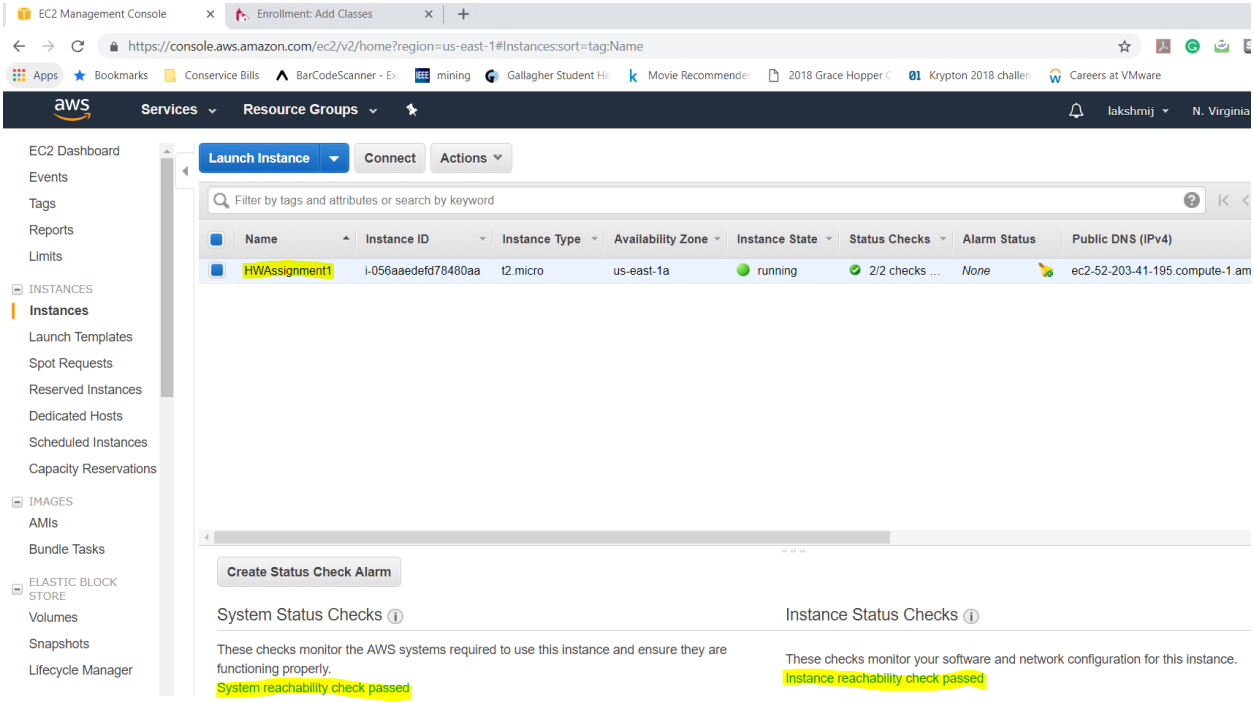
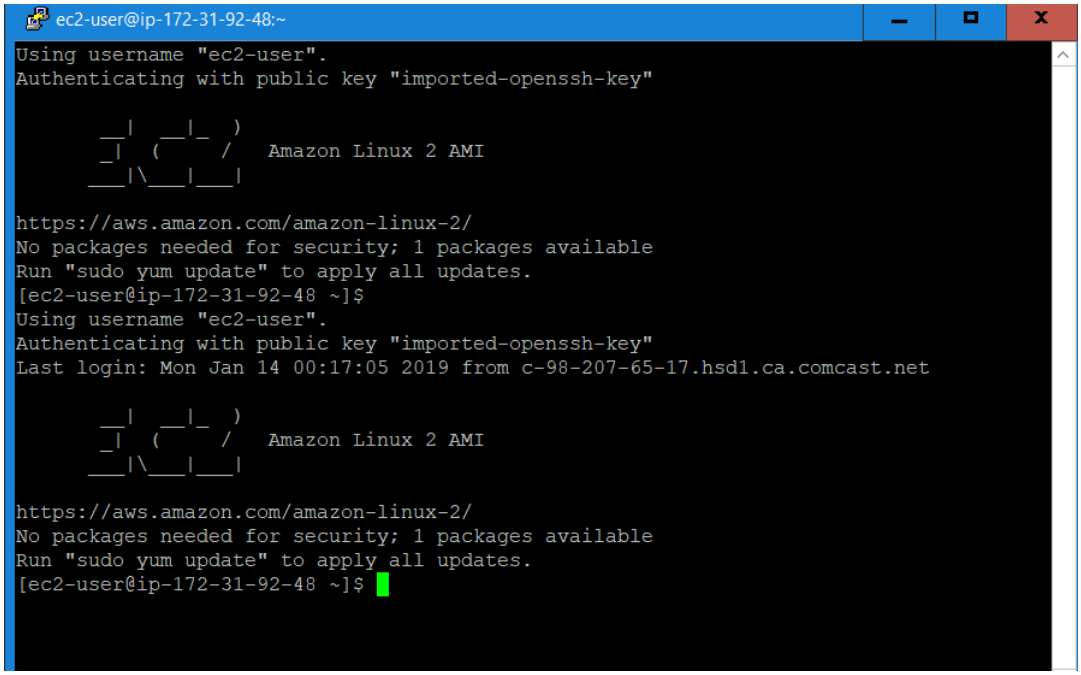
B. Install a LAMPs web server

