

# Azure Functions

Azure Functions is a serverless solution that allows you to write less code, maintain less infrastructure, and save on costs. Instead of worrying about deploying and maintaining servers, the cloud infrastructure provides all the up-to-date resources needed to keep your applications running.

## Azure Portal Access

Login Portal: <https://portal.azure.com/>

Student numbers:

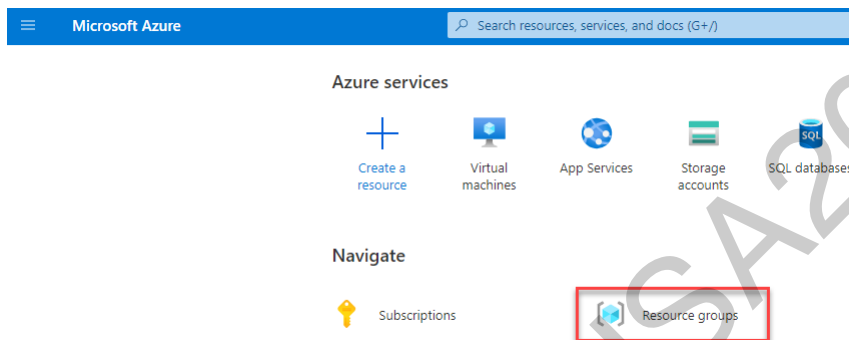
- Student numbers are generally a number between 1 and 60.
- We normally write these student numbers with preceding 0s.
- For example, Student number 1 is "Student001".
- We frequently replace your student number for "####" in this lab guide.
- Most of the time when you see ### in this lab guide, you will need to replace it with your student number, e.g. student 5 will need to replace "###" with "005".

Assigned Azure accounts for students are as follows...

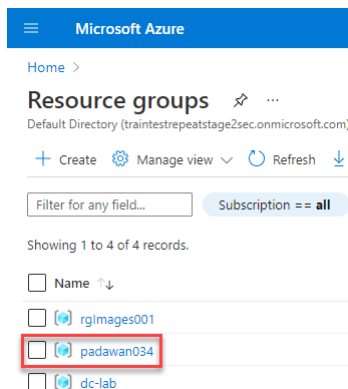
- Username (### is your student number): padawan###@traintestrepeatstage2sec.onmicrosoft.com
- Password: h0w1N0w2BROWN321COW
- Resource Group w/ Write Access (### is your student number): padawan###

## Creating an Azure Function App

Click on the "Resource group" icon:



Browse to your resource group and click on the name, e.g. padawan###:



Click on the "Create" button resource:

Home > Resource groups > padawan034

Resource groups

Default Directory (traintestrepeatstage2sec.onmicr...)

Filter for any field...

Name ↑↓

- ad-hunting-lab
- dc-lab
- padawan034
- rgImages001

Overview

- Activity log
- Access control (IAM)
- Tags
- Events

Settings

- Deployments
- Security
- Policies
- Properties
- Locks

Cost Management

- Cost analysis
- Cost alerts (preview)

Essentials

Subscription (change) : Pay-As-You-Go

Subscription ID : 74078d2e-d4de-4ca7-ad70-282472836afa

Tags (change) : [Click here to add tags](#)

Deployments : 1 Succeeded

Location : East US

Filter for any field...

Type == all X Location == all X Add filter

Showing 1 to 6 of 6 records.  Show hidden types

Name ↑↓	Type ↑↓	Location
vm016s034	Virtual machine	East US
vm016s034_disk1_3b1598a39af34ec18220026add0c9fe4	Disk	East US
vm016s034NSG	Network security group	East US
vm016s034PublicIP	Public IP address	East US
vm016s034VMNic	Network interface	East US
vm016s034VNET	Virtual network	East US

Search for "Function App"...

Home > Resource groups > padawan034 > Create a resource

Get started

Recently created

Categories

- AI + Machine Learning
- Analytics
- Blockchain

Function App

Windows Server 2019 Datacenter

Ubuntu Server 20.04 LTS

And press the "Enter" button...

We should then see this page...

Home > Resource groups > padawan034 > Create a resource > Function App

Function App

Microsoft

★ ★ ★ ★ ☆ 4.0 (1393 ratings)

Create

Where we will want to click the "Create" button.

Configure the following settings (replacing ## with your student number):

- Subscription: Pay-As-You-Go
- Resource Group: padawan034
- Function App Name: padawan###redir
- Publish: Code
- Runtime Stack: .NET
- Version: 3.1
- Region: East US

Your screen should now look similar to the following...

