Additional Information to add in as part of RMF work.

• Repository/Registry section needs to be rebuilt, using aptly instead of apt-mirror • Add Table of Contents

Armory Instructions

• see README

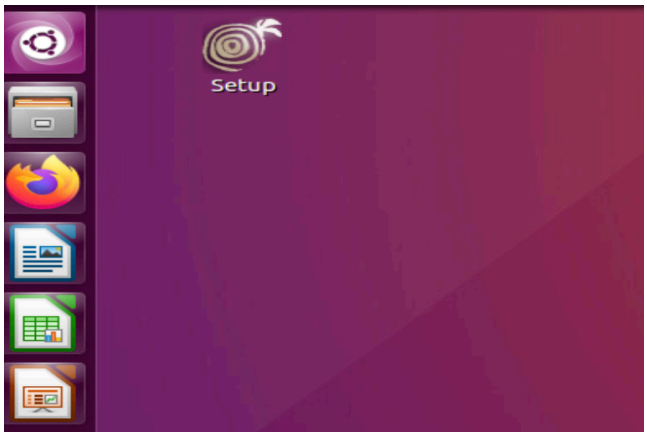
Deploy Standalone Node

With a Standalone deployment strategy, there is one single bare metal node that hosts all the services used by a Master, a Storage, and Sensor nodes. Because of this, the node requires additional resources. Within the DDS-M kit, one node (model num ?) will have enough Ram and CPU, but additional storage will have to be configured. There is in the neighborhood of 27 TB of storage available, however it is not pulled into the storage pull during the automated deployment. This can be done to the user's discretion after the automated deployment is complete.

There are three ways to run through the Security Onion configuration. The setup wizard, the setup TUI, or running a pre-configured configuration file. The most common way is the setup wizard.

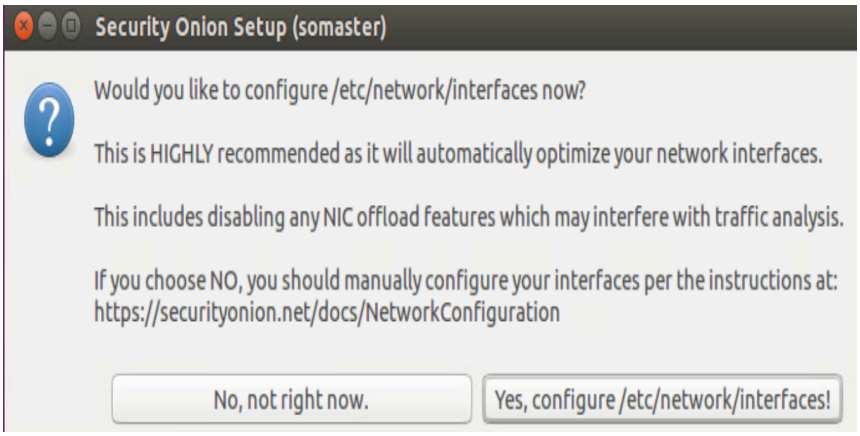
Setup Wizard

Follow the steps below to install Security Onion using the setup wizard.

