TÉCNICO
LISBOA

Cloud Computing and Virtualization

Lab. 3 - Introduction to AWS

Goals of the lab

Goal: Set up an auto-scaling web server

aws

Root user sign in

Email: your-account@your-domain

Password Forgot password?

••••••••••

Sign in

Sign in to a different account

Create a new AWS account

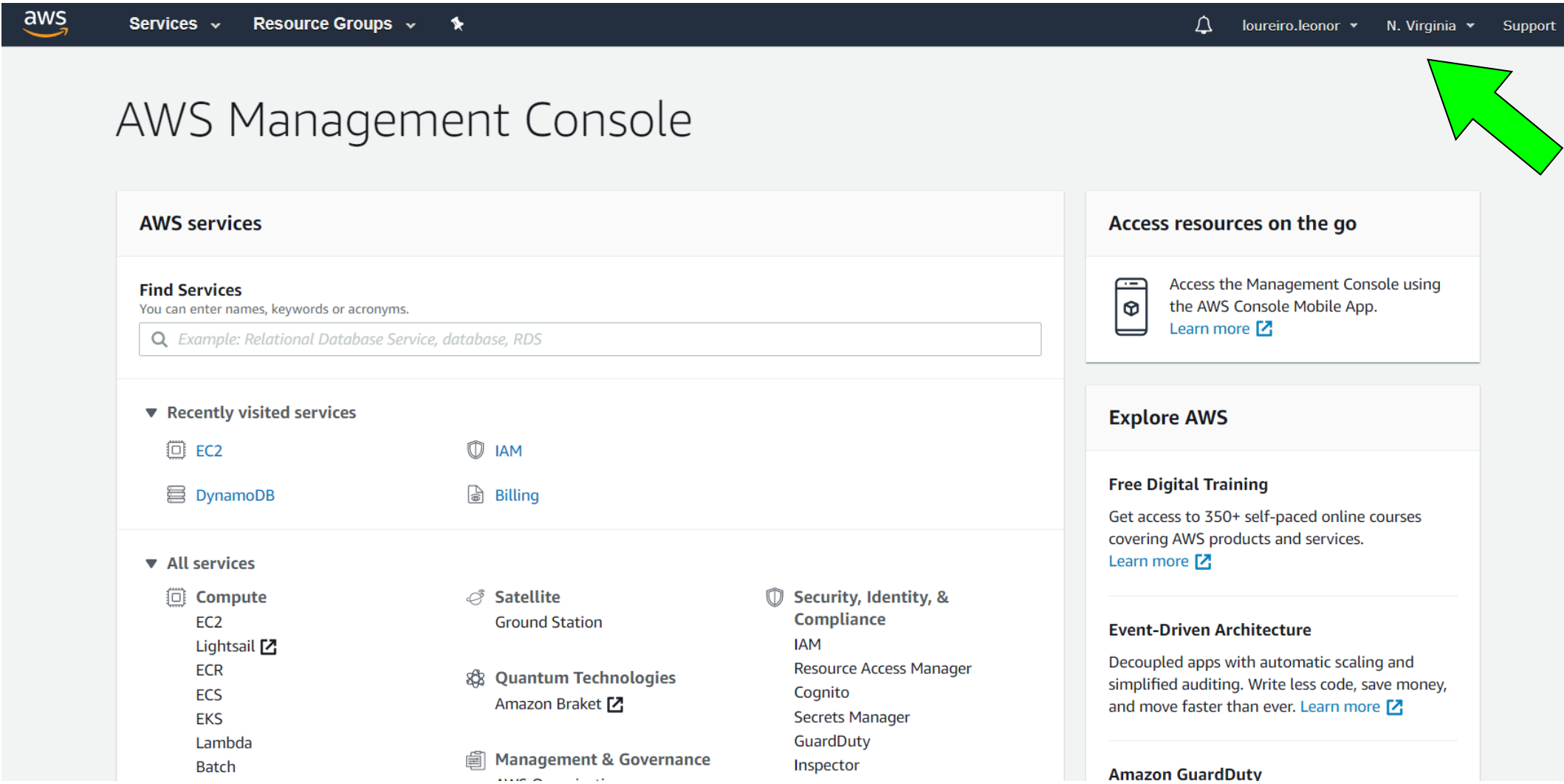
About Amazon.com Sign In

Amazon Web Services uses information from your Amazon.com account to identify you and allow access to Amazon Web Services. Your use of this site is governed by our Terms of Use and Privacy Policy linked below. Your use of Amazon Web Services products and services is governed by the AWS Customer Agreement linked below unless you have entered into a separate agreement with Amazon Web Services or an AWS Value Added Reseller to purchase these products and services. The AWS Customer Agreement was updated on March 31, 2017. For more information about these updates, see Recent Changes.

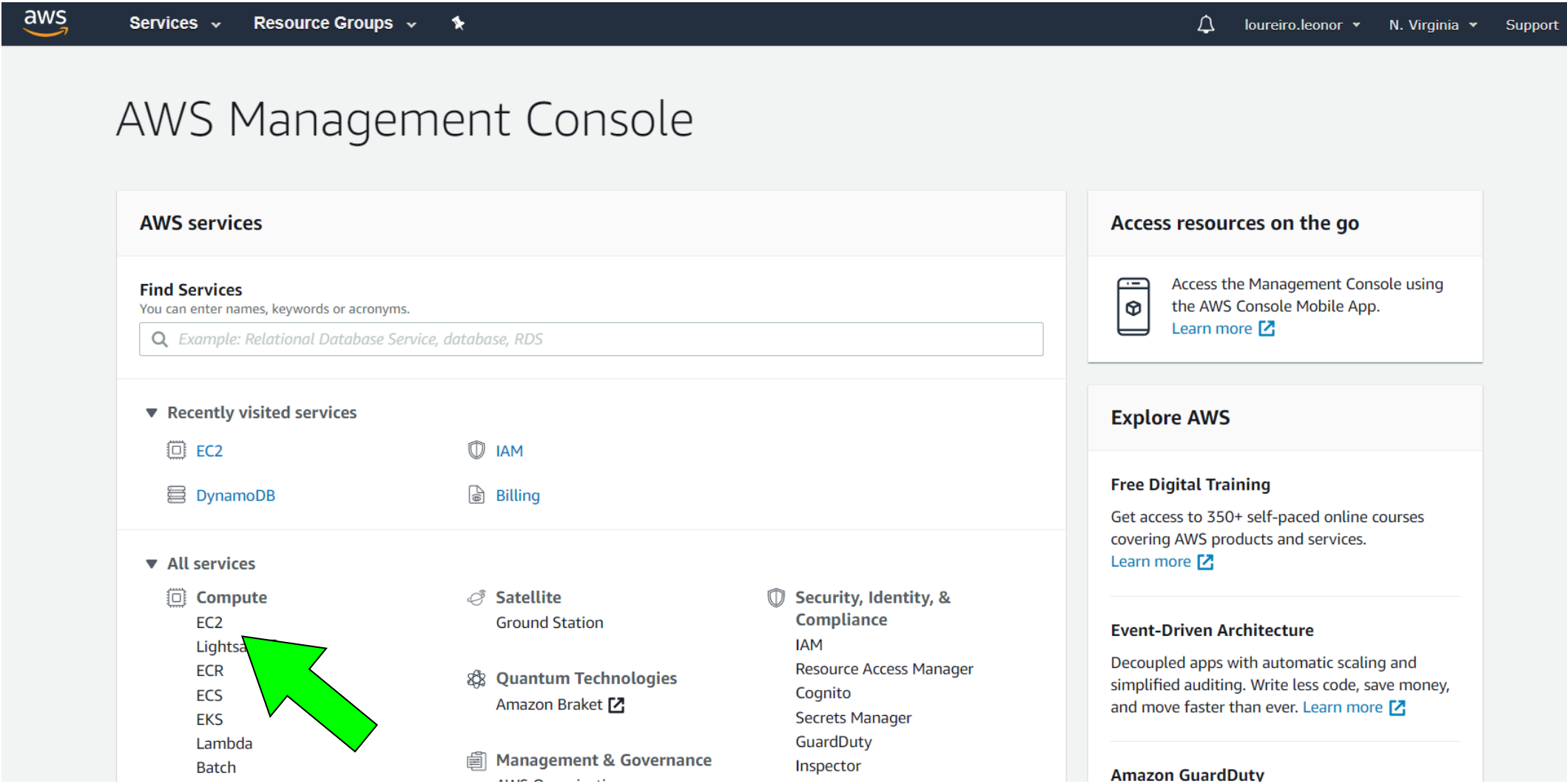
 create-verify-aws-account - PowerPoint (Unlicensed Product) AWS Customer Agreement

English

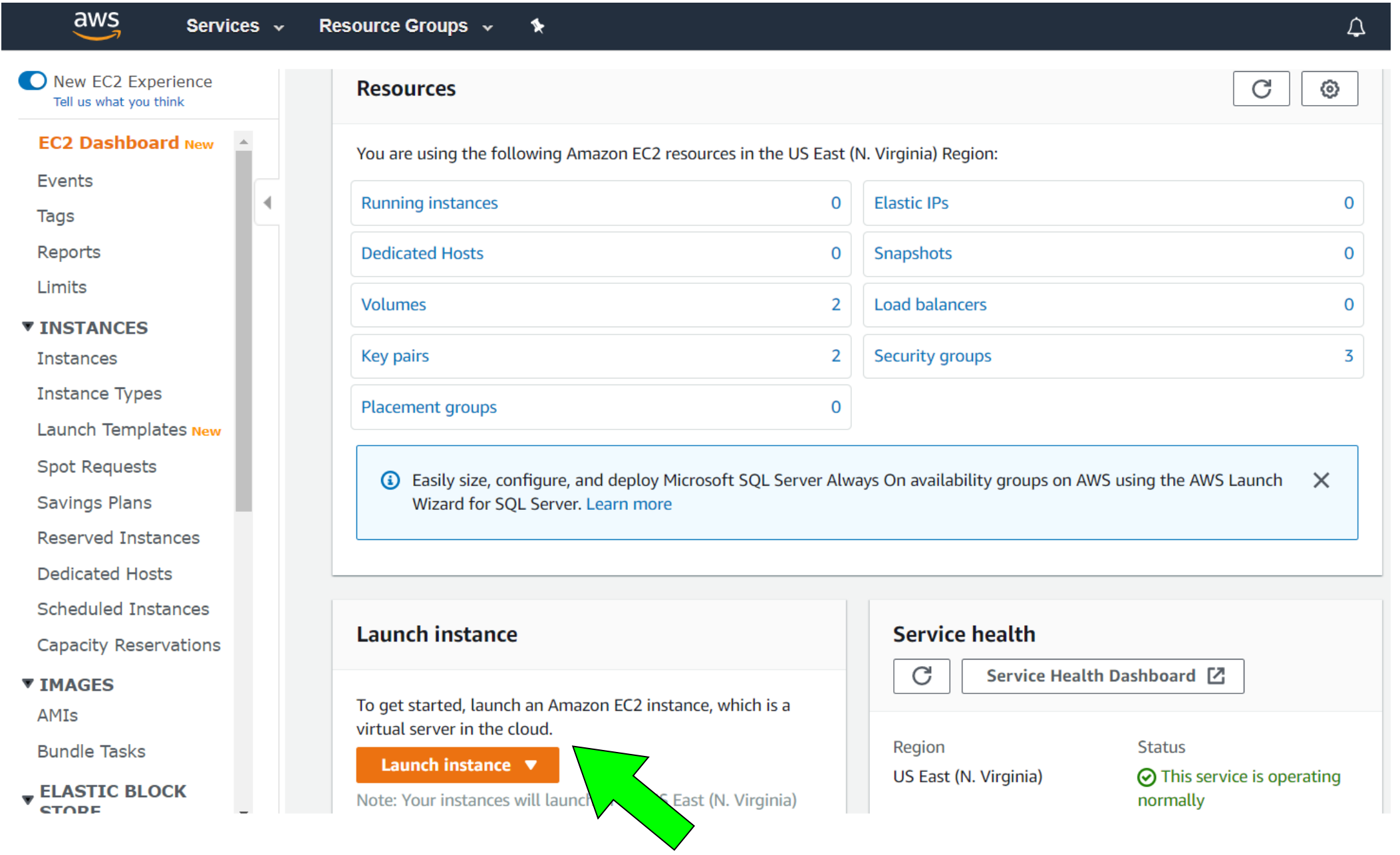
Select US East North Virginia



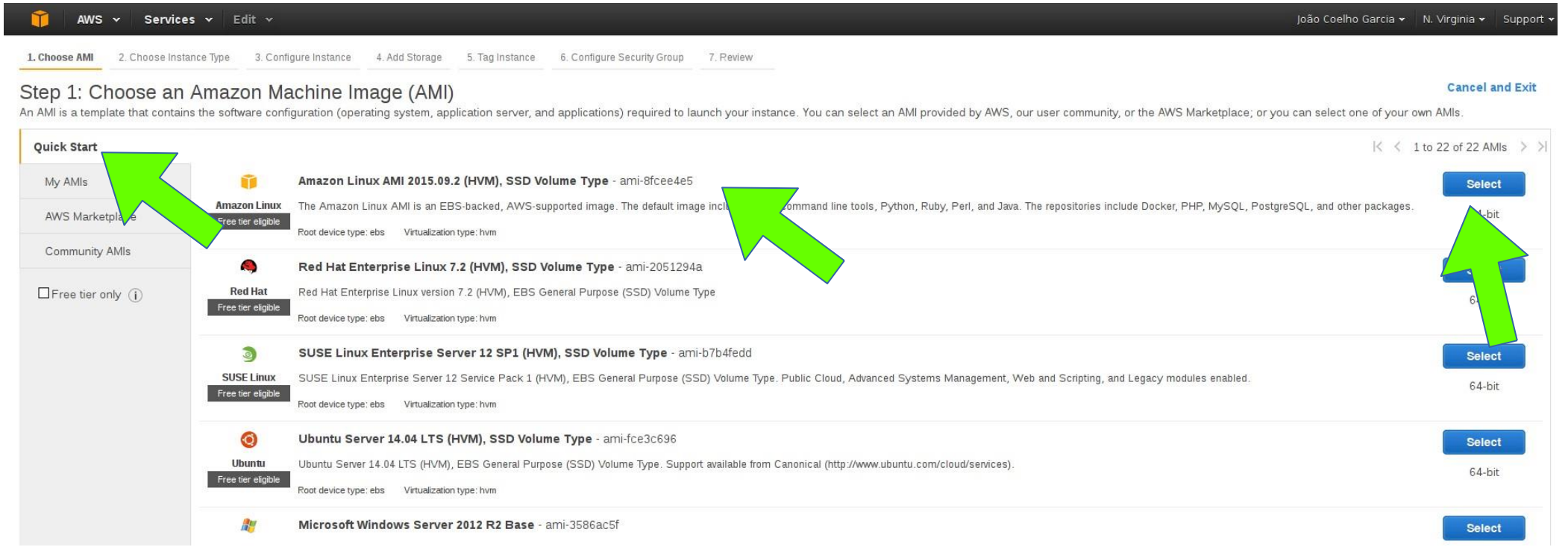
Select EC2


aws
Services
Resource Groups
loureiro.leonor
N. Virginia
Support
AWS Management Console
AWS services
Find Services
You can enter names, keywords or acronyms.
Example: Relational Database Service, database, RDS
Recently visited services
EC2
IAM
DynamoDB
Billing
All services
Compute
EC2
Lightsa
ECR
ECS
EKS
Lambda
Batch
Satellite
Ground Station
Quantum Technologies
Amazon Braket
Management & Governance
Security, Identity, & Compliance
IAM
Resource Access Manager
Cognito
Secrets Manager
GuardDuty
Inspector
Access resources on the go
Access the Management Console using the AWS Console Mobile App.
Learn more
Explore AWS
Free Digital Training
Get access to 350+ self-paced online courses covering AWS products and services.
Learn more
Event-Driven Architecture
Decoupled apps with automatic scaling and simplified auditing. Write less code, save money, and move faster than ever. Learn more
Amazon GuardDuty

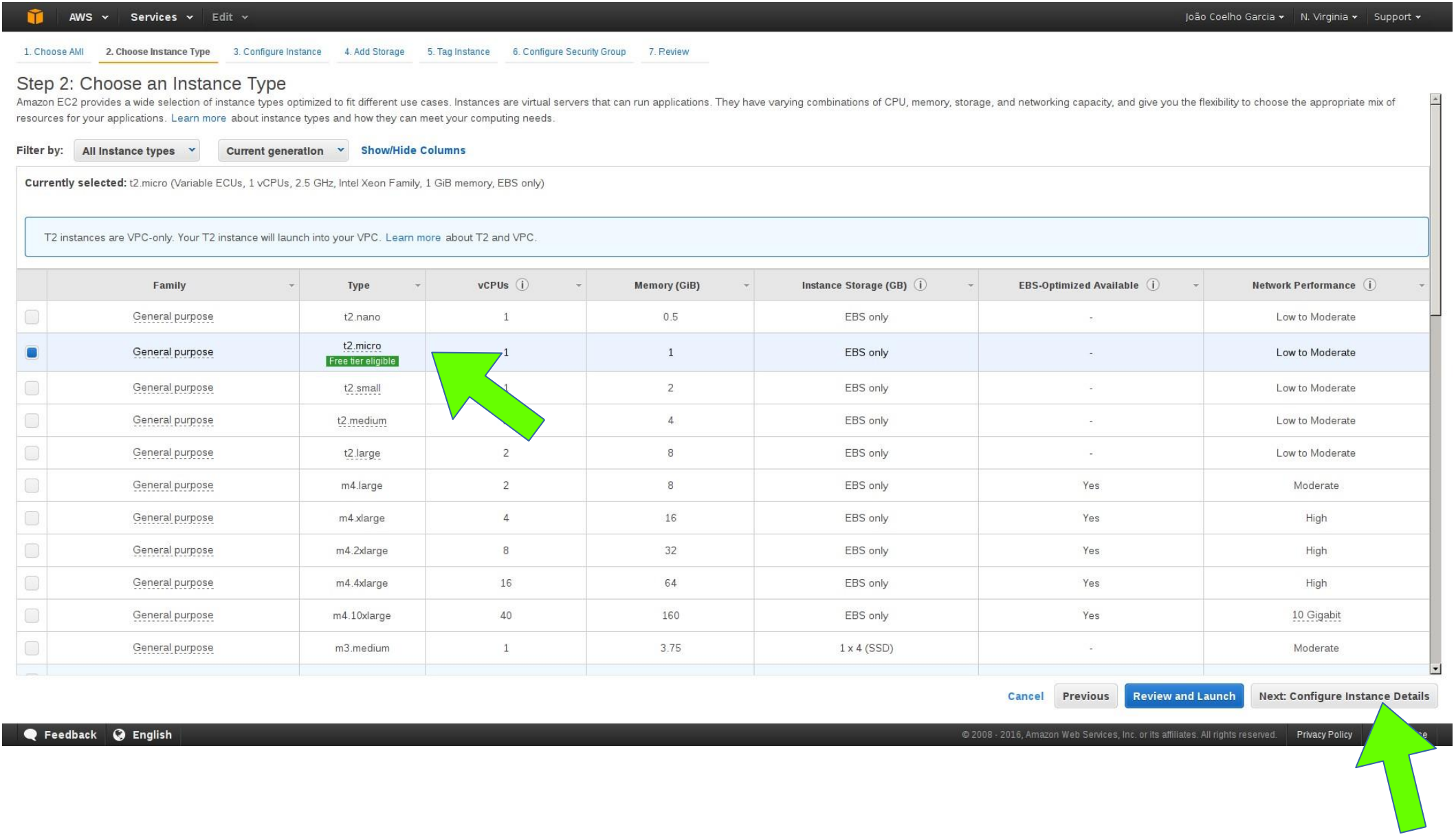
Launch an Instance



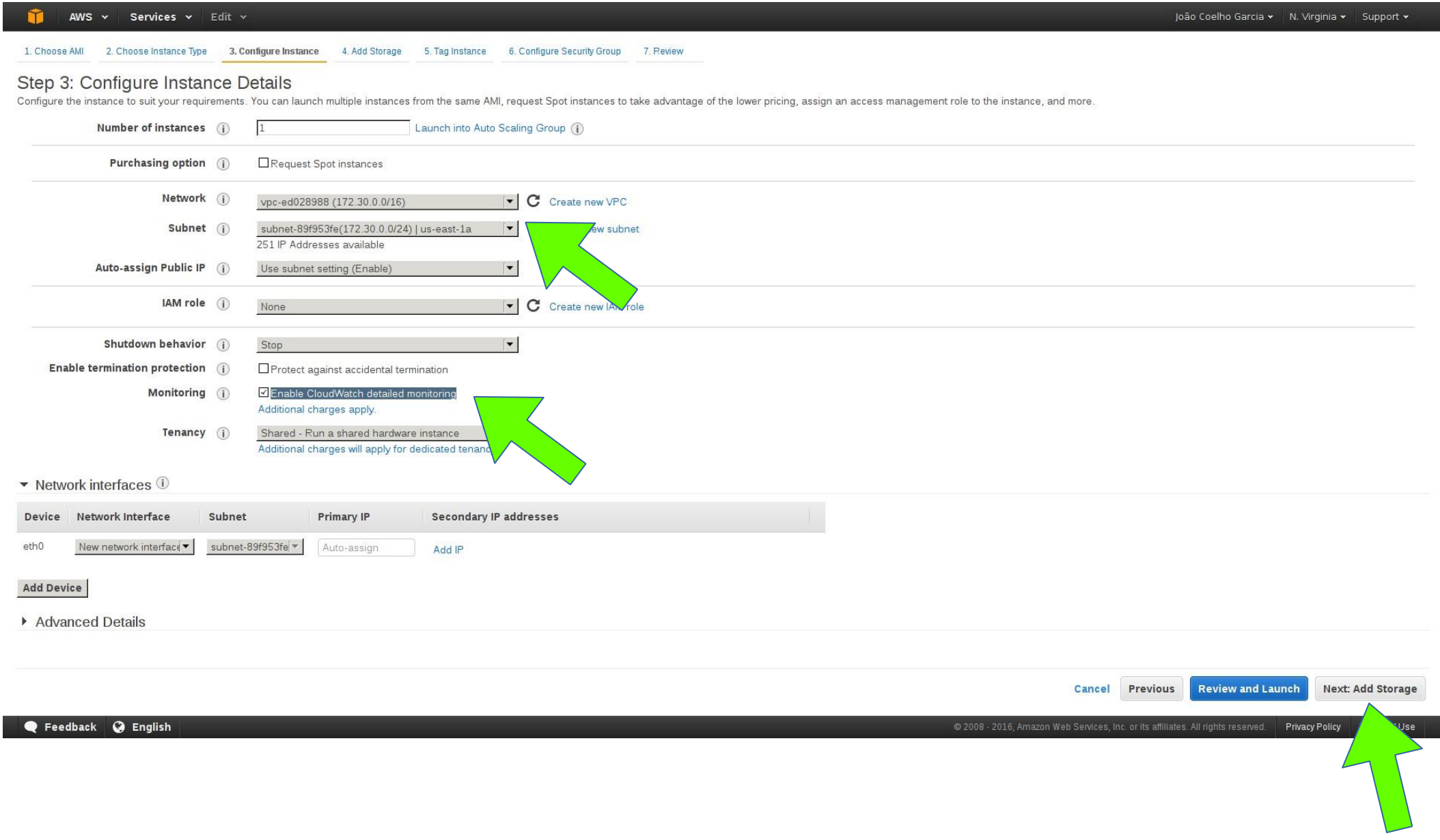
Pick AWS Linux from QuickStart



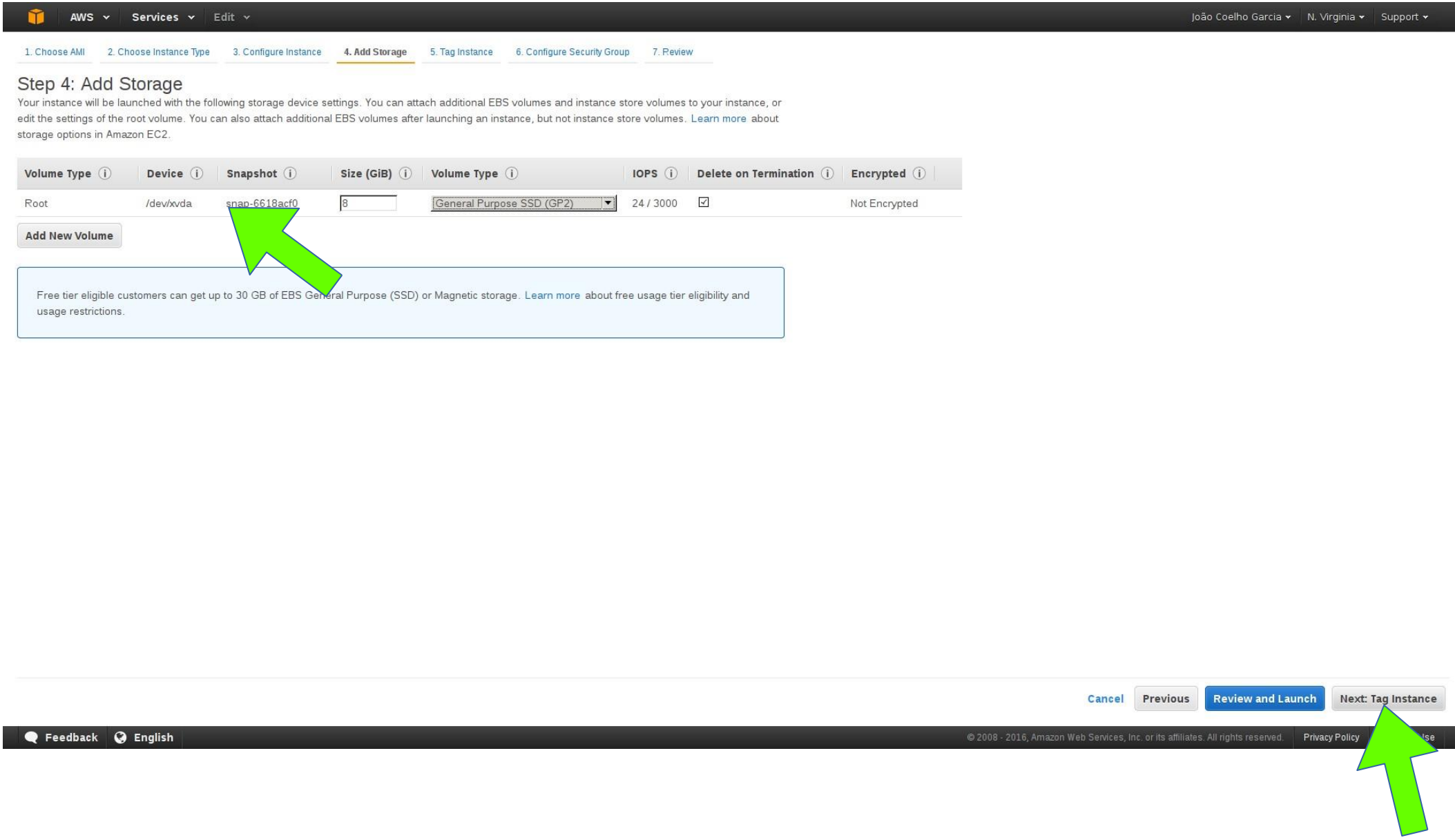
Pick a free tier machine



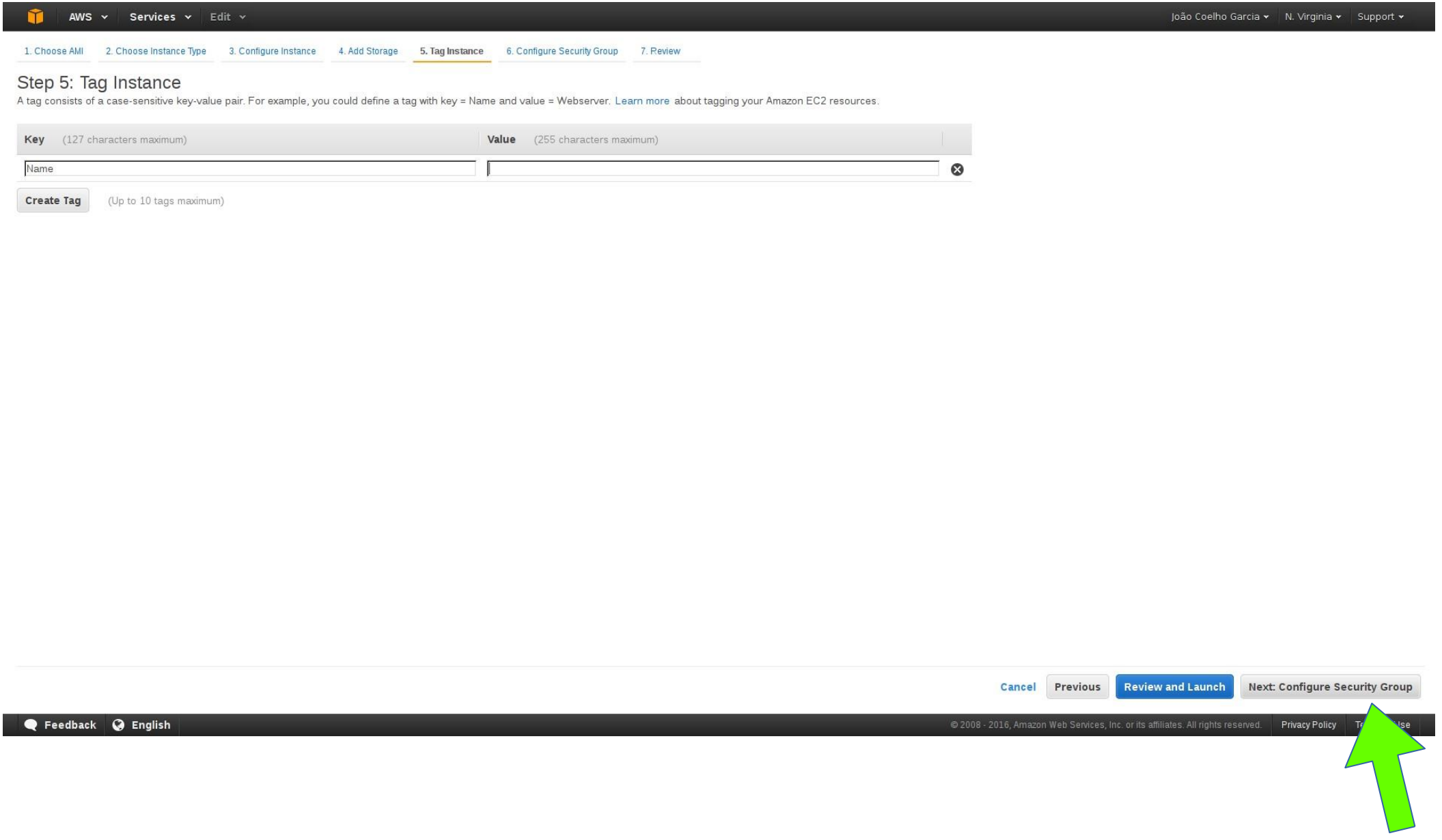
Select a subnet and enable monitoring



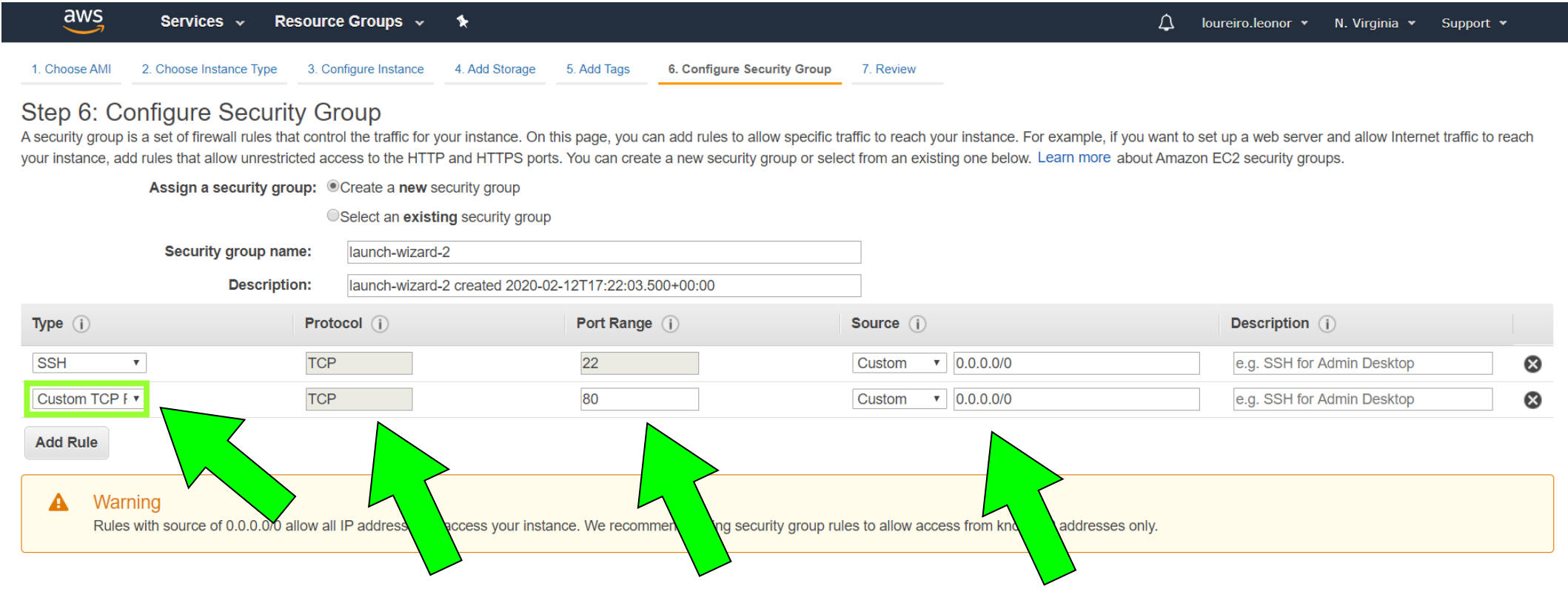
Use default storage



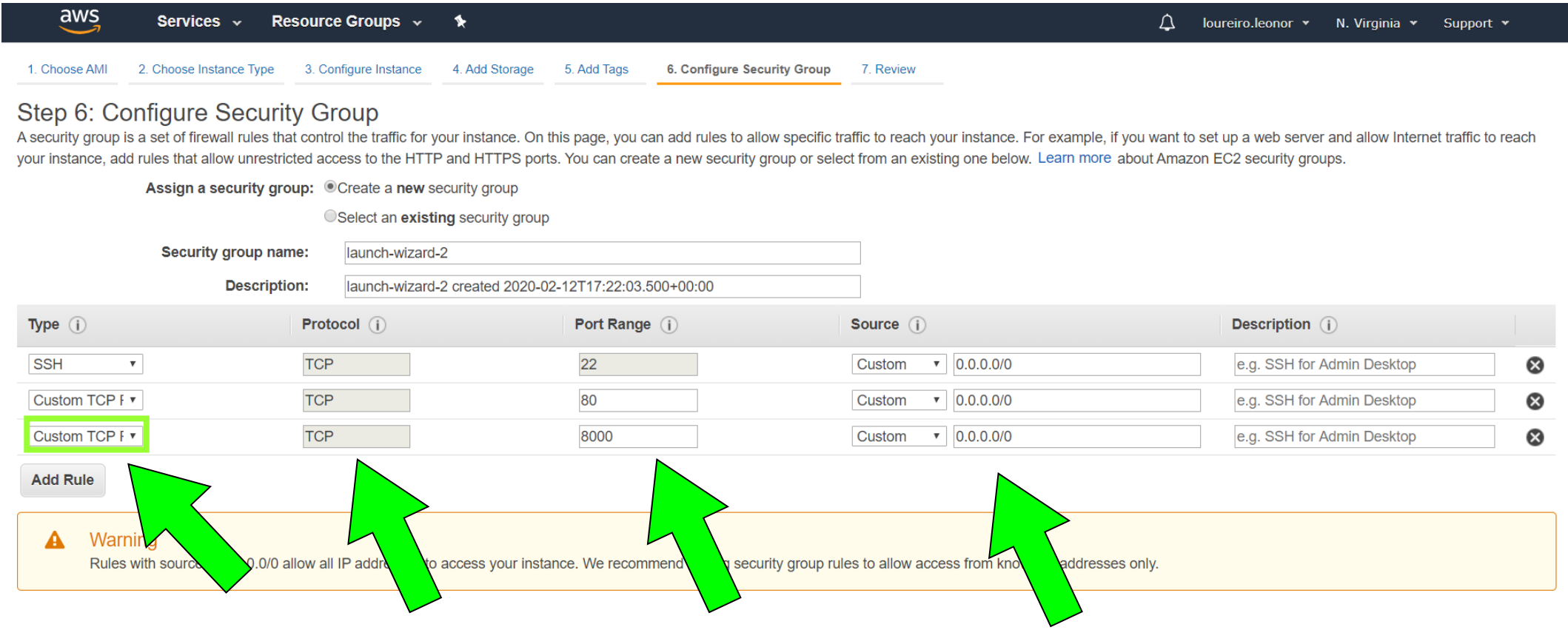
Don't use tags for now...