## Create Function App

Basics **Hosting** Monitoring Tags Review + create

Create a function app, which lets you group functions as a logical unit for easier management, deployment and sharing of resources. Functions lets you execute your code in a serverless environment without having to first create a VM or publish a web application.

### Project Details

Select a subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource Group \*  [Create new](#)

### Instance Details

Function App name \*  .azurewebsites.net

Publish \*  Code  Docker Container

Runtime stack \*

Version \*

Region \*

**Review + create** < Previous Next : Hosting >

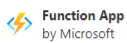
Now click the "Review + create" button.

Then click the "Create" button...

## Create Function App

Basics Hosting Monitoring Tags **Review + create**

### Summary



### Details

Subscription	74078d2e-d4de-4ca7-ad70-282472836afa
Resource Group	padawan034
Name	padawan034redir
Runtime stack	.NET 3.1

### Hosting

#### Storage (New)

Storage account	storageaccountpadawb5a9
-----------------	-------------------------

#### Plan (New)

Plan type	Consumption (Serverless)
Name	ASP-padawan034-acfc
Operating System	Windows
Region	East US
SKU	Dynamic

### Monitoring

Application Insights	Not enabled
----------------------	-------------

**Create** < Previous Next > [Download a template for automation](#)

Wait for the "Deployment is in progress" message to change to the "Your deployment is complete" message...

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo and a search bar. Below it, the breadcrumb trail reads "Home > Microsoft.Web-FunctionApp-Portal-65cca370-a4ad | Overview". The main content area displays a deployment status of "Your deployment is complete" with a green checkmark. It includes details such as "Deployment name: Microsoft.Web-FunctionApp-Portal-65cca370-a...", "Subscription: Pay-As-You-Go", and "Resource group: padawan034". A "Go to resource" button is highlighted with a red box.

And then click the "Go to resource" button.

From here, click the "Proxies" link...

The screenshot shows the Microsoft Azure portal interface for the "padawan034redir" Function App. The breadcrumb trail is "Home > Microsoft.Web-FunctionApp-Portal-65cca370-a4ad > padawan034redir". The left sidebar has the "Proxies" link highlighted with a red box. The main content area shows the "Proxies" page with a "+ Add" button highlighted with a red box. Below the button, there's a search bar for "Filter by name..." and a table with "Proxy name" and "No results.".

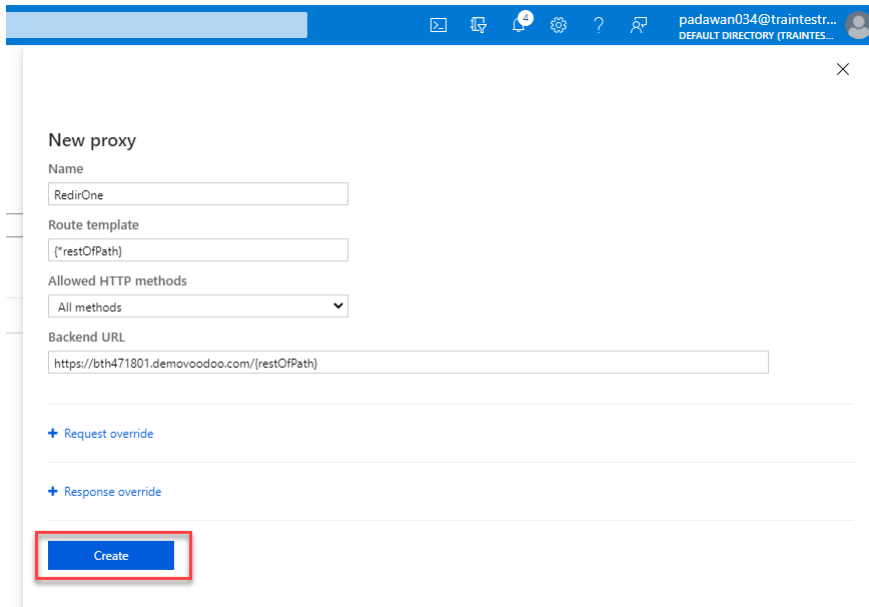
And then click the "+ Add" button...

This screenshot is similar to the previous one, showing the "Proxies" page for "padawan034redir". The "+ Add" button is highlighted with a red box. The "Filter by name..." search bar is visible, and the table below it shows "No results."