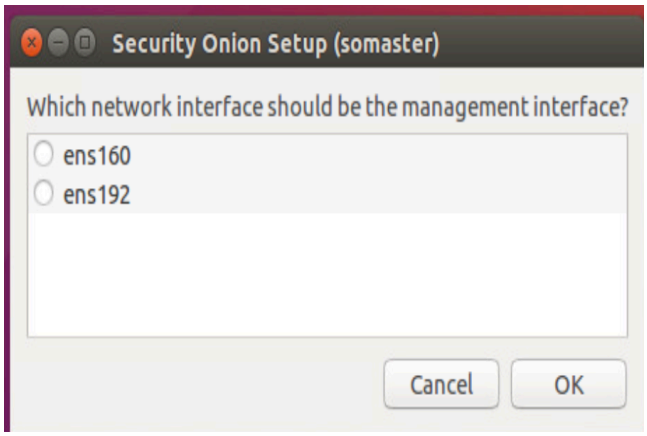


Navigate to the Desktop and double click the Setup icon

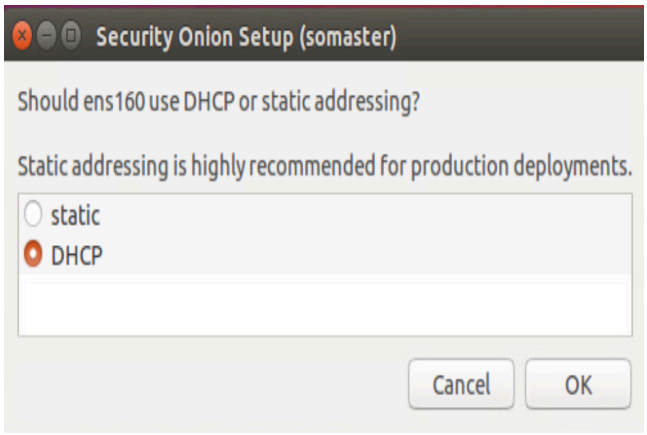
A welcome screen will appear



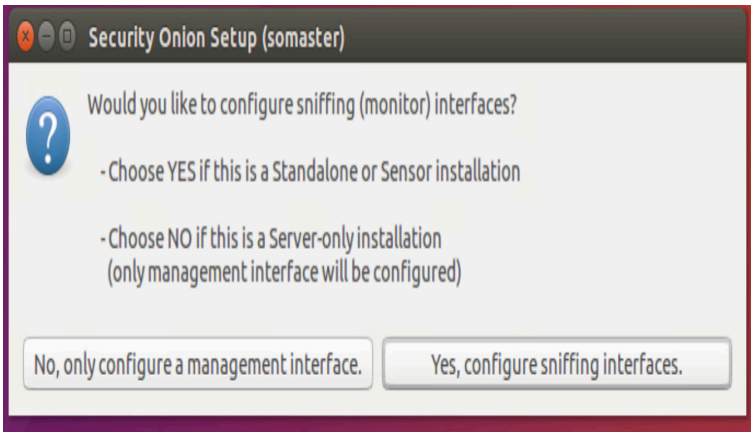
During the initial setup, choose to configure the network interfaces



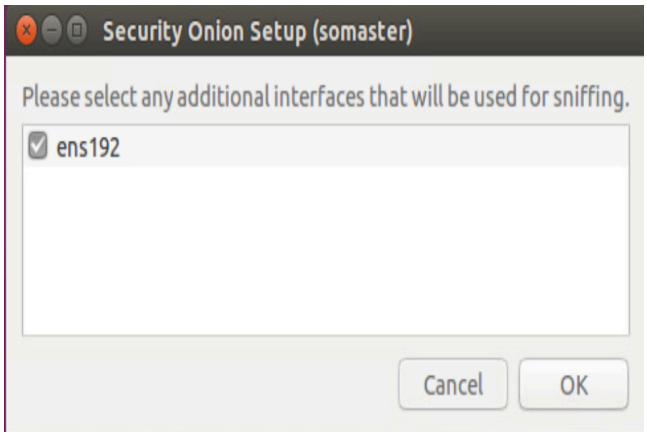
Select which interface should be the management interface



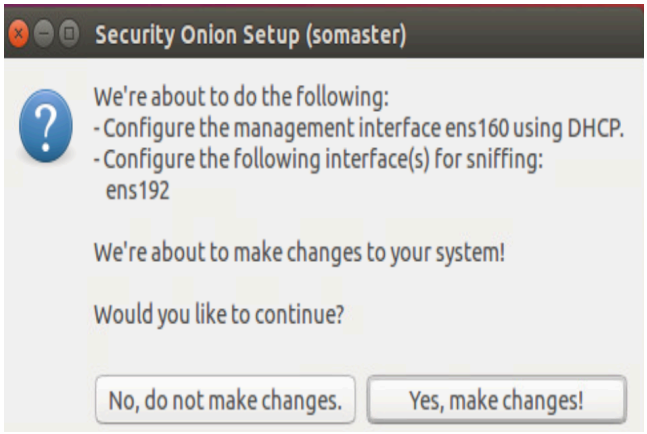
For this deployment, choose DHCP, however setting static network information is an option