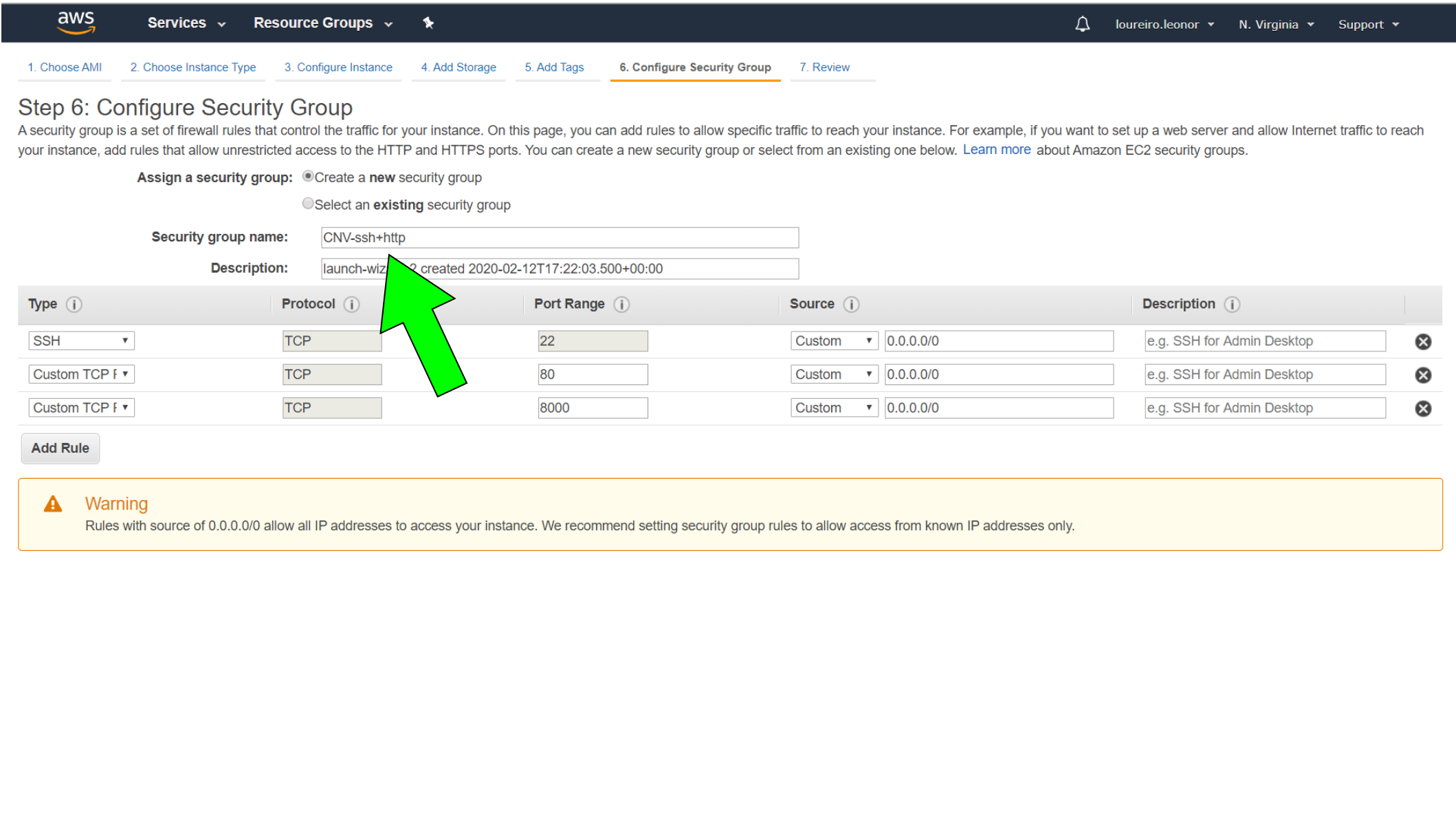
Add inbound network rules to security group (1)



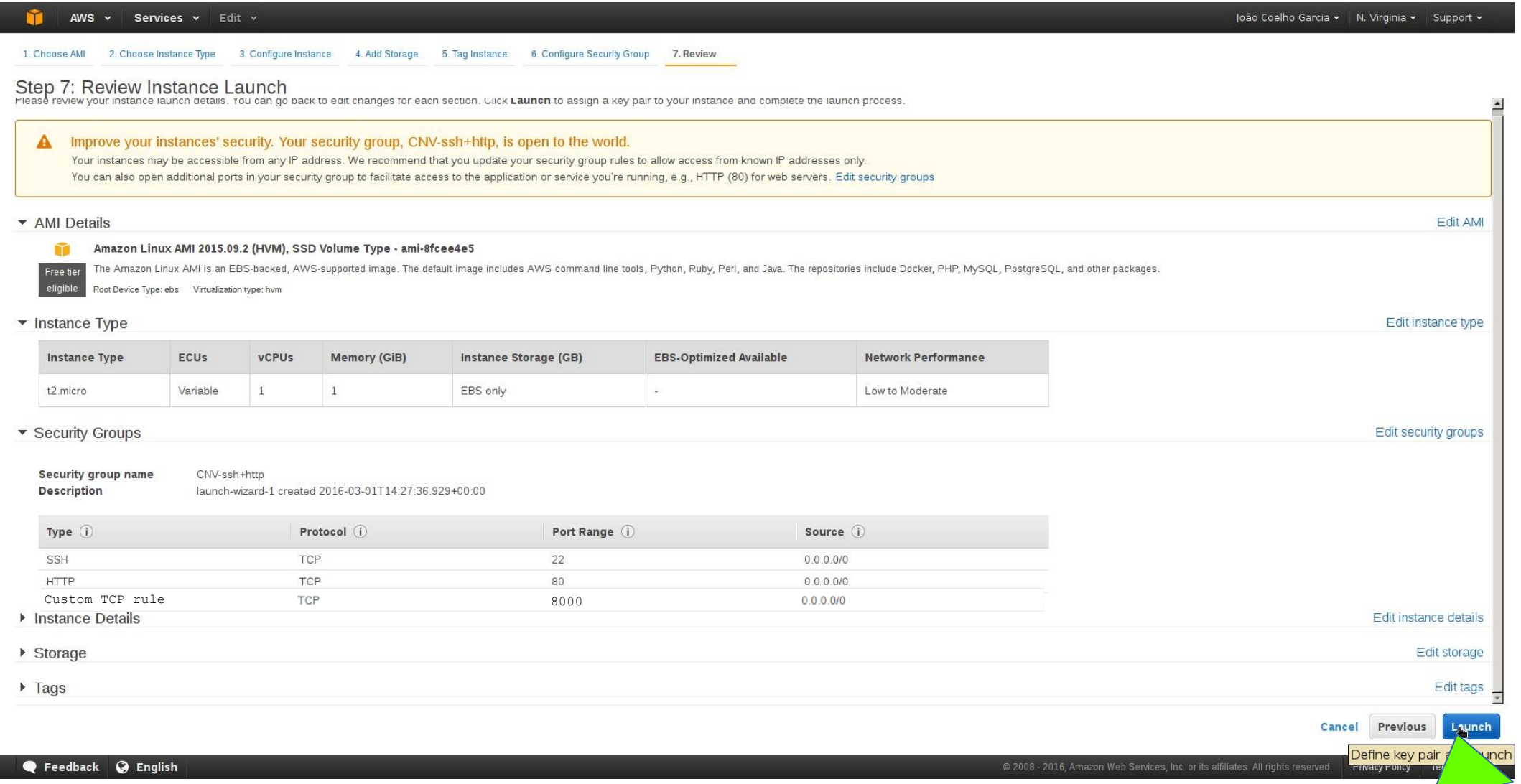
Add inbound network rules to security group (2)



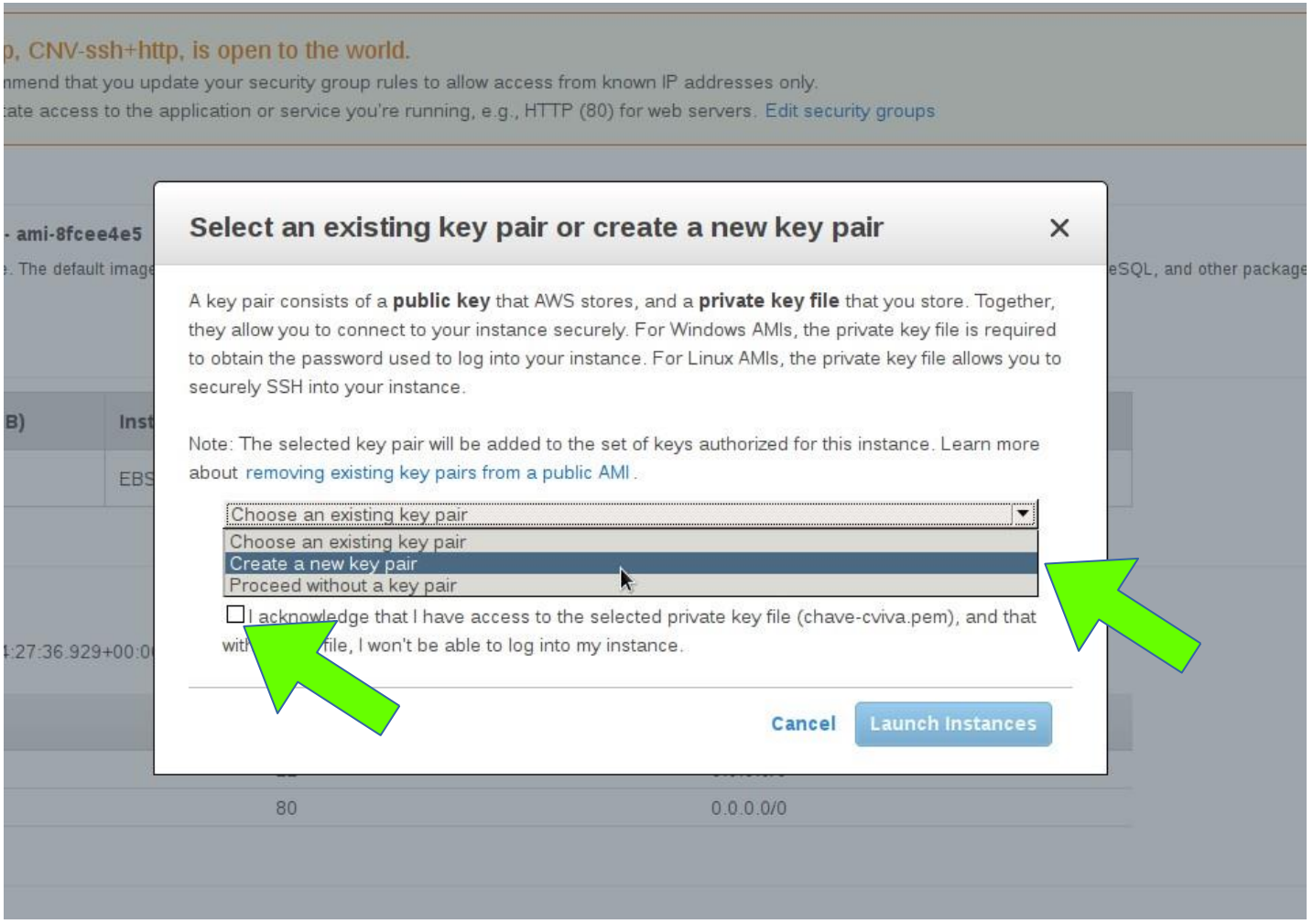
Add name to security group



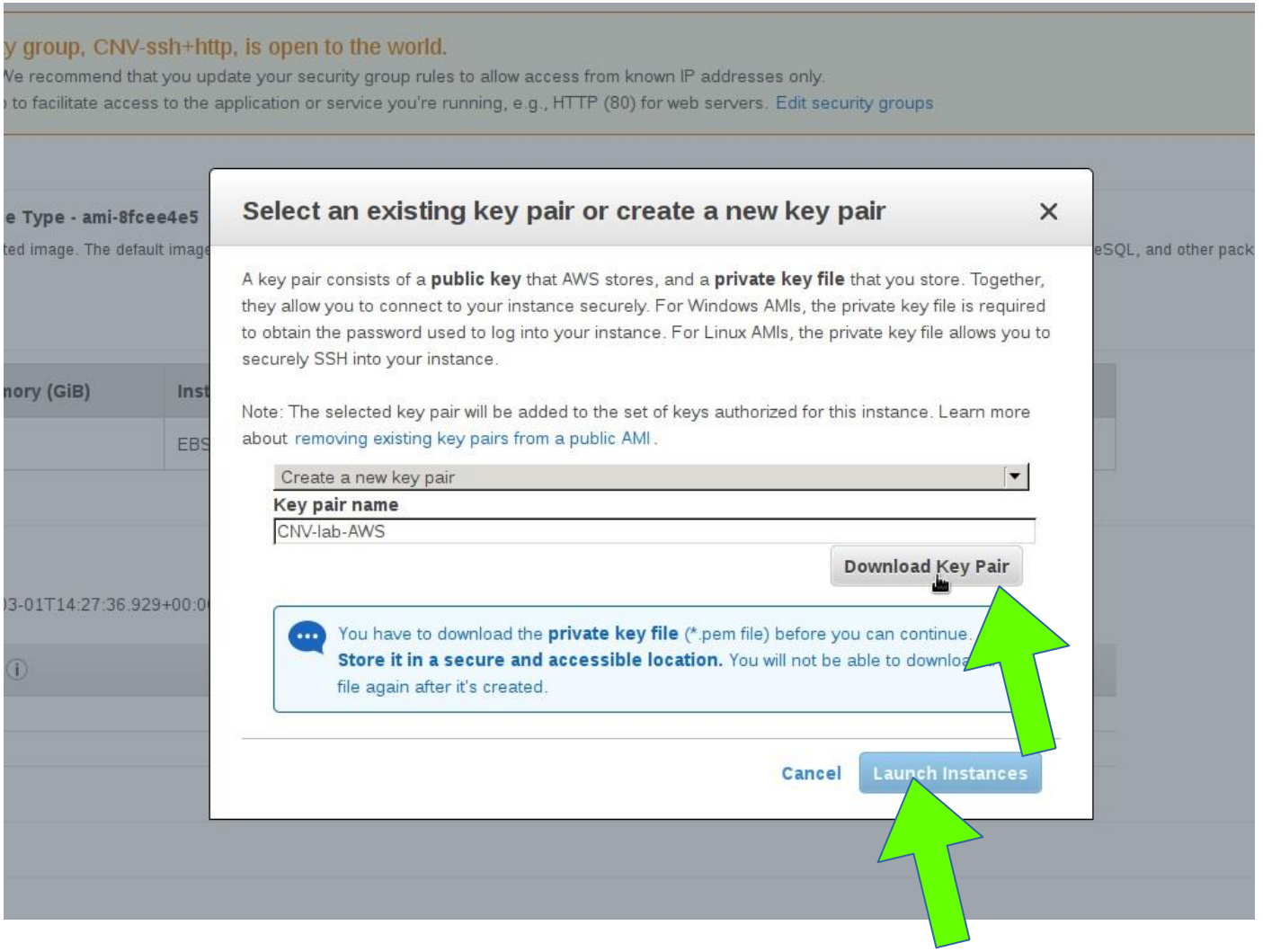
Review and Launch



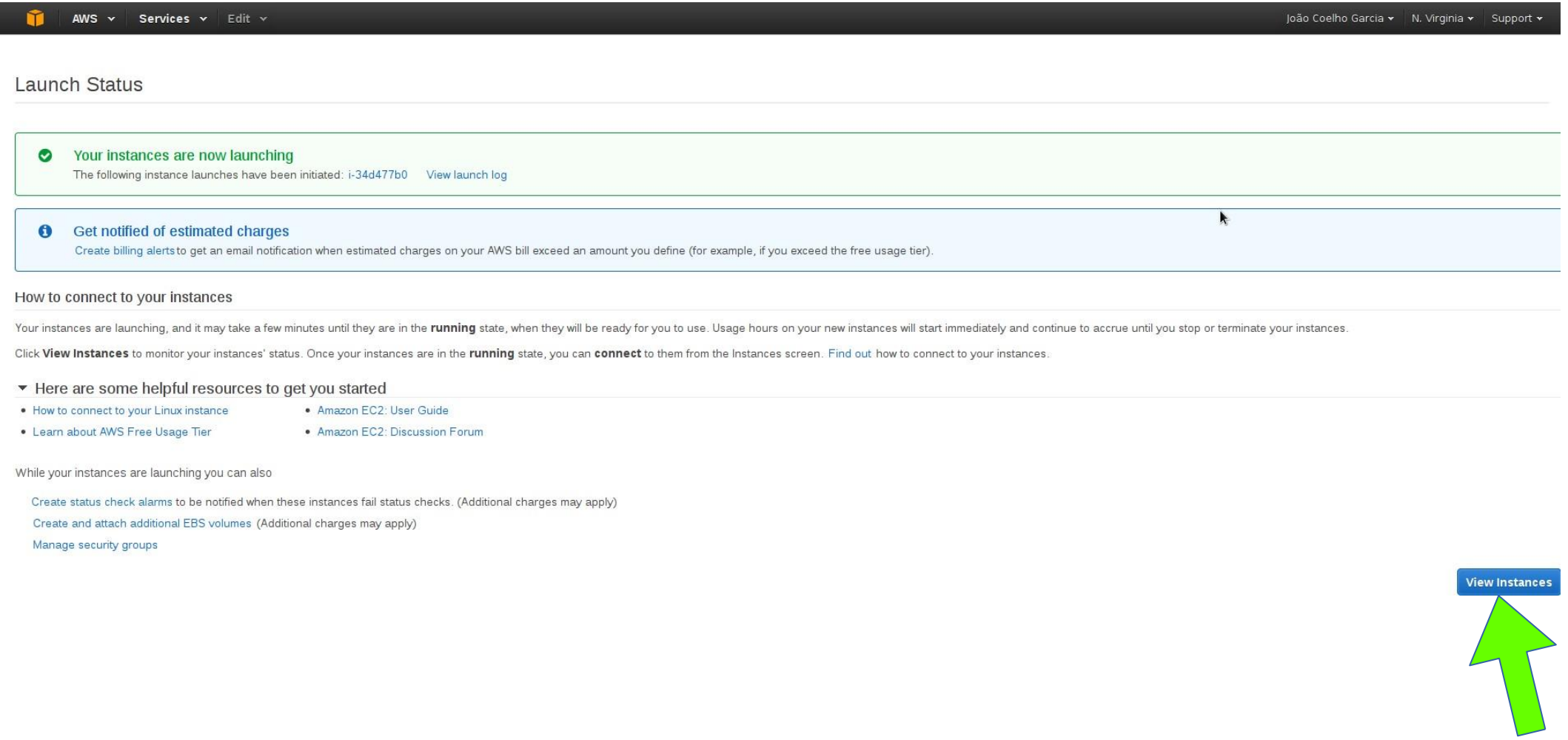
Create a key pair to connect to instance



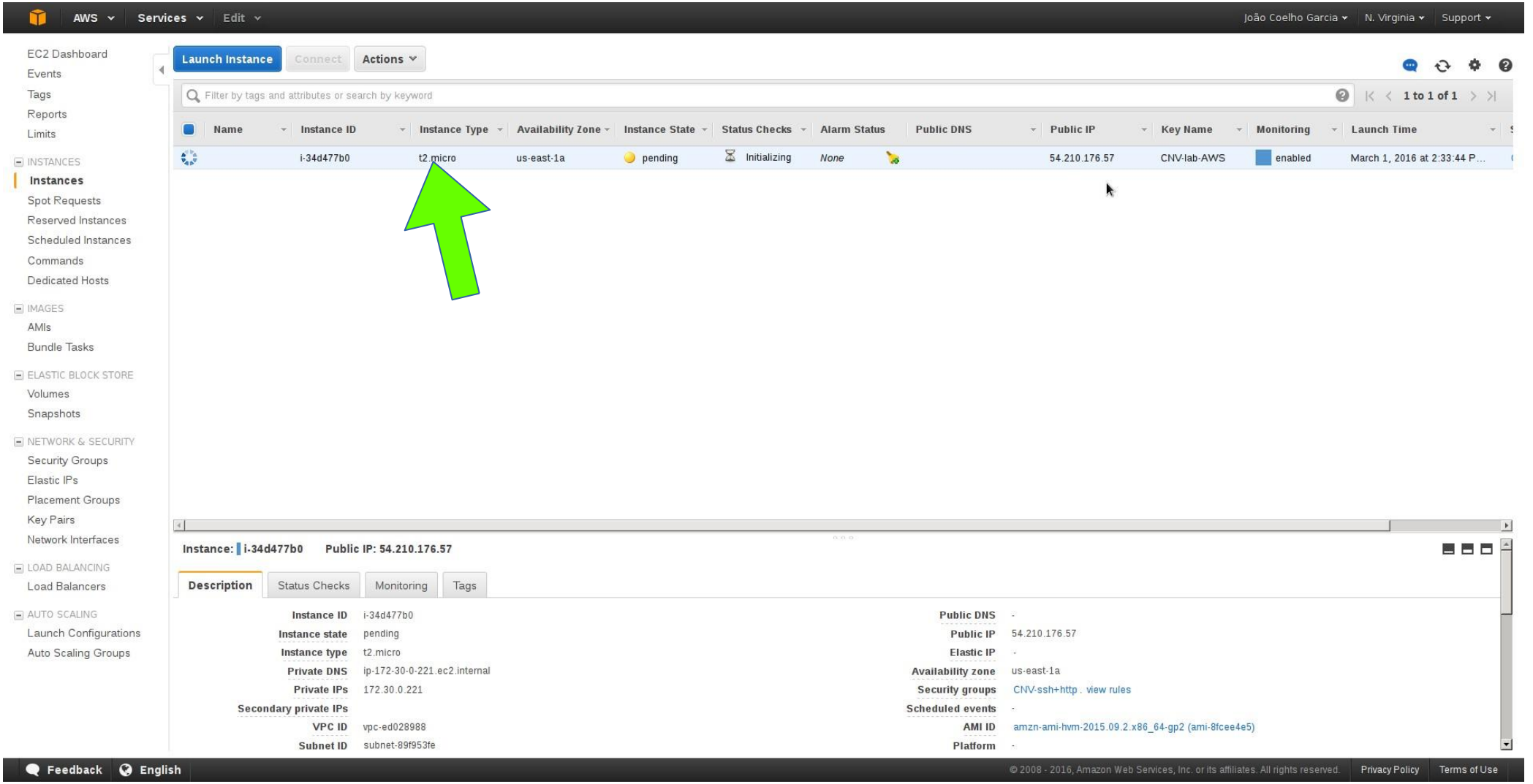
Download key pair and launch



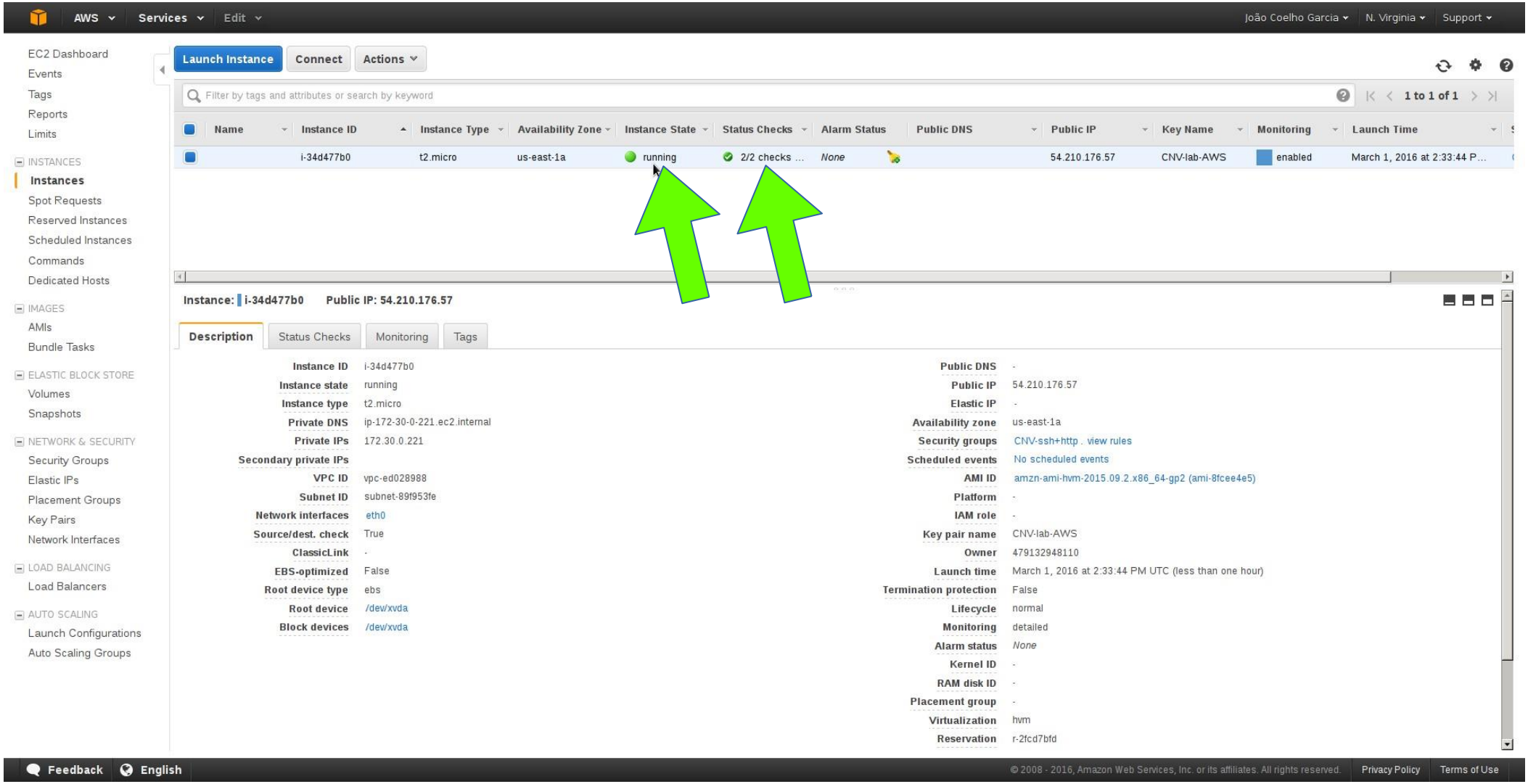
Instances starting...



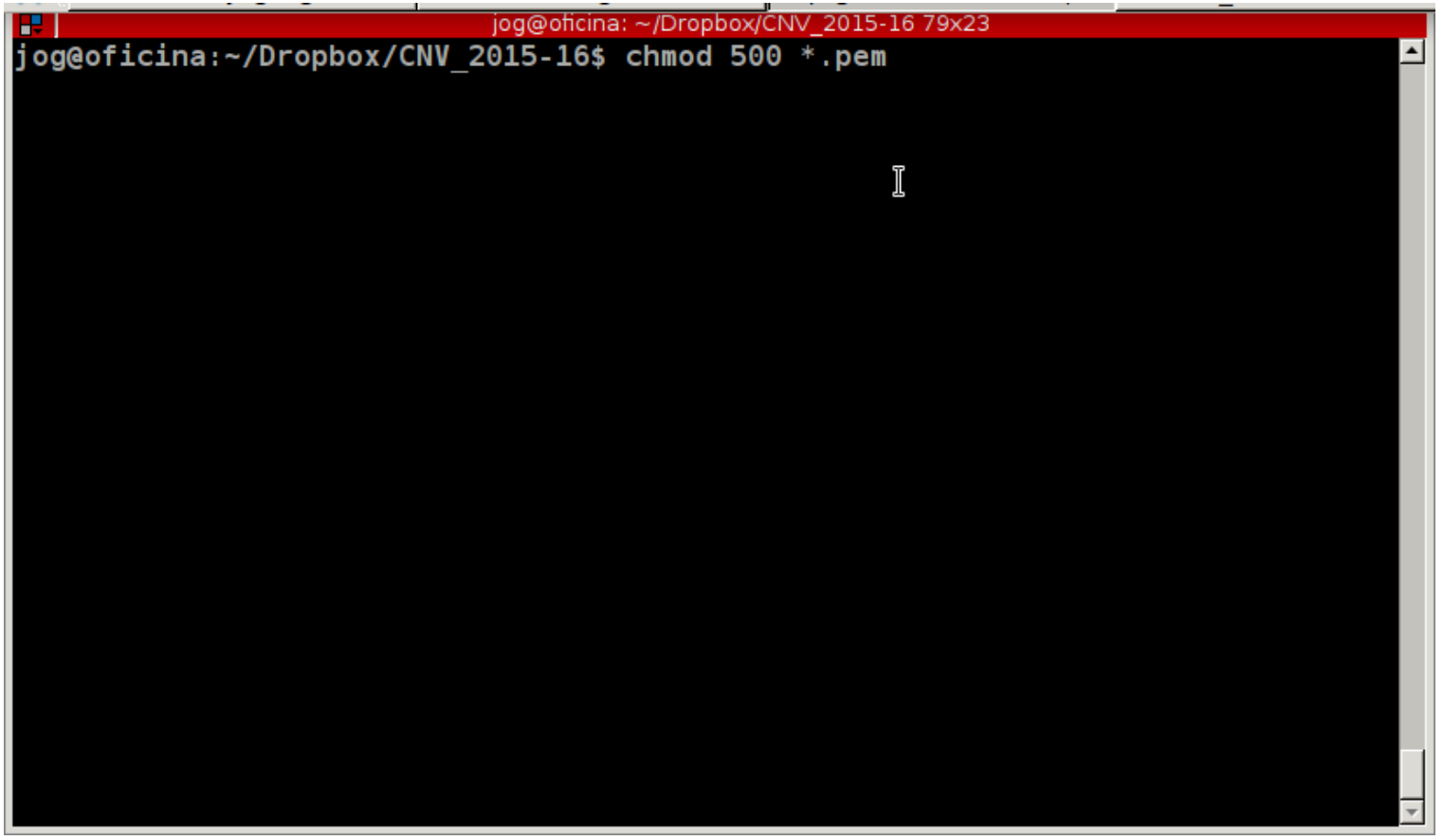
Check starting instances



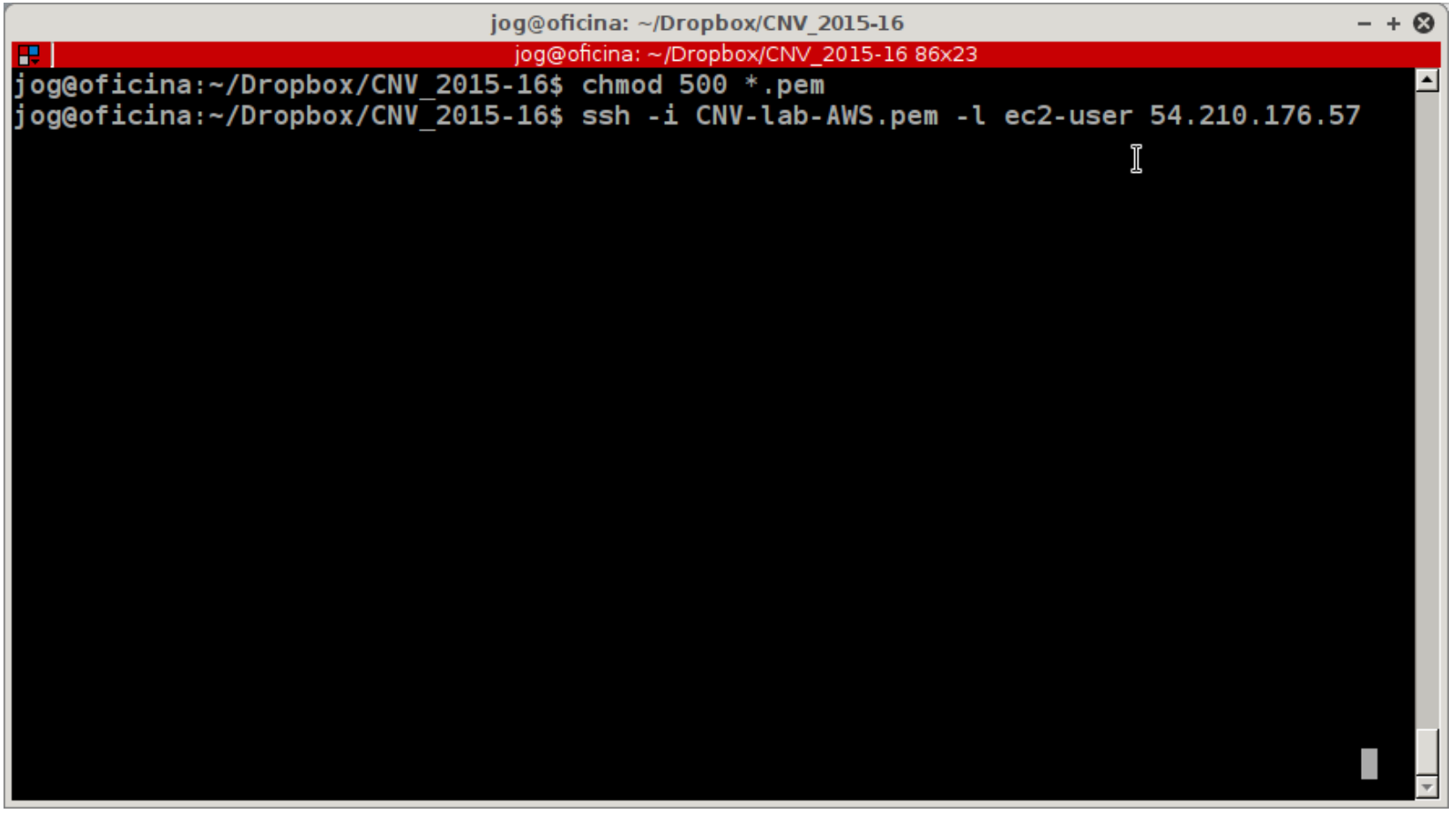
Now it's running!!



