



## 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
Update Security Onion components (*not* OS)	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 from node(s) to Manager
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://securityonion.net/docs">https://securityonion.net/docs</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 Files	
Configuration	Location
Most configuration is done via salt in either the global pillar or the minion pillar. More information at <a href="https://securityonion.net/docs/salt">https://securityonion.net/docs/salt</a>	
Salt	<a href="https://securityonion.net/docs/salt">https://securityonion.net/docs/salt</a>
Global Pillar	/opt/so/saltstack/local/pillar/global.sls
Minion Pillar	/opt/so/saltstack/local/pillar/minions/MINIONID.sls
Suricata Config	global or minion pillars
Suricata Docs	<a href="https://securityonion.net/docs/suricata">https://securityonion.net/docs/suricata</a>
Zeek Config	global or minion pillars
Zeek Docs	<a href="https://securityonion.net/docs/zeek">https://securityonion.net/docs/zeek</a>
Filebeat Docs	<a href="https://securityonion.net/docs/filebeat">https://securityonion.net/docs/filebeat</a>
Logstash Config	/opt/so/saltstack/local/pillar/minions/MINIONID.sls
Logstash Docs	<a href="https://securityonion.net/docs/logstash">https://securityonion.net/docs/logstash</a>
Redis maxmemory	/opt/so/saltstack/local/pillar/global.sls
Redis Docs	<a href="https://securityonion.net/docs/redis">https://securityonion.net/docs/redis</a>
Elasticsearch Config	global and minion pillars
Elasticsearch Docs	<a href="https://securityonion.net/docs/elasticsearch">https://securityonion.net/docs/elasticsearch</a>
Curator Config	/opt/so/saltstack/local/pillar/global.sls
Curator Docs	<a href="https://securityonion.net/docs/curator">https://securityonion.net/docs/curator</a>
Not managed by Salt	
Wazuh	/opt/so/conf/wazuh/ossec.conf
Wazuh Information	<a href="https://securityonion.net/docs/wazuh">https://securityonion.net/docs/wazuh</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
Filebeat	/opt/so/log/filebeat/filebeat.log
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
Wazuh	/nsm/wazuh/logs/ossec.log
Other log files	/opt/so/log/

Performance Tuning	
Target	Parameter/File
File	/opt/so/saltstack/local/pillar/minions/MINIONID.sls
Suricata Workers	suriprocs
Suricata Info	<a href="https://securityonion.net/docs/suricata">https://securityonion.net/docs/suricata</a>
Zeek Workers	zeek_lbprocs
Zeek Info	<a href="https://securityonion.net/docs/zeek">https://securityonion.net/docs/zeek</a>

Packet Filtering with BPF	
Scope	File
BPF Information	<a href="https://securityonion.net/docs/bpf">https://securityonion.net/docs/bpf</a>
Global BPF	/opt/so/saltstack/local/pillar/global.sls
Minion BPF	/opt/so/saltstack/local/pillar/minions/MINIONID.sls

Rule and Alert Management	
Configuration	File
NIDS Alert Docs	<a href="https://securityonion.net/docs/managing-alerts">https://securityonion.net/docs/managing-alerts</a>
NIDS Rule Thresholds	global or minion pillar
Disabled Rules (Manager)	/opt/so/saltstack/local/pillar/minions/MINIONID.sls
Wazuh Rules (Default)	/opt/so/rules/hids/ruleset/
Wazuh Rules (Custom)	/opt/so/rules/hids/local_rules.xml
Elastalert	/opt/so/rules/elastalert/
Zeek Intel	/opt/so/saltstack/local/salt/zeek/policy/intel/intel.dat

## 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/
Wazuh HIDS Alerts and Logs	/nsm/wazuh/logs/
Elasticsearch (Manager/Heavy/Search)	/nsm/elasticsearch/nodes/<x>/indices/
Docker Registry	/nsm/docker-registry/
Strelka analyzed files	/nsm/strelka/processed/
Grafana	/nsm/grafana/
so-import-pcap	/nsm/import/
osquery	/nsm/osquery/

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

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

Security Onion Version: 2.3  
 Last Modified: 08.08.2022