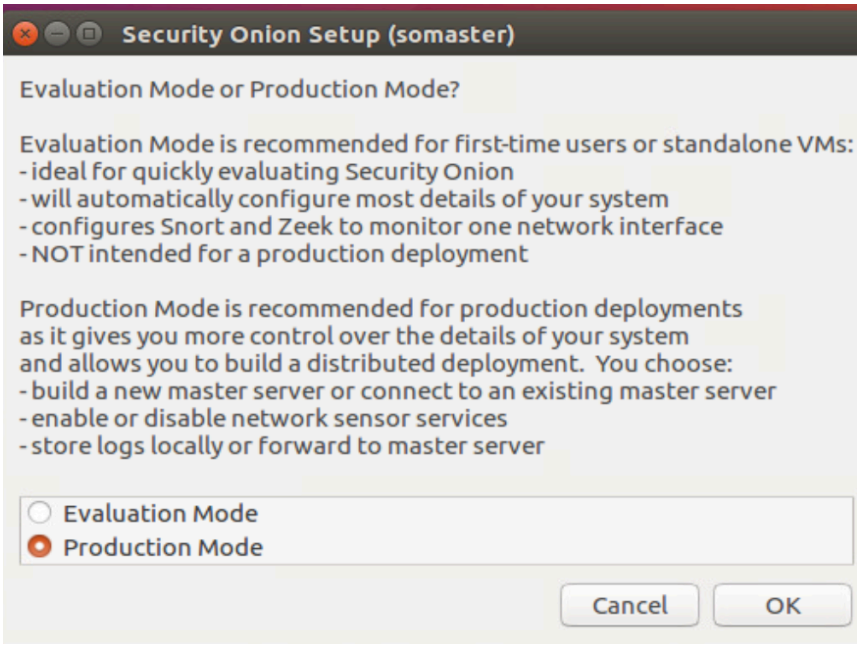
For the Standalone deployment, choose Yes to configure a sniffing interface



You may choose which interfaces you want to be the sniffing interfaces. If there is only one, it will be selected by default

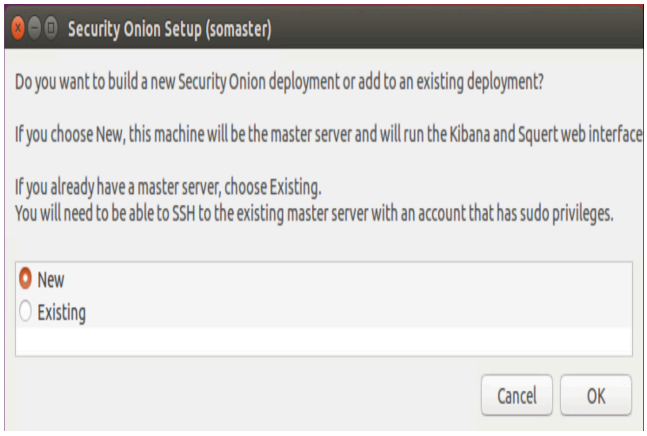


Accept the prompt to make Network changes. At this point the wizard will ask to reboot, click Yes

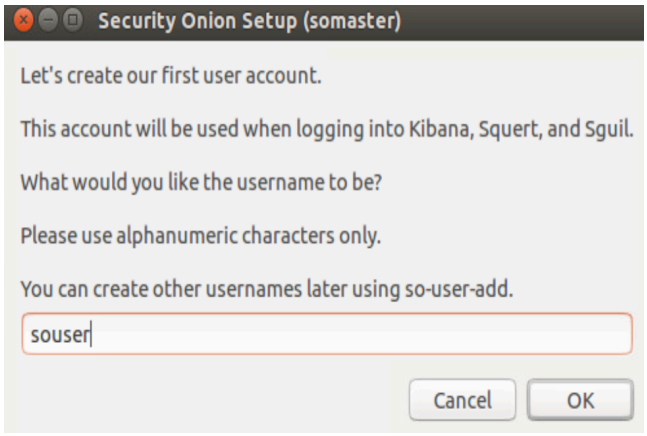


Once the box reboots, log back in and click on the Setup icon again. Skip Network configuration