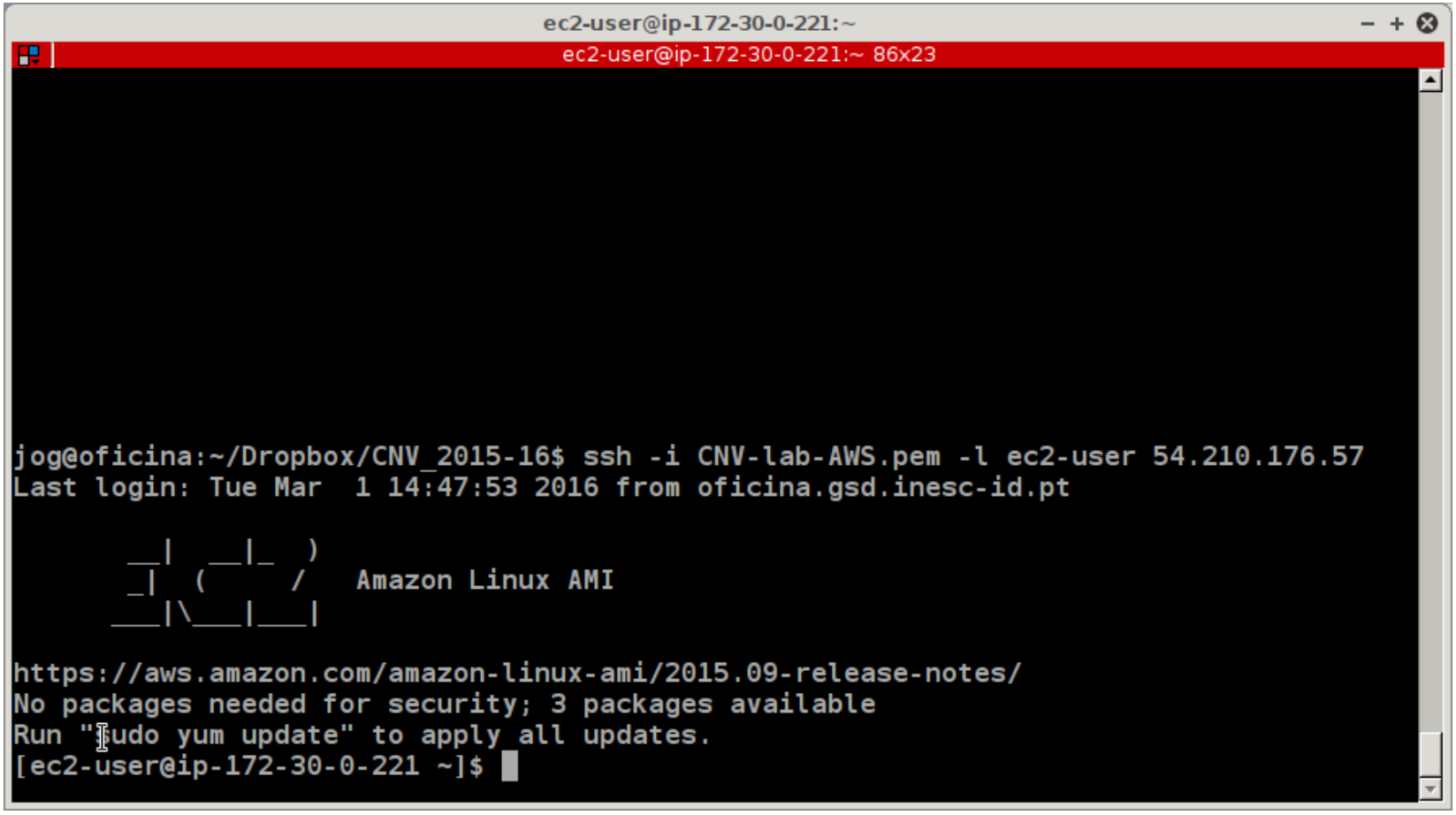
Decrease permissions on key



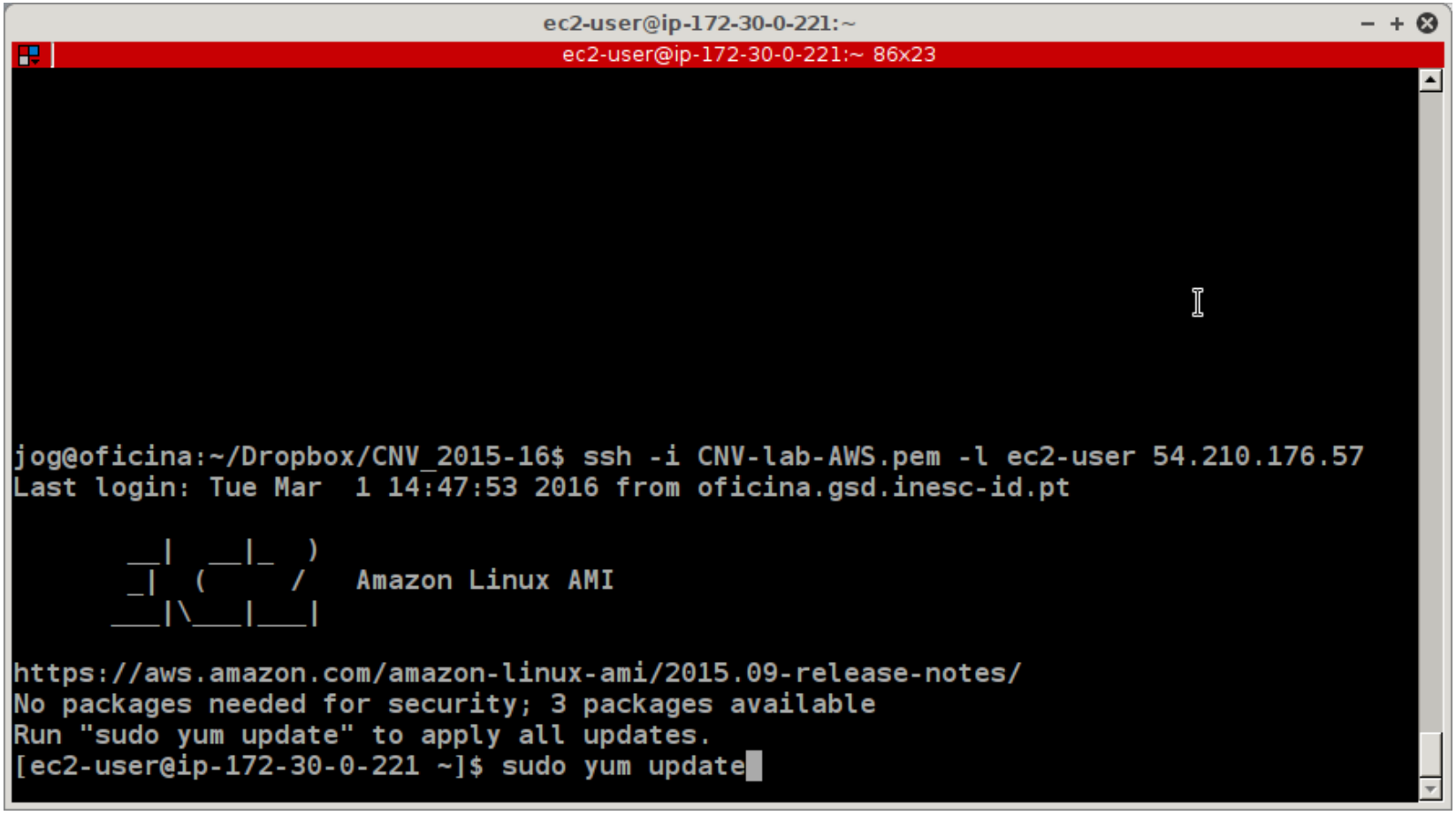
Ssh into instance



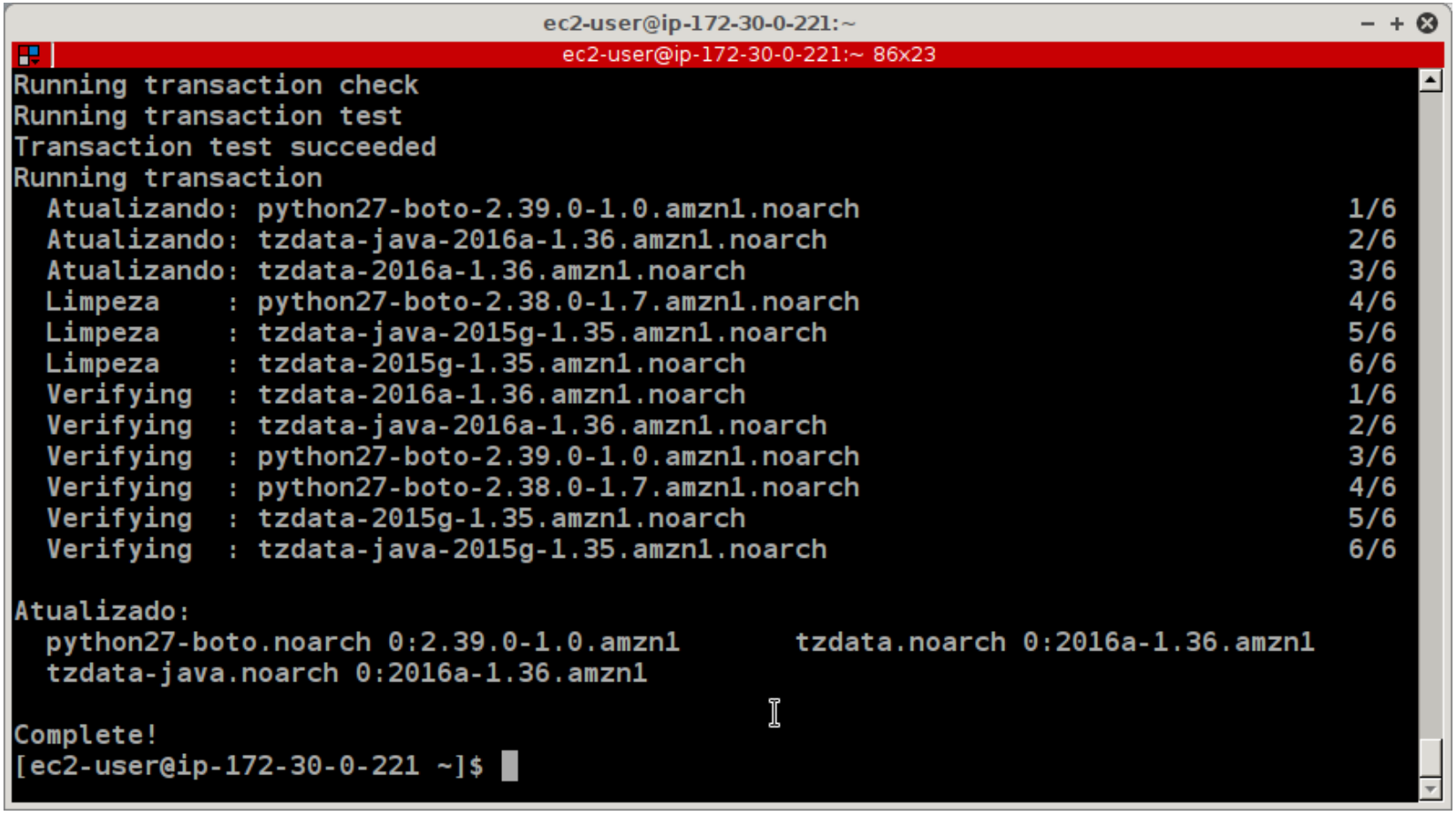
Logged in!


ec2-user@ip-172-30-0-221:~
ec2-user@ip-172-30-0-221:~ 86x23
jog@oficina:~/Dropbox/CNV_2015-16$ ssh -i CNV-lab-AWS.pem -l ec2-user 54.210.176.57
Last login: Tue Mar 1 14:47:53 2016 from oficina.gsd.inesc-id.pt
__| __|_)
_| (/   Amazon Linux AMI
___|___|___|
https://aws.amazon.com/amazon-linux-ami/2015.09-release-notes/
No packages needed for security; 3 packages available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-30-0-221 ~]$

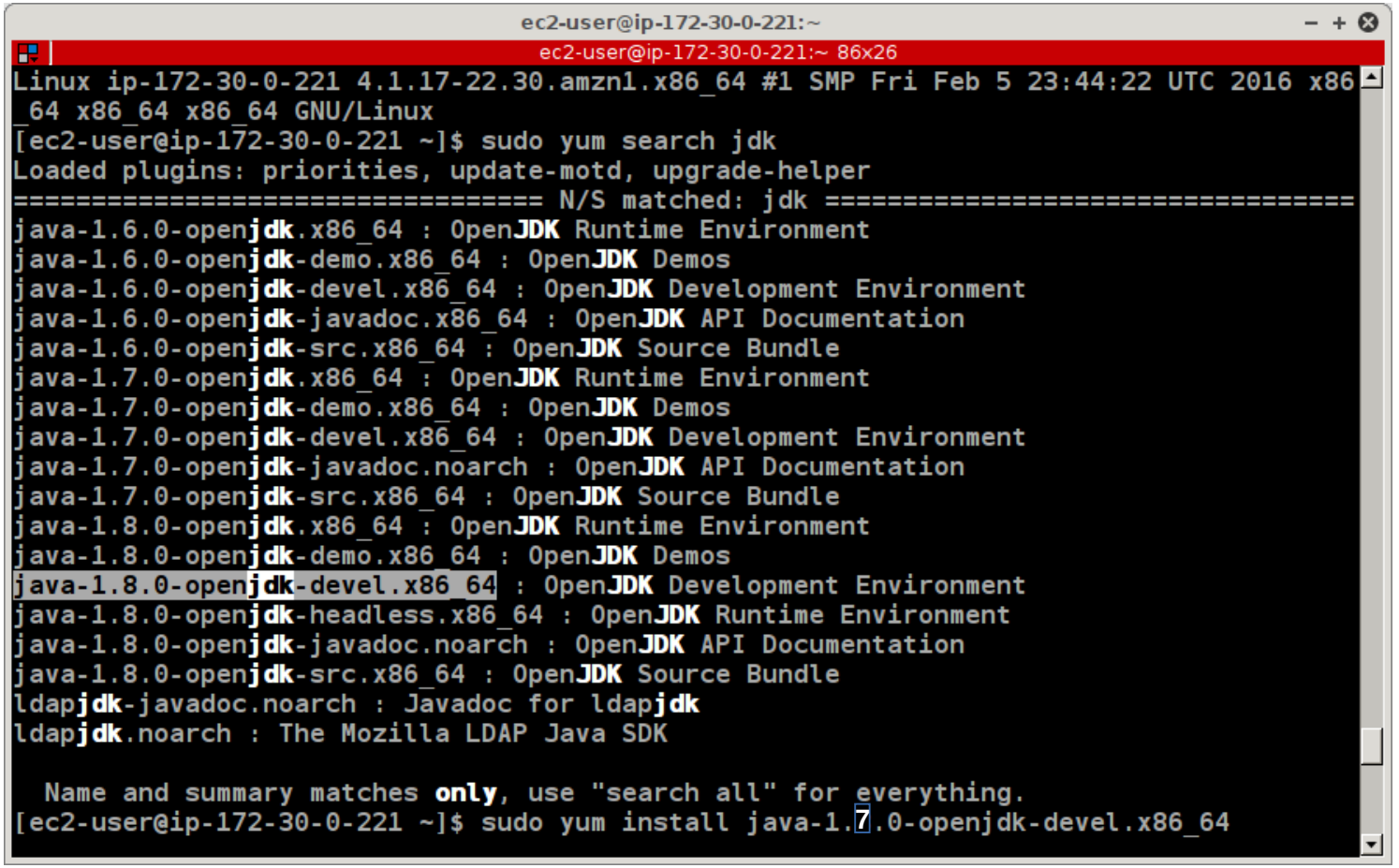
Update packages



Updated!


ec2-user@ip-172-30-0-221:~
ec2-user@ip-172-30-0-221:~ 86x23
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
Atualizando: python27-boto-2.39.0-1.0.amzn1.noarch 1/6
Atualizando: tzdata-java-2016a-1.36.amzn1.noarch 2/6
Atualizando: tzdata-2016a-1.36.amzn1.noarch 3/6
Limpeza : python27-boto-2.38.0-1.7.amzn1.noarch 4/6
Limpeza : tzdata-java-2015g-1.35.amzn1.noarch 5/6
Limpeza : tzdata-2015g-1.35.amzn1.noarch 6/6
Verifying : tzdata-2016a-1.36.amzn1.noarch 1/6
Verifying : tzdata-java-2016a-1.36.amzn1.noarch 2/6
Verifying : python27-boto-2.39.0-1.0.amzn1.noarch 3/6
Verifying : python27-boto-2.38.0-1.7.amzn1.noarch 4/6
Verifying : tzdata-2015g-1.35.amzn1.noarch 5/6
Verifying : tzdata-java-2015g-1.35.amzn1.noarch 6/6
Atualizado:
python27-boto.noarch 0:2.39.0-1.0.amzn1 tzdata.noarch 0:2016a-1.36.amzn1
tzdata-java.noarch 0:2016a-1.36.amzn1
Complete!
[ec2-user@ip-172-30-0-221 ~]$

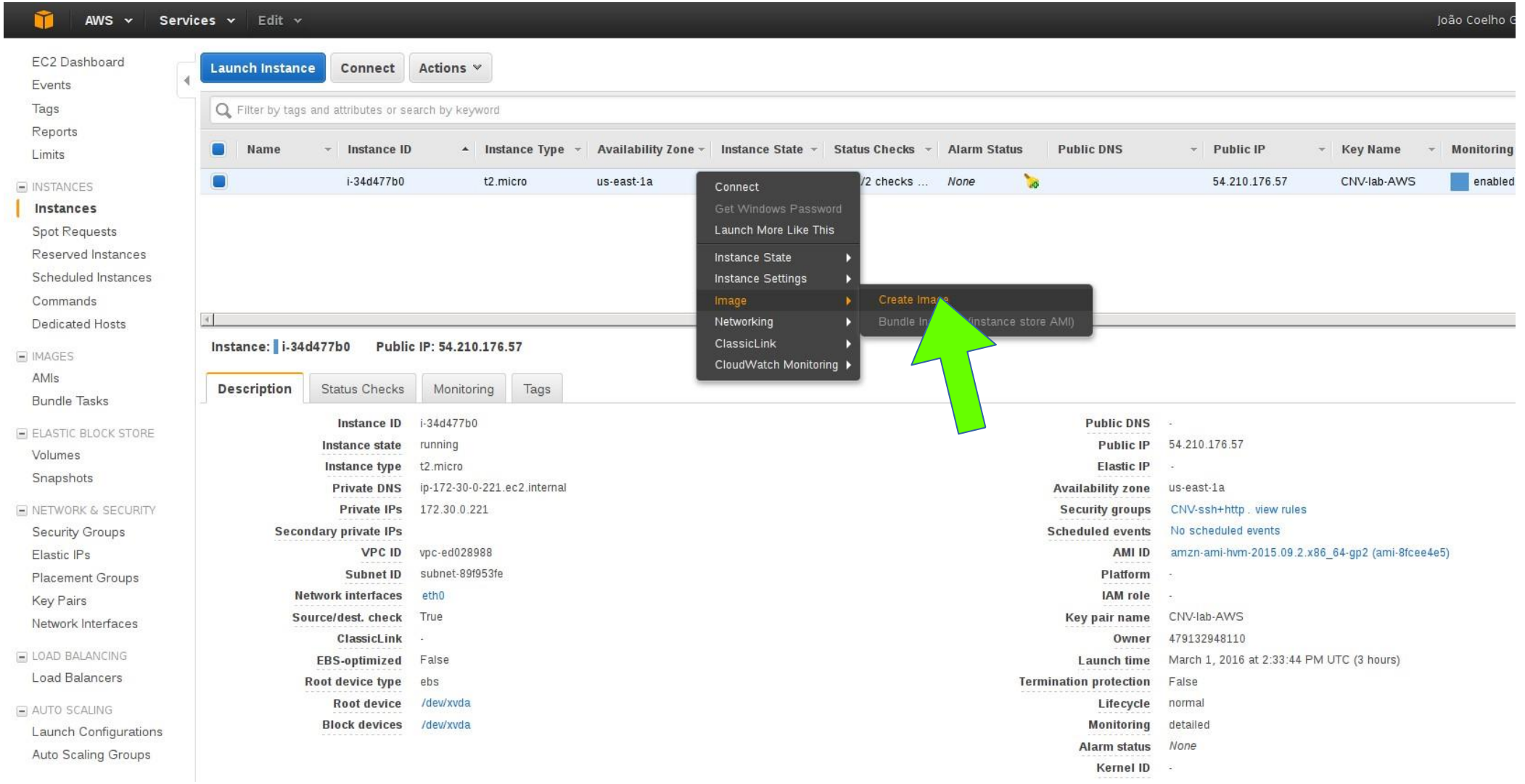
Install Java SDK



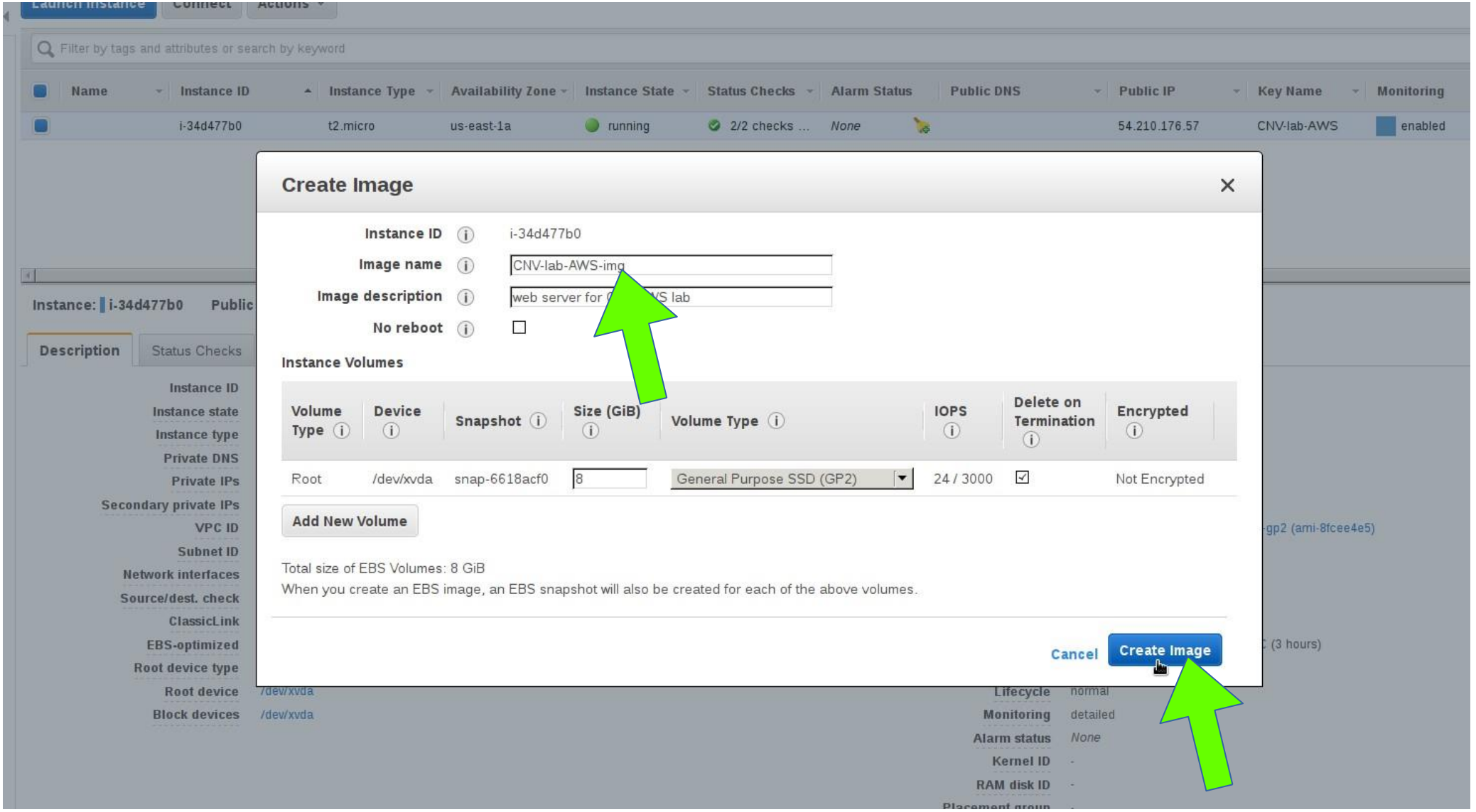
Setup your Application Software

- At this point, setup up the Java application that will be used (transfer it using scp or develop it at the AWS instance directly)
- Don't forget to make sure that the application server is running at startup, e.g. by launching it inside /etc/rc.local or an equivalent mechanism
- e.g., java -cp ~ec2-user WebServer
- *(you will need sudo rights)*

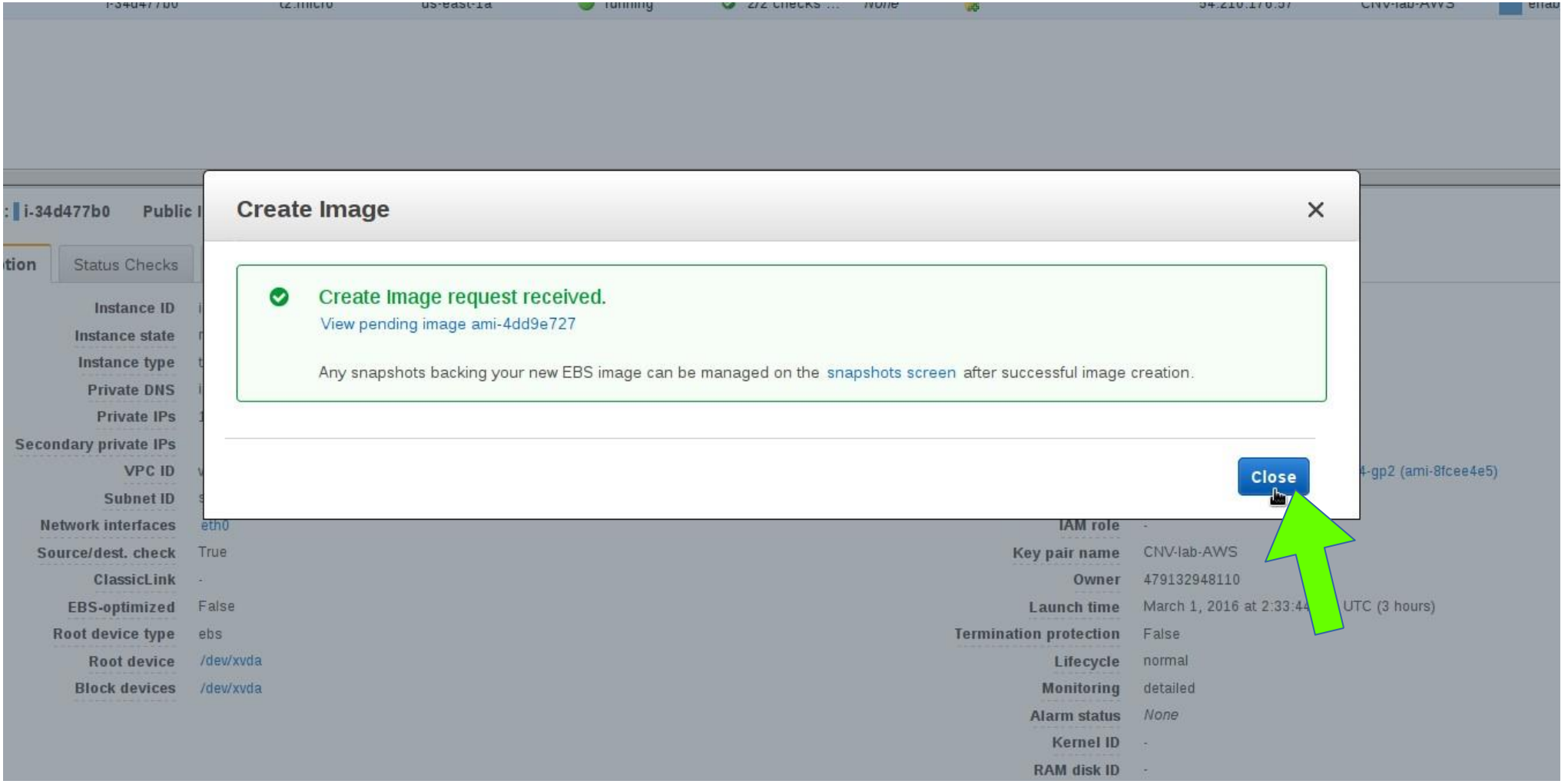
Once the web server is running at startup (e.g. /etc/rc.local), create image.



