



Version 3.0

Operations Guide
January 2018



Doc Version 1.1

Table of contents

1	Overview	3
2	Cluster Health and Monitoring	4
3	Configuration files	5
4	SearchGuard	6
5	Logstash Templates	8
6	Installing Agents	9
6.1	NXLOG SIEM Agents for Microsoft Hosts	9
6.2	Filebeat SIEM agents for Linux or Apache	11
6.3	OSSEC HIDS Agents for Windows Hosts	14
6.4	For Linux agents:	15
6.5	SYSLOG	17
7	Inputs	18
7.1	Logstash	18
7.2	Troubleshooting SYSLOGS	22
7.3	Catch all syslog filter	23
7.4	Troubleshooting Cisco ASA syslogs	24
8	Alerting	26
8.1	411	26
8.2	Adding a search	26
8.3	Setting notifications	29
8.4	Advanced	30
8.5	Users and groups	31
8.6	Index Overview	33
8.7	Add Index	33
8.8	How to setup Alerts examples in 411	35
8.9	Windows user account password set to non-expiring alert	35
8.10	Guest account login alert	36
8.11	Windows User account added to security group alert	37
8.12	Windows user account added to universal security group alert	38
8.13	Login attempt to Disabled windows user account alert	39
8.14	Slack	40
8.15	Logstash	43
9	OSINT	44
9.1	Minemeld	44
9.2	Minemeld interface	44
9.3	Dashboard	45
9.4	Nodes	45
9.5	Adding a whitelist/nodal indicator	48
9.6	Adding a generic indicator	49
9.7	Adding a node	50
9.8	Supported nodes	53
9.9	Miners	53

10 Active Threat Detection Pfsense/Apache	55
10.1 Minemeld.....	55
10.2 Logstash.....	56
10.3 Elastic search/kIbana	58
10.4 Sysmon/Windows EXE Detection.....	58
11 HIDS	60
11.1 Rulesets	60
11.2 Management	60
12 Incident Response	61
12.1 Administration.....	61
12.2 Usage.....	62
13 The How TO OF SIEMonster Dashboards	64
13.1 Introduction	64
13.2 Overview	64
13.3 Discovery	65
13.4 Visualizations	70
13.5 Dashboards.....	88
14 Dradis integration	90
15 OpenAudit – Asset Discovery	91
16 Frequently Asked Questions	93
16.1 Configuration / Installation	93
16.2 Backup/Scaling.....	93
16.3 Backup.....	93
16.4 Rancher Server MySQL backup/migration	93
16.5 Physical disk expansion	95
17 Troubleshooting	102
18 Changing Passwords	103

1 OVERVIEW

This document is the SIEMonster Operational and Usage guide. This document should be followed post the building of the SIEMonster in the document SIEMonster V3.0 Build Guide. This covers all SIEMonster builds including VMware, VirtualBox, Amazon and Bare metal.

