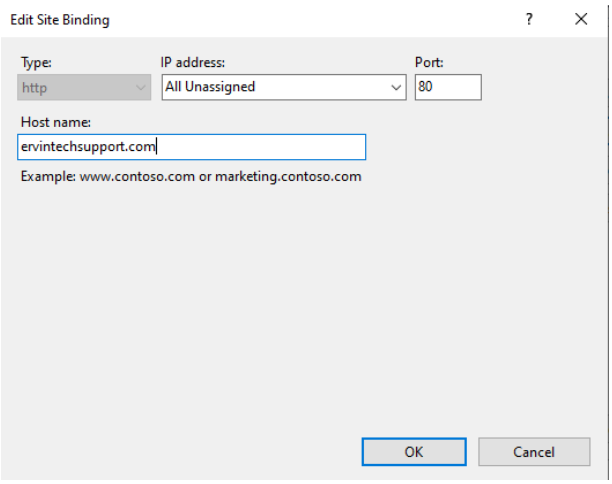
- Select "Edit Bindings…"



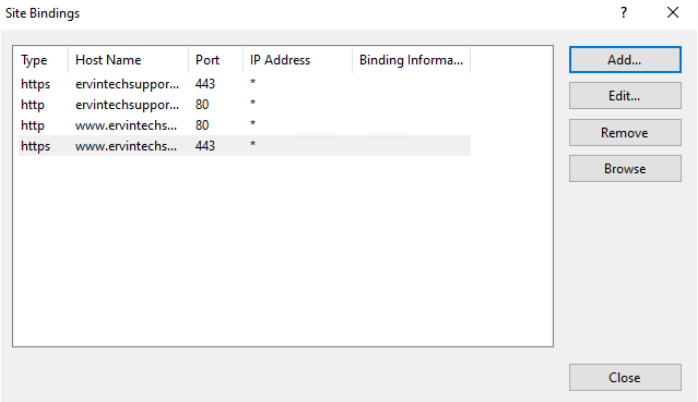
- Select “Edit…”



- You’ll then fill out the Host name, keep the SSL certificate to localhost for now. That’ll be rebinded later



- You’ll also have to fill out the host name for port 80 (HTTP) as well.

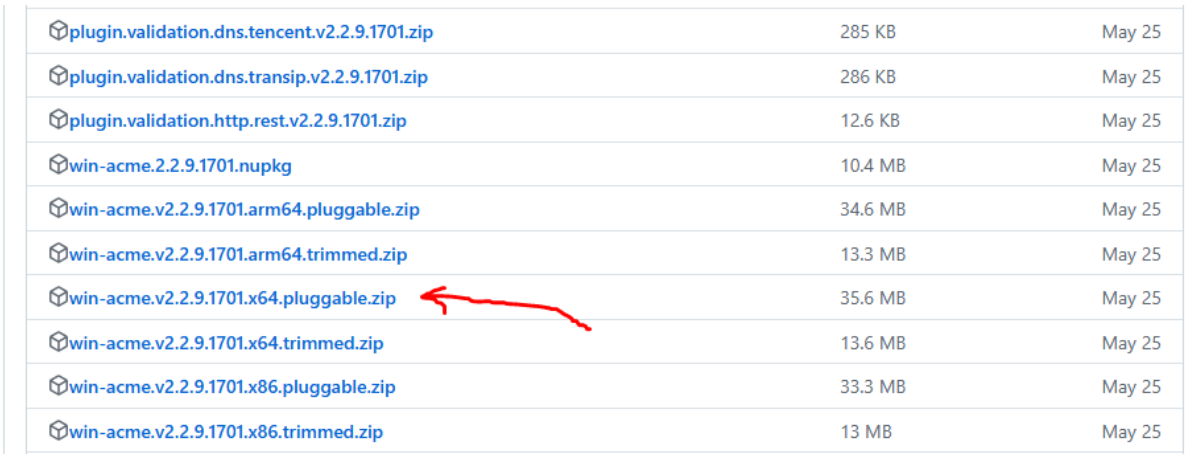


- I’ve also included the (www.) separately. Do this same to avoid potential future problems
- You’ll now have Port 443 and Port 80 (HTTPS and HTTP) both with the hostname of your domain.
- Close the IIS Manager