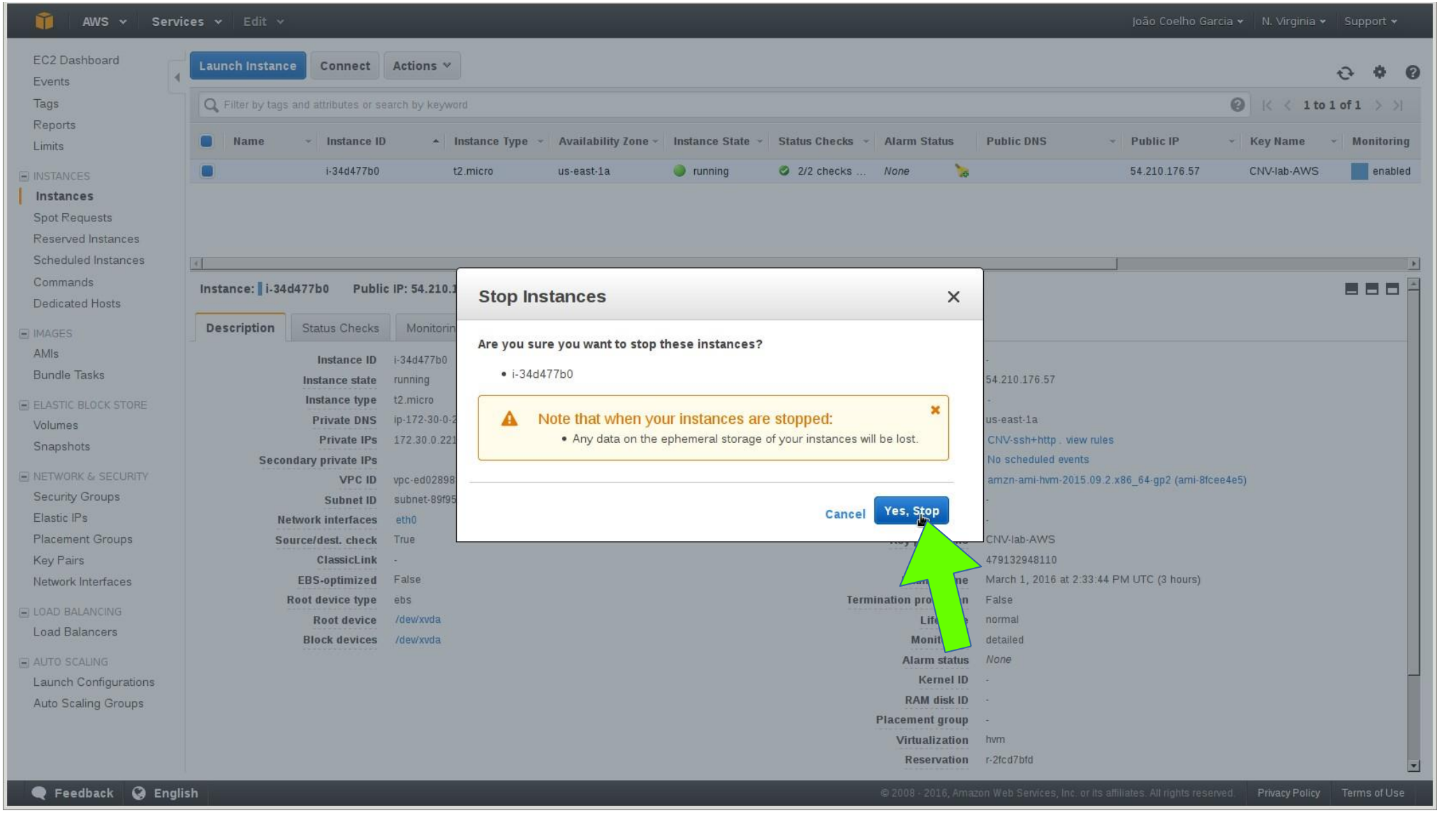
Give it a name and create it



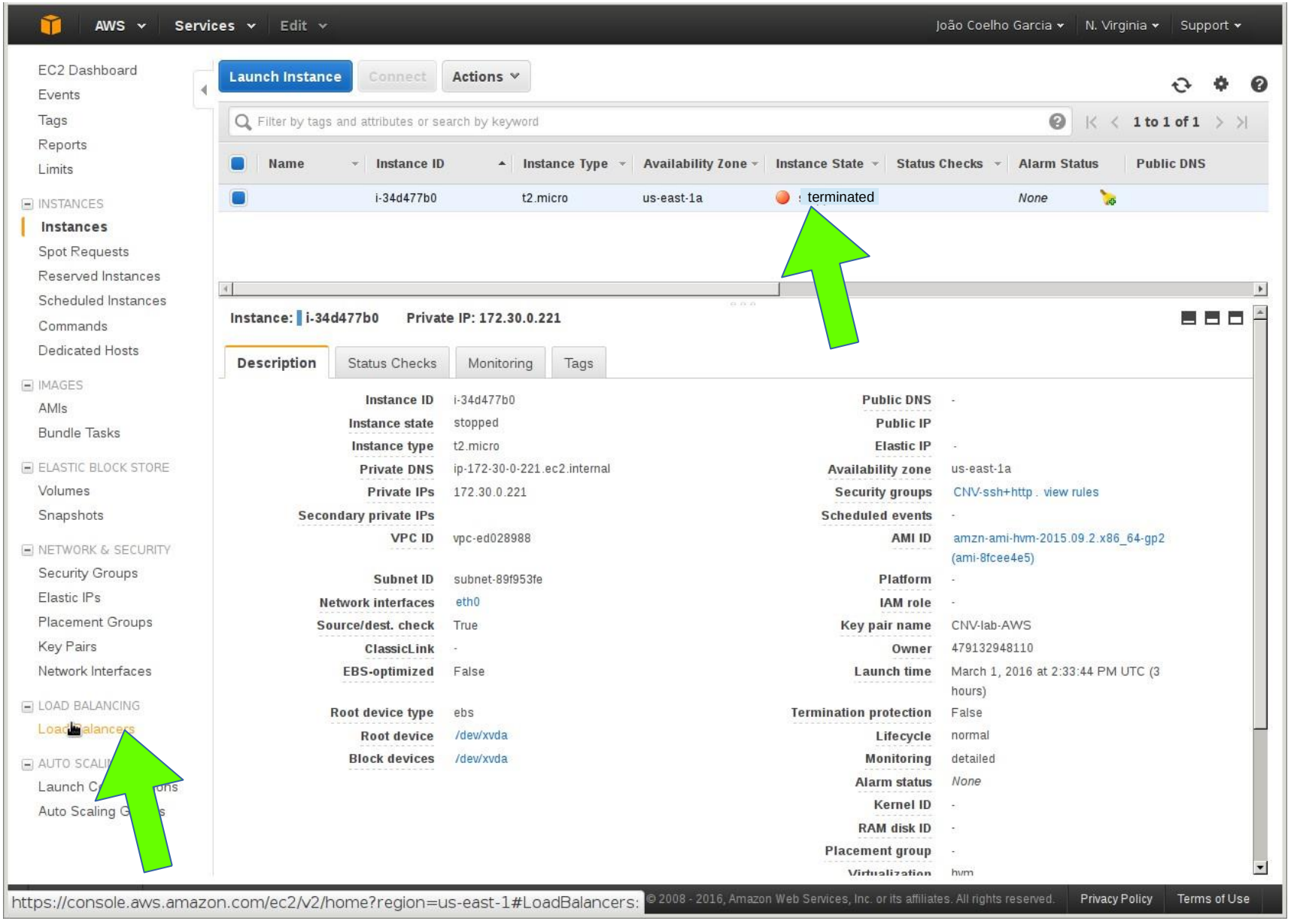
It may take a litle time for the request to be fulfilled



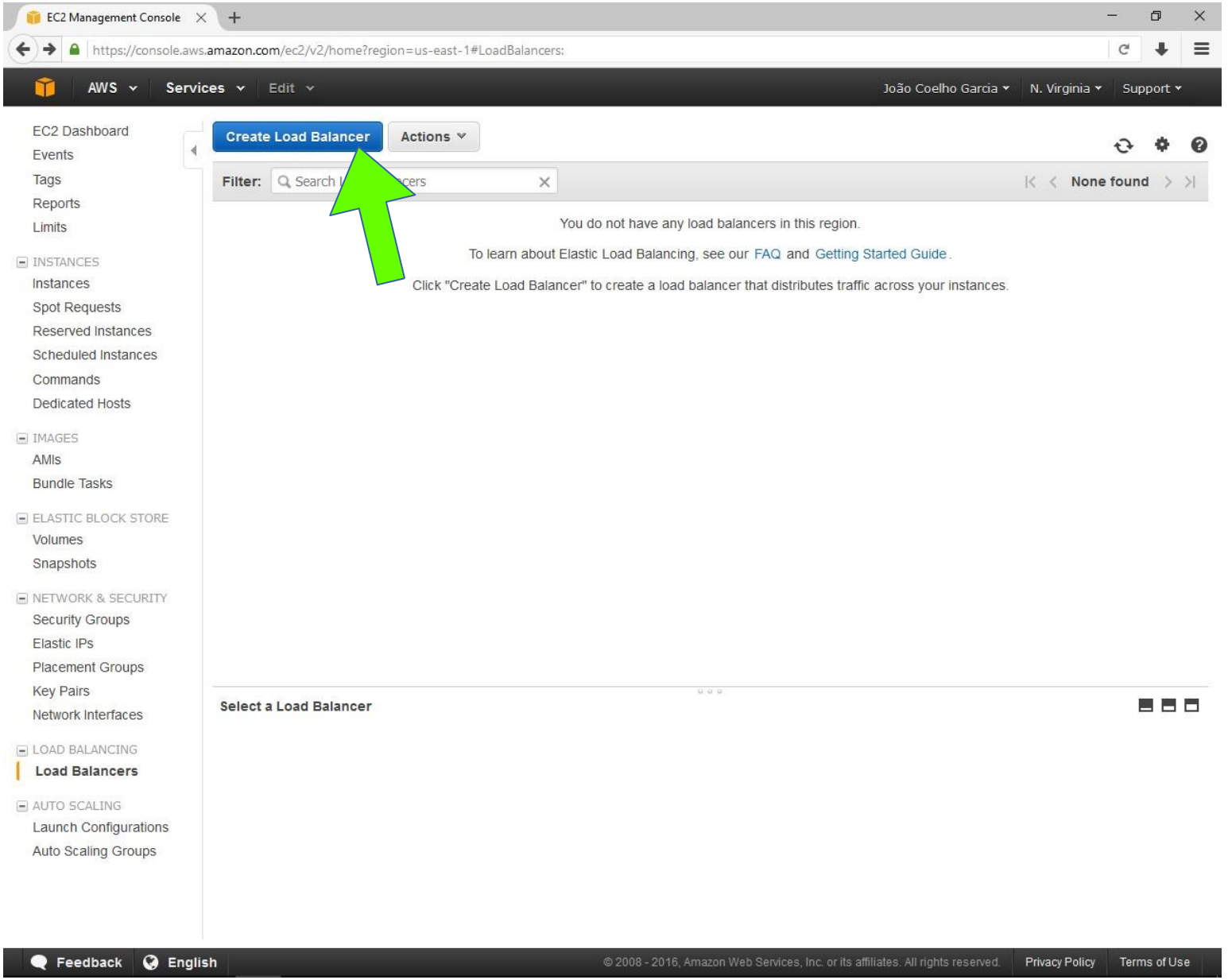
Once the image is created, right click the instance and **terminate** it.



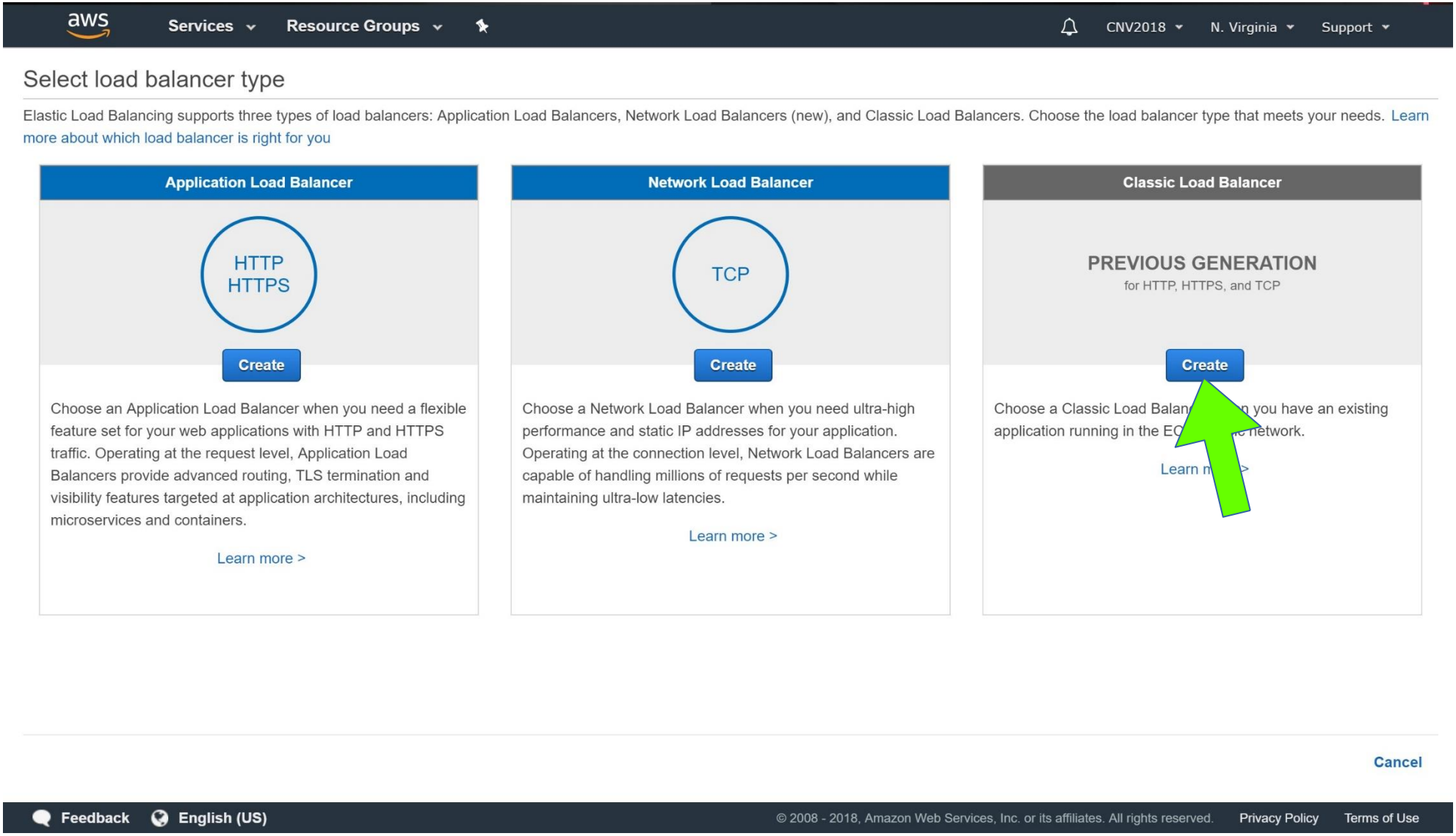
It's terminated…
Let's create a load balancer...



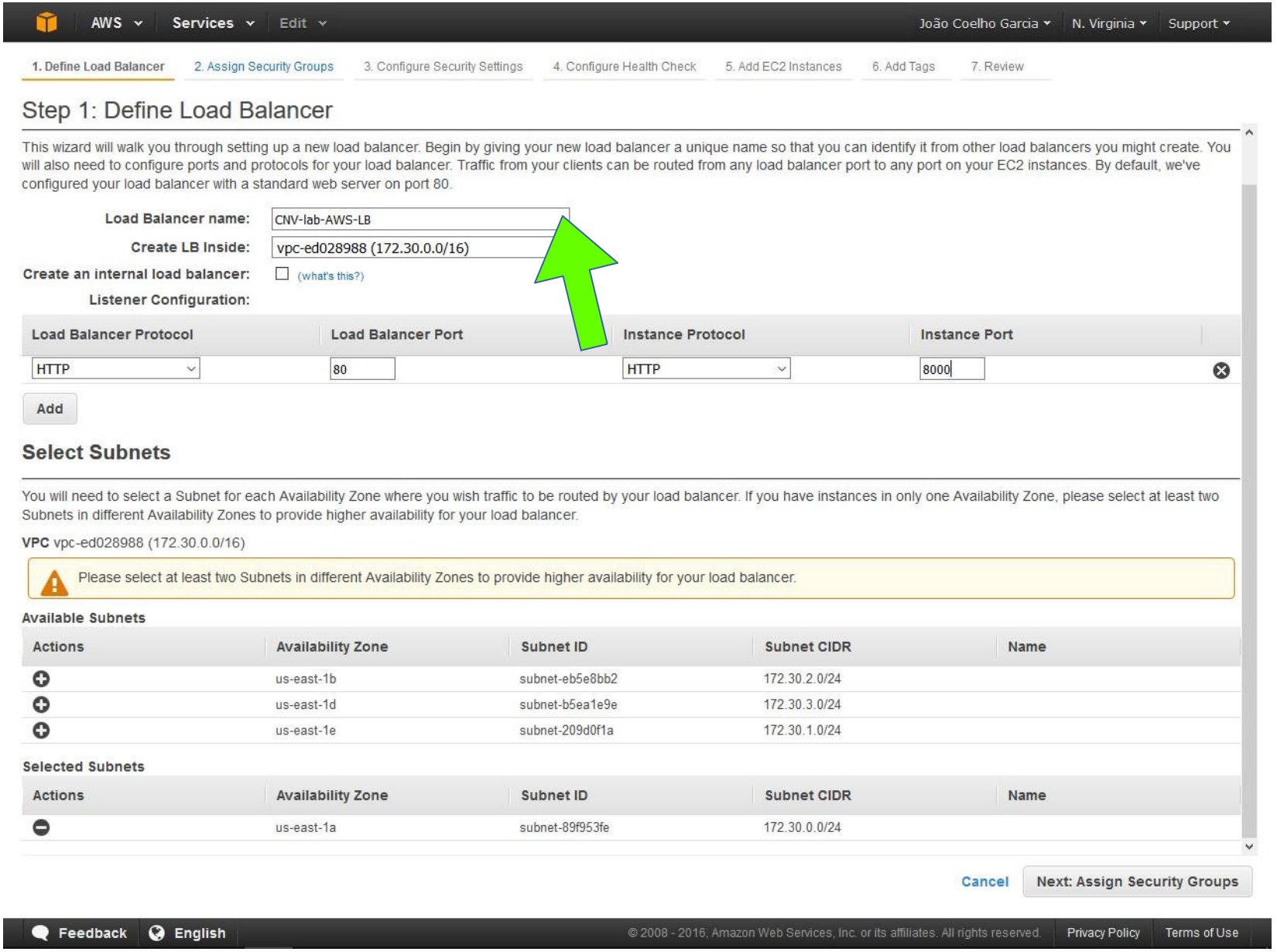
Click on create...



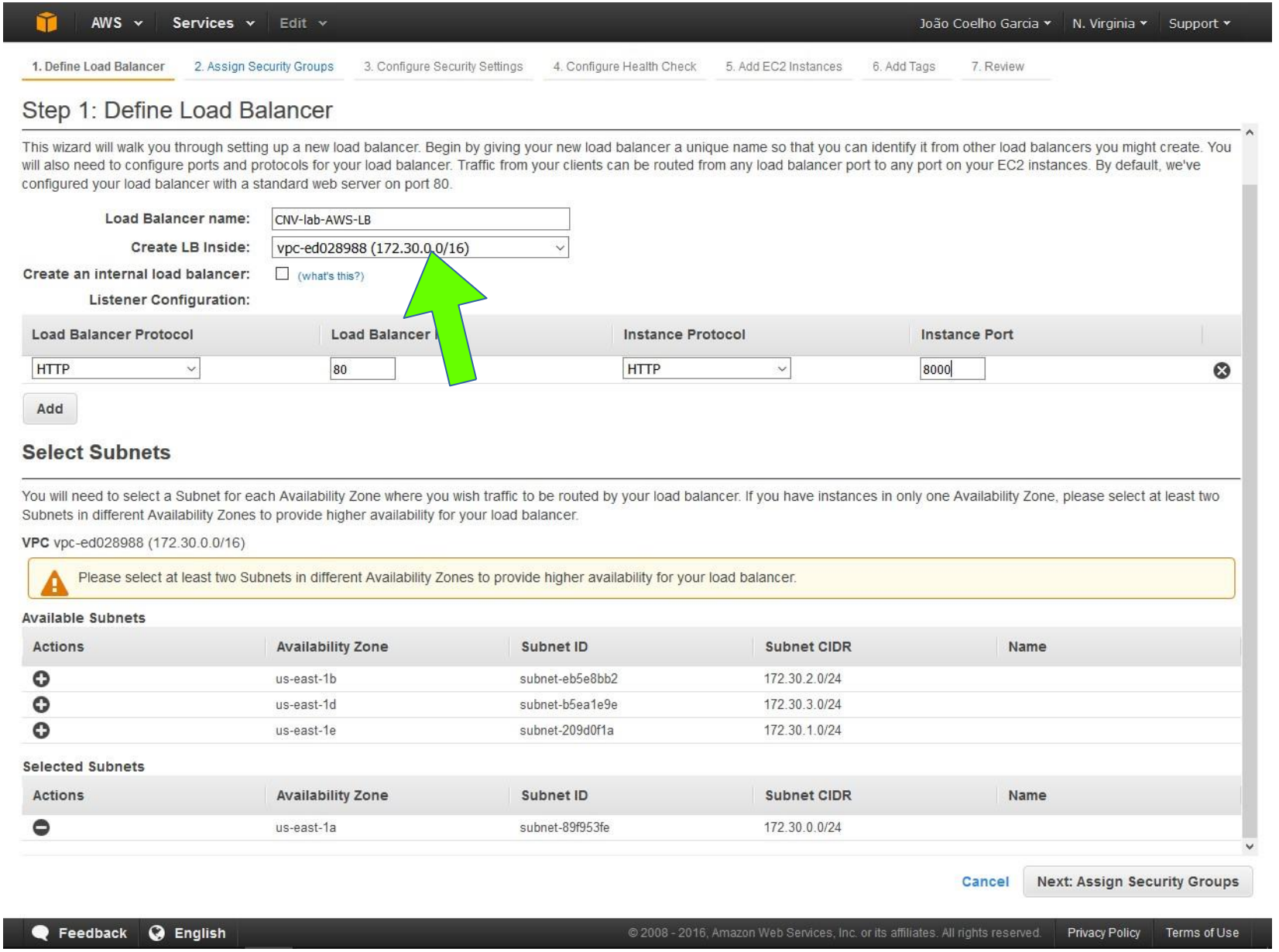
Pick a classic Load Balancer



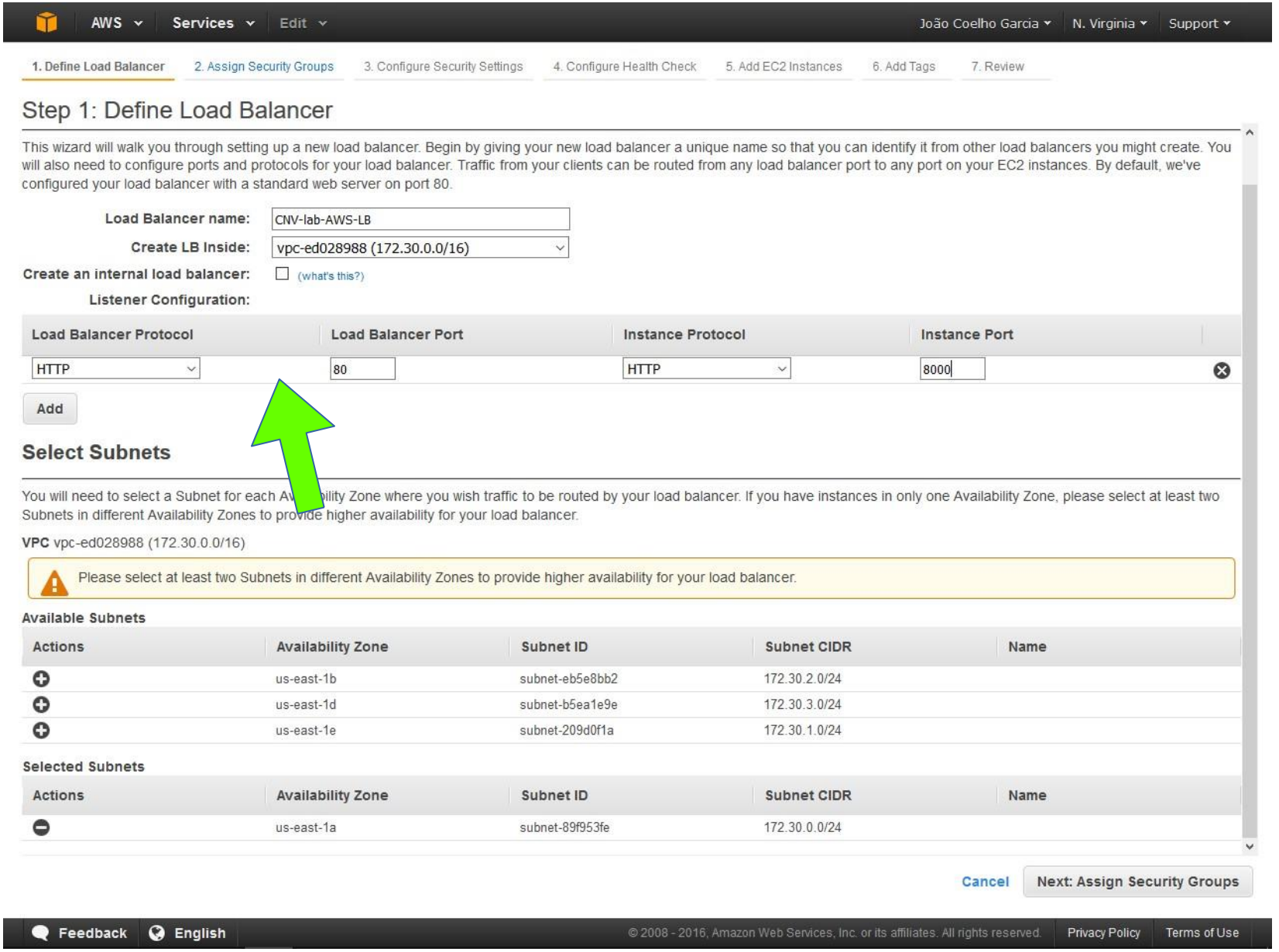
Give it a name..



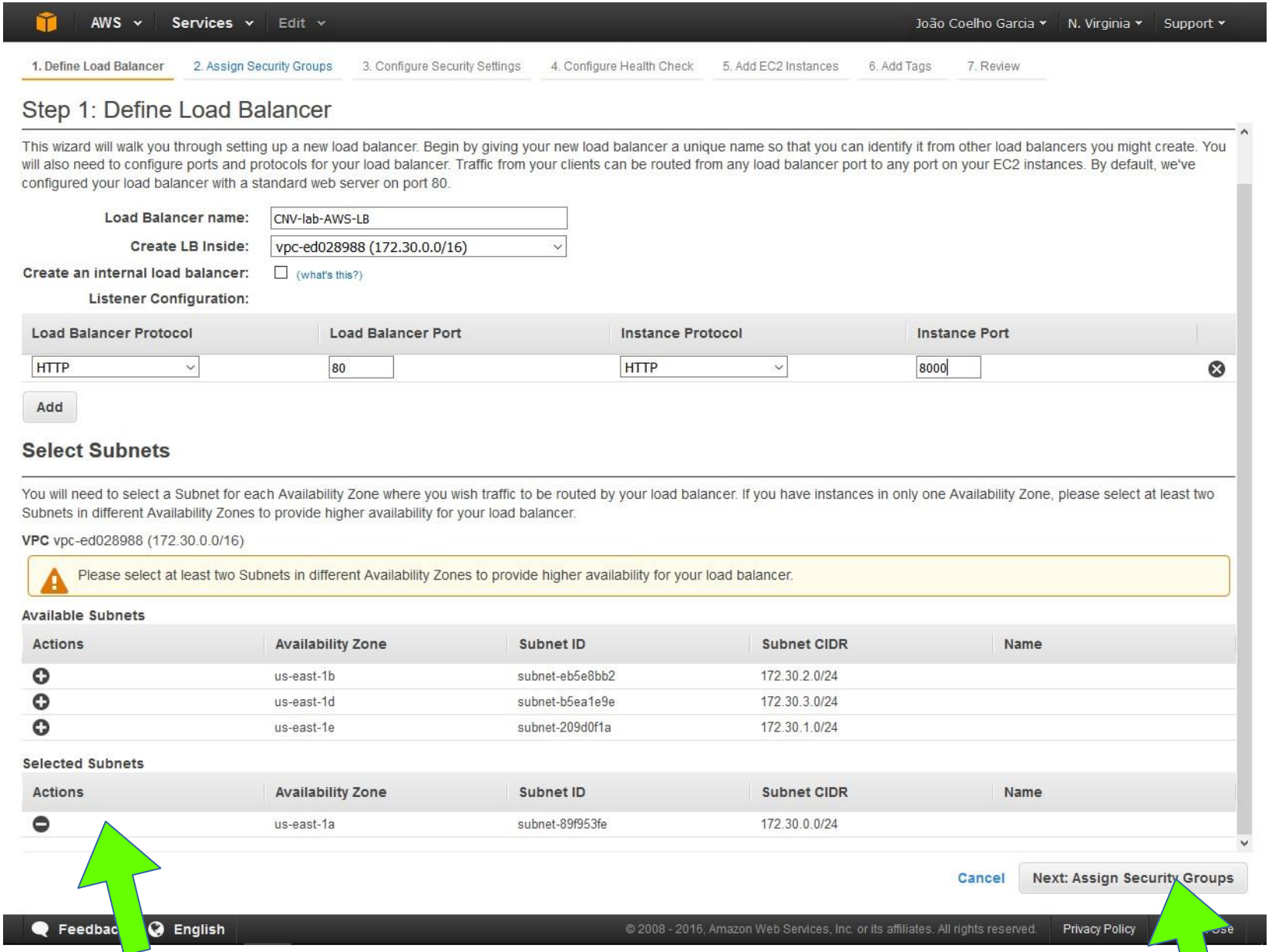
Create it inside your default VPC



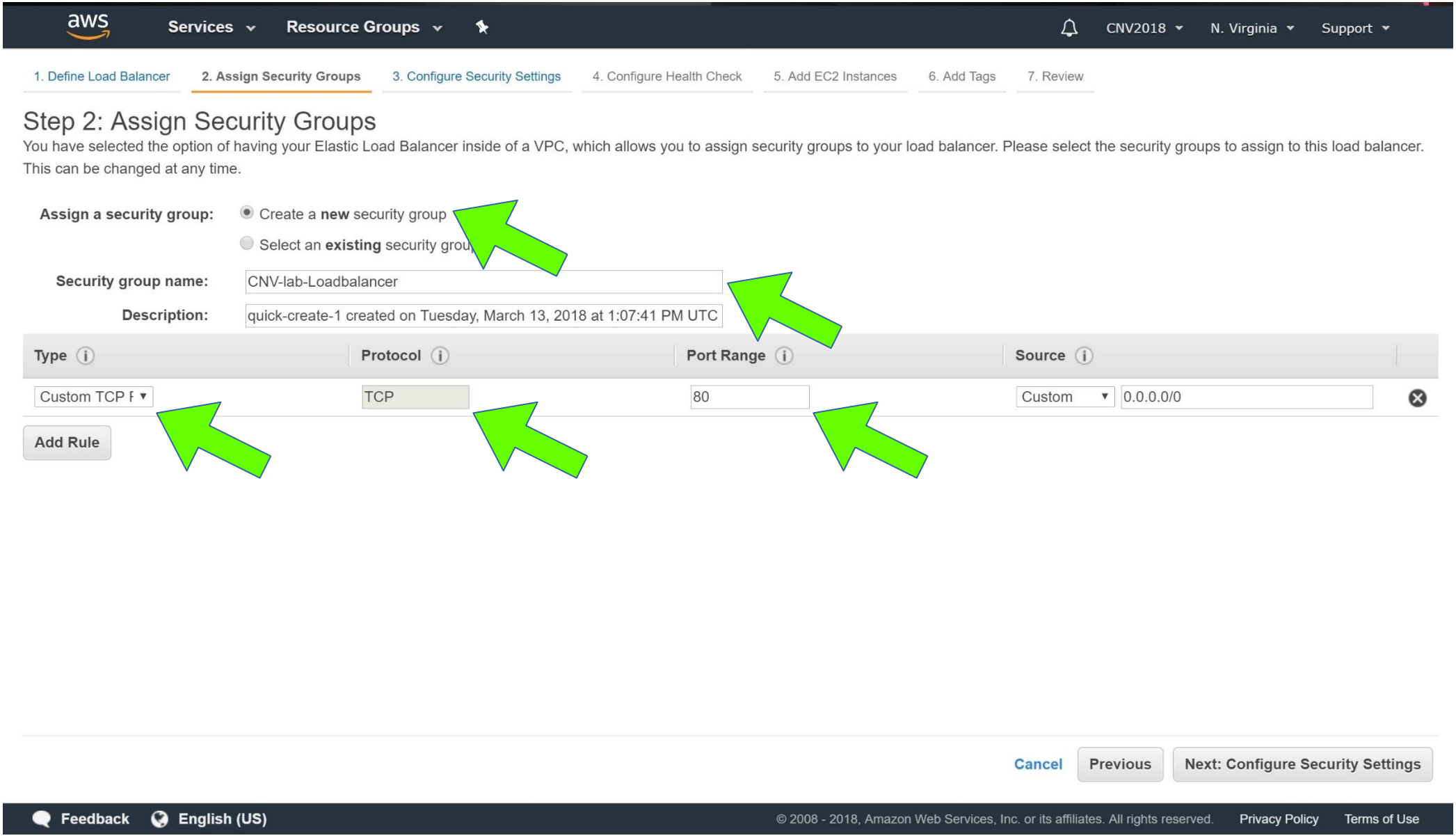
Connect external and internal traffic



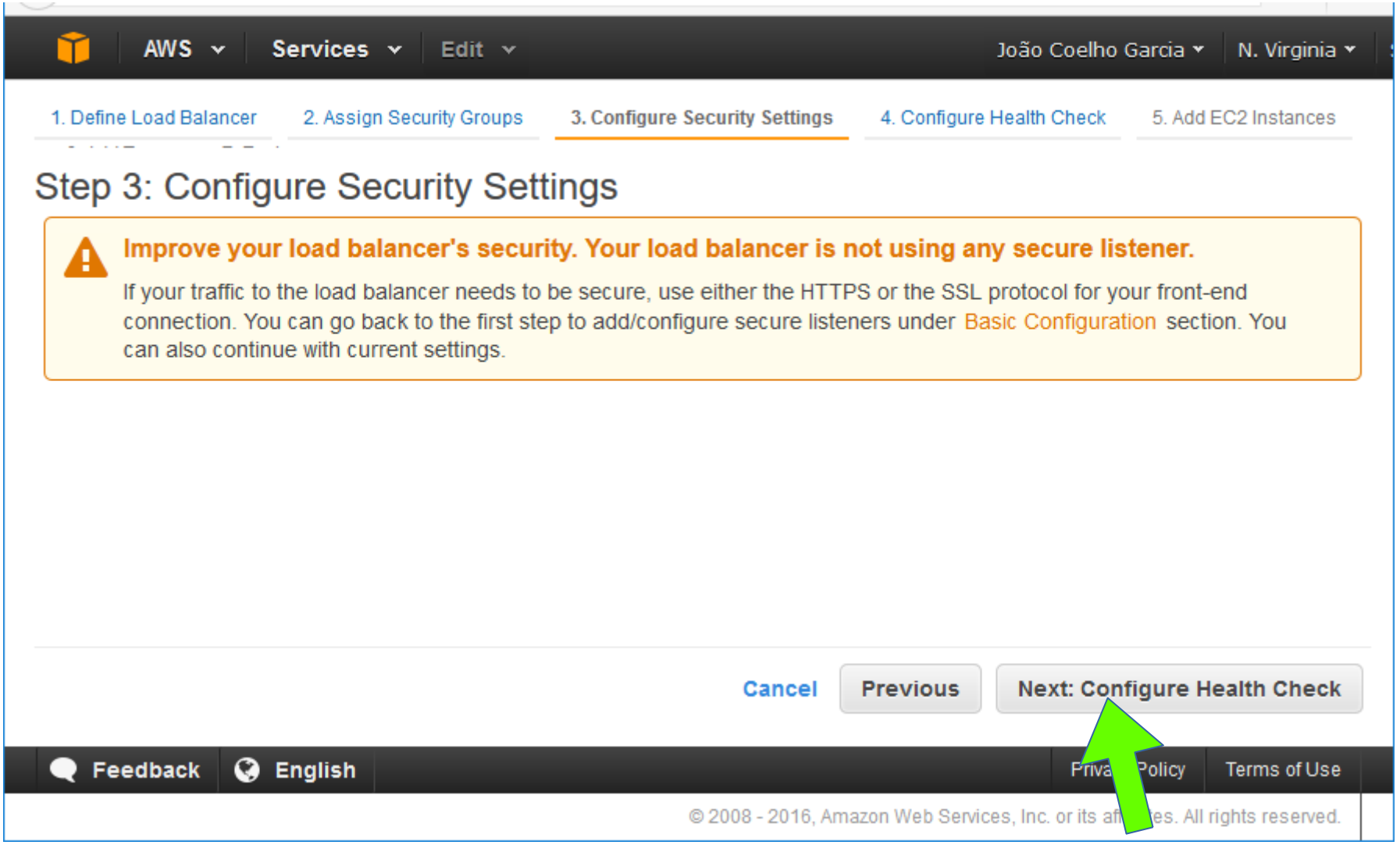
Add a subnet


AWS
Services
Edit
João Coelho Garcia
N. Virginia
Support
1. Define Load Balancer
2. Assign Security Groups
3. Configure Security Settings
4. Configure Health Check
5. Add EC2 Instances
6. Add Tags
7. Review
Step 1: Define Load Balancer
This wizard will walk you through setting up a new load balancer. Begin by giving your new load balancer a unique name so that you can identify it from other load balancers you might create. You will also need to configure ports and protocols for your load balancer. Traffic from your clients can be routed from any load balancer port to any port on your EC2 instances. By default, we've configured your load balancer with a standard web server on port 80.
Load Balancer name:
CNV-lab-AWS-LB
Create LB Inside:
vpc-ed028988 (172.30.0.0/16)
Create an internal load balancer:
(what's this?)
Listener Configuration:
Load Balancer Protocol
Load Balancer Port
Instance Protocol
Instance Port
HTTP
80
HTTP
8000
Add
Select Subnets
You will need to select a Subnet for each Availability Zone where you wish traffic to be routed by your load balancer. If you have instances in only one Availability Zone, please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.
VPC vpc-ed028988 (172.30.0.0/16)
Please select at least two Subnets in different Availability Zones to provide higher availability for your load balancer.
Available Subnets
Actions
Availability Zone
Subnet ID
Subnet CIDR
Name
us-east-1b
subnet-eb5e8bb2
172.30.2.0/24
us-east-1d
subnet-b5ea1e9e
172.30.3.0/24
us-east-1e
subnet-209d0f1a
172.30.1.0/24
Selected Subnets
Actions
Availability Zone
Subnet ID
Subnet CIDR
Name
us-east-1a
subnet-89f953fe
172.30.0.0/24
Cancel
Next: Assign Security Groups
Feedback
English
© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy

