Contents

Execution Steps

1. [Manually] Creat S3 bucket with name myapp-6291-7066-6893-demo

2. [AWS CLI] Upload myApp.zip includes data of {index.html , me.jbg}

aws s3 cp .\myApp.zip s3://myapp-6291-7066-6893-demo/

3. [Manually] Create ketpair "myAppNVirginiaEC2KP.pem" to be used in EC2Web instances in CF template && "jumbbox-key.pem" for Bastion Host

4. Run CF template

aws cloudformation create-stack --stack-name myWebApp --region us-east-1 --template-body file://networkandserver.yml --parameters file://networkandserver.json --capabilities "CAPABILITY_IAM" "CAPABILITY_NAMED_IAM"

aws cloudformation update-stack --stack-name myWebApp --region us-east-1 --template-body file://networkandserver.yml --parameters file://networkandserver.json --capabilities "CAPABILITY_IAM" "CAPABILITY_NAMED_IAM"

aws cloudformation delete-stack --stack-name myWebApp --region us-east-1

5. [Manually] Create Bastion Host in a publicsubnet.

ServerSpecs:

Amazon Linux 2 AMI (HVM), SSD Volume Type

t2.micro

myAppVPC

publicsubnet

Auto Assign public IP

Storage:

8 GB

Tags:

Name=JumbBox

SG:

Name=JumbBox-SG

Inbound Rules= Allow SSH on port 22, Source=MY IP, Description=Administrator Access

Keypair:

jumbbox-key.pem

6. Connect to jumbbox and verify connection to EC2 instances

ssh -i "jumbbox-key.pem" ec2-user@<JumbBox PublicIP> #just to check ssh connection

scp -i "jumbbox-key.pem" myAppNVirginiaEC2KP.pem ec2-uer@<JumbBox PublicIP>:/home/ec2-user/myAppNVirginiaEC2KP.pem #copy from host machine to jumbbox server

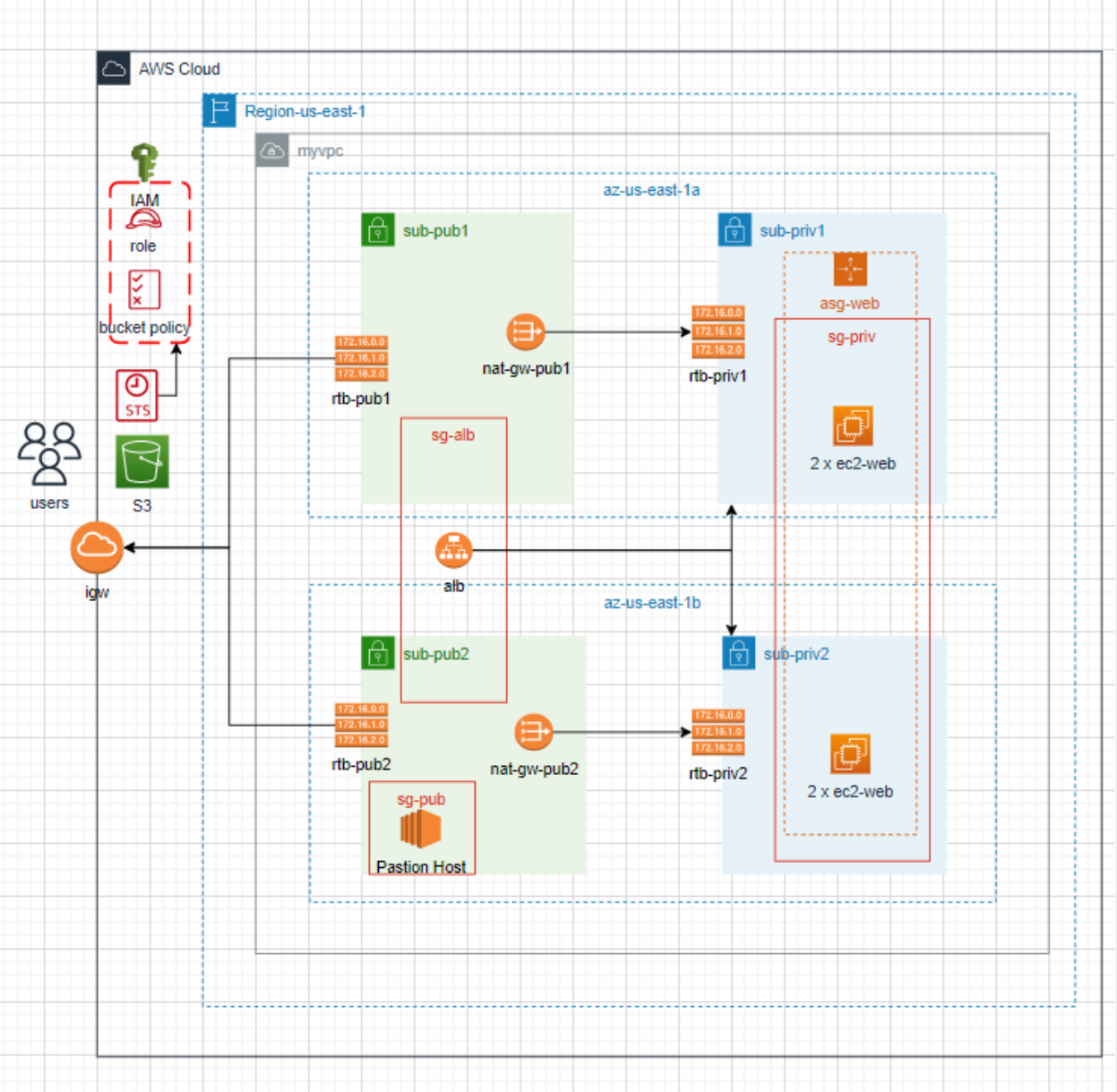
ssh -i "jumbbox-key.pem" ec2-user@<JumbBox PublicIP>

ls

chmod 400 myAppNVirginiaEC2KP.pem

ssh -i "myAppNVirginiaEC2KP.pem" ubuntu@<EC2-PrivateIP>

Schematic Design



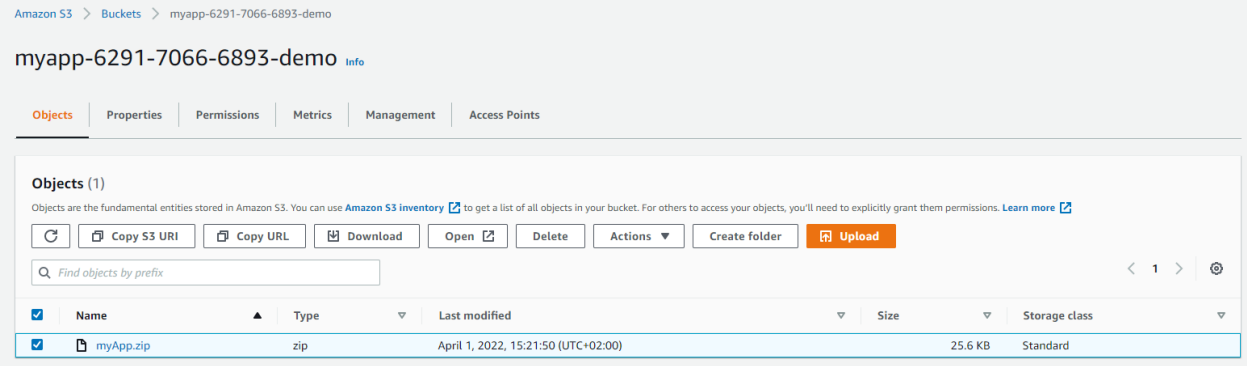
Keypairs

Key pairs (4) Info

Filter key pairs

Name	Type	Fingerprint	ID
egfwd-aws-1	rsa	bc:b5:5b:c4:9d:dd:6c:25:75:4c:14:03:8…	key-064b0ada10e4af624
jumbbox-key	rsa	b7:62:80:6b:82:5b:ac:01:80:7d:05:02:3…	key-095c1da37c4a4ff82
myAppNVirginiaEC2KP	rsa	d9:6a:84:f5:93:38:59:33:ac:94:e6:5b:1…	key-0fb9111d0f2ff4972
vockey	rsa	d2:c7:91:0b:b1:99:9b:8b:cd:24:35:12:f…	key-00c5a26f18a86770c

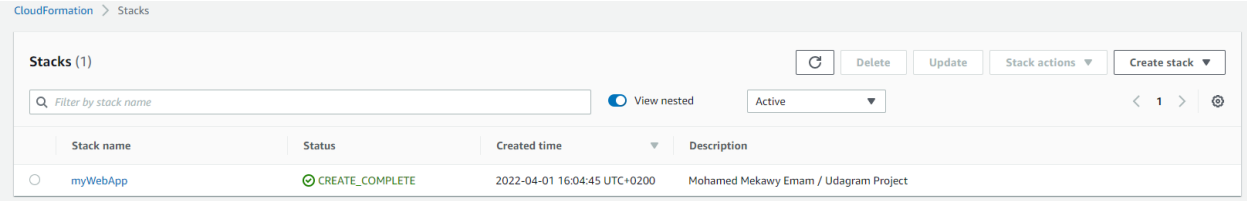
S3 Bucket



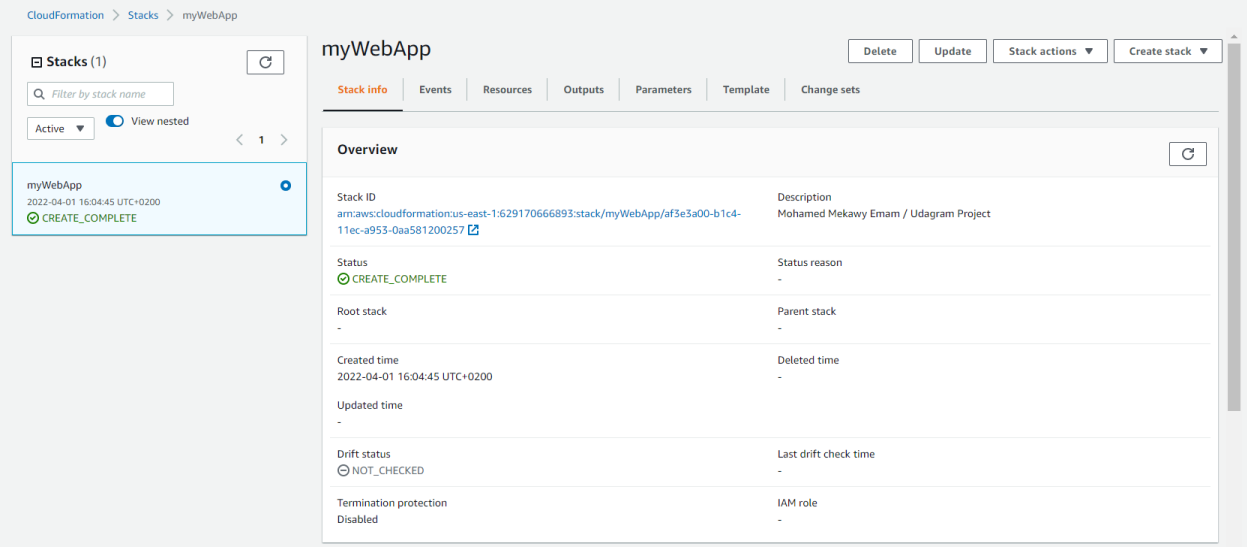
Running CF template

```
PS C:\Users\mohamed.mekawy\Desktop\Data\Udacity\EgFwdAWS\MohamedMekawy-p2\Deploy-a-High-Availability-Web-App-Using-CloudFormation> aws cloudformation create-stack  --stack-name myWebApp --region us-east-1 --template-body file://networkandserver.yml --parameters file://networkandserver.json --capabilities "CAPABILITY_IAM" "CAPABILITY_NAMED_IAM"
{
    "StackId": "arn:aws:cloudformation:us-east-1:629170666893:stack/myWebApp/af3e3a00-b1c4-11ec-a953-0aa581200257"
}
```