Steps:

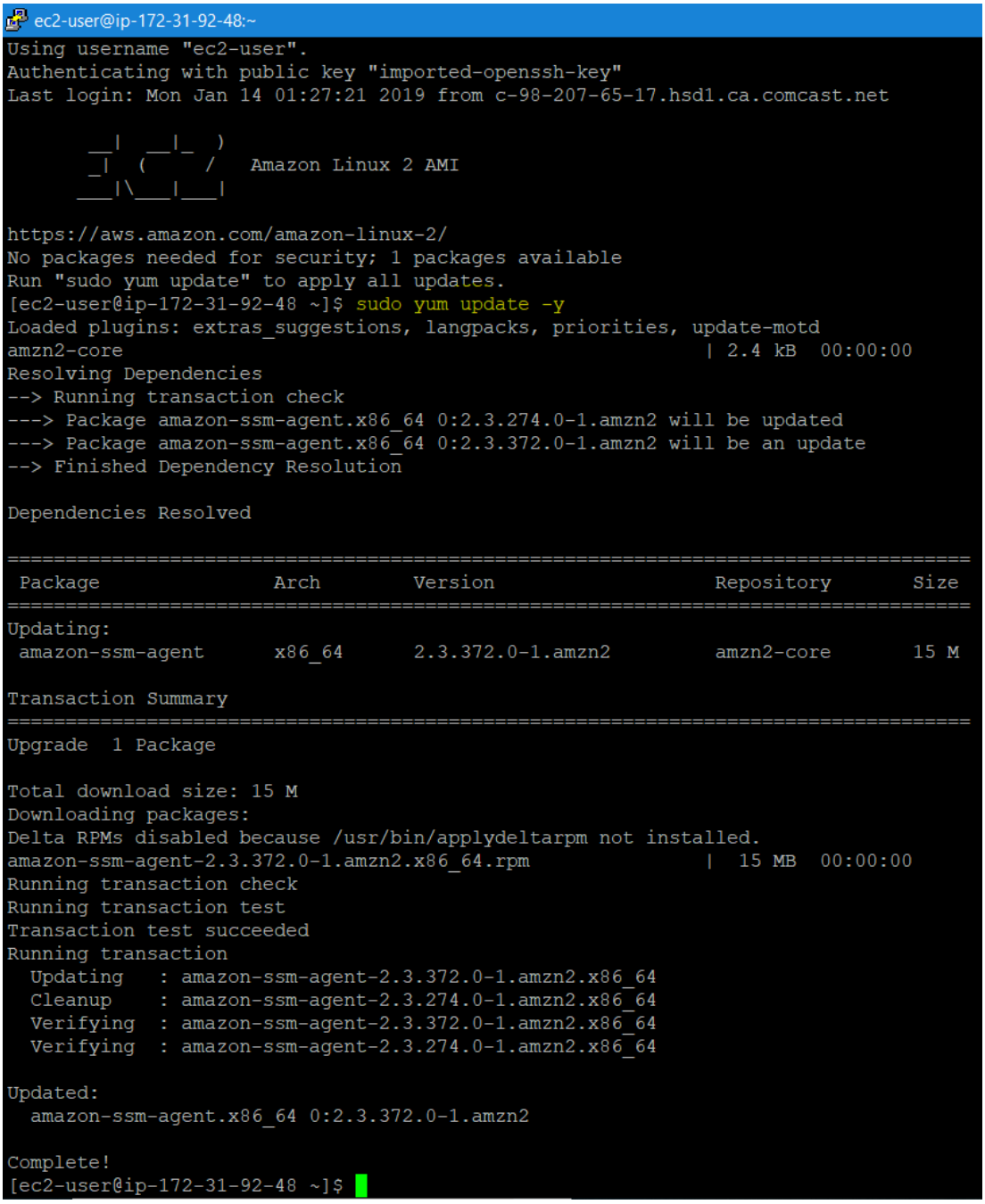
1) Create an instance as explained in http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EC2_GetStarted.html