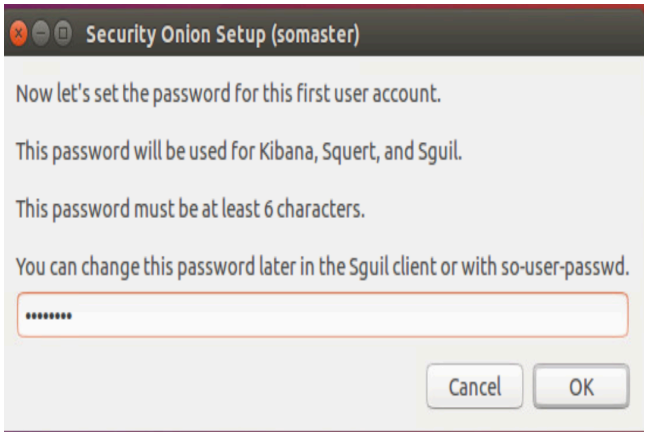
this time. It will then prompt to choose between Evaluation and Production mode. Choose Production mode



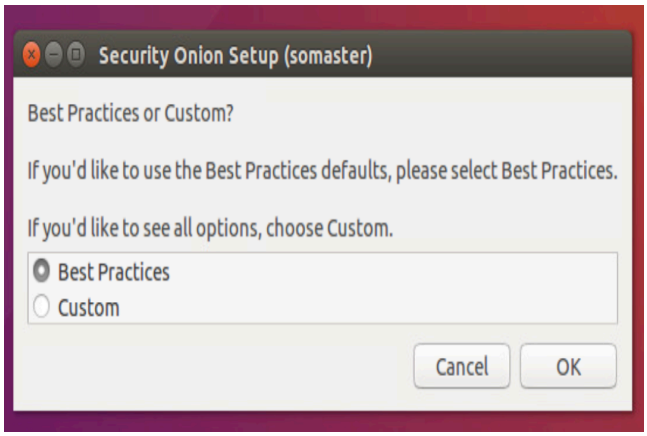
This is a Standalone deployment which serves as the Master, Sensor and Storage node so choose New



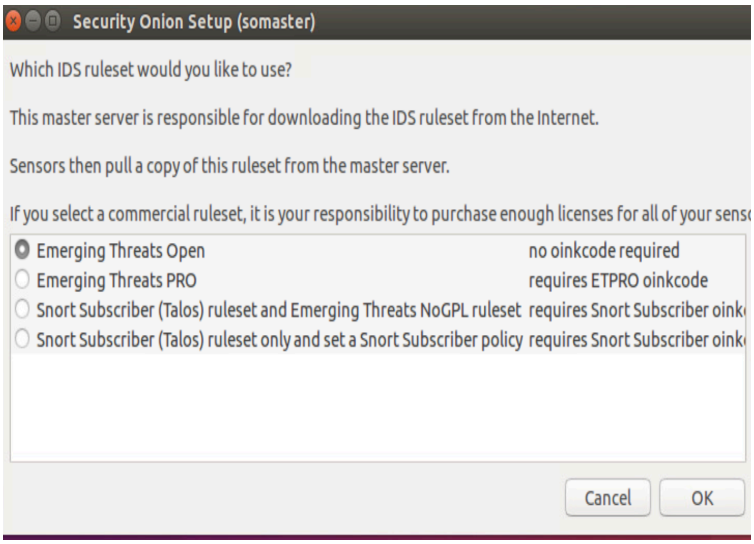
Enter a name for the Security Onion user



