Security Onion Installation Guide

Note:

This installation guide is for Security Onion installation that is not on the ISO image provided by Security Onion. In the example below, it is shown on a Kali box, but other Linux distributions work similarly. These steps must be taken to properly install an instance of Security Onion and performing them out of order may cause errors.

Manager Node

Hardware Requirements:

4-8 CPU cores

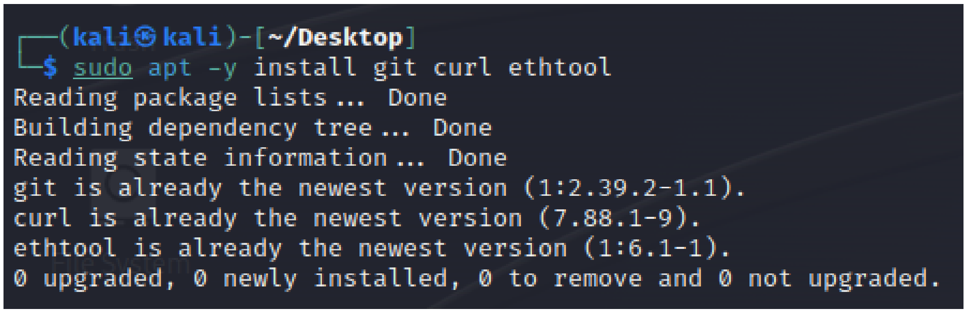
16 GB RAM

200GB to 1TB of disk space

Installation:

Step 1.

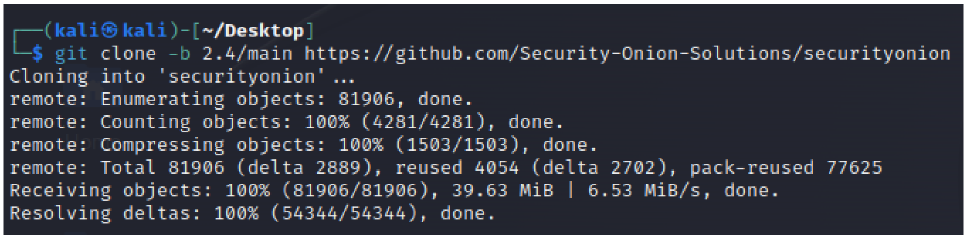
A user should open a terminal on the machine and run the following command: “sudo apt –y install git curl ethtool”. This command will update git, curl, and ethtool commands or verify that they are up to date.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt -y install git curl ethtool
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.39.2-1.1).
curl is already the newest version (7.88.1-9).
ethtool is already the newest version (1:6.1-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Step 2.

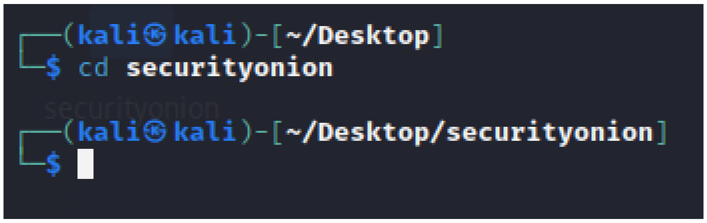
Next, a user should run the command “git clone –b 2.4/main https://github.com/Security-Onion-Solutions/securityonion”. This command will copy the current GitHub repository for Security Onion onto the VM.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ git clone -b 2.4/main https://github.com/Security-Onion-Solutions/securityonion
Cloning into 'securityonion' ...
remote: Enumerating objects: 81906, done.
remote: Counting objects: 100% (4281/4281), done.
remote: Compressing objects: 100% (1503/1503), done.
remote: Total 81906 (delta 2889), reused 4054 (delta 2702), pack-reused 77625
Receiving objects: 100% (81906/81906), 39.63 MiB | 6.53 MiB/s, done.
Resolving deltas: 100% (54344/54344), done.
```

Step 3.

Then, a user should run the command “cd securityonion”. This will transer them into the directory where the downloaded files are stored.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd securityonion

┌──(kali㉿kali)-[~/Desktop/securityonion]
└─$ 
```

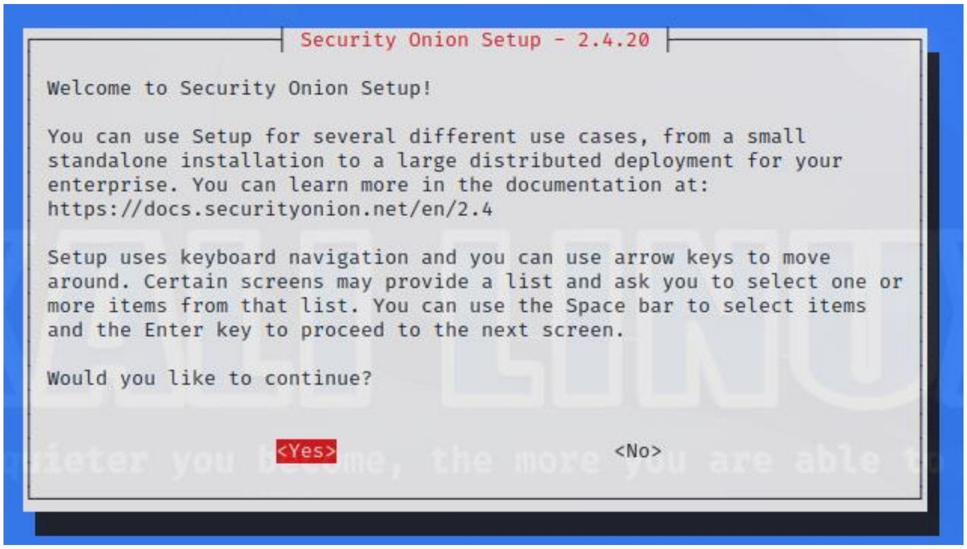
Step 4.

Finally, a user should run the command “sudo bash so-setup-network". This will start the configuration of a Security Onion instance.

Configuration:

Step 1.

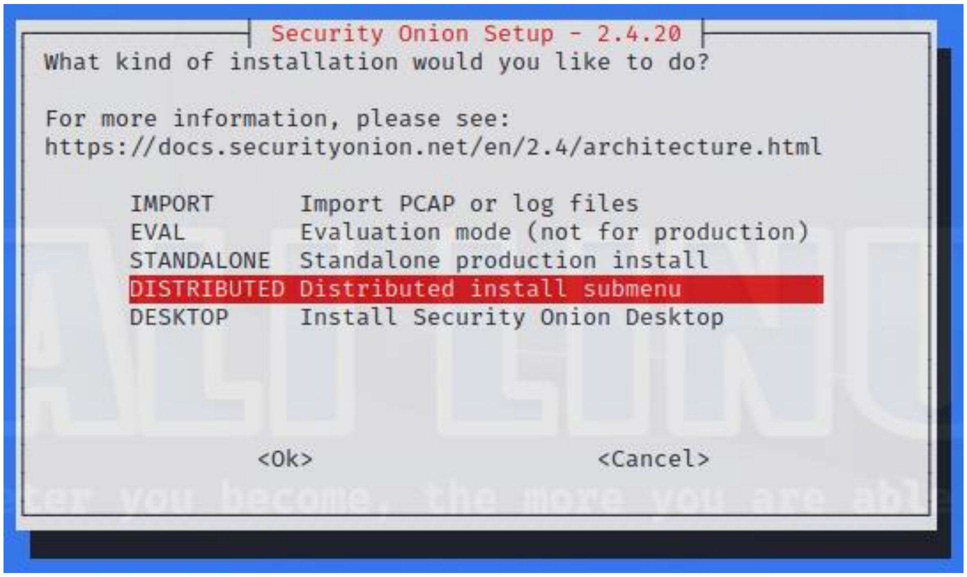
A user will first see the screen below, they should use the arrow keys to navigate to <Yes> which will be highlighted in red when selected and hit enter.



```
Security Onion Setup - 2.4.20

Welcome to Security Onion Setup!

You can use Setup for several different use cases, from a small
standalone installation to a large distributed deployment for your
enterprise. You can learn more in the documentation at:
https://docs.securityonion.net/en/2.4

Setup uses keyboard navigation and you can use arrow keys to move
around. Certain screens may provide a list and ask you to select one or
more items from that list. You can use the Space bar to select items
and the Enter key to proceed to the next screen.

Would you like to continue?

                <Yes>                        <No>
```

Step 2.