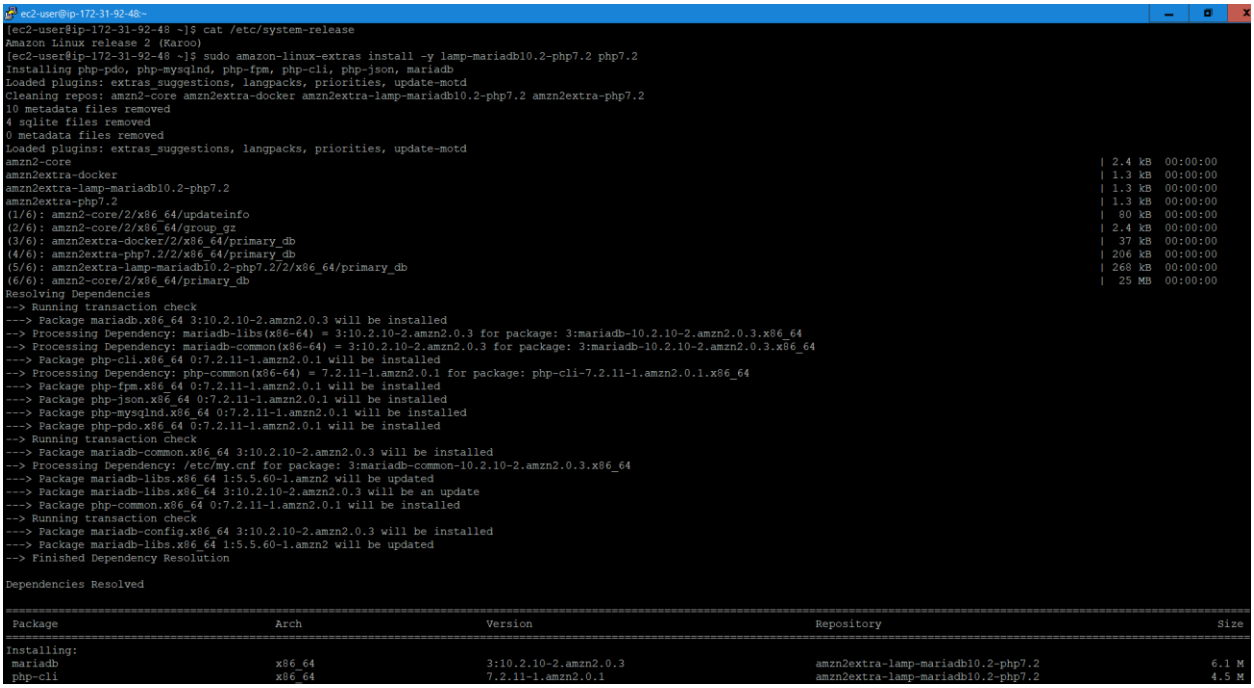
2) Connect via putty

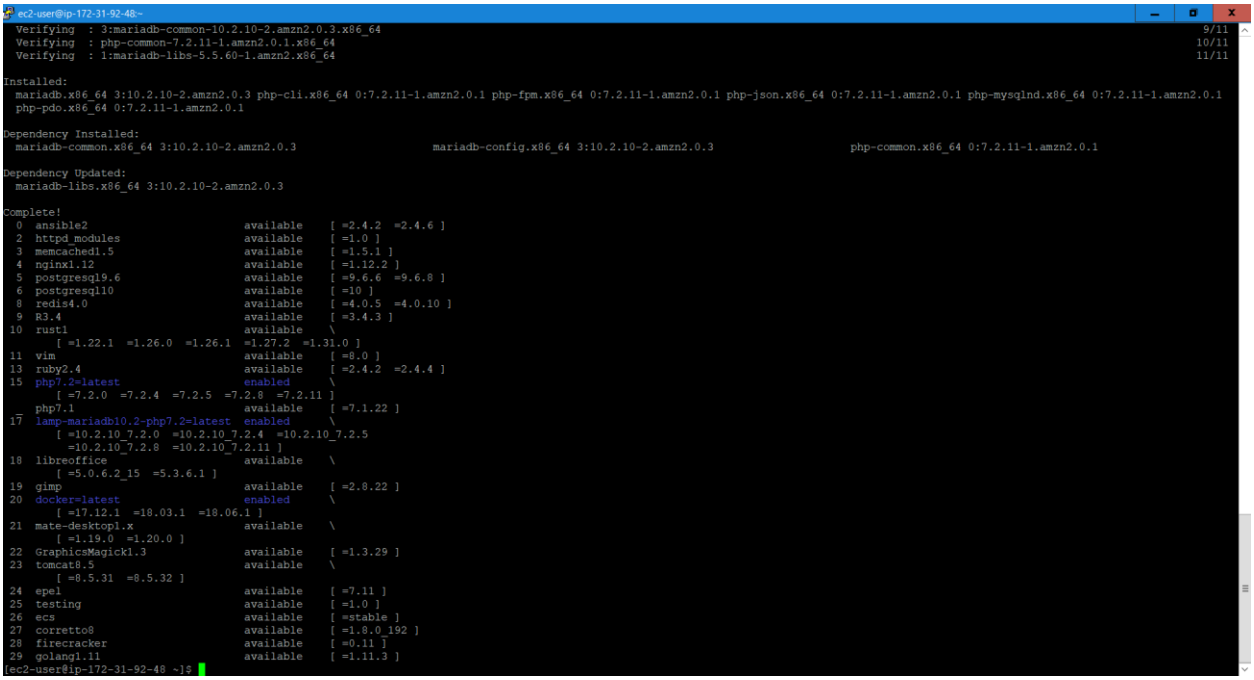


3) Perform a quick software update on your instance using **sudo yum update -y**

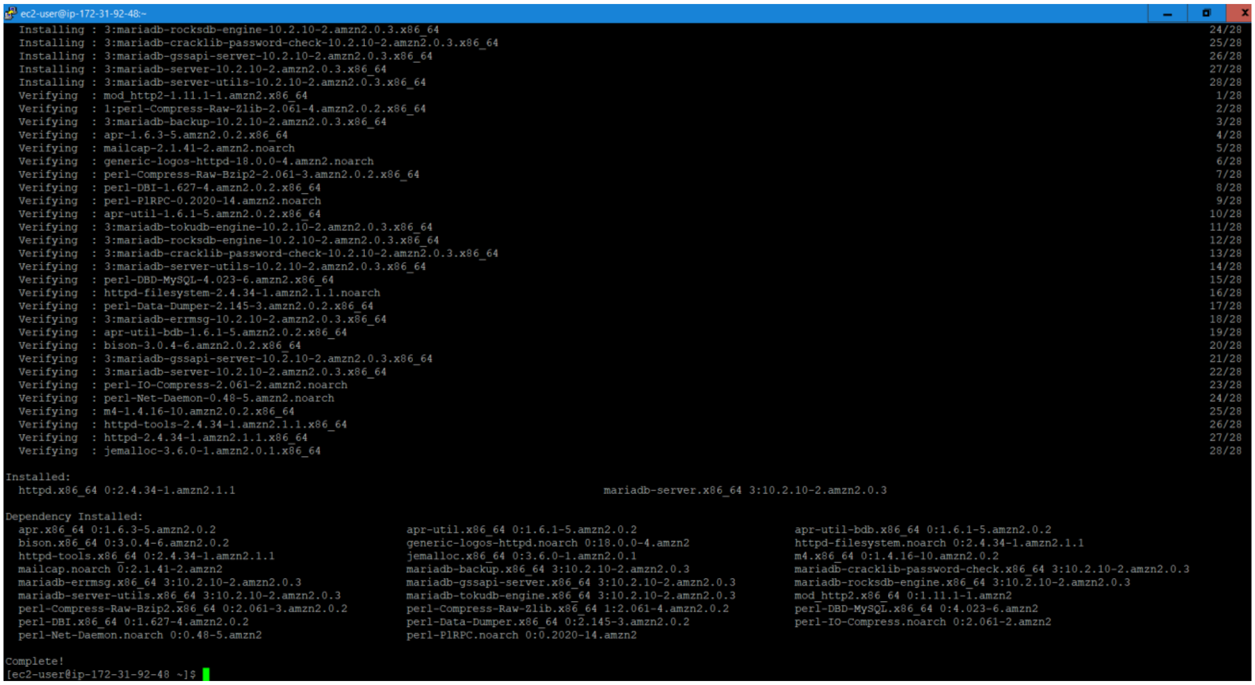


4) Install the lamp-mariadb10.2-php7.2 and php7.2 Amazon Linux Extras repositories to get the latest