Then set the following settings, replacing ##### with your uniquely previously generated subdomain name:

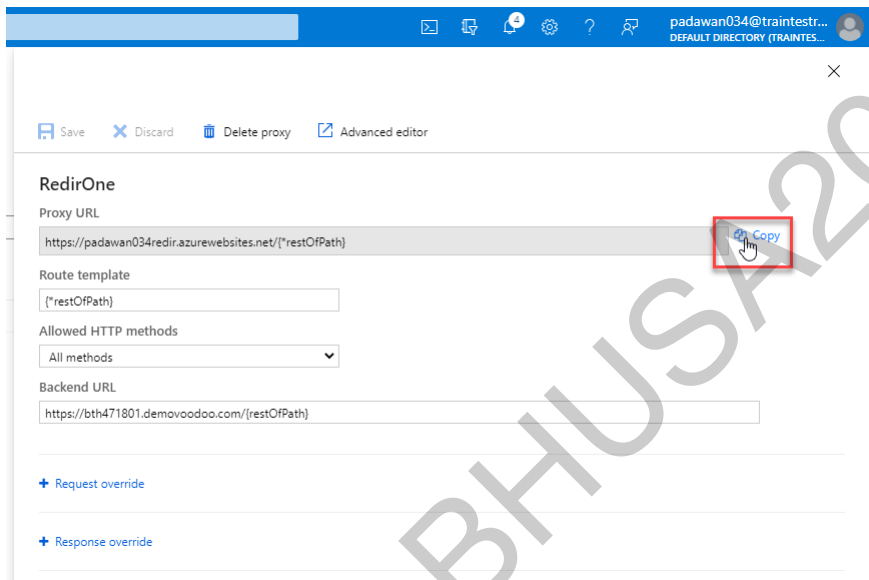
- Name: RedirOne
- Route template: {\*restOfPath}
- Allowed HTTP methods: All methods
- Backend URL: https://#####.demovoodoo.com/{restOfPath}

The screen should now look similar to the following...



The click the "Create" button.

Now click the "Copy" button to grab the URL...



We should now have a URL similar to the following...

```
https://padawan034redir.azurewebsites.net/{*restOfPath}
```

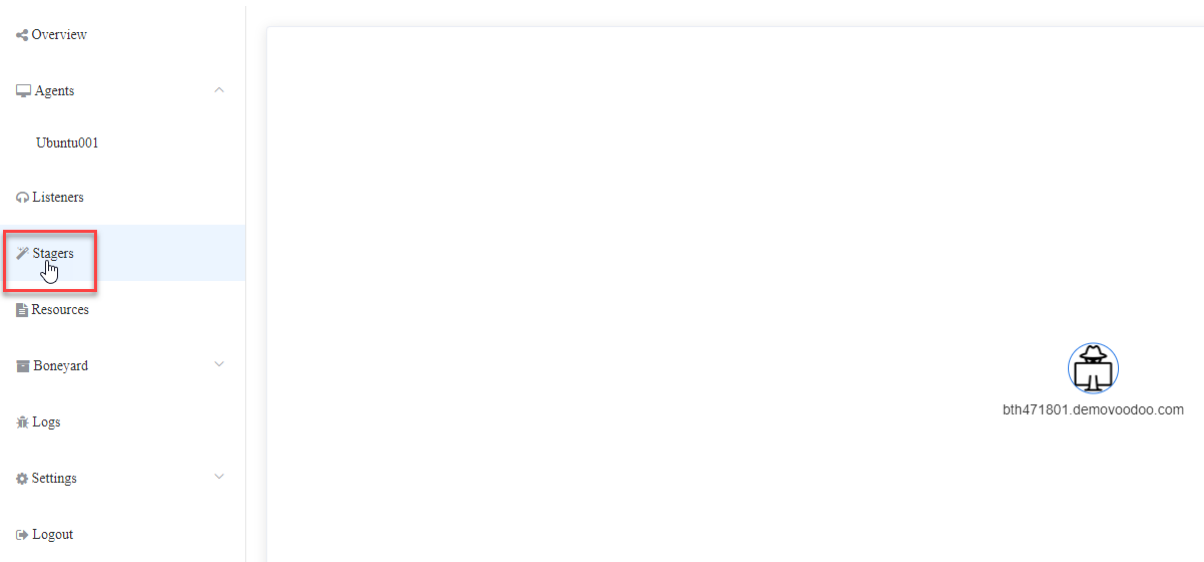
Check to see if the Voodoo LP docker container is still running on the public EC2 instance...

```
ubuntu@ip-10-0-1-215:~$ sudo su -
root@ip-10-0-1-215:~# cd /shared/
root@ip-10-0-1-215:/shared# docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
31200dbc33b8 cnoio/voodooce2020 "/usr/bin/python /ap..." 18 seconds ago Up 17 seconds 0.0.0.0:443->5000/tcp silly_khayyam
```