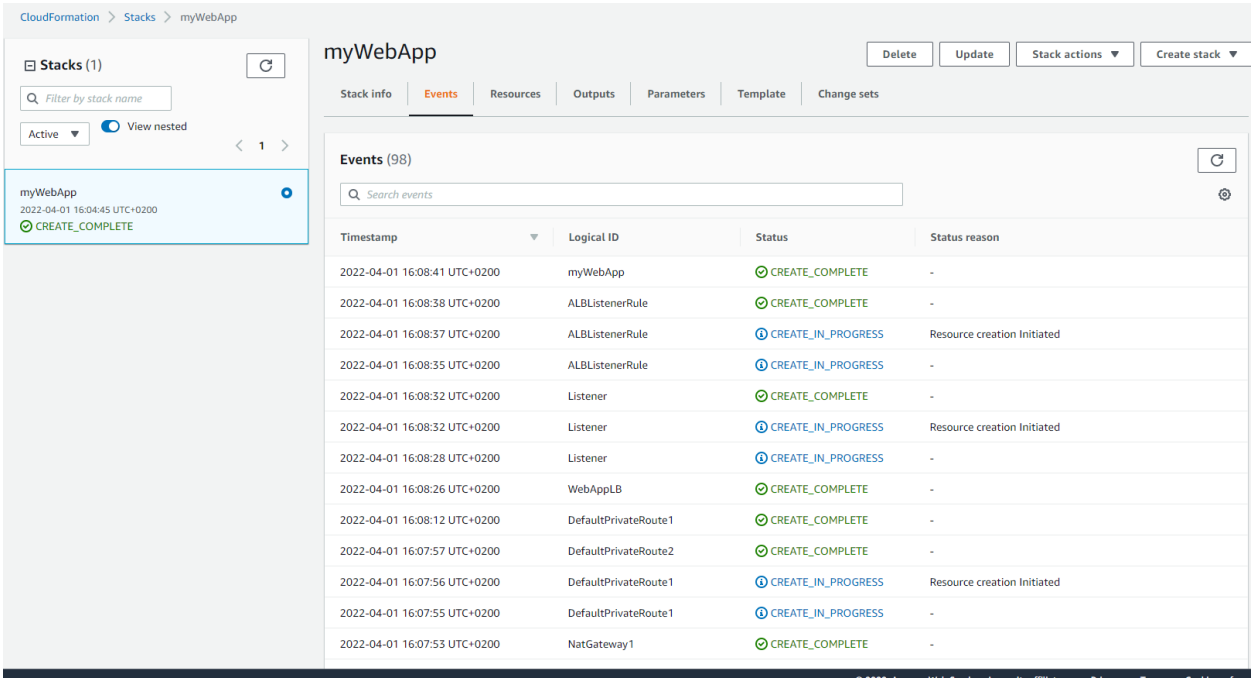
CloudFormation Stack



Stack Info



Stack Events



CloudFormation > Stacks > myWebApp

Stacks (1)

Filter by stack name

Active | View nested | 1

myWebApp
2022-04-01 16:04:45 UTC+0200
CREATE_COMPLETE

myWebApp

Delete | Update | Stack actions | Create stack

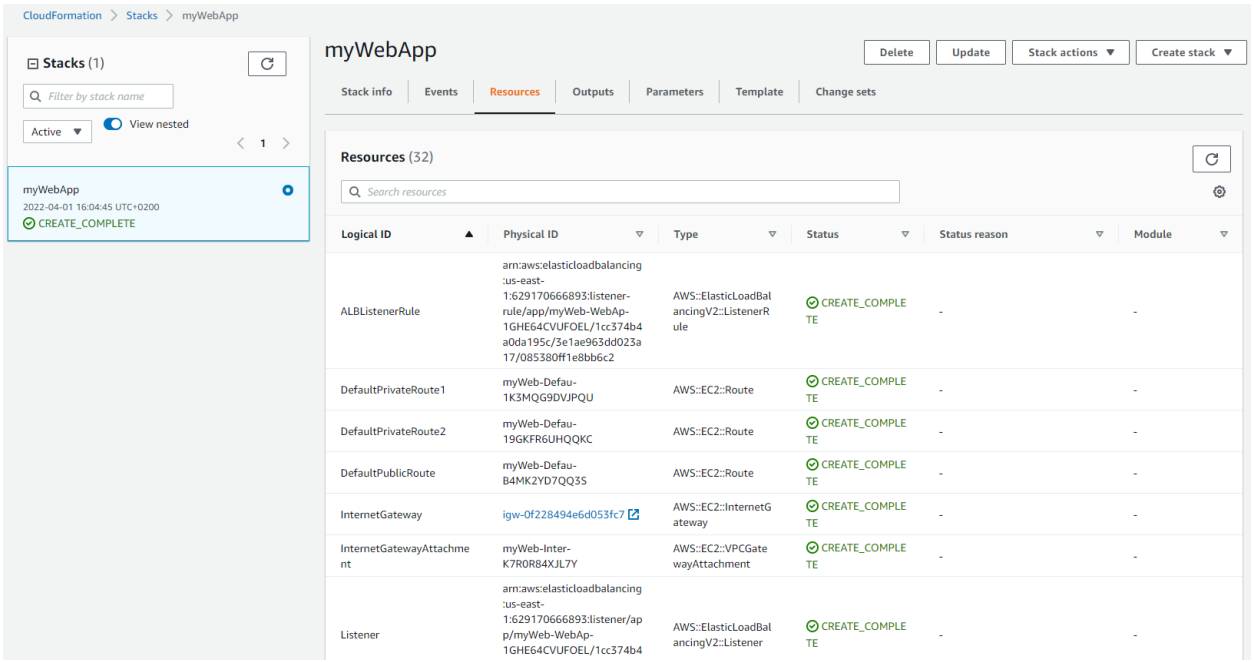
Stack info | Events | Resources | Outputs | Parameters | Template | Change sets

Events (98)

Search events

Timestamp	Logical ID	Status	Status reason
2022-04-01 16:08:41 UTC+0200	myWebApp	CREATE_COMPLETE	-
2022-04-01 16:08:38 UTC+0200	ALBListenerRule	CREATE_COMPLETE	-
2022-04-01 16:08:37 UTC+0200	ALBListenerRule	CREATE_IN_PROGRESS	Resource creation Initiated
2022-04-01 16:08:35 UTC+0200	ALBListenerRule	CREATE_IN_PROGRESS	-
2022-04-01 16:08:32 UTC+0200	Listener	CREATE_COMPLETE	-
2022-04-01 16:08:32 UTC+0200	Listener	CREATE_IN_PROGRESS	Resource creation Initiated
2022-04-01 16:08:28 UTC+0200	Listener	CREATE_IN_PROGRESS	-
2022-04-01 16:08:26 UTC+0200	WebAppLB	CREATE_COMPLETE	-
2022-04-01 16:08:12 UTC+0200	DefaultPrivateRoute1	CREATE_COMPLETE	-
2022-04-01 16:07:57 UTC+0200	DefaultPrivateRoute2	CREATE_COMPLETE	-
2022-04-01 16:07:56 UTC+0200	DefaultPrivateRoute1	CREATE_IN_PROGRESS	Resource creation Initiated
2022-04-01 16:07:55 UTC+0200	DefaultPrivateRoute1	CREATE_IN_PROGRESS	-
2022-04-01 16:07:53 UTC+0200	NatGateway1	CREATE_COMPLETE	-

Stack Resources



CloudFormation > Stacks > myWebApp

Stacks (1)

Filter by stack name

Active | View nested | 1

myWebApp
2022-04-01 16:04:45 UTC+0200
CREATE_COMPLETE

myWebApp

Delete | Update | Stack actions | Create stack

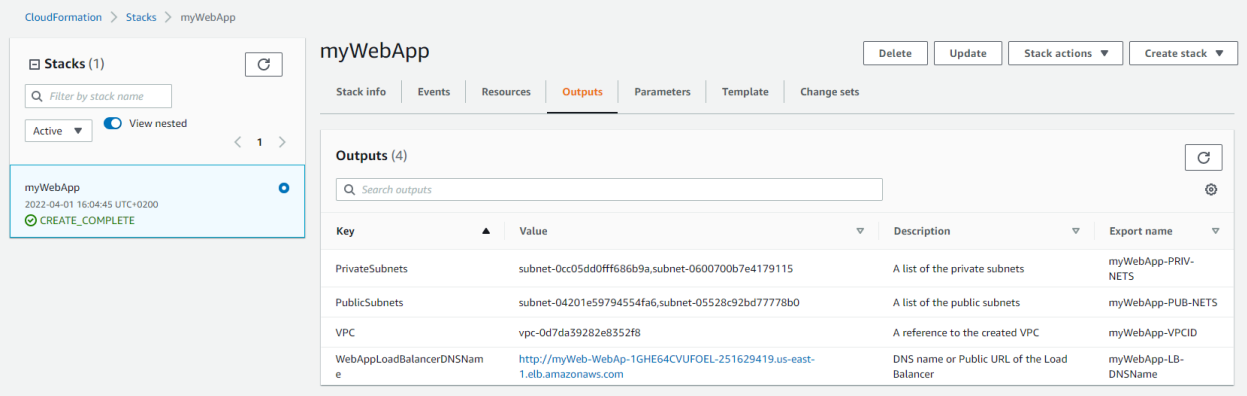
Stack info | Events | Resources | Outputs | Parameters | Template | Change sets

Resources (32)

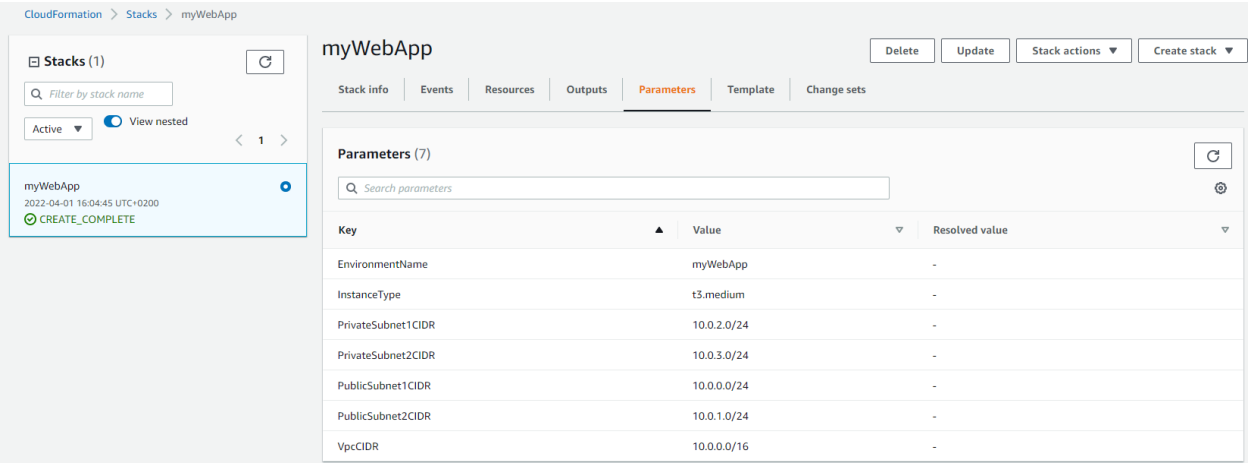
Search resources

Logical ID	Physical ID	Type	Status	Status reason	Module
ALBListenerRule	arn:aws:elasticloadbalancing:us-east-1:629170666893:listener-rule/app/myWeb-WebAp-1GHE64CVUFOEL/1cc374b4a0da195c/3e1ae963dd023a17/085380ff1e8bb6c2	AWS::ElasticLoadBalancingV2::ListenerRule	CREATE_COMPLETE	-	-
DefaultPrivateRoute1	myWeb-Defau-1K3MQG9DVJPQU	AWS::EC2::Route	CREATE_COMPLETE	-	-
DefaultPrivateRoute2	myWeb-Defau-19GKFR6UHQQKC	AWS::EC2::Route	CREATE_COMPLETE	-	-
DefaultPublicRoute	myWeb-Defau-B4MK2YD7QQ3S	AWS::EC2::Route	CREATE_COMPLETE	-	-
InternetGateway	igw-0f228494e6d053fc7	AWS::EC2::InternetGateway	CREATE_COMPLETE	-	-
InternetGatewayAttachment	myWeb-Inter-K7R0R84XJL7Y	AWS::EC2::VPCGatewayAttachment	CREATE_COMPLETE	-	-
Listener	arn:aws:elasticloadbalancing:us-east-1:629170666893:listener/app/myWeb-WebAp-1GHE64CVUFOEL/1cc374b4	AWS::ElasticLoadBalancingV2::Listener	CREATE_COMPLETE	-	-