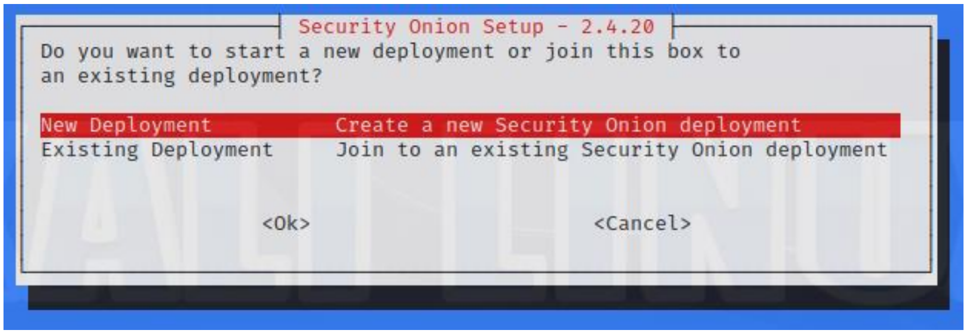
Next, a user will see this screen, they should navigate using the arrow keys to the installation that they would like to use, for this project it is **Distributed**, then hit enter.



```
Security Onion Setup - 2.4.20
What kind of installation would you like to do?

For more information, please see:
https://docs.securityonion.net/en/2.4/architecture.html

      IMPORT      Import PCAP or log files
      EVAL        Evaluation mode (not for production)
      STANDALONE  Standalone production install
      DISTRIBUTED Distributed install submenu
      DESKTOP     Install Security Onion Desktop

               <Ok>                    <Cancel>
```

Step 3.

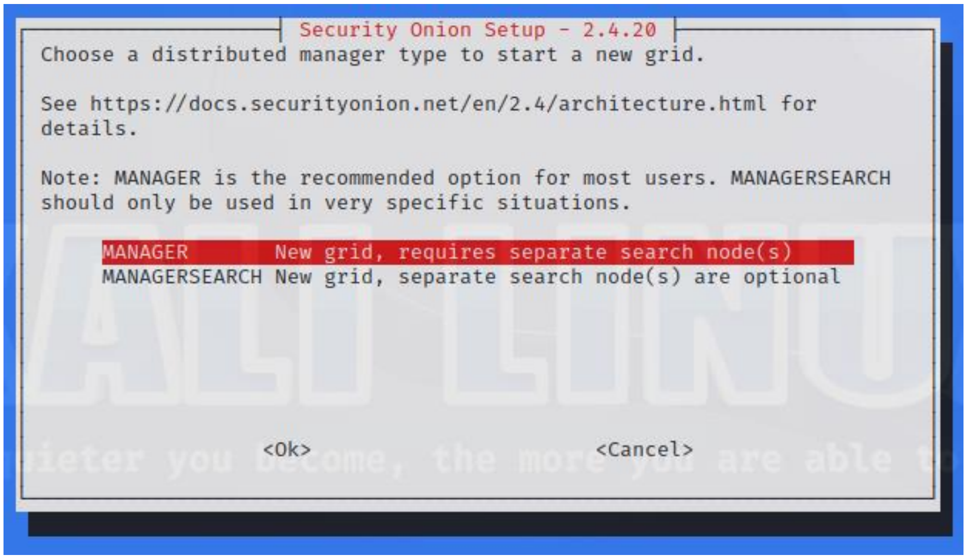
A user will then see two options, new deployment or existing deployment. Since this is the manager node that must come first, select **New Deployment**, and hit enter.



```
┤ Security Onion Setup - 2.4.20 ├
Do you want to start a new deployment or join this box to
an existing deployment?

New Deployment            Create a new Security Onion deployment
Existing Deployment       Join to an existing Security Onion deployment


                  <Ok>                      <Cancel>
```

Step 4.

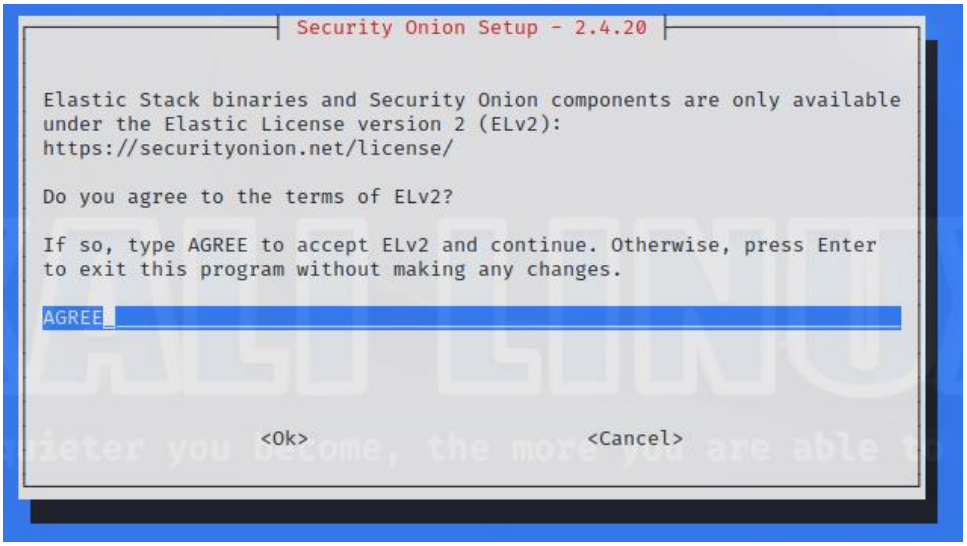
Two options for manager nodes will come up, navigate to **Manager**, then hit enter.



```
┤ Security Onion Setup - 2.4.20 ├
Choose a distributed manager type to start a new grid.

See https://docs.securityonion.net/en/2.4/architecture.html for
details.

Note: MANAGER is the recommended option for most users. MANAGERSEARCH
should only be used in very specific situations.

     MANAGER       New grid, requires separate search node(s)
     MANAGERSEARCH New grid, separate search node(s) are optional




                  <Ok>                      <Cancel>
```

Step 5.

