F5 Cloud Training Bootcamp

Consistent Security Policy in Multi-cloud Environment Lab

TMOS Version: 14 - 13

Lab enviornments: Azure - Ravello

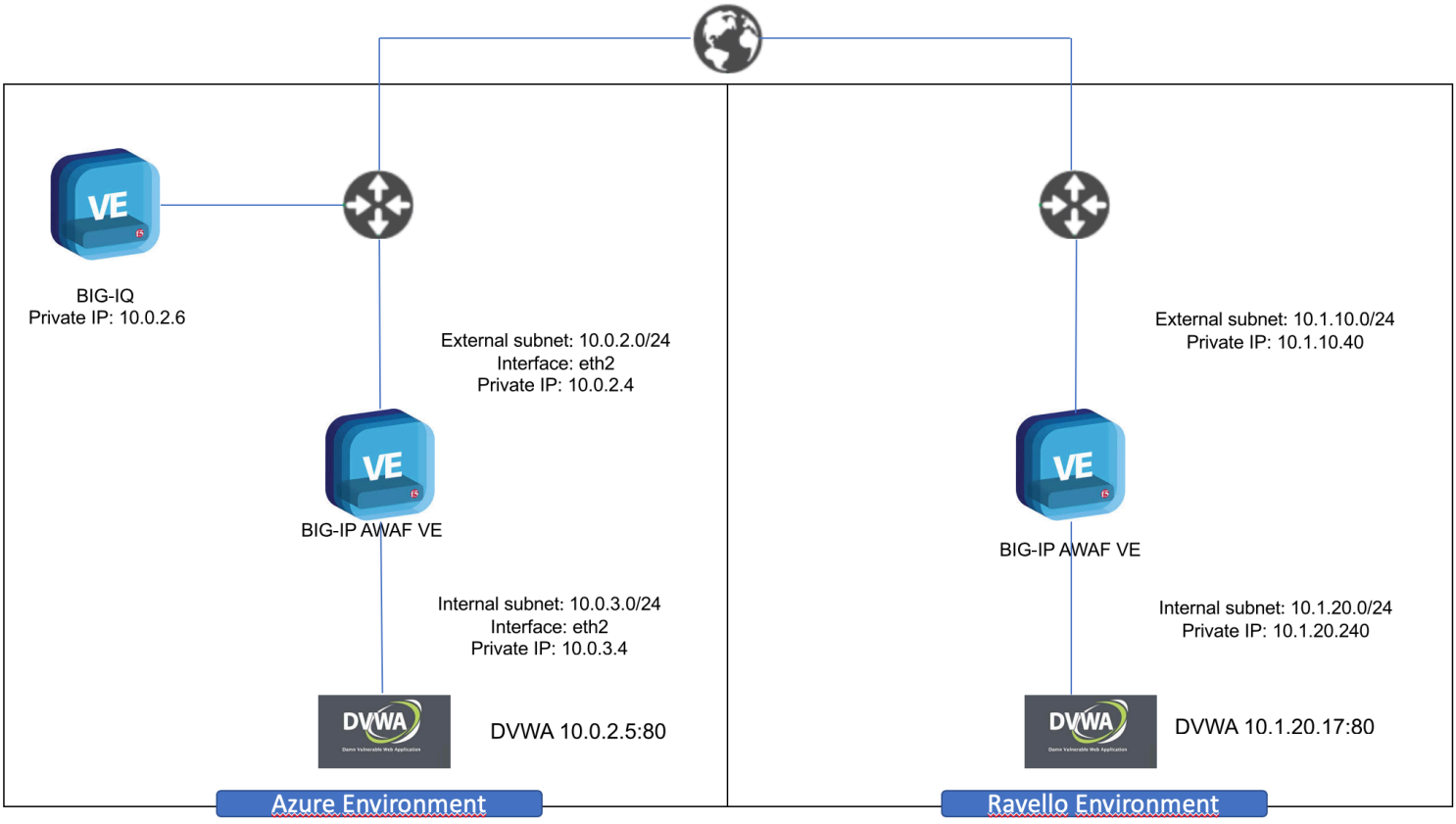
Windows 7 External

LAMP 4

BIG-IQ

Tabla de contenido

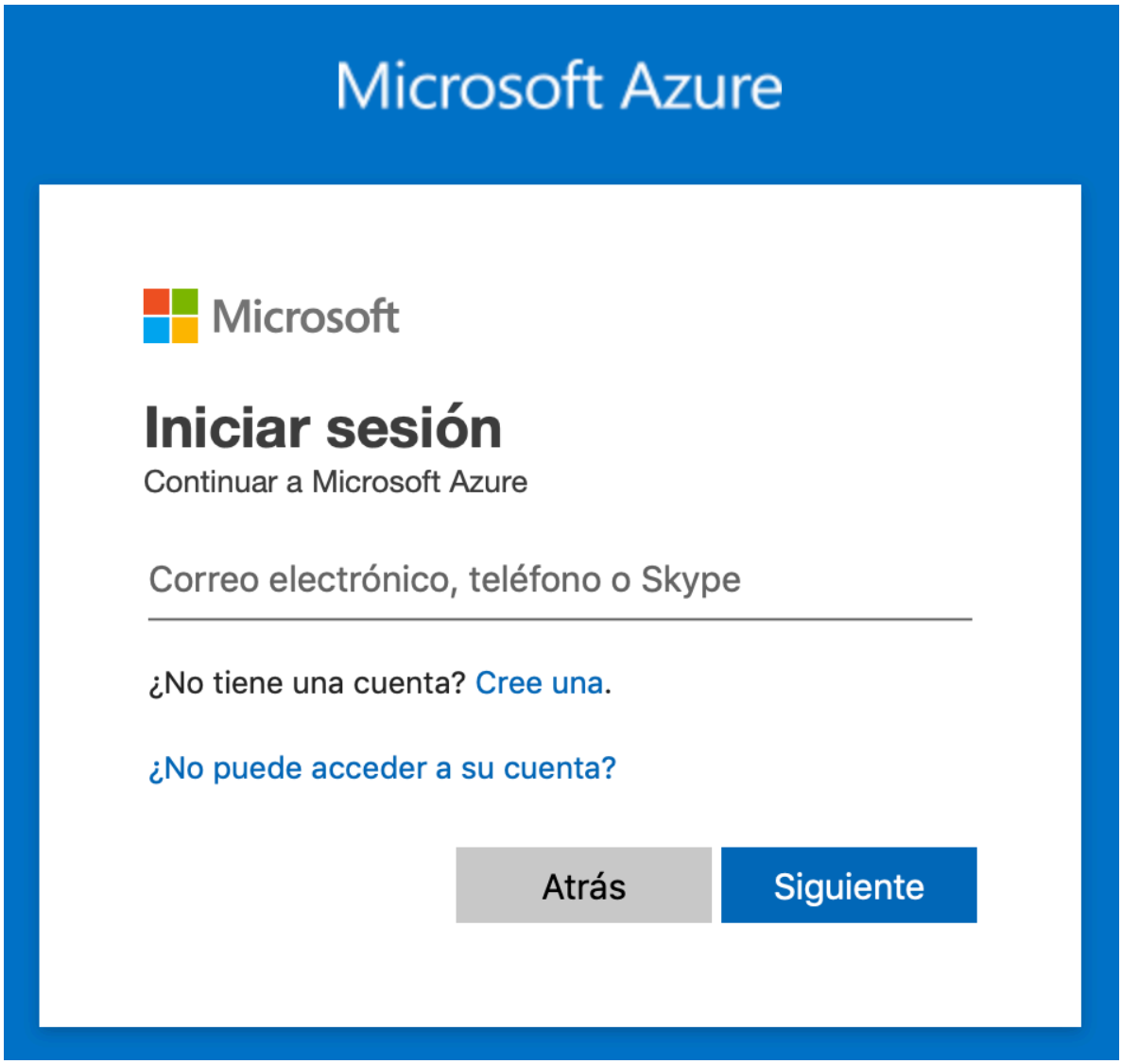
Training Lab Architecture



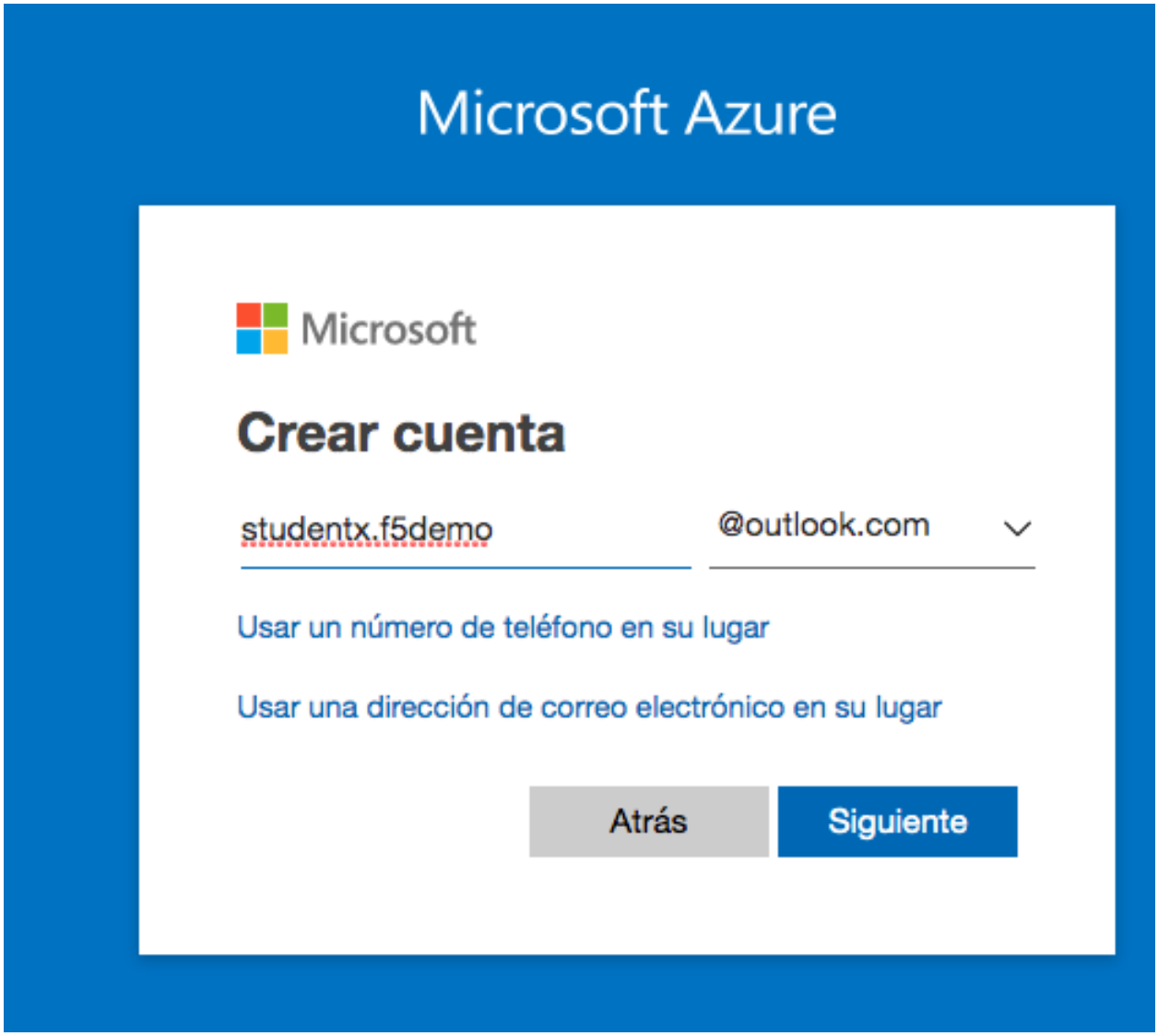
Part 1- F5 Azure ARM Template Deploying the BIG-IP VE in Azure - 3 NIC

Task 1 – Azure Login

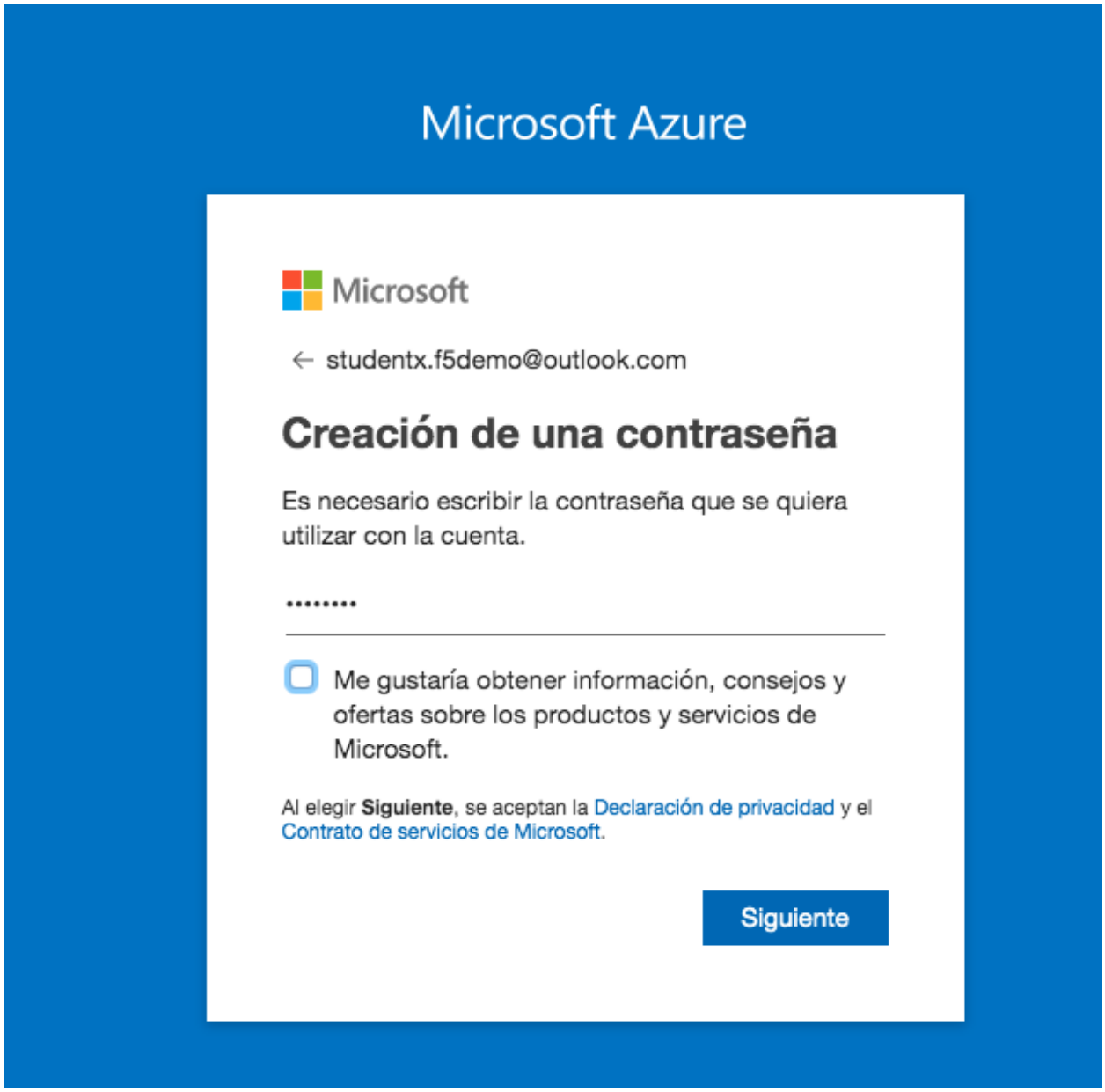
You will need to access Microsoft Azure Portal in order to deploy the required virtual systems.