1.4.2.2. Install Win-ACME and Generate an SSL Certificate

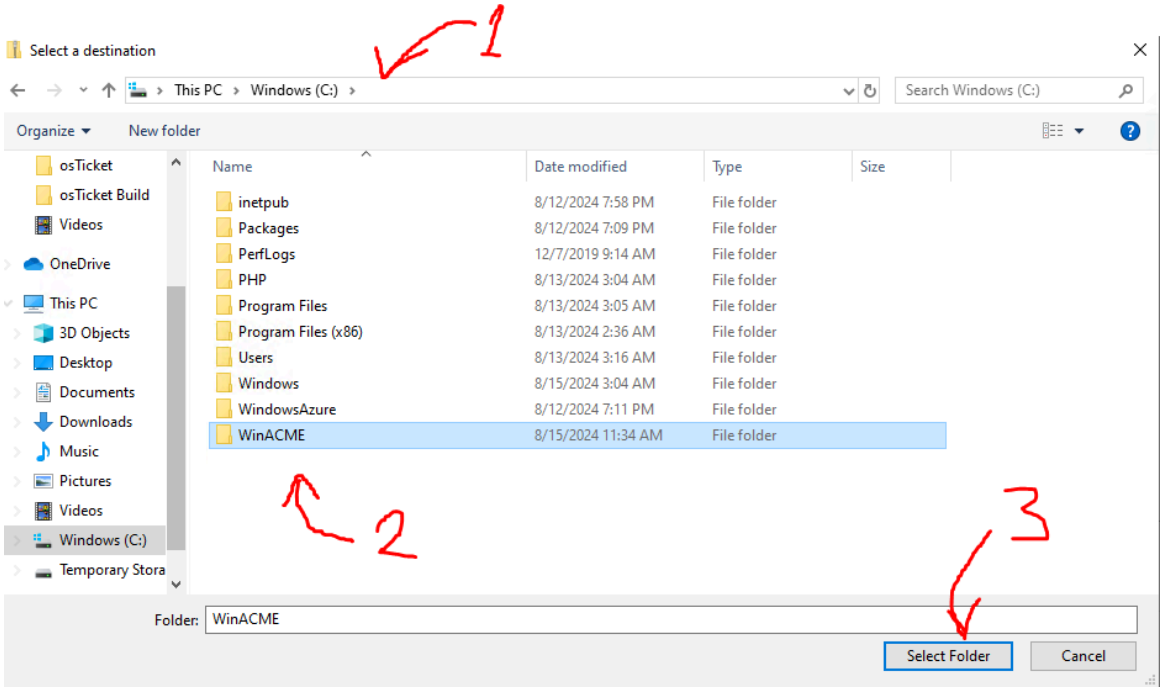
Secondly we'll install Win-ACME for Let's Encrpyt:

Go to: [Releases · win-acme/win-acme · GitHub]



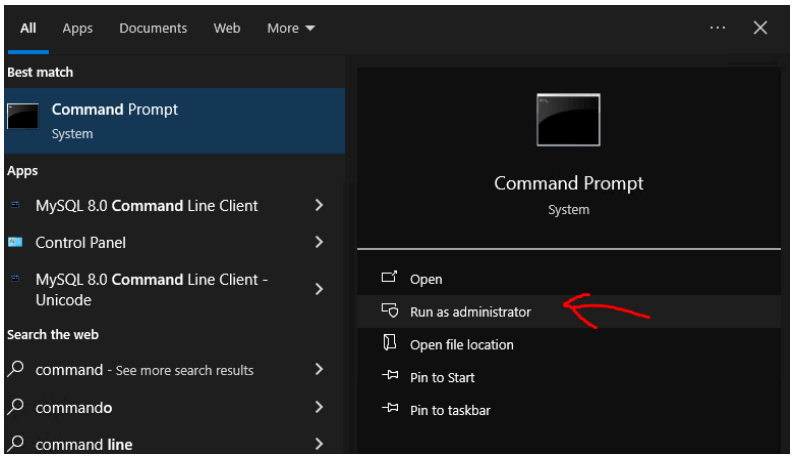
plugin.validation.dns.tencent.v2.2.9.1701.zip	285 KB	May 25
plugin.validation.dns.transip.v2.2.9.1701.zip	286 KB	May 25
plugin.validation.http.rest.v2.2.9.1701.zip	12.6 KB	May 25
win-acme.2.2.9.1701.nupkg	10.4 MB	May 25
win-acme.v2.2.9.1701.arm64.pluggable.zip	34.6 MB	May 25
win-acme.v2.2.9.1701.arm64.trimmed.zip	13.3 MB	May 25
win-acme.v2.2.9.1701.x64.pluggable.zip	35.6 MB	May 25
win-acme.v2.2.9.1701.x64.trimmed.zip	13.6 MB	May 25
win-acme.v2.2.9.1701.x86.pluggable.zip	33.3 MB	May 25
win-acme.v2.2.9.1701.x86.trimmed.zip	13 MB	May 25

- Scroll down to Assets
- Look for the latest win-acme version that is "pluggable" - this means it includes all plugins.
- Make sure it's x64 too, that's for 64 bit. (86x refers to 32 bit)
- Make sure it's NOT arm64 either. arm64 is designed for ARM-based processors - typically found in some laptops, tablets, and certain types of servers.