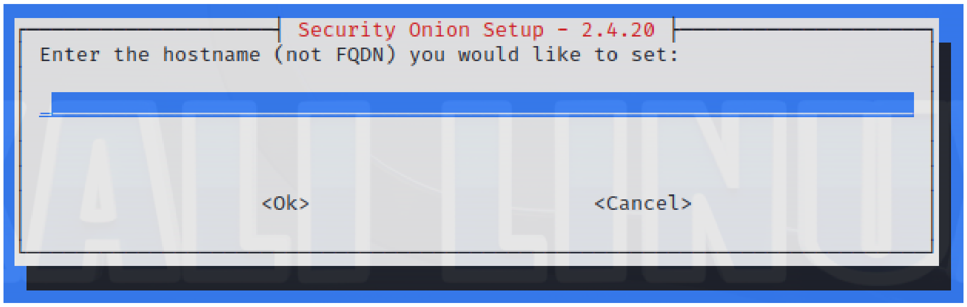
The next section will ask about agreeing to the terms of Elastic License, **type AGREE** in the text box, then hit enter.



```
Security Onion Setup - 2.4.20

Elastic Stack binaries and Security Onion components are only available
under the Elastic License version 2 (ELv2):
https://securityonion.net/license/

Do you agree to the terms of ELv2?

If so, type AGREE to accept ELv2 and continue. Otherwise, press Enter
to exit this program without making any changes.

AGREE_

          <Ok>                          <Cancel>
```

Step 6.

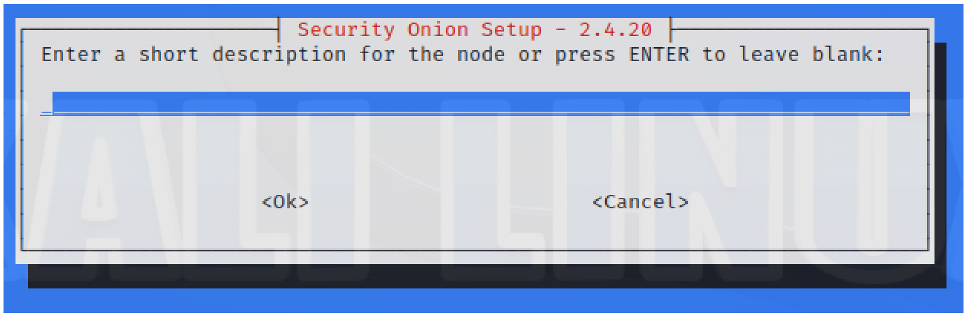
A box will come up asking what hostname should be set, this is by situation and up to the user.



```
Security Onion Setup - 2.4.20
Enter the hostname (not FQDN) you would like to set:

_

          <Ok>                          <Cancel>
```

Step 7.

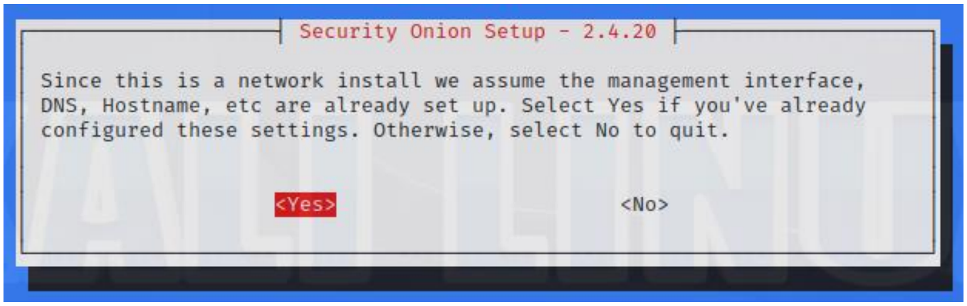
A box will come up asking for a short description, this is by situation and up to the user, but can be left blank.



```
Security Onion Setup - 2.4.20
Enter a short description for the node or press ENTER to leave blank:

_

          <Ok>                          <Cancel>
```

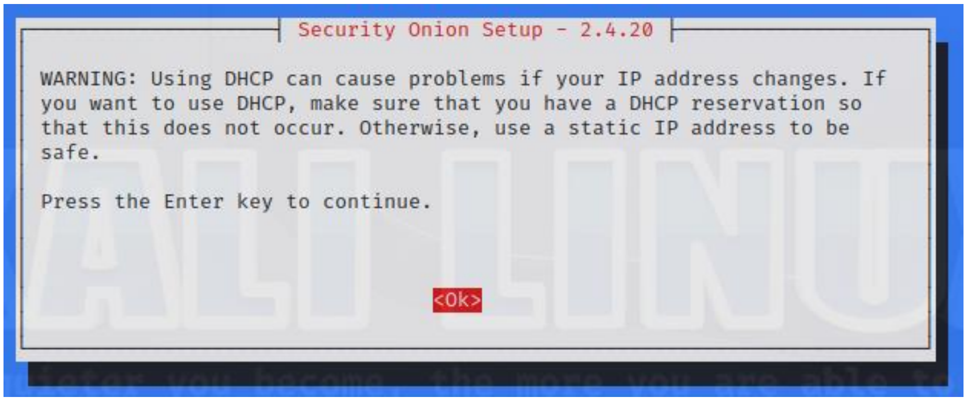
Step 8.

It will ask about DNS and network connectivity, click **Yes**.



```
Security Onion Setup - 2.4.20

Since this is a network install we assume the management interface,
DNS, Hostname, etc are already set up. Select Yes if you've already
configured these settings. Otherwise, select No to quit.
```

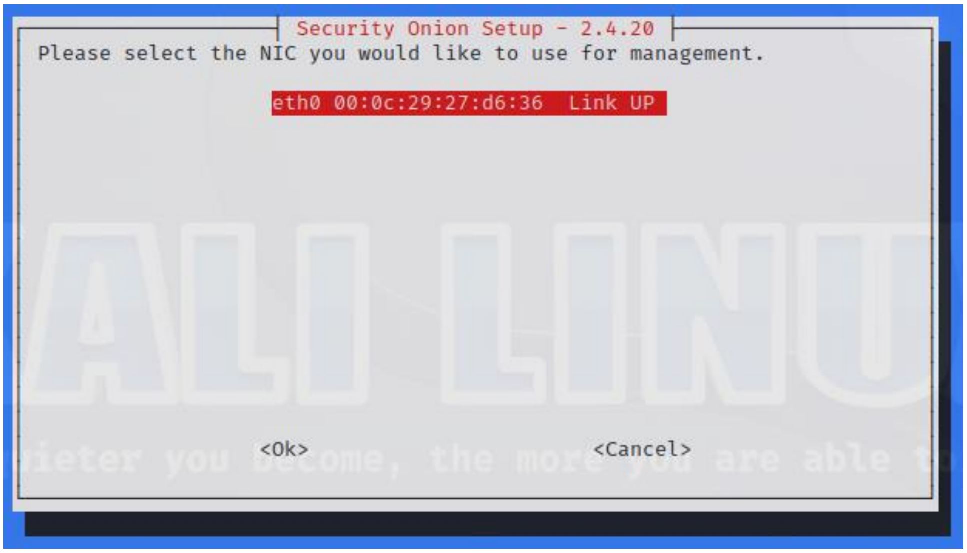
It will warn about DHCP and recommends static IP addresses.



```
Security Onion Setup - 2.4.20

WARNING: Using DHCP can cause problems if your IP address changes. If
you want to use DHCP, make sure that you have a DHCP reservation so
that this does not occur. Otherwise, use a static IP address to be
safe.

Press the Enter key to continue.
```