versions of the LAMP MariaDB and PHP packages for Amazon Linux 2 using the command **sudo amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2**





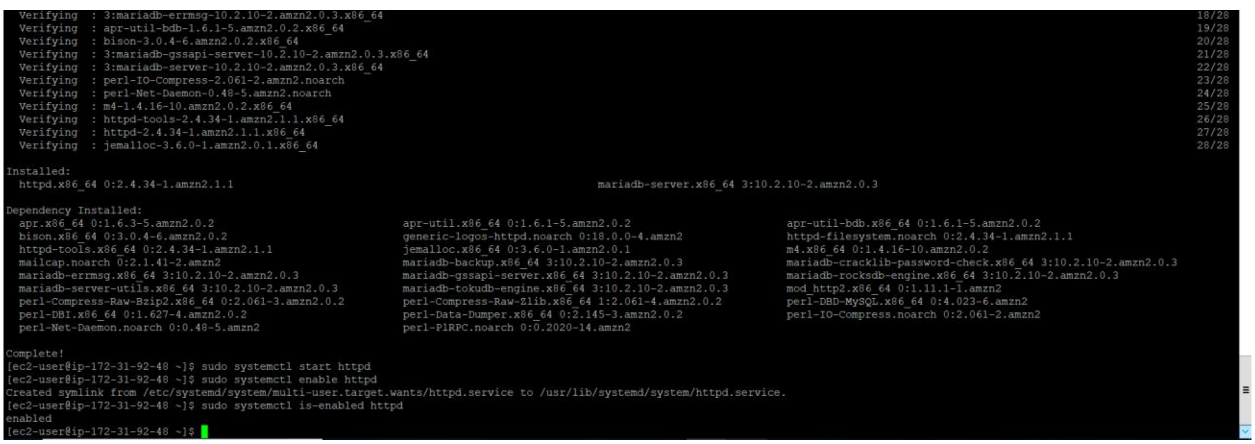
5) Install the Apache web server, MariaDB, and PHP software packages using the command **sudo yum install -y httpd mariadb-server**