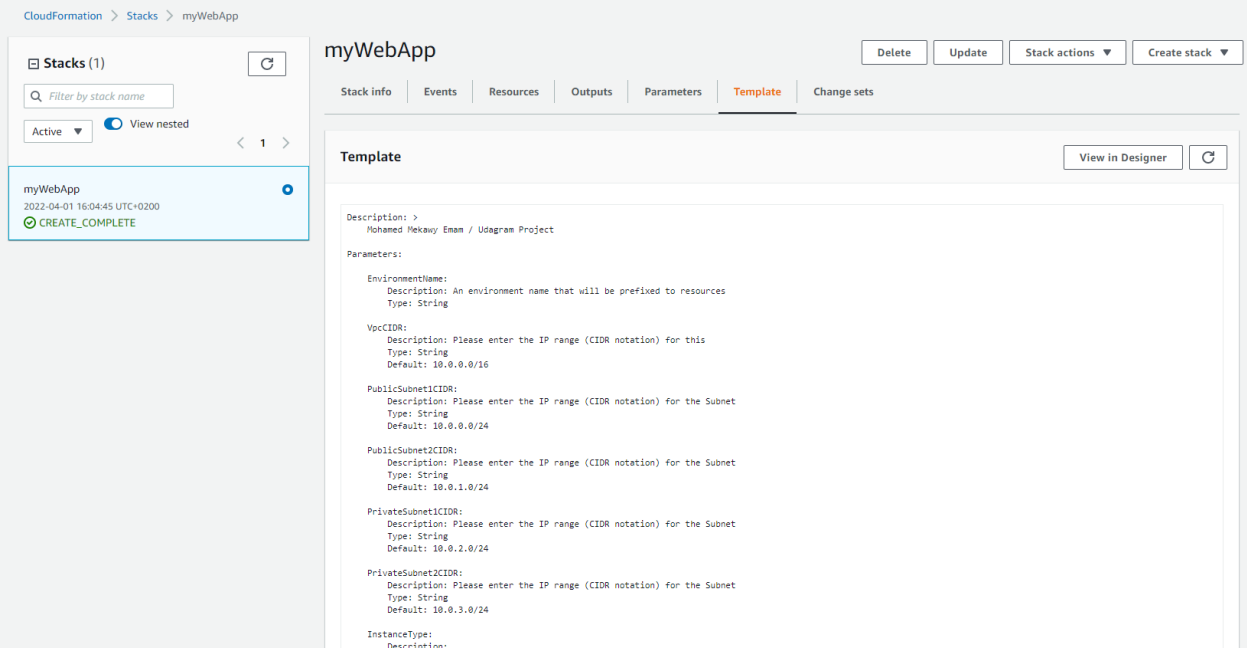
Stack Outputs



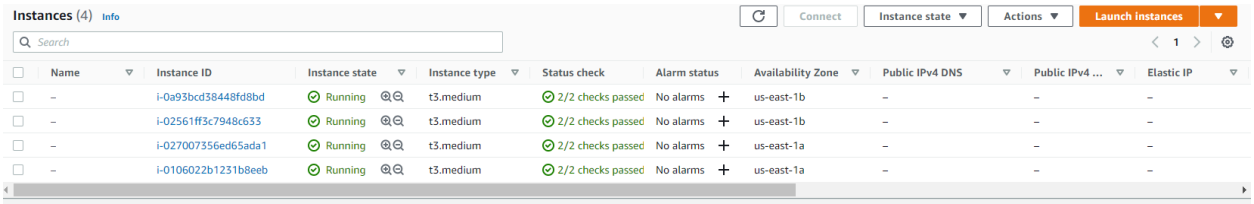
Stack Parameters



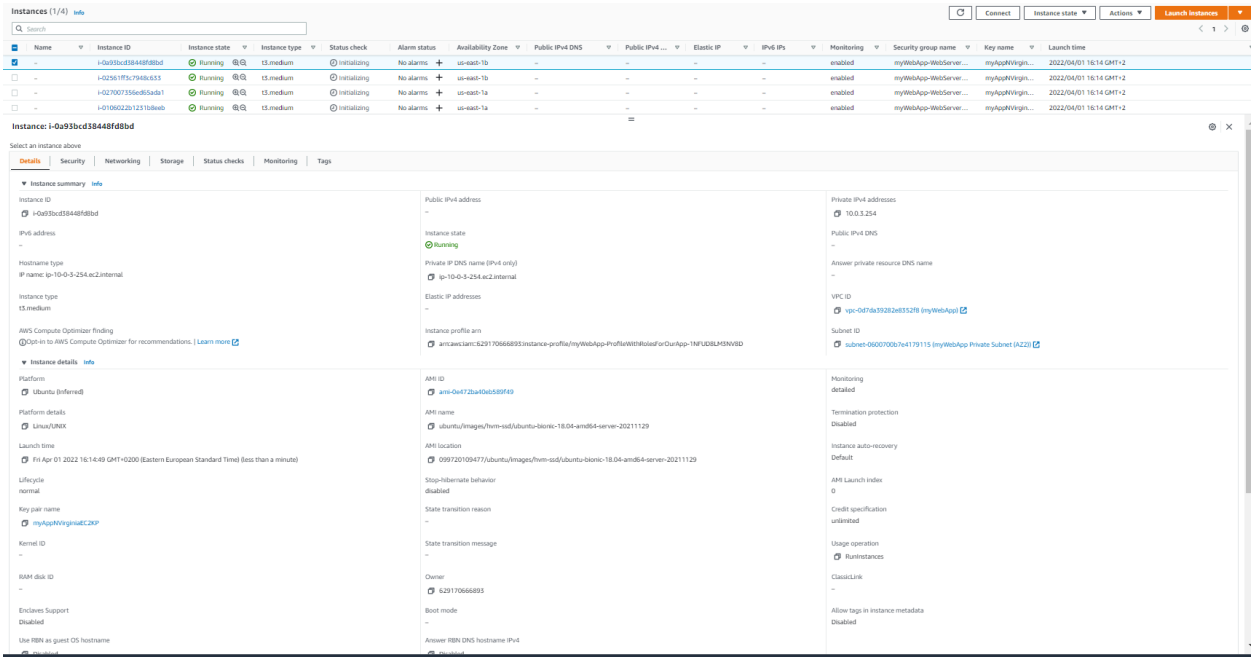
Stack Template



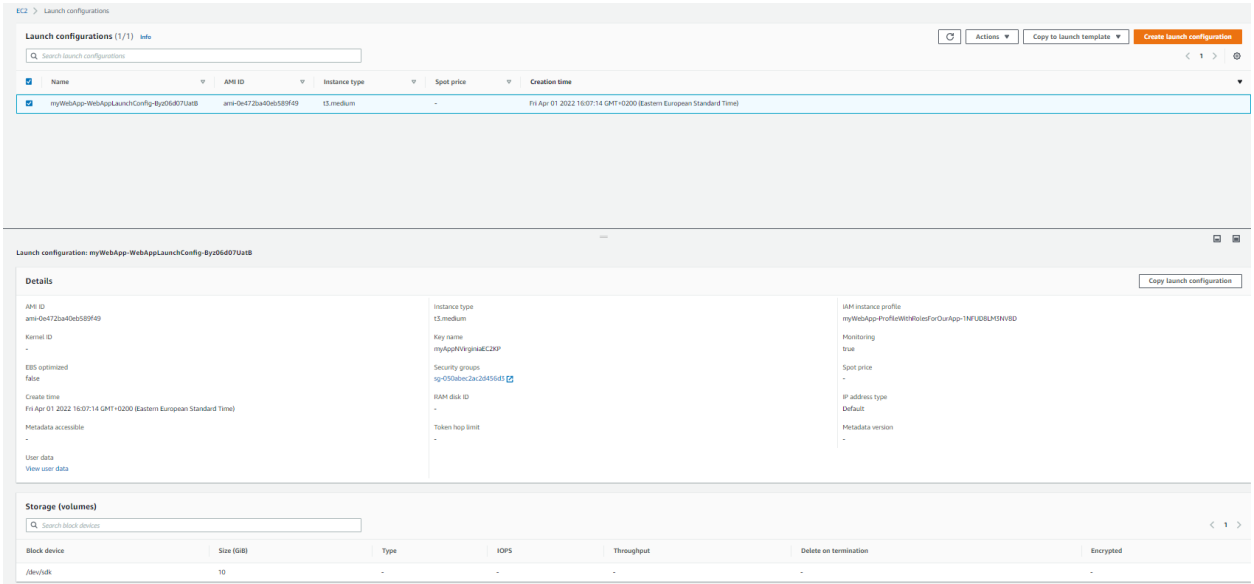
EC2 Instances



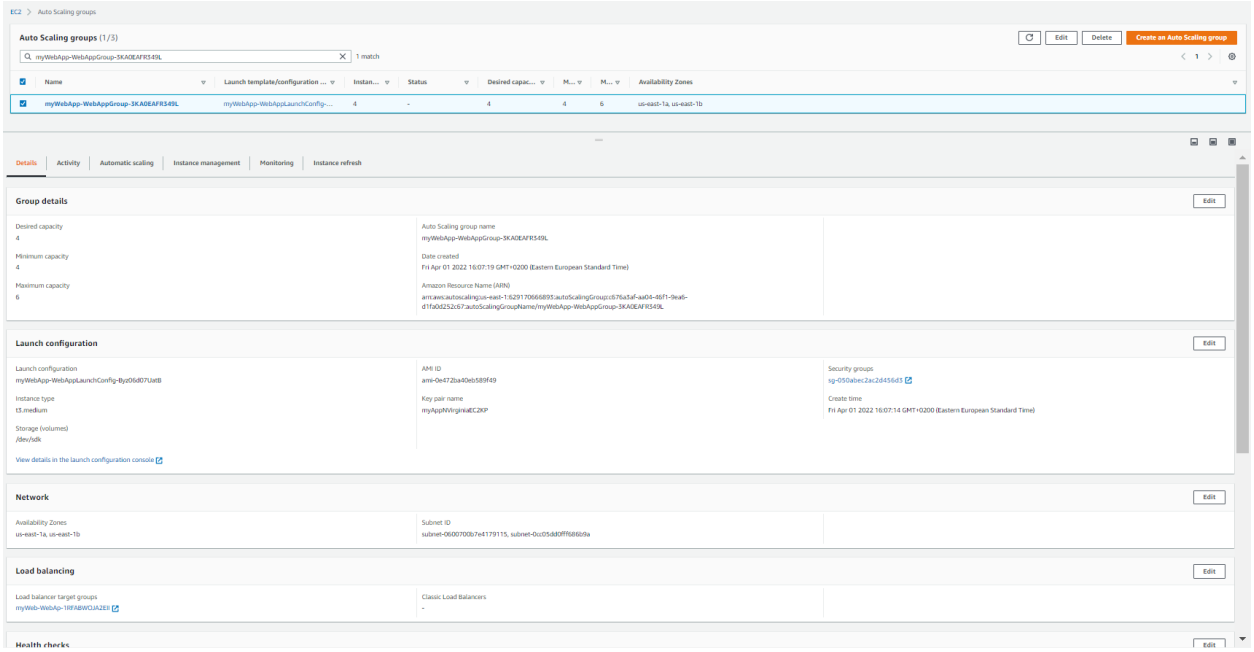
Instance Details



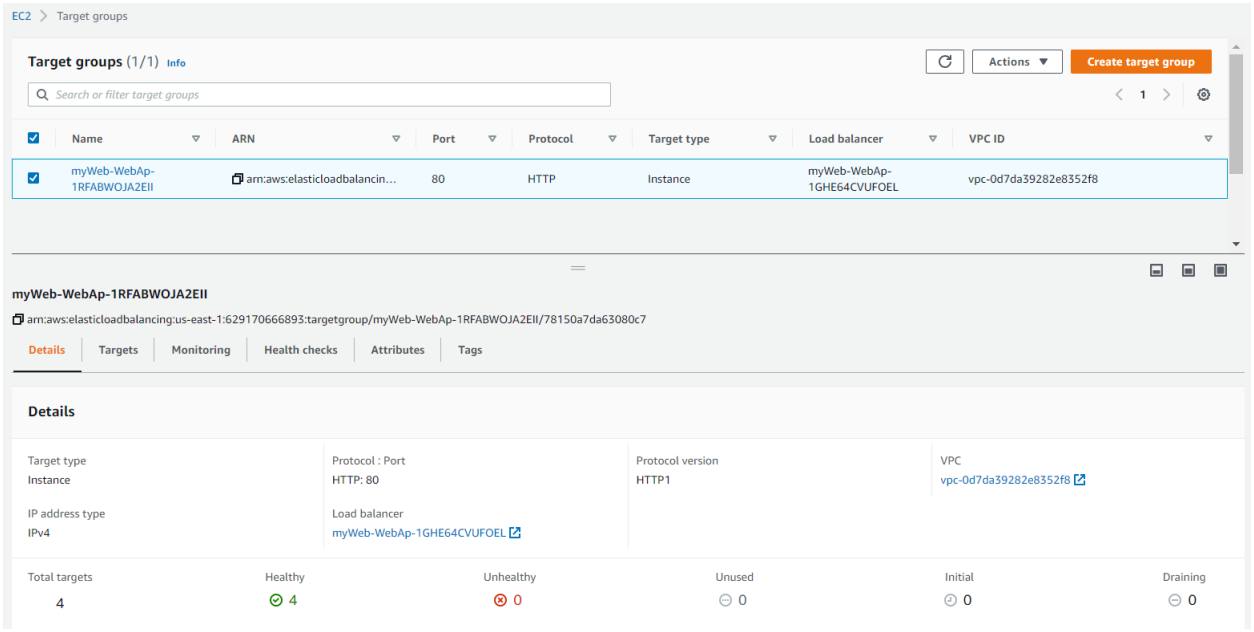
Launch Configuration

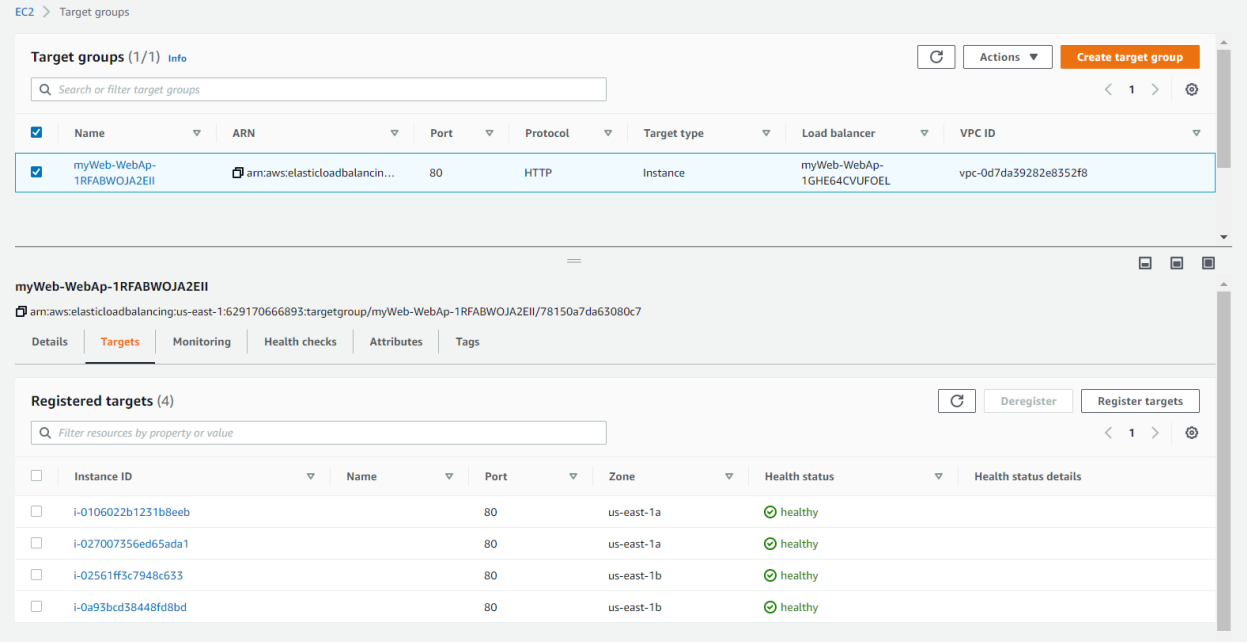


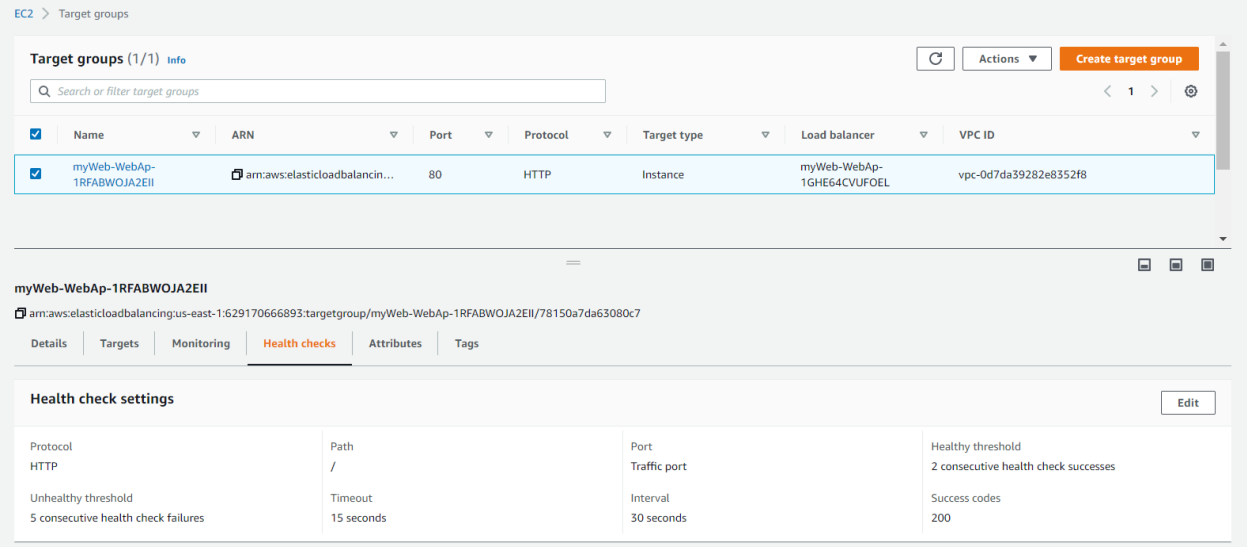
Auto Scaling Group



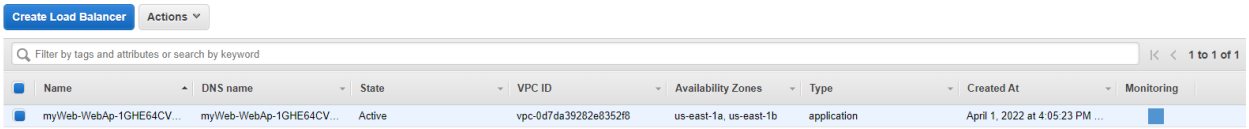
Target Group

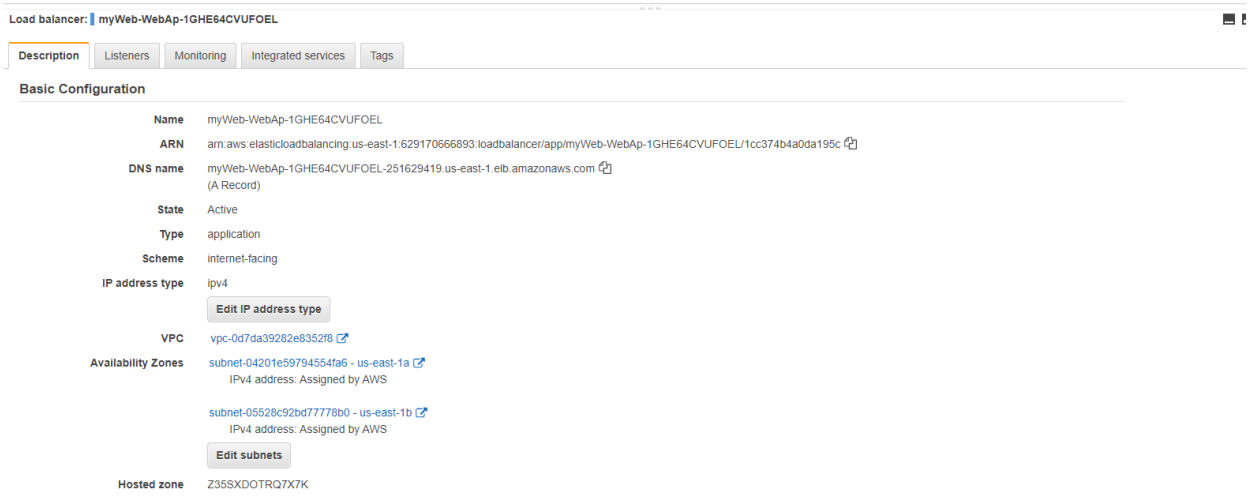


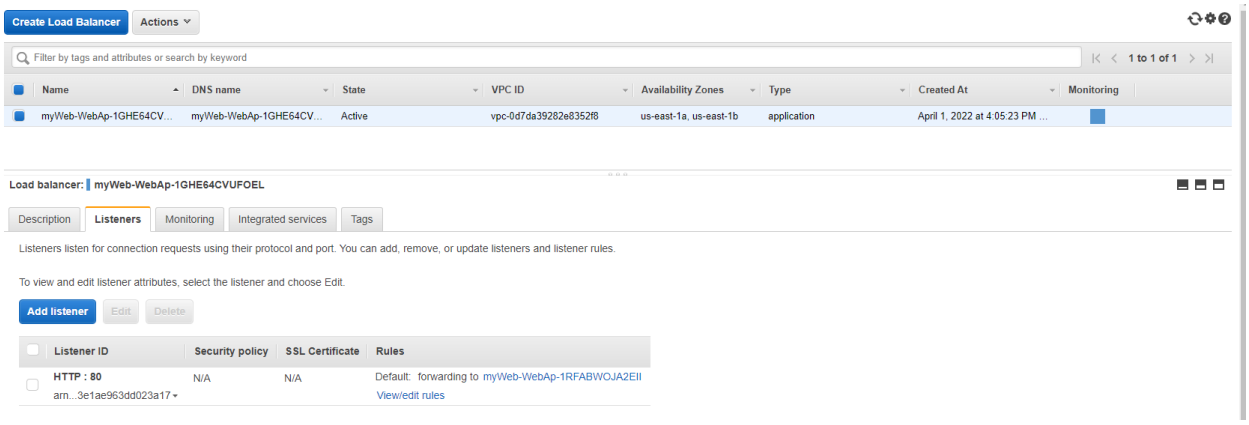

EC2 > Target groups
Target groups (1/1) Info
Actions
Create target group
Search or filter target groups
1
Name
ARN
Port
Protocol
Target type
Load balancer
VPC ID
myWeb-WebAp-1RFABWOJA2EII
arn:aws:elasticloadbalancin...
80
HTTP
Instance
myWeb-WebAp-1GHE64CVUFOEL
vpc-0d7da39282e8352f8
myWeb-WebAp-1RFABWOJA2EII
arn:aws:elasticloadbalancing:us-east-1:629170666893:targetgroup/myWeb-WebAp-1RFABWOJA2EII/78150a7da63080c7
Details
Targets
Monitoring
Health checks
Attributes