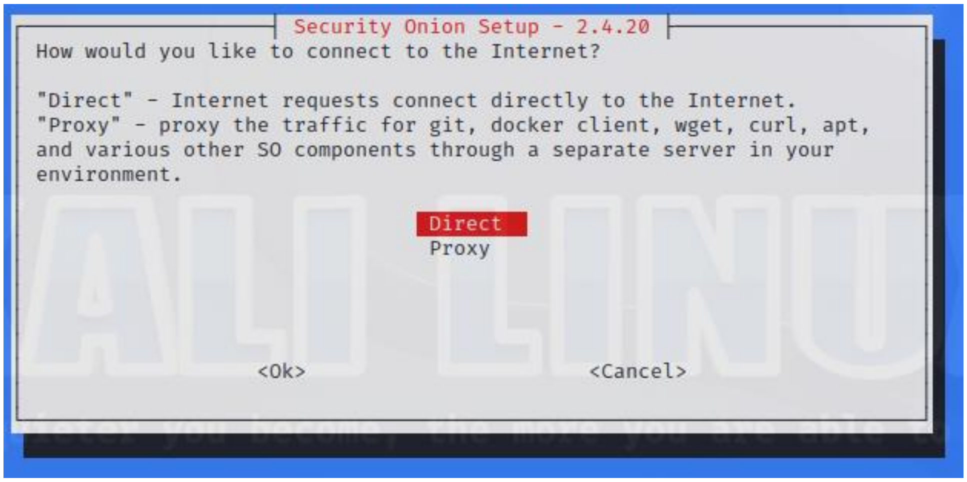
Step 9.

It will ask to select a NIC to use for management or a way to connect, select the best option.



```
Security Onion Setup - 2.4.20
Please select the NIC you would like to use for management.

eth0 00:0c:29:27:d6:36  Link UP
```

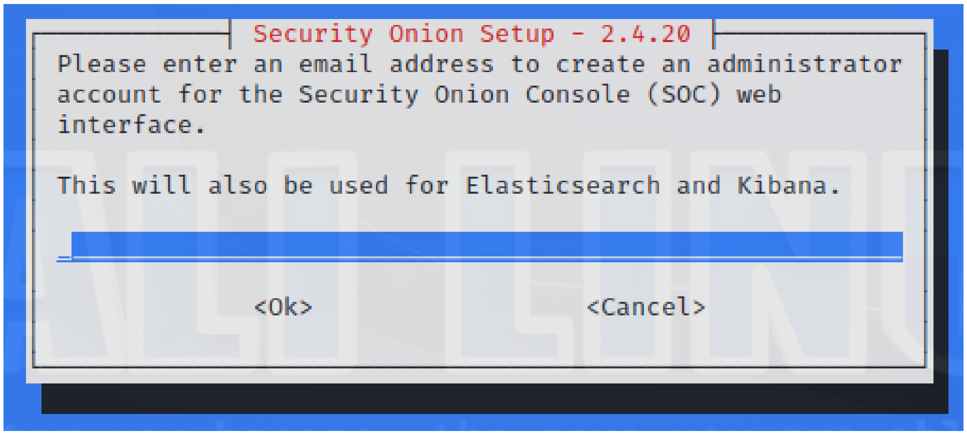
It also asks about direct vs proxy internet connection.



```
Security Onion Setup - 2.4.20
How would you like to connect to the Internet?

"Direct" - Internet requests connect directly to the Internet.
"Proxy" - proxy the traffic for git, docker client, wget, curl, apt,
and various other SO components through a separate server in your
environment.

                      Direct
                      Proxy

          <Ok>                      <Cancel>
```

Step 10.

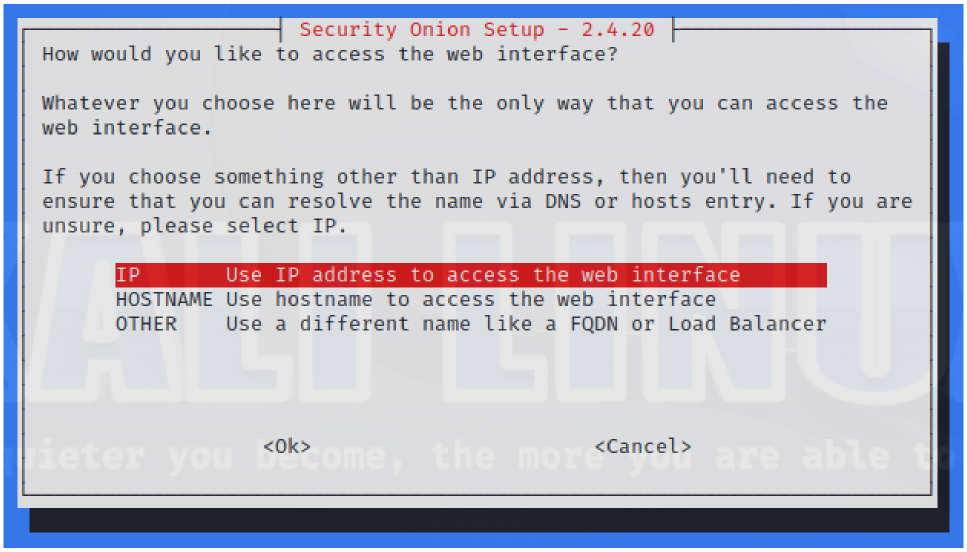
It will ask about an email address to be used for Elasticsearch and Kibana.



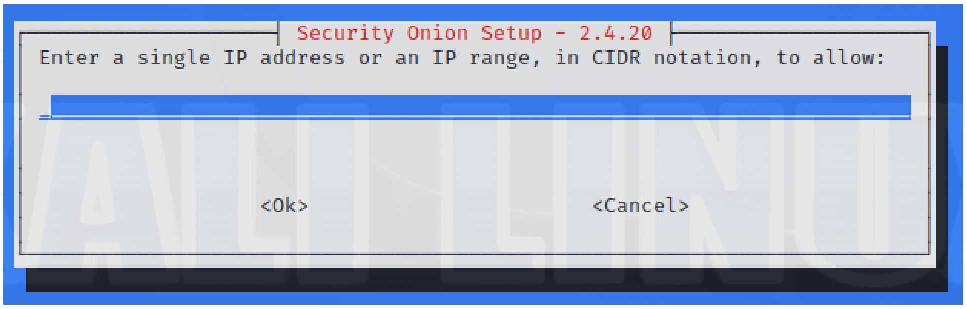
```
Security Onion Setup - 2.4.20
Please enter an email address to create an administrator
account for the Security Onion Console (SOC) web
interface.

This will also be used for Elasticsearch and Kibana.

_

          <Ok>                      <Cancel>
```

Step 11.

It asks how the web interface should be accessed.



