

# F5 Cloud Training Bootcamp

## Consistent Security Policy in Multi-cloud Environment Lab

TMOS Version: 14 - 13

Lab environments: Azure - Ravello

Windows 7 External

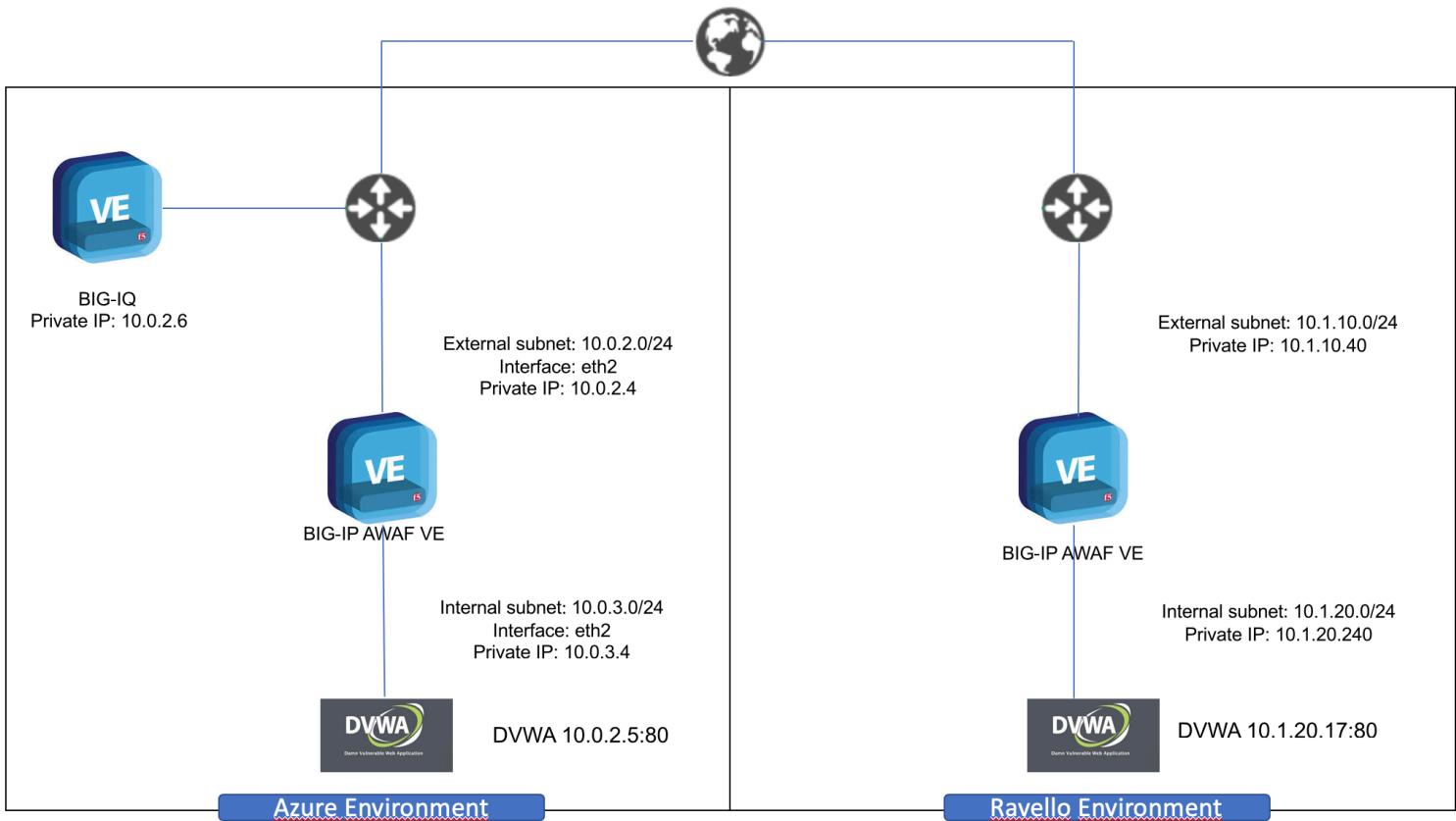
LAMP 4

BIG-IQ

## Tabla de contenido

<b>Training Lab Architecture .....</b>	<b>3</b>
Task 1 – Azure Login .....	4
Task 2 – Github Login.....	4
Task 3 – Deploy the BIG-IP VE in Azure - 3 NIC .....	15
Task 4 – Deploy a DVWA .....	19
Task 5 – Configure the DVWA app on the BIG-IP .....	23
Task 6 – Configure an Azure Load Balancer and a NAT .....	Error! Marcador no definido.
Task 7 – Deploy a BIG-IQ BYOL .....	24
Task 8 - Ravello Environment .....	28
Task 9 – Deploy a Consistent Security Policy .....	31