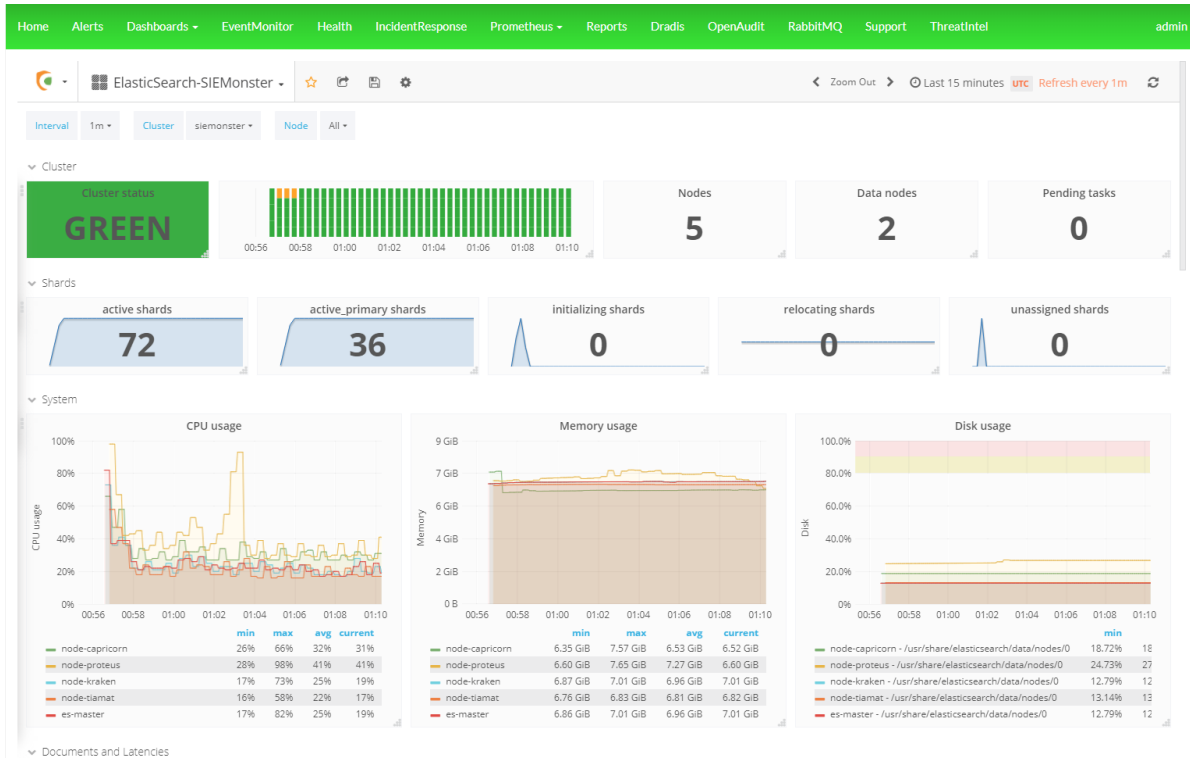
This guide covers all the details on configuration, agents install, dashboard configurations and health and monitoring. It is designed to be a one stop shop of all the configuration details to get you on your way with SIEMonster.

There are also sections on how to setup your own Dashboards and adding Vulnerability assessment reports to your SIEM as well as asset discovery.

If there are any details missing from this guide, please info info@siemonster.com or follow the online SIEMonster community on the SIEMonster website.

2 CLUSTER HEALTH AND MONITORING

To monitor your cluster and stack health and detailed statistics we have included a health monitor. This can be accessed from the 'Health' Menu item:



Cluster Health checking

On the command line at the Proteus appliance cluster health may be found using the command:

- `curl -k https://elastic:elastic-password@localhost:9200/_cluster/health?pretty`

Where 'elastic-password' is the password allocated during deployment.

```
rancher@proteus ~ $ curl -k https://elastic:s13M0nSterV3@localhost:9200/_cluster/health?pretty
{
  "cluster_name" : "siemonster",
  "status" : "green",
  "timed out" : false,
  "number_of_nodes" : 5,
  "number_of_data_nodes" : 2,
  "active_primary_shards" : 26,
  "active_shards" : 52,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

Curl output

3 CONFIGURATION FILES

SIEMONSTER V3 now incorporates an NFS shared file system across the cluster to allow the centralization of key configuration files in a single folder. This folder can be found on the Makara instance in the root folder /nfs

The layout of this folder is typically as follows with Rancher adding random suffixes to maintain unique entries. This allows for easy backups up your configuration.