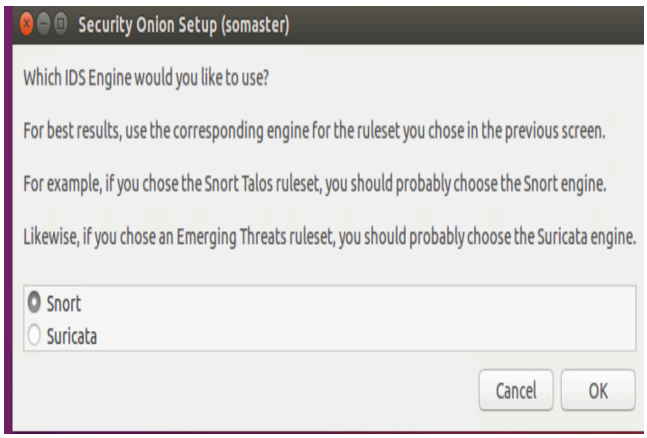
Set the users password



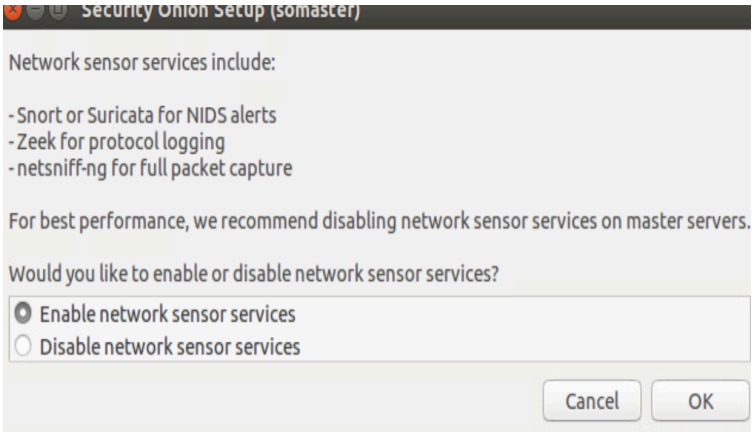
Choose Best Practices



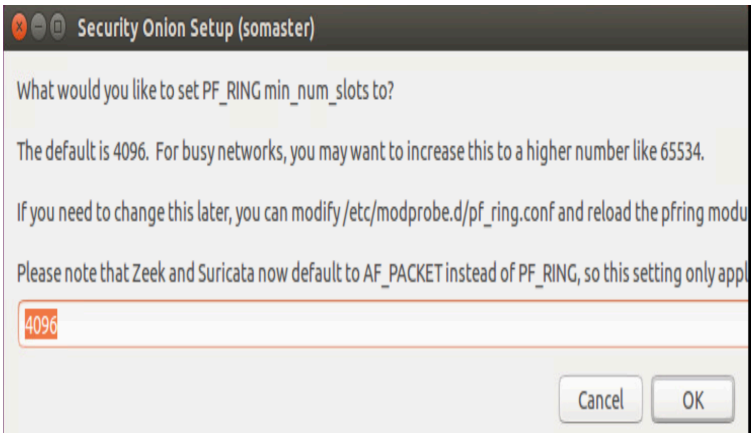
This deployment does not supply and licences that require purchases, leave the default selection and click OK



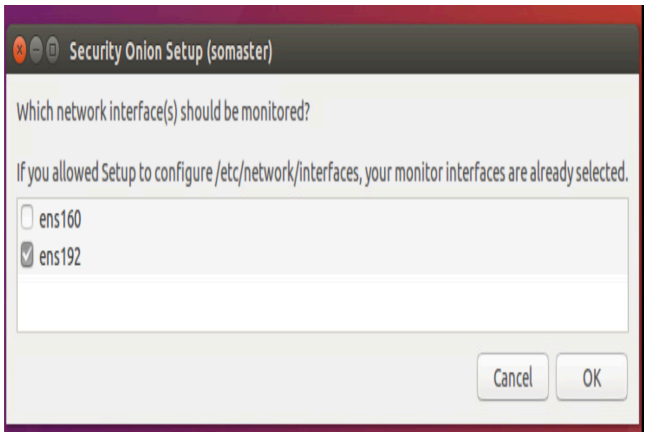
Choose either Snort or Suricata. This documentation covers Snort