# Training Lab Architecture

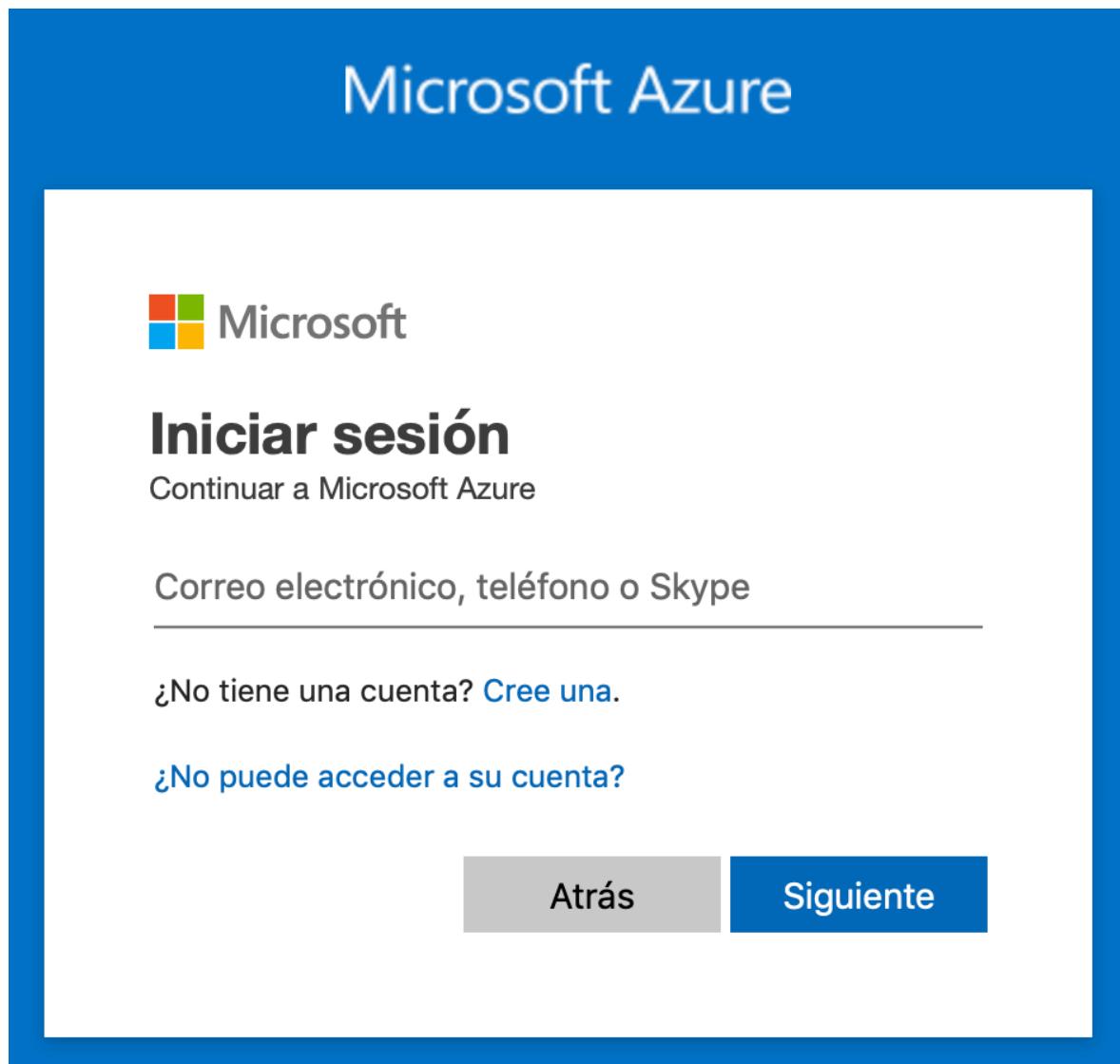


# **Part 1- F5 Azure ARM Template**

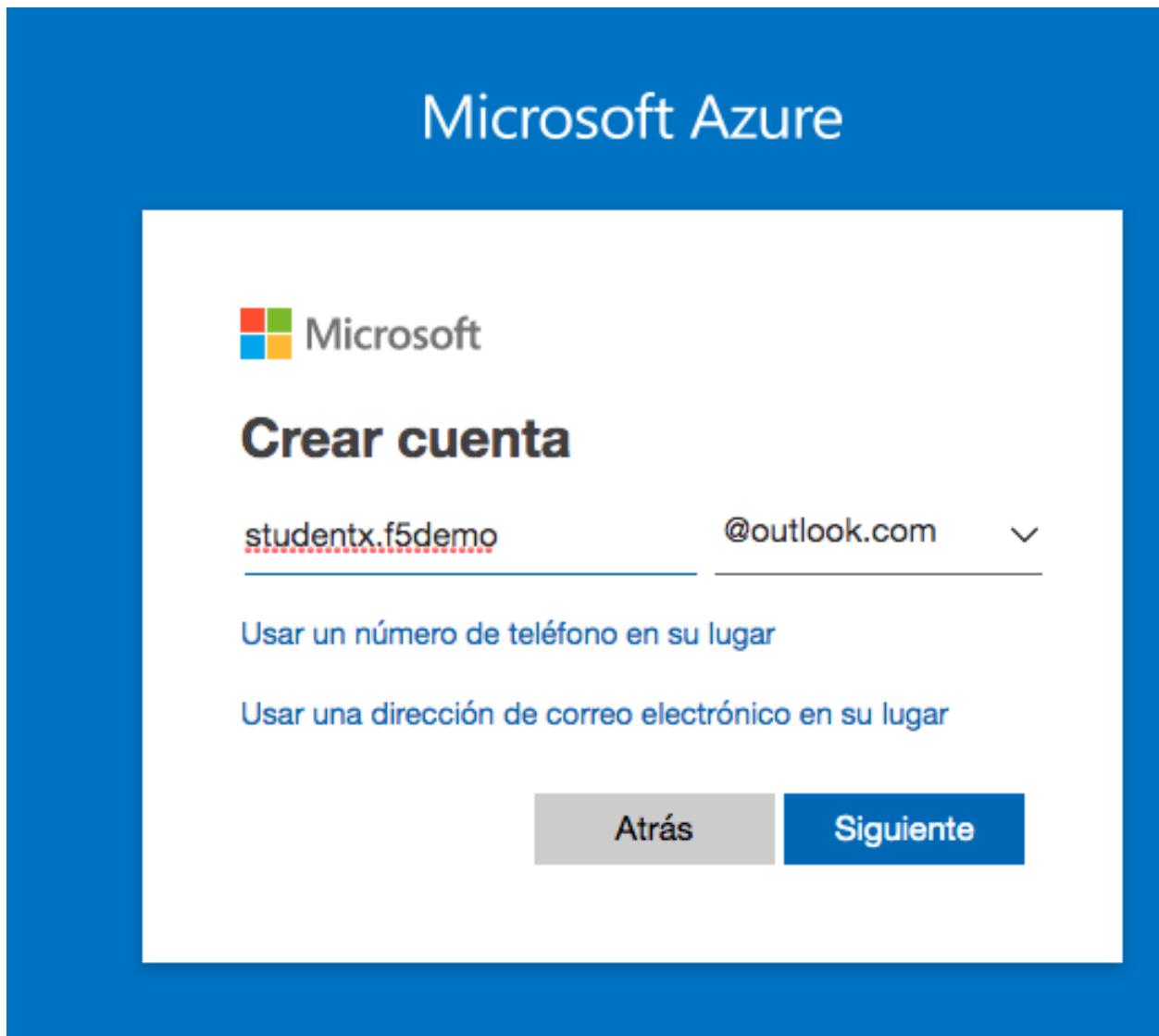
## **Deploying the BIG-IP VE in Azure - 3 NIC**

### **Task 1 – Azure Login**

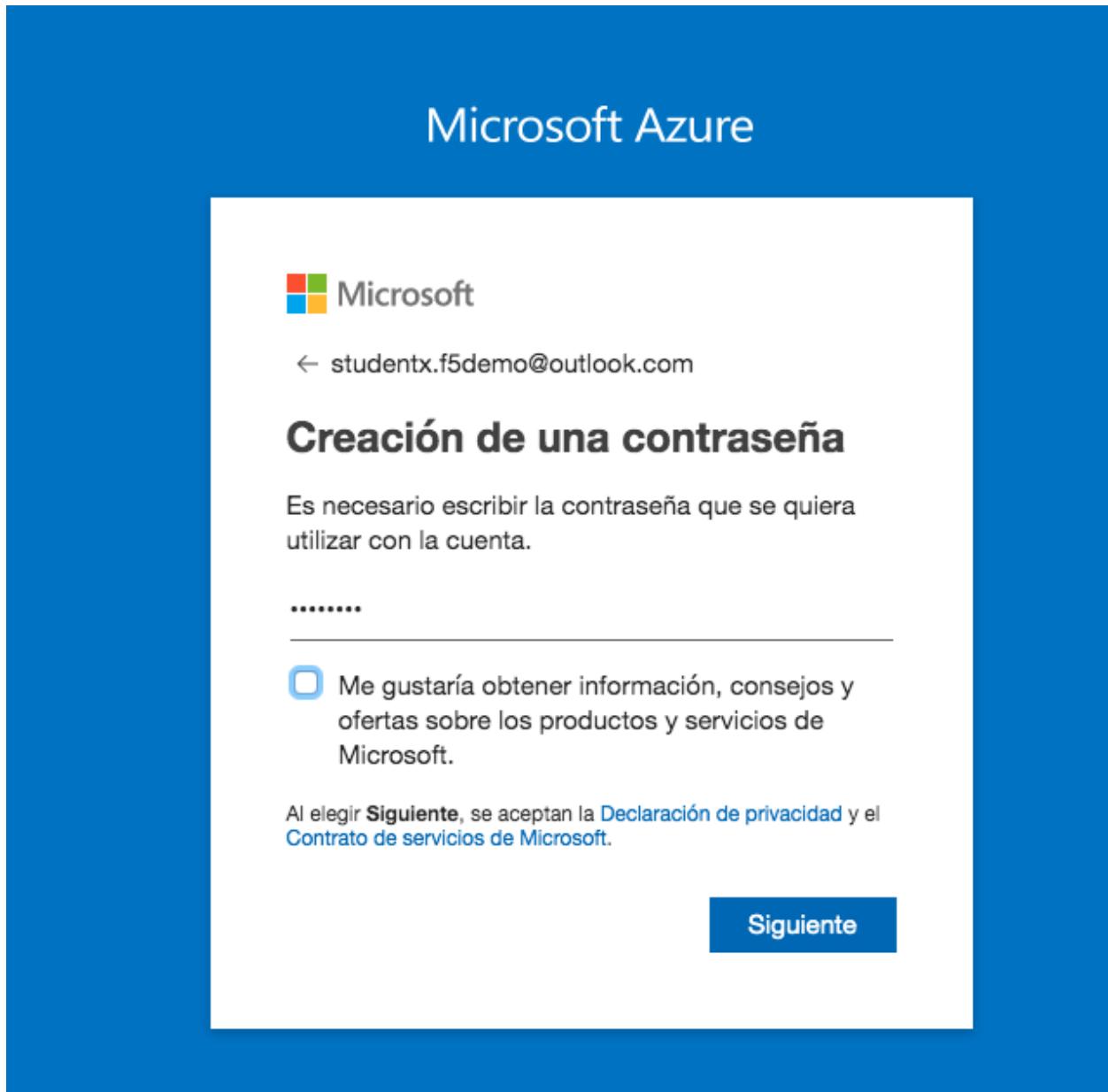
You will need to access Microsoft Azure Portal in order to deploy the required virtual systems.



