

Search Node - Security Onion Distribution Installation

8/1/2025 - *Security Onion 2.4.160*

So based on the architecture we have officially setup our manager node & forward nodes, now we need to setup op search which will be storing the information from the forward nodes.

Forward Nodes

Strelka - Suricata - Zeek

Strelka - Suricata - Zeek

Elastic Agent

Elastic Agent

Forward Logs

Forward Logs

Manager

Logstash

Queue

Redis

Load Balance

Elasticsearch

Logstash

Logstash

Parse & Index

Parse & Index

Elasticsearch

Elasticsearch

Prune

Prune

Index
Management

Index
Management

Search Nodes

Security Onion 2.4 - Distributed Deployment
Created by Security Onion Solutions

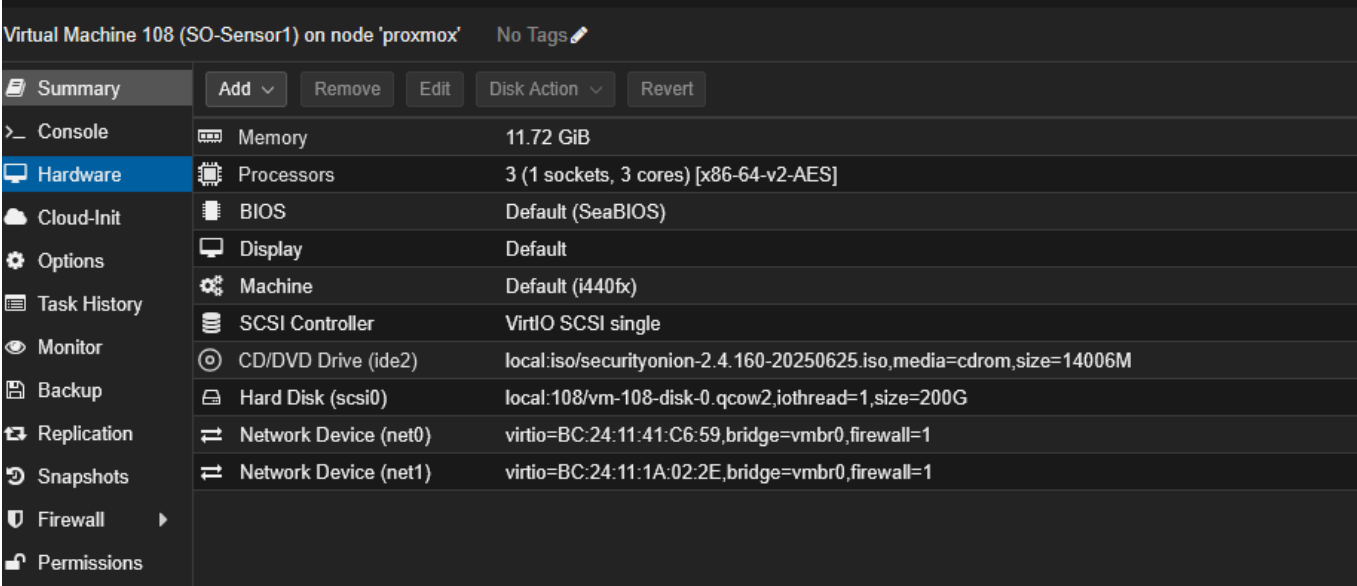
****Step 1: Creating The**

Node VM & Preparing the ISO**

Create your VM using the Security Onion ISO, here [Machine Requirements](#) is a photo of the required resources needed per application, since we have deployed the manager node and we are now setting up the sensor we are going to be creating a VM with 3 cores & 10 GBs of ram.

This sensor will be sending network traffic from the network to Security onion to be analyzed and processed.

Since we are deploying a network sniffing device like Suricata or zeek we need 2 NICs on the device to ensure one to communicate with the manager and the other for network monitoring (in a actual organization environment this would be connected to a SPAN port on a switch which has all network traffic being mirrored to that port).