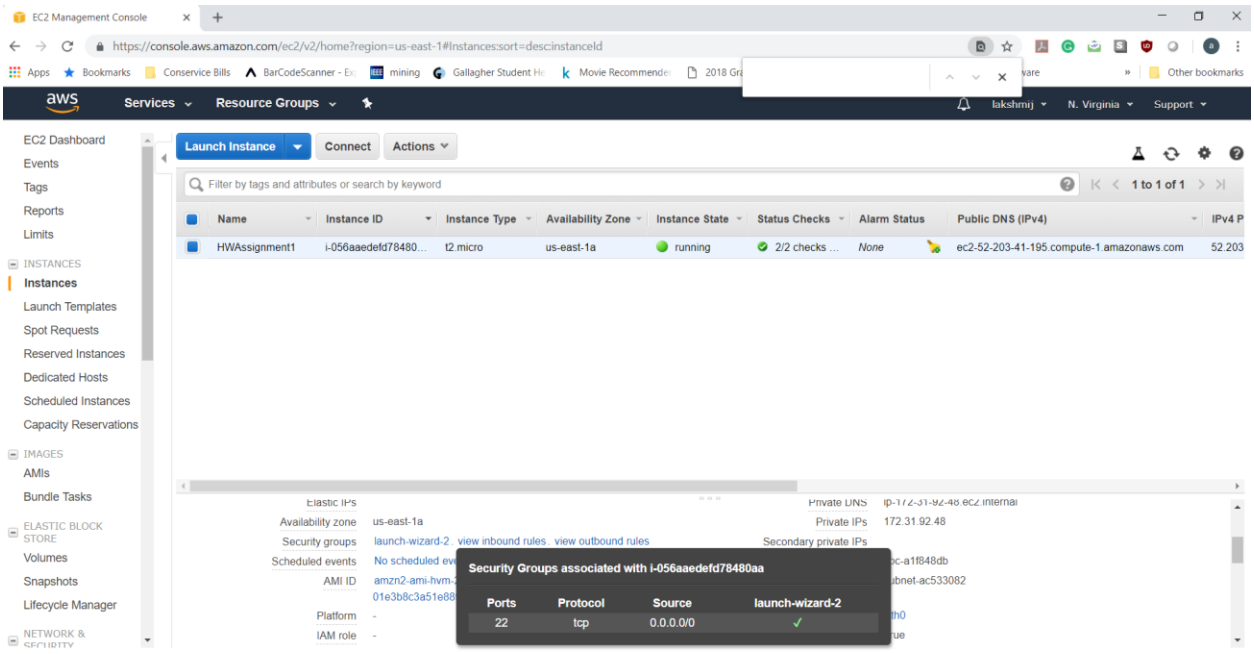
6) Start the Apache web server using the command **sudo systemctl start httpd**

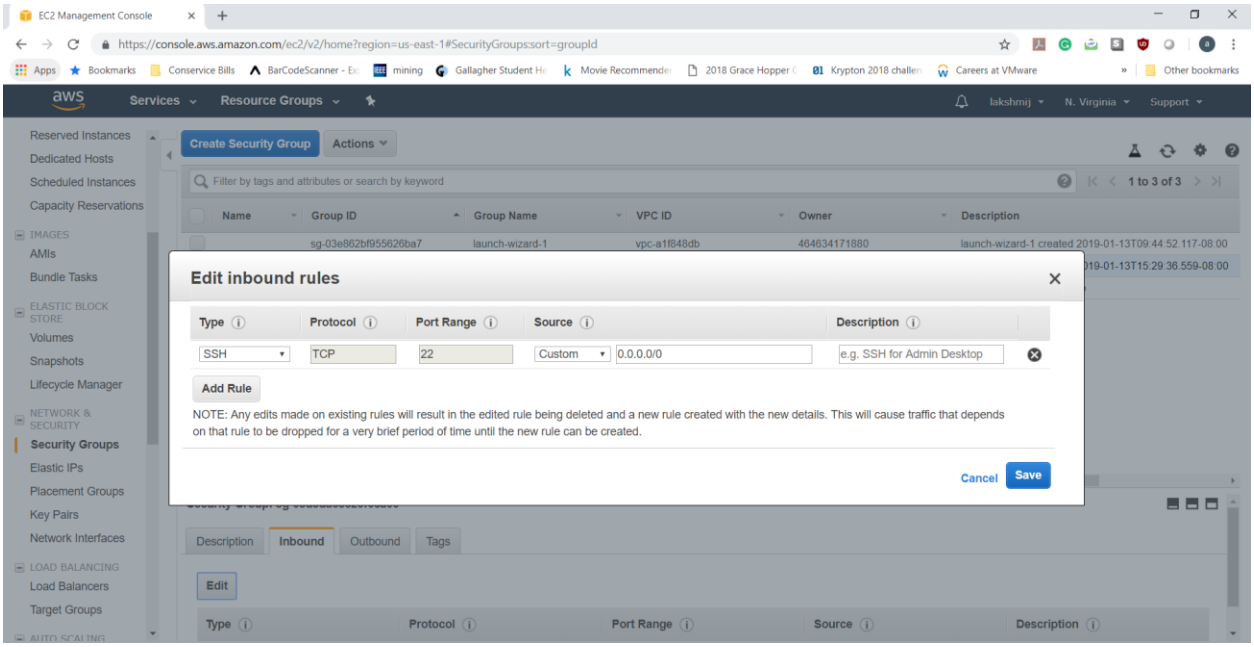
7) Use the **sudo systemctl enable httpd** command to configure the Apache web server to start at each system boot.