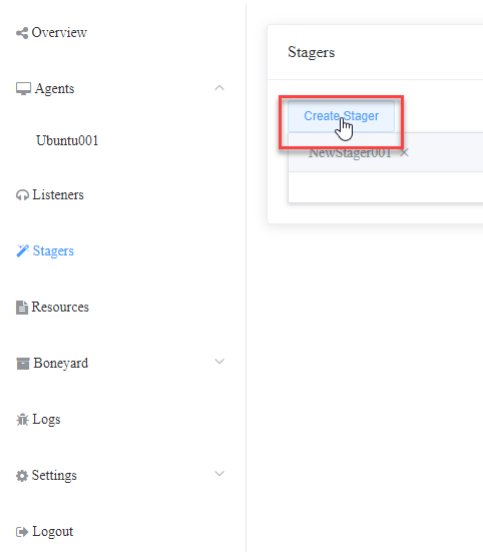
If you do not see it running in the "docker ps" command output, then start it up again via these commands...

```
root@ip-10-0-1-215:~# cd /shared/
root@ip-10-0-1-215:/shared# cnoio_voodooce
```

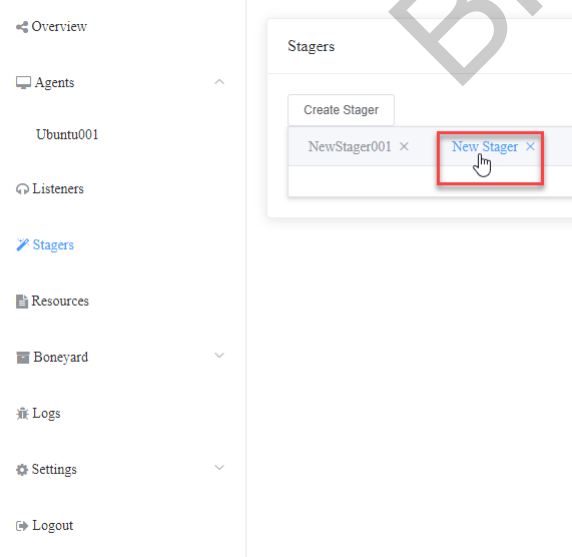
Using this information, let's create a new Voodoo stager which will use this Azure Function App as a redirector for our HTTPS comms, by first logging into the Voodoo LP (e.g. <https://#####.demovoodoo.com/>) and then secondly clicking the "Stager" link on the left hand side of web interface:



Then click the "Create stager" button



Then click on the name of the new stager...



Configure the new stager with the following settings (replacing ### with your student number):

- Name: AzureRedir
- Communication Style: HTTPS Call-back
- Domain: padawan###redir.azurewebsites.net
- Port: 443
- Callback interval (seconds): 1
- URL Path: /CRL/partial\_update
- Proxy: Use host settings
- Custom Headers: <None, N/A, Leave Blank>
- Target: Linux

- Architecture: x64
- Host Process: /usr/bin/apt
- Command Argument / Passphrase: update

The screen should now look similar to the following...

Stagers

Create Stager

NewStager001 x AzureRedir x

Some features are disabled in the community edition

Name AzureRedir

Communication Style  HTTPS Call-back  TCP Call-back  UDP Call-back  TLS Call-in

Domain padawan034redir.azurewebsites.net

Port 443

Callback interval (seconds) 1

URL Path /CRU/partial\_update

Proxy  Use host settings  Use specified proxy  Don't use a proxy

Custom headers Select Value

Target  Linux  Windows  Darwin  Android

Architecture  x64  ARM  ARM64

Host process /usr/bin/apt

Command Argument / Passphrase update

Now click the "Update" button...



Communication Style  HTTPS Call-back  TCP Call-back  UDP Call-back  TLS Call-in

Domain

Port

Callback interval (seconds)

URL Path

Proxy  Use host settings  Use specified proxy  Don't use a proxy

Custom headers

Target  Linux  Windows  Darwin  Android

Architecture  x64  ARM  ARM64

Host process

When we click on the agent, we should be able to run commands on the remote target via the redirector...