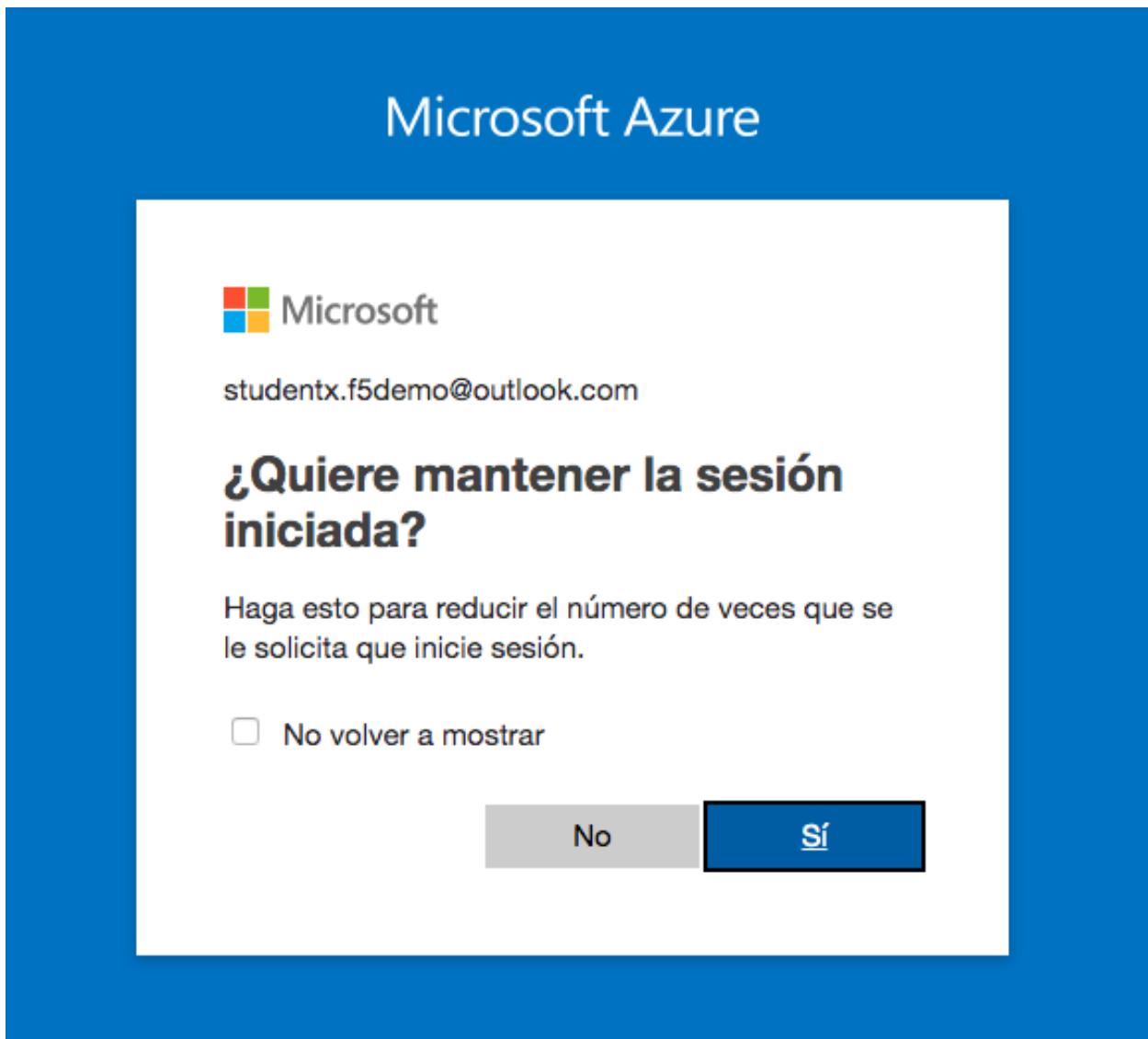
We will use studentx.f5demo with the domain outlook.com, replace the “x” with your student number:



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:

The screenshot shows the Azure portal interface. At the top, there's a blue header bar with icons for back, forward, search, notifications (4), help, and user profile. To the right of the user profile is a gear icon, which is highlighted with a red arrow. Below the header, a modal window titled "Portal settings" is open. It contains a message about switching directories or filtering subscriptions, a link to "Click here", and a dropdown menu for "Log me out when inactive" set to "Never".

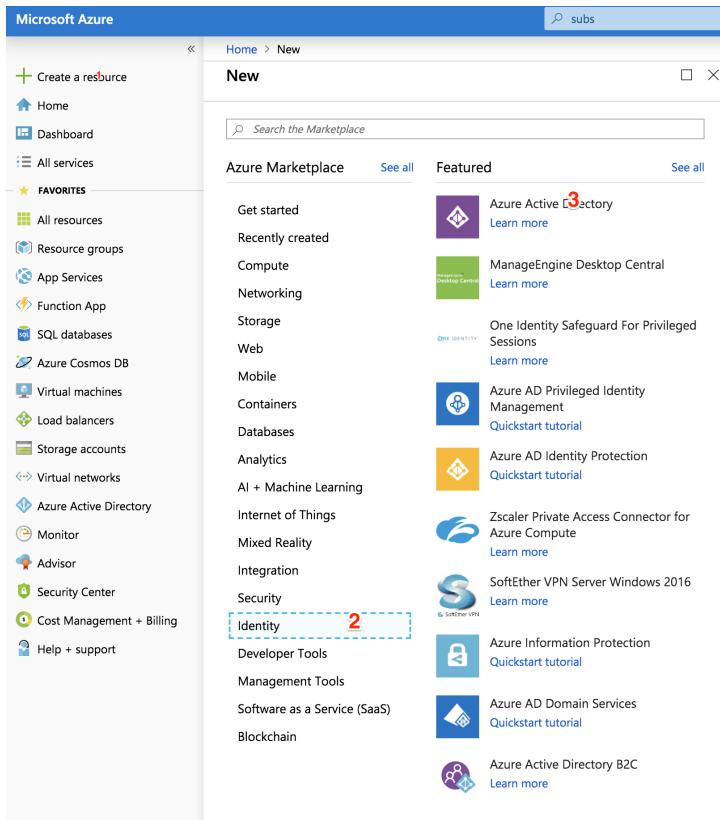
Below the "Portal settings" modal, another modal window titled "Configuración del portal" is open. This window has a title bar with an "X". Inside, there are several configuration sections:

- "¿Quiere cambiar los directorios o filtrar suscripciones? Haga clic aquí": A link to change directory or filter subscriptions.
- "Cerrar sesión cuando esté inactivo": A dropdown menu set to "Nunca" (Never).
- "Elija la vista predeterminada": Buttons for "Inicio" (selected) and "Panel".
- "Elegir un tema": A row of four circular theme options, the first one is checked.
- "Tema de contraste alto": Buttons for "Ninguno" (selected), "Blanco", and "Negro".
- "Notificaciones del sistema": Buttons for "Habilitar" (selected) and "Deshabilitar".
- "Permitir que se cambie el tema al hacer doble clic en el panel": Buttons for "Habilitar" (selected) and "Deshabilitar".
- "Nueva experiencia de navegación "Todos los recursos)": Buttons for "Habilitar" (selected) and "Deshabilitar".
- "Idioma (es necesario actualizar)": A dropdown menu set to "English", which is highlighted with a red arrow.
- "Formato regional (es necesario actualizar)": A dropdown menu set to "English (United States)".
- "¿Pertenece a Microsoft Partner Network (MPN)?": A link to "Vincular el id. de asociado a esta cuenta de Azure".
- "Restaurar la configuración predeterminada": A link.
- "Exportar todas las opciones de configuración": A link.
- "Eliminar todas las opciones de configuración y los paneles privados": A link.

At the bottom of the configuration window, there are two buttons: "Actualizar" (highlighted with a red arrow) and "Cancelar".

## Create a directory:

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



The screenshot shows the Microsoft Azure 'New' blade in the Marketplace. On the left, there's a sidebar with 'Create a resource' and a list of services under 'FAVORITES'. The main area has tabs for 'Azure Marketplace', 'See all', 'Featured', and 'See all'. A search bar at the top says 'Search the Marketplace'. Below it, there are several cards for different services, each with an icon, name, and a 'Learn more' link. One card for 'Identity' is highlighted with a red dashed box and the number '2' in red. The 'Identity' card includes icons for 'One Identity Safeguard For Privileged Sessions', 'Azure AD Privileged Identity Management', 'Azure AD Identity Protection', 'Zscaler Private Access Connector for Azure Compute', 'SoftEther VPN Server Windows 2016', 'Azure Information Protection', 'Azure AD Domain Services', and 'Azure Active Directory B2C'.

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:

Home > f8cdef31-a31e-4b4a-93e4-5f571e91255a - Overview > Create directory

### Create directory

\* Organization name ⓘ  
Fselatam ✓

\* Initial domain name ⓘ  
asfselatam ✓  
asfselatam.onmicrosoft.com

Country or region ⓘ  
United States

 Directory creation will take about one minute.