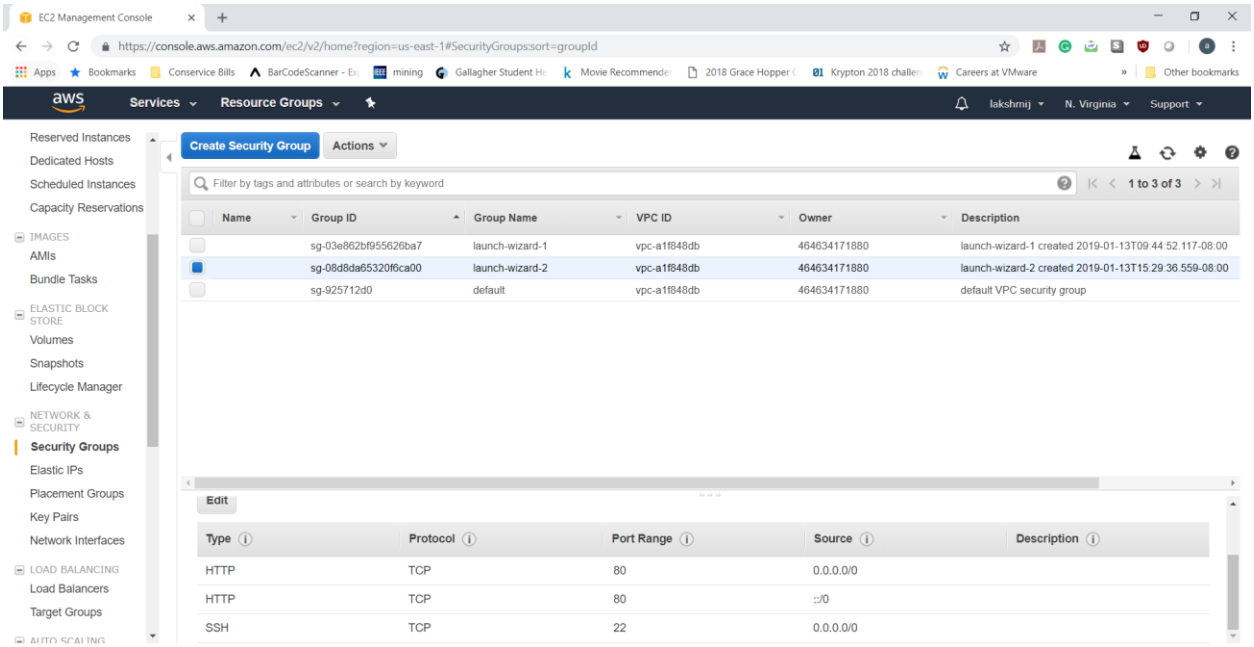
8) Verify that httpd is on by running using the **sudo systemctl is-enabled httpd** command



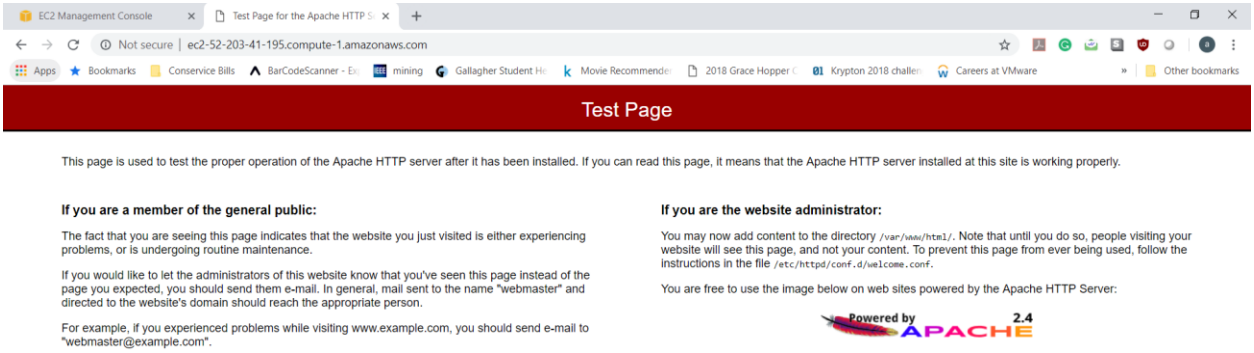
9) Add a security rule to allow inbound HTTP (port 80) connections to your instance


EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:sort=desc:instanceId
Services
Resource Groups
lakshmij
N. Virginia
Support
EC2 Dashboard
Events
Tags
Reports
Limits
INSTANCES
Instances
Launch Templates
Spot Requests
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager
Launch Instance
Connect
Actions
Filter by tags and attributes or search by keyword
1 to 1 of 1
Name
Instance ID
Instance Type
Availability Zone
Instance State
Status Checks
Alarm Status
Public DNS (IPv4)
HWAssignment1
i-056aaedefd78480...
t2.micro
us-east-1a
running
2/2 checks ...
None
ec2-52-203-41-195.compute-1.amazonaws.com
Availability zone
us-east-1a
Security groups
launch-wizard-2. view inbound rules. view outbound rules
Private IPs
172.31.92.48
Secondary private IPs
Security Groups associated with i-056aaedefd78480aa
Ports
Protocol
Source
launch-wizard-2
22
tcp
0.0.0.0/0


EC2 Management Console
https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#SecurityGroups:sort=groupId
Services
Resource Groups
lakshmij
N. Virginia
Support
Reserved Instances
Dedicated Hosts
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
Bundle Tasks
ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager
NETWORK & SECURITY
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
LOAD BALANCING
Load Balancers
Target Groups
Create Security Group
Actions
1 to 3 of 3
Name
Group ID
Group Name
VPC ID
Owner
Description
launch-wizard-1
vpc-a1f848db
464634171880
Edit inbound rules
Type
Protocol
Port Range
Source
Description
SSH
TCP
22
Custom
0.0.0.0/0
e.g. SSH for Admin Desktop
Add Rule
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.
Cancel
Save
Description
Inbound
Outbound
Tags
Edit
Type
Protocol
Port Range
Source
Description