```
makara rancher # ls -l /nfs
total 88
drwxr-xr-x. 2 root  root  4096 Jan 13 03:45 siemonster-project-vagrant_alertmanager_5fb4d
drwxr-xr-x. 2 root  root  4096 Jan 13 03:51 siemonster-project-vagrant_elastalert_rules_c1317
drwxr-xr-x. 4  102  102 4096 Jan 13 03:46 siemonster-project-vagrant_es-config_051c9
drwxr-xr-x. 3  104  107 4096 Jan 13 03:54 siemonster-project-vagrant_grafana_data_d7e0b
drwxrwxr-x. 2 root  root  4096 Jan 13 03:53 siemonster-project-vagrant_logstash-collector_676cc
drwxrwxr-x. 2 root  root  4096 Jan 13 03:57 siemonster-project-vagrant_logstash-indexer_488e1
drwxr-xr-x. 3 nobody nobody 4096 Jan 13 03:46 siemonster-project-vagrant_prometheus_data_25648
drwxr-xr-x. 2 nobody nobody 4096 Jan 13 03:46 siemonster-project-vagrant_prometheus_rules_ec91d
drwxrwxrwx. 2  122  129 4096 Jan 13 03:54 siemonster-project-vagrant_reports_config_5e967
drwxr-xr-x. 2 root  root  4096 Jan 13 03:54 siemonster-project-vagrant_reports_e36c2
drwxr-xr-x. 4 root  root  4096 Jan 13 03:51 siemonster-project-vagrant_syslog-ng_0035f
```

NFS directory listing

4 SEARCHGUARD

Elasticsearch cluster protection & Role based access control is now provided by SearchGuard, an open source alternative to Elastic X-pack security.

All endpoints providing feed or query mechanisms are run over TLS 1.2 connections with required authentication that was configured at install time. However, for subsequent users other than the first user this will need to be added in SearchGuard manually.

Access to Kibana from the dashboard uses the trusted proxy option, where the web application username must be registered with SearchGuard. During installation, the administrator email was automatically added, providing Kibana access.

Creating new users, adding or changing roles and role mapping can be simply defined as a 2-part process. On the shared file system on the Makara server under the /nfs folder the SearchGuard configuration files may be edited.

```
drwxr-xr-x. 2 root root 4096 Jan 14 00:55 siemonster-project-vagrant_alertmanager_c760b
drwxr-xr-x. 2 root root 4096 Jan 14 00:54 siemonster-project-vagrant_elastalert_rules_202ed
drwxr-xr-x. 4 102 102 4096 Jan 14 00:54 siemonster-project-vagrant_es-config_d5980
drwxr-xr-x. 2 33 33 4096 Jan 14 00:56 siemonster-project-vagrant_rouroneone-data_0bd87
drwxr-xr-x. 4 104 107 4096 Jan 14 01:15 siemonster-project-vagrant_grafana_data_feefl
drwxrwxr-x. 2 root root 4096 Jan 14 23:23 siemonster-project-vagrant_logstash-collector_52956
drwxrwxr-x. 2 root root 4096 Jan 14 22:18 siemonster-project-vagrant_logstash-indexer_6d728
drwxr-xr-x. 361 nobody nobody 20480 Jan 14 23:43 siemonster-project-vagrant_prometheus_data_e34ae
drwxr-xr-x. 2 nobody nobody 4096 Jan 14 00:55 siemonster-project-vagrant_prometheus_rules_3f47b
drwxr-xr-x. 3 root root 4096 Jan 14 01:31 siemonster-project-vagrant_reports_b0341
```

These files are located at /nfs/project_name_es-config_xxx/config/searchguard

```
makara siemonster-project-vagrant_es-config_d5980 # ls -l searchguard/
total 48
-rw-r--r--. 1 102 102 1764 Jan 14 00:54 sg_action_groups.yml
-rw-r--r--. 1 102 102 779 Jan 14 04:41 sg_config.yml
-rw-r--r--. 1 102 102 597 Jan 14 05:17 sg_internal_users.yml
-rw-r--r--. 1 102 102 2645 Jan 14 23:33 sg_roles.yml
-rw-r--r--. 1 102 102 860 Jan 14 00:56 sg_roles_mapping.yml
drwxr-xr-x. 6 102 102 4096 Jan 14 00:55 ssl
```

The next stage is to commit these changes to the Elasticsearch es-master container.

Creating a new user:

1. The user will have first been created in the web application
2. Edit the sg_internal_users.yml file as shown above

