

Encrypting SoftNAS root volume

Symptoms

By default SoftNAS do not ship an encrypted AMI, but we support the encrypted AMIs our customers create based on our AMIs

Purpose

You want to create an AMI with an Encrypted EBS root volume which can be used to deploy multiple SoftNAS instances in your AWS cloud environment without having the need to do it manually on each new deployment

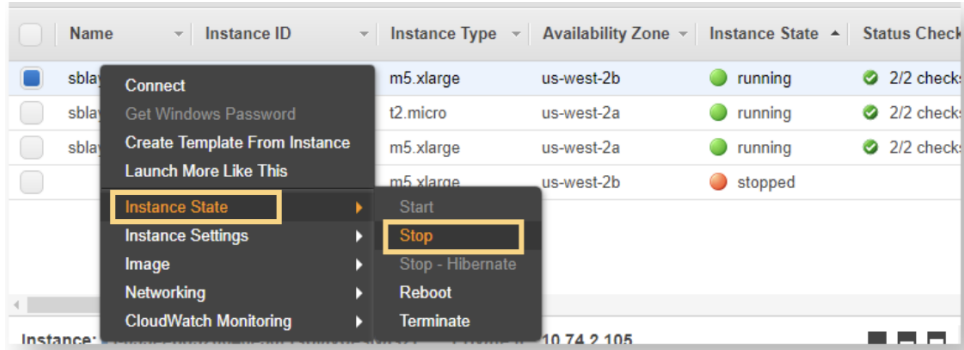
Resolution

Please follow the AWS instructions below:

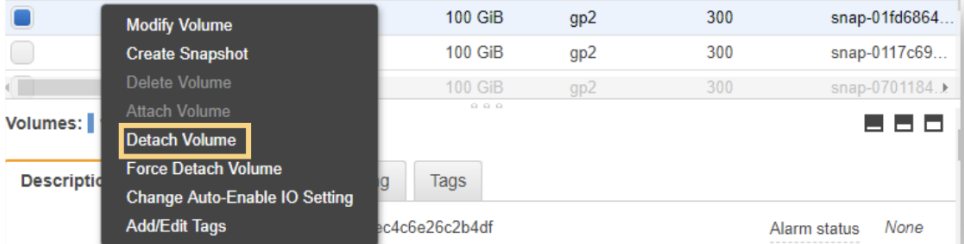
1. Launch a SoftNAS AMI from the Community or Market Place as you normally would
2. Next, ssh into the instance and delete this file --> /etc/udev/rules.d/70-persistent-net.rules

```
root@nas1:/home/ec2-user# rm /etc/udev/rules.d/70-persistent-net.rules
rm: remove regular file '/etc/udev/rules.d/70-persistent-net.rules'? y
root@nas1:/home/ec2-user#
```

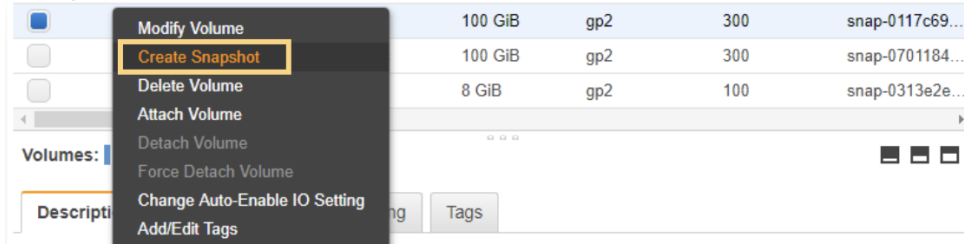
3. Next, Shutdown the instance



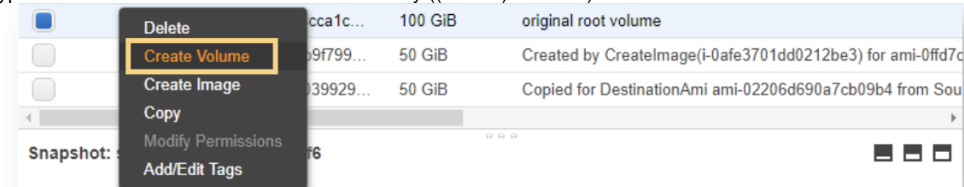
4. Detach current root volume



5. Create a snapshot of the detached root volume



6. Create a new volume from the snapshot with "Encryption" enabled. NOTE: be sure to select the same AZ your instance is on and check the Encryption button! then select the default master key ((default) aws/ebs)