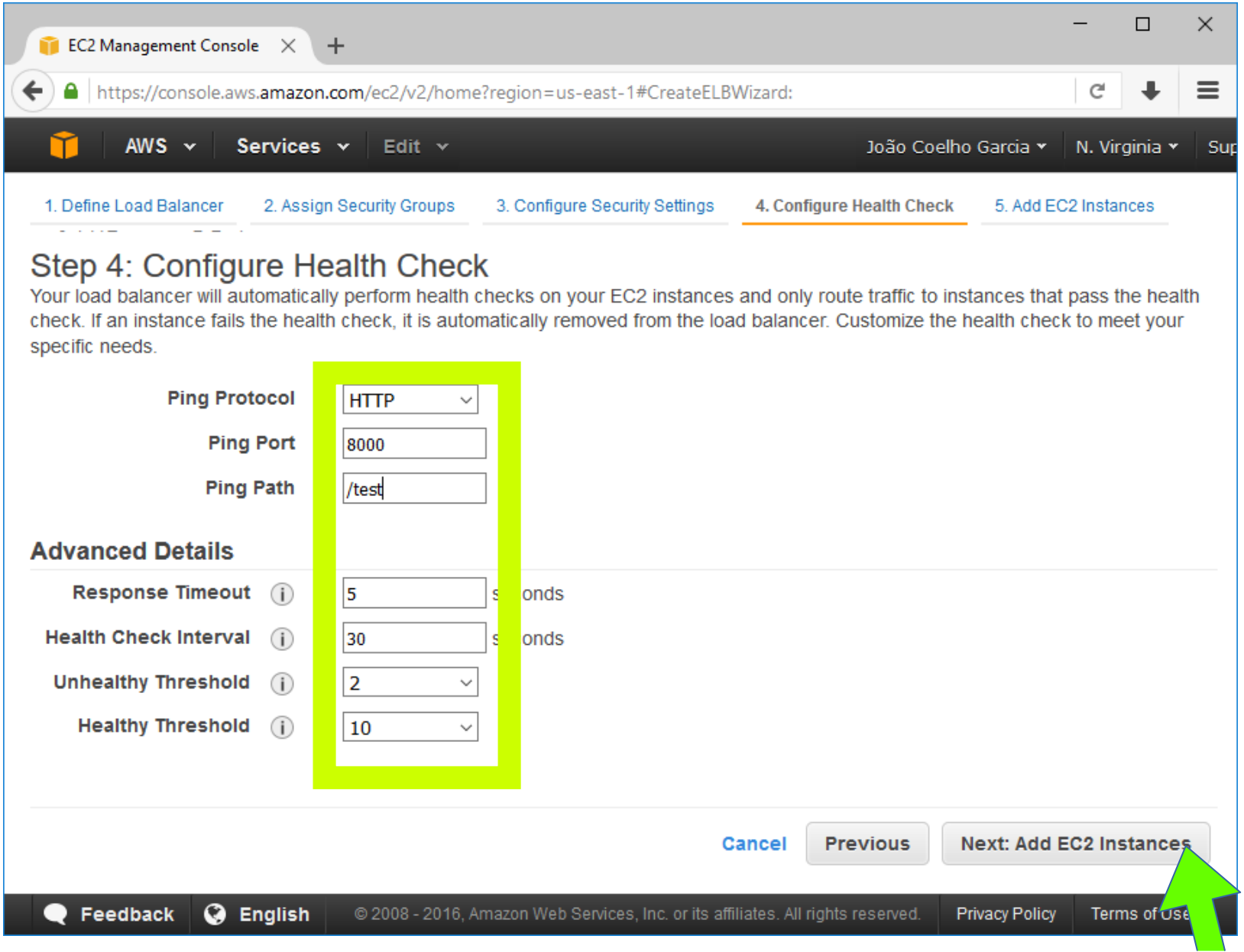
Create a New Security Group



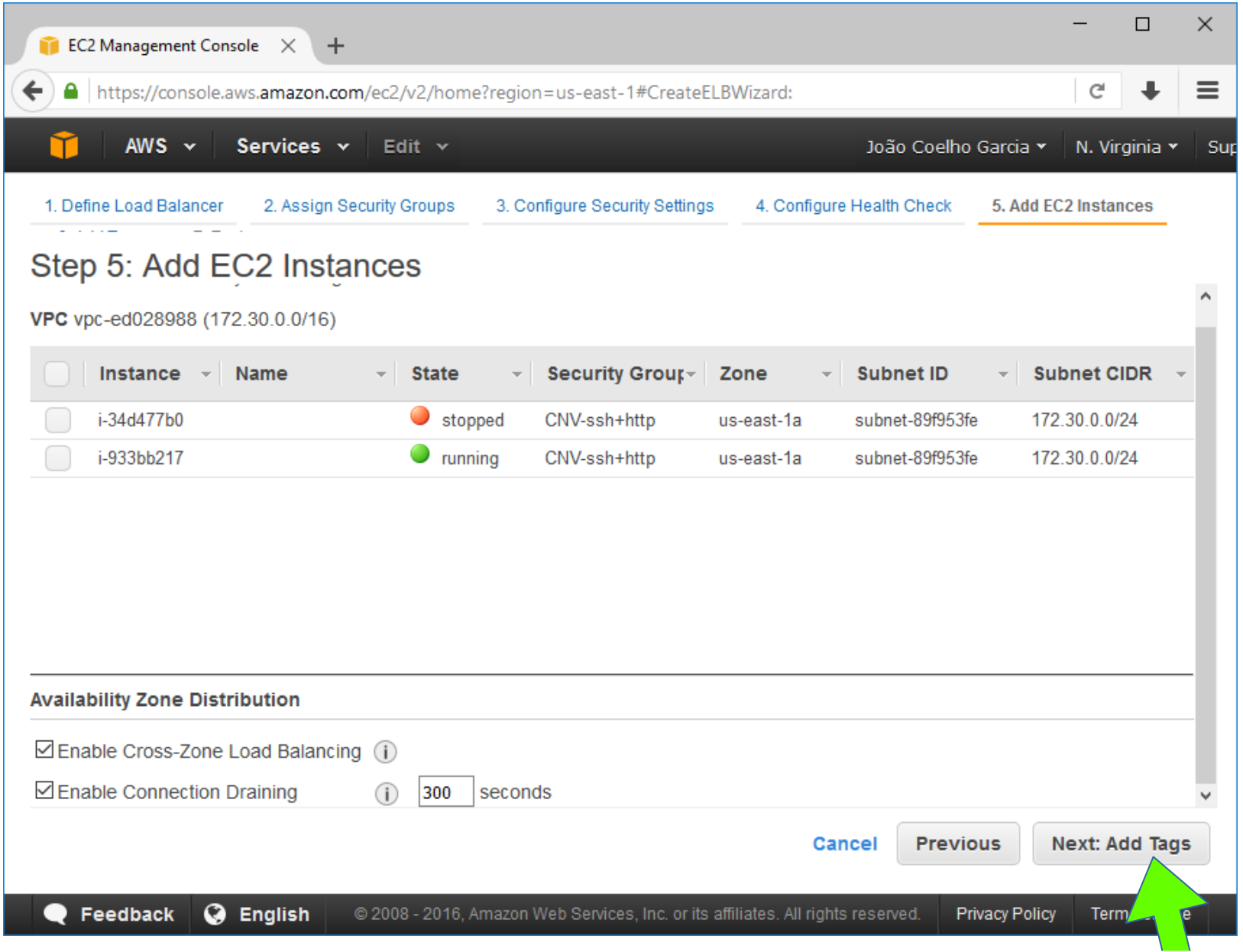
Ignore this warning..



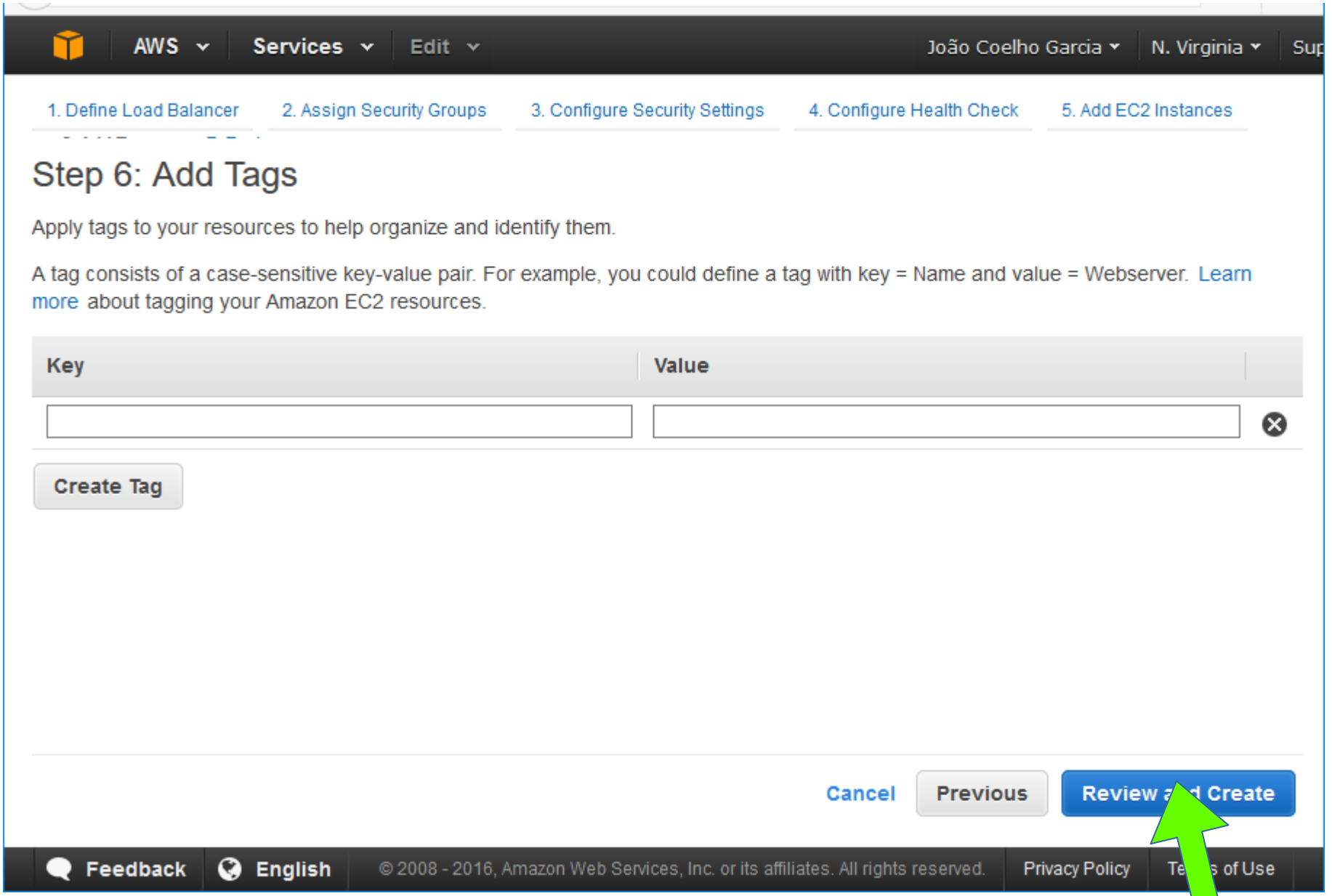
Configure the health check



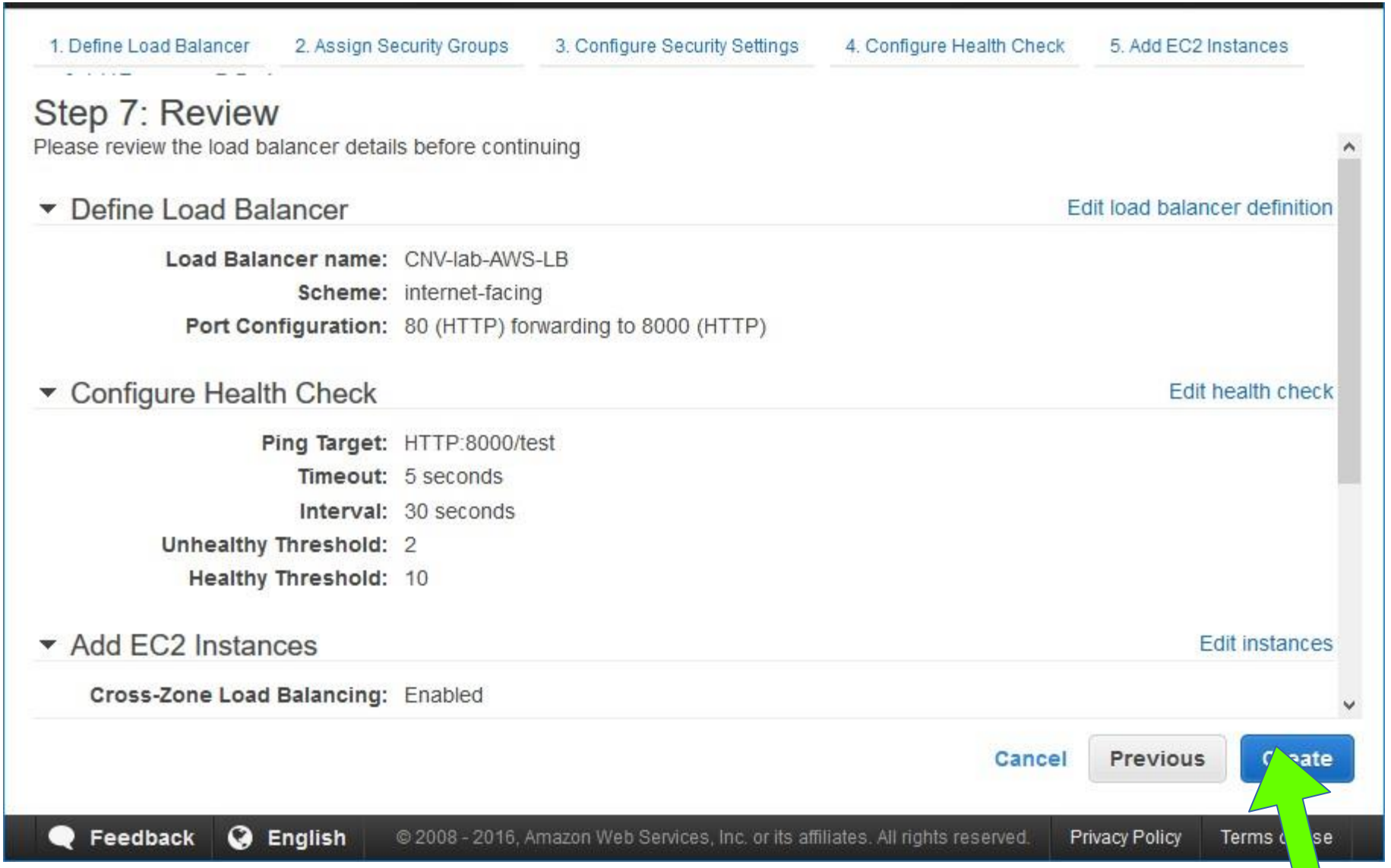
Don't add instances



You don't need tags



Review and Create



Load Balancer Creation Status

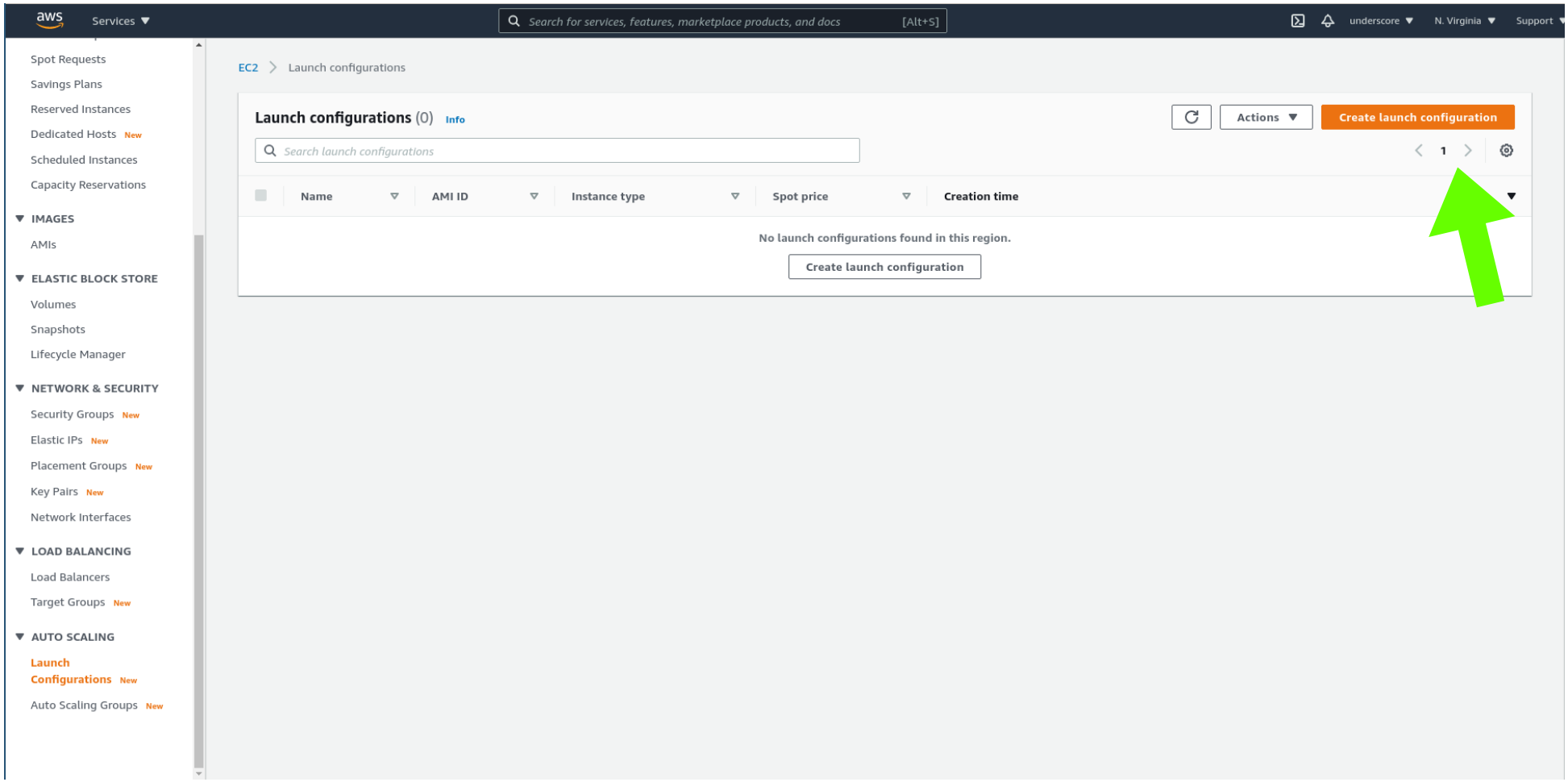
Successfully crea1ed load balancer

Load balancer CPI*,'-lab-A .'S-LB as success fuIlY created

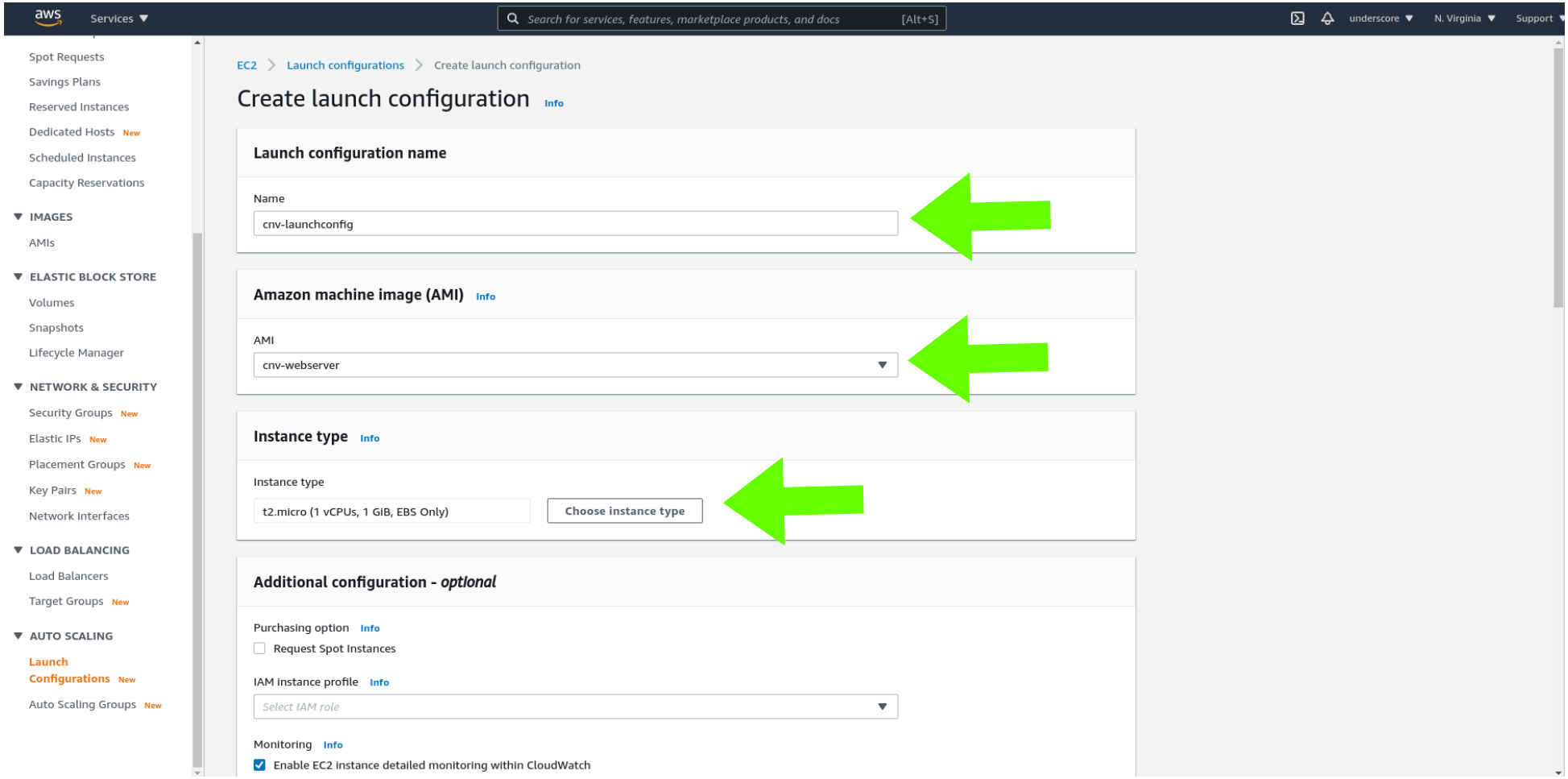
LJote It maV taKe a fe. minutes for Your instant es to become active in the ne. load balanc er