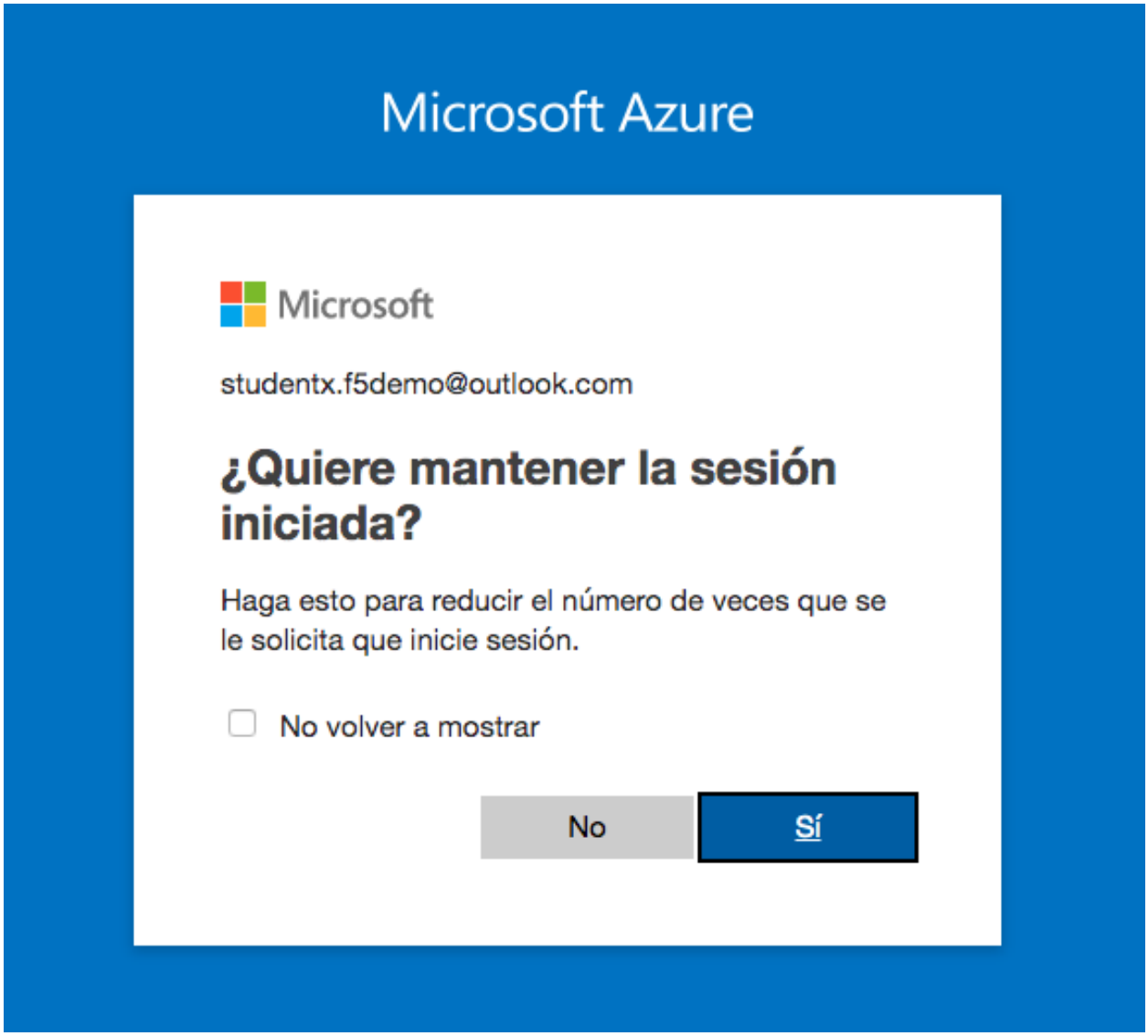
We will use studentx.f5demo with the domain outlook.com, replace the “x” with your student number:



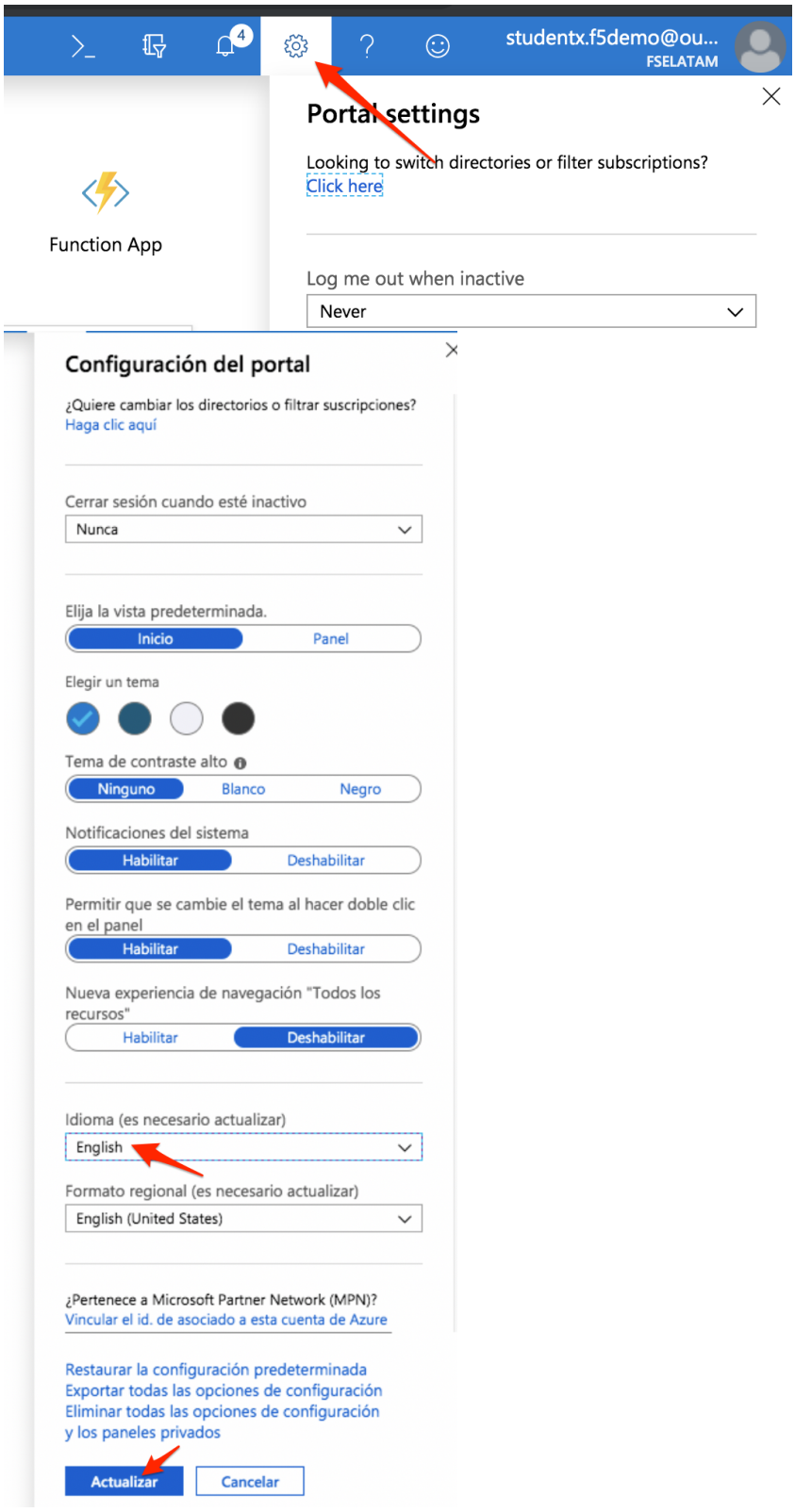
If password asked use “$$Fs3L4t4m$$” without quotes and click on next:



Azure will ask you if you wanna keep your session started we will choose “yes”:

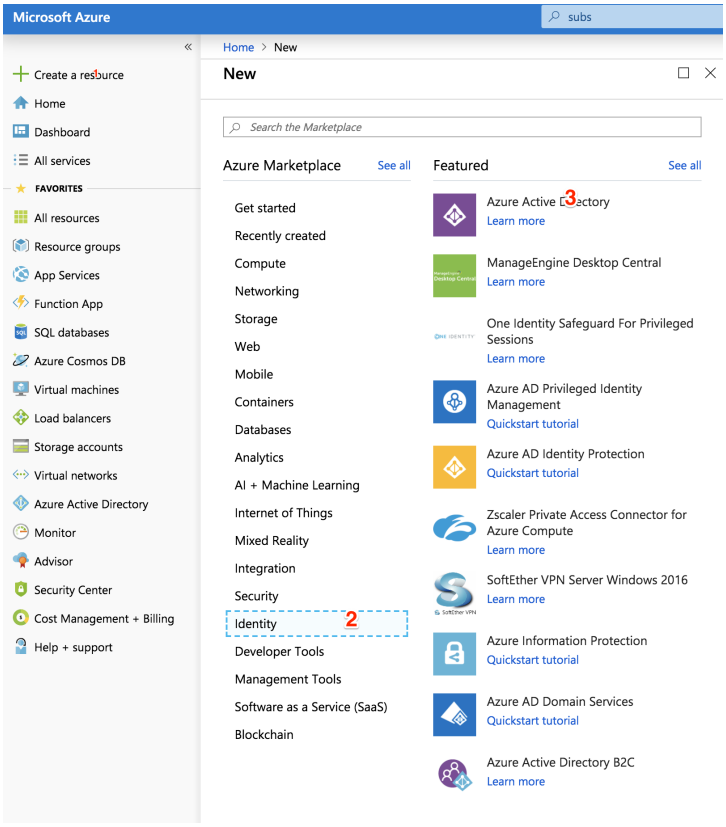


Click on the gear on the right and change the language to English to make more easy to go through this guide:



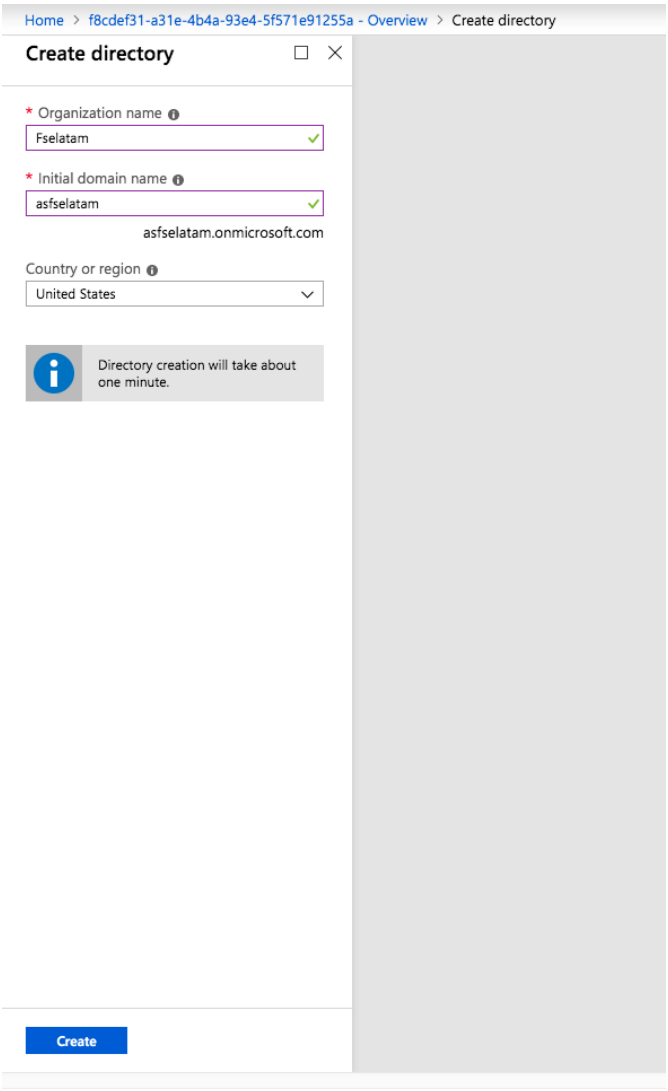
Create a directory:

Select **Create a resource**, select **Identity**, and then select **Azure Active Directory**.

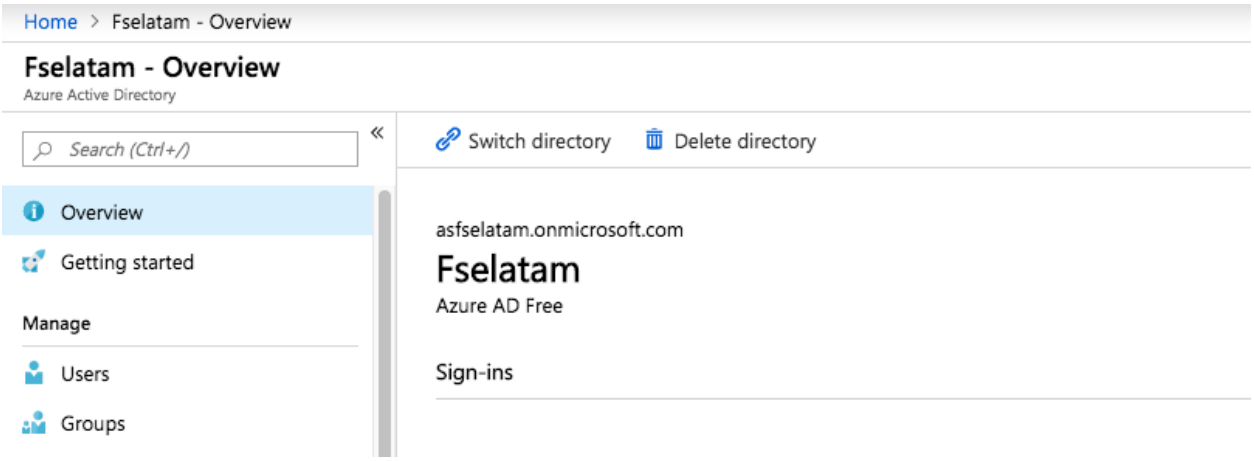


The **Create directory** page appears.

