

# Security Onion

## COMMON TASKS

General Maintenance	
Task	Command
All Scripts	/usr/sbin/so*
Check Status of All Services	so-status
Start/Stop/Restart Individual Service	so-<service>-<verb>
Start/Stop/Restart Suricata	so-suricata-<verb>
Start/Stop/Restart Zeek	so-zeek-<verb>
Start/Stop/Restart Elasticsearch	so-elasticsearch-<verb>
Add SOC User (Manager)	so-user-add
List SOC users (Manager)	so-user-list
Disable SOC user (Manager)	so-user-disable EMAIL@DOMAIN
Update Rules (Manager)	so-rule-update
Check Redis Queue Length (Manager)	so-redis-count
Add Firewall Rules (Analyst, Beats, Syslog, etc.)	so-allow
Advanced Firewall Control	so-firewall
Security Onion Update	soup

Salt Commands (from Manager)	
Task	Command
Verify Nodes are Up	salt \* test.ping
Execute Command on all Nodes	salt \* cmd.run '<command>'
Sync all Nodes	salt \* state.highstate
Check service status on all nodes	salt \* so.status

Port/Protocols/Services (Distributed Deployment)	
Port/Protocol	Service/Purpose
22/tcp (node/Manager)	SSH access
4505-4506/tcp (Manager)	Salt communication from node(s) to Manager
443/tcp (Manager)	Security Onion Console (SOC) web interface

Support	
Blog	<a href="https://blog.securityonion.net">https://blog.securityonion.net</a>
Docs	<a href="https://docs.securityonion.net/en/2.4/">https://docs.securityonion.net/en/2.4/</a>
Community Support Forum	<a href="https://securityonion.net/discussions">https://securityonion.net/discussions</a>
Training, Professional Services, Hardware Appliances	<a href="https://securityonionsolutions.com">https://securityonionsolutions.com</a>

## IMPORTANT FILES

Configuration	
Component	Documentation
Most configuration is done via web interface. More information at <a href="https://docs.securityonion.net/en/2.4/administration.html">https://docs.securityonion.net/en/2.4/administration.html</a>	
Salt	<a href="https://docs.securityonion.net/en/2.4/salt.html">https://docs.securityonion.net/en/2.4/salt.html</a>
Suricata	<a href="https://docs.securityonion.net/en/2.4/suricata.html">https://docs.securityonion.net/en/2.4/suricata.html</a>
Zeek	<a href="https://docs.securityonion.net/en/2.4/zeek.html">https://docs.securityonion.net/en/2.4/zeek.html</a>
Elastic Agent	<a href="https://docs.securityonion.net/en/2.4/elastic-agent.html">https://docs.securityonion.net/en/2.4/elastic-agent.html</a>
Logstash	<a href="https://docs.securityonion.net/en/2.4/logstash.html">https://docs.securityonion.net/en/2.4/logstash.html</a>
Redis	<a href="https://docs.securityonion.net/en/2.4/redis.html">https://docs.securityonion.net/en/2.4/redis.html</a>
Elasticsearch	<a href="https://docs.securityonion.net/en/2.4/elasticsearch.html">https://docs.securityonion.net/en/2.4/elasticsearch.html</a>
Curator	<a href="https://docs.securityonion.net/en/2.4/curator.html">https://docs.securityonion.net/en/2.4/curator.html</a>
Not managed by web interface	
SSH	<a href="https://docs.securityonion.net/en/2.4/ssh.html">https://docs.securityonion.net/en/2.4/ssh.html</a>

Diagnostic Logs	
Description	File/Directory
Suricata	/opt/so/log/suricata/suricata.log
Stenographer	/opt/so/log/stenographer/stenographer.log
Zeek Logs Directory	/nsm/zeek/logs/current/
Zeek Diag Logs	stderr.log, reporter.log, loaded_scripts.log
Strelka	/opt/so/log/strelka/
Logstash	/opt/so/log/logstash/logstash.log
Elasticsearch	/opt/so/log/elasticsearch/<hostname>.log
Elastalert	/opt/so/log/elastalert/elastalert.log
Kibana	/opt/so/log/kibana/kibana.log
InfluxDB	/opt/so/log/influxdb/
Other log files	/opt/so/log/

Performance Tuning	
Target	Parameter/File
Suricata Info	<a href="https://docs.securityonion.net/en/2.4/suricata.html">https://docs.securityonion.net/en/2.4/suricata.html</a>
Zeek Info	<a href="https://docs.securityonion.net/en/2.4/zeek.html">https://docs.securityonion.net/en/2.4/zeek.html</a>

Packet Filtering with BPF	
Scope	File
BPF Information	<a href="https://docs.securityonion.net/en/2.4/bpf.html">https://docs.securityonion.net/en/2.4/bpf.html</a>

Rule and Alert Management	
Configuration	File
Managing Rules	<a href="https://docs.securityonion.net/en/2.4/rules.html">https://docs.securityonion.net/en/2.4/rules.html</a>
Local Rules	<a href="https://docs.securityonion.net/en/2.4/local-rules.html">https://docs.securityonion.net/en/2.4/local-rules.html</a>
Managing Alerts	<a href="https://docs.securityonion.net/en/2.4/managing-alerts.html">https://docs.securityonion.net/en/2.4/managing-alerts.html</a>
Elastalert	<a href="https://docs.securityonion.net/en/2.4/elastalert.html">https://docs.securityonion.net/en/2.4/elastalert.html</a>

## DATA

Data Directories	
Data	Directory
Packet Capture (Sensor)	/nsm/pcap/
Suricata Data (Sensor)	/nsm/suricata/
Zeek (Archived) (Sensor)	/nsm/zeek/logs/<yyyy-mm-dd>/
Zeek (Current Hour) (Sensor)	/nsm/zeek/logs/current/
Zeek Extracted Files (Sensor)	/nsm/zeek/extracted/complete/
Elasticsearch (Manager/Heavy/Search)	/nsm/elasticsearch/nodes/<x>/indices/
Docker Registry	/nsm/docker-registry/
Strelka analyzed files	/nsm/strelka/processed/
InfluxDB	/nsm/influxdb/
so-import-pcap	/nsm/import/
so-import-evtx	/nsm/import/

Originally Designed by: Chris Sanders  
<http://www.chrissanders.org> - @chrissanders88

Updated by: Security Onion Solutions  
<https://securityonionsolutions.com> - @securityonion

Security Onion Version: 2.4  
 Last Modified: 06.15.2023

Security Onion