Close

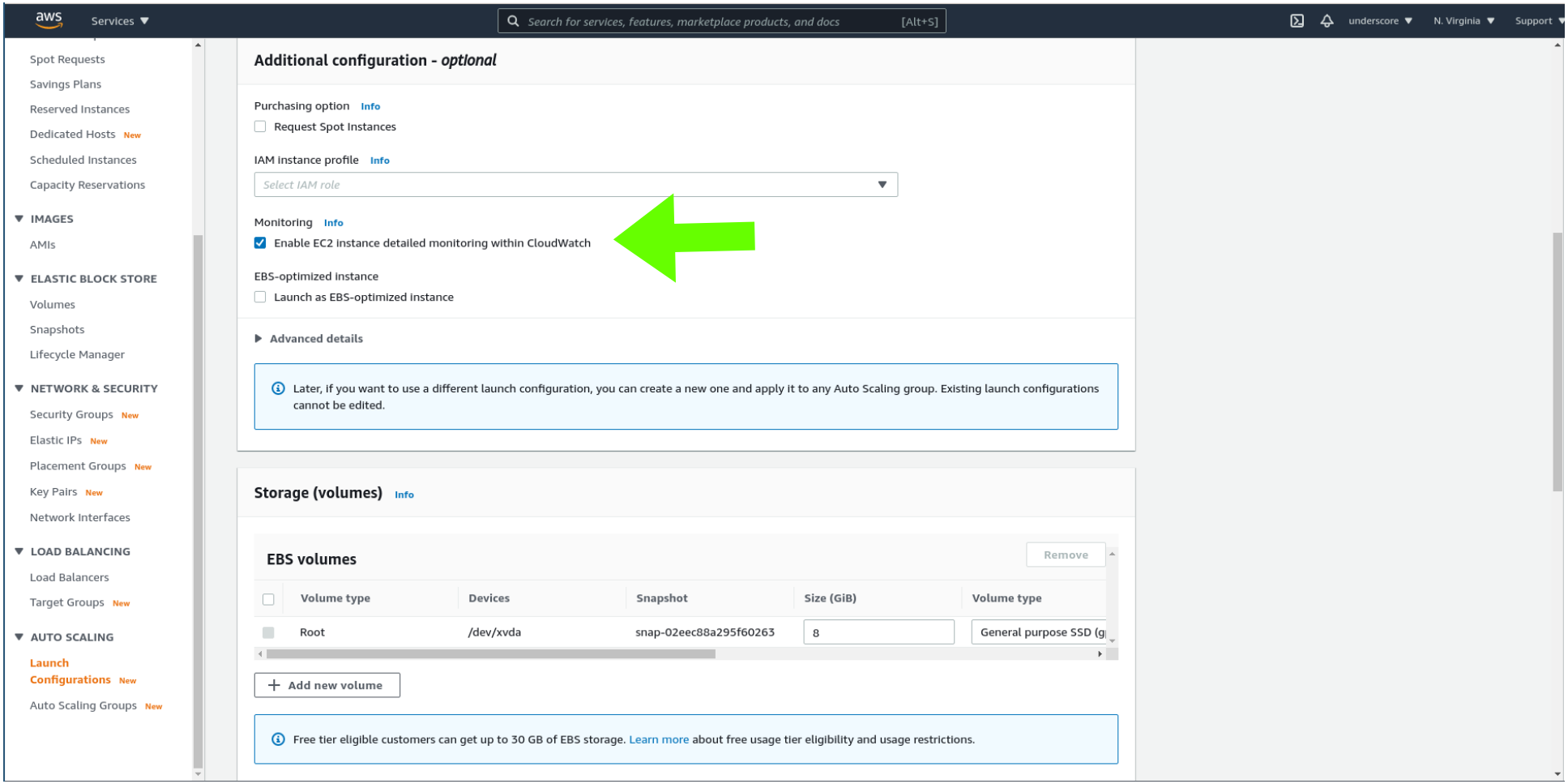
Create a Launch Configuration



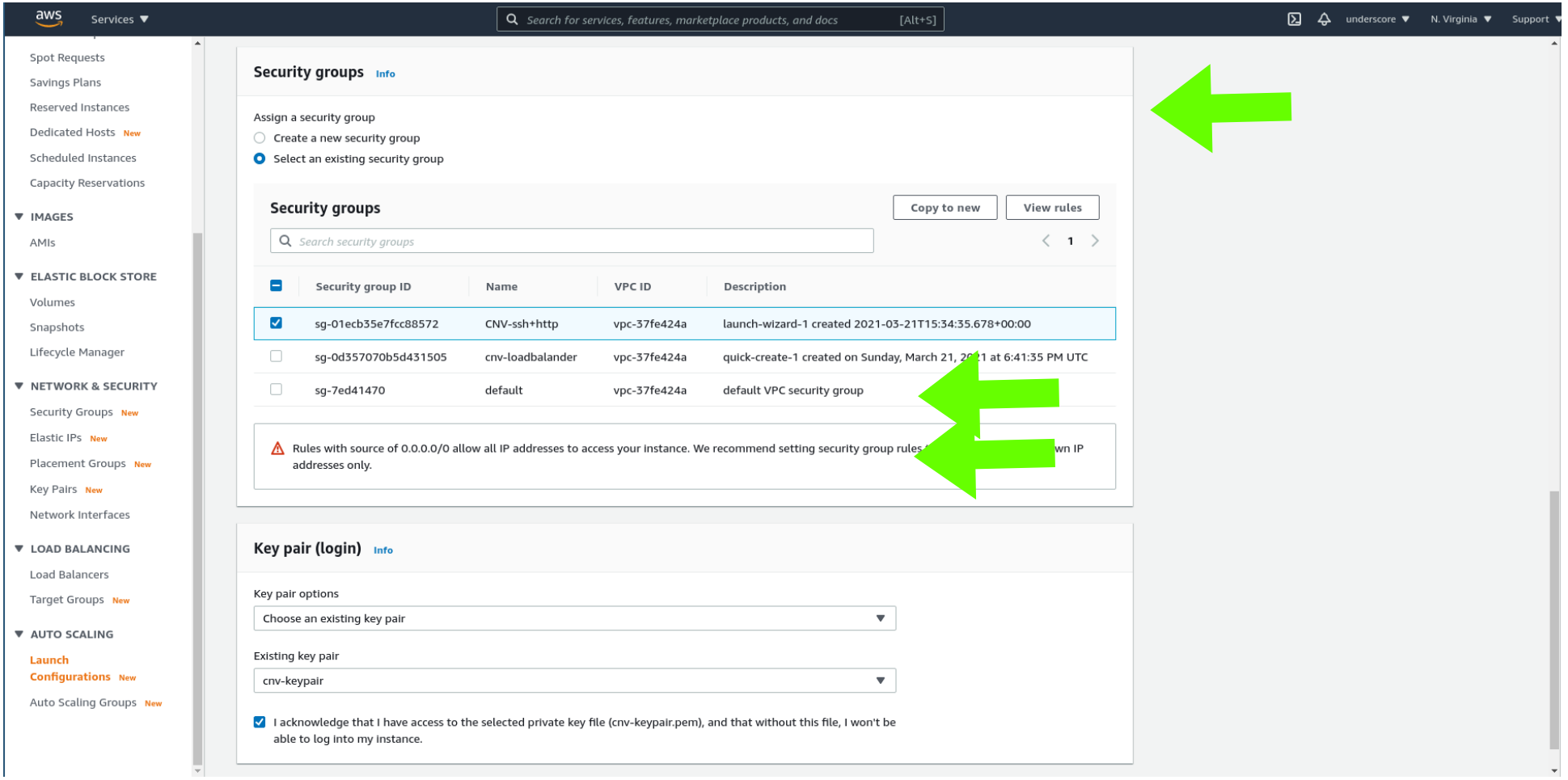
Fill name, AMI, Instance type…



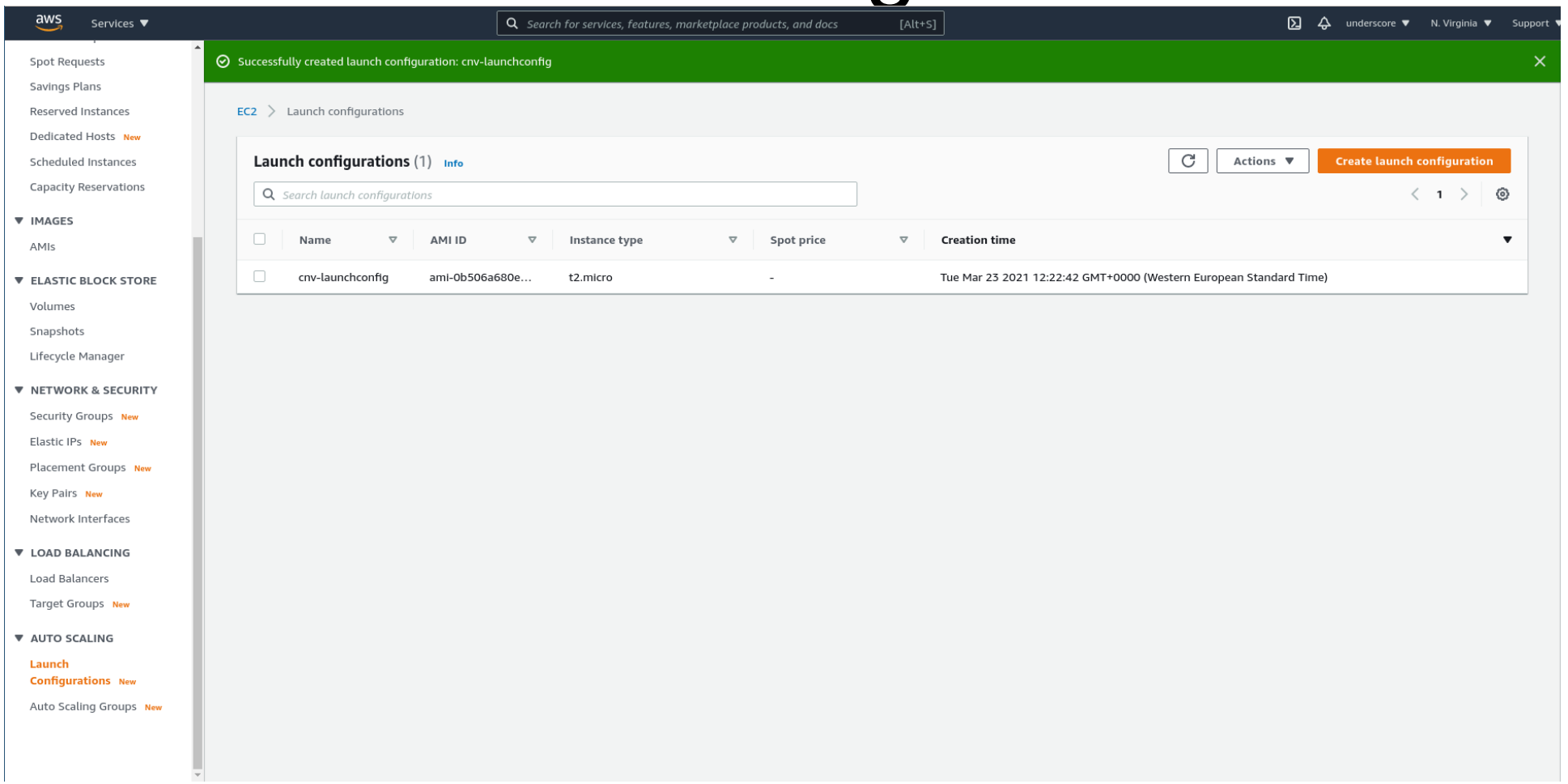
Enable Monitoring…



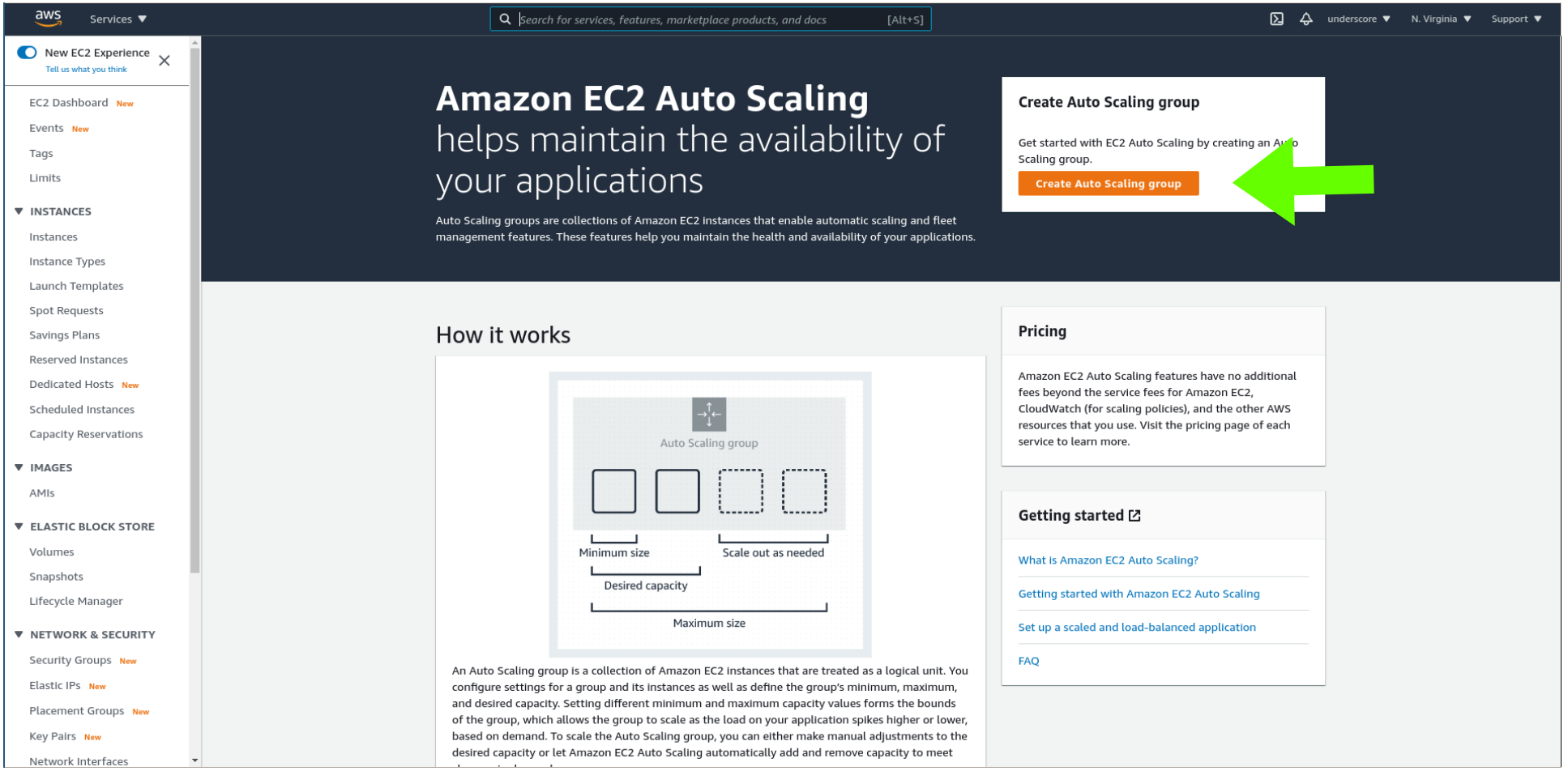
Select the exiting security group and key pair. Finish creation.



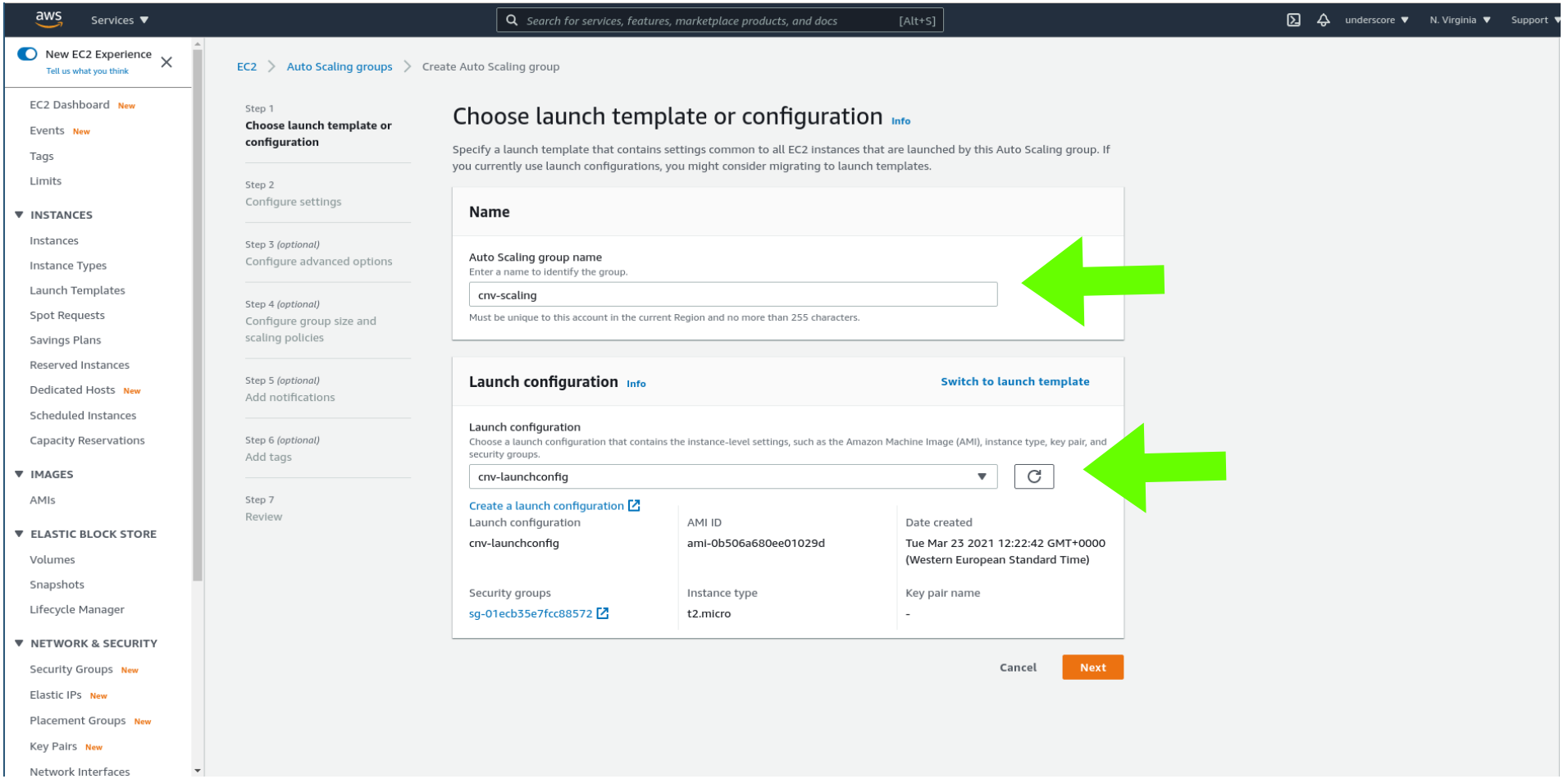
You should see the new-ly created launch configuration



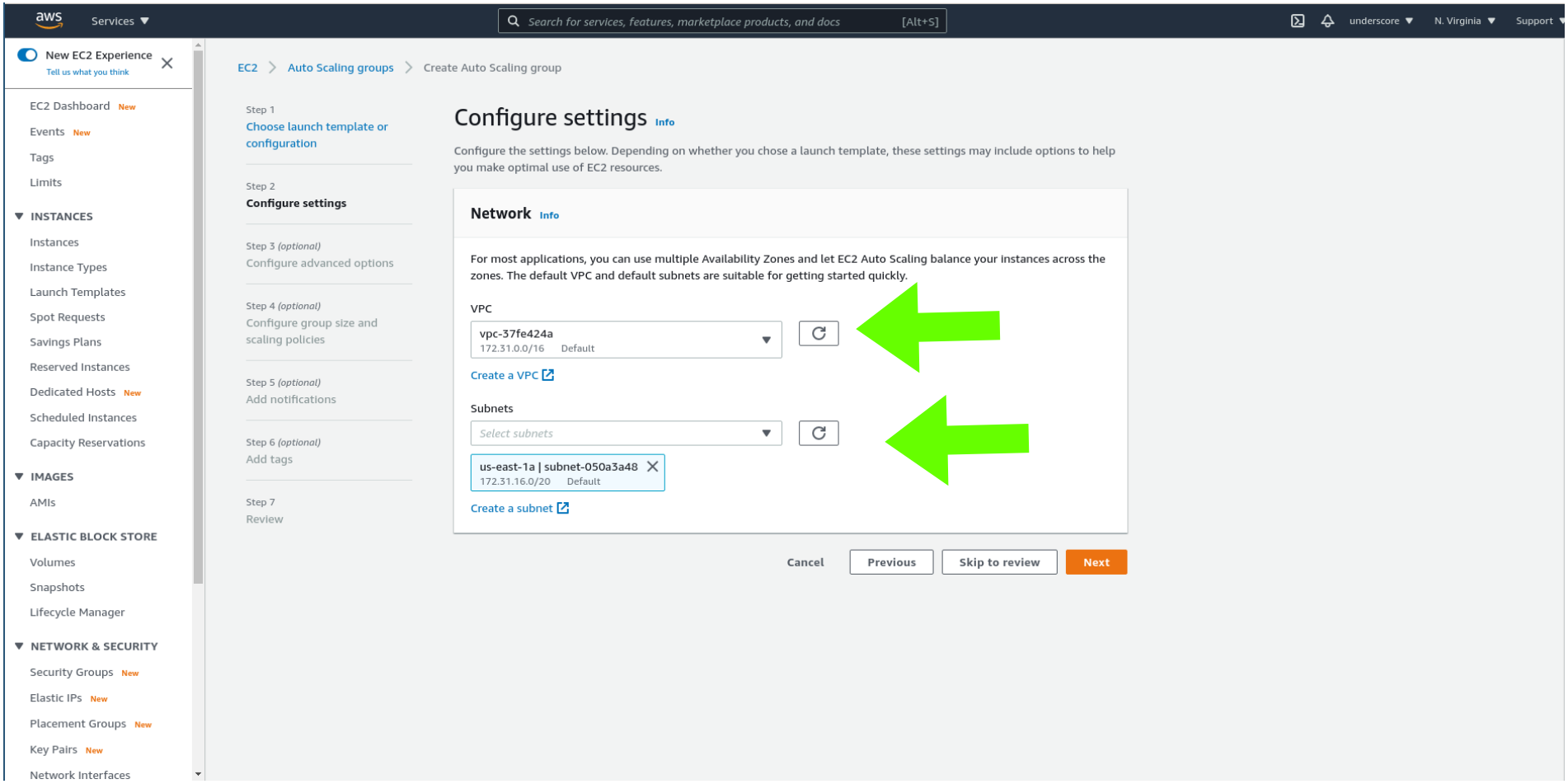
Create an Auto Scaling group



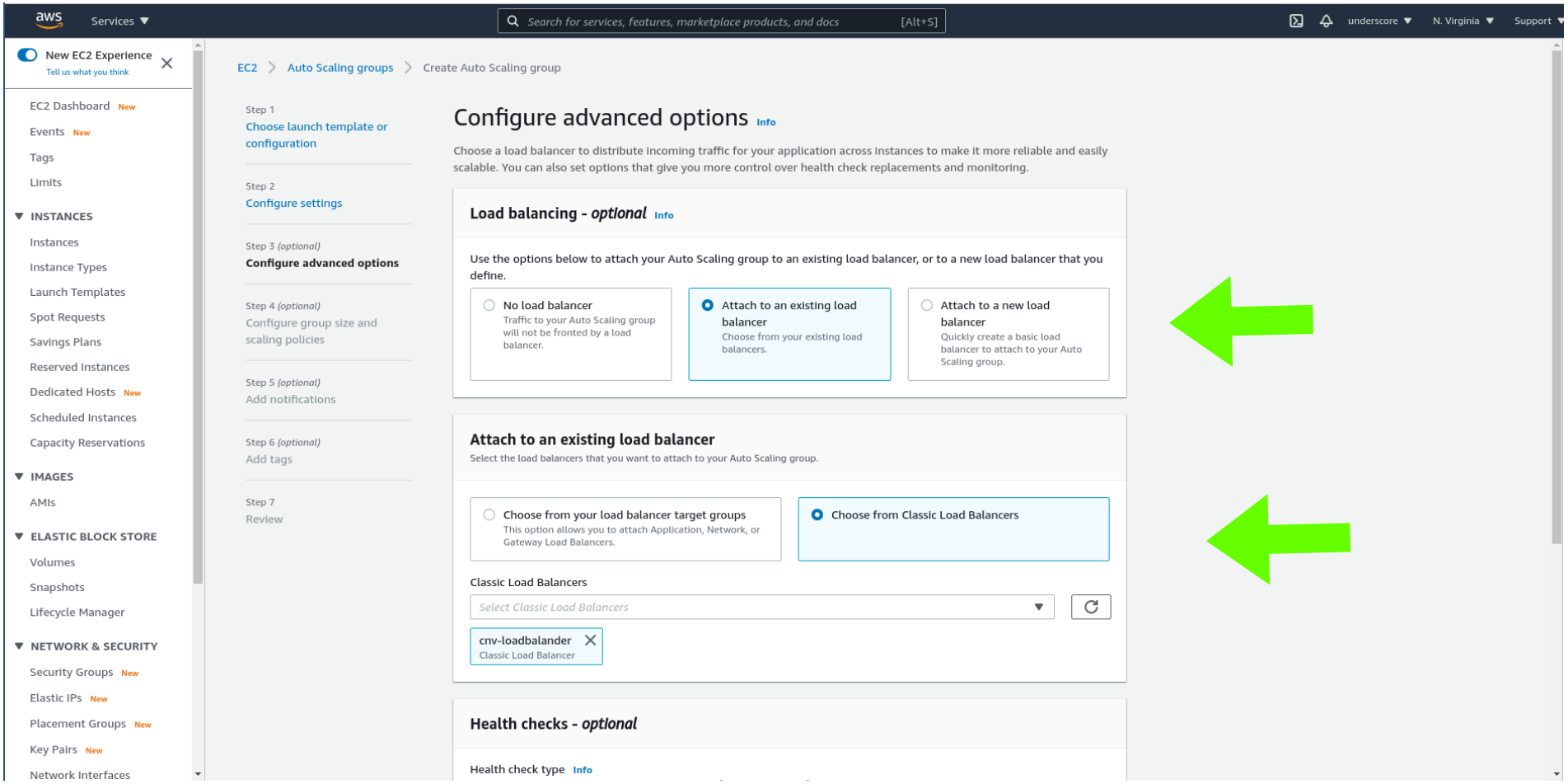
Fill the name and select the previously created launch config…



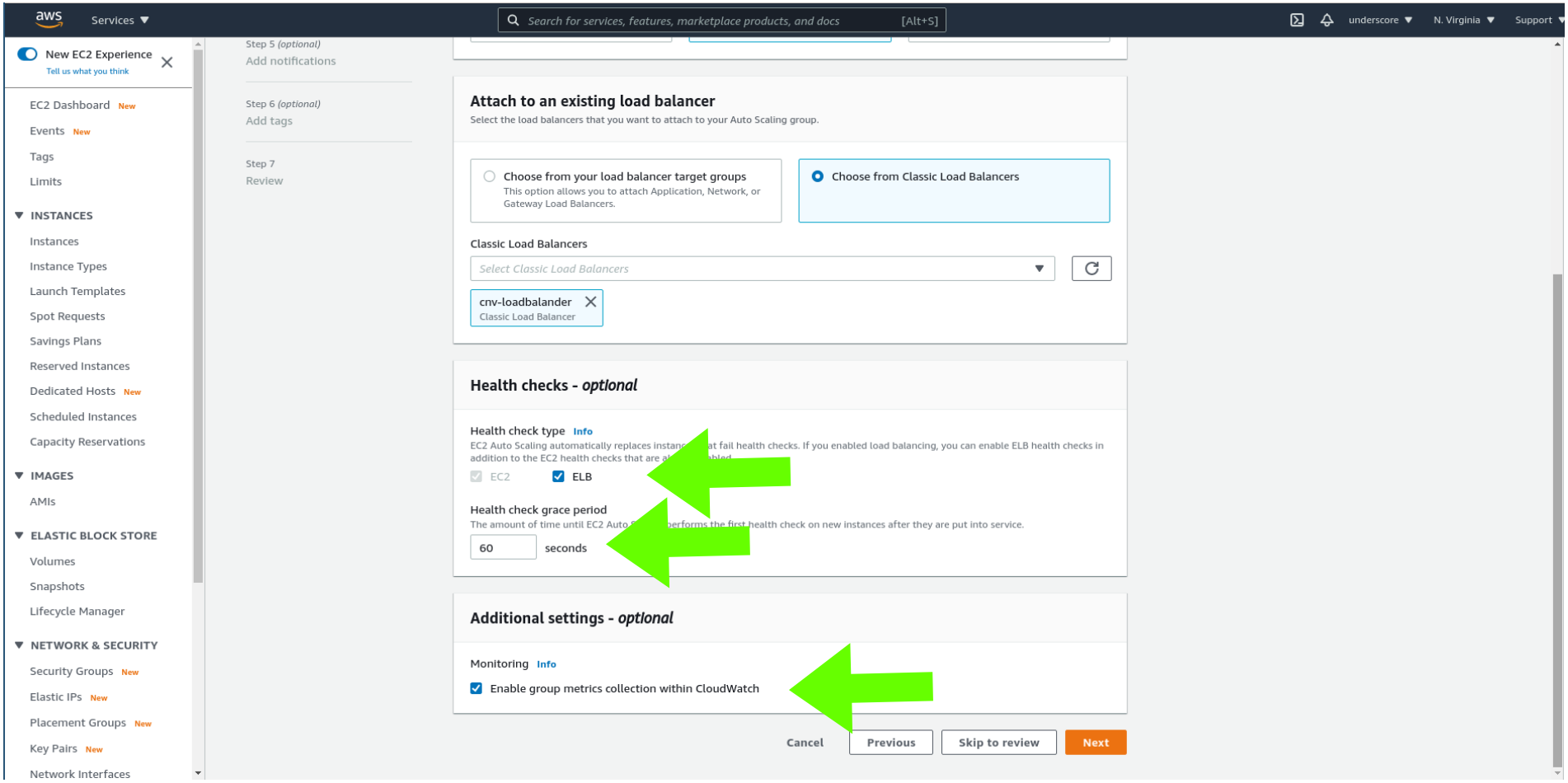
Select the exiting VPC and subnet…



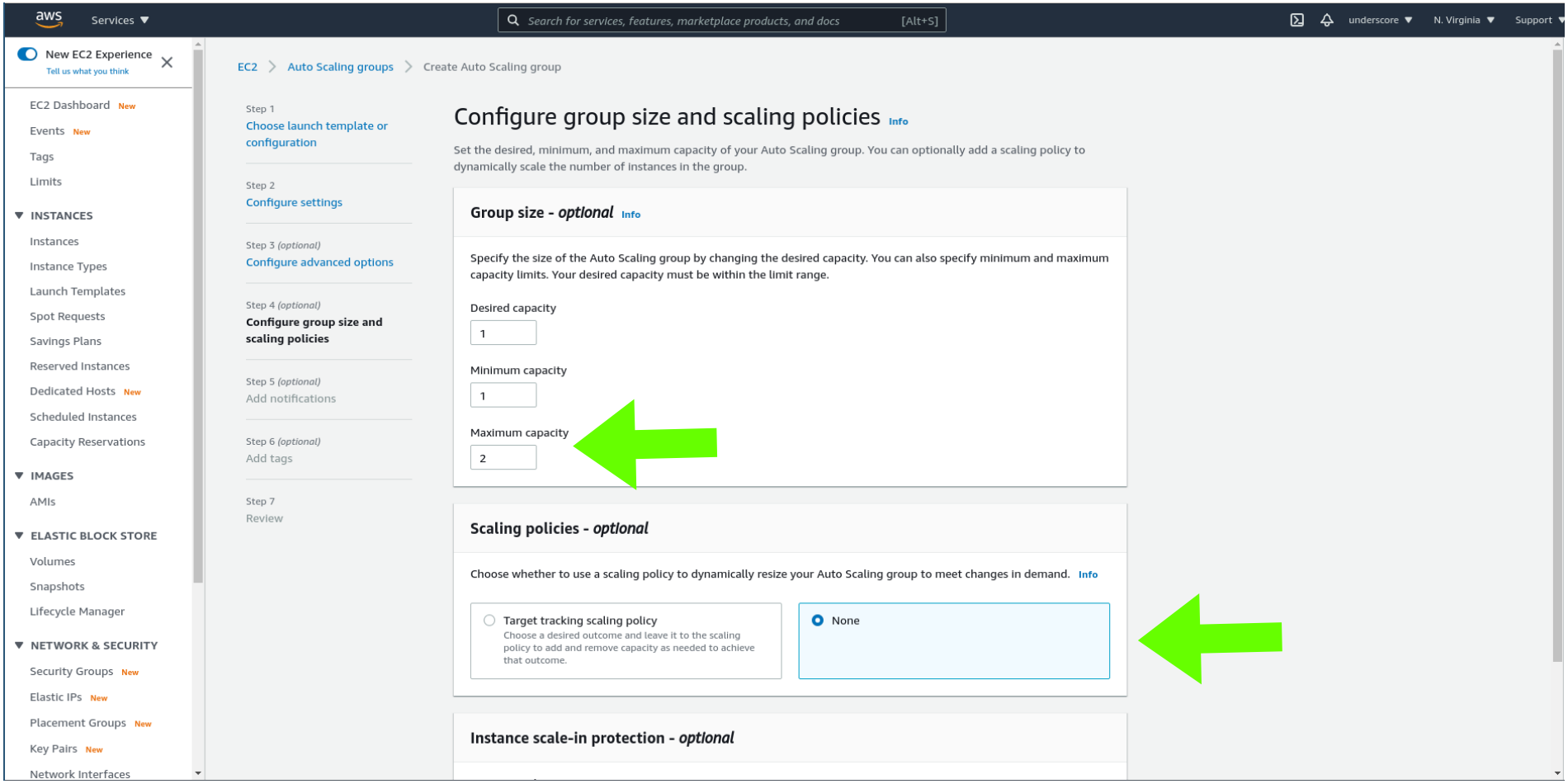
Select the exiting load balander…



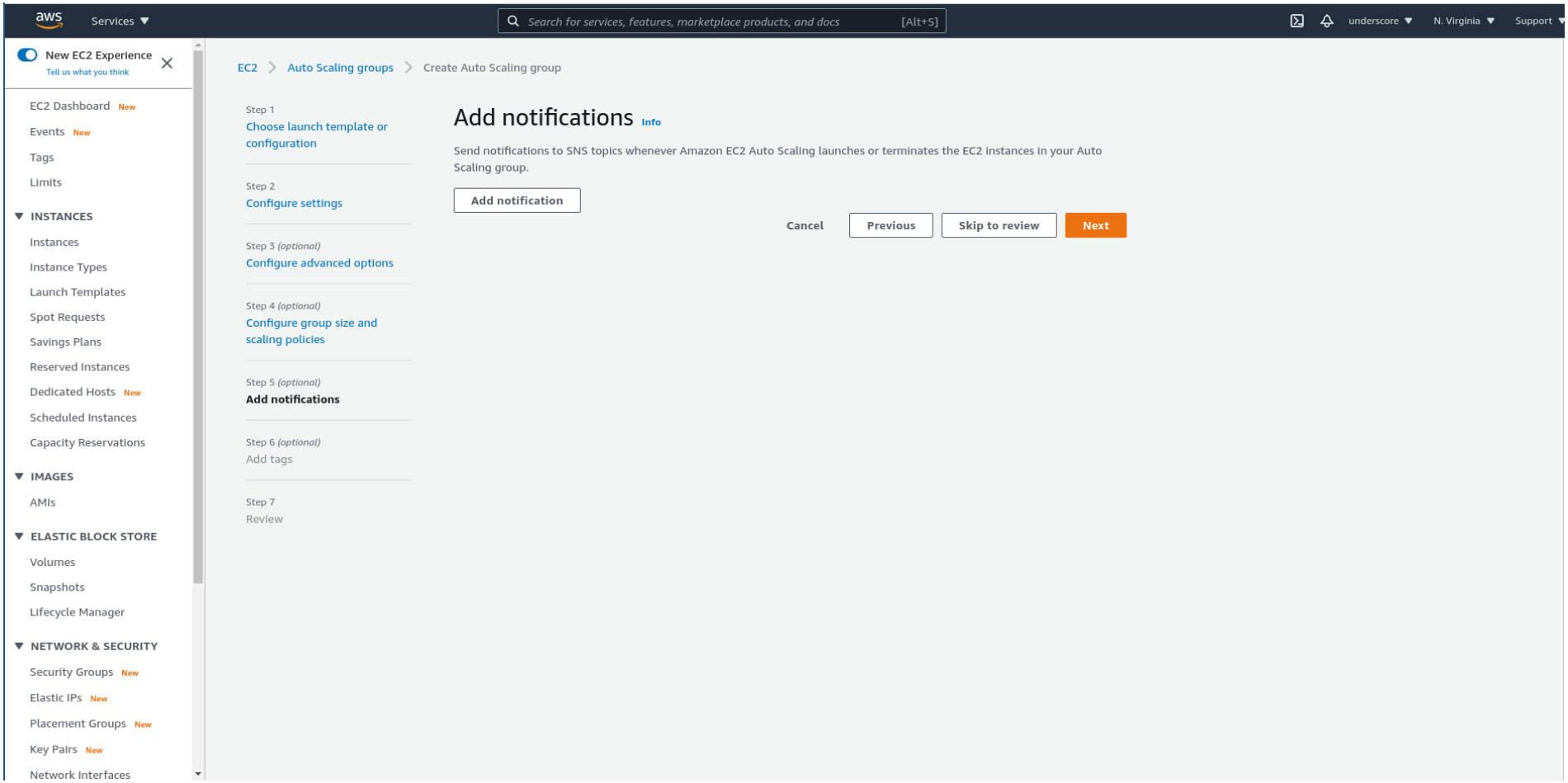
Select ELB health checks with 60s grace period. Enable monitoring…



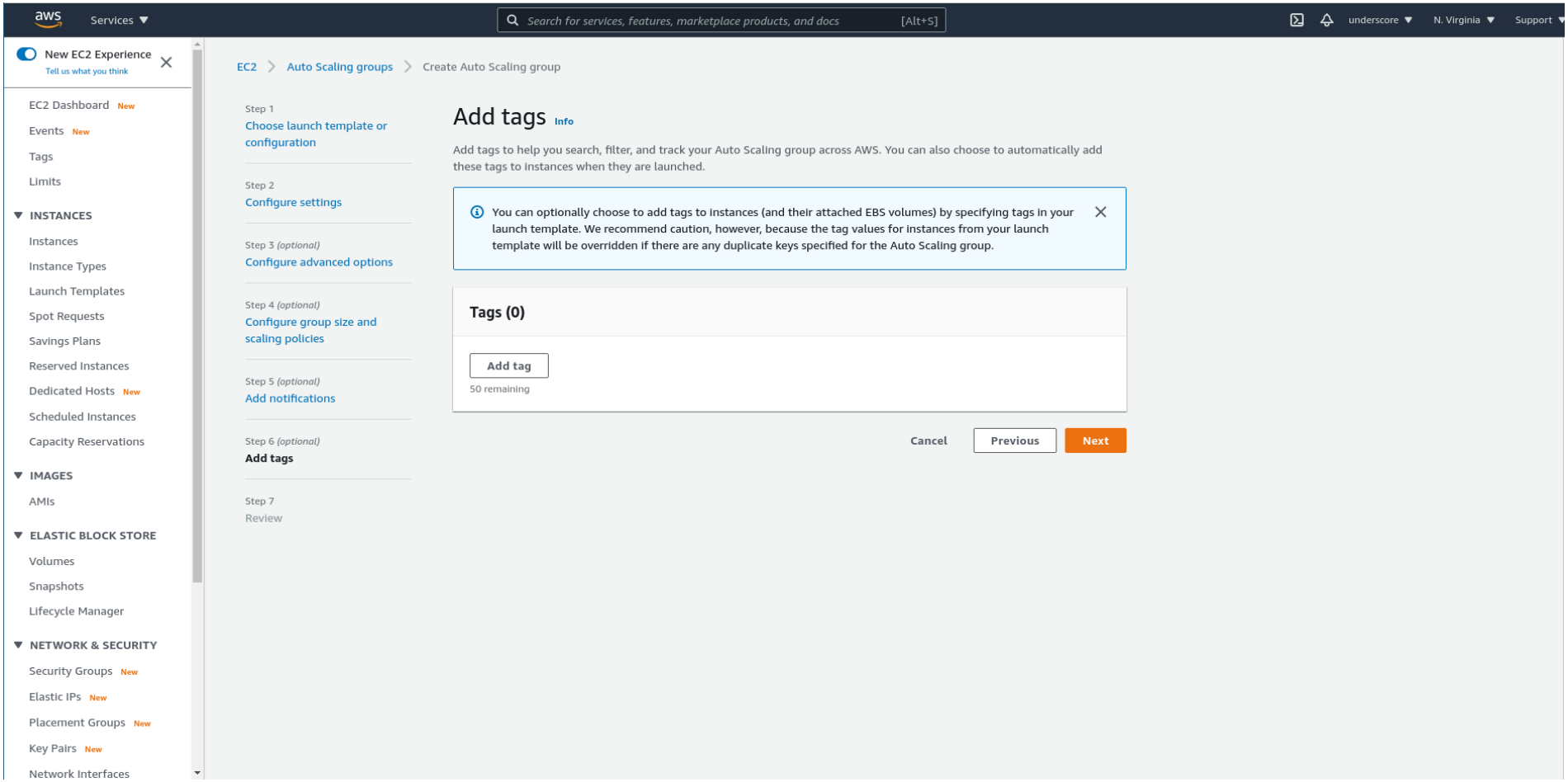
Pick a max capaticy (eg, 2). Select no scaling policies (for now)…



