

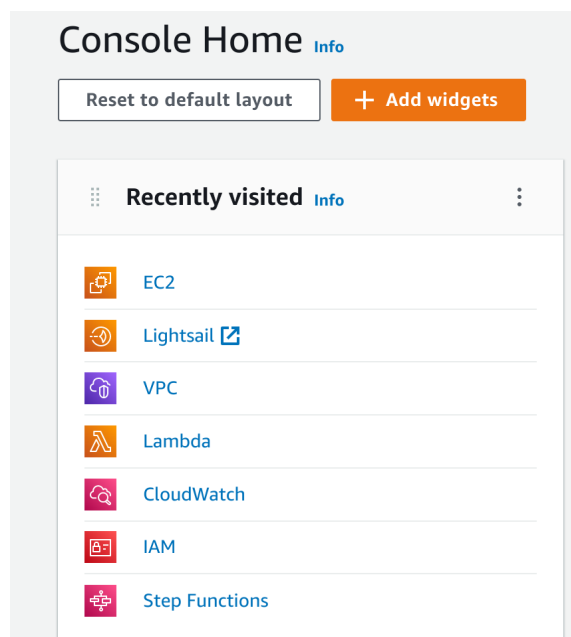
#### #### aws\_public\_ec2\_setup

# Instructions to set up public AWS EC2

e.g. to host a flask server, dashboard, REST api endpoint, etc.

### Go to: AWS

<https://us-east-1.console.aws.amazon.com>

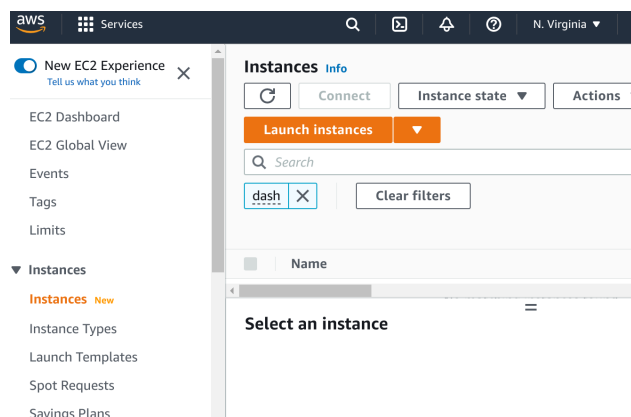


### Go to: EC2

<https://us-east-1.console.aws.amazon.com/ec2/>

### Go to: instances

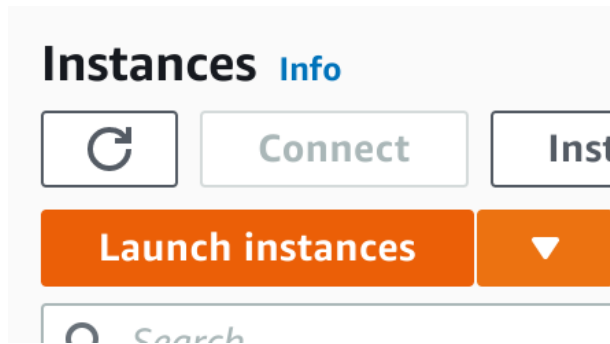
the instances tab



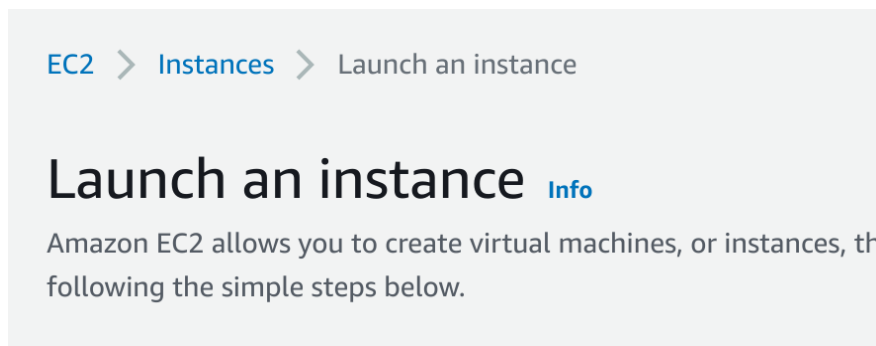
## ## Launch Instance:

Hit the big orange button that says "Launch instances"

*(plural...for some reason...which of course takes to you "launch an instance" singular)*