Overview Agents Ubuntu001 **Bevad** Listeners Stagers Resources Boneyard Logs Settings Logout

**Bevad** 3.15.173.195:41410 Amazon.com Inc. Columbus, Ohio 2021-07-22 23:03:54 ver 1.8

Console File System Process List Network Alerts Notes Export

Filter: Search  Include task output

```

18 ls /
-rw-r----- root root 6990432 2018-05-20 14:06:38 vmlinuz.old
dr-xr-xr-x root root 0 2021-07-21 17:44:22 sys
drwxr-xr-x root root 4096 2021-07-21 17:45:44 lib64
-rw-r--r-- root 12690404 2021-07-22 07:11:03 initrd.img
drwxrwxrwx root root 4096 2021-07-22 22:57:49 tmp
drwxr-xr-x root root 3240 2021-07-21 17:44:25 dev
drwxr-xr-x root root 12288 2021-07-22 07:00:07 sbin
drwxr-xr-x root root 4096 2021-05-22 10:53:51 mnt
drwxr-xr-x root root 4096 2021-07-21 17:47:09 opt
drwx----- root root 4096 2021-07-22 00:06:49 root
drwxr-xr-x root root 4096 2021-07-21 17:44:31 snap
drwxr-xr-x root root 4096 2018-05-22 10:53:51 media
drwxr-xr-x root root 1140 2021-07-22 15:38:24 run
drwxr-xr-x root root 4096 2021-07-22 07:11:03 boot
drwxr-xr-x root root 4096 2021-07-22 15:14:16 etc
-rw-r--r-- root root 12708948 2021-07-22 07:10:57 initrd.img.old
dr-xr-xr-x root root 0 2021-07-21 17:44:20 proc
-rw----- root root 7091968 2021-04-16 13:14:49 vmlinuz
drwxr-xr-x root root 4096 2018-05-22 10:53:51 srv
drwxr-xr-x root root 4096 2021-07-21 17:46:55 shared
drwxr-xr-x root root 4096 2021-07-22 07:00:20 bin
drwxr-xr-x root root 4096 2021-07-21 17:45:57 lib
drwxr-xr-x root root 4096 2021-07-22 07:10:51 ..
drwxr-xr-x root root 4096 2018-05-22 10:55:50 var
drwxr-xr-x root root 4096 2021-07-22 07:10:51 .
drwxr-xr-x root root 4096 2021-07-21 17:44:30 home
drwxr-xr-x root root 4096 2021-07-21 17:44:55 usr
drwx----- root root 16384 2018-05-22 11:00:44 lost+found

```

If we browse back over to the Azure's web portal, and view the main page regarding the Azure Function App we just created, after waiting a few minutes, we should see activity as our Azure Function is being utilized to redirect these call-back comms to the Voodoo LP...

Microsoft Azure

Search resources, services, and docs (G+)

Home > Microsoft.Web-FunctionApp-Portal-65cca370-a4ad >

### padawan034redir

Function App

Search (Ctrl+/) <<

Overview (highlighted)

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Security

Events (preview)

Functions

Functions

App keys

App files

Proxies

Deployment

Deployment slots

Deployment Center

Settings

Configuration

Authentication

Authentication (classic)

Application Insights

Identity

Backups

Custom domains

TLS/SSL settings

Networking

Networking (preview)

Scale up (App Service plan)

Browse Refresh Stop Restart Swap Get publish profile Reset publish profile Download app content Delete Send us your feedback

Click here to access Application Insights for monitoring and profiling for your app. →

#### Essentials

Resource group (change) : padawan034

Status : Running

Location : East US

Subscription (change) : Pay-As-You-Go

Subscription ID : 74078d2e-d4de-4ca7-ad70-282472836afa

Tags (change) : Click here to add tags

URL : http

Operating System : Win

App Service Plan : ASF

Properties : See

Runtime version : 3.1.

#### Metrics

Features (9) Notifications (1) Quickstart

##### Memory working set

Memory working set (Sum)  
padawan034redir  
27.26 MB

##### Function Execution Count

Function Execution Count (Sum)  
padawan034redir  
336

https://portal.azure.com/#@trainrestrepeatstage2sec.onmicrosoft.com/resource/subscriptions/74078d2e-d4de-4ca7-ad70-282472836afa/...

## References

References:

- <https://docs.microsoft.com/en-us/azure/azure-functions/functions-overview>
- <https://docs.microsoft.com/en-us/azure/azure-functions/functions-proxies>