```
admin:
  hash: '$2a$12$kLcTxxta/kyyEf.sgxWR5u1tnP9hkweEDbW8imV.qr/xv2rarzREG' #admin
  username: jim@siemonster.com
  roles:
    - admin

newuser:
  hash: '$2a$12$kLcTxxta/kyyEf.sgxWR5u1tnP9hkweEDbW8imV.qr/xv2rarzREG' #admin
  username: user01@example.com
  roles:
    - admin
```

In this example, a new user has been created who is registered in the web application with the email address user01@example.com. (hash is not used) The system uses authentication headers & session tokens from the web application, so this user must have first logged on to the system to access Kibana.

For none web users, i.e. agent type Elasticsearch feeds, a new password hash can be created using the hash tool on the es-master container.

Execute a shell to this container and run the following command if the password is MyS3cRetP@ss
 plugins/search-guard-5/tools/hash.sh -p MyS3cRetP@ss


```
root@siemonster-project-vagrant-es-master-1:/usr/share/elasticsearch# plugins/search-guard-5/tools/hash.sh -p MyS3cRetP@ss
$2a$12$mWuL78w1HSERRIckwvUmebyPS127iErqtgE2M1hHhPRHE1cjiPz6
```

The hash required will be returned.

3. Changes must be committed to Elasticsearch by executing a shell to the es-master container from the Rancher UI, and running the command `/run/auth/sgadmin.sh`

➤ Shell: siemonster-project-vagrant-es-master-1

```
root@siemonster-project-vagrant-es-master-1:/usr/share/elasticsearch# /run/auth/sgadmin.sh
Search Guard Admin v5
Will connect to siemonster-project-vagrant-es-master-1:9300 ... done

### LICENSE NOTICE Search Guard ###

If you use one or more of the following features in production
make sure you have a valid Search Guard license
(See https://floragunn.com/searchguard-validate-license)

* Kibana Multitenancy
* LDAP authentication/authorization
* Active Directory authentication/authorization
* REST Management API
* JSON Web Token (JWT) authentication/authorization
* Kerberos authentication/authorization
* Document- and Fieldlevel Security (DLS/FLS)
* Auditlogging

In case of any doubt mail to <sales@floragunn.com>
#####
Contacting elasticsearch cluster 'elasticsearch' and wait for YELLOW clusterstate ...
Clustername: siemonster
Clusterstate: GREEN
Number of nodes: 5
Number of data nodes: 2
searchguard index already exists, so we do not need to create one.
Populate config from /usr/share/elasticsearch/config/searchguard/
Will update 'config' with /usr/share/elasticsearch/config/searchguard/sg_config.yml
  SUCC: Configuration for 'config' created or updated
Will update 'roles' with /usr/share/elasticsearch/config/searchguard/sg_roles.yml
  SUCC: Configuration for 'roles' created or updated
Will update 'rolesmapping' with /usr/share/elasticsearch/config/searchguard/sg_roles_mapping.yml
  SUCC: Configuration for 'rolesmapping' created or updated
Will update 'internalusers' with /usr/share/elasticsearch/config/searchguard/sg_internal_users.yml
  SUCC: Configuration for 'internalusers' created or updated
Will update 'actiongroups' with /usr/share/elasticsearch/config/searchguard/sg_action_groups.yml
  SUCC: Configuration for 'actiongroups' created or updated
Done with success
root@siemonster-project-vagrant-es-master-1:/usr/share/elasticsearch# █
```

If there are any syntax issues they will be shown in the above output including the relevant file. These changes are immediately live and no container restarts are required.

Further information regarding defining roles and permissions can be found at <http://docs.search-guard.com/latest/roles-permissions>

5 LOGSTASH TEMPLATES

There are 2 instances of Logstash in use, Logstash-Collector is for data ingestion & Logstash-Indexer is for the parsing of event data. Data ingested to the Logstash_collector is output in JSON format to the RabbitMQ Message Broker. The Logstash-Indexer uses RabbitMQ as an input, parses and correlates data before forwarding to Elasticsearch.

To better analyse and visualise incoming logs into Logstash from Windows, Linux, Syslogs and alike, we have developed a better architecture that will allow for quicker device parsers to be written. The premise being, to re-organising the way Logstash processes the config files for better flow and understanding and fast new device take-up. For example, a new Cisco ASA firewall hits the market, currently no configuration file has a parser for it. A listening catch-all will ensure it is picked up in a generic syslog listener. Once identified the fields will then be moved across into the ASA config file.

Logstash-Indexer configuration files can be found within the NFS mounted shared folder on Makara /nfs, the format of the subfolder is siemonster-project-yourproject-container_name_xxxxx