## # "launch an instance" singular



## ## Configure:

1. Name and tags -> clear meaningful name, nothing is too obvious. recommended format: "ec2\_purpose\_yourname\_datetime"
2. Application and OS Images (Amazon Machine Image) -> default amazon linux
3. Instance type -> nano (scroll down)
4. Key pair (login) -> select or make new pair
5. Network settings...(see below)

## # Network settings:

1. firewall security group: create or select
2. "Allow SSH traffic from": must be on to use EC2 connect later (or SSH in yourself)
3. "Allow HTTPs traffic from the internet": If you want this to be public, allow.
4. http: maybe leave insecure http off.

▼ Network settings [Get guidance](#)

Edit

Network [Info](#)

vpc-c840bcb5

Subnet [Info](#)

No preference (Default subnet in any availability zone)

Auto-assign public IP [Info](#)

Enable

**Firewall (security groups) [Info](#)**

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group

☐ Select existing security group

We'll create a new security group called 'launch-wizard-9' with the following rules:

☒ Allow SSH traffic from

Helps you connect to your instance

Anywhere

0.0.0.0/0

☒ Allow HTTPs traffic from the internet

To set up an endpoint, for example when creating a web server

☐ Allow HTTP traffic from the internet

To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

×

#### #### Network settings (continued...)

6. Storage (volumes -> use default

7. Advanced details Info -> ignore

8. Summary -> nothing to do or change here, examine if you want.

#### ## Select: Launch Instance

EC2 > [Instances](#) > Launch an instance

## Launching instance

Please wait while we launch your instance.

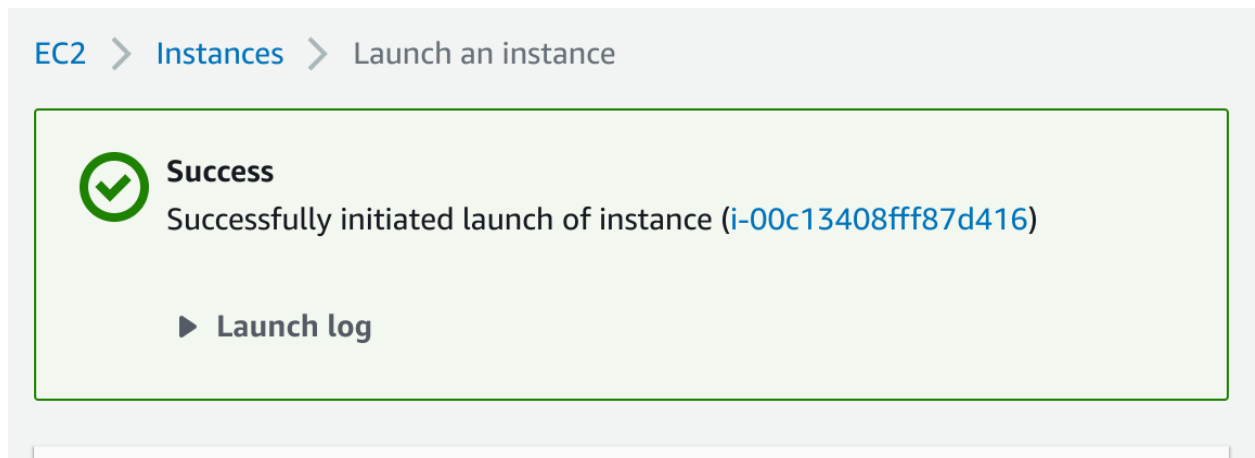
Do not close your browser while this is loading.