Tags
Registered targets (4)
Deregister
Register targets
Filter resources by property or value
Instance ID
Name
Port
Zone
Health status
Health status details
i-0106022b1231b8eeb
80
us-east-1a
healthy
i-027007356ed65ada1
80
us-east-1a
healthy
i-02561ff3c7948c633
80
us-east-1b
healthy
i-0a93bcd38448fd8bd
80
us-east-1b
healthy

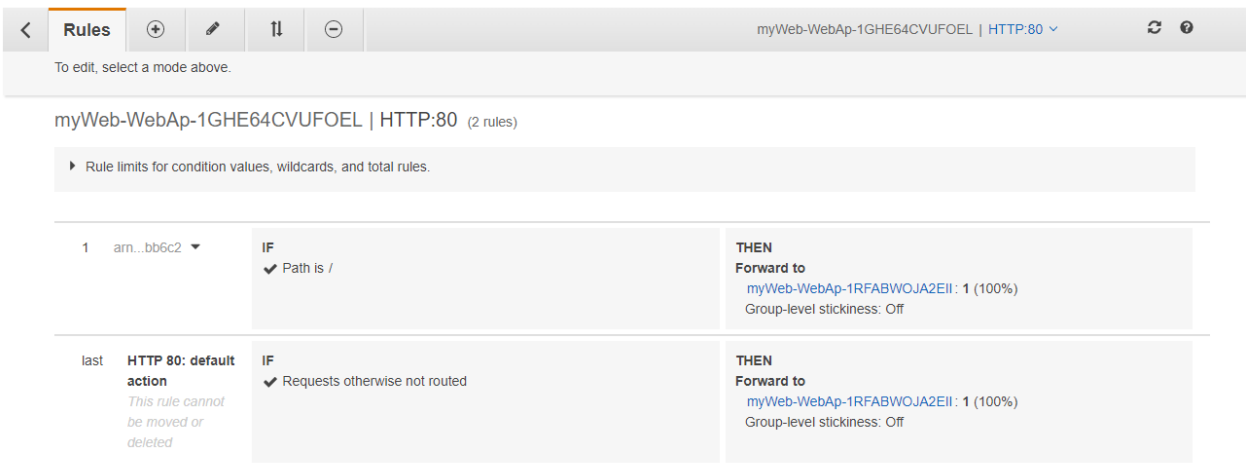

EC2 > Target groups
Target groups (1/1) Info
Actions
Create target group
Search or filter target groups
1
Name
ARN
Port
Protocol
Target type
Load balancer
VPC ID
myWeb-WebAp-1RFABWOJA2EII
arn:aws:elasticloadbalancin...
80
HTTP
Instance
myWeb-WebAp-1GHE64CVUFOEL
vpc-0d7da39282e8352f8
myWeb-WebAp-1RFABWOJA2EII
arn:aws:elasticloadbalancing:us-east-1:629170666893:targetgroup/myWeb-WebAp-1RFABWOJA2EII/78150a7da63080c7
Details
Targets
Monitoring
Health checks
Attributes
Tags
Health check settings
Edit
Protocol
HTTP
Path
/
Port
Traffic port
Healthy threshold
2 consecutive health check successes
Unhealthy threshold
5 consecutive health check failures
Timeout
15 seconds
Interval
30 seconds
Success codes
200