**Create**

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

Home > Fselatam - Overview

### Fselatam - Overview

Azure Active Directory

Search (Ctrl+ /) <  Switch directory  Delete directory

 Overview  Getting started

**Manage**

 Users  Groups

asfselatam.onmicrosoft.com  
**Fselatam**  
Azure AD Free

Sign-ins

## 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:

The screenshot shows the Microsoft Azure portal interface. On the left, there's a sidebar with various service icons like Home, Dashboard, All services, Favorites, and more. The main area is titled 'Subscriptions' and shows a list of existing subscriptions. A search bar at the top contains the text 'subs'. A red box highlights the 'Subscriptions' link in the search results, which is also labeled with a red '2'. Another red box highlights the 'Add' button next to the search bar, labeled with a red '3'.

choose the free evaluation option:

This screenshot shows the 'Agregar suscripción' (Add subscription) page. At the top, it says 'Agregar suscripción'. On the left, there's a large blue button with white text that says 'Agregar suscripción' and 'Microsoft Azure'. The main content area is titled 'SELECCIONAR UNA OFERTA' (Select an offer). It features a section for 'Evaluación gratuita' (Free evaluation) with a brief description: 'Acceso completo a todos los servicios. Explorar el servicio que deseé.' (Full access to all services. Explore the service you want.) and a 'Más información' (More information) link. A red arrow points from the text 'Explorar el servicio que deseé.' towards the 'Más información' link.

Fill up with all the data needed on the form:

The screenshot shows the Microsoft Azure free account registration process. At the top, it says "Microsoft Azure" and "studentx.f5demo@outlook.com Cerrar sesión". The main title is "Registro de cuenta gratuita de Azure" with the subtitle "Empiece con un crédito de \$200 durante 30 días y continúe de forma gratuita." Below this, there's a section titled "1 Acerca de usted" containing fields for "País o región" (Colombia), "Nombre" (1), "Apellido" (2), "Dirección de correo electrónico" (3), "Teléfono" (4), and "CIF de la empresa" (Optional). To the right, under "Incluido", are several benefits: "12 meses de productos gratuitos" (with a description about virtual machines and storage), "\$200 de crédito" (with a description about trying Azure services), "Más de 25 productos gratuitos para siempre" (with a description about serverless, storage, and AI products), and "Sin cargos automáticos" (with a description about no automatic charges unless updated). A blue "Siguiente" button is at the bottom of the form.

Confirm it with your phone number:

This screenshot shows the verification step. It includes a summary of previous information and a new section for verification. The "1 Acerca de usted" section is collapsed. The "2 Verificación de identidad mediante teléfono" section is expanded, showing a note that having a phone number allows sending text messages or calling to verify identity. It has fields for "Código de país" (Colombia (+57)), "Número de teléfono" (Ejemplo: 3 315 012345), and a note "Este campo es obligatorio.". Below these are two buttons: "Envíeme un mensaje de texto" and "Llámeme". The "Código de verificación" field is empty, with a note "Este campo es obligatorio.". At the bottom are two buttons: "Comprobar código" and "No he recibido ningún código." To the right, under "Incluido", are the same four benefit sections as the previous screenshot, along with a fifth one: "Sin cargos automáticos".

(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.**

The screenshot shows the Azure portal interface for managing a subscription. The left sidebar lists various management categories like Overview, Access control (IAM), and Cost Management. The main content area displays subscription details for 'Evaluación gratuita'. At the top, there are several action buttons: Upgrade subscription, Manage, Transfer, Cancel subscription (which is highlighted with a red arrow), Rename, and Change directory. A warning message states: 'Your free credit expires in 21 days. Upgrade to a pay-as-you-go subscription to keep going with your account.' Below this, detailed subscription information is shown, including Subscription ID, Directory, My role, Offer, and Offer ID. To the right, there are sections for Costs (Costs by resource and Spending rate and forecast) and a note about trying Azure Cost Management. The top right corner shows the user's email (studentx.fsdemo@ou...) and the directory (FSELATAM).

## Task 2 – Github Login

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



### Sign in to GitHub

Username or email address

Password [Forgot password?](#)

[Sign in](#)

New to GitHub? [Create an account.](#)

[Terms](#) [Privacy](#) [Security](#) [Contact GitHub](#)

## 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.

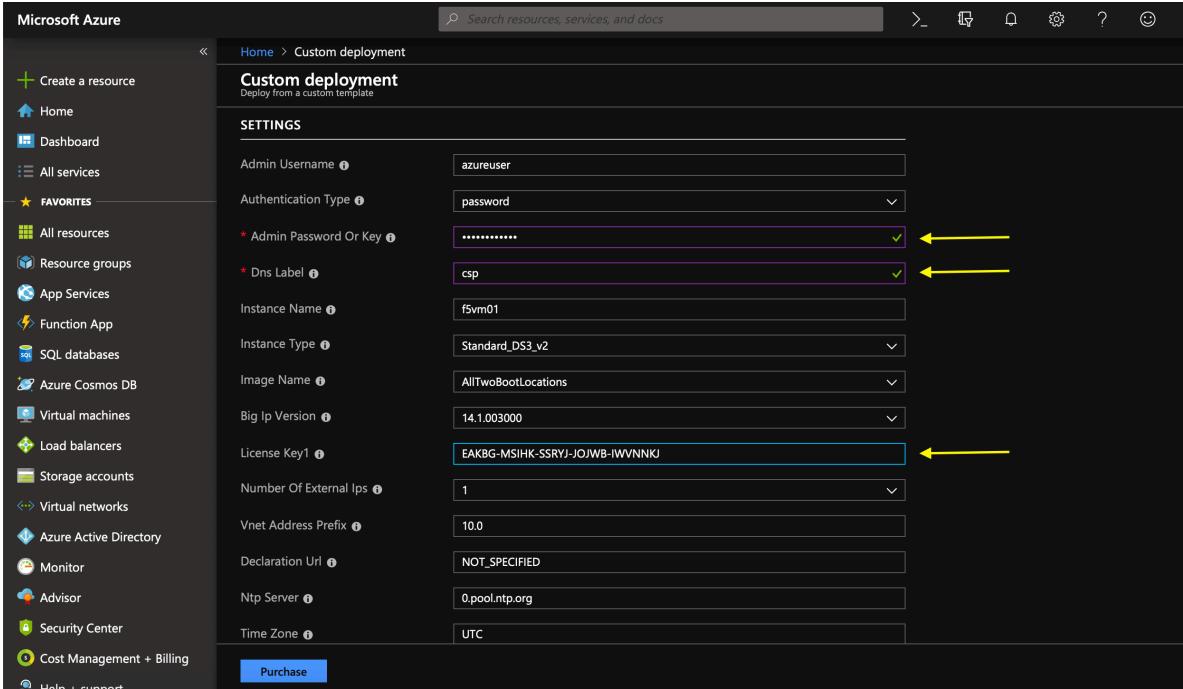
- Click on “Create new”

The screenshot shows the 'Custom deployment' page in the Microsoft Azure portal. In the 'BASICS' section, the 'Subscription' is set to 'f5-AZR\_4261\_SALES\_SA\_ALL'. The 'Resource group' dropdown is open, displaying 'Select a resource group' and 'Create new'. The 'Location' is set to '(US) East US'. In the 'SETTINGS' section, the 'Admin Username' is 'azureuser', 'Authentication Type' is 'password', 'Admin Password Or Key' is empty, 'Dns Label' is empty, and 'Instance Name' is 'f5vm01'. A blue 'Purchase' button is at the bottom.

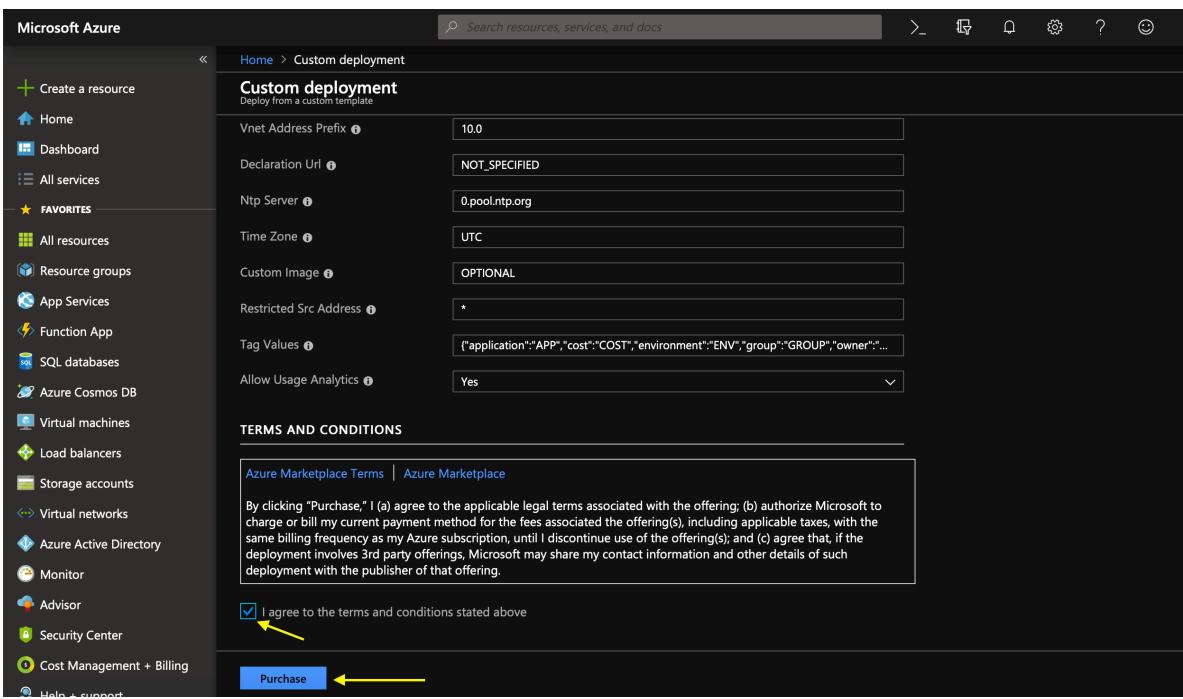
- Give a name to the resource group and click in “OK” and make sure the Location is set on “(US) East US”.