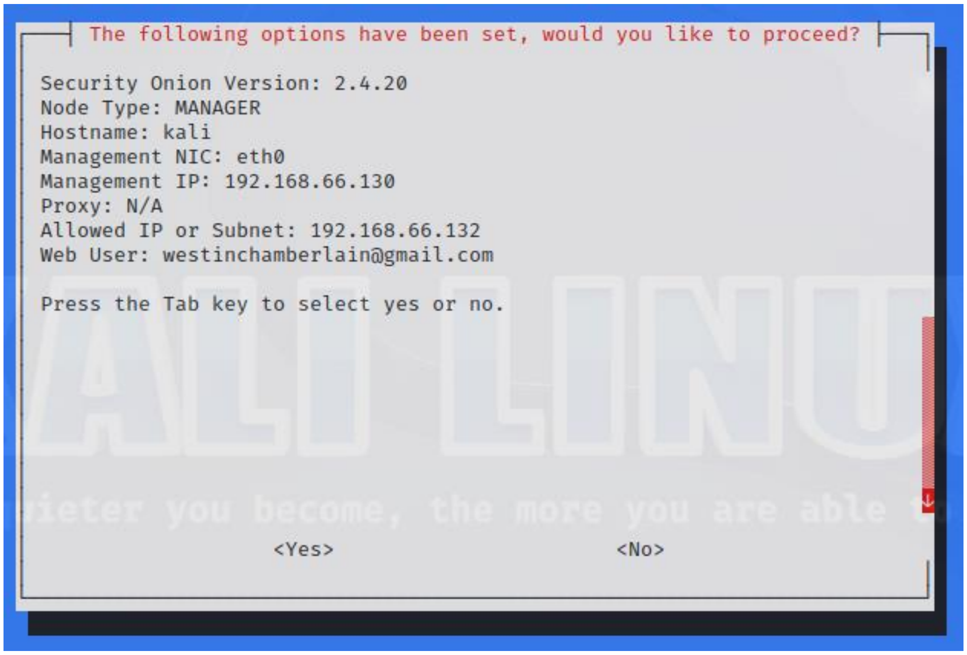
```
Security Onion Setup - 2.4.20
How would you like to access the web interface?

Whatever you choose here will be the only way that you can access the
web interface.

If you choose something other than IP address, then you'll need to
ensure that you can resolve the name via DNS or hosts entry. If you are
unsure, please select IP.

      IP       Use IP address to access the web interface
      HOSTNAME Use hostname to access the web interface
      OTHER    Use a different name like a FQDN or Load Balancer
```



```
Security Onion Setup - 2.4.20
Enter a single IP address or an IP range, in CIDR notation, to allow:
```

Step 12.

Example final output:



```
The following options have been set, would you like to proceed?

Security Onion Version: 2.4.20
Node Type: MANAGER
Hostname: kali
Management NIC: eth0
Management IP: 192.168.66.130
Proxy: N/A
Allowed IP or Subnet: 192.168.66.132
Web User: westinchamberlain@gmail.com

Press the Tab key to select yes or no.
```

Forward Node

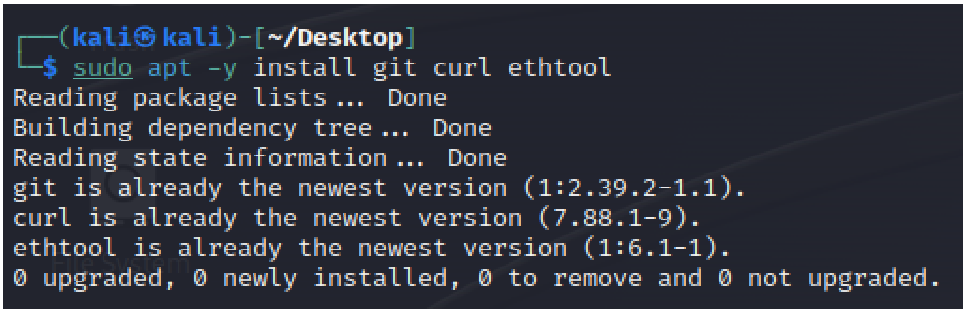
Hardware Requirements:

Very dependent on traffic captured.

Installation:

Step 1.

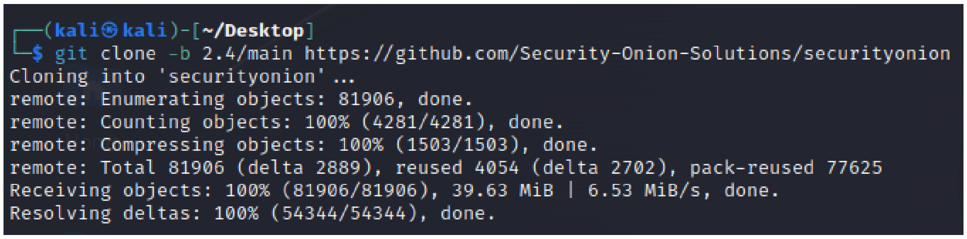
A user should open a terminal on the machine and run the following command: “sudo apt –y install git curl ethtool”. This command will update git, curl, and ethtool commands or verify that they are up to date.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo apt -y install git curl ethtool
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
git is already the newest version (1:2.39.2-1.1).
curl is already the newest version (7.88.1-9).
ethtool is already the newest version (1:6.1-1).
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Step 2.

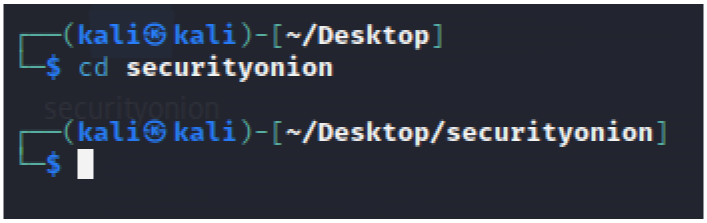
Next, a user should run the command “git clone –b 2.4/main https://github.com/Security-Onion-Solutions/securityonion”. This command will copy the current GitHub repository for Security Onion onto the VM.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ git clone -b 2.4/main https://github.com/Security-Onion-Solutions/securityonion
Cloning into 'securityonion'...
remote: Enumerating objects: 81906, done.
remote: Counting objects: 100% (4281/4281), done.
remote: Compressing objects: 100% (1503/1503), done.
remote: Total 81906 (delta 2889), reused 4054 (delta 2702), pack-reused 77625
Receiving objects: 100% (81906/81906), 39.63 MiB | 6.53 MiB/s, done.
Resolving deltas: 100% (54344/54344), done.
```

Step 3.

Then, a user should run the command “cd securityonion”. This will transer them into the directory where the downloaded files are stored.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ cd securityonion

┌──(kali㉿kali)-[~/Desktop/securityonion]
└─$ ▌
```

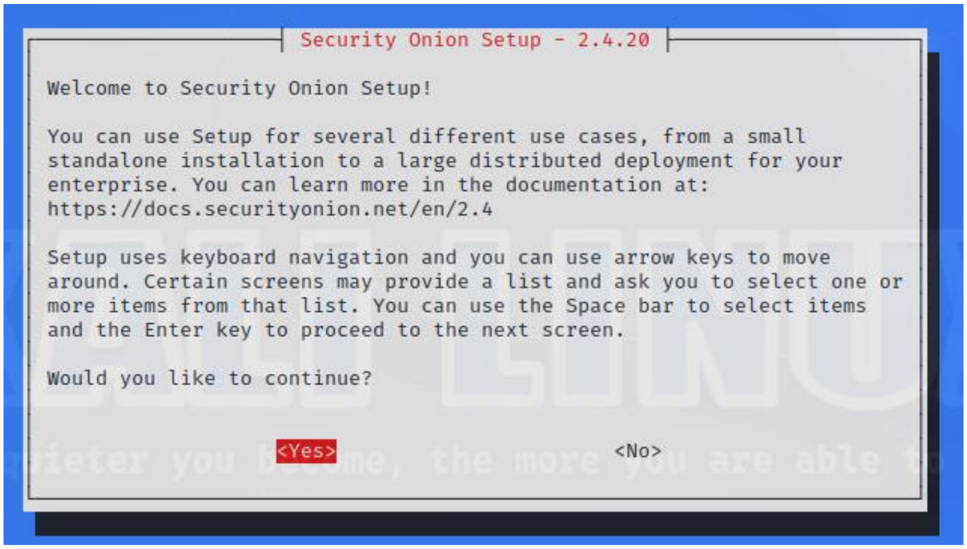
Step 4.