- Go to C:/ and create a folder called WinACME

- Extract the zipped file into the C:/WinACME



- Open a Command Prompt with Administrator Privileges

win-acme 2.2.9.1701

```
Microsoft Windows [Version 10.0.19045.4780]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ErvinLabUser1>iisreset /restart

Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted

C:\Users\ErvinLabUser1>cd c:\winACME

c:\WinACME>wacs.exe

 A simple Windows ACMEv2 client (WACS)
 Software version 2.2.9.1701 (release, pluggable, standalone, 64-bit)
 Connecting to https://acme-v02.api.letsencrypt.org/...
 Connection OK!
 Scheduled task not configured yet
 Please report issues at https://github.com/win-acme/win-acme

 N: Create certificate (default settings)
 M: Create certificate (full options)
 R: Run renewals (0 currently due)
 A: Manage renewals (0 total)
 O: More options...
 Q: Quit

 Please choose from the menu: n
```

- Make sure your IIS Manager is closed
- Type “iisreset /restart” - this will reset your IIS so the new bindings have been applied
- Navigate to the directory where you extracted WinACME

    - So type “cd C:\winACME”
- Run this command, “wacs.exe”
- Type N for creating a new certificate with the default settings

Select win-acme 2.2.9.1701

```
c:\WinACME>wacs.exe

 A simple Windows ACMEv2 client (WACS)
 Software version 2.2.9.1701 (release, pluggable, standalone, 64-bit)
 Connecting to https://acme-v02.api.letsencrypt.org/...
 Connection OK!
 Scheduled task not configured yet
 Please report issues at https://github.com/win-acme/win-acme

 N: Create certificate (default settings)
 M: Create certificate (full options)
 R: Run renewals (0 currently due)
 A: Manage renewals (0 total)
 O: More options...
 Q: Quit

 Please choose from the menu: n

 Running in mode: Interactive, Simple

 Please select which website(s) should be scanned for host names. You may
 input one or more site identifiers (comma-separated) to filter by those
 sites, or alternatively leave the input empty to scan *all* websites.

 1: Default Web Site (2 bindings)

 Site identifier(s) or <Enter> to choose all: <Enter>

 1: ervintechsupport.com (Site 1)
 2: www.ervintechsupport.com (Site 1)

 Listed above are the bindings found on the selected site(s). By default all
 of them will be included, but you may either pick specific ones by typing the
 host names or identifiers (comma-separated) or filter them using one of the
 options from the menu.

 P: Pick bindings based on a search pattern
 A: Pick *all* bindings

 Binding identifiers(s) or menu option: a

 1: ervintechsupport.com
 2: www.ervintechsupport.com

 Please pick the main host, which will be presented as the subject of the certificate: 1

 1: ervintechsupport.com (Site 1)
 2: www.ervintechsupport.com (Site 1)

 Continue with this selection? (y*/n) - yes
```

- First press “Enter” to see all the bindings
- The press “A” as you want to pick all the bindings
- Then type “1” to assign a certificate to the first domain
- Then type “y” as yes to continue with this selection

```
win-acme 2.2.9.1701

Please select which website(s) should be scanned for host names. You may
input one or more site identifiers (comma-separated) to filter by those
sites, or alternatively leave the input empty to scan *all* websites.

1: Default Web Site (1 binding)

Site identifier(s) or <Enter> to choose all: <Enter>

1: ervintechsupport.com (Site 1)

Listed above are the bindings found on the selected site(s). By default all
of them will be included, but you may either pick specific ones by typing the
host names or identifiers (comma-separated) or filter them using one of the
options from the menu.

P: Pick bindings based on a search pattern
A: Pick *all* bindings

Binding identifiers(s) or menu option: 1

1: ervintechsupport.com (Site 1)

Continue with this selection? (y*/n) - yes

Source generated using plugin IIS: ervintechsupport.com

Terms of service:    C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\LE-SA-v1.4-April-3-2024.pdf

Open in default application? (y/n*)
```

- Prior to this, you may be asked to see the subscriber agreement
- Type “y” for continuing with the select
- Then type “y” to open the terms and services

Version 1.4
3 April 2024
Page 1 of 6

Let’s Encrypt

Subscriber Agreement

This Subscriber Agreement **(“Agreement”)** is a legally binding contract between you and, if applicable, the company, organization or other entity on behalf of which you are acting (collectively, **“You” or “Your”**) and Internet Security Research Group **(“ISRG,” “We,” or “Our”)** regarding Your and Our rights and duties relating to Your acquisition and use of SSL/TLS digital certificates issued by ISRG.

If you are acting on behalf of a company, organization or other entity, You represent that you have the authority to bind such entity to this Agreement.