Fill up with the name of the organization **fselatamsx** and with the initial domain name **asxfselatam** where **x** is your student number and click on create:



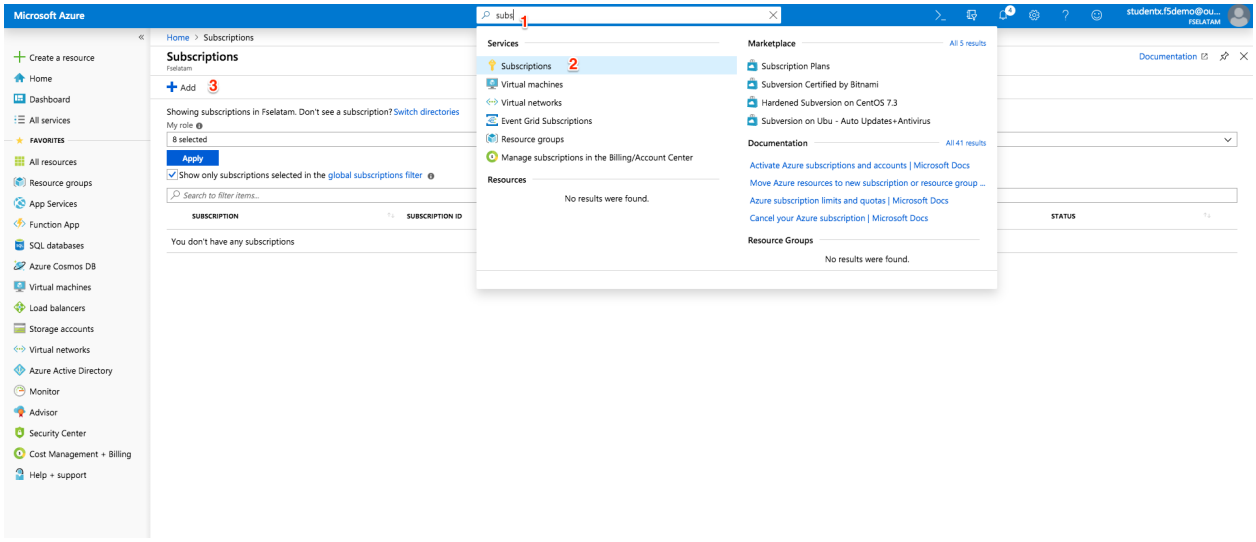
And now you can check under **Azure Active Directory** the directory you already created:



Create a subscription:

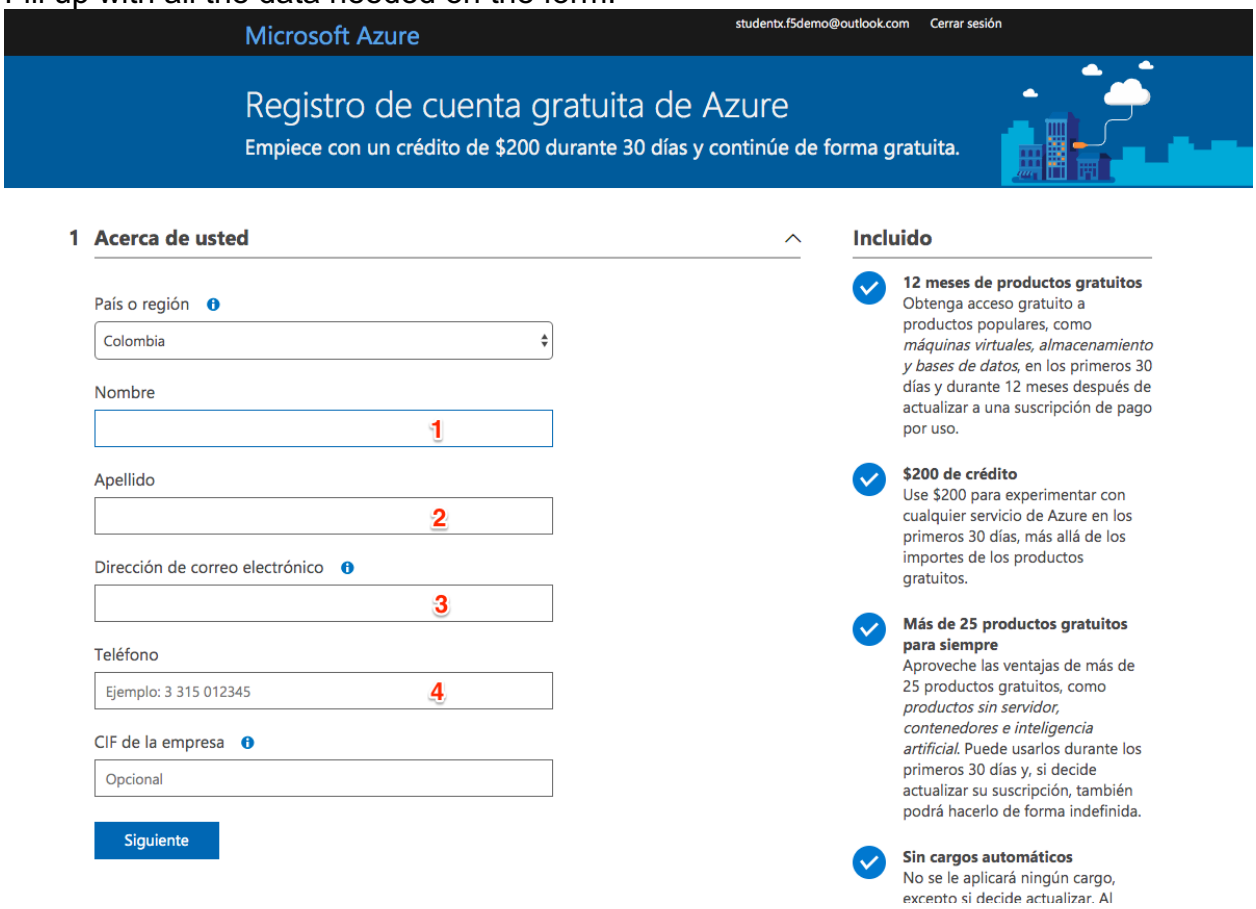
Note: you will need for this step a credit card and a valid phone number to get SMS.

On the search pane you will write “Subs” and click on **Subscriptions** after you will add a new one:

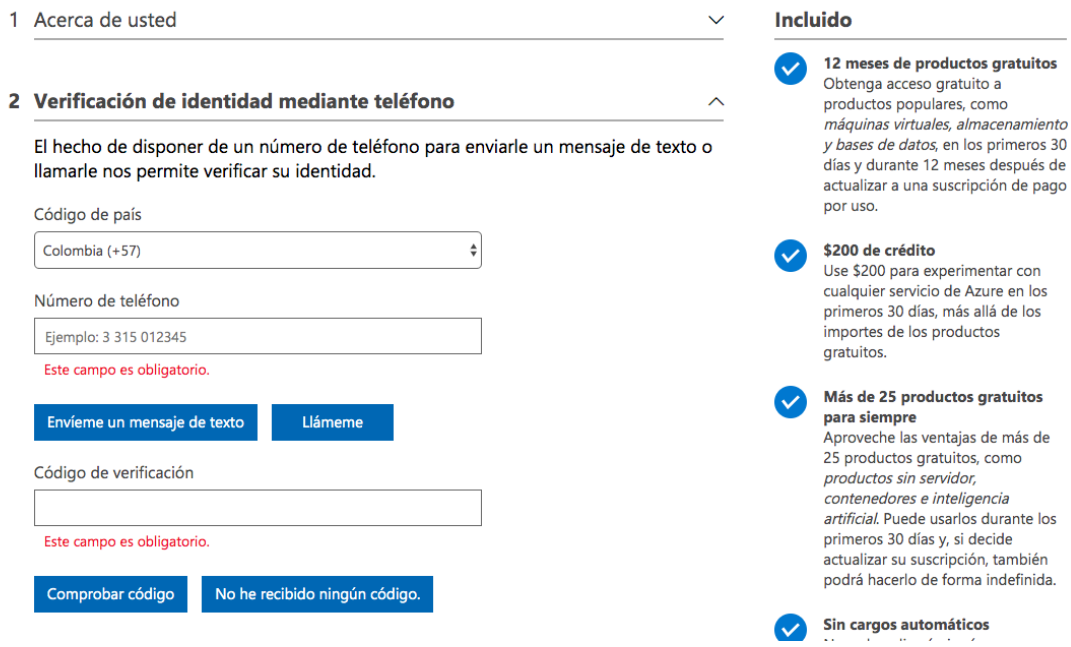


choose the free evaluation option:

Fill up with all the data needed on the form:

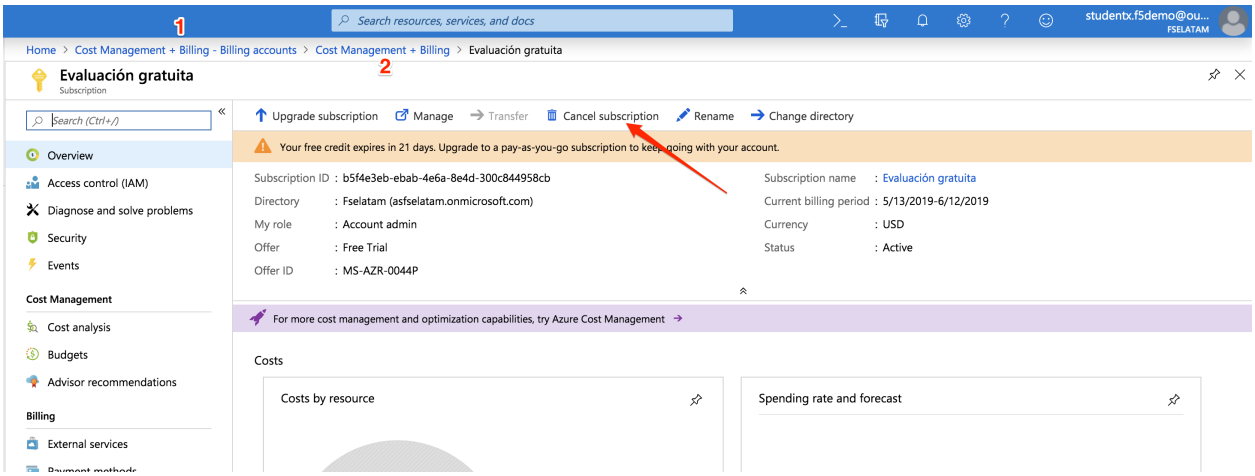


Confirm it with your phone number:



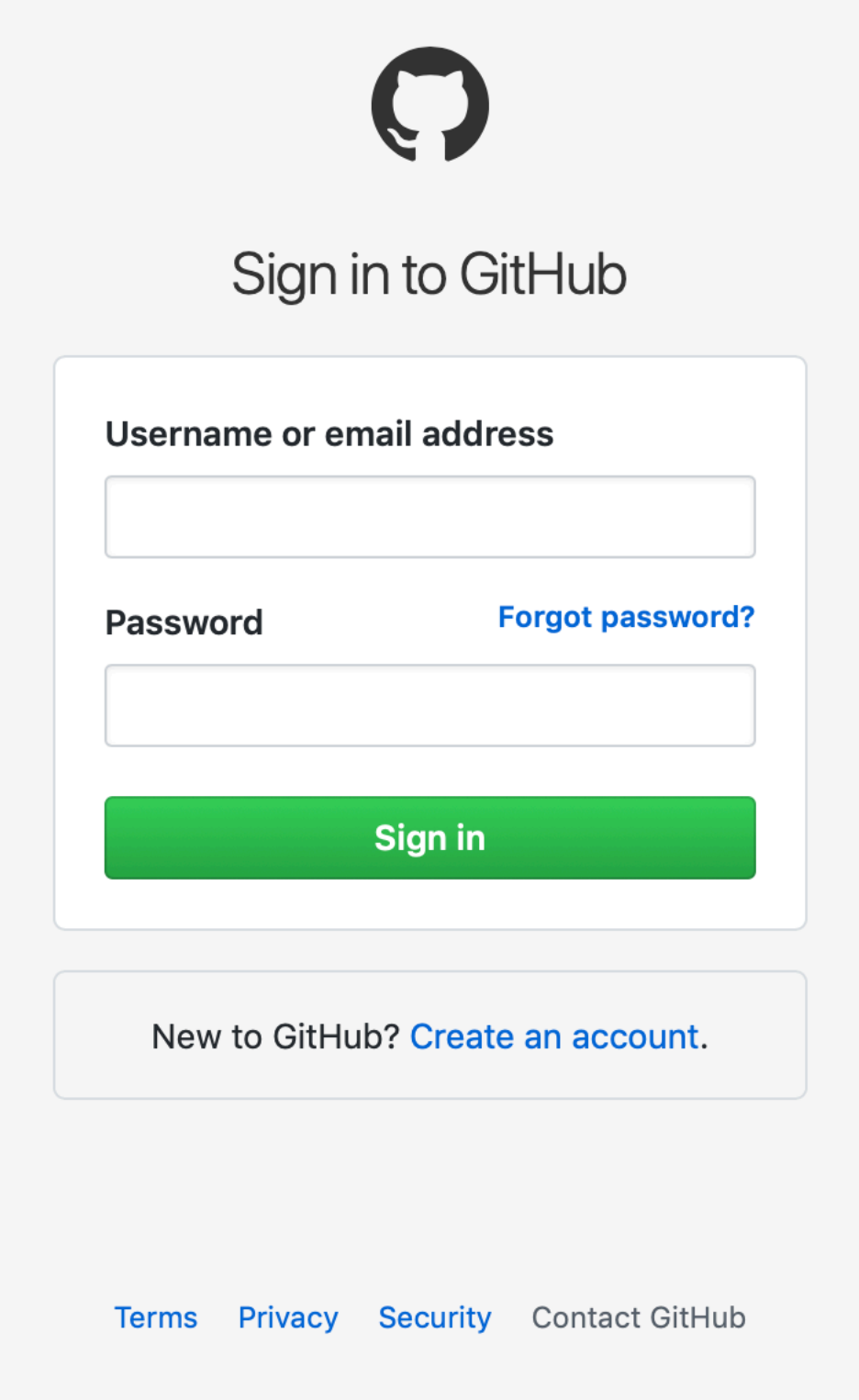
(Optional) Cancel a Subscription:

NOTE: you need to do this after the lab is over and to don't get billed for azure resources used in this lab.



Task 2 – Github Login

Create a Github account: https://github.com/



Task 3 – Deploy the BIG-IP VE in Azure - 3 NIC

This solution uses an ARM template to launch a three NIC deployment of a cloud-focused BIG-IP VE in Microsoft Azure. Traffic flows from the BIG-IP VE to the dvwa application. This is the standard on-premise-like cloud design where the BIG-IP VE instance is running with a management, front-end application traffic (Virtual Server) and back-end application interface.