Finally, a user should run the command “sudo bash so-setup-network". This will start the configuration of a Security Onion instance.

Configuration:

Step 1.

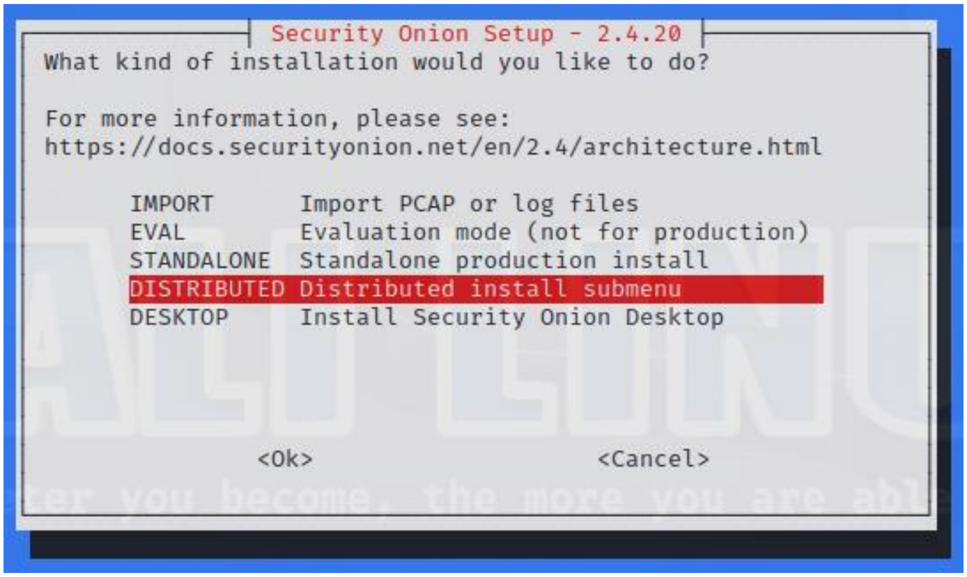
A user will first see the screen below, they should use the arrow keys to navigate to <Yes> which will be highlighted in red when selected and hit enter.



```
Security Onion Setup - 2.4.20

Welcome to Security Onion Setup!

You can use Setup for several different use cases, from a small
standalone installation to a large distributed deployment for your
enterprise. You can learn more in the documentation at:
https://docs.securityonion.net/en/2.4

Setup uses keyboard navigation and you can use arrow keys to move
around. Certain screens may provide a list and ask you to select one or
more items from that list. You can use the Space bar to select items
and the Enter key to proceed to the next screen.

Would you like to continue?

                  <Yes>                    <No>
```

Step 2.

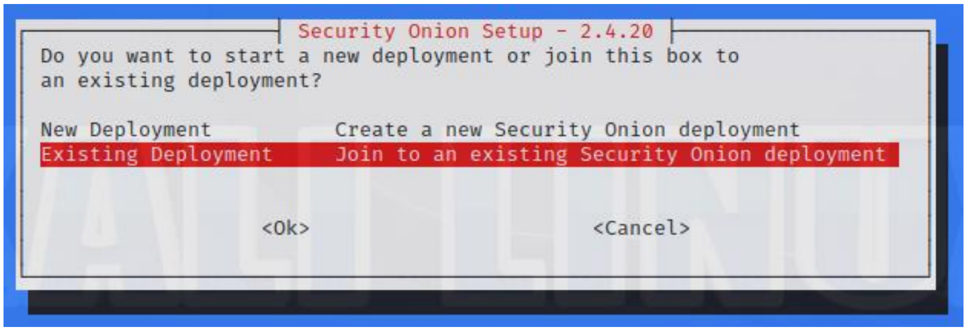
Next, a user will see this screen, they should navigate using the arrow keys to the installation that they would like to use, for this project it is **Distributed**, then hit enter.



```
Security Onion Setup - 2.4.20
What kind of installation would you like to do?

For more information, please see:
https://docs.securityonion.net/en/2.4/architecture.html

     IMPORT      Import PCAP or log files
     EVAL        Evaluation mode (not for production)
     STANDALONE  Standalone production install
     DISTRIBUTED Distributed install submenu
     DESKTOP     Install Security Onion Desktop

            <Ok>                  <Cancel>
```

Step 3.

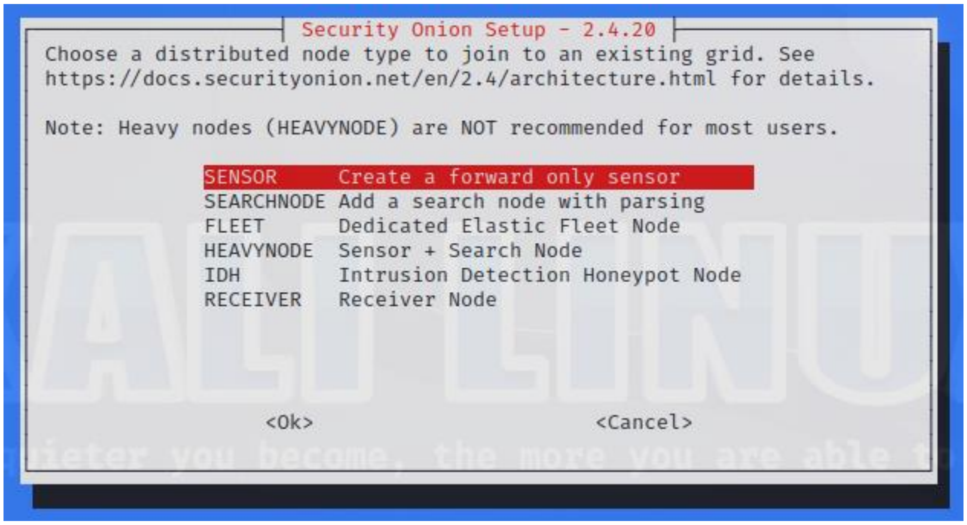
A user will then see two options, new deployment or existing deployment. Since this is the forward node, select **Existing Deployment**, and hit enter.



```
Security Onion Setup - 2.4.20
Do you want to start a new deployment or join this box to
an existing deployment?

New Deployment          Create a new Security Onion deployment
Existing Deployment     Join to an existing Security Onion deployment

                  <Ok>                      <Cancel>
```

Step 4.