```
makara nfs # ls -l siemonster-project-vagrant_logstash-indexer_488e1
total 84
-rw-rw-r--. 1 root root  310 Dec 10 00:01 000-inputs.conf
-rw-rw-r--. 1 root root  460 Dec 30 06:39 01-wazuh-filter.conf
-rw-rw-r--. 1 root root 8369 Dec  9 23:58 10-windows-events-filter.conf
-rw-rw-r--. 1 root root 1249 Dec  9 23:58 20-ufw-filter.conf
-rw-rw-r--. 1 root root  584 Dec  9 23:58 25-squid-filter.conf
-rw-rw-r--. 1 root root 3714 Dec  9 23:58 30-apache-filter.conf
-rw-rw-r--. 1 root root 6000 Dec  9 23:58 40-tpot-filter.conf
-rw-rw-r--. 1 root root 2894 Dec 10 00:04 90-osint-filter.conf
-rw-rw-r--. 1 root root 3824 Dec 14 00:00 999-outputs.conf
```

The layout of the files in the logstash-indexer subfolder is

000-inputs - Receives the logs and tags them

999-outputs - Send the logs to Elasticsearch based on their tags.

The filter files per device now fall in between 000-Input and 999-output, between process the files based on their tags, i.e. 10-Windows, 30-Apache. So, rather than have config files with inputs, filters and outputs we have separation of function. Within the SIEMonster stack, if the log creation times are local time then they should be correctly displayed in Kibana.

If syslog time zones need to alter. E.g. Endpoint time zone differences, then the specific time zone can be added in the Logstash configuration file.

Edit 10-windows-events-filter.conf file and replace the time zone fields with your own time zone.

<http://joda-time.sourceforge.net/timezones.html>

vi /nfs/xxx-logstash-indexer_xxxxx/10-windows-events-filter.conf

```
}
date {
  match => ["EventTime", "YYYY-MM-dd HH:mm:ss"]
  remove_field => [ "EventTime" ]
  timezone => "Australia/Melbourne"
}
```

Time zone mods

Restart logstash-indexer container:

Active	logstash-indexer ⓘ	Image: ikurturso/logstash-indexer:1.0	Service	1 Container	⌵ ⓘ
				1 Co	Upgrade ⓘ
					Restart ⓘ

6 INSTALLING AGENTS

Now that the **SIEMonster** is up and running. It's time to install some agents to get some data into the SIEM. You will need to install an agent on the boxes that support agents like Windows and Linux. For boxes that don't support agents you will need to forward syslogs to the SIEM.

The basic premise for endpoint installation is the following.

- Generate a certificate on Proteus using the script provided
- Copy the certificate off Proteus
- Download the zip file and unzip
- Install the agent on the endpoint, with the Certificate and Configuration file
- Change the configuration file on the endpoint to point to connect back to Proteus on **SIEMonster**.

6.1 NXLOG SIEM AGENTS FOR MICROSOFT HOSTS

NXLOG is a universal log collector and forwarder. The software NXLOG can be found directly from the vendor or the link shown below.

- agents.siemonster.com/agent-pack.zip

SHA256

3f7b81e3fddd50ba900722aaf813f7eeb0514012b52d465a7550ce5ad46a6f4a

The zip file contains two of the three files you will need for your endpoint. The two files are nxlog.conf & nxlog*.msi You will need to change the IP address and port number to the Proteus IP address. You can do this in notepad on the conf file. A command has been provided below so you can generate the required SSL certificate (the 3rd needed file)

Create SSL certificate

Certificate for endpoint: SSL certificates for transport must be created to ensure encryption between the client and the SIEM to protect your data travelling to the SIEM.

To generate the certificate, the following commands can be used within the Logstash container:

Option 1: FQDN – DNS