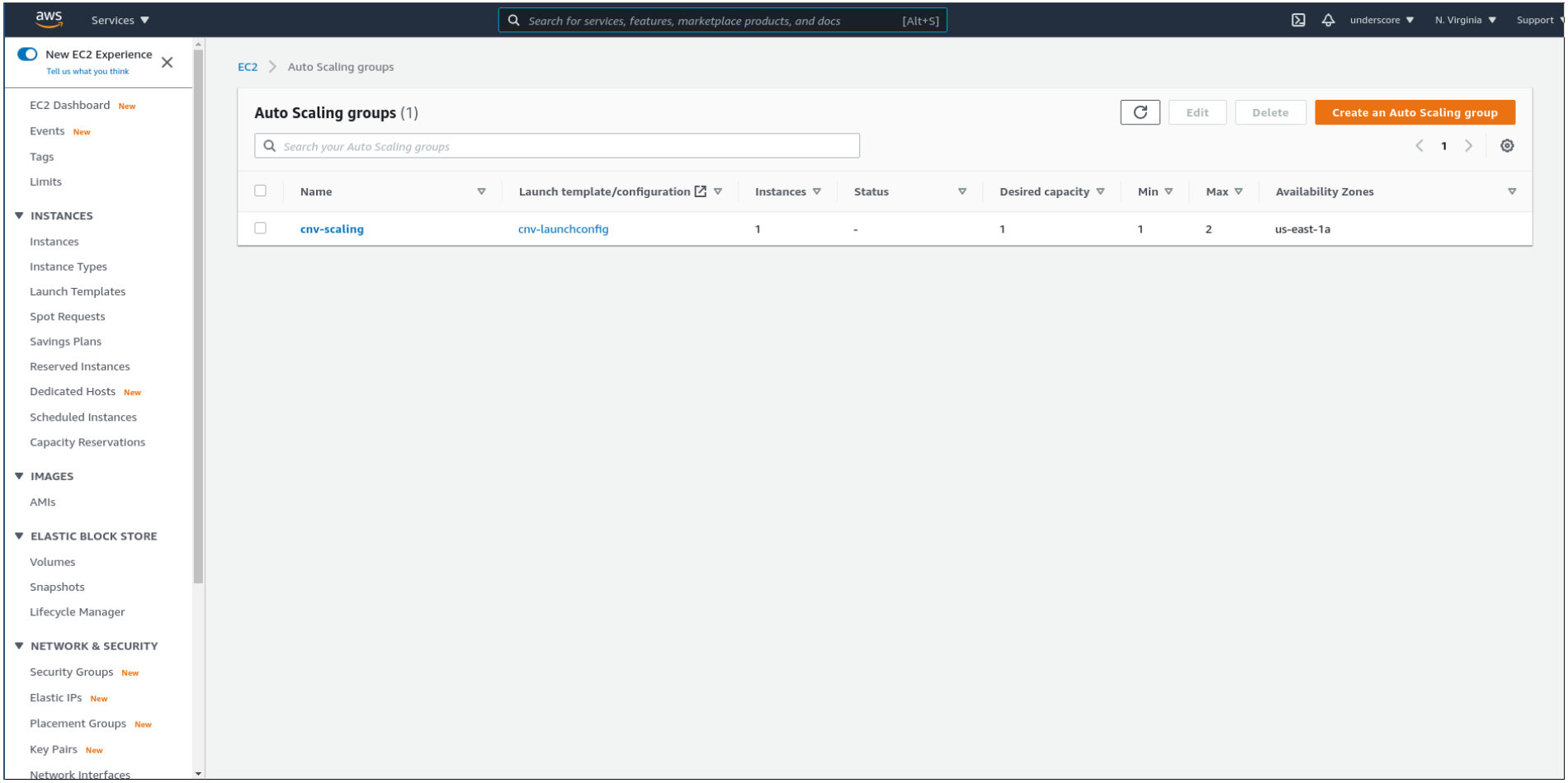
No notifications needed…



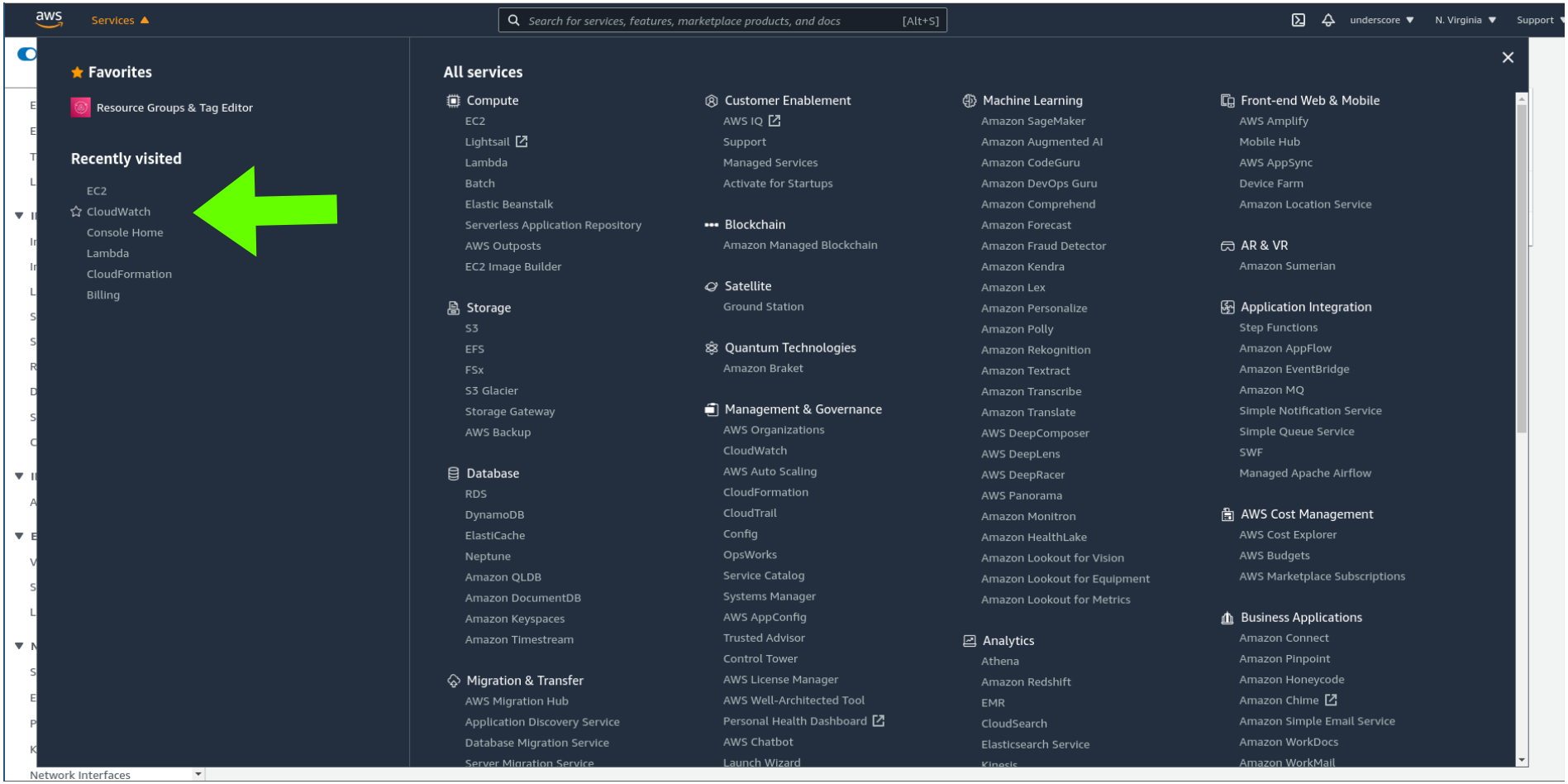
No tags needed…

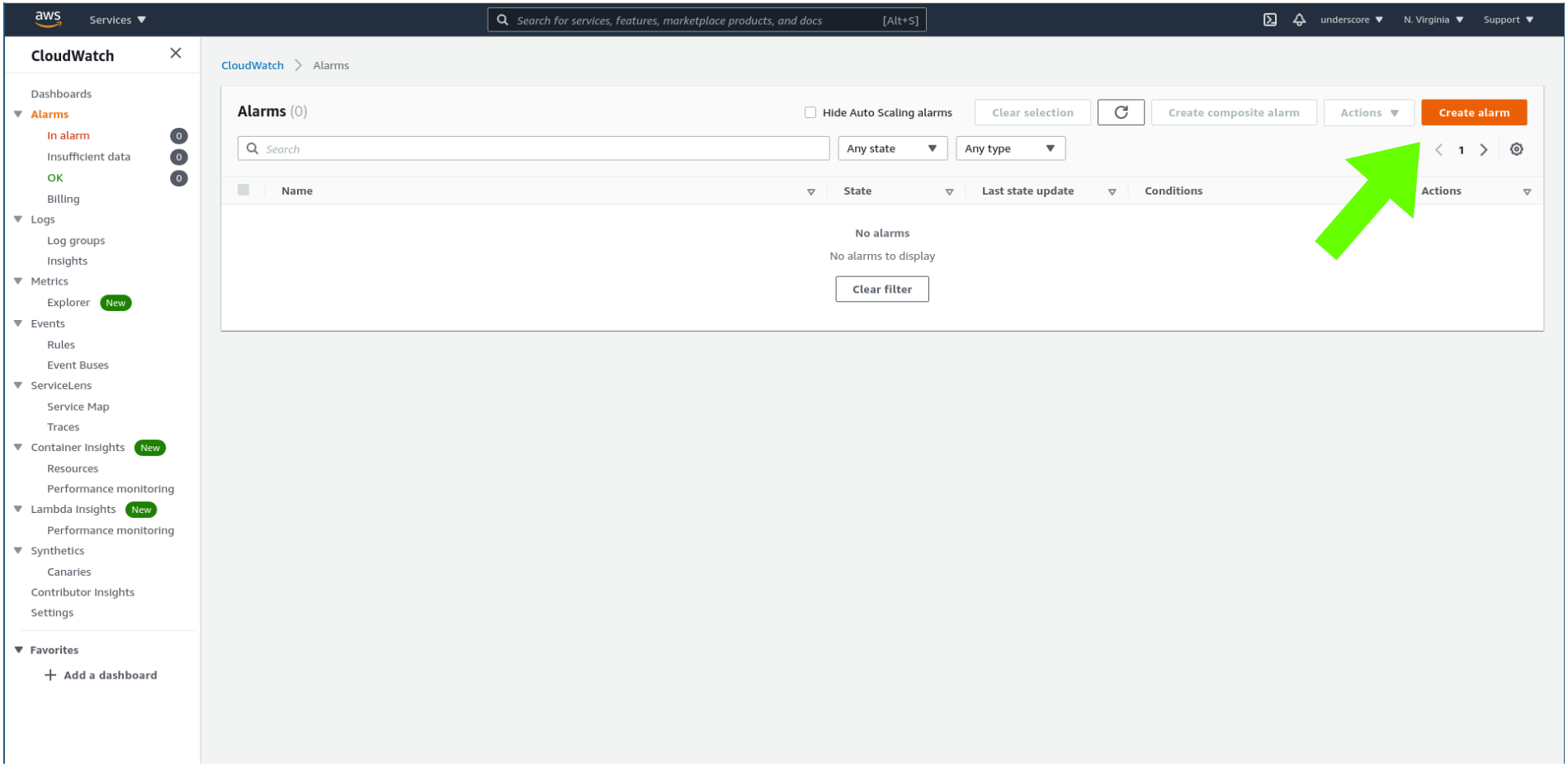


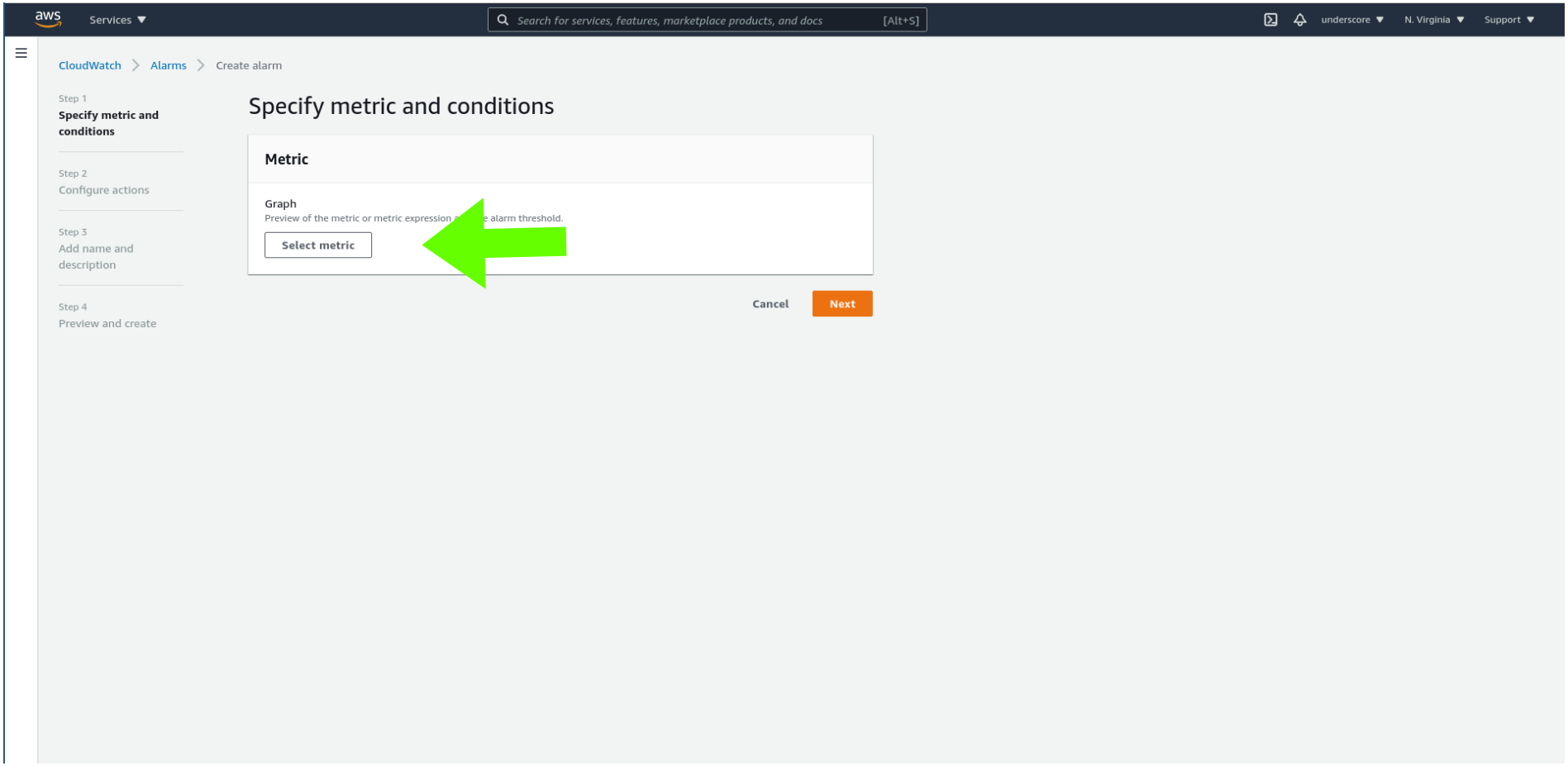
After review and create, you should see the new scaling group.



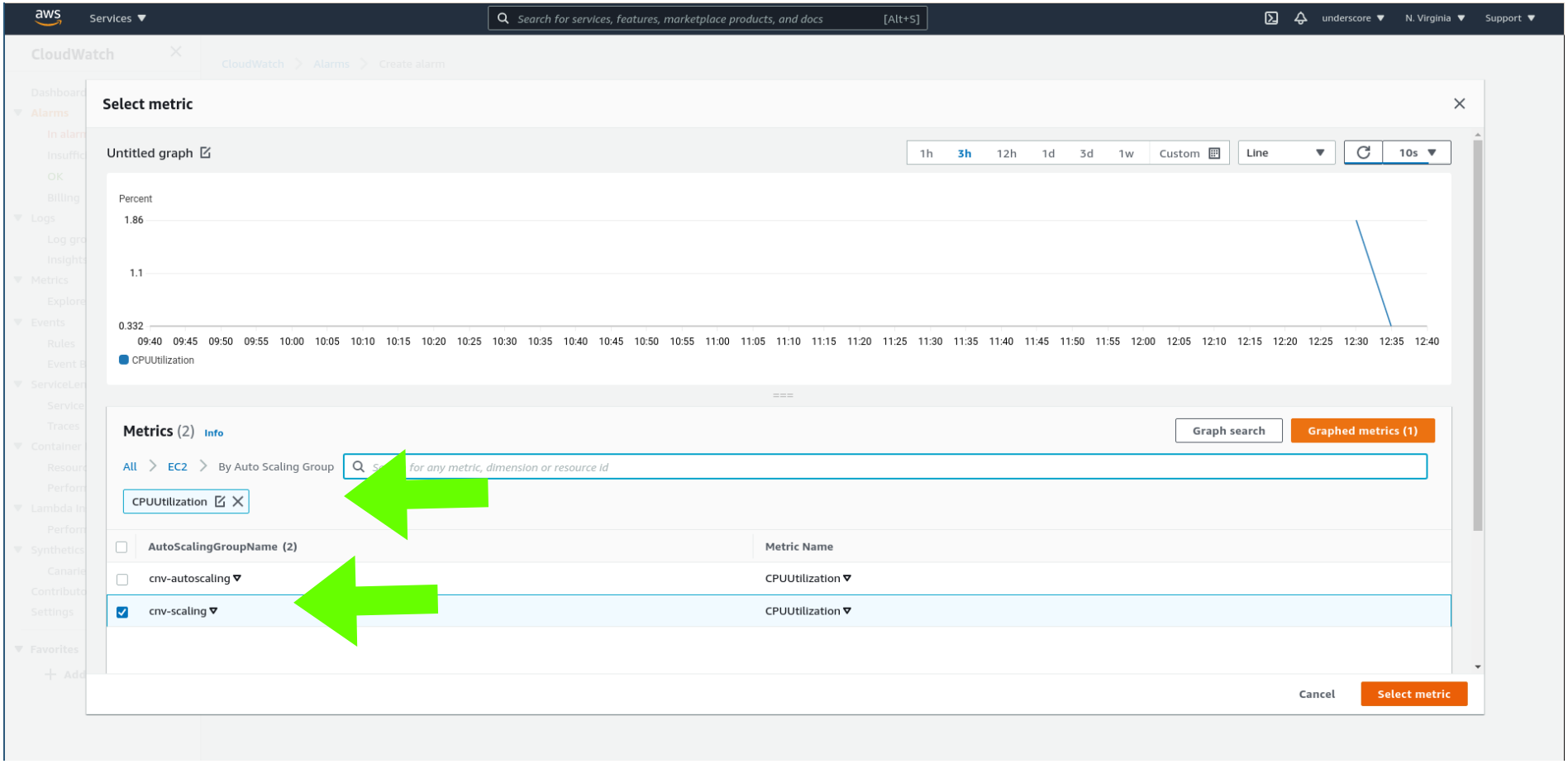
Create two Alarms in CloudWatch



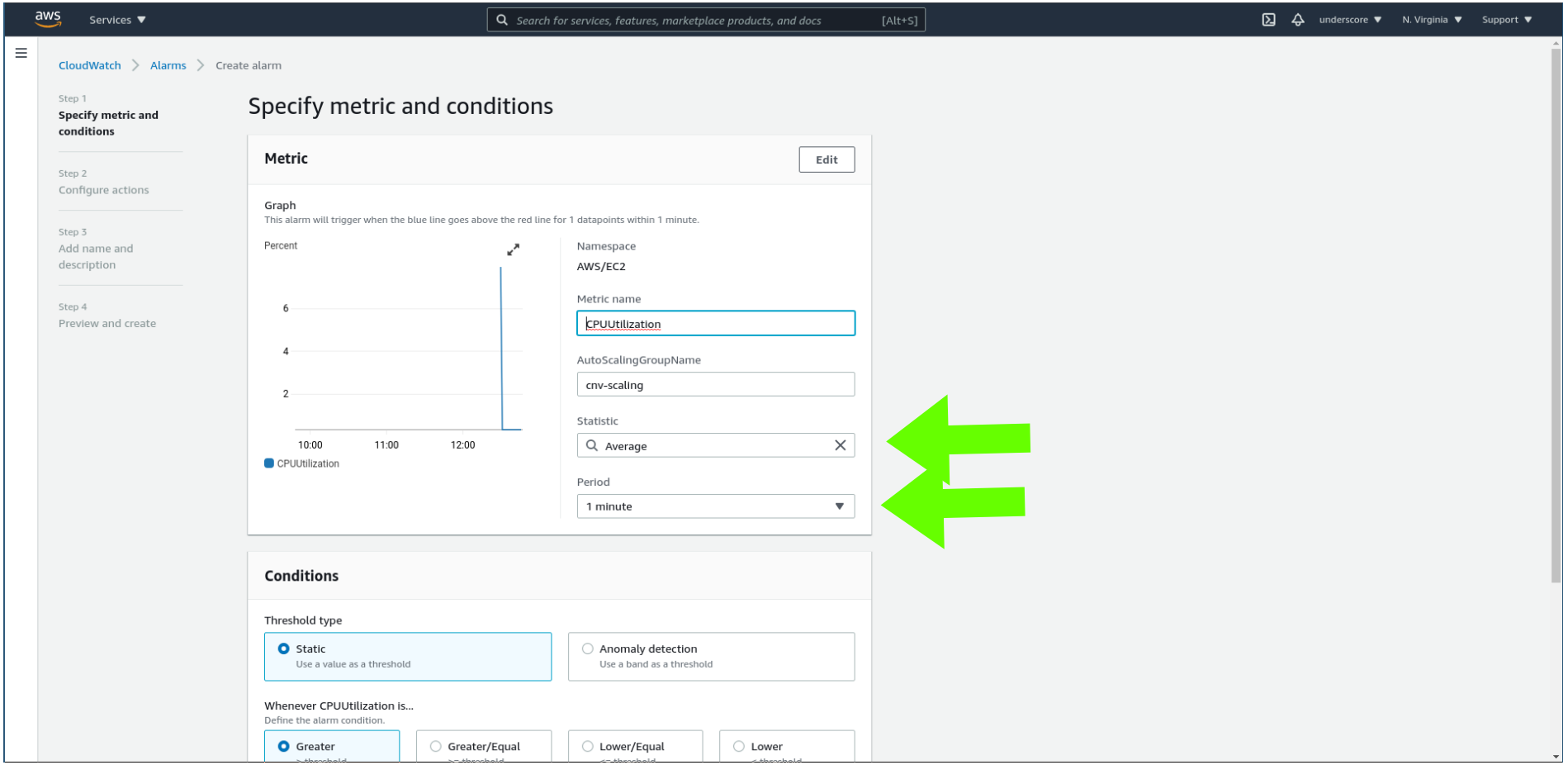

aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
underscore
N. Virginia
Support
CloudWatch
Dashboards
Alarms
In alarm 0
Insufficient data 0
OK 0
Billing
Logs
Log groups
Insights
Metrics
Explorer New
Events
Rules
Event Buses
ServiceLens
Service Map
Traces
Container Insights New
Resources
Performance monitoring
Lambda Insights New
Performance monitoring
Synthetics
Canaries
Contributor Insights
Settings
Favorites
Add a dashboard
CloudWatch > Alarms
Alarms (0)
Hide Auto Scaling alarms
Clear selection
Create composite alarm
Actions
Create alarm
Search
Any state
Any type
1
Name
State
Last state update
Conditions
Actions
No alarms
No alarms to display
Clear filter


aws
Services
Search for services, features, marketplace products, and docs
[Alt+S]
underscore
N. Virginia
Support
CloudWatch
Alarms
Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Specify metric and conditions
Metric
Graph
Select metric
Cancel
Next

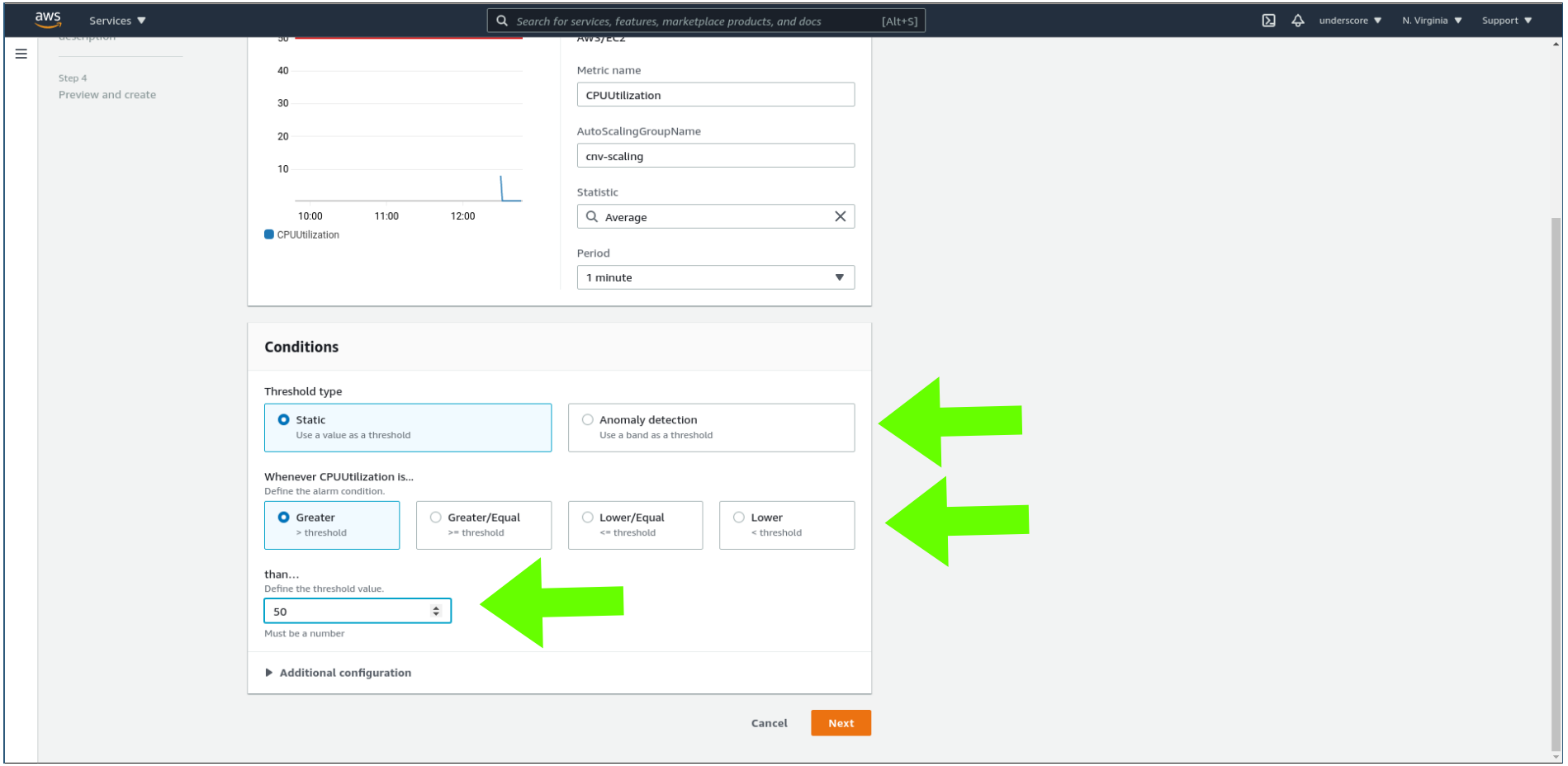
Select ‘CPUUtilization’ metric for the previously created scaling group…



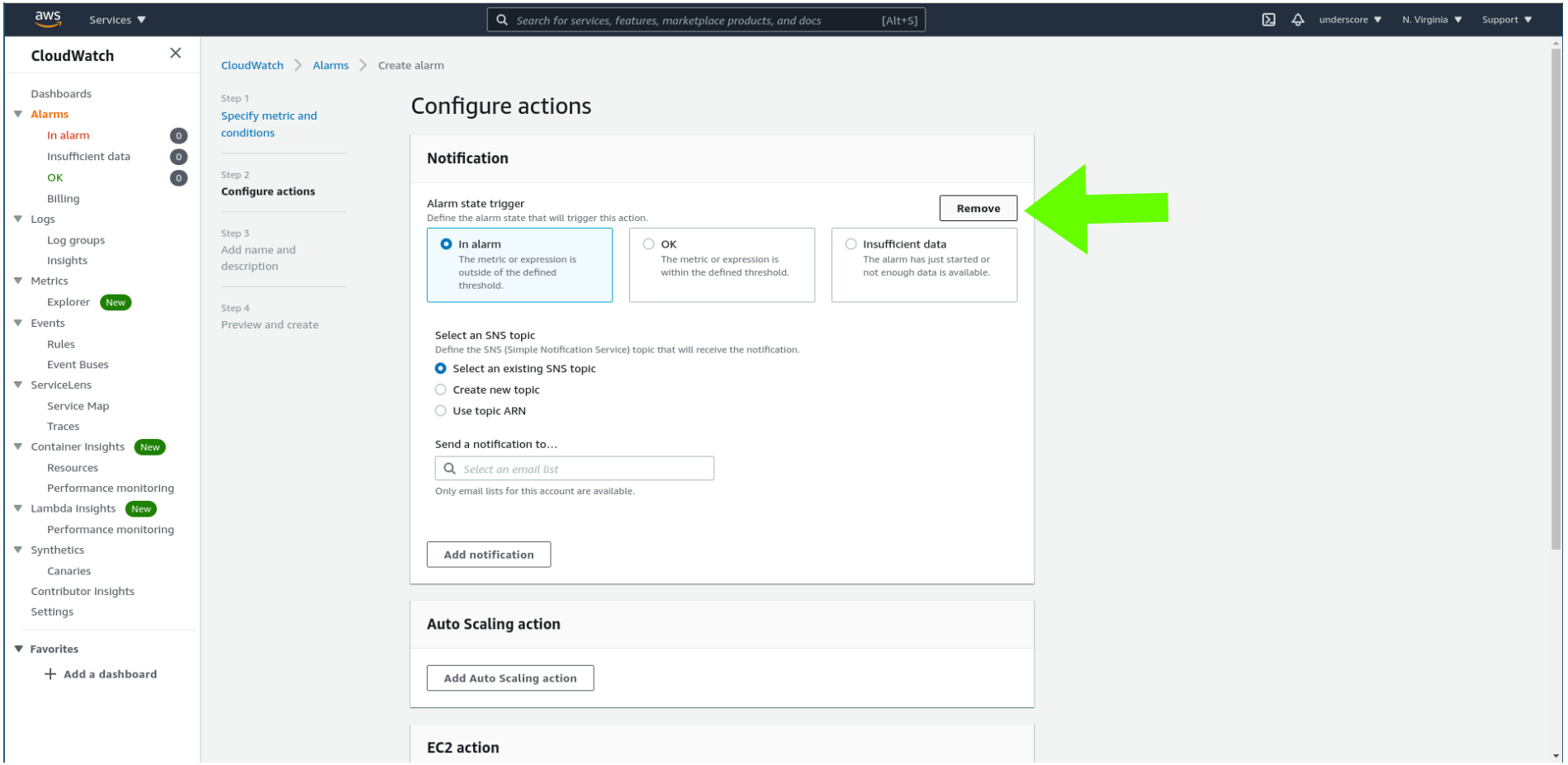
Select ‘Average’ for statistic and ‘Period’ (e.g., 1 minute)

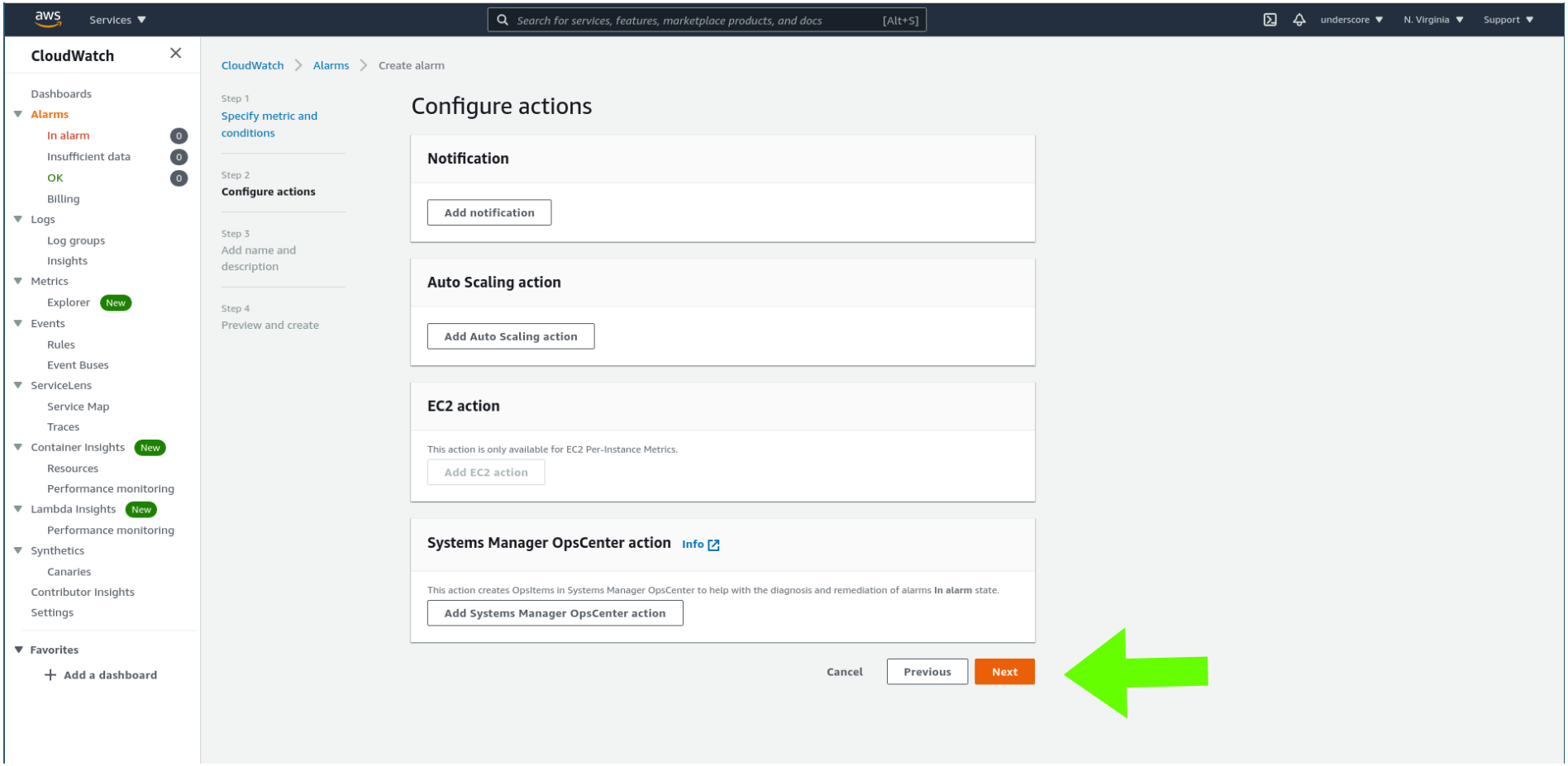


Static threshold, greater, 50% (i.e. alarm goes off is avg CPU > 50%)