The screenshot shows the 'Custom deployment' page in the Microsoft Azure portal. A modal dialog is displayed over the 'Resource group' dropdown. The dialog text reads: 'A resource group is a container that holds related resources for an Azure solution.' It has a 'Name' input field containing 'consistent-security-policy-RG'. Below the input field are 'OK' and 'Cancel' buttons. The 'OK' button is highlighted with a yellow arrow. The 'Resource group' dropdown above the dialog shows 'Select a resource group' and 'Create new'.

- 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

The screenshot shows the Azure portal interface for the 'consistent-security-policy-RG' resource group. On the left, the navigation menu includes 'Create a resource', 'Home', 'Dashboard', 'All services', 'FAVORITES' (with 'Resource groups' selected), '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', and 'Help + support'. The main content area displays the 'Overview' tab for the resource group, showing a subscription ID and deployment status. Below this is a table listing 13 items, including network interfaces, security groups, and public IP addresses, all located in the 'East US' region. A yellow arrow points to the 'csp-ext-nsg' row. The URL bar indicates the current path is 'Home > Resource groups > consistent-security-policy-RG > csp-ext-nsg - Inbound security rules'. The right-hand pane shows the 'Inbound security rules' section for the 'csp-ext-nsg' network security group. It lists three rules: 'AllowVnetInBound' (Priority 65000, Allow), 'AllowAzureLoadBalancerInBo...' (Priority 65001, Allow), and 'DenyAllInBound' (Priority 65500, Deny). The 'Add' button and 'Default rules' link are visible at the top of the rule list. A yellow arrow also points to the 'Inbound security rules' link in the left sidebar.

- 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.

The screenshot shows the Azure portal interface for a virtual machine named f5vm01. The left sidebar contains a navigation menu with various service icons and links. The main content area is titled 'f5vm01' and 'Virtual machine'. It features a top bar with actions: Connect, Start, Restart, Stop, Capture, Delete, Refresh, and a search bar. Below this is the 'Overview' section with detailed resource group information and a table of properties. A 'Tags' section lists application, cost, environment, group, and owner tags. At the bottom, there are two charts: 'CPU (average)' and 'Network (total)'. The CPU chart shows usage over a one-hour period, and the Network chart shows traffic over the same period.

- 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.

Home > Resource groups > consistent-security-policy-RG > Get Started

## Get Started

dwva

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”

The screenshot shows the Azure portal interface. On the left, a sidebar lists various services: 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, and Help + support. The 'Create a resource' option is highlighted. The main content area shows the 'Resource groups' blade for 'consistent-security-policy-RG'. The top navigation bar includes 'Home > Resource groups > consistent-security-policy-RG > Get Started > Damn Vulnerable Web App'. The page title is 'Damn Vulnerable Web App' with the subtitle 'edgeNEXUS'. It features a 'Create' button and a 'Save for later' button. A link 'Want to deploy programmatically? Get started →' is also present. Below this, a detailed description of DVWA is provided: 'Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.' At the bottom, there is a preview window showing the DVWA application's homepage with various exploit modules listed.

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

<b>Resource Group</b>	Select your RG
<b>Virtual Machine Name</b>	dvwa
<b>Region</b>	(US) East US
<b>Authentication type</b>	Password
<b>Username</b>	Set a user name
<b>Password</b>	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:

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

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

The screenshot shows a web browser window for the DVWA setup page at `40.117.59.207/setup.php`. The page has a navigation bar with tabs: **Setup DVWA** (highlighted), **Instructions**, and **About**.

### Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.  
If you get an error make sure you have the correct user credentials in: `/var/www/html/config/config.inc.php`  
If the database already exists, it will be cleared and the data will be reset.  
You can also use this to reset the administrator credentials ("admin // password") at any stage.

### Setup Check

Operating system: \*nix  
Backend database: MySQL  
PHP version: 5.6.30-0+deb8u1  
Web Server SERVER\_NAME: 40.117.59.207  
PHP function display\_errors: Disabled  
PHP function safe\_mode: Disabled  
PHP function allow\_url\_include: Enabled  
PHP function allow\_url\_fopen: Enabled  
PHP function magic\_quotes\_gpc: Disabled  
PHP module php-gd: Installed  
reCAPTCHA key: 6LdK7xIAzAAJQTrL7fu6I-oPi8KHieAT\_yJg  
Writable folder /var/www/html/hackable/uploads/: Yes  
Writable file /var/www/html/external/phpids/0.6/lib/IDS/tmp/phpids\_log.txt: Yes

**Status in red:** indicate there will be an issue when trying to complete some modules.

Unable to connect to the database.

Damn Vulnerable Web Application (DVWA) v1.9

## 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**.

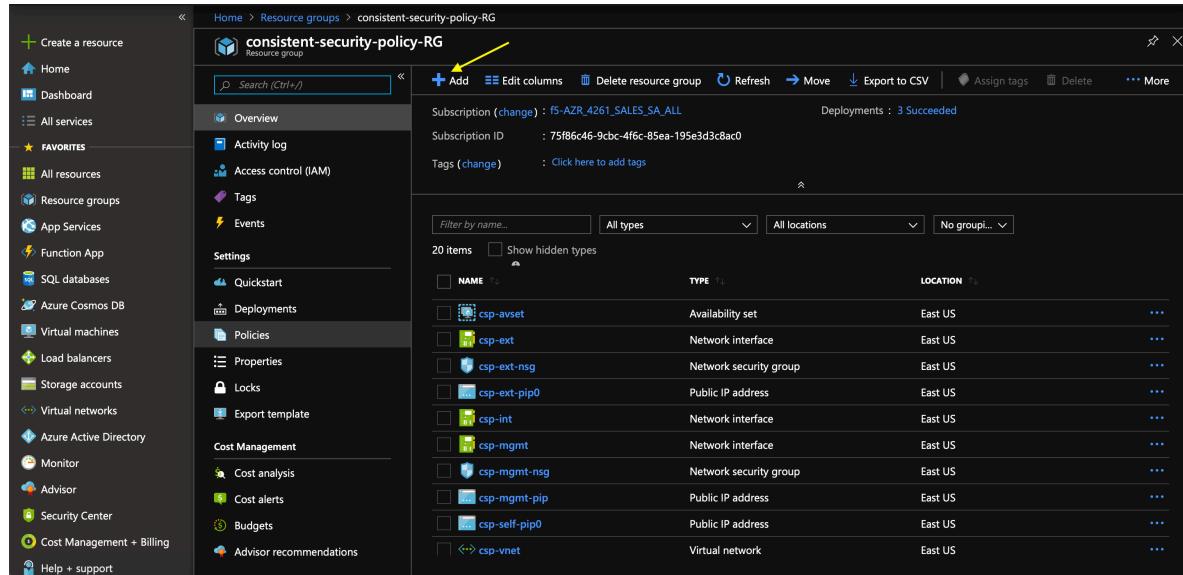
Name	dvwa_pool
Health Monitors	dvwa_monitor
New Members	Address: 10.0.2.5 Service Port: 80 *Click on <b>Add</b>