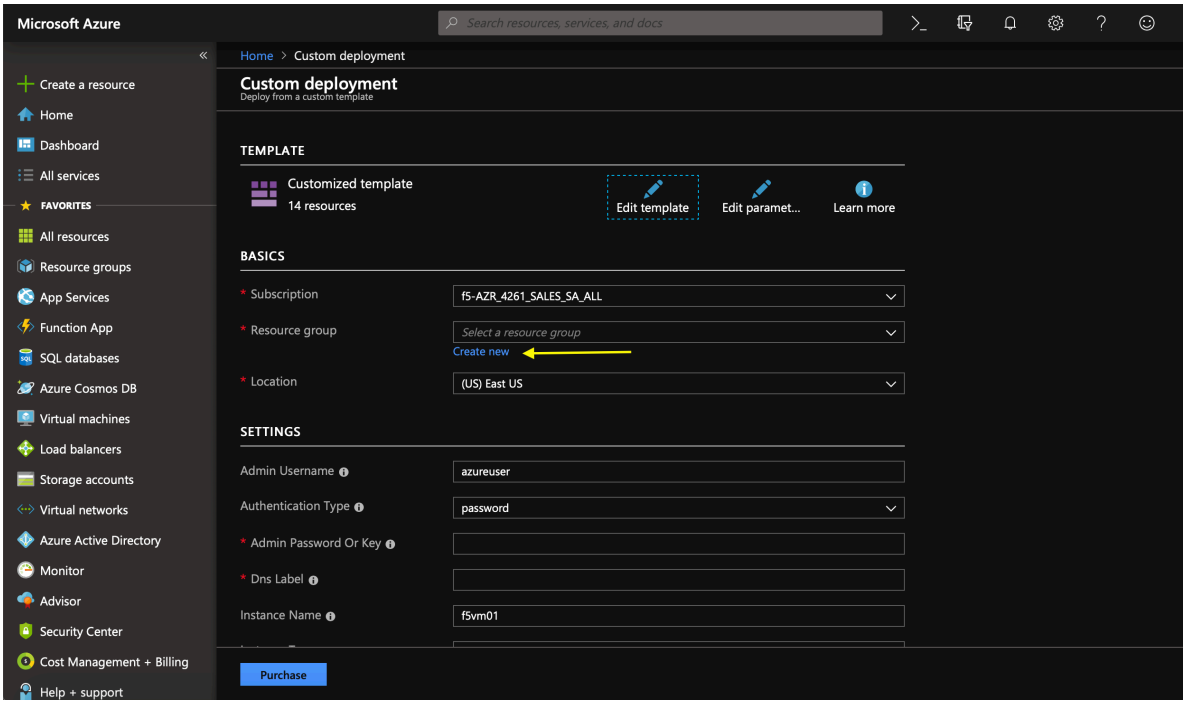
Access to the following link:

https://github.com/F5Networks/f5-azure-arm-templates/tree/master/supported/standalone/3nic/new-stack/byol

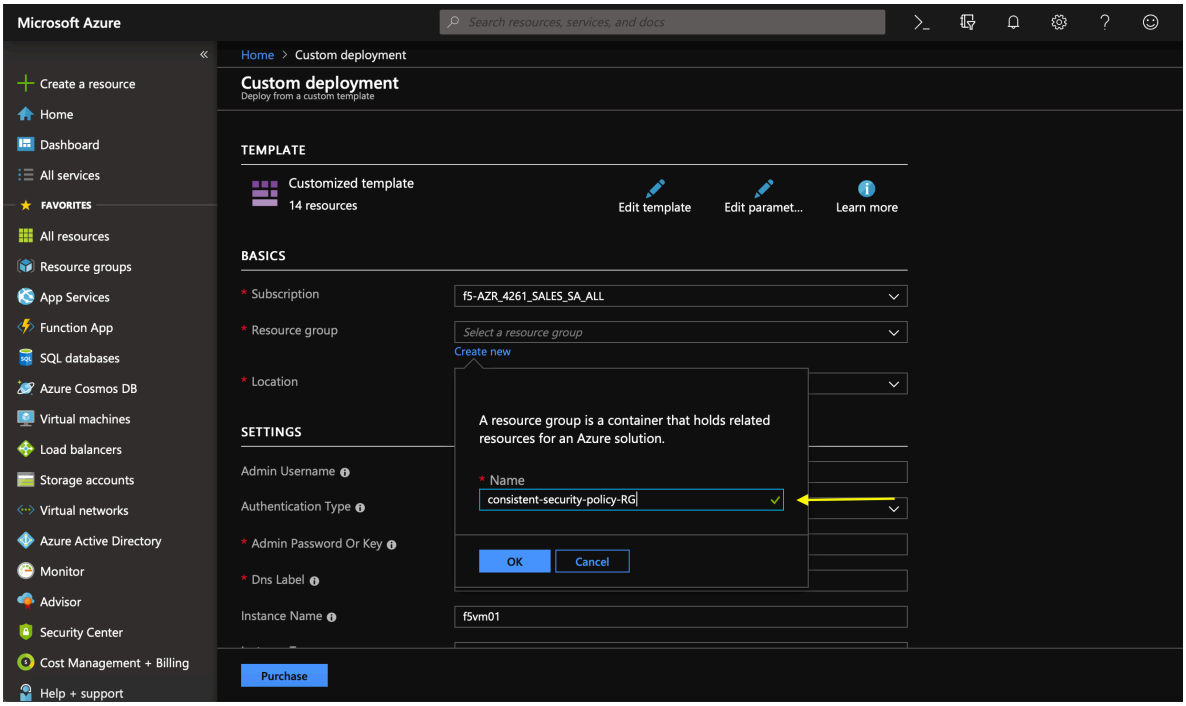
- Navigate the page and click on Deploy to Azure button: This allows you to use an existing BIG-IP license.

This action takes you to the Azure portal.

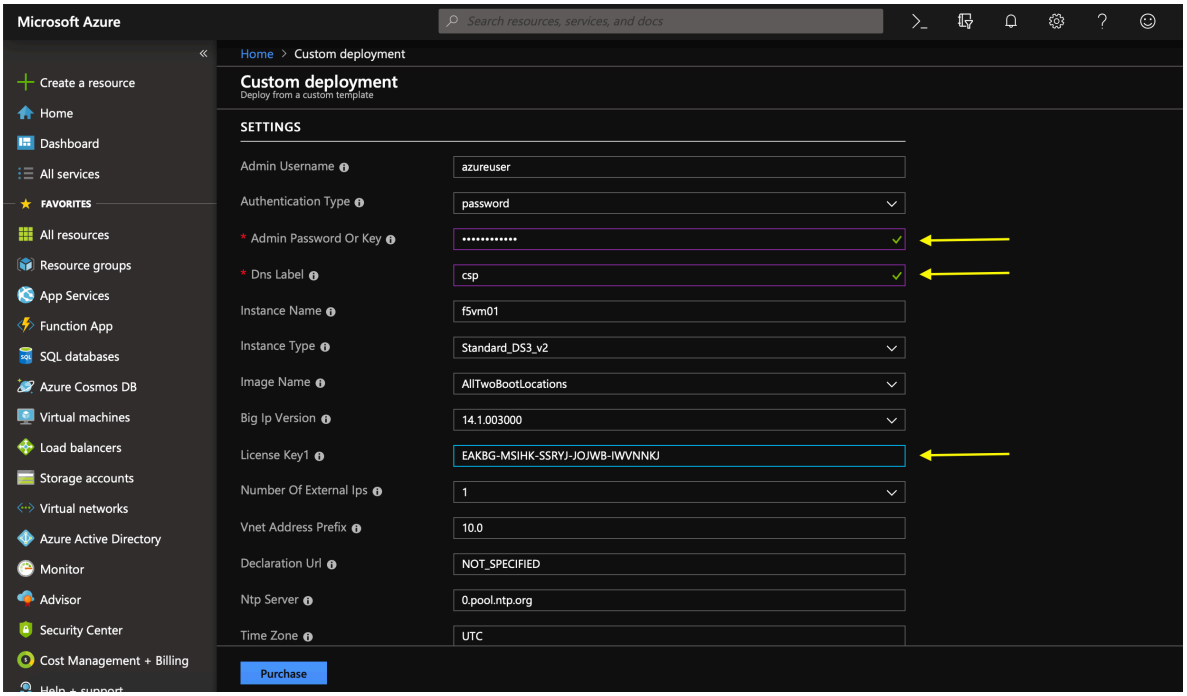
- Click on “Create new”



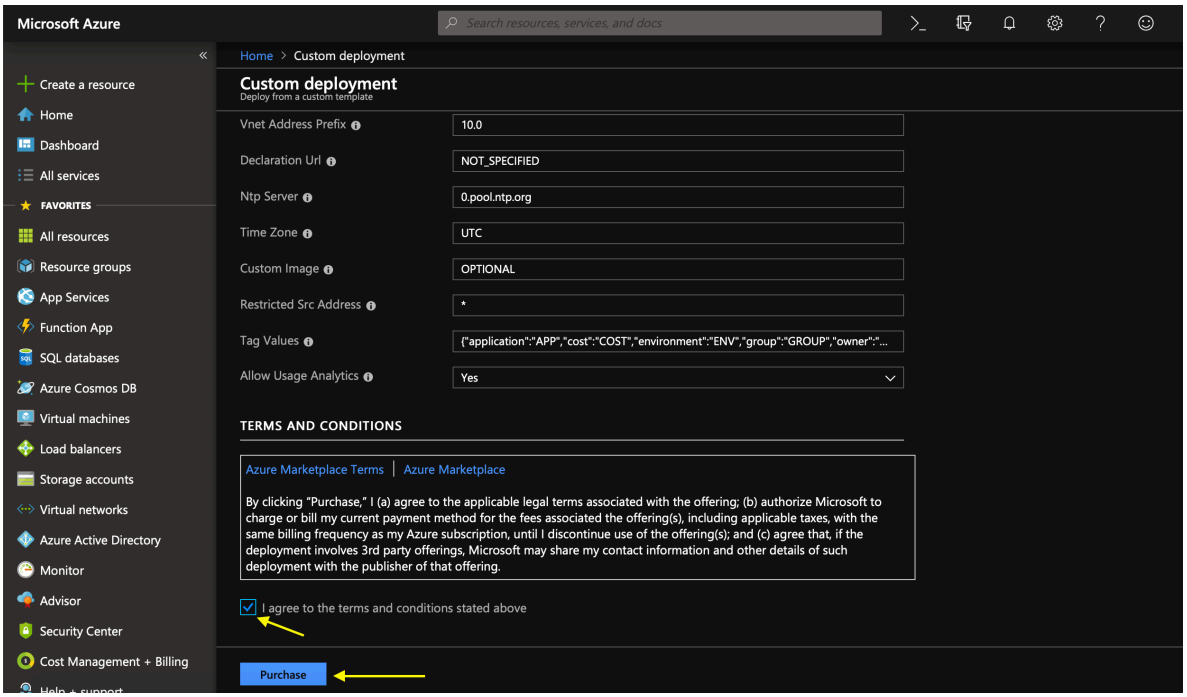
- Give a name to the resource group and click in “OK” and make sure the Location is set on “(US) East US”.



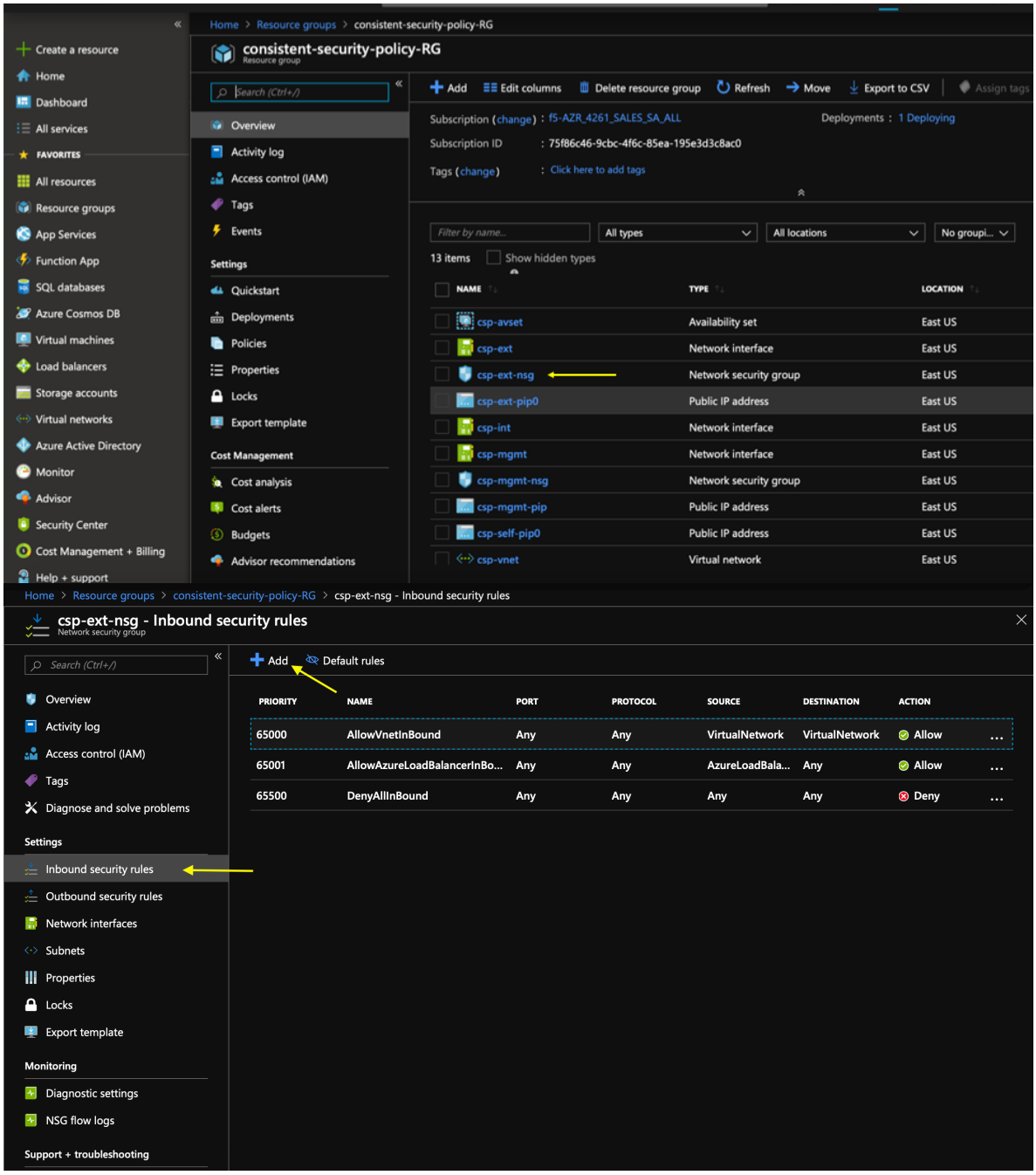
- Set an Admin Password and a DNS label. Then use a F5-BIG-VE-BT-25M-V16-LIC license.