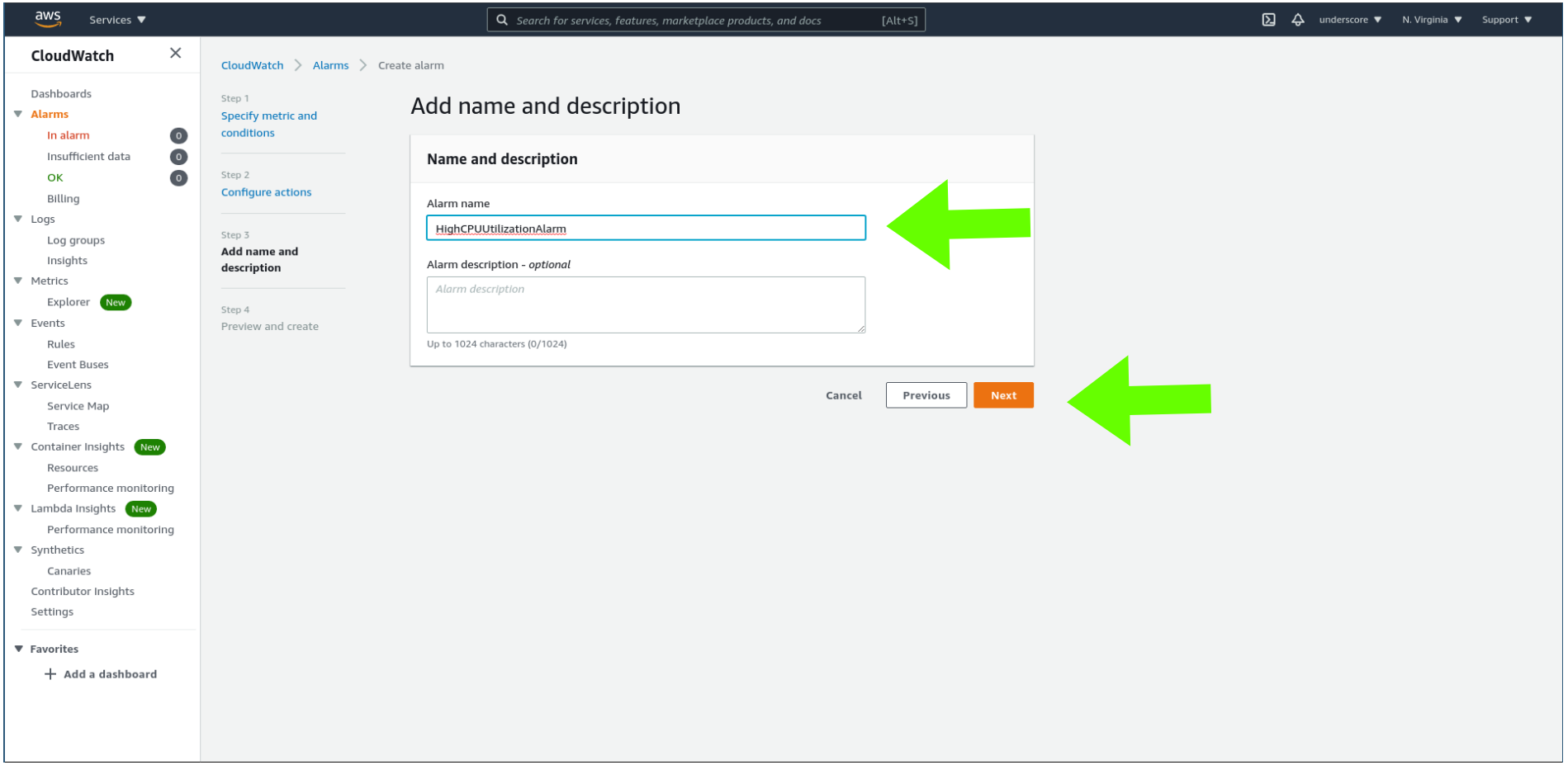


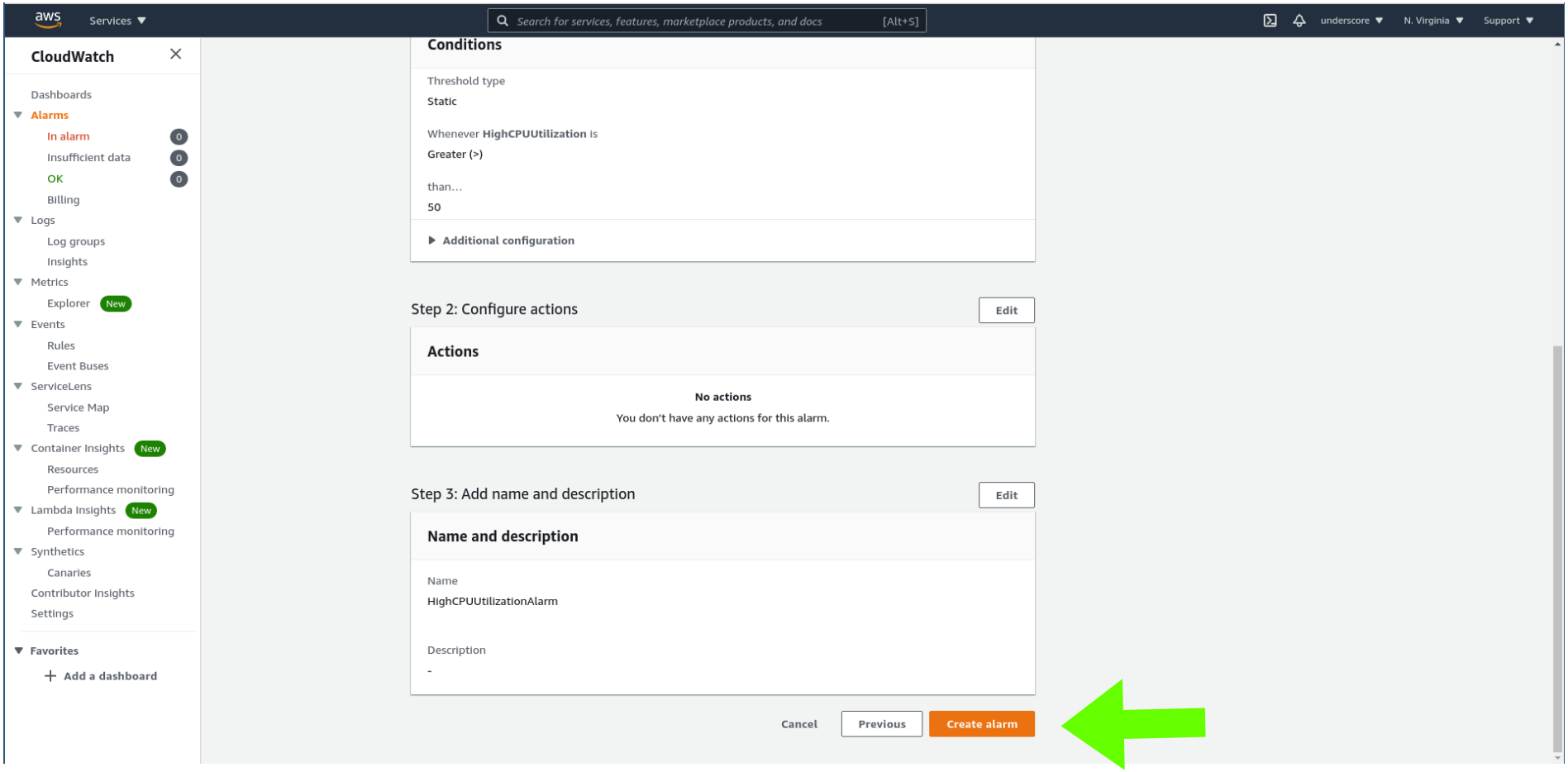
No notifications needed…



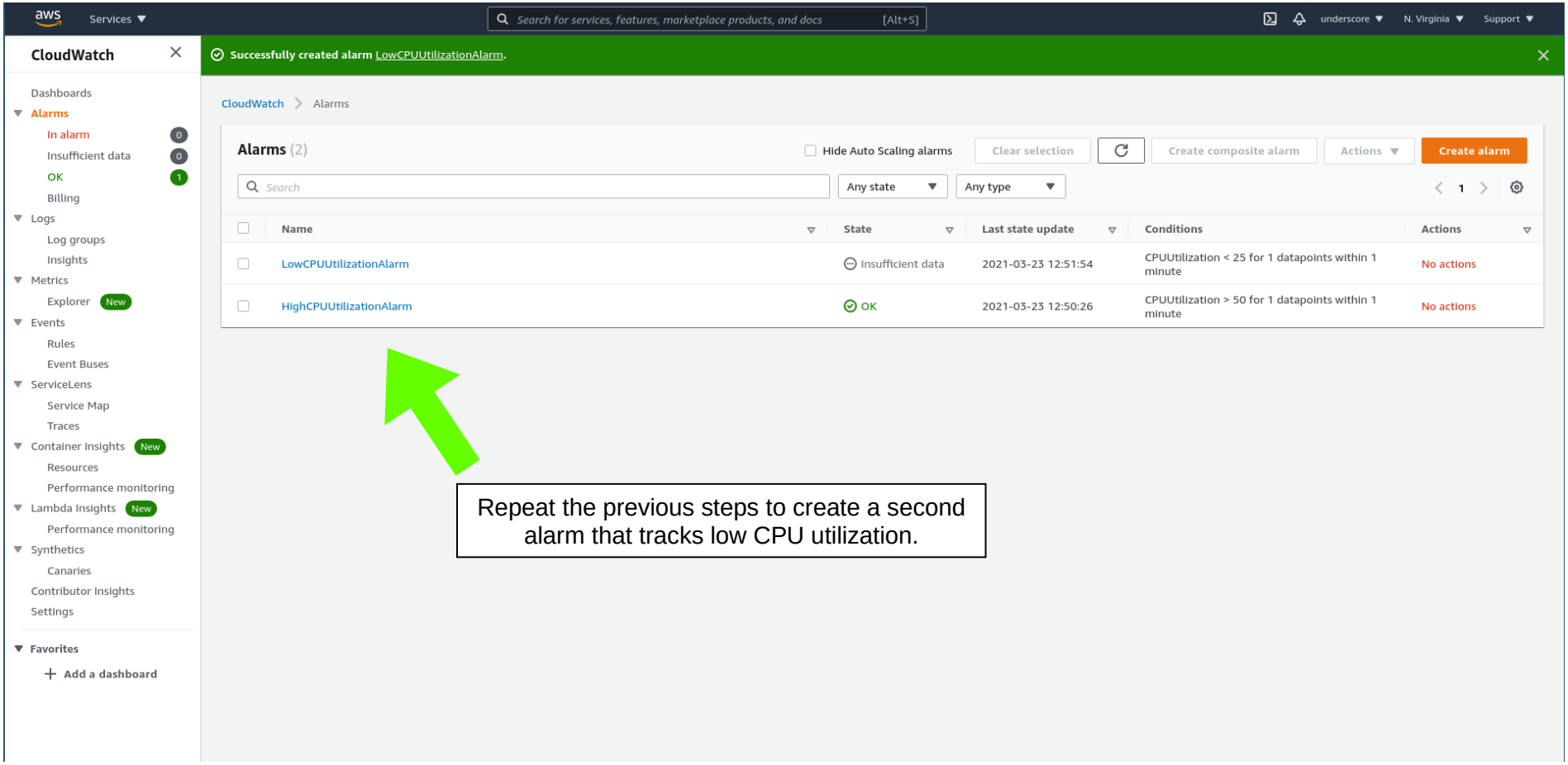

aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
underscore
N. Virginia
Support
CloudWatch
Dashboards
Alarms
In alarm 0
Insufficient data 0
OK 0
Billing
Logs
Log groups
Insights
Metrics
Explorer New
Events
Rules
Event Buses
ServiceLens
Service Map
Traces
Container Insights New
Resources
Performance monitoring
Lambda Insights New
Performance monitoring
Synthetics
Canaries
Contributor Insights
Settings
Favorites
Add a dashboard
CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Configure actions
Notification
Add notification
Auto Scaling action
Add Auto Scaling action
EC2 action
This action is only available for EC2 Per-Instance Metrics.
Add EC2 action
Systems Manager OpsCenter action Info
This action creates OpsItems in Systems Manager OpsCenter to help with the diagnosis and remediation of alarms In alarm state.
Add Systems Manager OpsCenter action
Cancel
Previous
Next

Give a name to the alarm…

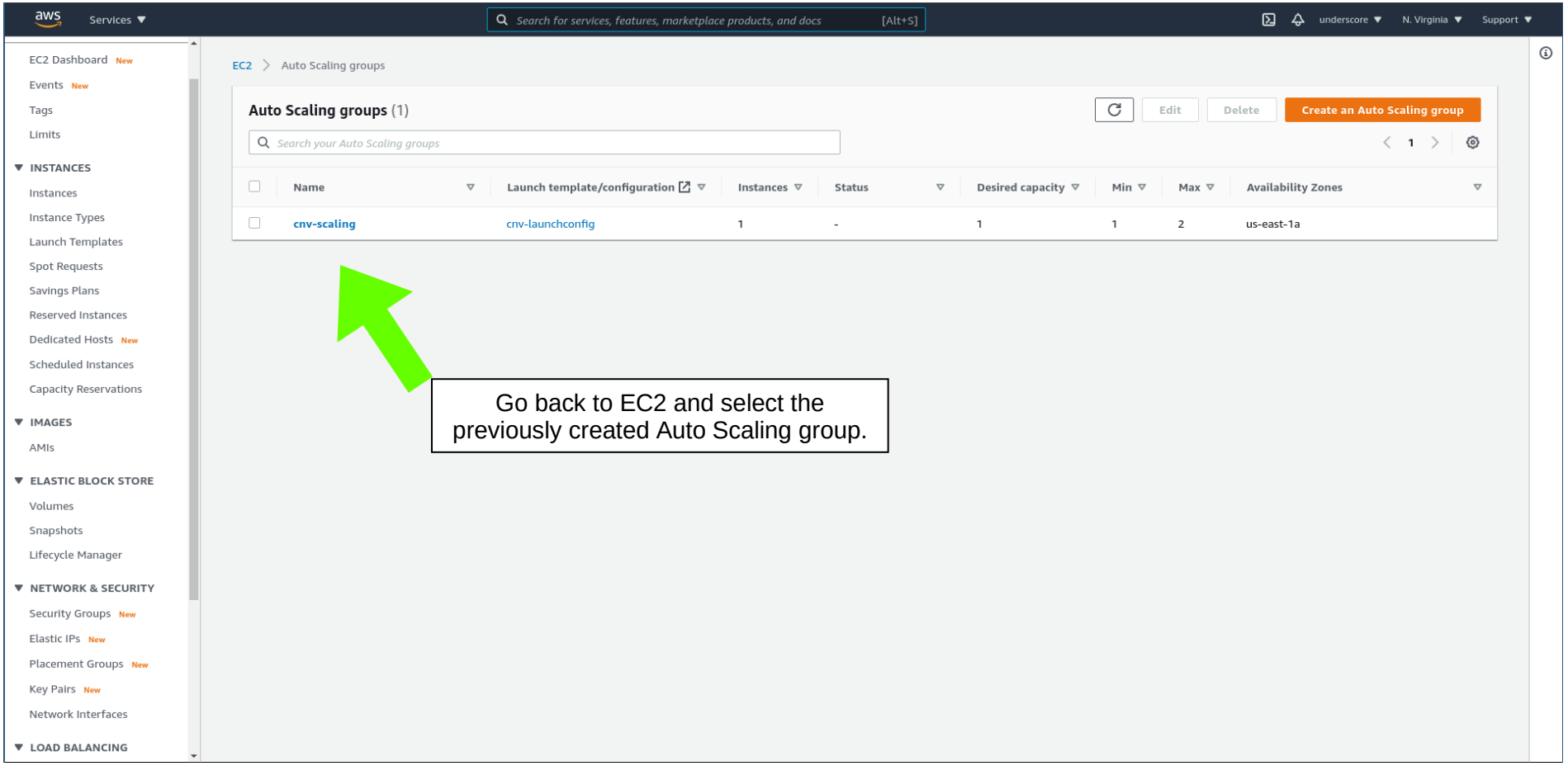


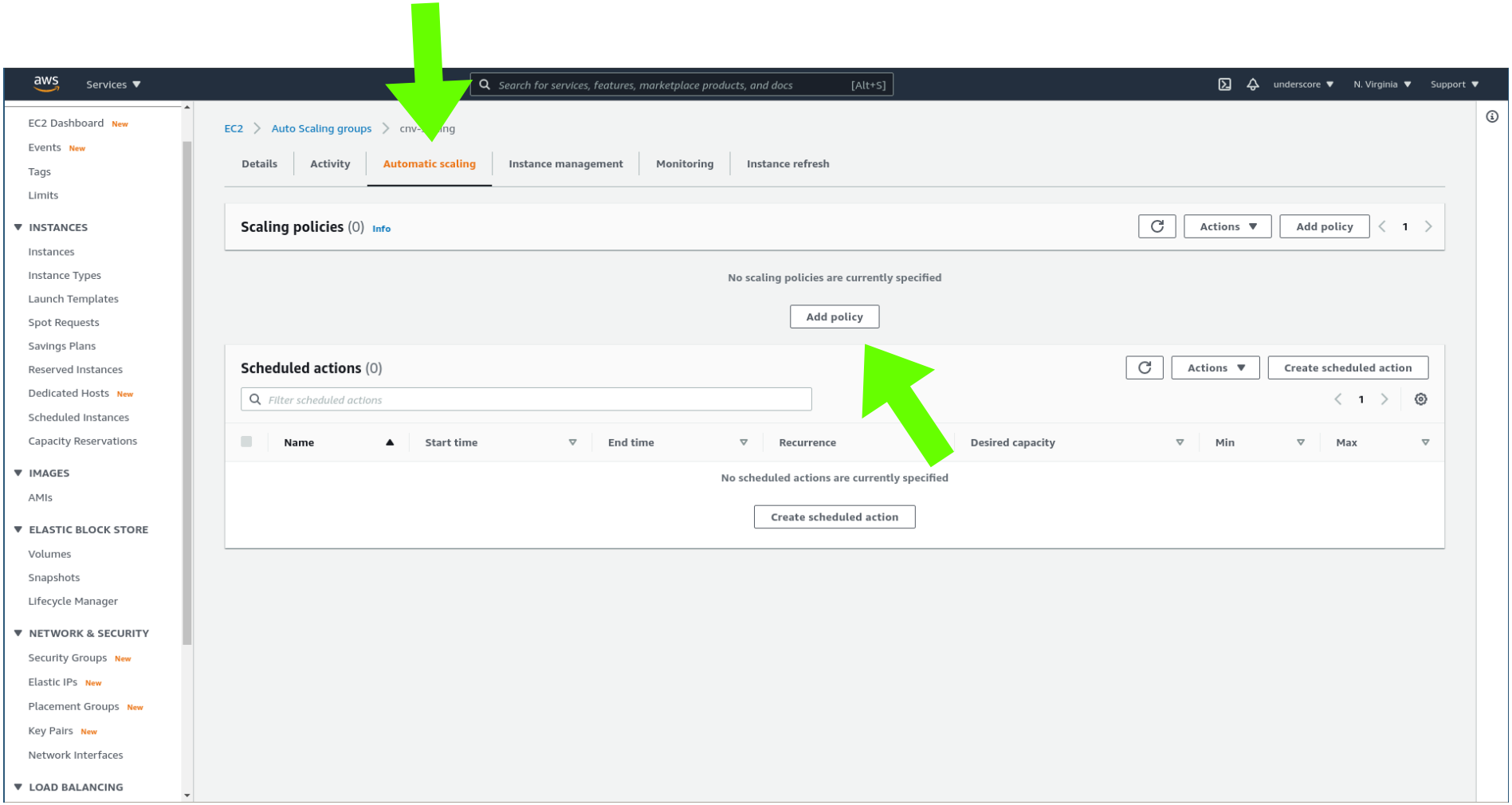

aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
underscore
N. Virginia
Support
CloudWatch
Dashboards
Alarms
In alarm 0
Insufficient data 0
OK 0
Billing
Logs
Log groups
Insights
Metrics
Explorer New
Events
Rules
Event Buses
ServiceLens
Service Map
Traces
Container Insights New
Resources
Performance monitoring
Lambda Insights New
Performance monitoring
Synthetics
Canaries
Contributor Insights
Settings
Favorites
Add a dashboard
Conditions
Threshold type
Static
Whenever HighCPUUtilization is
Greater (>)
than...
50
Additional configuration
Step 2: Configure actions
Edit
Actions
No actions
You don't have any actions for this alarm.
Step 3: Add name and description
Edit
Name and description
Name
HighCPUUtilizationAlarm
Description
-
Cancel
Previous
Create alarm

After repeating for a low CPU utilization alarm…

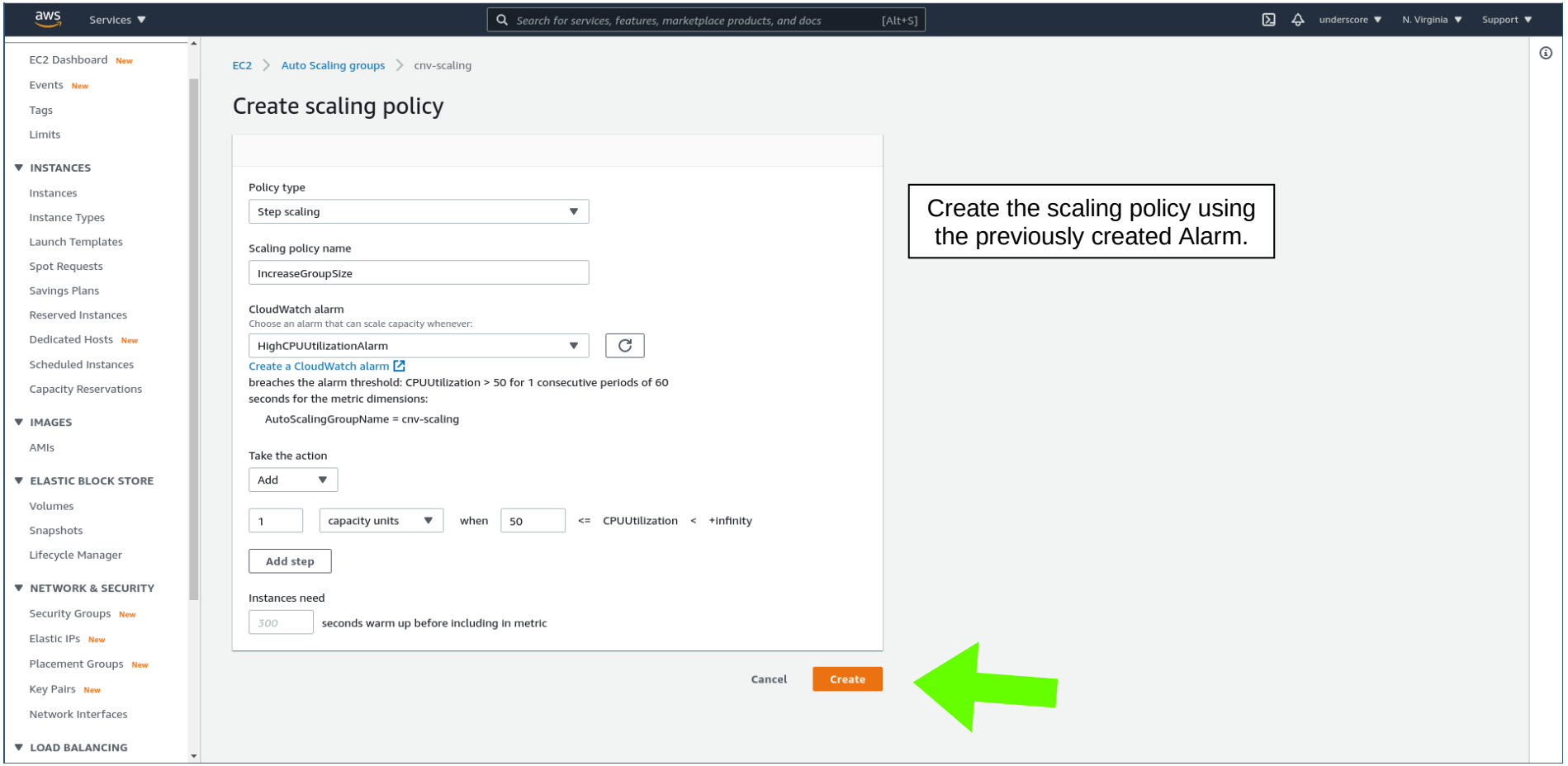


Create two Scaling Policies in EC2

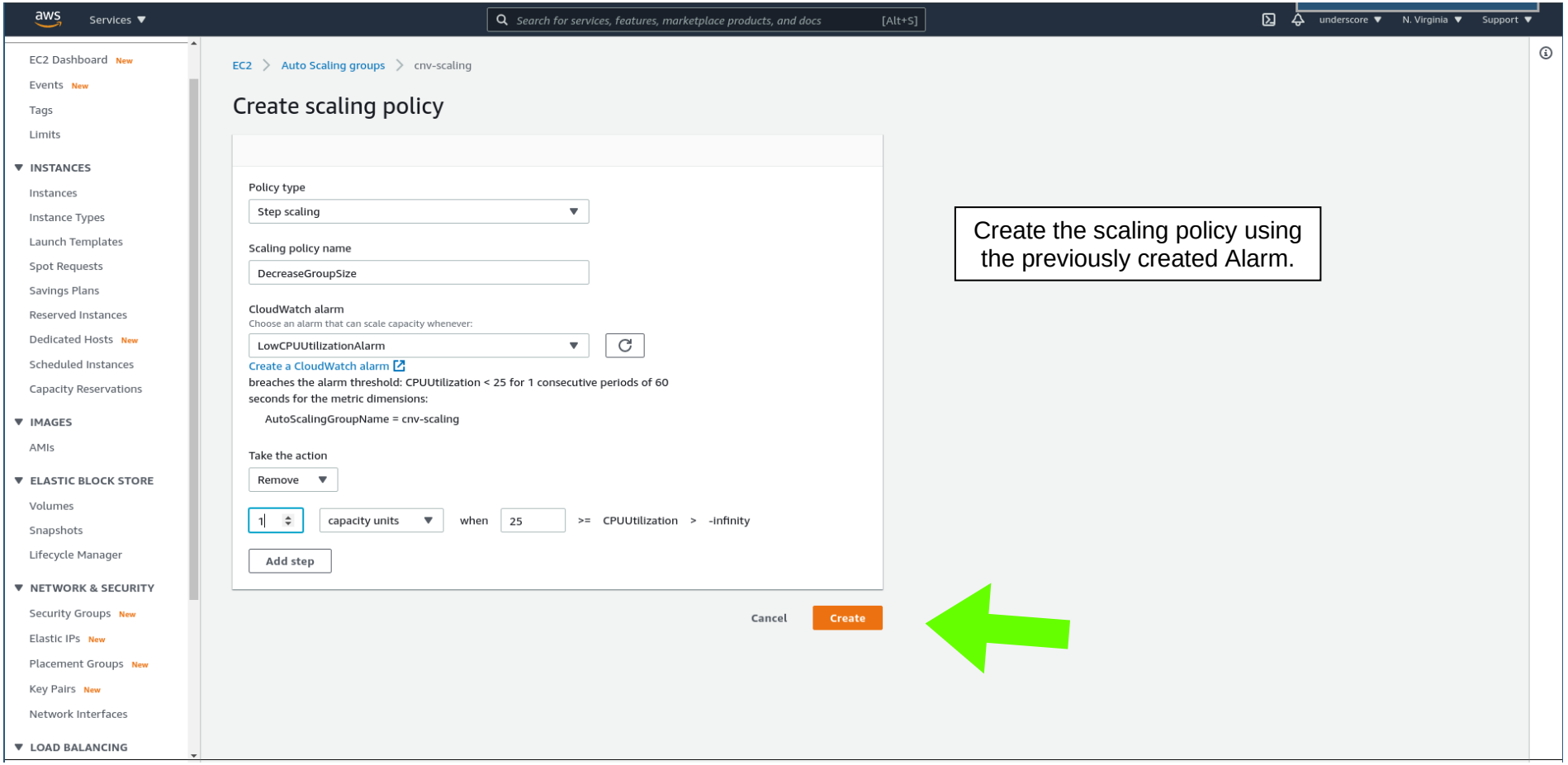



aws
Services
Search for services, features, marketplace products, and docs [Alt+S]
underscore
N. Virginia
Support
EC2 Dashboard New
Events New
Tags
Limits
INSTANCES
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts New
Scheduled Instances
Capacity Reservations
IMAGES
AMIs
ELASTIC BLOCK STORE
Volumes
Snapshots
Lifecycle Manager
NETWORK & SECURITY
Security Groups New
Elastic IPs New
Placement Groups New
Key Pairs New
Network Interfaces
LOAD BALANCING
EC2
Auto Scaling groups
Details
Activity
Automatic scaling
Instance management
Monitoring
Instance refresh
Scaling policies (0) Info
Actions
Add policy
1
No scaling policies are currently specified
Add policy
Scheduled actions (0)
Actions
Create scheduled action
Filter scheduled actions
1
Name
Start time
End time
Recurrence
Desired capacity
Min
Max
No scheduled actions are currently specified
Create scheduled action

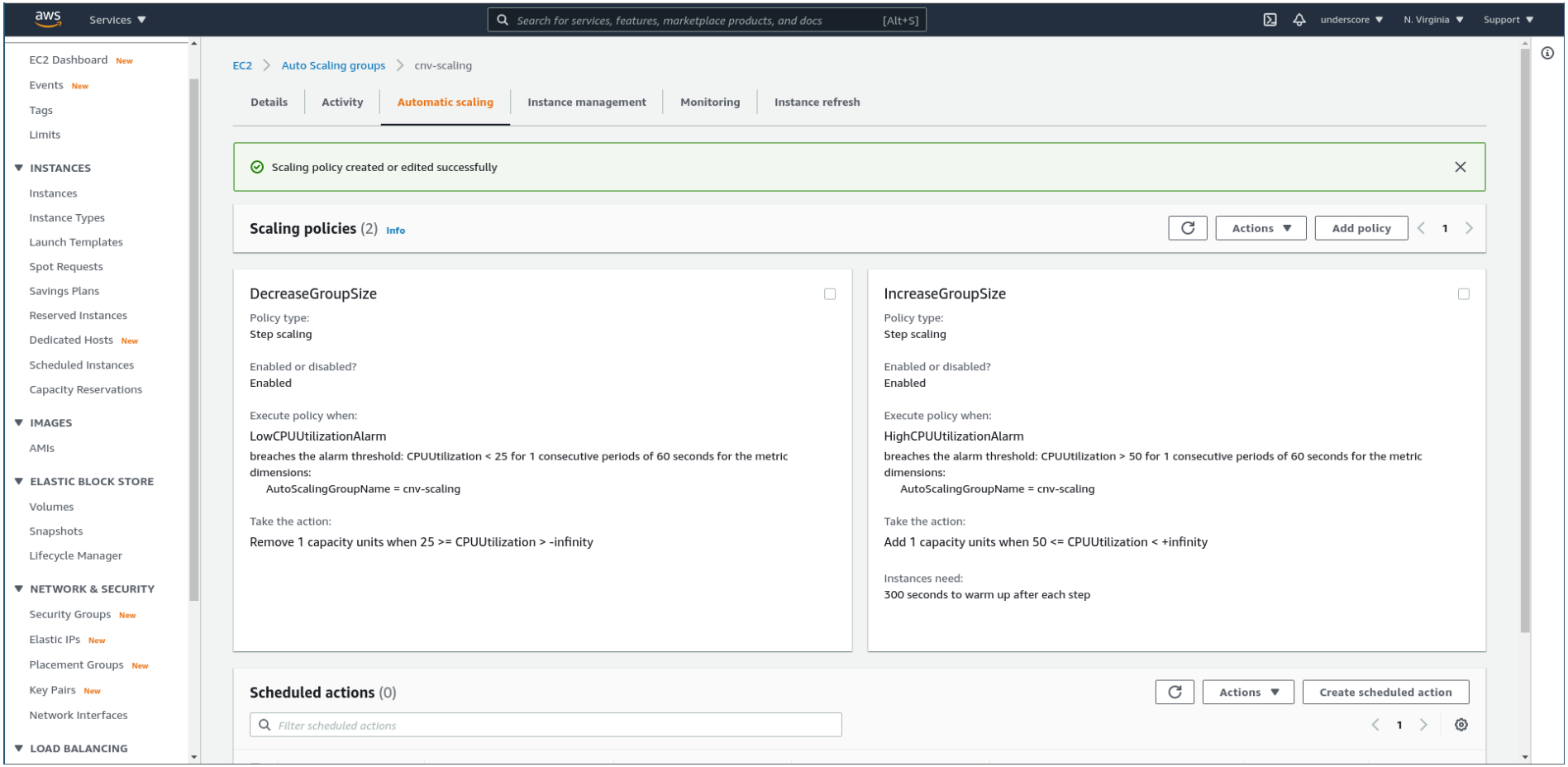
Select ‘Step scaling’, give a name to the policy and select the alarm…



Repeat for the other alarm



You should see now both policies…



Try it!

Wait for an instance of the Auto-Scale group to initialize

Generate (lots of) accesses to your web server cluster

(e.g. several browser tabs)

Attention: Before you leave

Shut your Auto-Scaler down!

Don’t waste credits!

Good work in the Cloud!