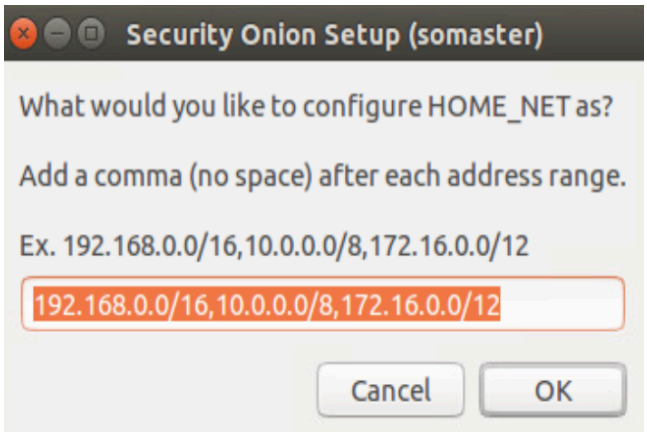
This is a Standalone deployment, so choose the option to Enable Network Services



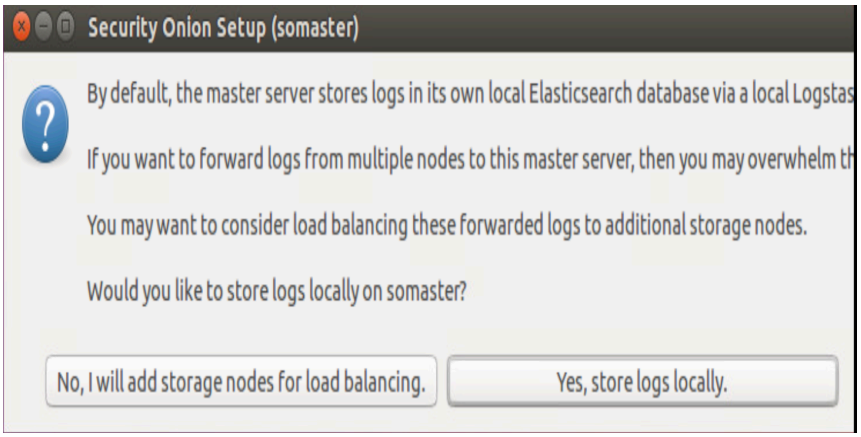
Choose the default



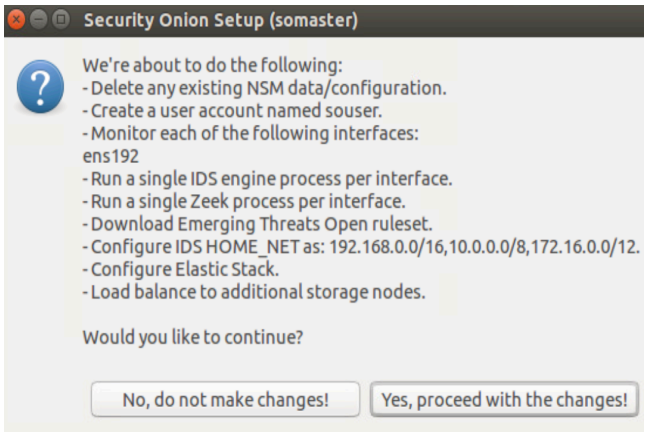
Sniffing interfaces were previsouly selected, so click OK with the defaults here