ALB Load Balancer



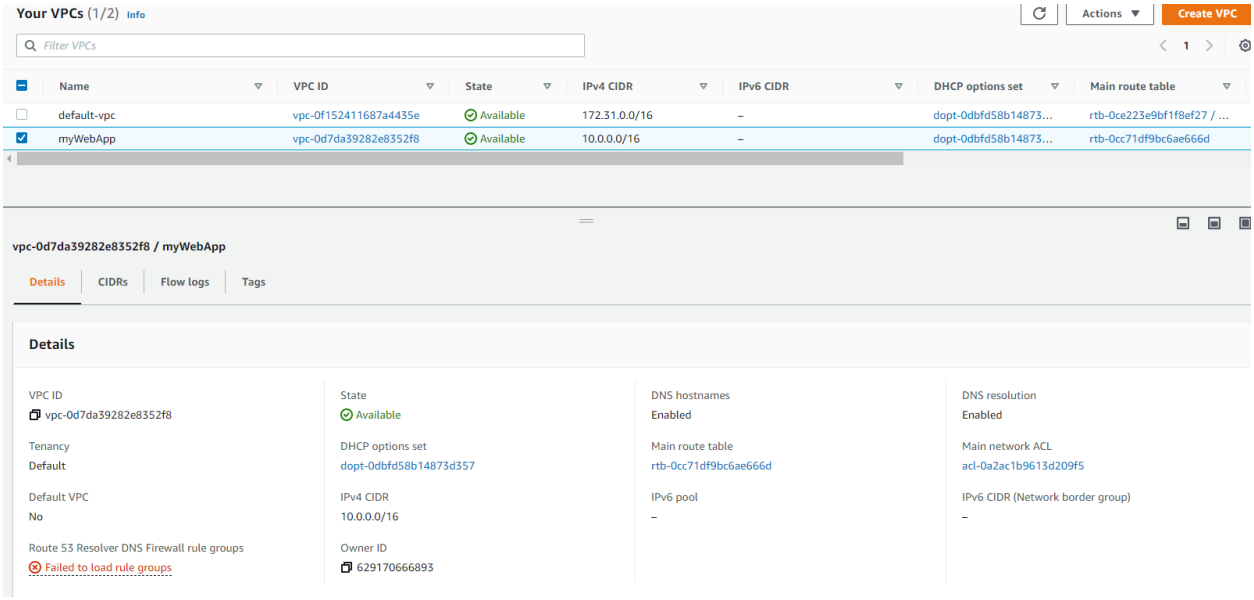






Networking

VPC



Your VPCs (1/2) Info

Actions | Create VPC

Filter VPCs

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Main route table
default-vpc	vpc-0f152411687a4435e	Available	172.31.0.0/16	–	dopt-0dbfd58b14873...	rtb-0ce223e9bf1f8ef27 / ...
myWebApp	vpc-0d7da39282e8352f8	Available	10.0.0.0/16	–	dopt-0dbfd58b14873...	rtb-0cc71df9bc6ae666d

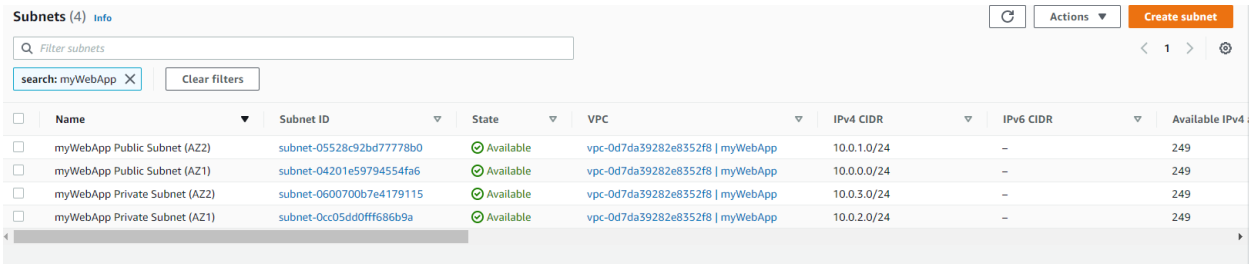
vpc-0d7da39282e8352f8 / myWebApp

Details | CIDRs | Flow logs | Tags

Details

VPC ID vpc-0d7da39282e8352f8	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-0dbfd58b14873d357	Main route table rtb-0cc71df9bc6ae666d	Main network ACL acl-0a2ac1b9613d209f5
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –	IPv6 CIDR (Network border group) –
Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 629170666893		

Subnets



Subnets (4) Info

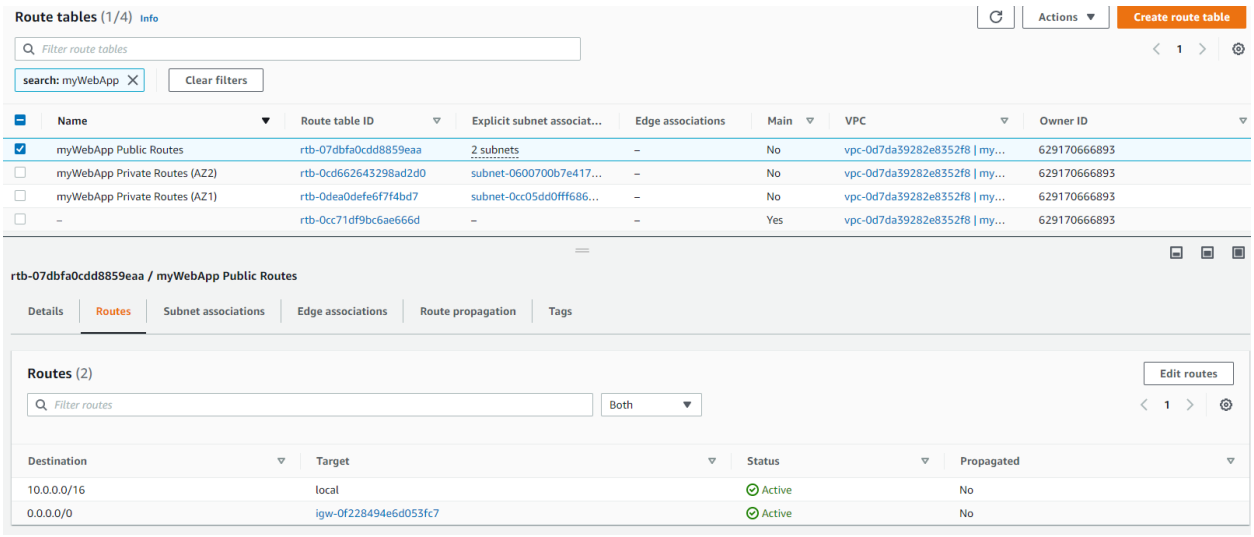
Actions | Create subnet

Filter subnets

search: myWebApp | Clear filters

Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4
myWebApp Public Subnet (AZ2)	subnet-05528c92bd77778b0	Available	vpc-0d7da39282e8352f8 | myWebApp	10.0.1.0/24	–	249
myWebApp Public Subnet (AZ1)	subnet-04201e59794554fa6	Available	vpc-0d7da39282e8352f8 | myWebApp	10.0.0.0/24	–	249
myWebApp Private Subnet (AZ2)	subnet-0600700b7e4179115	Available	vpc-0d7da39282e8352f8 | myWebApp	10.0.3.0/24	–	249
myWebApp Private Subnet (AZ1)	subnet-0cc05dd0fff686b9a	Available	vpc-0d7da39282e8352f8 | myWebApp	10.0.2.0/24	–	249

Route Tables



Route tables (1/4) Info

Actions | Create route table

Filter route tables

search: myWebApp | Clear filters

Name	Route table ID	Explicit subnet associat...	Edge associations	Main	VPC	Owner ID
myWebApp Public Routes	rtb-07dbfa0cdd8859eaa	2 subnets	–	No	vpc-0d7da39282e8352f8 | my...	629170666893
myWebApp Private Routes (AZ2)	rtb-0cd662643298ad2d0	subnet-0600700b7e417...	–	No	vpc-0d7da39282e8352f8 | my...	629170666893
myWebApp Private Routes (AZ1)	rtb-0dea0defe6f7f4bd7	subnet-0cc05dd0fff686...	–	No	vpc-0d7da39282e8352f8 | my...	629170666893
–	rtb-0cc71df9bc6ae666d	–	–	Yes	vpc-0d7da39282e8352f8 | my...	629170666893

rtb-07dbfa0cdd8859eaa / myWebApp Public Routes

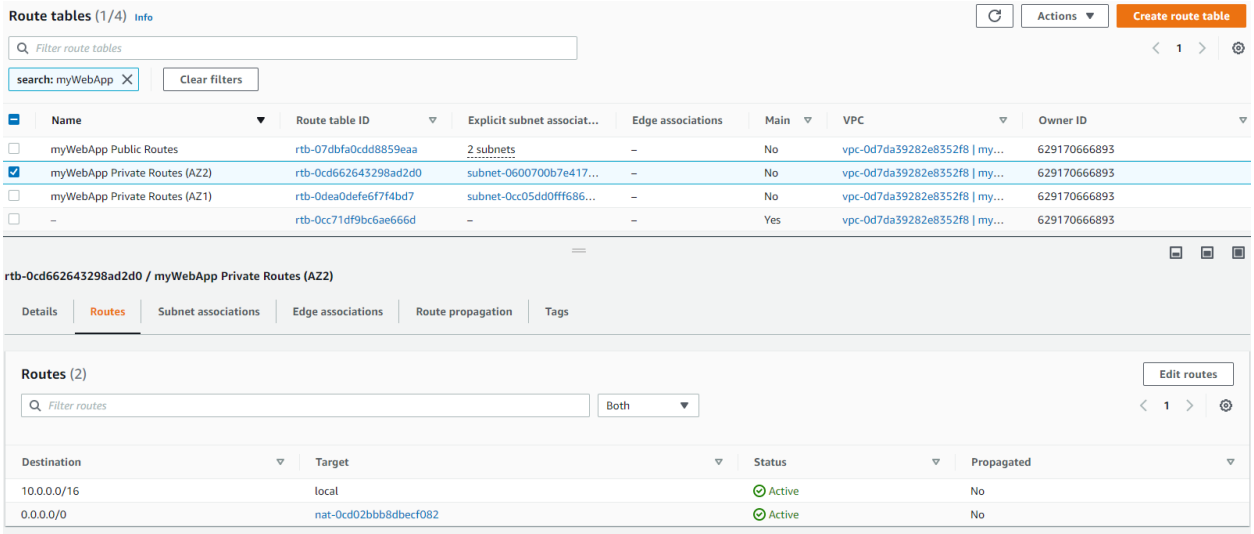
Details | Routes | Subnet associations | Edge associations | Route propagation | Tags

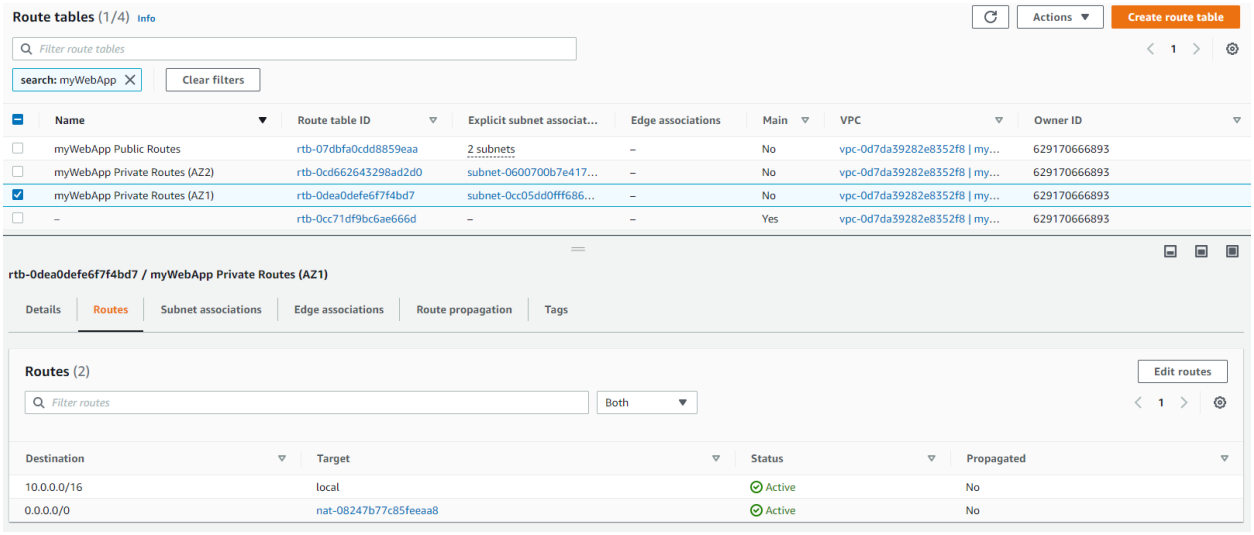
Routes (2)