↻ Launch initiation

69%

▶ Details

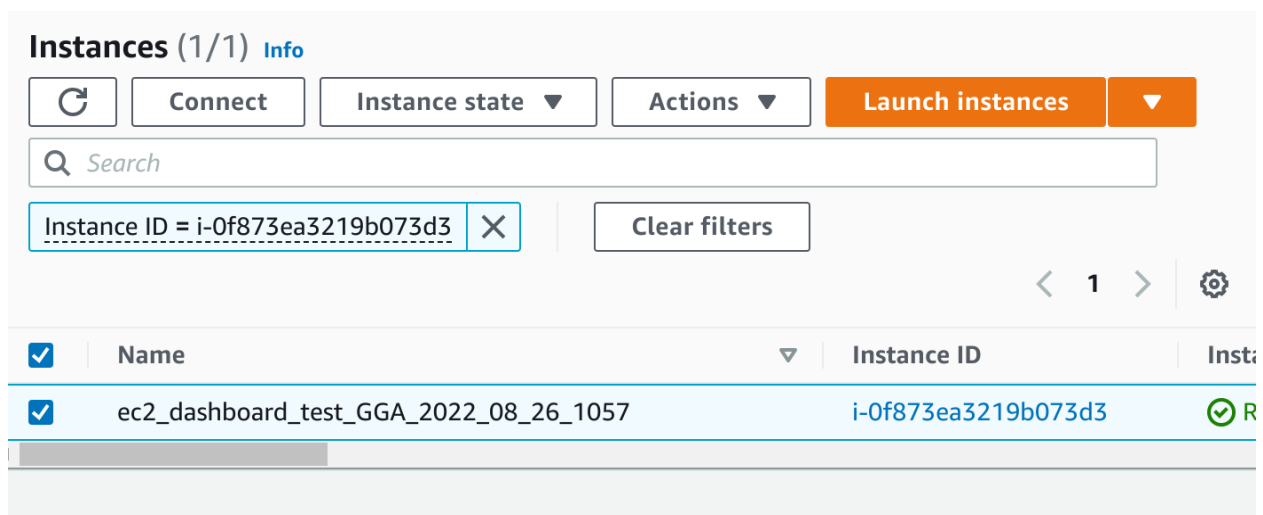
## click on blue random string .... (obviously!...?)



## Back at instances window:

your instance should now be highlighted: click on "connect" to connect via web

This is much easier than local-cli ssh (web connect is one of the few actually useful working advances AWS has made).



# configure in "security"

(Obviously, since you want to do network configuration, and you have the choice of 'networking' you instead need to go to "security." So user friendly.)



## Another random blue-string-click

In the "Security" tab, under "security groups" (plural?) you see a random blue-string-link. click on that (to configure networking...obviously...)

Instance: i-0f873ea3219b073d3 (ec2\_dashboard\_test\_GGA\_2022\_08\_26\_1057)

The screenshot shows the AWS Management Console interface for an EC2 instance. The top navigation bar includes tabs for Details, Security (which is selected and highlighted in orange), Networking, Storage, Status checks, Monitoring, and Tags. Below the tabs, there is a section titled "Security details" with a downward arrow. This section is divided into two columns. The left column contains "IAM Role" with a value of "-" and "Security groups" with a link to "sg-0db3475a6b53fcb3f (launch-wizard-10)". The right column contains "Owner ID" with a value of "451917392135".

## "Inbound rules" You are here!

Finally: This is the basic, rudimentary, necessary, "start here" configuration menu that all this has been leading up to (and should have started with), yet for some obscene reason AWS makes it impossible to even find.

The screenshot shows the "Inbound rules (1/1)" configuration page in the AWS Management Console. At the top, there are three buttons: a refresh button, "Manage tags", and "Edit inbound rules". Below these buttons is a search bar with the placeholder text "Filter security group rules". To the right of the search bar are navigation controls showing "< 1 >" and a settings gear icon.

### Click "edit inbound rules"

This is a close-up screenshot of the "Edit inbound rules" button, which is a large, rectangular button with a dark border and the text "Edit inbound rules" in a bold, sans-serif font.

### Make and save new rules.  
Using the following tool (which you should see now),

EC2 > Security Groups > sg-0db3475a6b53fcb3f - launch-wizard-10 > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
sg-0089de7ff69db6c39	HTTPS ▼	TCP	443	Custom <input type="text" value="0.0.0.0/0"/>		<div>Delete</div>
<div>Add rule</div>						

Cancel

Preview changes

Save rules

Create and save (using the big orange "Save rules" button) the rules in this table.  
Existing rules may need to be modified or replaced (e.g. HTTPS may be set to custom, set it to Anywhere IPV4)

...

	Type	(Protocol)	Port Range	Source	(to)
1.	HTTPS TCP	TCP	443	Anywhere IPV4	0.0.0.0/0
2.	Custom TCP	TCP	8080	Anywhere IPV4	0.0.0.0/0
3.	SSH	TCP	22	Custom	0.0.0.0/0

...