Create Volume

Snapshot ID `snap-0da1e4cca1c413af6`

Volume Type `General Purpose SSD (gp2)`

Size (GiB) `100` (Min: 1 GiB, Max: 16384 GiB)

IOPS `300 / 3000` (Baseline of 3 IOPS per GiB with a minimum of 100 IOPS, burstable to 3000 IOPS)

Availability Zone* `us-west-2a`

Throughput (MB/s) Not applicable

Encryption Encrypt this volume

Master Key `aws/ebs`

7. Attach the newly created root Volume with EBS encryption to the instance as `/dev/sda1`

Attach Volume

This volume is encrypted and can only be attached to an instance that supports EBS encryption. Your supported instances are listed below.

Volume `vol-0703999eaf545a4b9` in `us-west-2b`

Instance `i-0cec5e6b97b99980f` in `us-west-2b`

Device `/dev/sda1`
Linux Devices: `/dev/sdf` through `/dev/sdp`

Note: Newer Linux kernels may rename your devices to `/dev/xvdf` through `/dev/xvdp` internally, even when the device name entered here (and shown in the details) is `/dev/sdf` through `/dev/sdp`.

[Cancel](#) [Attach](#)

8. Create AMI image of the instance (named something like Encrypted SoftNAS AMI)

Create Image

Instance ID `i-0cec5e6b97b99980f`

Image name `Encrypted SoftNAS AMI`

Image description

No reboot

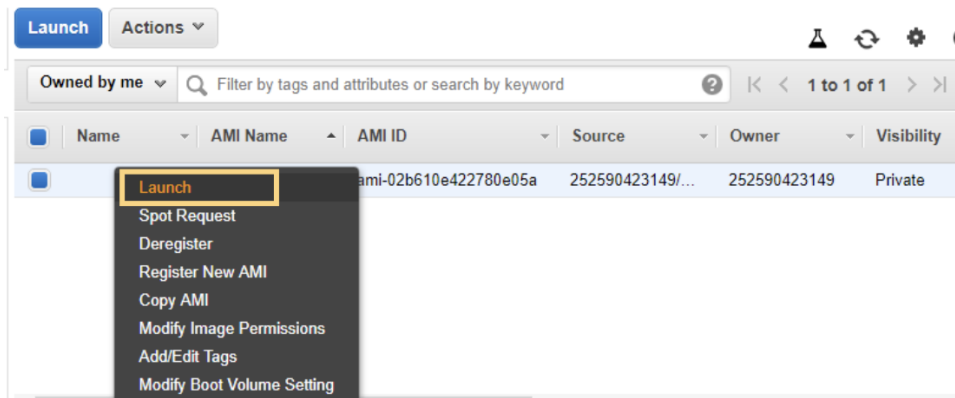
Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	<code>/dev/sda1</code>	<code>snap-01fd6864cc5667fd2</code>	<code>100</code>	<code>General Purpose S</code>	<code>300 / 3000</code>	<code>N/A</code>	<input checked="" type="checkbox"/>	<code>Encrypted</code>

[Add New Volume](#)

Total size of EBS Volumes: 100 GiB
When you create an EBS image, an EBS snapshot will also be created for each of the above volumes.

[Cancel](#) [Create Image](#)

9. After creating the new AMI is done, create a new instance with the "Encrypted SoftNAS AMI"



10. Now any instances created with this AMI will have the root volume encrypted.