```
openssl req -x509 -batch -nodes -days 3650 -newkey rsa:2048 -keyout /etc/pki/tls/private/logstash-forwarder.key -out /etc/pki/tls/certs/logstash-forwarder.crt -subj '/CN=Proteus_server_fqdn'
```

Option 2: IP Address

Within the Logstash-Collector container, edit the OpenSSL configuration file:

If you don't have nano you will need to install it

```
apt-get update && apt-get install nano
```

```
nano etc/ssl/openssl.cnf
```

Find the [v3_ca] section in the file and add the following below it:

```
subjectAltName = IP: Proteus_IP_Address
```

Save & exit.

Generate the certificates:

```
openssl req -config /etc/ssl/openssl.cnf -x509 -days 3650 -batch -nodes -newkey rsa:2048 -keyout /etc/logstash/logstash-forwarder.key -out /etc/logstash/logstash-forwarder.crt
```

Using either option will produce a certificate in the following folder: /etc/logstash/logstash-forwarder.crt.

Both Options must do the following.:

Open an SSH terminal session to the Proteus server, and copy the certificate from the Logstash container to the localhost as follows:

Use the 'docker ps' command to locate the Logstash-Collector container:

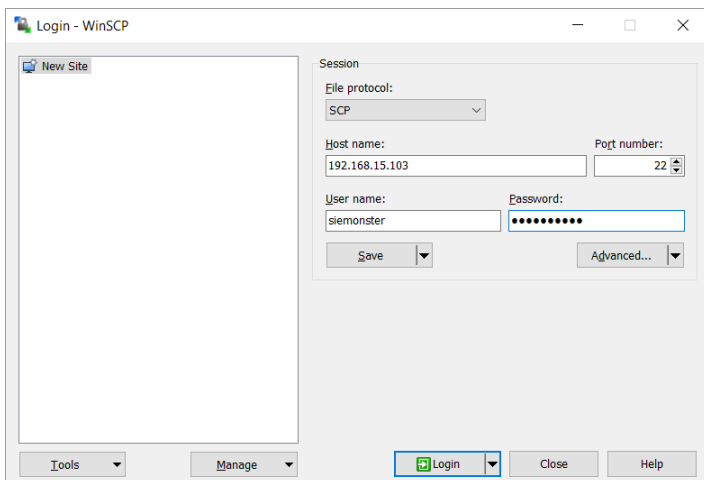
```
CONTAINER ID          IMAGE
8233ea9707e8        ikuturso/logstash-collector:1.1
ash-collector-1-5fda34cc
48807ee0916c        bonniernews/logstash_exporter
ash-indexer-exporter-1-415b49ca
```

Use 'docker cp <Container ID>' to grab the certificate:

```
docker cp 8233ea9707e8:/etc/logstash/logstash-forwarder.crt .
```

(note the single dot at the end of the command)

Copy this file off for your endpoint.



The corresponding private key is located at /etc/pki/tls/private/logstash-forwarder.key

Installation on Endpoint with the 3 components

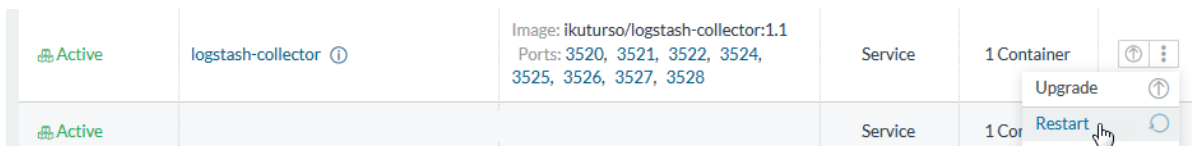
- Install the NXLOG msi on your Microsoft endpoint with Admin credentials.
- Copy over the modified nxlog.conf file to "C:\Program Files (x86)\nxlog\conf" on your endpoint. Ensure the name of the copied file is nxlog.conf not nxlog.conf.conf. May require view file extensions in Windows.
- Copy the certificate (use WinSCP or SCP) to "C:\Program Files (x86)\nxlog\cert" on your endpoint.
- Start the NXlog service

Makara SIEM steps

On Makara, for SSL transport of logs, edit the `/nfs/logstash-collector.xxx/00-inputs.conf` if you need to specify a different port.