EC2 > Security Groups > sg-0db3475a6b53fcb3f - launch-wizard-10 > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
sg-0089de7ff69db6c39	HTTPS ▼	TCP	443	Anywhere-IPV4 <input type="text" value="0.0.0.0/0"/>		<div>Delete</div>
-	Custom TCP ▼	TCP	8080	Anywhere-IPV4 <input type="text" value="0.0.0.0/0"/>		<div>Delete</div>
<div>Add rule</div>						

Cancel

Preview changes

Save rules

Another example rule set:

Set **Type** *HTTP*, **Protocol** *TCP*, **Port range** *80*, and **Source** to "*0.0.0.0/0*".

Set **Type** *HTTP*, **Protocol** *TCP*, **Port range** *80*, and **Source** to "*::/0*".

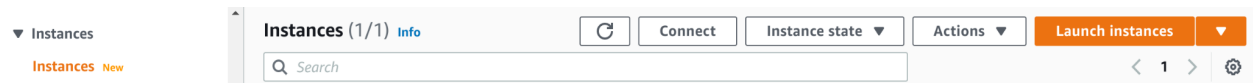
Set **Type** *Custom TCP*, **Protocol** *TCP*, **Port range** *8080*, and **Source** to "*0.0.0.0/0*".

Set **Type** *SSH*, **Protocol** *TCP*, **Port range** *22*, and **Source** to "*0.0.0.0/0*".

Set **Type** *HTTPS*, **Protocol** *TCP*, **Port range** *443*, and **Source** to "*0.0.0.0/0*".

Done.