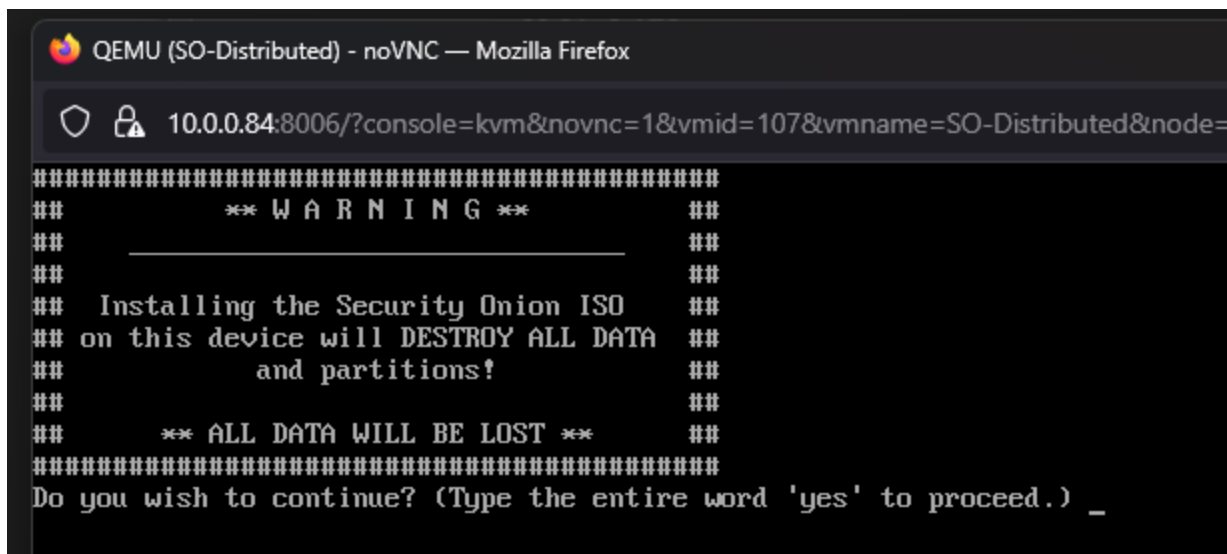


The screenshot shows the configuration interface for a Proxmox Virtual Machine (VM) named 'Virtual Machine 108 (SO-Sensor1)' on a node named 'proxmox'. The interface is in dark mode. On the left is a sidebar with navigation options: Summary, Console, Hardware (selected), Cloud-Init, Options, Task History, Monitor, Backup, Replication, Snapshots, Firewall, and Permissions. The main area displays the configuration for the selected 'Hardware' tab. At the top of the main area are buttons: 'Add', 'Remove', 'Edit', 'Disk Action', and 'Revert'. The configuration table lists various hardware components and their settings.

Component	Value
Memory	11.72 GiB
Processors	3 (1 sockets, 3 cores) [x86-64-v2-AES]
BIOS	Default (SeaBIOS)
Display	Default
Machine	Default (i440fx)
SCSI Controller	VirtIO SCSI single
CD/DVD Drive (ide2)	local:iso/securityonion-2.4.160-20250625.iso,media=cdrom,size=14006M
Hard Disk (scsi0)	local:108/vm-108-disk-0.qcow2,iosthread=1,size=200G
Network Device (net0)	virtio=BC:24:11:41:C6:59,bridge=vbr0,firewall=1
Network Device (net1)	virtio=BC:24:11:1A:02:2E,bridge=vbr0,firewall=1

Once you have created the VM make sure you start it

Once the VM is started, connect to the console and let the ISO do it's initialization required, once it's done with what it needs to do you will be prompted with;

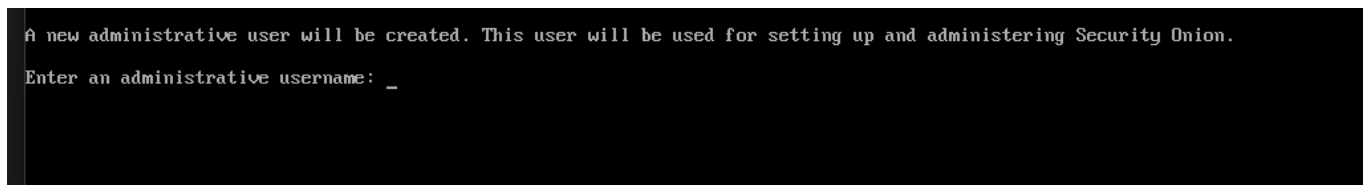


```
QEMU (SO-Distributed) - noVNC — Mozilla Firefox
10.0.0.84:8006/?console=kvm&novnc=1&vmid=107&vmname=SO-Distributed&node=
#####
##          ** W A R N I N G **          ##
##          _____                    ##
##  Installing the Security Onion ISO      ##
##  on this device will DESTROY ALL DATA  ##
##          and partitions!                ##
##          ** ALL DATA WILL BE LOST **   ##
#####
Do you wish to continue? (Type the entire word 'yes' to proceed.) _
```