- Accept the terms and conditions and click con “Purchase”



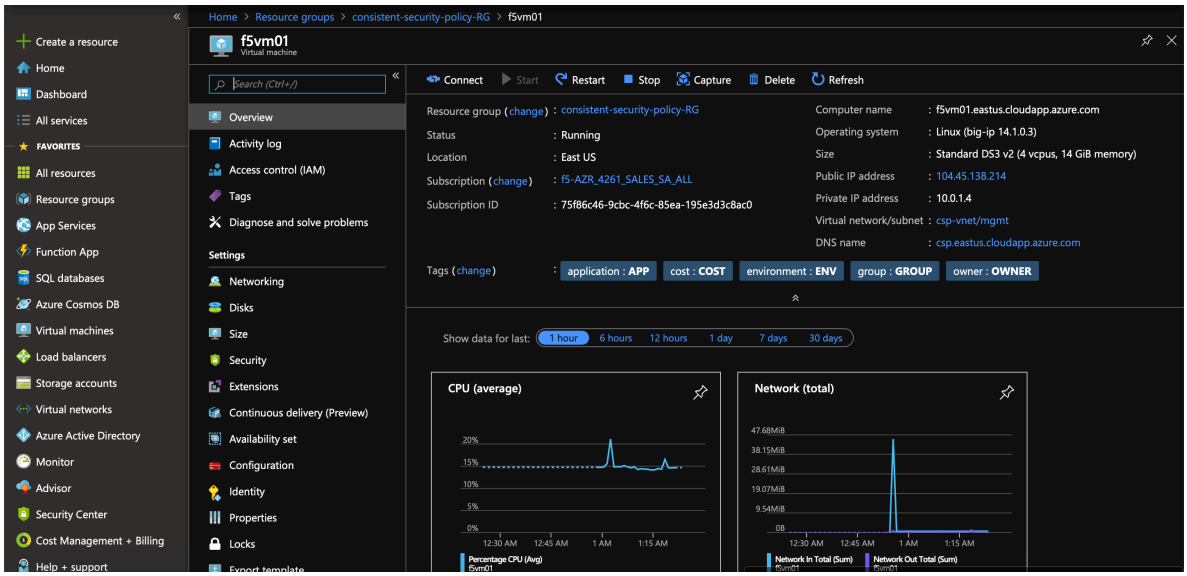
- Navigate to the Resource Groups label. You will find the configured objects. Click on >Network security group> Inbound security rules> Add



- Use the Following information and then click “Add”:

Source	IP Addresses
Source IP Addresses/CIDR Ranges	Set your public IP address
Destination Port Ranges	80
Name	Port_80

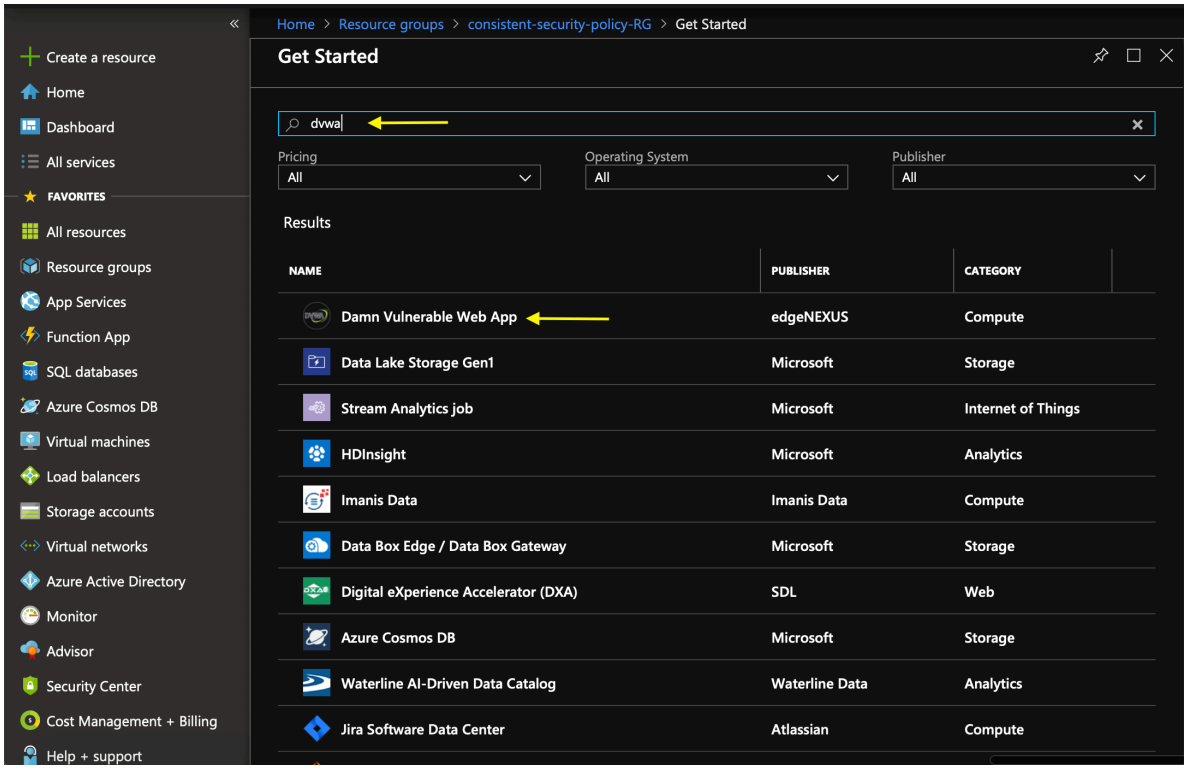
- Navigate to the Resource Group and find the f5vm01. This is the deployed BIG-IP.



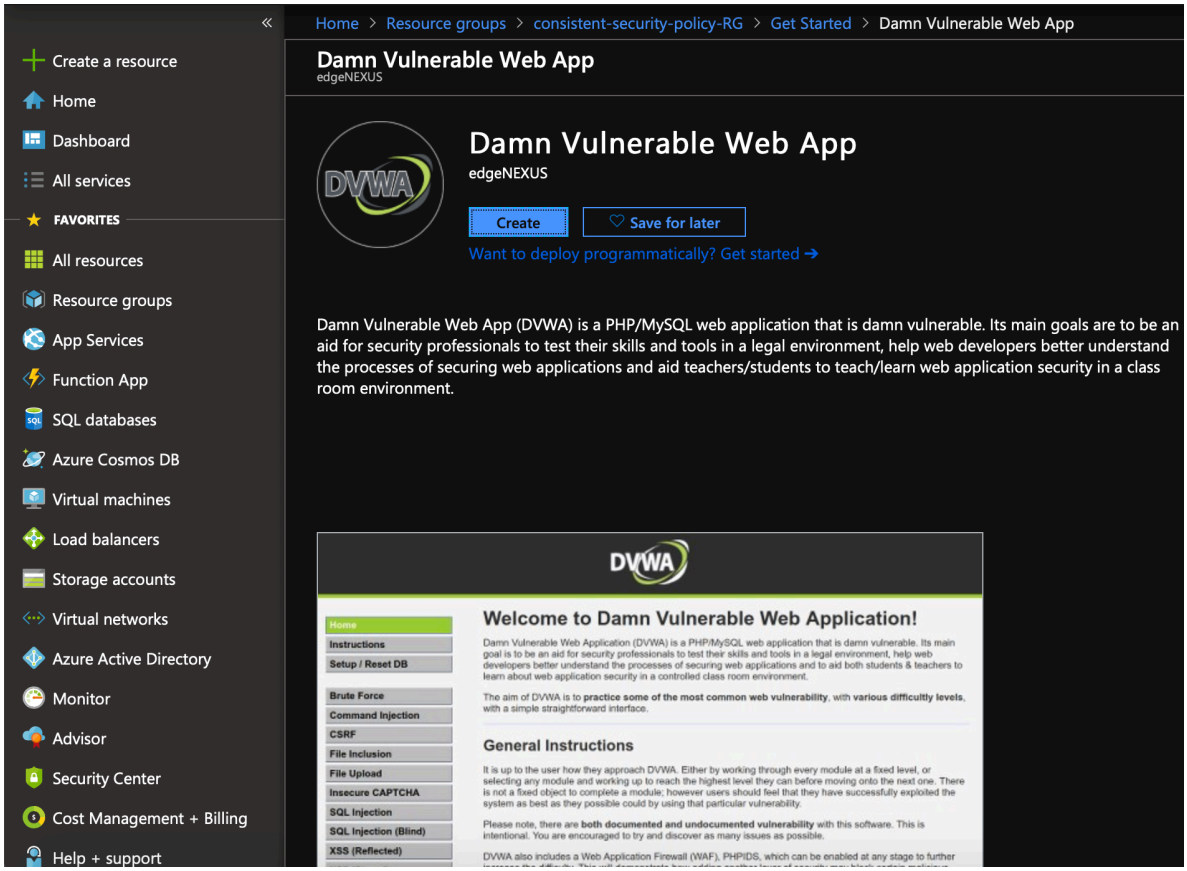
- Test connectivity to the BIG-IP by entering the Public IP address in a web browser. Navigate to Self IPs and note that there exist 2 IPs, associated to an external and internal VLAN.
- Provision ASM Module: System>Resource Provisioning > ASM > Nominal

Task 4 – Deploy a DVWA

- Navigate to the Resource Group and click on “Add”
- In the search field write “dvwa”, press enter and click on Damn Vulnerable Web App by edgeNEXUS.


Create a resource
Home
Dashboard
All services
FAVORITES
All resources
Resource groups
App Services
Function App
SQL databases
Azure Cosmos DB
Virtual machines
Load balancers
Storage accounts
Virtual networks
Azure Active Directory
Monitor
Advisor
Security Center
Cost Management + Billing
Help + support
Home > Resource groups > consistent-security-policy-RG > Get Started
Get Started
dvwa
Pricing
All
Operating System
All
Publisher
All
Results
NAME
PUBLISHER
CATEGORY
Damn Vulnerable Web App
edgeNEXUS
Compute
Data Lake Storage Gen1
Microsoft
Storage
Stream Analytics job
Microsoft
Internet of Things
HDInsight
Microsoft
Analytics
Imanis Data
Imanis Data
Compute
Data Box Edge / Data Box Gateway
Microsoft
Storage
Digital eXperience Accelerator (DXA)
SDL
Web
Azure Cosmos DB
Microsoft
Storage
Waterline AI-Driven Data Catalog
Waterline Data
Analytics
Jira Software Data Center
Atlassian
Compute

- Click on “Create”



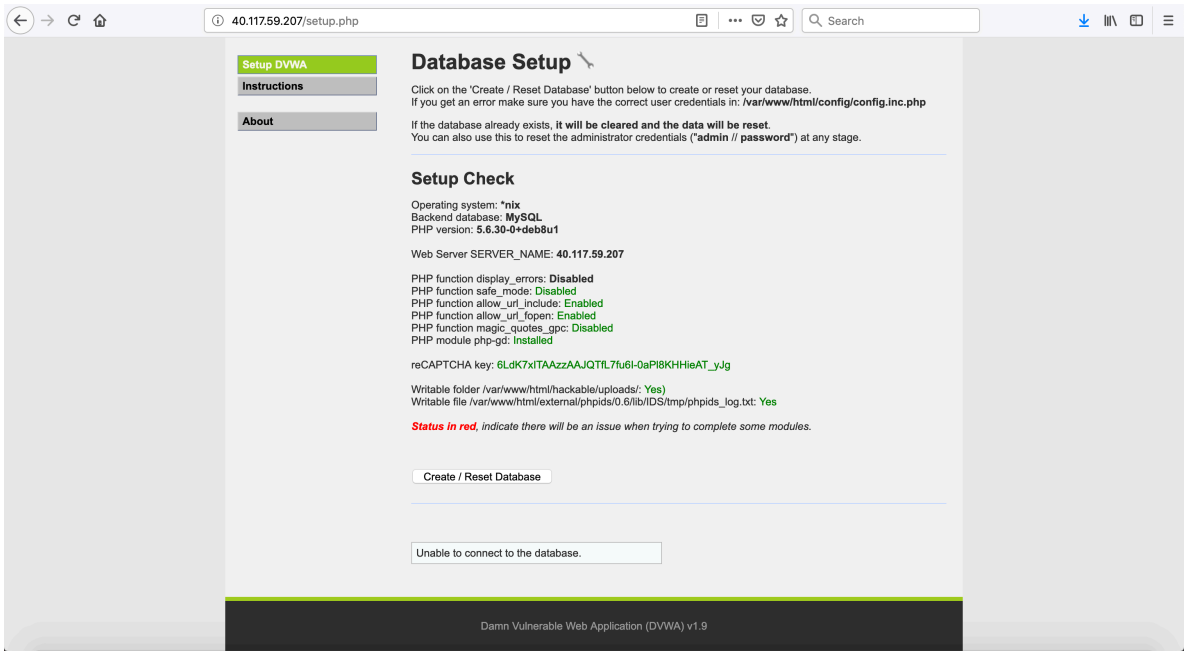
- Use the Following information and then click “Add”:

Resource Group	Select your RG
Virtual Machine Name	dvwa
Region	(US) East US
Authentication type	Password
Username	Set a user name
Password	Set a password and confirm it

- Click on “Review + Create”
- Navigate to the Resource Group, find the dvwa Network Security Group and use the following information for add an Inbound Security Rule:

Source	IP Addresses
Source IP Addresses/CIDR Ranges	Set your public IP address
Destination Port Ranges	80
Name	Port_80

- Test connectivity to the DVWA app by entering the Public IP address in a web browser. Click on Create/Reset Database.



Task 5 – Configure the DVWA app on the BIG-IP

- Use a web browser to access and log in to BIG-IP by the VM Public IP.
- Create a HTTP Monitor
  - Open the **Local Traffic > Monitors** page, and then click **Create**
  - Use the following information for the new monitor, and then click **Finished**.

Name	dvwa_monitor
Type	HTTP
Send String	GET \login.php\r\n

- Create a new Pool of Servers
  - Open the **Pools > Pool List** page, and then click **Create**
  - Use the following information for the new Pool of Servers, and then click **Finished**.

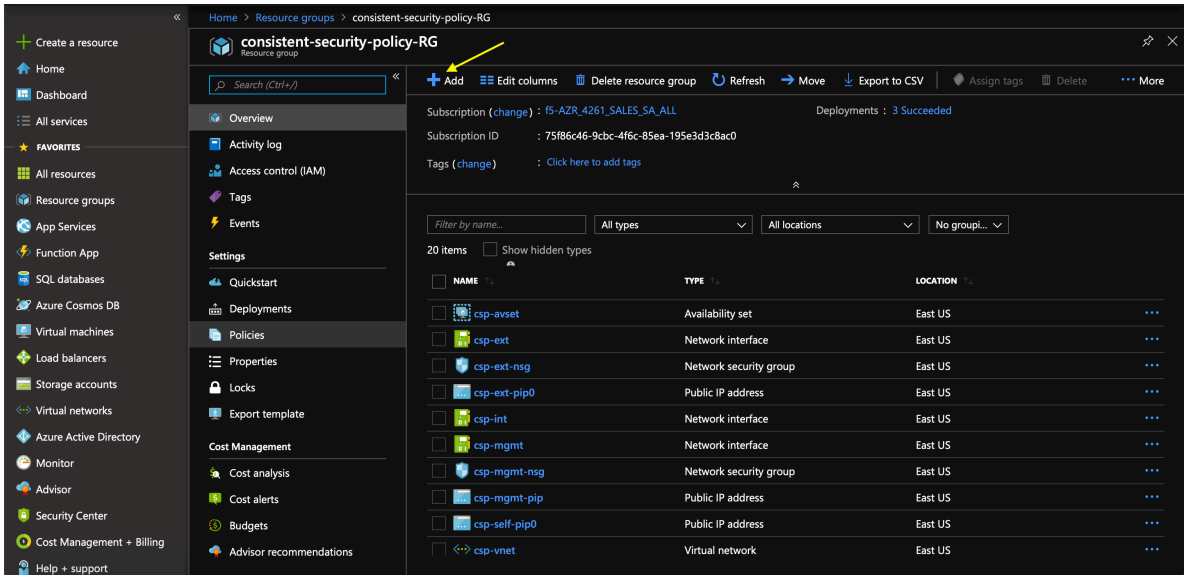
Name	dvwa_pool
Health Monitors	dvwa_monitor
New Members	Address: 10.0.2.5 Service Port: 80 *Click on **Add**

- Create a Virtual Server
  - Open the Local **Traffic > Virtual Servers > Virtual Server List** page, and then click **Create**
  - Use the following information for the new Virtual Server, and then click **Finished**.