```
tcp {
  port => 3521
  ssl_enable => true
  ssl_cert => "/etc/pki/tls/certs/logstash-forwarder.crt"
  ssl_key => "/etc/pki/tls/private/logstash-forwarder.key"
  ssl_verify => false
  codec => json_lines { charset => CP1252 }
  tags => ["eventlog"]
}
```

Restart Logstash-Collector on the Proteus appliance if any changes are made:



Check that the NXLOG agent has connected:

- Install net-tools if netstat not available: `apt-get update && apt-get install net-tools`
- `netstat -ant | grep 3522` (or other configured port)

The connection may take up to 2-3 minutes to be established. See the troubleshooting section should no connection be established. Once established, repeat the installation on other hosts.

6.2 FILEBEAT SIEM AGENTS FOR LINUX OR APACHE

Filebeat is a lightweight, open source shipper for log file data. As the next-generation Logstash Forwarder, Filebeat tails logs and quickly sends this information to Logstash for further parsing or to Elasticsearch for centralized storage and analysis. **SIEMonster** uses this agent for collecting logs from Unix hosts, typically Apache web logs. The latest Filebeat agent Debian 64 package may be downloaded from:

agents.siemonster.com/filebeat-5.5.2-amd64.deb

SHA256 Checksum:

`cd05f6cee84e855deeb74f86579b43f563dec12d5909927eb94d49cb939f5ae3`

Transfer this file via SCP to the target server and install using the following command:

- `sudo dpkg -i filebeat-5.5.2-amd64.deb`

Once installed the filebeat service will be inactive and the configuration file can be found at `/etc/filebeat/filebeat.yml`. This configuration file must be modified to suit the logs being monitored and the IP address of the Proteus server.

Create a certificate as shown in the previous section and retrieve the SSL certificate from the Proteus appliance `~/logstash-forwarder.crt` and copy via SCP and transfer to the target server. On the target

server, copy the certificate to /etc/pki/tls/certs/logstash-forwarder.crt. If this location does not exist, create using the command:

- `sudo mkdir -p /etc/pki/tls/certs`

Secure the certificate as follows:

- `sudo chown root:root /etc/pki/tls/certs/logstash-forwarder.crt`
- `sudo chmod 644 /etc/pki/tls/certs/logstash-forwarder.crt`

Edit the Filebeat configuration file /etc/filebeat/filebeat.yml as follows: The first element to change will be the 'paths' directive in the prospectors' section see Figure Below.

For example, to modify this for Apache logs this path may be altered to:

`/var/log/apache2/access.log`. Change the port assignment to 3520 for Apache logs.

```
##### Filebeat #####
filebeat:
  # List of prospectors to fetch data.
  prospectors:
    # Each - is a prospector. Below are the prospector specific configurations
    -
      # Paths that should be crawled and fetched. Glob based paths.
      # To fetch all ".log" files from a specific level of subdirectories
      # /var/log/*/*.log can be used.
      # For each file found under this path, a harvester is started.
      # Make sure not file is defined twice as this can lead to unexpected behaviour.
      paths:
        - /var/log/apache2/access.log
        #- c:\programdata\elasticsearch\logs\*
```

Filebeat path modification on remote Apache server.

- Next locate the Logstash output section and enter the IP address of the Proteus server.