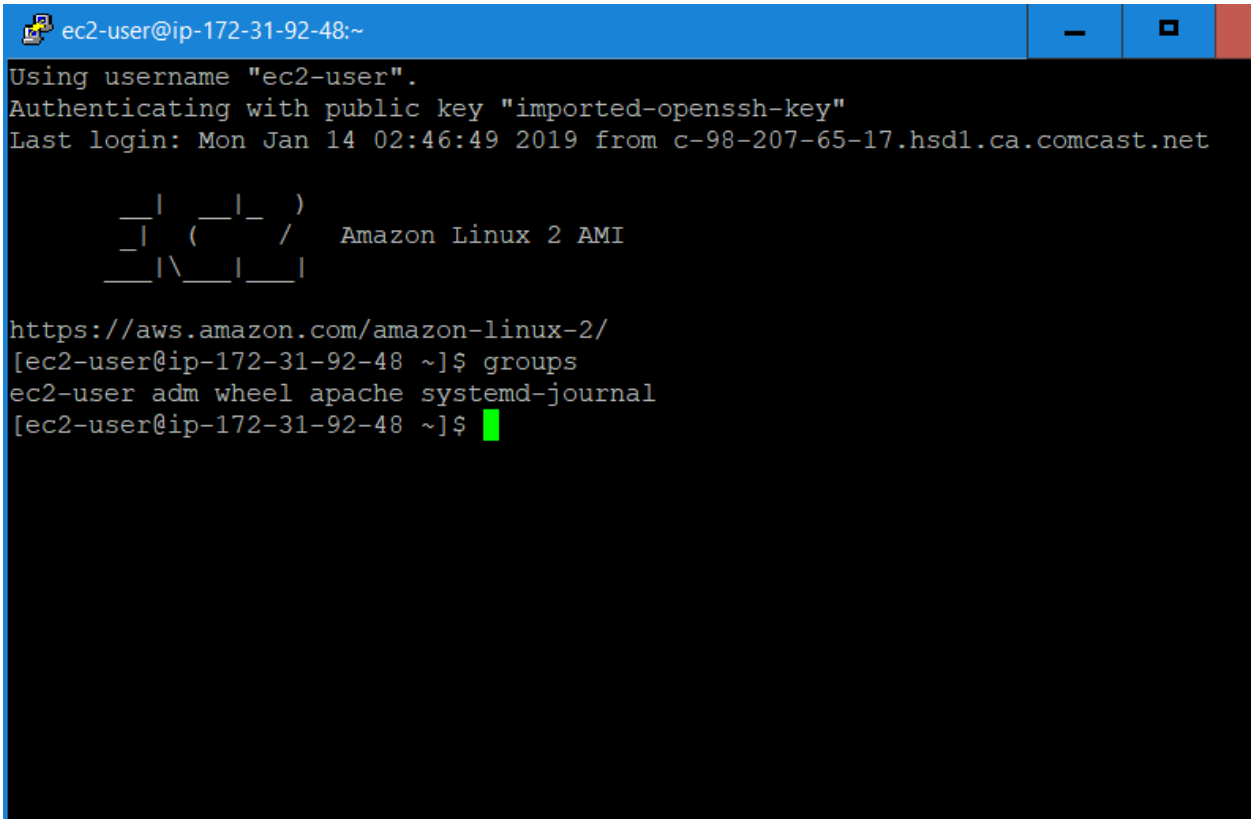


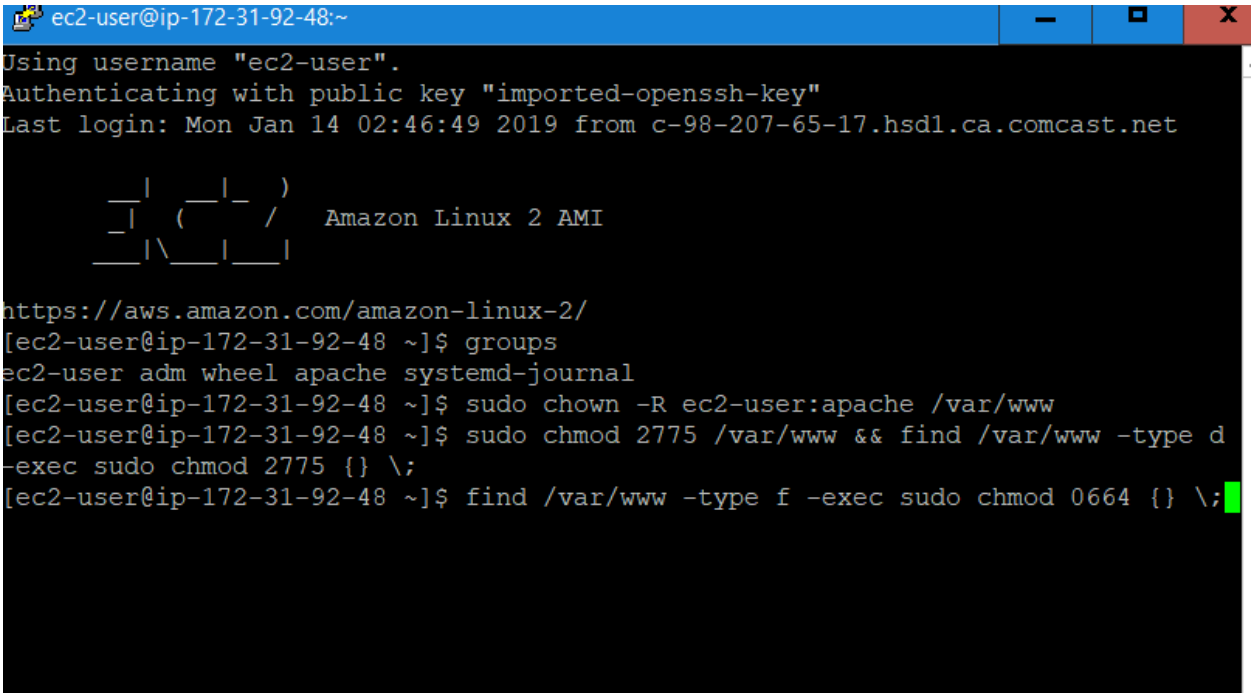
10) Test your web server. In a web browser, type the public DNS address (or the public IP address) of your instance.



To set file permissions

1. Add your user (in this case, ec2-user) to the apache group.


ec2-user@ip-172-31-92-48:~
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Last login: Mon Jan 14 02:46:49 2019 from c-98-207-65-17.hsd1.ca.comcast.net
__| __|_)
_| (/   Amazon Linux 2 AMI
___|___|___|
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-92-48 ~]$ groups
ec2-user adm wheel apache systemd-journal
[ec2-user@ip-172-31-92-48 ~]$


ec2-user@ip-172-31-92-48:~
Using username "ec2-user".
Authenticating with public key "imported-openssh-key"
Last login: Mon Jan 14 02:46:49 2019 from c-98-207-65-17.hsd1.ca.comcast.net
__| __|_)
_| (/   Amazon Linux 2 AMI
___|___|___|
https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-92-48 ~]$ groups
ec2-user adm wheel apache systemd-journal
[ec2-user@ip-172-31-92-48 ~]$ sudo chown -R ec2-user:apache /var/www
[ec2-user@ip-172-31-92-48 ~]$ sudo chmod 2775 /var/www && find /var/www -type d
-exec sudo chmod 2775 {} \;
[ec2-user@ip-172-31-92-48 ~]$ find /var/www -type f -exec sudo chmod 0664 {} \;

2. Now, ec2-user (and any future members of the apache group) can add, delete, and edit files in the Apache document root, enabling you to add content, such as a static website or a PHP application.