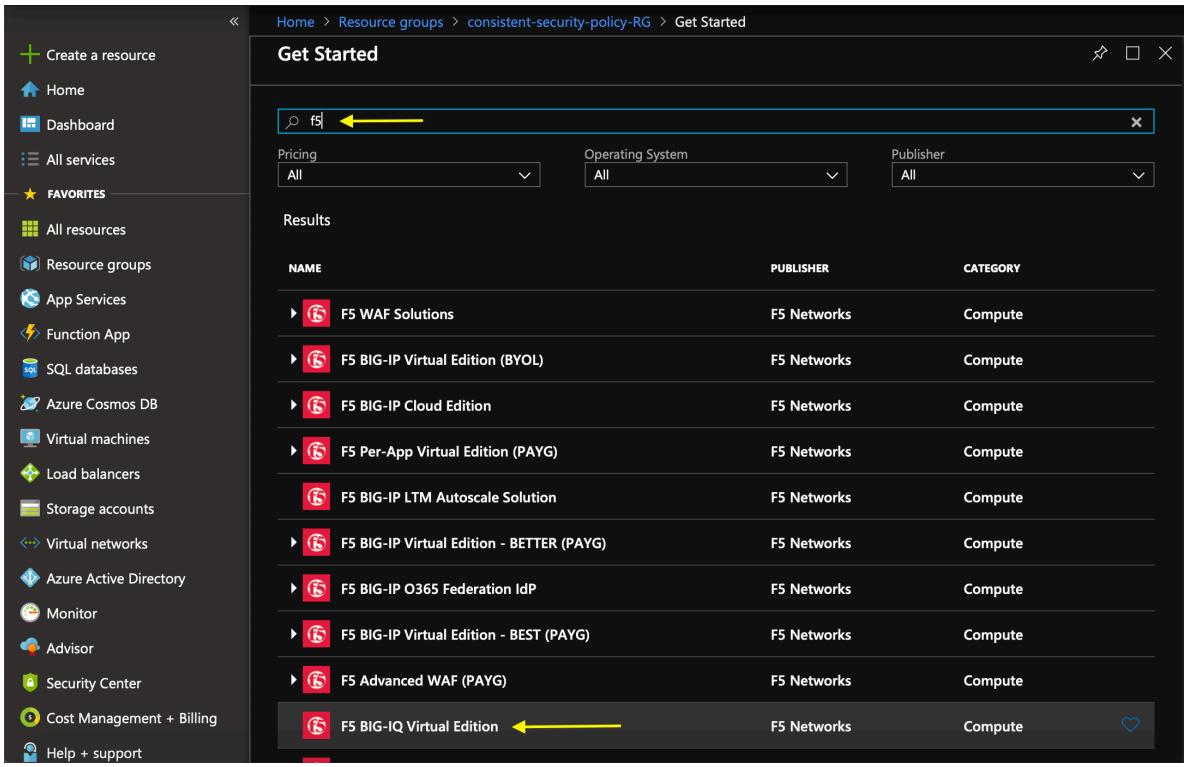
Name	dvwa_vs
Destination Address /Mask	10.0.2.4
Service Port	80
HTTP Profile	http
Source Address Translation	Auto Map
Default Pool	acme_pool

Task 6 – Deploy a BIG-IQ BYOL

- Navigate to the Resource Group and click on “Add”



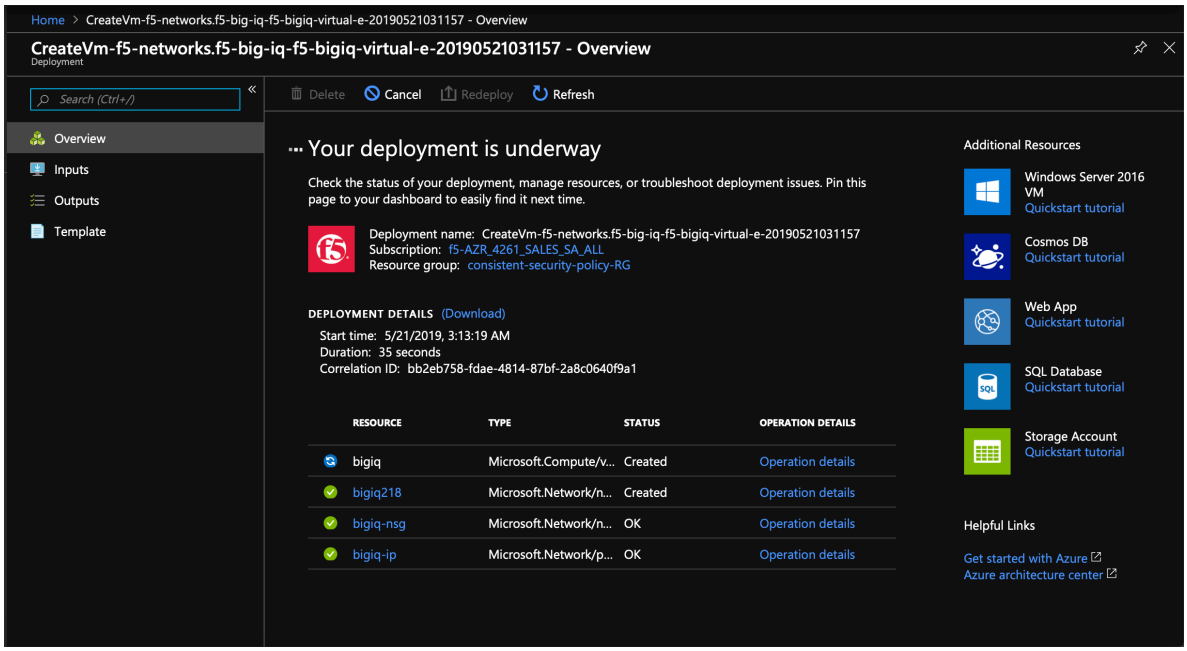
- Type f5 in the search field and press Enter
- Click on F5 BIG-IQ Virtual Edition



- Use the following information for the new BIG-IQ.

Resource Group	Choose your RG
Virtual Machine Name	bigiq
Region	(US) East US
Username	Choose an username
Password	Choose your password
Confirm Password	Confirm the password

- Click on “Next : Disks >”
- Click on “Next : Networking >” and for the “Subnet” field choose mgmt (10.0.1.0/24)
- Click on “Review + create”

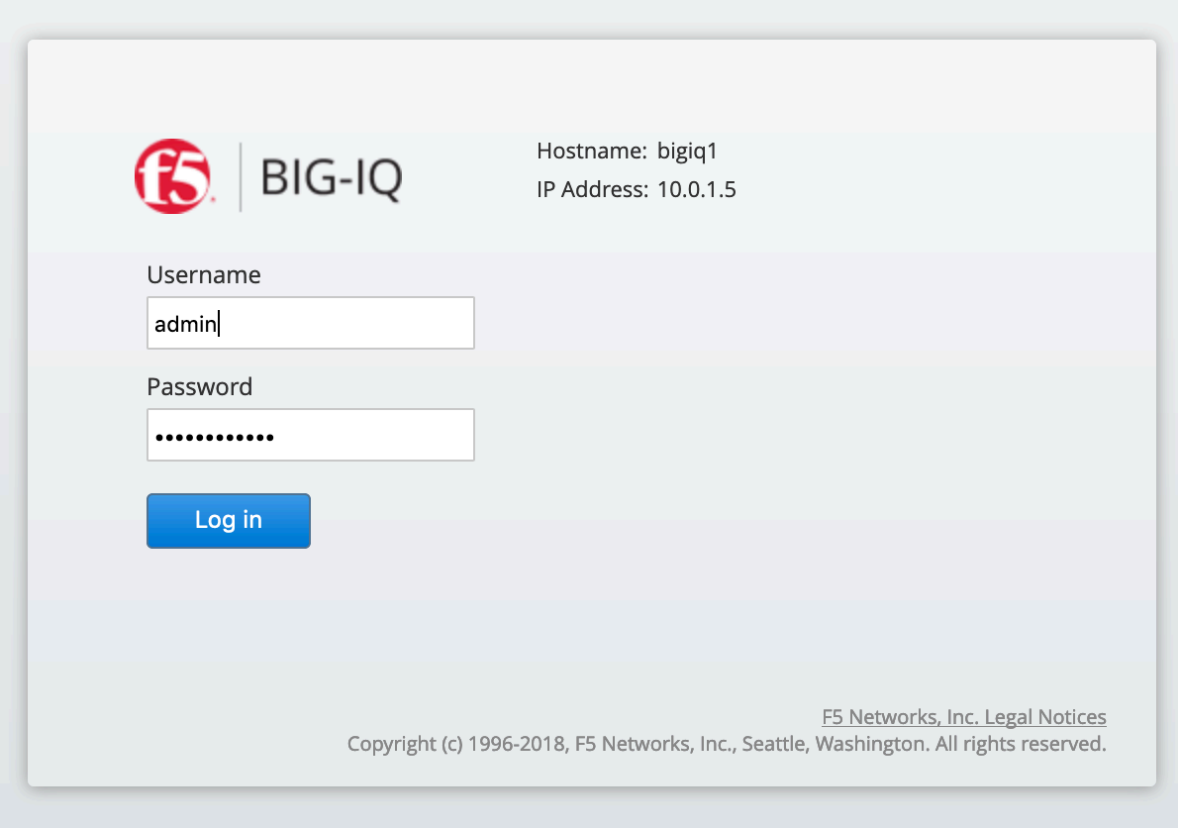


- Click on >Network security group> Inbound security rules> Add

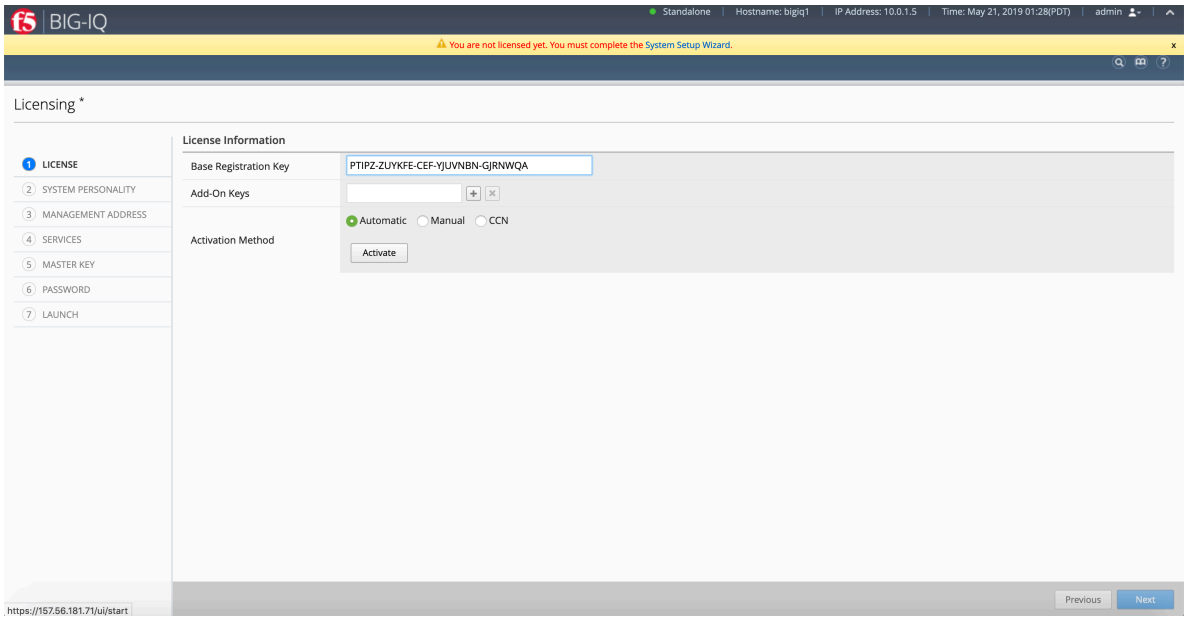
- Use the Following information and then click “Add”:

Source	IP Addresses
Source IP Addresses/CIDR Ranges	Set your public IP address
Destination Port Ranges	443
Name	Port_443

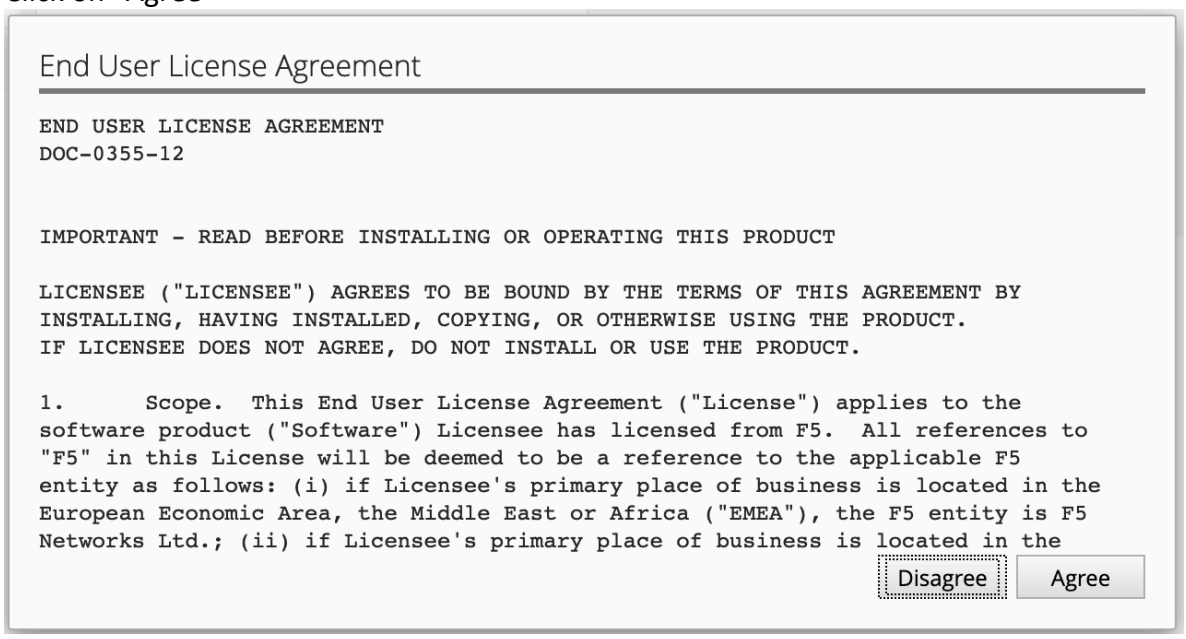
- Use a web browser to access and log in to BIG-IQ by the VM Public IP and login