- 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

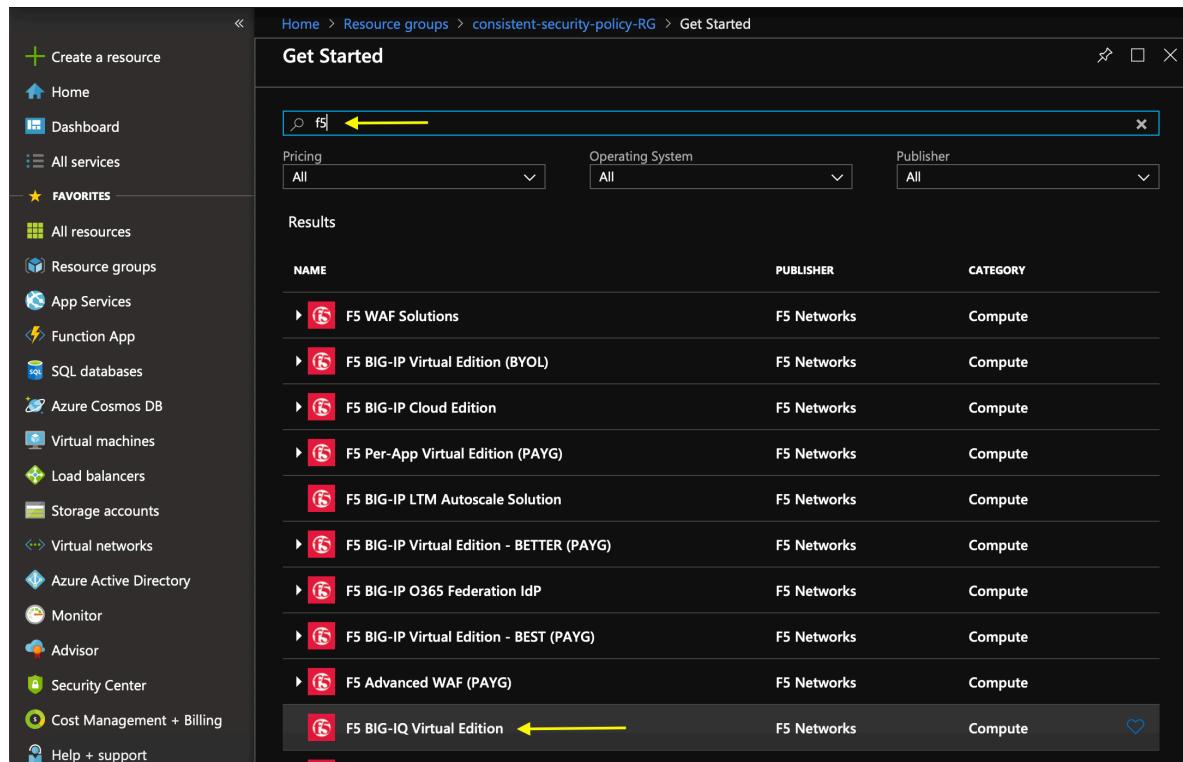
## Task 6 – Deploy a BIG-IQ BYOL

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



The screenshot shows the Azure Resource Groups blade for the 'consistent-security-policy-RG'. The left sidebar includes options like 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, and Help + support. The main area displays the 'consistent-security-policy-RG' details, including its subscription information (change: f5-AZR\_4261\_SALES\_SA\_ALL, ID: 75f86c46-9cbc-4f6c-85ea-195e3d3c8ac0), deployment status (3 Succeeded), and a list of 20 items. A yellow arrow points to the '+ Add' button at the top of the list.

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



The screenshot shows the Azure Marketplace search results for 'f5'. The search bar contains 'f5' with a yellow arrow pointing to it. The results table has columns for NAME, PUBLISHER, and CATEGORY. The results listed are: F5 WAF Solutions, F5 BIG-IP Virtual Edition (BYOL), F5 BIG-IP Cloud Edition, F5 Per-App Virtual Edition (PAYG), F5 BIG-IP LTM Autoscale Solution, F5 BIG-IP Virtual Edition - BETTER (PAYG), F5 BIG-IP O365 Federation IdP, F5 BIG-IP Virtual Edition - BEST (PAYG), F5 Advanced WAF (PAYG), and F5 BIG-IQ Virtual Edition. The 'F5 BIG-IQ Virtual Edition (BYOL)' item is highlighted with a yellow arrow pointing to it.

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

<b>Resource Group</b>	Choose your RG
<b>Virtual Machine Name</b>	bigiq
<b>Region</b>	(US) East US
<b>Username</b>	Choose an username
<b>Password</b>	Choose your password
<b>Confirm Password</b>	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”

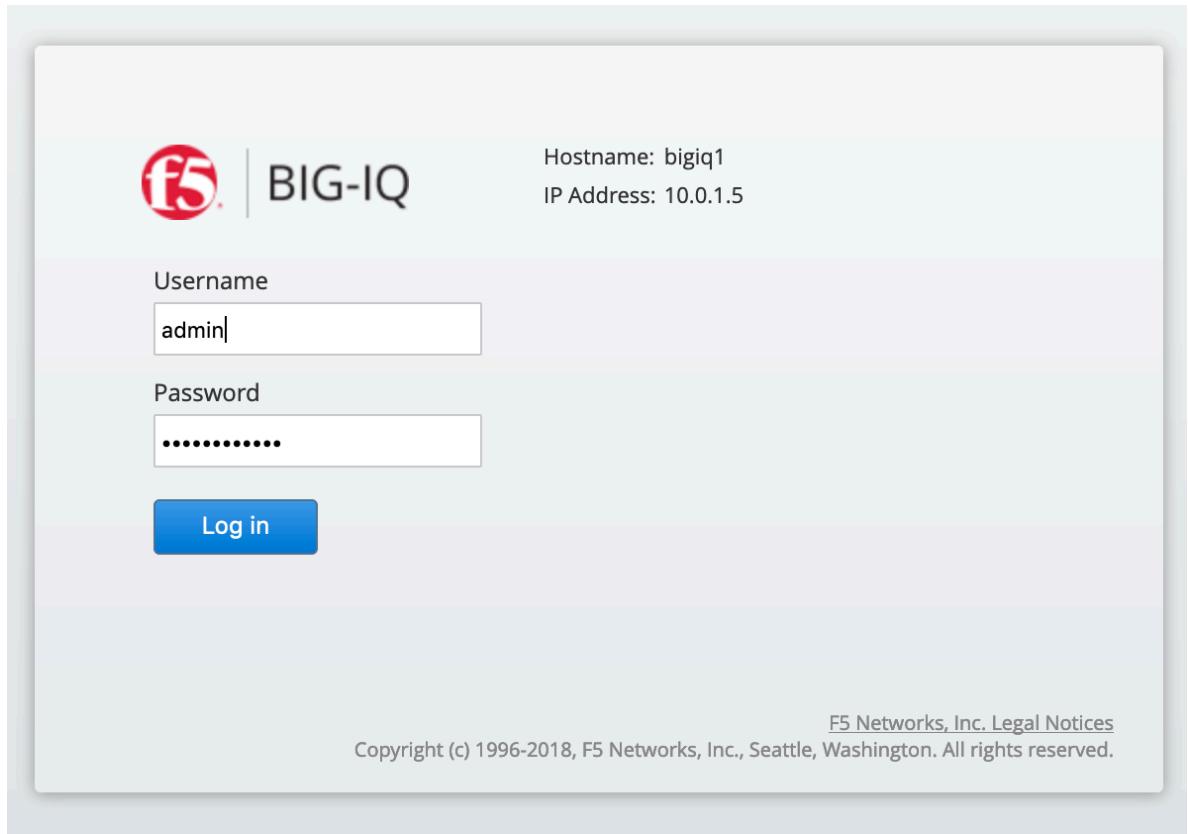
The screenshot shows the Azure portal's deployment overview for a VM named 'CreateVm-f5-networks.f5-big-iq-f5-biq-virtual-e-20190521031157'. The deployment status is 'underway'. The resources created are:

RESOURCE	TYPE	STATUS	OPERATION DETAILS
bigiq	Microsoft.Compute/vm	Created	<a href="#">Operation details</a>
bigiq218	Microsoft.Network/networkInterface	Created	<a href="#">Operation details</a>
bigiq-nsg	Microsoft.Network/networkSecurityGroups	OK	<a href="#">Operation details</a>
bigiq-ip	Microsoft.Network/publicIPAddresses	OK	<a href="#">Operation details</a>

- Click on >Network security group> Inbound security rules> Add
- Use the Following information and then click “Add”:

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

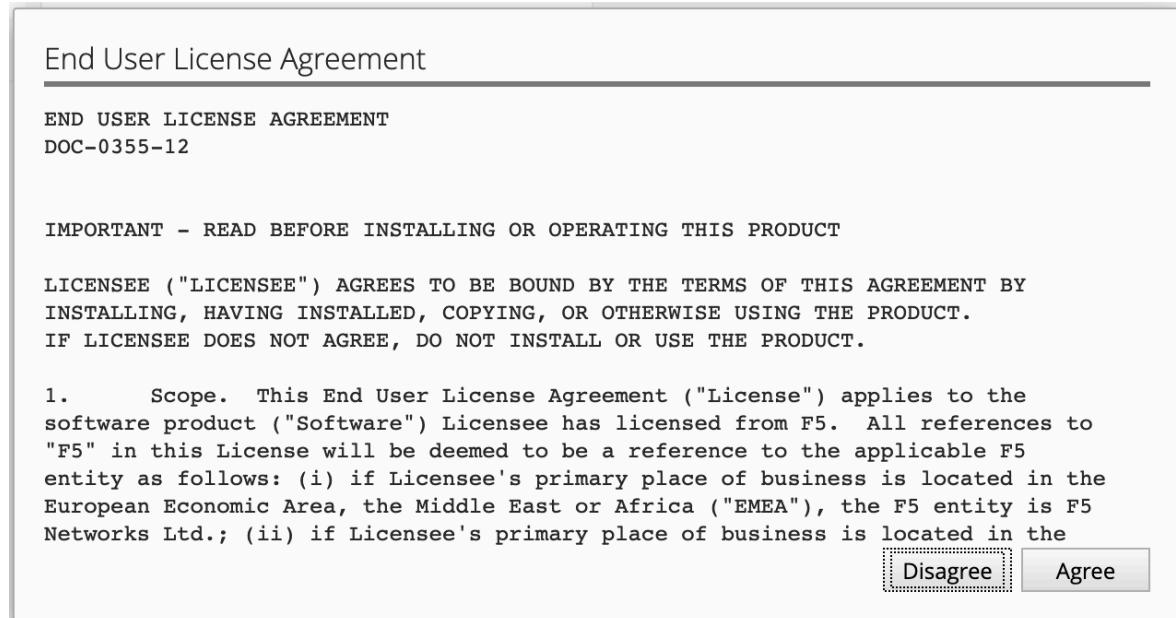
- Use a web browser to access and log in to BIG-IQ by the VM Public IP and login



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

The screenshot shows the "Licensing" screen of the BIG-IQ configuration interface. The left sidebar has a navigation menu with items 1 through 7. Item 1, "LICENSE", is selected and highlighted in blue. The main content area is titled "License Information". It contains fields for "Base Registration Key" (containing the value "PTIPZ-ZUYKFE-CEF-YJUVNBN-GJRNWQA") and "Add-On Keys" (with a plus sign and minus sign button). Below these are radio buttons for "Automatic", "Manual", and "CCN" activation methods, with "Automatic" being selected. A large "Activate" button is located at the bottom of this section. At the very bottom of the page, there are "Previous" and "Next" navigation buttons.

- 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

Congratulations, you have successfully licensed and performed the initial configuration for BIG-IQ Centralized Management.

Summary	
Hostname	bigiq1
Discovery Address	10.0.1.5
DNS Lookup Servers	168.63.129.16
DNS Search Domains	uzcff0@hazube305p2hqlw1f.bx.internal.cloudapp.net
Time Servers	Base Registration Key: VJDGV-VXRTXN-MKO-SOSWWOWW-HWIKWDX Add-On Keys: LXZLYZE-DAWKZKJ License Activation Date: Jul 09, 2019 02:00:00(EST) License Status: License expires in 31 day(s), 15 hour(s). Active Modules: BIG-IQ, VE, Centralized Manager, Max Instances System Personality: BIG-IQ Central Management

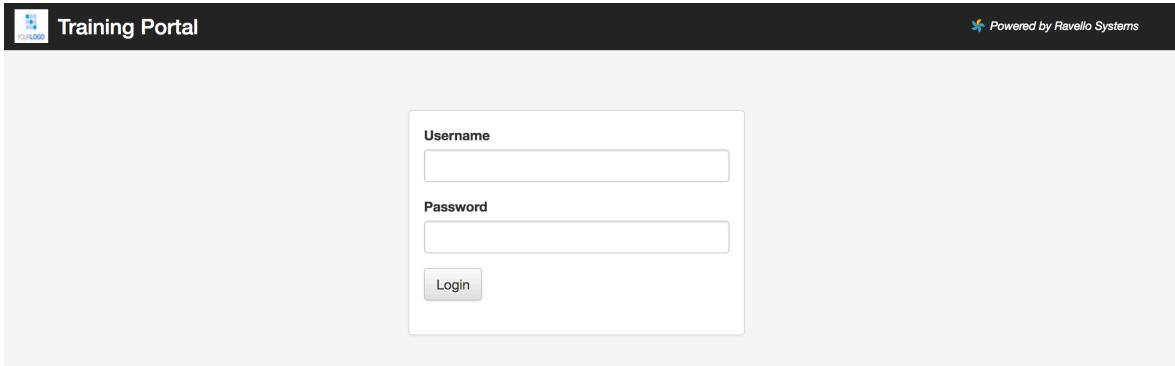
Previous

- 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: studentXX

Password: studentXX

Now you can see the available environment for the training:



Here are the available environments for this class:			
Name	# of VMs	# of running VMs	Actions
1 Day Training Lab Basis ASM - v13 - V2	3	3	<a href="#">View</a>

- Now you can click **View**.

 Training Portal

Hi, student1 student1 [Logout](#)

Powered by Ravello Systems

## 1 Day Training Lab Basis ASM - v13

[▶ Start](#) [■ Stop](#) [⟳ Restart](#) [⟳ Refresh](#)

<input type="checkbox"/> VM name	Status	IP	DNS	Actions
<input type="checkbox"/> Windows 7 External	STARTED	129.146.152.130	windows7external-1daytraininglabbas-jx1iwixs.srv.r...	<a href="#">» Go!</a> <a href="#">Console</a>
<input type="checkbox"/> LAMP v4 (Chris Manly)	STARTED			<a href="#">» Go!</a> <a href="#">Console</a>
<input type="checkbox"/> BIGIP_v13A	STARTED	129.146.153.151	bigipv13a-1daytraininglabbas-0rjr7lpm.srv.ravcloud...	<a href="#">» Go!</a> <a href="#">Console</a>

[◀ Back to Apps](#)

## 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>

The screenshot shows the F5 BIG-IP Configuration Utility login interface. On the left, there's a sidebar with fields for 'Hostname' (f5bigip.acme.com) and 'IP Address' (10.1.1.150). Below these are fields for 'Username' and 'Password', both of which are currently empty and highlighted with yellow. At the bottom of the sidebar is a 'Log in' button. The main right-hand panel has a header that reads 'BIG-IP Configuration Utility' and 'F5 Networks, Inc.'. It contains a welcome message: 'Welcome to the BIG-IP Configuration Utility.' followed by 'Log in with your username and password using the fields on the left.' At the bottom of the main panel, there's a copyright notice: '(c) Copyright 1996-2017, F5 Networks, Inc., Seattle, Washington. All rights reserved.' and links to 'F5 Networks, Inc. Legal Notices'.

- 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.

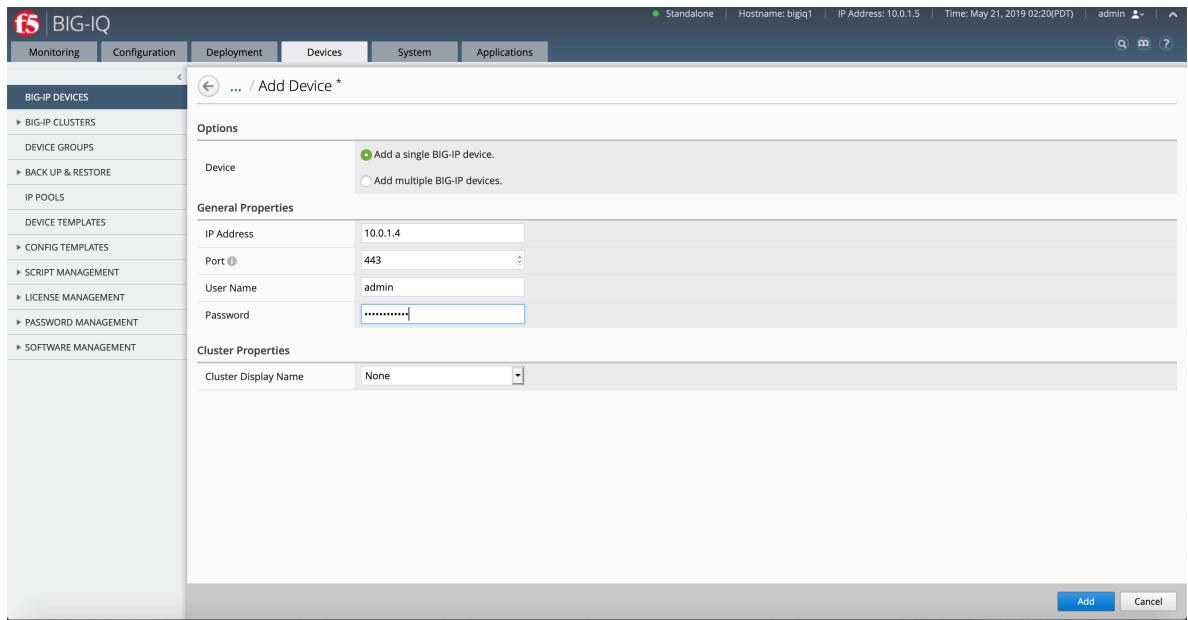
Name	dvwa_op_vs
Destination Address /Mask	10.1.10.35
Service Port	80
HTTP Profile	http
Source Address Translation	Automap
Default Pool	dvwa_op_pool

