

Bootstrap Scripts

<https://docs.aws.amazon.com/cdk/v2/guide/bootstrapping.html>

1. At your EC2 dashboard, click on launch instance
2. Of course, you would want to use the Amazon Linux 2 Kernel which is the free tier
3. So to do the bootstrap scripts you have to go down to the very bottom and you will see advanced details, expand that.
 - a. You then want to find "User Data" which looks like this below
4. You then want to input the script into the field

User data [Info](#)

```
#!/bin/bash
yum update -y
yum install httpd -y
service httpd start
cd /var/www/html
echo "<html><body><h1>Hello, this is Cam Cam</h1></body></html>" >
index.html
```

5. Then here you would use your standard storage
6. Find the security group. This may be under the network settings
7. Here you would like to name the security group.
 - a. Everything in this security group is going to be a web server
8. Add a rule to where the type shows SSH, HTTP & HTTPS

And remember 0.0.0.0/0

^ open that IP range. You wouldn't want to do this for SSH or RDP because this opens for an attack within your EC2 instances

Type Info	Protocol Info	Port range Info
ssh ▼	TCP	22
Source type Info	Source Info	Description - optional Info
Anywhere ▼	<input type="text" value="Add CIDR, prefix list or security group ID"/> 0.0.0.0/0 ✕	e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, Multiple sources) Remove

Type Info	Protocol Info	Port range Info
HTTP ▼	TCP	80
Source type Info	Source Info	Description - optional Info
Custom ▼	<input type="text" value="Add CIDR, prefix list or security group ID"/> <input type="text" value="::/0 ✕"/> <input type="text" value="0.0.0.0/8 ✕"/>	e.g. SSH for admin desktop

▼ Security group rule 3 (TCP, 443, Multiple sources) Remove

Type Info	Protocol Info	Port range Info
HTTPS ▼	TCP	443
Source type Info	Source Info	Description - optional Info
Custom ▼	<input type="text" value="Add CIDR, prefix list or security group ID"/> <input type="text" value="::/0 ✕"/> <input type="text" value="0.0.0.0/16 ✕"/>	e.g. SSH for admin desktop

9. Once all of that is created and verified click launch
10. Before launching you would have to create a new key pair

☒ Create new key pair
 ☐ Proceed without key pair

Key pair name

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type
☒ RSA
 RSA encrypted private and public key pair
☐ ED25519
 ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format
☒ .pem
 For use with OpenSSH
☐ .ppk
 For use with PuTTY

Cancel
Create key pair

- a. Here I named it "CamBSS" for Cams BootStrap Script
11. This will then download the .pem file
12. Click Launch Instance
13. Once that is completed click "view all instances"
14. The instance is now going to sit behind a security group that is open to port 80
15. Once you select the instance that was launched/created if you select the "security" tab

Instance: i-0b13c64da49db6f9e

Details
 Security
 Networking
 Storage
 Status checks
 Monitoring
 Tags

▼ Security details

- And down below are the inbound rules

▼ Inbound rules

Security group rule ID	Port range	Protocol	Source	Security groups
sgr-0419b717b6f874869	80	TCP	0.0.0.0/8	DMZ_Web
sgr-0ed042ea4f62dcc53	443	TCP	::/0	DMZ_Web
sgr-088e525a76b0b4636	443	TCP	0.0.0.0/16	DMZ_Web
sgr-017b459a67423b6cf	22	TCP	0.0.0.0/0	DMZ_Web
sgr-04b63f72c5ab472f5	80	TCP	::/0	DMZ_Web

17. I went back and changed the inbound rules for port 443 and port range 80. See down below

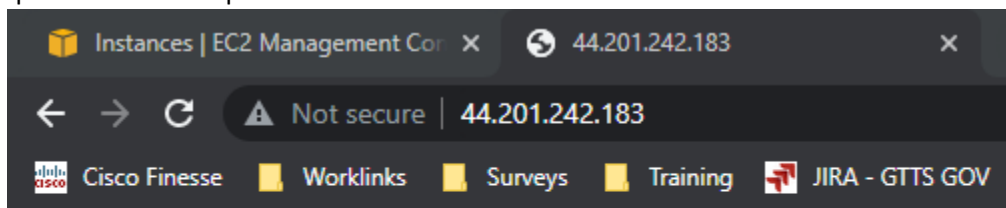
Info

80	Anywhe...	0.0.0.0/0 X
443	Custom	::/0 X
443	Anywhe...	0.0.0.0/0 X
22	Custom	0.0.0.0/0 X
80	Anywhe...	::/0 X

18. Once everything looks good, go back into the instance and go into the detail tab where it has the public IPv4 address

Details	Security	Networking	Storage	Status checks	Monitoring	Tags
▼ Instance summary Info						
Instance ID i-0b13c64da49db6f9e		Public IPv4 address 44.201.242.183 open address				
IPv6 address -		Instance state Running				
Hostname type IP name: ip-172-31-89-124.ec2.internal		Private IP DNS name (IPv4 only) ip-172-31-89-124.ec2.internal				

19. Copy and paste that public address and it should take you to the script for a webpage you implemented on step 4 above.



Hello, this is Cam Cam

20. The reason we can see this is because we opened up port 80 on our security group.

- If we deleted port 80 of course we would no longer go into the webpage.