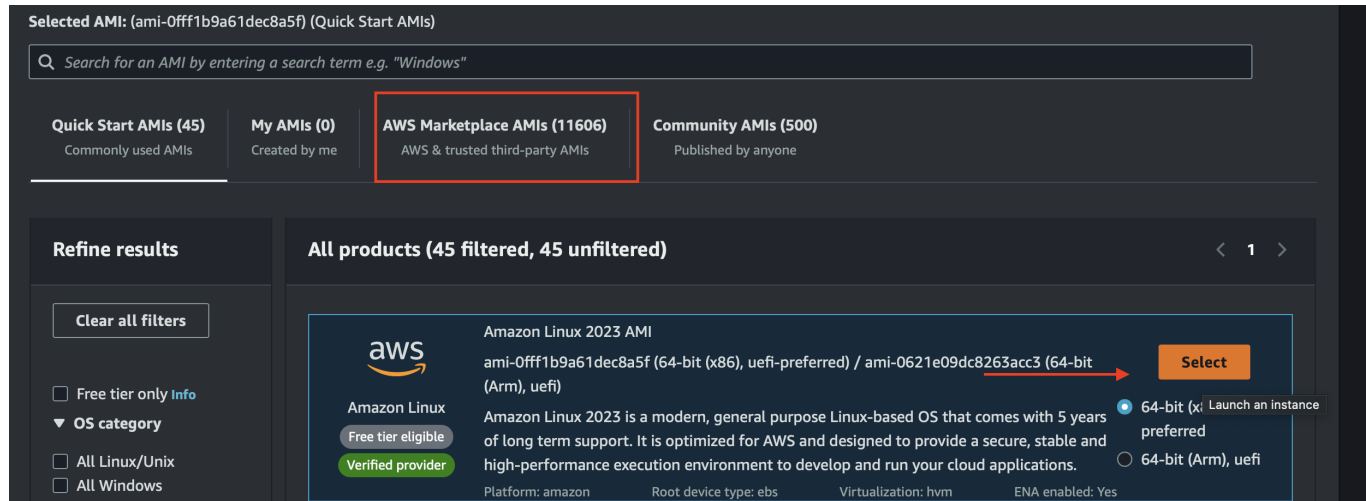


03. AWS SecOnion Lab Setup - Linux AMI Setup

AWS SecOnion Lab Setup - Linux AMI Setup

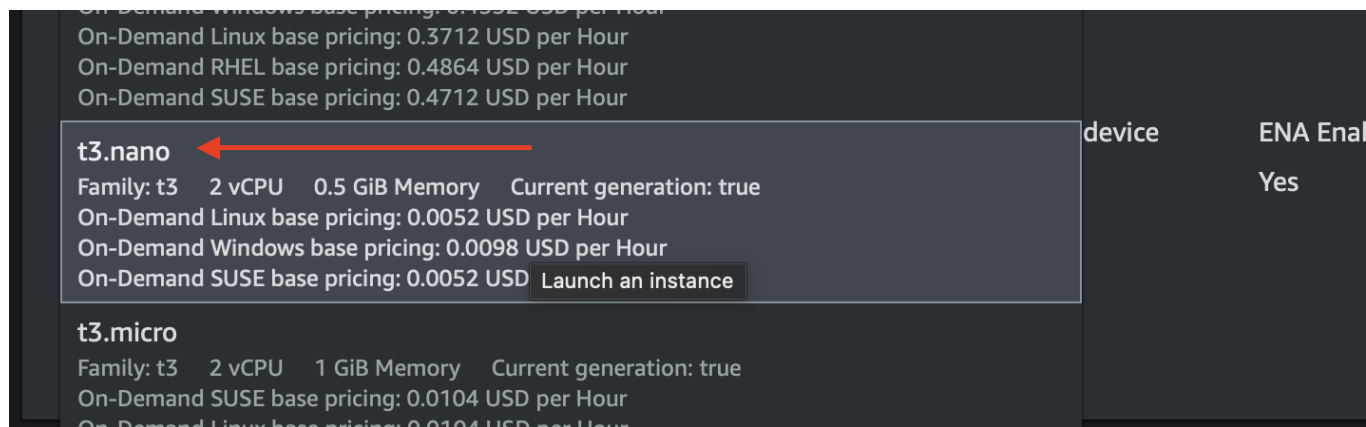
Click on Launch instances and select the basic Amazon AMI instance:



IMPORTANT: Instance type must be a t3.nano or above

Amazon Nitro instances are build to handle traffic mirroring and other related tasks that are needed for Security Onion to operate properly.

Mirror targets must be AWS Nitro Instances



Select the appropriate ssh key you create or create a new one:

▼ **Instance type** [Info](#) | [Get advice](#)

Launch an instance

Instance type

t3.nano

Family: t3 2 vCPU 0.5 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0052 USD per Hour
On-Demand Windows base pricing: 0.0098 USD per Hour
On-Demand SUSE base pricing: 0.0052 USD per Hour

☒ All generations

[Compare instance types](#)


Additional costs apply for AMIs with pre-installed software

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

SOProject

 [Create new key pair](#)

Network Configuration

Things to do:

VPC: Ensure the VPC matches the one initially created

Subnet: Ensure subnet is Public1 (same as SecurityOnion instance)

Auto-assign public IP: Enabled

Create Security Group: Ensure you enter a name and description (Linux instance should have its own security group).

Add inbound rules for all traffic:

VPC - required | [Info](#)

vpc-05ae635dc657b1187 (project-vpc)
10.0.0.0/16

Subnet | [Info](#)

subnet-0a249fd5788dafc01 project-subnet-public1-us-east-1a
VPC: vpc-05ae635dc657b1187 Owner: 481665085987
Availability Zone: us-east-1a Zone type: Availability Zone
IP addresses available: 4088 CIDR: 10.0.0.0/20

Auto-assign public IP | [Info](#) Launch an instance

Enable

Additional charges apply when outside of **free tier allowance**

Firewall (security groups) | [Info](#)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Security group name - required

Linux_Security_SG

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and . _ - / () # , @ [] + = & ; { } ! \$ *

Description - required | [Info](#)

Linux_SG

Add a security group rule for All Traffic

Add security group rule

▼ Security group rule 2 (All, All, 0.0.0.0/0) Remove

Type	Protocol	Port range
All traffic	All	All

Source type	Source	Description - optional
Custom	0.0.0.0/0	e.g. SSH for admin desktop

Launch the instance:

If you created a separate key you must change the permissions on the key using chmod.

```
ssh -i projects_linux.pem ec2-user@44.203.81.254
```

```

Downloads — ec2-user@ip-10-0-8-173:~ — ssh -i projects_linux.pem ec...

The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/HT208050.
[johns:~ johnesaw$ cd Downloads/
[johns:Downloads johnesaw$ ssh -i projects_linux.pem ec2-user@18.207.181.59
The authenticity of host '18.207.181.59 (18.207.181.59)' can't be established.
ED25519 key fingerprint is SHA256:pjAqdZsKpbWW8VpNLCwS+mO96KB5oQJOv3CzVveemPc.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:81: 44.203.81.254
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '18.207.181.59' (ED25519) to the list of known hosts.

#_
~\_ #####_ Amazon Linux 2023
~~ \_#####\
~~ \###|
~~ \#/ https://aws.amazon.com/linux/amazon-linux-2023
~~ V~' '→
~~~
~~~. .
~~~/_/
_/_/m/'

Last login: Sat Oct 12 05:24:53 2024 from 146.70.189.123
[ec2-user@ip-10-0-8-173 ~]$
```