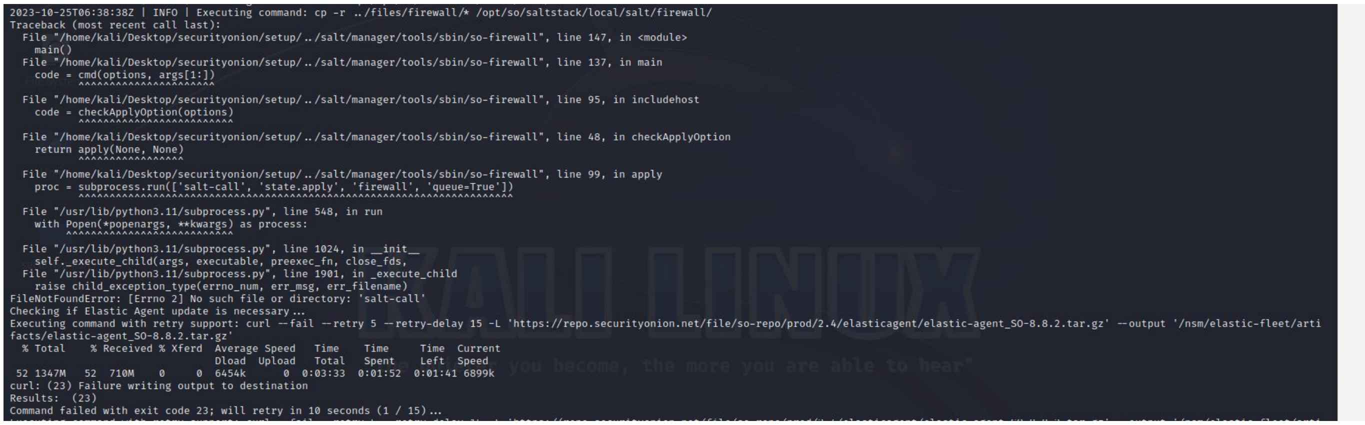
Select the type of distributed node being selected, in this case **Sensor**, and hit enter.



```
Security Onion Setup - 2.4.20
Choose a distributed node type to join to an existing grid. See
https://docs.securityonion.net/en/2.4/architecture.html for details.

Note: Heavy nodes (HEAVYNODE) are NOT recommended for most users.

             SENSOR     Create a forward only sensor
             SEARCHNODE Add a search node with parsing
             FLEET      Dedicated Elastic Fleet Node
             HEAVYNODE  Sensor + Search Node
             IDH        Intrusion Detection Honeypot Node
             RECEIVER   Receiver Node

                  <Ok>                      <Cancel>
```

Errors:

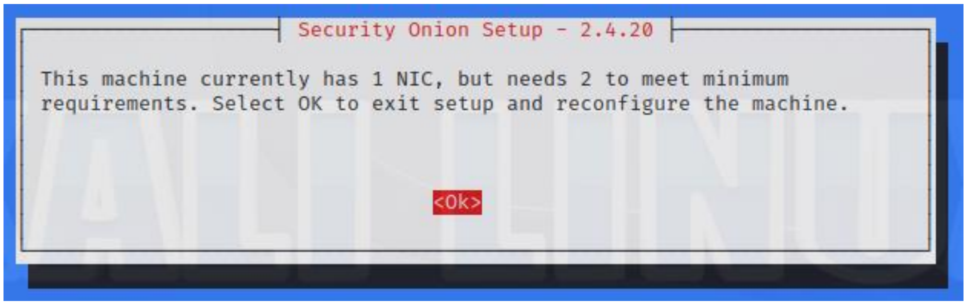
Manager Node:



```
2023-10-25T06:38:38Z | INFO | Executing command: cp -r ../files/firewall/* /opt/so/saltstack/local/salt/firewall/
Traceback (most recent call last):
  File "/home/kali/Desktop/securityonion/setup/../salt/manager/tools/sbin/so-firewall", line 147, in <module>
    main()
  File "/home/kali/Desktop/securityonion/setup/../salt/manager/tools/sbin/so-firewall", line 137, in main
    code = cmd(options, args[1:])
           ^^^^^^^^^^^^^^^^^^^^^^

  File "/home/kali/Desktop/securityonion/setup/../salt/manager/tools/sbin/so-firewall", line 95, in includehost
    code = checkApplyOption(options)
           ^^^^^^^^^^^^^^^^^^^^^^^^^

  File "/home/kali/Desktop/securityonion/setup/../salt/manager/tools/sbin/so-firewall", line 48, in checkApplyOption
    return apply(None, None)
           ^^^^^^^^^^^^^^^^^

  File "/home/kali/Desktop/securityonion/setup/../salt/manager/tools/sbin/so-firewall", line 99, in apply
    proc = subprocess.run(['salt-call', 'state.apply', 'firewall', 'queue=True'])
           ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^

  File "/usr/lib/python3.11/subprocess.py", line 548, in run
    with Popen(*popenargs, **kwargs) as process:
         ^^^^^^^^^^^^^^^^^^^^^^^^^^^

  File "/usr/lib/python3.11/subprocess.py", line 1024, in __init__
    self._execute_child(args, executable, preexec_fn, close_fds,
  File "/usr/lib/python3.11/subprocess.py", line 1901, in _execute_child
    raise child_exception_type(errno_num, err_msg, err_filename)
FileNotFoundError: [Errno 2] No such file or directory: 'salt-call'
Checking if Elastic Agent update is necessary...
Executing command with retry support: curl --fail --retry 5 --retry-delay 15 -L 'https://repo.securityonion.net/file/so-repo/prod/2.4/elasticagent/elastic-agent_SO-8.8.2.tar.gz' --output '/nsm/elastic-fleet/arti
facts/elastic-agent_SO-8.8.2.tar.gz'
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
 52 1347M   52  710M    0     0  6454k      0  0:03:33  0:01:52  0:01:41 6899k
curl: (23) Failure writing output to destination
Results:  (23)
Command failed with exit code 23; will retry in 10 seconds (1 / 15)...
```

When trying to configure, it fails when trying to complete installation after configuration is complete.

Forward Node:



Security Onion Setup - 2.4.20

This machine currently has 1 NIC, but needs 2 to meet minimum requirements. Select OK to exit setup and reconfigure the machine.

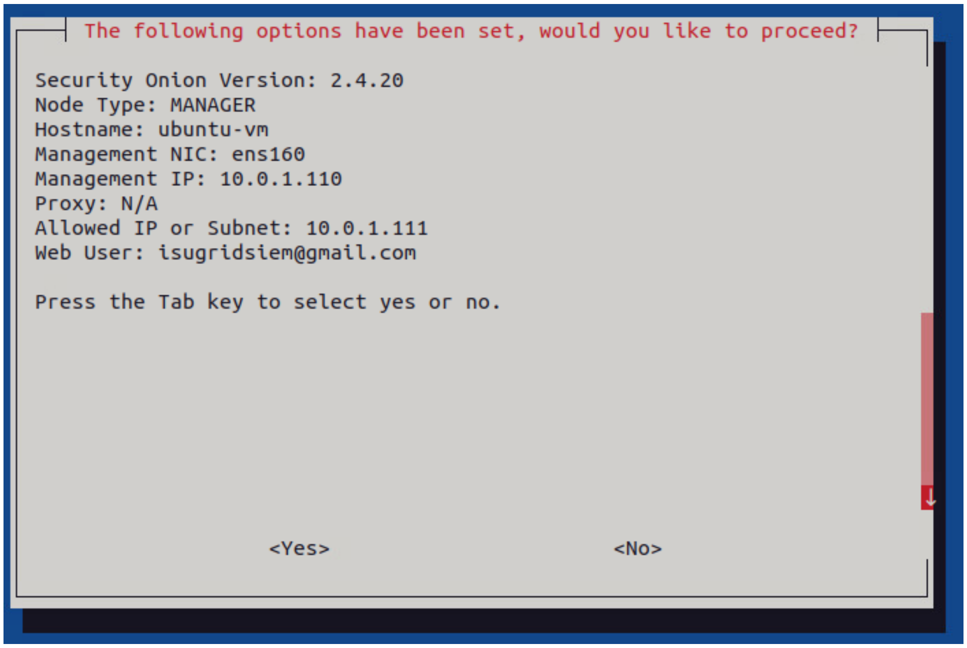
Documents:

https://docs.securityonion.net/en/latest/installation.html

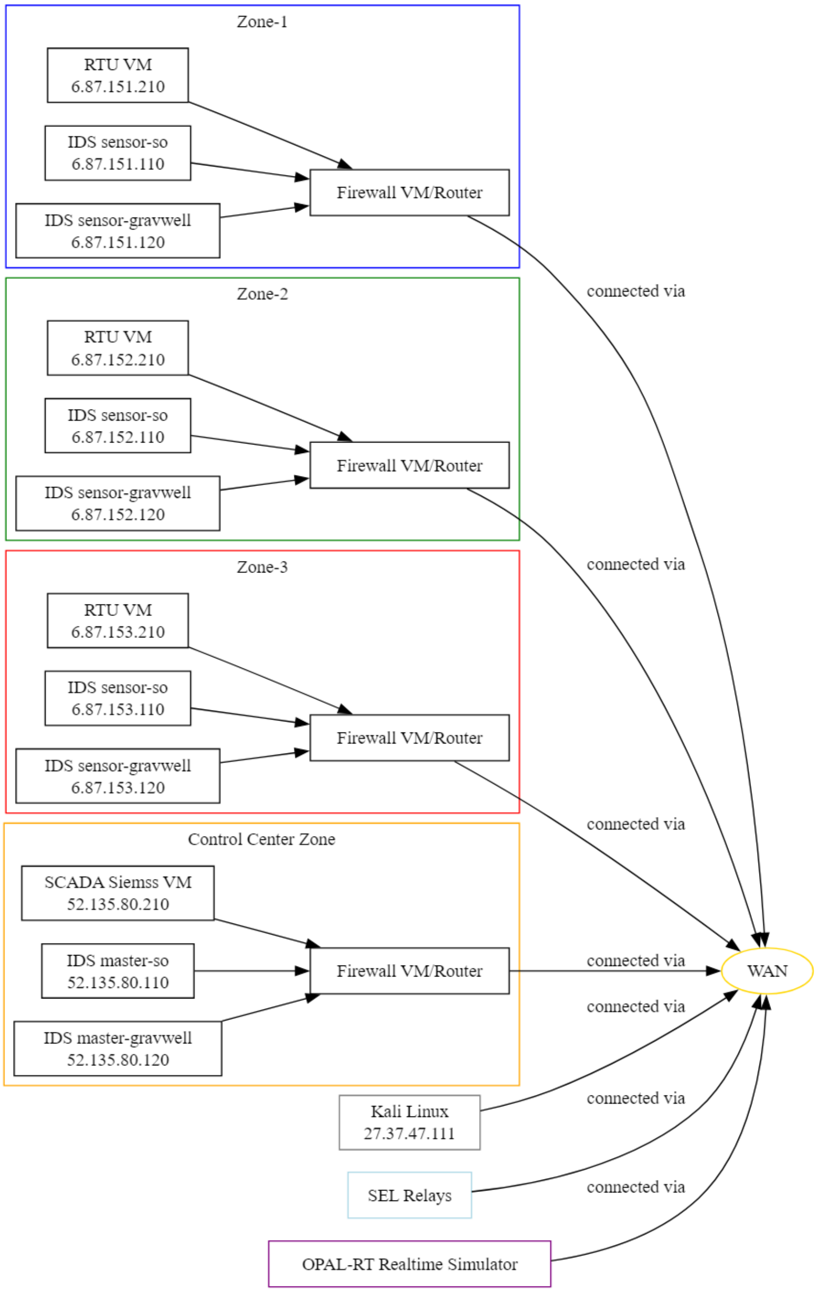
https://docs.securityonion.net/en/latest/configuration.html#configuration

https://docs.securityonion.net/en/latest/post-installation.html#post-installation

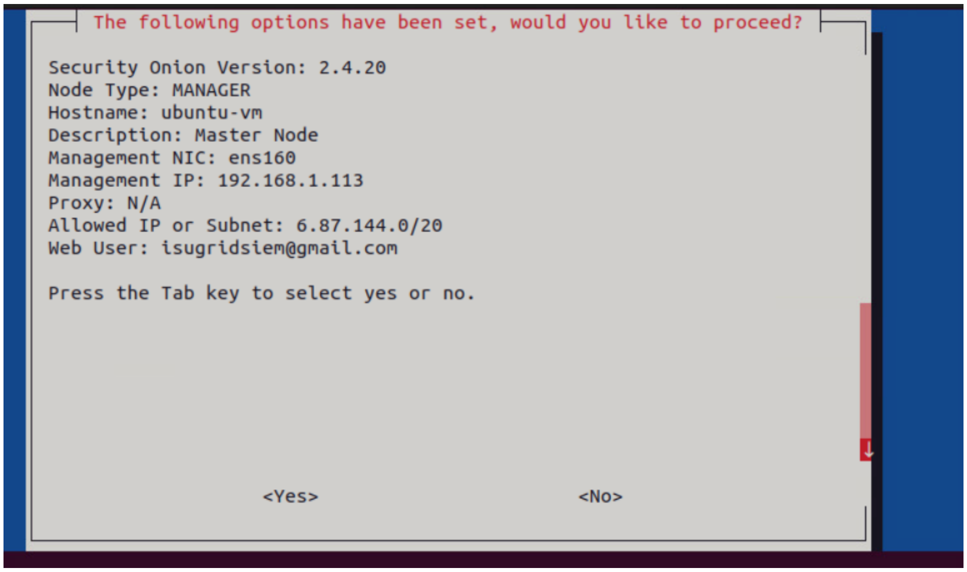
Current Installation:

- Warning about only 164 GB of free space available instead of 200 GB
- Warning about possibly an unsupported OS
- Hostname – ubuntu-vm
- isugridsiem@gmail.com - icpslab@123
- 

```
The following options have been set, would you like to proceed?

Security Onion Version: 2.4.20
Node Type: MANAGER
Hostname: ubuntu-vm
Management NIC: ens160
Management IP: 10.0.1.110
Proxy: N/A
Allowed IP or Subnet: 10.0.1.111
Web User: isugridsiem@gmail.com

Press the Tab key to select yes or no.
```



-
- Use the public IP for Manager node, also for sensor nodes
- Sensor1 – 6.87.151.110
- Sensor1 and Sensor3 ping eachother and then install manager node security onion, then ping again to see if security onion creates new firewall rules

- 

```
The following options have been set, would you like to proceed?

Security Onion Version: 2.4.20
Node Type: MANAGER
Hostname: ubuntu-vm
Description: Master Node
Management NIC: ens160
Management IP: 192.168.1.113
Proxy: N/A
Allowed IP or Subnet: 6.87.144.0/20
Web User: isugridsiem@gmail.com

Press the Tab key to select yes or no.
```

- Cannot set up manager node on sensor 3 vm; it fails unsure if this is because the manager node is set up on another machine.
- The pings work before installation and fail pings from other devices after, but can still ping them.
- Online it is declared to be the NIC or NAT not having another IP address or a networking issue.
-