Since this is a fresh machine, we know we aren't going to be losing any data, so I am going to proceed by typing 'yes'

After proceeding you will be required to enter a administrator username & pass, for the sake of the lab I am going to keep it very simple and provide the username & pass

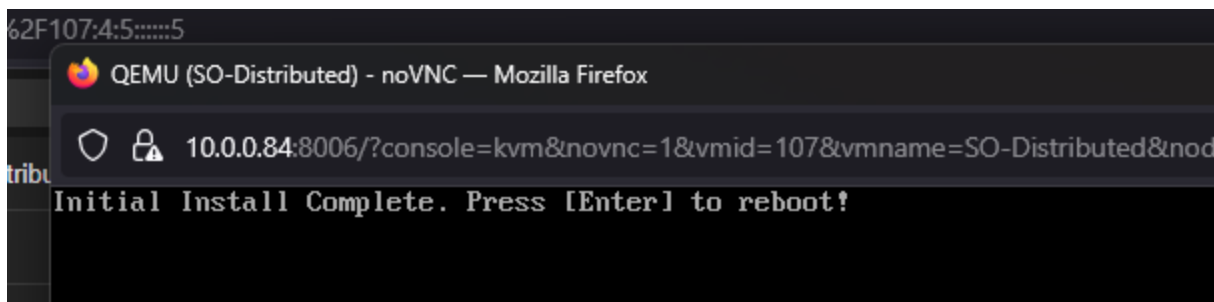
securityonion:securityonion



```
A new administrative user will be created. This user will be used for setting up and administering Security Onion.
Enter an administrative username: _
```

After that is done it is going to run through a few more startup things, be patient it can take some time.

Once it's done what it needs to do you'll see a message similar to this requesting you hit enter to reboot;



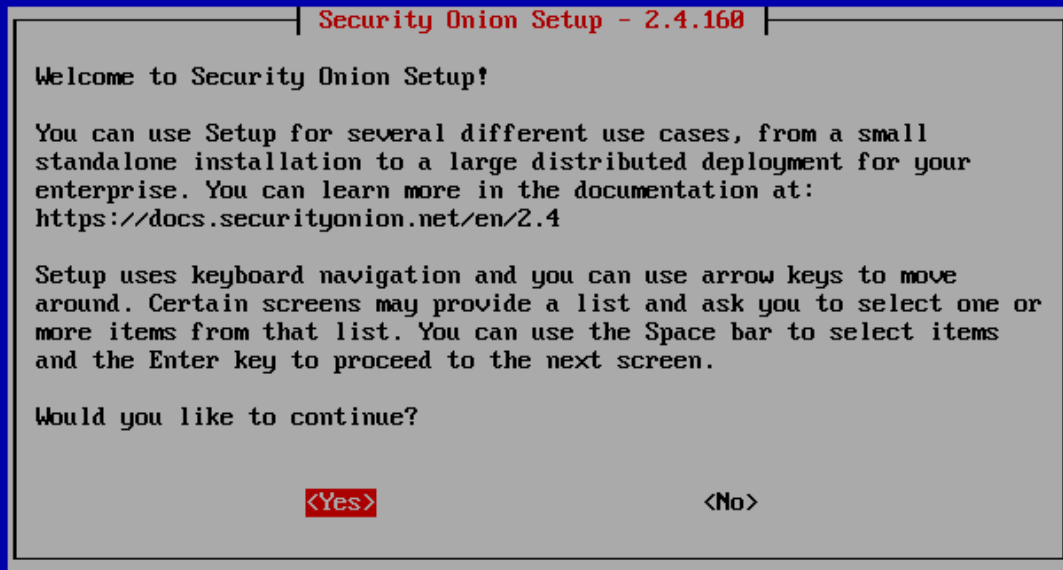
```
62F107:4:5:::5
QEMU (SO-Distributed) - noVNC — Mozilla Firefox
10.0.0.84:8006/?console=kvm&novnc=1&vmid=107&vmname=SO-Distributed&node=
Initial Install Complete. Press [Enter] to reboot!
```