Edit routes

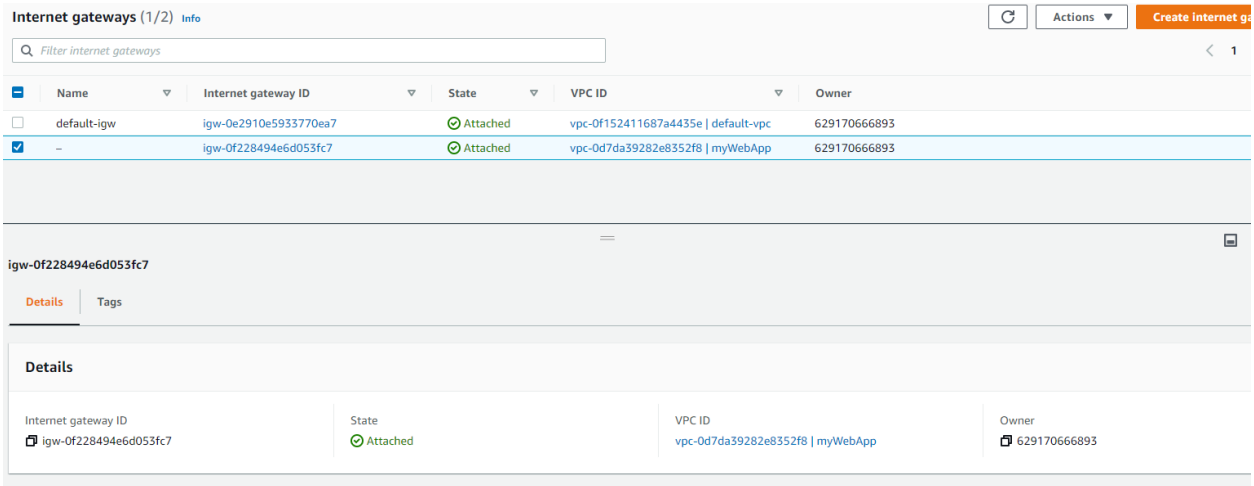
Filter routes | Both

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	igw-0f228494e6d053fc7	Active	No