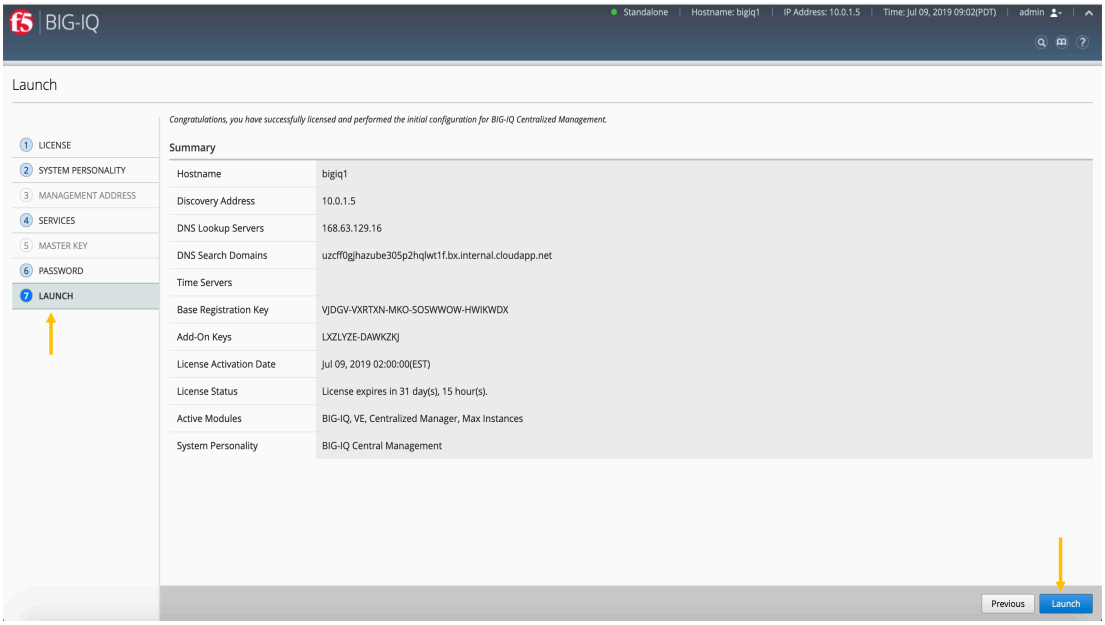
- License the BIG-IQ whit this license: F5-BIQ-VE-MAX-LIC
- Click on “Activate”



- Click on “Agree”



- For “System Personality” choose **BIG-IQ Central Management**
- For “Management Address”
- For “Services” let the defaults
- For “Master Key” set a phassphrase
- Skip Password section and click on “Launch” section

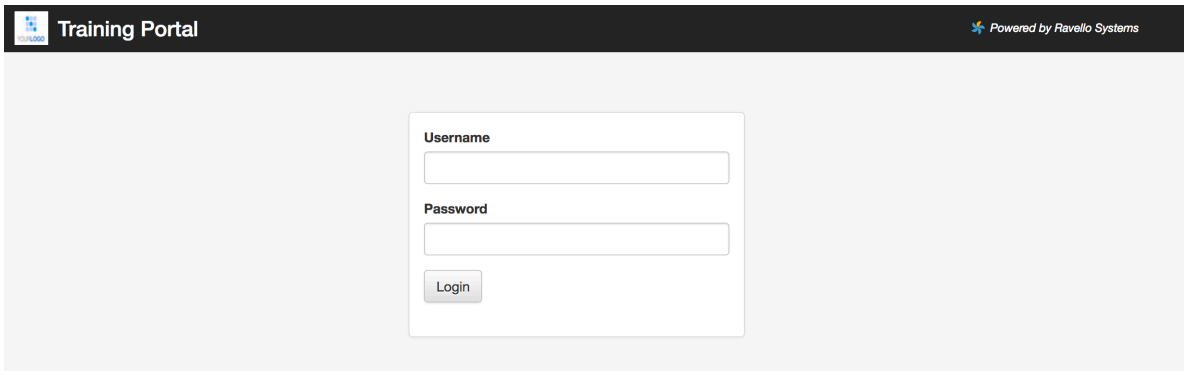


- Restart the services

Task 7 - Ravello Environment

You will need to access Ravello Training Portal in order to access the required virtual systems.

- Use a browser to access and login in to the Training portal:

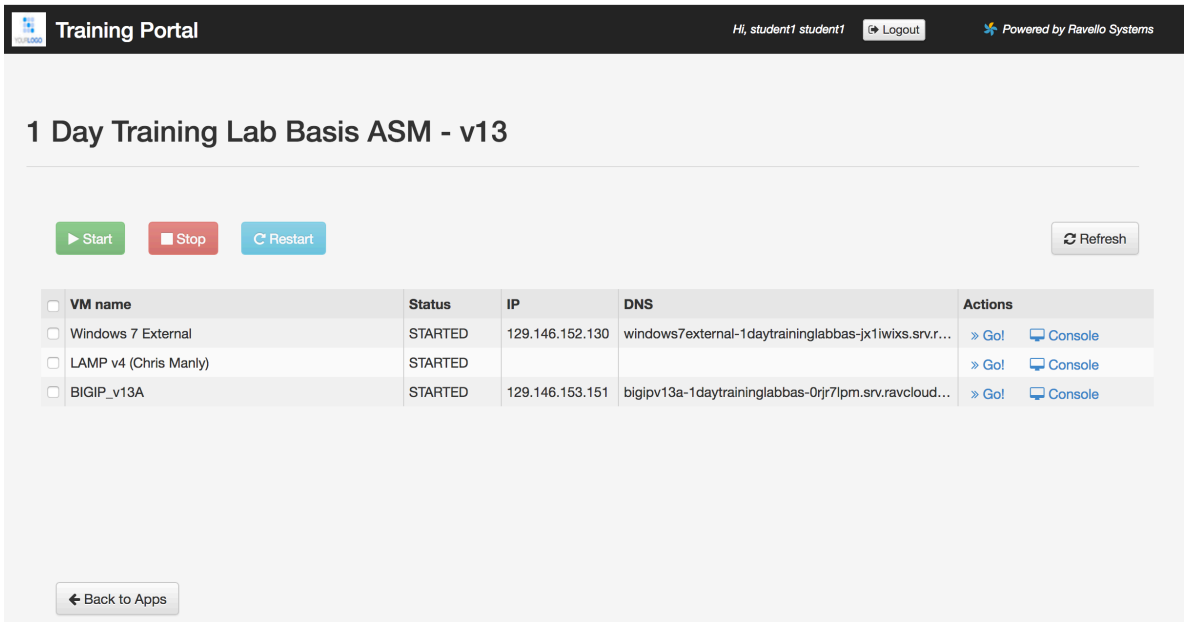


- Use the username and password assigned.

Username: student*XX*
Password: student*XX*

Now you can see the available environment for the training:

- Now you can click **View**.

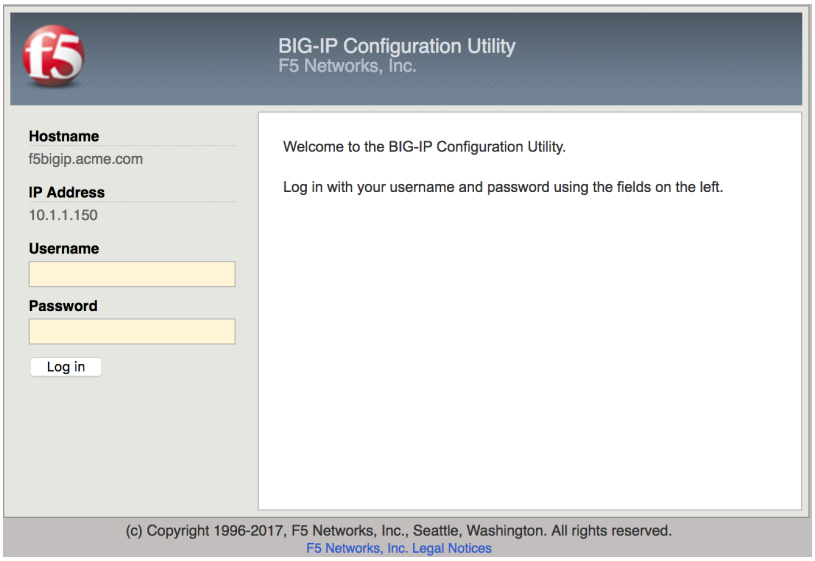


Credentials:

System	Username	Password
Win7 Jumpbox	external_user	P@ssw0rd!
BIGIP_v13A	admin	admin

- Login

On the **Windows_7_External** desktop, use a web browser to access and log in to https://10.1.1.245



- Use the following information, and then click Log In.

Username	admin
Password	admin

- Create a HTTP Monitor
  - Open the **Local Traffic > Monitors** page, and then click **Create**
  - Use the following information for the new monitor, and then click **Finished**.

Name	dvwa_op_monitor
Type	HTTP
Send String	GET \login.php\r\n

- Create a new Pool of Servers
  - Open the Pools > Pool List page, and then click Create
  - Use the following information for the new Pool of Servers, and then click Finished.

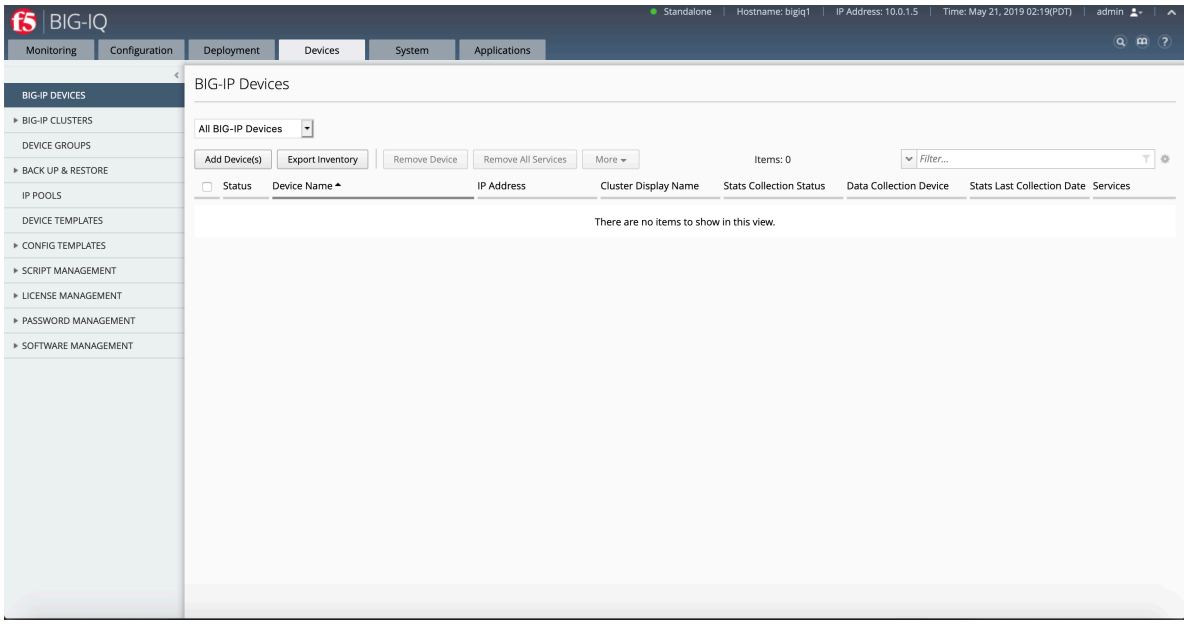
Name	dvwa_op_pool
Health Monitors	dvwa_op _monitor
New Members	Address: 10.1.20.17 Service Port: 80 *Click on **Add**

- Create a Virtual Server
  - Open the Local Traffic > Virtual Servers > Virtual Server List page, and then click Create
  - Use the following information for the new Virtual Server, and then click Finished.

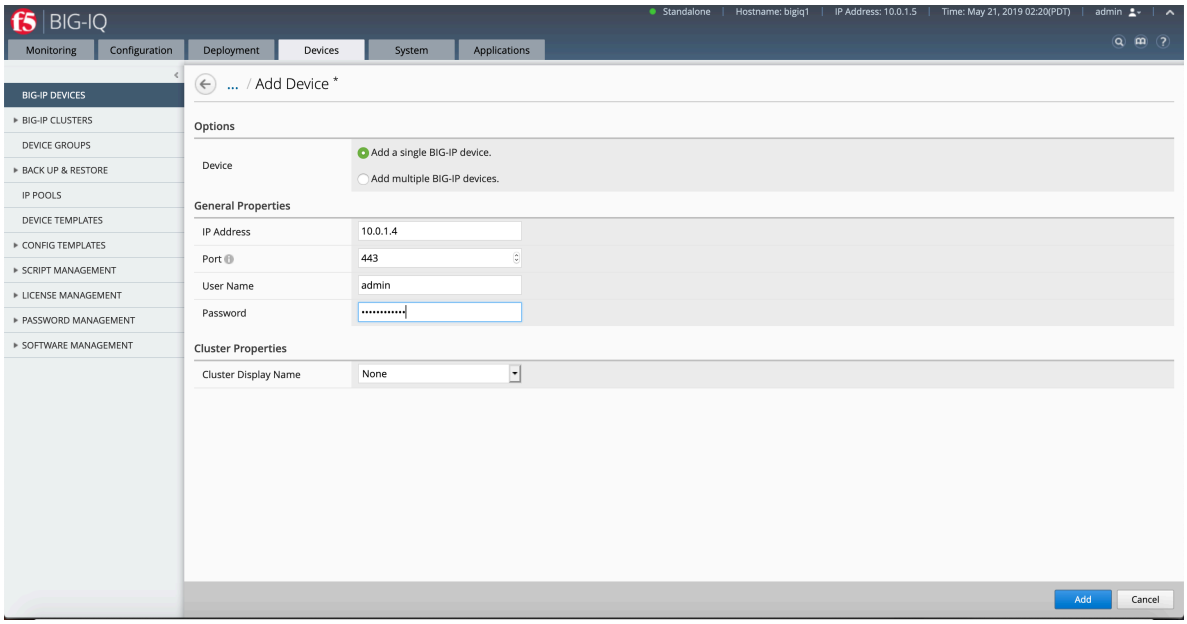
Name	dvwa_op _vs
Destination Address /Mask	10.1.10.35
Service Port	80
HTTP Profile	http
Source Address Translation	Automap
Default Pool	dvwa_op_pool

