This section gives a step-by-step process to launch an EC2 Linux instance from a Linux platform.

A. Launch an instance

1. From the AWS Management Console, select EC2 and, once signed in, go to Launch Instance Tab.

2. To determine the processor architecture when you want to match the instance with the hardware,

enter the command

uname -m

and choose an appropriate Amazon Linux AMI by pressing Select.

3. Choose Instance Details to control the number, size, and other settings for instances.

4. To learn how the system works, press Continue to select the default settings.

5. Define the instance’s security, as discussed in Section 11.3: In the Create Key Pair page enter a

name for the pair and then press Create and Download Key Pair.

6. The key-pair file downloaded in the previous step is a .pem file, and it must be hidden to prevent

unauthorized access. If the file is in the directory awcdir/dada.pem enter the commands

cd awcdir

chmod 400 dada.pem

7. Configure the firewall. Go to the page Configure firewall, select the option Create a New Security

Group, and provide a Group Name. Normally we use ssh to communicate with the instance; the

default port for communication is port 8080, and we can change the port and other rules by creating

a new rule.

8. Press Continue and examine the review page, which gives a summary of the instance.

9. Press Launch and examine the confirmation page, then press Close to end the examination of the

confirmation page.

10. Press the Instances tab on the navigation panel to view the instance.

11. Look for your Public DNS name. Because by default some details of the instance are hidden, click

on the Show/Hide tab on the top of the console and select Public DNS.

12. Record the Public DNS as PublicDNSname; it is needed to connect to the instance from the Linux

terminal.

13. Use the ElasticIP panel to assign an Elastic IP address if a permanent IP address is required.

B. Connect to the instance using ssh and the TCP transport protocol.

1. Add a rule to the iptables to allow ssh traffic using the TCP protocol. Without this step, either

an access denied or permission denied error message appears when you’re trying to connect to

the instance.

sudo iptables -A iptables -p -tcp -dport ssh -j ACCEPT

2. Enter the Linux command:

ssh -i abc.pem ec2-user@PublicDNSname

If you get the prompt You want to continue connecting? respond Yes. A warning that the DNS

name was added to the list of known hosts will appear.

3. An icon of the Amazon Linux AMI will be displayed.

C. Gain root access to the instance

By default the user does not have root access to the instance; thus, the user cannot install any software.

Once connected to the EC2 instance, use the following command to gain root privileges:

sudo -i

Then use yum install commands to install software, e.g., gcc to compile C programs on the cloud.

D. Run the service ServiceName

If the instance runs under Linux or Unix, the service is terminated when the ssh connection is closed.

To avoid the early termination, use the command

nohup ServiceName

To run the service in the background and redirect stdout and stderr to files p.out and p.err, respectively,

execute the command

nohup ServiceName > p.out 2 > p.err &