1. Definitions and Terms

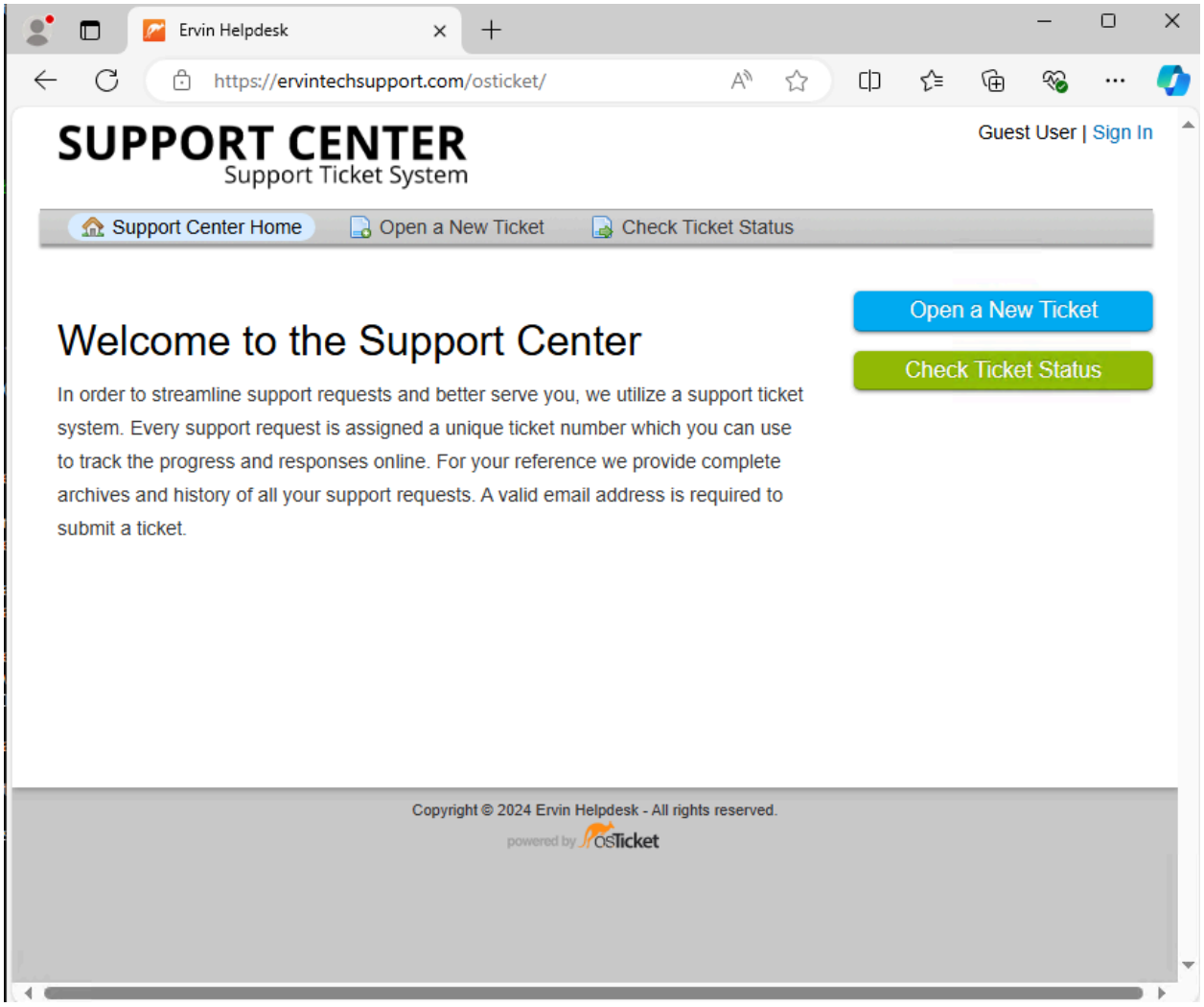
- Feel free to read through this

```
Adding renewal for [IIS] (any site), (any host)
Next renewal due after 2024/10/9
Certificate [IIS] (any site), (any host) created

N: Create certificate (default settings)
M: Create certificate (full options)
R: Run renewals (0 currently due)
A: Manage renewals (1 total)
O: More options...
Q: Quit

Please choose from the menu:
```

- After all that, it should be complete. We don't need to worry about a certificate for option 2, as it is automatically applied to it.



Your IT Helpdesk is now set up with your SSL certificate and a domain name! 😀

2. Conclusion

Setting up and securing your IT Helpdesk on a Windows 10 Virtual Machine in Azure involves several critical steps, from configuring a self-signed SSL certificate for initial HTTPS access to setting up an official SSL certificate using Win-ACME and Let's Encrypt for a custom domain. By carefully configuring IIS bindings, managing firewall rules both in Azure and on the VM itself, and verifying web server access, you've successfully deployed a live, secure osTicket environment.

This process not only enhances the security of your helpdesk but also prepares your system for real-world scenarios, ensuring reliable and secure service for users. Congratulations on completing the setup!