### Go back to the instances tab

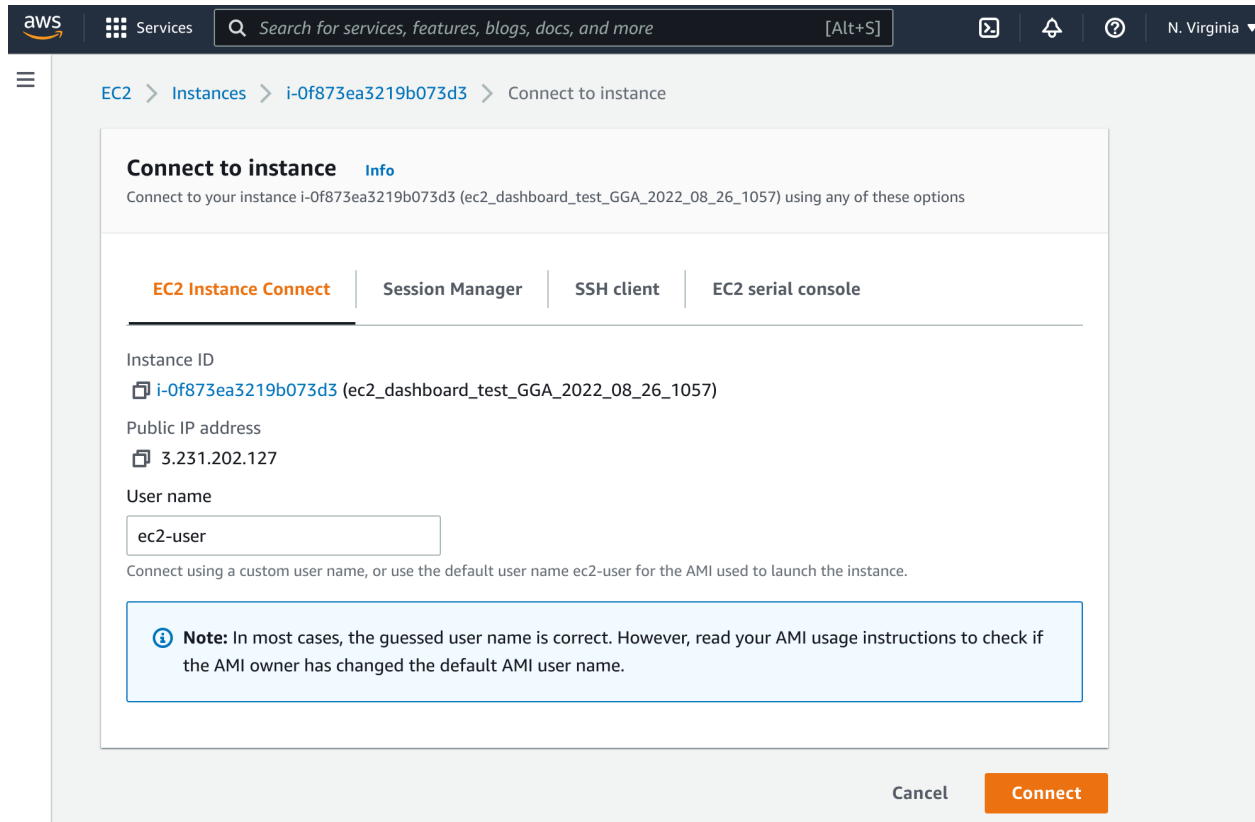


# Web Connect

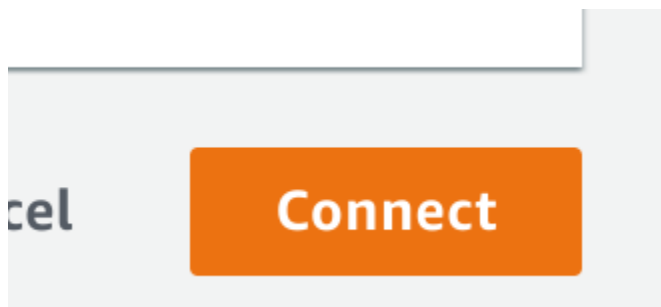
## click on "connect"



### In the 'connect to instance' window  
in the "EC2 Instance Connect" tab...

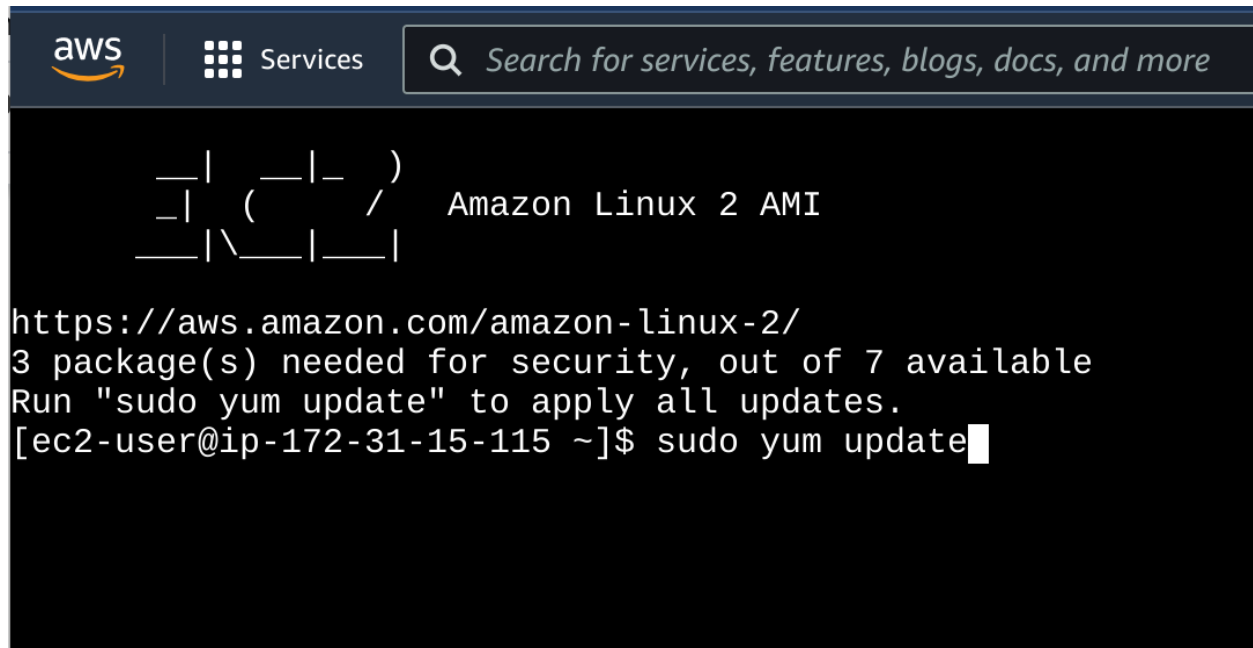


### Click on "Connect" (the big orange button)...(dejavu?)





### Like SSH but with no convoluted local aws-cli setup nightmare. (This is a good thing.)



### Optional steps

You are effectively done, but you may want to run these lines, e.g. if you are going to get files from github

...

```
$ sudo yum update -y
```

```
$ sudo yum install git -y
```

...