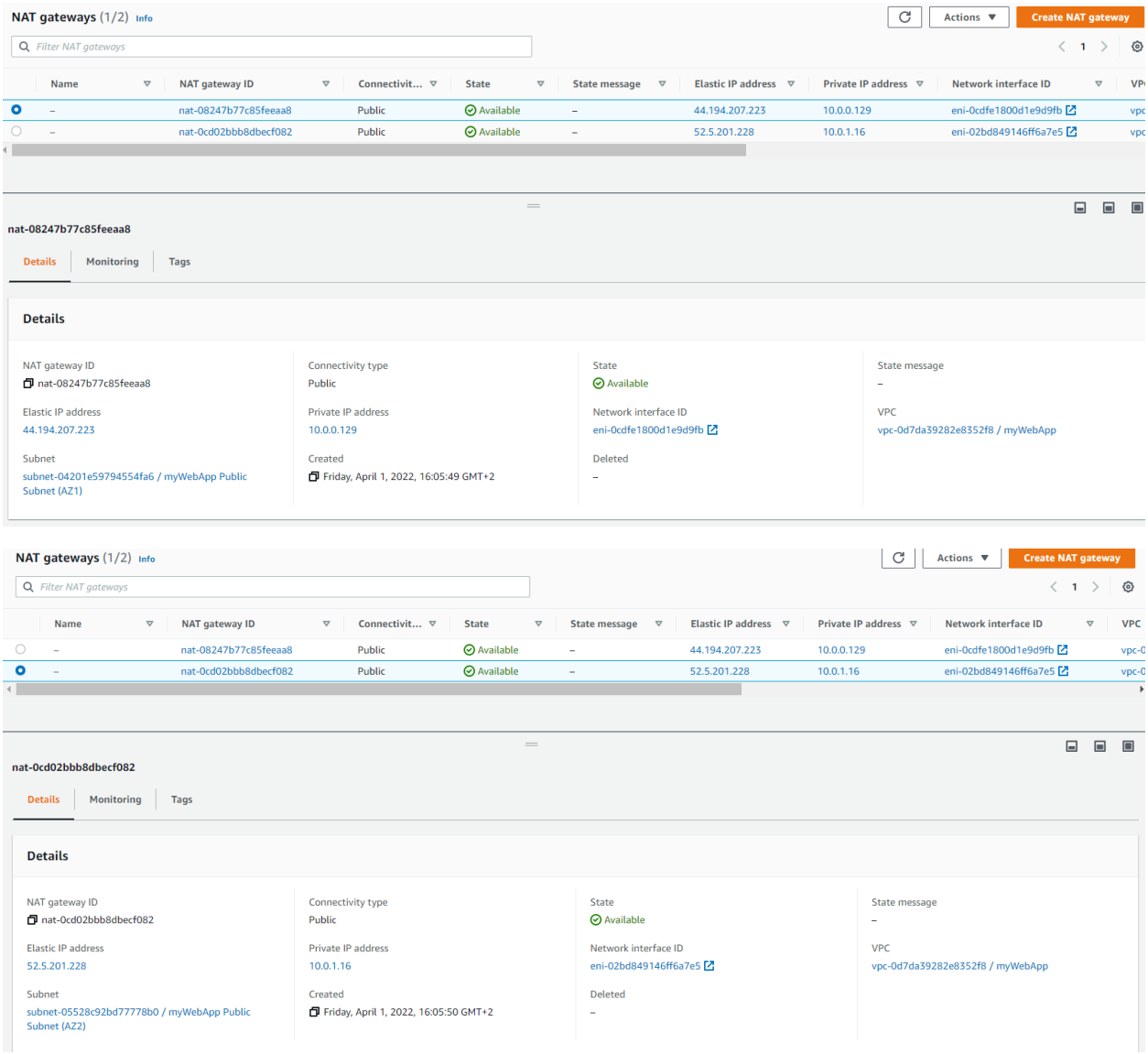




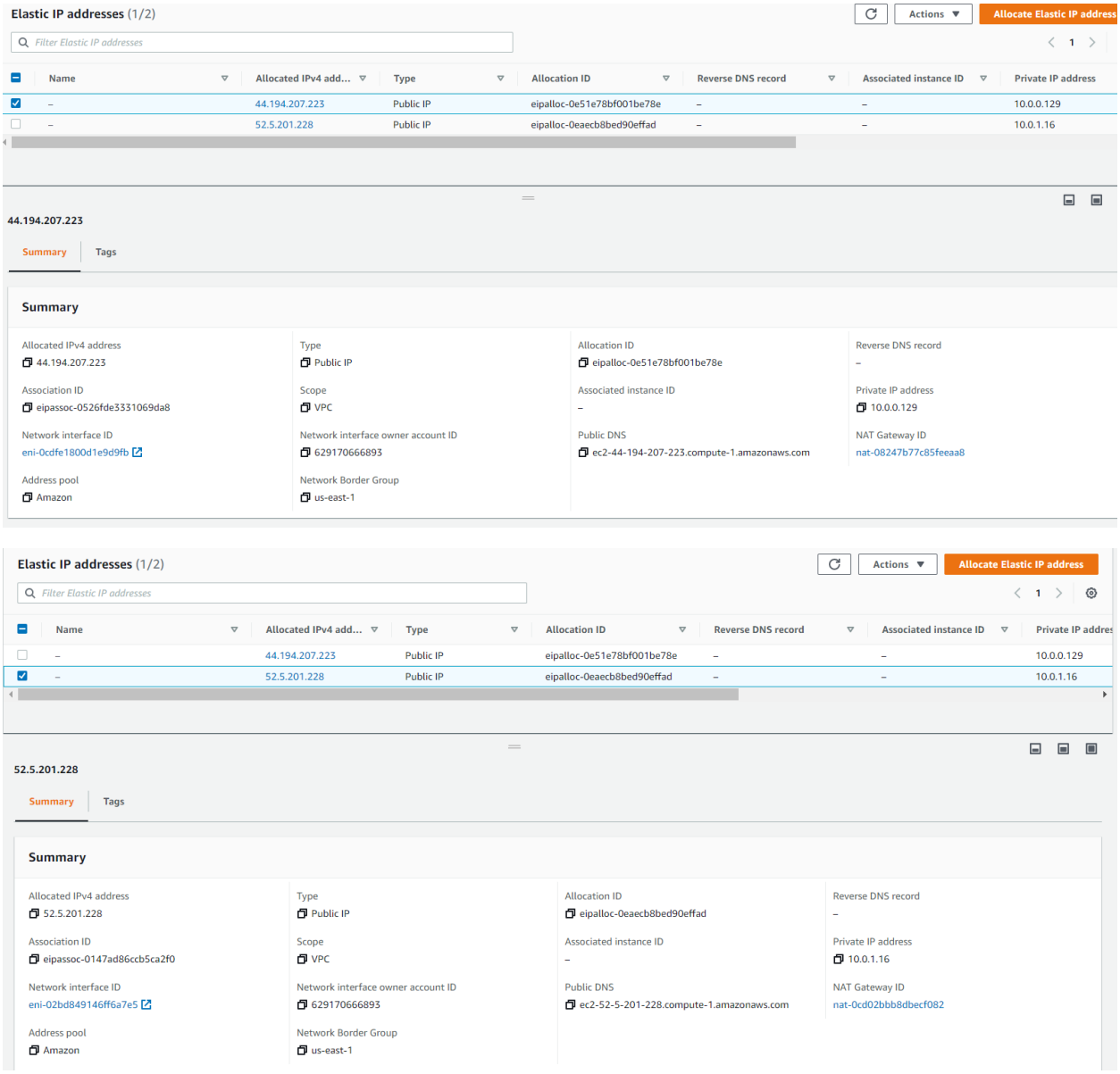
Internet Gateway



NAT Gateways

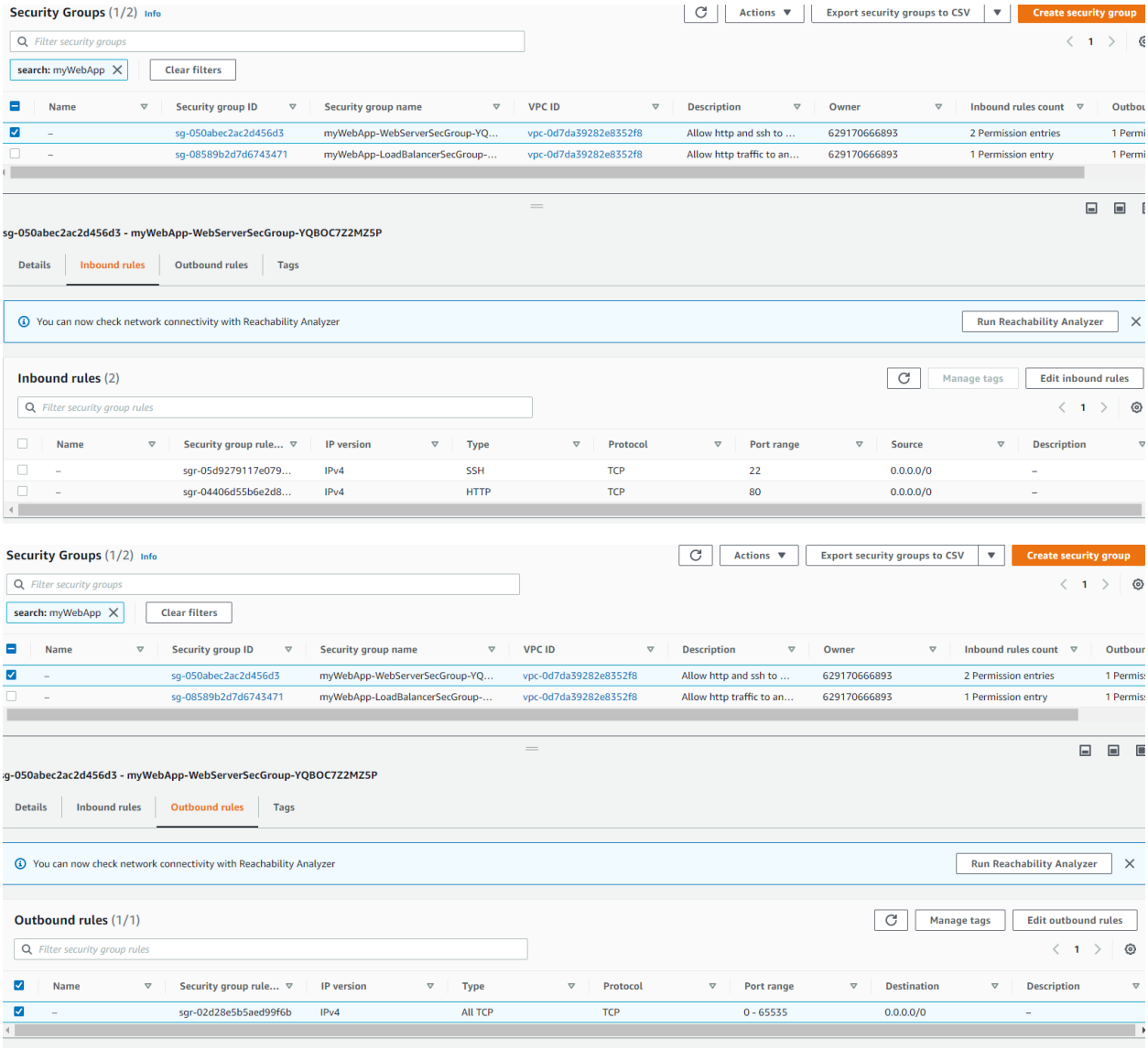


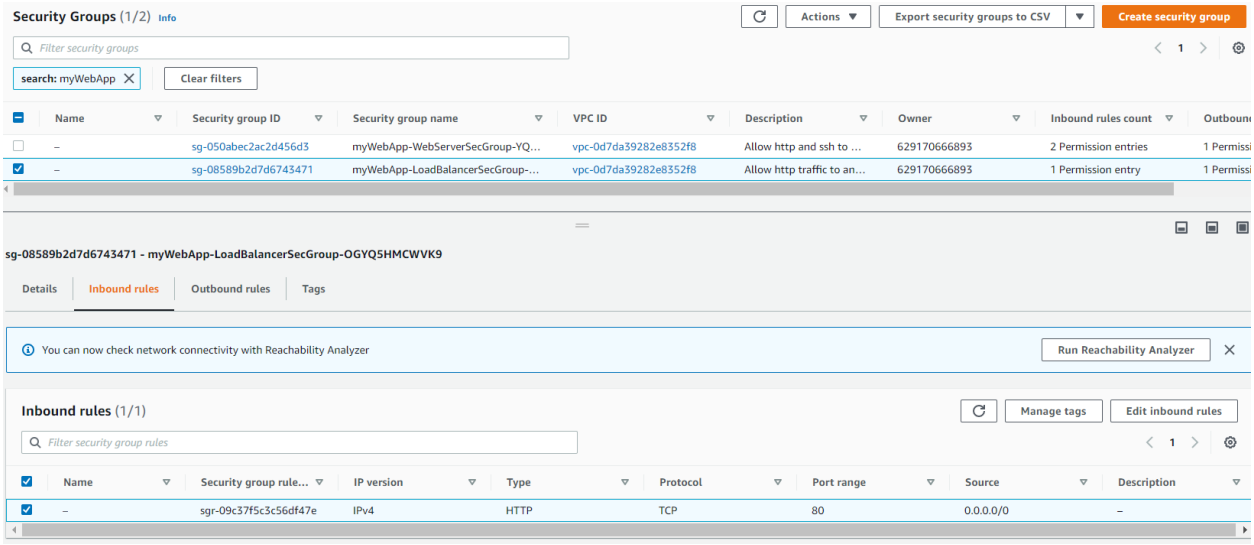
Elastic IPs

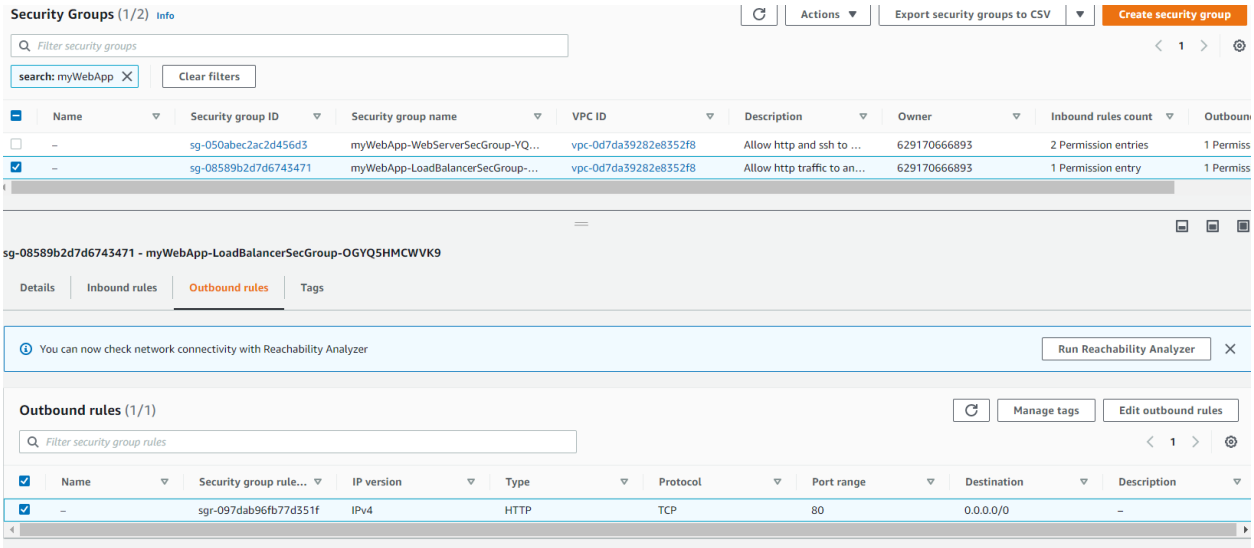

Elastic IP addresses (1/2)
Actions
Allocate Elastic IP address
Filter Elastic IP addresses
1
Name
Allocated IPv4 add...
Type
Allocation ID
Reverse DNS record
Associated instance ID
Private IP address
– 44.194.207.223 Public IP eipalloc-0e51e78bf001be78e – – 10.0.0.129
– 52.5.201.228 Public IP eipalloc-0eaecb8bed90effad – – 10.0.1.16
44.194.207.223
Summary
Tags
Summary
Allocated IPv4 address
44.194.207.223
Type
Public IP
Allocation ID
eipalloc-0e51e78bf001be78e
Reverse DNS record
–
Association ID
eipassoc-0526fde3331069da8
Scope
VPC
Associated instance ID
–
Private IP address
10.0.0.129
Network interface ID
eni-0cdfe1800d1e9d9fb
Network interface owner account ID
629170666893
Public DNS
ec2-44-194-207-223.compute-1.amazonaws.com
NAT Gateway ID
nat-08247b77c85feeaa8
Address pool
Amazon
Network Border Group
us-east-1

Elastic IP addresses (1/2)
Actions
Allocate Elastic IP address
Filter Elastic IP addresses
1
Name
Allocated IPv4 add...
Type
Allocation ID
Reverse DNS record
Associated instance ID
Private IP addres
– 44.194.207.223 Public IP eipalloc-0e51e78bf001be78e – – 10.0.0.129
– 52.5.201.228 Public IP eipalloc-0eaecb8bed90effad – – 10.0.1.16
52.5.201.228
Summary
Tags
Summary
Allocated IPv4 address
52.5.201.228
Type
Public IP
Allocation ID
eipalloc-0eaecb8bed90effad
Reverse DNS record
–
Association ID
eipassoc-0147ad86ccb5ca2f0
Scope
VPC
Associated instance ID
–
Private IP address
10.0.1.16
Network interface ID
eni-02bd849146ff6a7e5
Network interface owner account ID
629170666893
Public DNS
ec2-52-5-201-228.compute-1.amazonaws.com
NAT Gateway ID
nat-0cd02bbb8dbecf082
Address pool
Amazon
Network Border Group
us-east-1