## Task 8 – Deploy a Consistent Security Policy

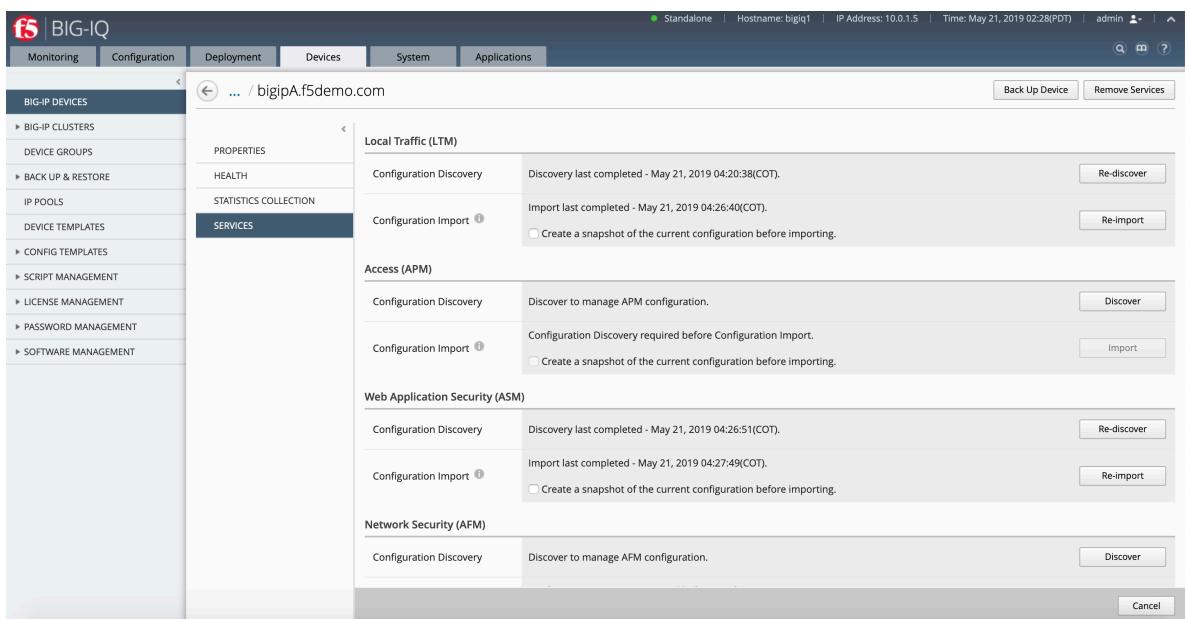
- Click on “Add Devices”

The screenshot shows the BIG-IQ Management interface. The top navigation bar includes tabs for Monitoring, Configuration, Deployment, Devices (which is selected), System, and Applications. The status bar at the top right indicates the device is Standalone, with Hostname: bigiq1, IP Address: 10.0.1.5, Time: May 21, 2019 02:19(PDT), and user admin. The left sidebar is collapsed, showing a list of management categories: BIG-IP DEVICES, BIG-IP CLUSTERS, DEVICE GROUPS, BACK UP & RESTORE, IP POOLS, DEVICE TEMPLATES, CONFIG TEMPLATES, SCRIPT MANAGEMENT, LICENSE MANAGEMENT, PASSWORD MANAGEMENT, and SOFTWARE MANAGEMENT. The main content area is titled 'BIG-IP Devices' and displays a table with the following columns: Status, Device Name, IP Address, Cluster Display Name, Stats Collection Status, Data Collection Device, Stats Last Collection Date, and Services. A message at the bottom of the table says 'There are no items to show in this view.'

- 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 on “Discover” and then click on “Import”



- Navigate on Configuration>Policies>Import

The screenshot shows the BIG-IQ Configuration interface. The top navigation bar includes Monitoring, Configuration (selected), Deployment, Devices, System, and Applications. The Configuration menu has several sections: ACCESS, LOCAL TRAFFIC, DNS, NETWORK, SECURITY, and Web Application Security. Under SECURITY, there are Threat Intelligence, Network Security, Fraud Protection Services, and Shared Security. The left sidebar under Devices is expanded, showing Policies (selected), Virtual Servers, Attack Signatures, Signature Sets, Cookie Protection, and Shared Security. The main content area displays a table titled 'Policies' with one item: 'templates-default'. The table columns are Name, Partition, Type, Available for Templates, Application Language, Parent, and Enforcement Mode. The 'Import' button in the toolbar is highlighted with a red arrow. Another red arrow points to the 'Policies' link in the sidebar.

- Import the Consistent Policy for the DVWA application

The screenshot shows the 'Import Policy' dialog box. The title bar says '... / Import Policy \*'. It has a 'Upload .xml file' section with a 'File Name' field containing 'exported\_dvwa-csp-template\_template\_2019-05-20\_07-35.xml' and a 'Choose File...' button. Below it is a 'Policy Name (Optional)' field with a dropdown menu. There is a large dashed rectangular area labeled 'Drop Policy Here'. At the bottom right are 'Import' and 'Cancel' buttons. The left sidebar is identical to the previous screenshot, showing the Policies section selected.

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

The screenshot shows the F5 BIG-IQ Configuration interface. The left sidebar is collapsed. The main navigation bar has tabs: Monitoring, Configuration (which is selected), Deployment, Devices, System, and Applications. Under Configuration, there are several sections: ACCESS (Access Groups, LOCAL TRAFFIC, DNS, NETWORK), SECURITY (Threat Intelligence, Network Security, Fraud Protection Services, Web Application Security), Devices, Policies, and Virtual Servers (which is selected). The main content area shows the properties of a Virtual Server named 'dvwa\_onPrem\_vs'. The 'Attached Policy' field contains '/Common/dvwa-csp'. A red arrow points to this field. Another red arrow points to the 'Save & Close' button at the bottom right of the dialog. Below the properties, there's a section titled 'Shared Objects: Policies' with a table showing two items: 'dvwa-csp' (Common, Security, No) and 'templates-default' (Common, Security, Yes (Default Policy)).

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

The screenshot shows the 'New Deployment - Web Application Security' dialog. The left sidebar is collapsed. The main navigation bar has tabs: Monitoring, Configuration (selected), Deployment, Devices, System, and Applications. Under Configuration, the 'Virtual Servers' section is selected. The dialog has tabs: General, Deployment, and Method. In the General tab, the 'Name' field is set to 'consistent\_security\_policy\_deploy'. In the Deployment tab, 'Current Changes' is selected under Source, 'All Changes' is selected under Source Scope, and 'Deploy Immediately' is selected under Method. The Method tab also has options for 'Create evaluation'. Below the tabs, there are two sections: 'Available' and 'Selected'. The 'Available' section shows a dropdown menu 'ASM Virtual Servers' with four items: 'cookie\_stealer\_server', 'csrf\_virtual', 'inactive', and 'inactive'. The 'Selected' section shows two items: 'dvwa\_onPrem\_vs' and 'dvwa\_vs', both checked. At the bottom right are 'Deploy' and 'Cancel' buttons.

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

The screenshot shows the BIG-IQ Configuration interface with the 'Deployment' tab selected. A deployment named 'New Deployment - Web Application Security' is open. In the 'Available' section, there is a table with three rows: 'csrf\_virtual' (Common, bigipA.f5demo.com), 'inactive' (Common, bigipA.f5demo.com), and 'inactive' (Common, fsvm01.eastus.cloudapp.azure.com). In the 'Selected' section, two devices are listed: 'bigipA.f5demo.com' (Address 129.213.195.104) and 'fsvm01.eastus.cloudapp.azure.com' (Address 10.0.1.4). Below the 'Selected' list are 'Deploy' and 'Cancel' buttons.

## 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

**Vulnerability: SQL Injection**

User ID:	<input type="text"/>	<input type="button" value="Submit"/>
----------	----------------------	---------------------------------------

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 #
```