So hit enter and carry on with the installation;

Step 2: Installing & Configuring The Forward Node

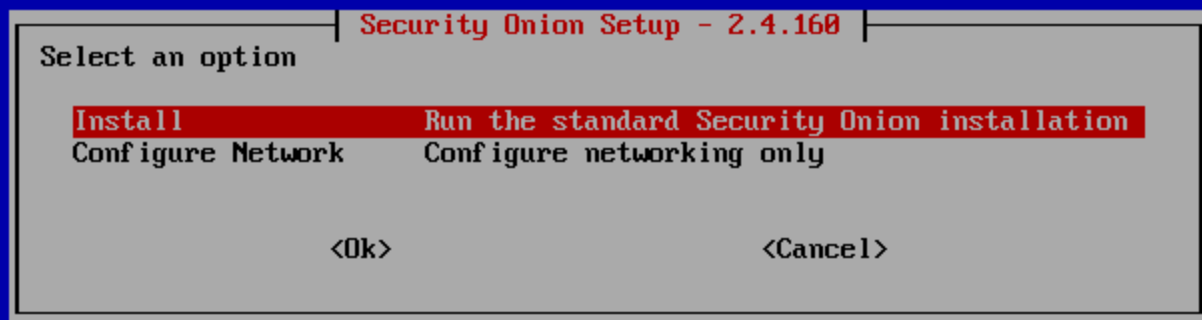
After the machine reboots, you will be prompted to enter you user & pass you previously entered.

After you have entered the credentials, you will see the configuration screen pop up.



This is where we begin to configure security onion; so obviously we wish to continue so I will be selecting "yes"

After selecting yes, you will be prompted on a screen with 2 options, this screen gives you the option to do the full install / configuration or just setup networking first. I'm going to be doing the install option as I want to do everything.



After selecting install, you are prompted with what kind of installation you want to do

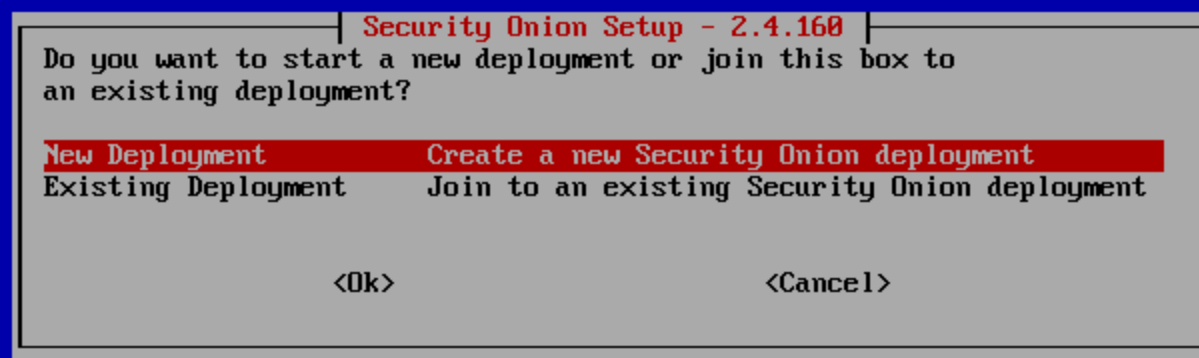


For more information regarding the different kinds of installs please visit;

<https://docs.securityonion.net/en/2.4/architecture.html>

Since we have previously installed a manager using the distributed type, we are going to be selecting that type

After you will receive a pop up asking what kind of deployment you want to do, since we already created the manager we are going to doing the existing deployment again to connect our Sensor or whatever we decide to setup to the manager



After you selected existing deployment you are going to be prompted with what you want to deploy a sensor we want to select the sensor option, but notice how there are a lot of different options for us to use, we can deploy another elastic fleet server, IDH (Intrusion Detection Honeypot), more backend storage by doing a search node, and a receiver node.