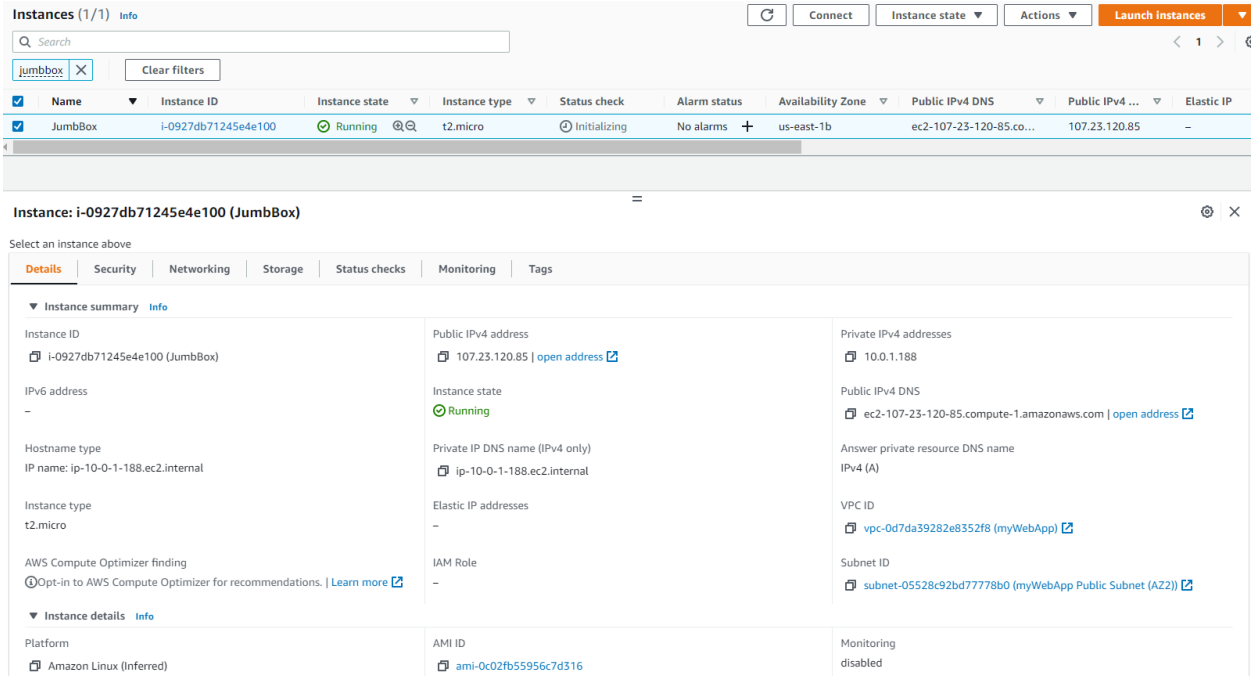
Security Groups

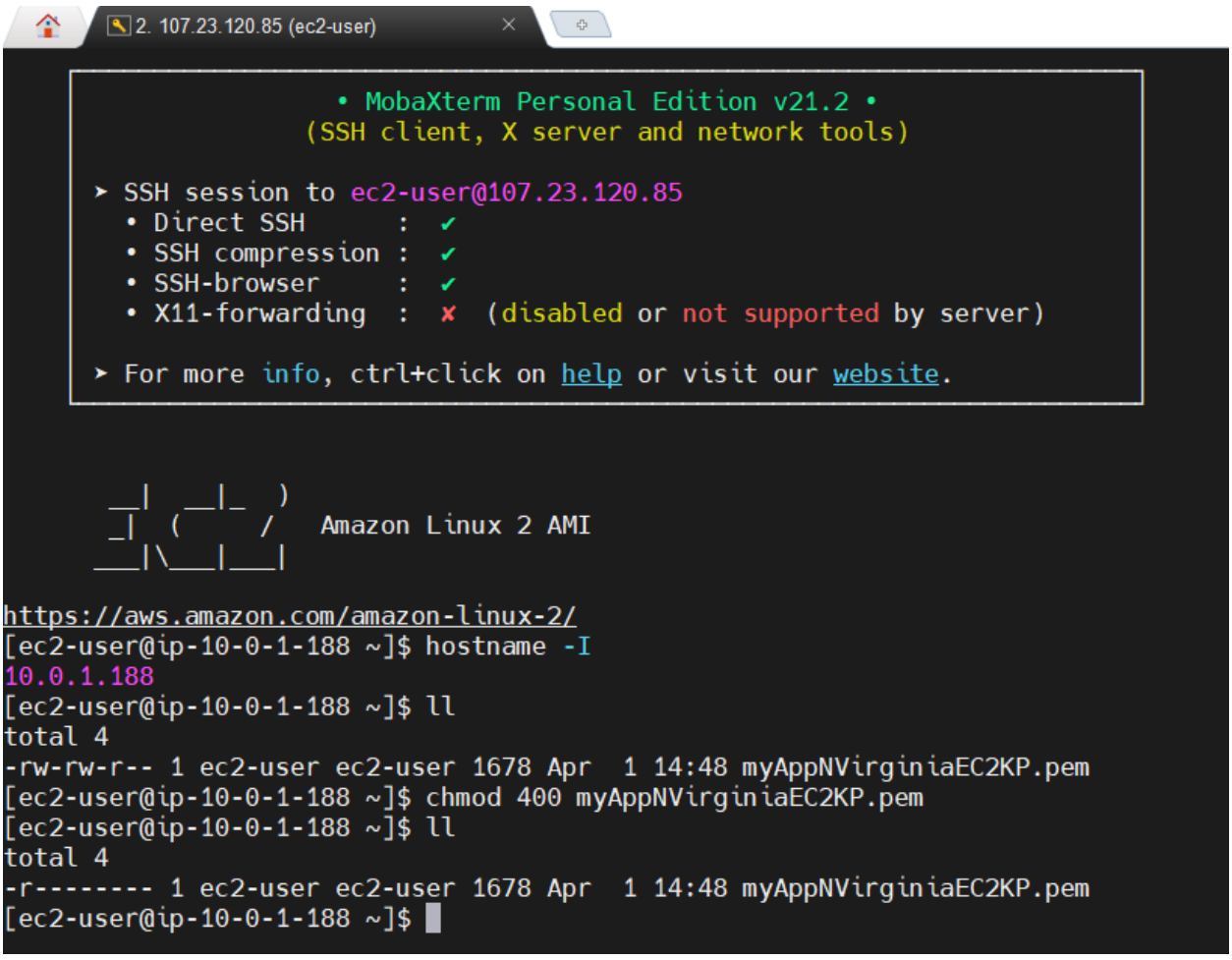


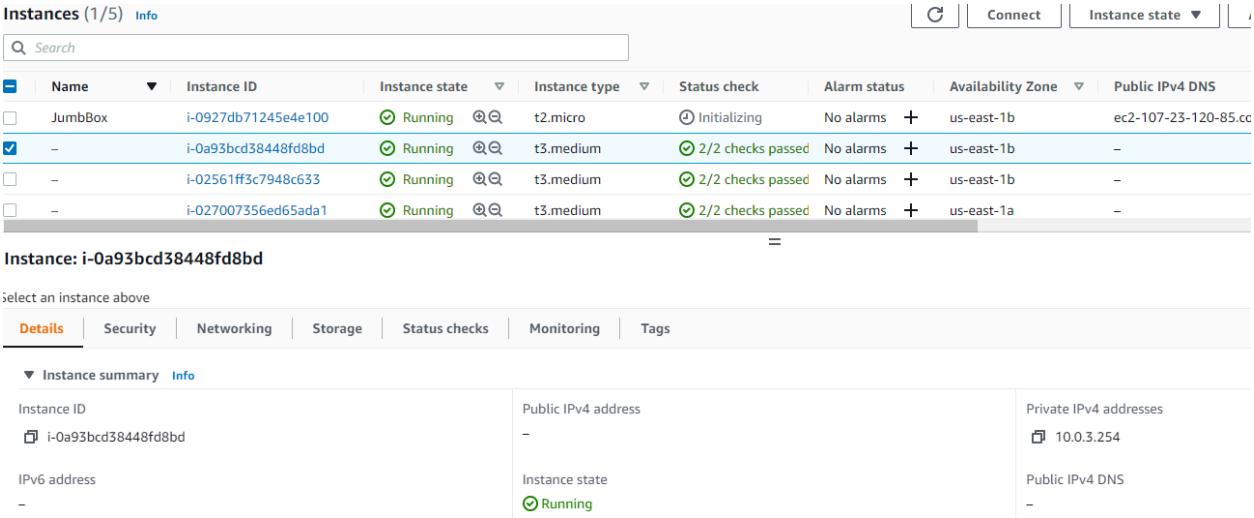

Security Groups (1/2) Info
Actions
Export security groups to CSV
Create security group
Filter security groups
search: myWebApp
Clear filters
Name
Security group ID
Security group name
VPC ID
Description
Owner
Inbound rules count
sg-050abec2ac2d456d3
myWebApp-WebServerSecGroup-YQ...
vpc-0d7da39282e8352f8
Allow http and ssh to ...
629170666893
2 Permission entries
sg-08589b2d7d6743471
myWebApp-LoadBalancerSecGroup-...
Allow http traffic to an...
1 Permission entry
sg-08589b2d7d6743471 - myWebApp-LoadBalancerSecGroup-OGYQ5HMCWVK9
Details
Inbound rules
Outbound rules
Tags
You can now check network connectivity with Reachability Analyzer
Run Reachability Analyzer
Inbound rules (1/1)
Manage tags
Edit inbound rules
Filter security group rules
Security group rule...
IP version
Type
Protocol
Port range
Source
sgr-09c37f5c3c56df47e
IPv4
HTTP
TCP
80
0.0.0.0/0

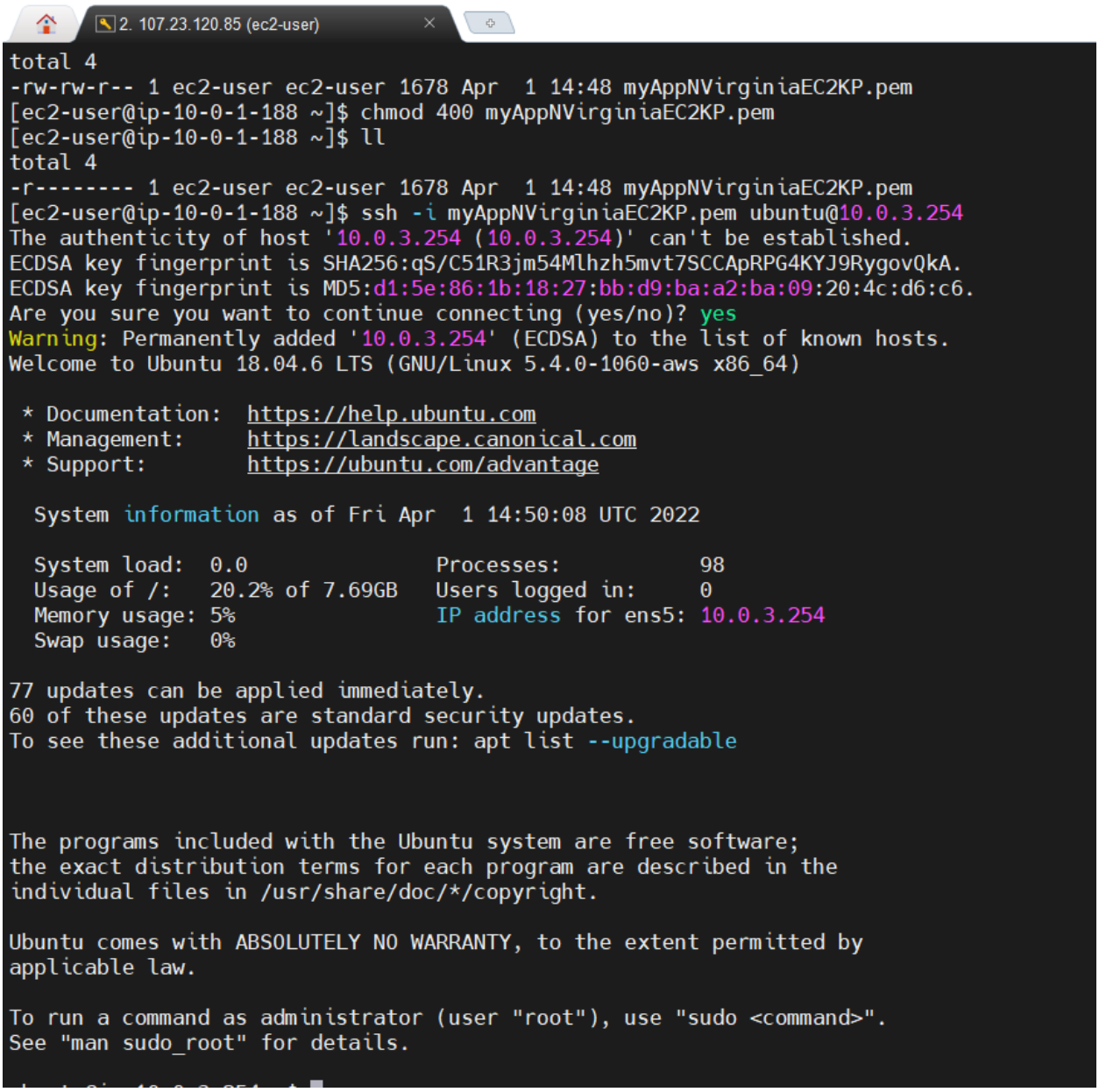

Security Groups (1/2) Info
Actions
Export security groups to CSV
Create security group
Filter security groups
search: myWebApp
Clear filters
Name
Security group ID
Security group name
VPC ID
Description
Owner
Inbound rules count
sg-050abec2ac2d456d3
myWebApp-WebServerSecGroup-YQ...
vpc-0d7da39282e8352f8
Allow http and ssh to ...
629170666893
2 Permission entries
sg-08589b2d7d6743471
myWebApp-LoadBalancerSecGroup-...
Allow http traffic to an...
1 Permission entry
sg-08589b2d7d6743471 - myWebApp-LoadBalancerSecGroup-OGYQ5HMCWVK9
Details
Inbound rules
Outbound rules
Tags
You can now check network connectivity with Reachability Analyzer
Run Reachability Analyzer
Outbound rules (1/1)
Manage tags
Edit outbound rules
Filter security group rules
Security group rule...
IP version
Type
Protocol
Port range
Destination
sgr-097dab96fb77d351f
IPv4
HTTP
TCP
80
0.0.0.0/0

Bastion Host




2. 107.23.120.85 (ec2-user)
• MobaXterm Personal Edition v21.2 •
(SSH client, X server and network tools)
➤ SSH session to ec2-user@107.23.120.85
• Direct SSH : ✔
• SSH compression : ✔
• SSH-browser : ✔
• X11-forwarding : ✘ (disabled or not supported by server)
➤ For more info, ctrl+click on help or visit our website.
Amazon Linux 2 AMI
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-188 ~]$ hostname -I
10.0.1.188
[ec2-user@ip-10-0-1-188 ~]$ ll
total 4
-rw-rw-r-- 1 ec2-user ec2-user 1678 Apr 1 14:48 myAppNVirginiaEC2KP.pem
[ec2-user@ip-10-0-1-188 ~]$ chmod 400 myAppNVirginiaEC2KP.pem
[ec2-user@ip-10-0-1-188 ~]$ ll
total 4
-r-------- 1 ec2-user ec2-user 1678 Apr 1 14:48 myAppNVirginiaEC2KP.pem
[ec2-user@ip-10-0-1-188 ~]$


Instances (1/5) Info
Connect
Instance state
Search
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
JumbBox i-0927db71245e4e100 Running t2.micro Initializing No alarms us-east-1b ec2-107-23-120-85.co
– i-0a93bcd38448fd8bd Running t3.medium 2/2 checks passed No alarms us-east-1b –
– i-02561ff3c7948c633 Running t3.medium 2/2 checks passed No alarms us-east-1b –
– i-027007356ed65ada1 Running t3.medium 2/2 checks passed No alarms us-east-1a –
Instance: i-0a93bcd38448fd8bd
Select an instance above
Details
Security
Networking
Storage
Status checks
Monitoring
Tags
Instance summary Info
Instance ID
i-0a93bcd38448fd8bd
Public IPv4 address
–
Private IPv4 addresses
10.0.3.254
IPv6 address
–
Instance state
Running
Public IPv4 DNS
–


2. 107.23.120.85 (ec2-user)
total 4
-rw-rw-r-- 1 ec2-user ec2-user 1678 Apr 1 14:48 myAppNVirginiaEC2KP.pem
[ec2-user@ip-10-0-1-188 ~]$ chmod 400 myAppNVirginiaEC2KP.pem
[ec2-user@ip-10-0-1-188 ~]$ ll
total 4
-r-------- 1 ec2-user ec2-user 1678 Apr 1 14:48 myAppNVirginiaEC2KP.pem
[ec2-user@ip-10-0-1-188 ~]$ ssh -i myAppNVirginiaEC2KP.pem ubuntu@10.0.3.254
The authenticity of host '10.0.3.254 (10.0.3.254)' can't be established.
ECDSA key fingerprint is SHA256:qS/C51R3jm54Mlhzh5mvt7SCCApRPG4KYJ9RygovQkA.
ECDSA key fingerprint is MD5:d1:5e:86:1b:18:27:bb:d9:ba:a2:ba:09:20:4c:d6:c6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.0.3.254' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 5.4.0-1060-aws x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
System information as of Fri Apr 1 14:50:08 UTC 2022
System load: 0.0 Processes: 98
Usage of /: 20.2% of 7.69GB Users logged in: 0
Memory usage: 5% IP address for ens5: 10.0.3.254
Swap usage: 0%
77 updates can be applied immediately.
60 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

```
ubuntu@ip-10-0-3-254:~$ ll /var/www/html/
total 68
drwxr-xr-x 2 root root  4096 Apr  1 14:08 ./
drwxr-xr-x 3 root root  4096 Apr  1 14:08 ../
-rw-r--r-- 1 root root  1075 Apr  1  2022 index.html
-rw-r--r-- 1 root root 25335 Nov  4 14:03 me.jpg
-rw-r--r-- 1 root root 26201 Apr  1 13:21 myApp.zip
ubuntu@ip-10-0-3-254:~$ systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
  Drop-In: /lib/systemd/system/apache2.service.d
           └─apache2-systemd.conf
   Active: active (running) since Fri 2022-04-01 14:15:09 UTC; 36min ago
  Process: 775 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 869 (apache2)
    Tasks: 55 (limit: 4617)
   CGroup: /system.slice/apache2.service
           ├─869 /usr/sbin/apache2 -k start
           ├─870 /usr/sbin/apache2 -k start
           └─871 /usr/sbin/apache2 -k start

Apr 01 14:15:09 ip-10-0-3-254 systemd[1]: Starting The Apache HTTP Server...
Apr 01 14:15:09 ip-10-0-3-254 systemd[1]: Started The Apache HTTP Server.
ubuntu@ip-10-0-3-254:~$
```

Final Output from ALB

Link: http://myweb-webap-1ghe64cvufoel-251629419.us-east-1.elb.amazonaws.com/