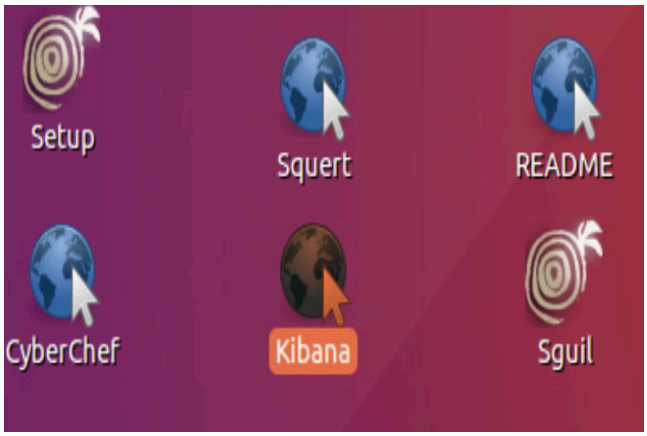
Click OK to defaults



Make sure to store logs locally as this is a Standalone Deployment



Yes! Proceed with changes



Once the installation is complete, these services will be available on the Desktop

TUI

Run this command from the shell that will open a TUI:

$ sosetup

Configuration File

Or copy the configuration file into the home directory, edit the file with the system settings, then run the setup. Steps as follows:

$ cp /usr/share/securityonion/sosetup.conf ~/

Edit the file and run:

$ sosetup -f ~/sosetup.conf

Check Installation Status

After the setup is complete, check on the status of the services using the command:

$ so-status

This will give you a quick view of all running services. For a more in-depth look, use:

$ sostat

Note – Kibana may take some time to start, if it is in a ‘Warn’ state, wait a few minutes and check again.

To restart all services:

$ so-restart

Users

It is important to note that the users that are created for Security Onion are completely separate then the users used by the Operating System. Think of them as different entities. You cannot log into Security Onion using OS level users and vice versa.

During the initial setup and configuration, the user will be prompted to create a user and password. Security Onion implements apache2 Single Sign On (SSO). After setup is complete, the user can be used to log into the Kibana dashboard as well as the Sguil analyst console. The user credentials are stored in the on-board MySQL database.

The initial user, as well as any users created following setup, are all considered ‘admin’ users. Out of the box there is no way to change the user’s permissions, that functionality requires a third-party license purchase. Because of this, it is important to note that some functionality may not be standard or expected. Should a user log into Kibana and modify the dashboard, the change is system wide. It is not tied to that user. Effectively all users are sharing one dashboard.

For auditing purposes, each user’s login and logout time is logged. Additionally, any failed login attempts are also logged. Creating users or changing user passwords does not get logged.

To create a new user, use the built-in command:

$ so-user-add

To update a user password use:

$ so-user-passwd

To see a list of users:

$ so-user-list

To disable a user:

$ so-user-disable

Tuning

• Default Kibana dashboards • Sguild dashboard • Using the so-pcap-import command to start piping in pcap data from network tap

Updating

In order to update the software packages and docker images on the Security Onion node, the repository must first be updated. Log into the repository, ensure it has internet access run:

$ sudo apt update -y

That will download the latest software packages. To download the latest docker images, there is a pre-packaged SO script to run:

$ ./so-elastic-airgap

Choose ‘Save’. The output will be a directory called securityonion-docker-airgap which will include a tar file of the images. Copy the entire directory to the Security Onion node:

$ scp -r securityonion-docker-airgap localuser@xx.xx.xx.xx:~/

That concludes the work that needs to be done on the repository. Next log into the Security Onion node and change directory into securityonion-docker-airgap:

$ cd securityonion-docker-airgap/

Run the script again but this time choose ‘Load’, this will update the docker images on the Security Onion node:

$ ./so-elastic-airgap

Finally, run the update command to update the OS software:

$ sudo apt update -y

Pre-Degaussing

Prior to Degaussing the equipment, the end user may want to offload some files for long term storage. The following instructions are meant to be suggestions only.

Retrieving all data from all databases on the node will be the most thorough method, however if the end user chooses the MySQL data retrieval can be broken into individual databases.

To grab all data from all databases on the node:

$ mysqldump --defaults-file=/etc/mysql/debian.cnf --all-databases > dump.sql

The end user may also want log files off of the node prior to destruction. Logs are stored in the /var/log/ directory.

The end user may want to save configuration files. Configuration files are store in the /etc/nsm/ directory.

Repair

During the installation, if any services fails to start you can simply re-run the setup and re-install to repair the system.