Task 8 – Deploy a Consistent Security Policy

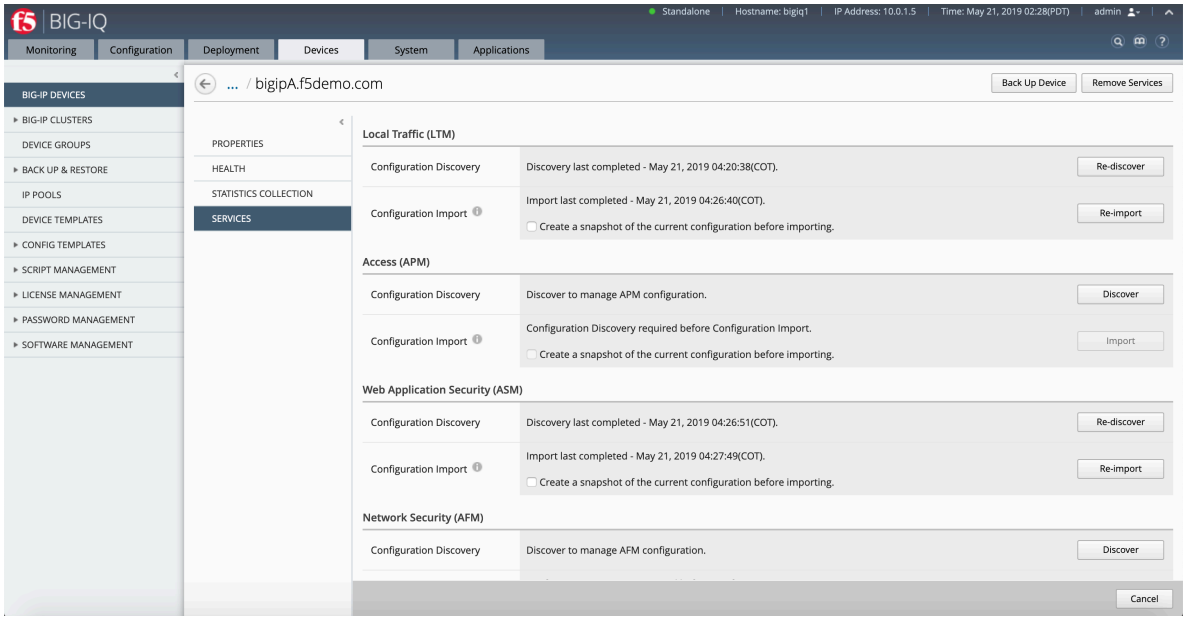
- Click on “Add Devices”



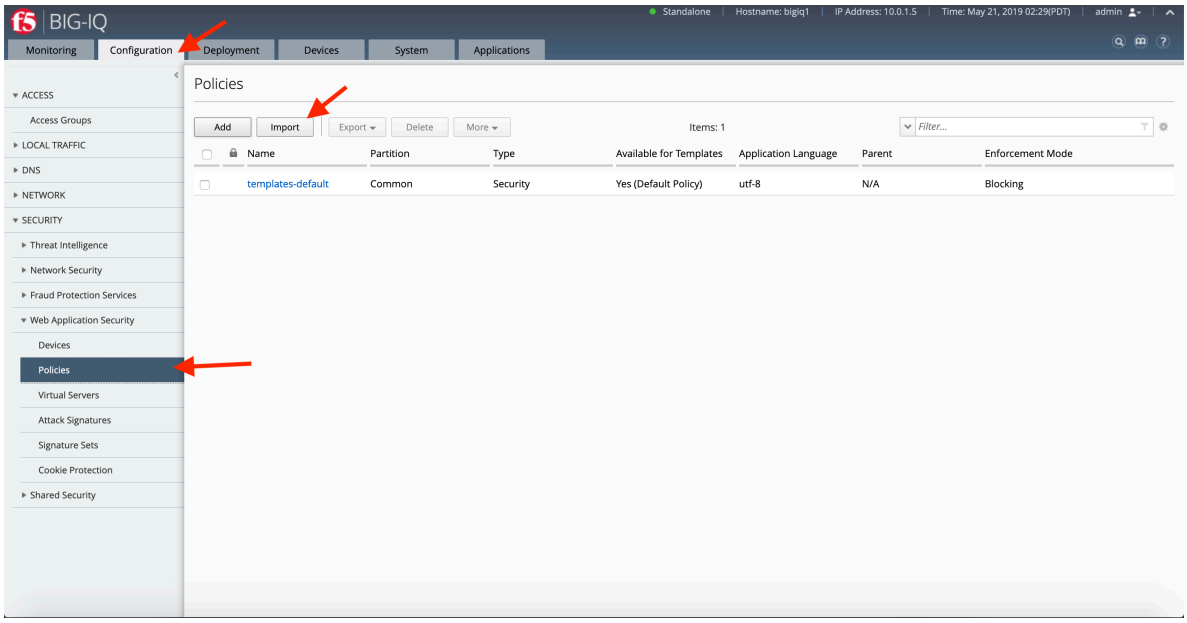
- Fill the General Properties for each deployed BIG-IP
  - The IP address for the Azure environment is the private VM IP
  - The IP address for the Ravello environment is the public IP NIC



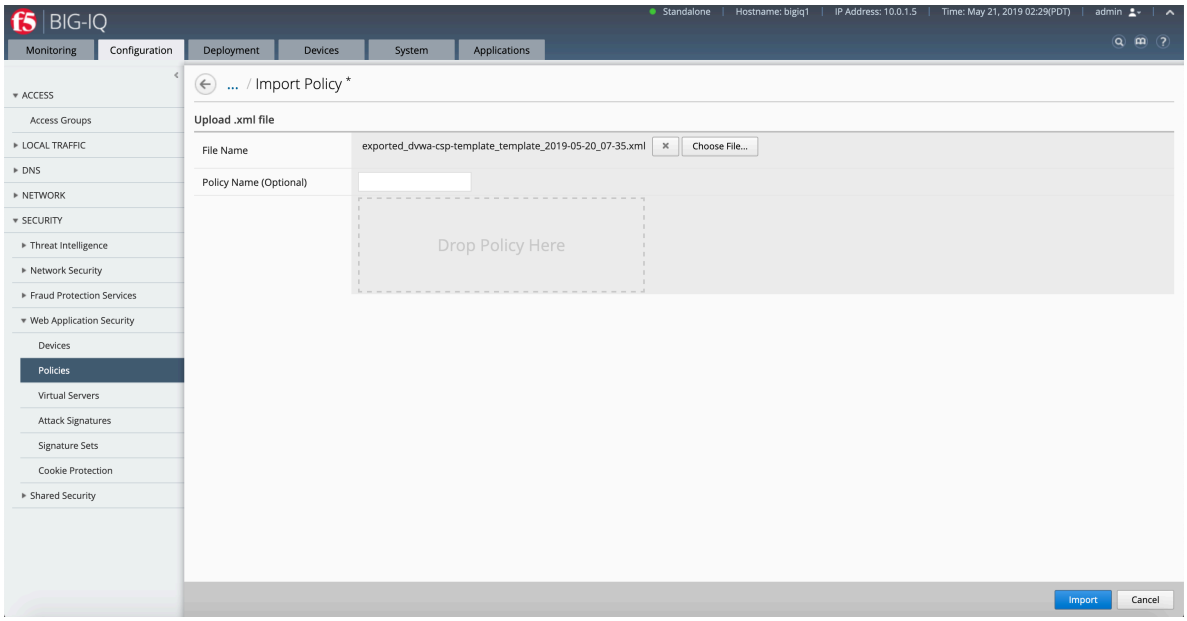
- Click on each BIG-IP and in the “Services” tab find the LTM and WAF Discovery services and click con “Discover” and then click on “Import”



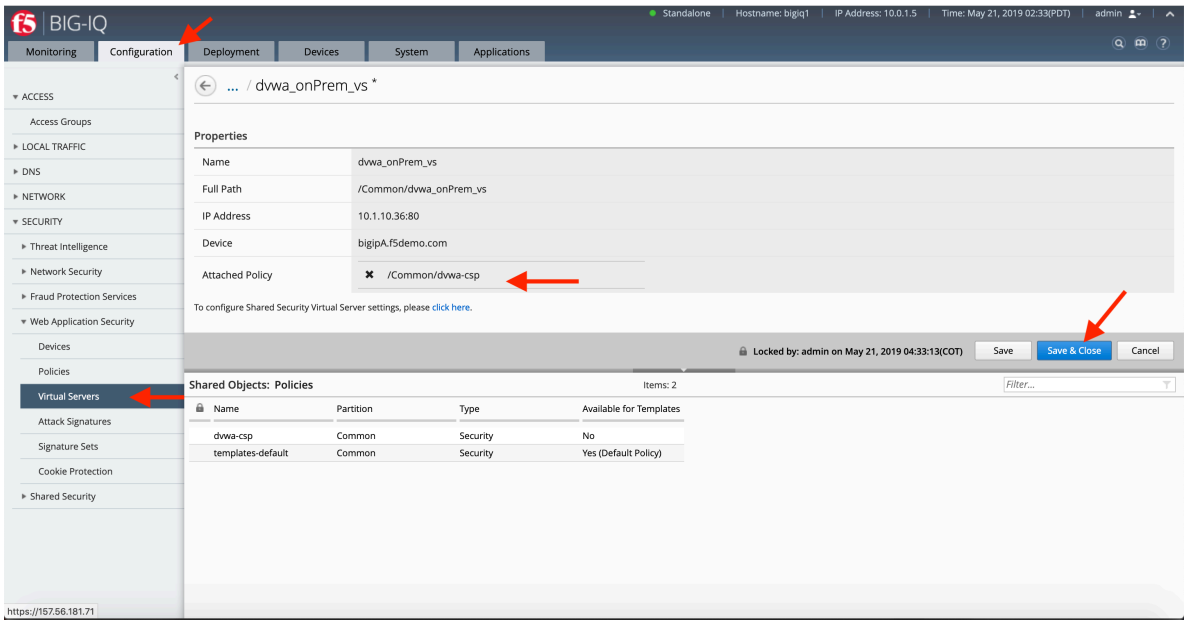
- Navigate on Configuration>Policies>Import



- Import the Consistent Policy for the DVWA application

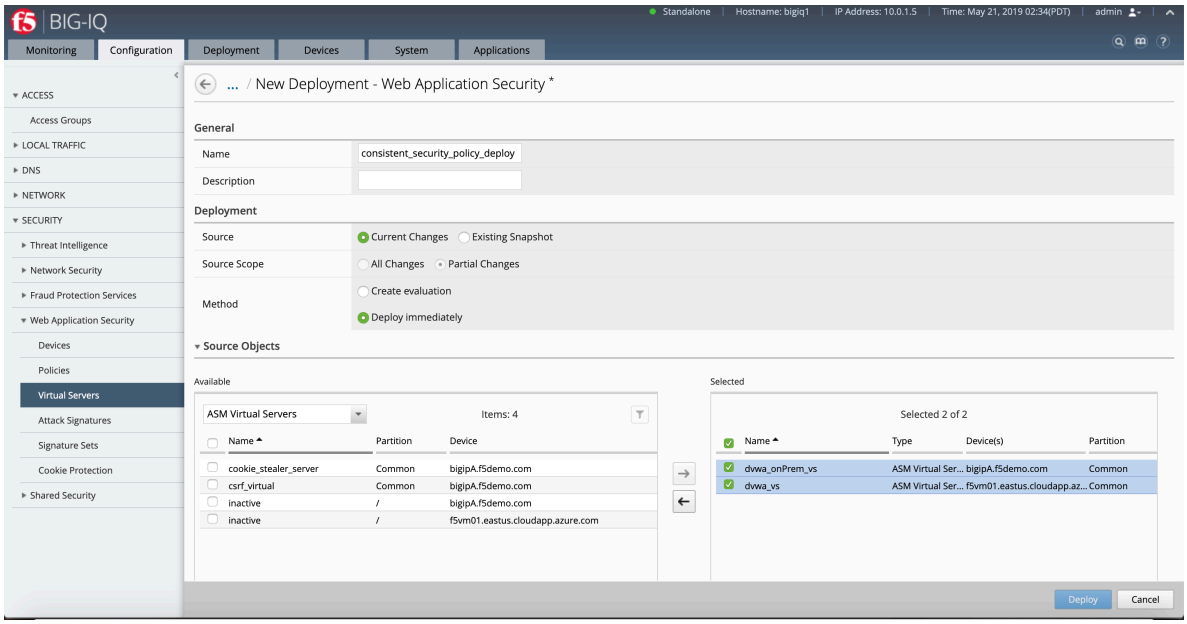


- Navigate on Configuration>Virtual Servers
- In the Virtual Server, for “Attached Policy” choose the dvwa-csp policy
- Click “Save & Close”

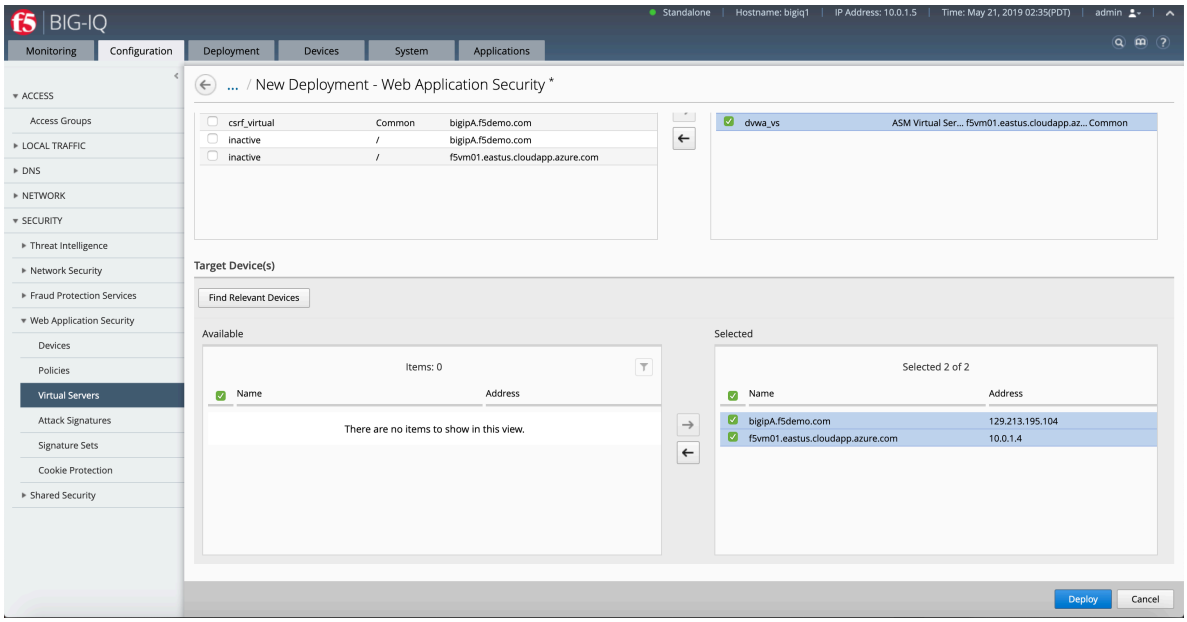


- Deploy the configuration

  - Click on “Deploy”
  - Give a name for the new deployment
  - Select the two vitual servers



- Click on “Find Relevant Devices”
- Select the two devices and click on “Deploy”

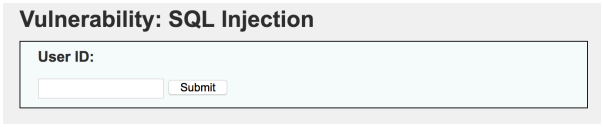


Task 9 – Check the Consistent Security Policy

- Check the configuration for the new deployment in each BIG-IP
- Do a SQL Injection Attack

- **SQL Injection:** Click **SQL Injection**, then in the **User ID** field copy and paste the following, and then click **Submit**:

```
%' or 1='1
```



You are presented with all the users in the database.

- In the **User ID** field copy and paste the following, and then click **Submit**:

```
%' or 1=1 union select null, concat ( 0x0a, user_id, 0x0a,
first_name, 0x0a, last_name, 0x0a, user, 0x0a, password) from
users #
```