```
### Logstash as output
logstash:
  # The Logstash hosts
  hosts: ["192.168.0.103:3520"]

  # Number of workers per Logstash host.
  #worker: 1
```

Proteus IP inserted

- For SSL transport is enabled by default

SSL Transport follow picture for correct path

On Makara, edit the file /nfs/xxx-logstash-collector_XXXXX/00-inputs.conf

```
input {
  beats {
    port => 3520
    ssl => true
    ssl_certificate => "/etc/logstash/logstash-forwarder.crt"
    ssl_key => "/etc/logstash/logstash-forwarder.key"
    codec => json_lines
    tags => ["apache"]
  }
}
```

Logstash beats configuration for Apache

Restart Logstash-Collector using the GUI command:

Active	logstash-collector ⓘ	Image: ikuturso/logstash-collector:1.1 Ports: 3520, 3521, 3522, 3524, 3525, 3526, 3527, 3528	Service	1 Container	⊕ ⓘ
Active			Service	1 Cor	Restart ↻

From the remote Apache Server test the SSL connection as follows:

- `sudo service filebeat stop`
- `curl -v --cacert /etc/pki/tls/certs/logstash-forwarder.crt https://192.168.0.103:3520` (Replace IP with yours)

A successful response should contain 'curl: (52) Empty reply from server'

An unsuccessful response will contain 'curl: (51) SSL: certificate verification failed (result: 5)'

See the troubleshooting section for diagnosing SSL problems.

Restart Filebeat with the command:

- `sudo service filebeat restart`

Test for connection status on the Proteus appliance:

- `netstat -ant |grep 3521` (or other configured port)

```
root@proteus:~/scripts# netstat -ant |grep 3520
tcp6      0      0 ::: 3520          :::*              LISTEN
tcp6      0      0 192.168.0.103:3520 192.168.0.104:54708 ESTABLISHED
```

Working connection

6.3 OSSEC HIDS AGENTS FOR WINDOWS HOSTS

OSSEC-Wazuh HIDS agents may be installed as follows to report to the OSSEC/Wazuh manager on the Proteus appliance. This is great edition to the SIEM. For detailed information on OSSEC-Wazuh have a look at the Wazuh reference manual <https://documentation.wazuh.com/2.1/>

OSSEC agents for Linux servers are installed via the OSSEC binary:
<https://documentation.wazuh.com/2.1/installation-guide/installing-wazuh-agent/index.html>
 (Server/Agent Unix)

Automated install:
 For Windows agents, an auto-deploy package is available:


http://agents.siemonster.com/wazuh_agent_deploy.zip

SHA256

a00266253eb471ee0bbcebb6d52280747bad93a1aa4c12a28904f94c728de58c

Extract the 3 files in the zip, edit the deploy.bat file and modify the -api_ip to the Proteus IP address & the -password to the configured Wazuh API password.

Run the 'deploy.bat' file as an administrator to install and register the agent. In the Wazuh dashboard within Kibana the newly registered agent should appear in the Agents section:



ID	Name	IP	Status
000	wazuh-manager	127.0.0.1	Active
001	SERVER9	172.20.8.1	Active

Note. The Wazuh agent may be flagged as a false positive by some AV products - <https://github.com/wazuh/wazuh/issues/210> in which case an alternate MSI installer is available <http://agents.siemonster.com/wazuh-agent-2.1.1-1.msi>

SHA256Checksum:
 4e933484131b58d04bedeebafd93bc2d5fbf33faaf18956ab629a13bfaf4187a

6.4 FOR LINUX AGENTS:

After installing the agent package run the following command from a terminal session:

```
/var/ossec/bin/agent-auth -m Proteus IP address
```

This will automatically register the agent, which will then be visible in the dashboard as above.

Manual installation:

On the Proteus appliance, execute shell access on the Wazuh container and run the following command:

- `/var/ossec/bin/manage_agents`

Note: Using a puTTY session from Windows to Proteus will allow easy copy and paste for generated keys than using vmware tools and copy/pasting.

The following options will be available:

```
[root@wazuh-manager /]# /var/ossec/bin/manage_agents

*****
* Wazuh v2.1.1 Agent manager.          *
* The following options are available: *
*****

(A)dd an agent (A) .
(E)xtract key for an agent (E) .
(L)ist already added agents (L) .
(R)emove an agent (R) .
(Q)uit.
Choose your action: A,E,L,R or Q: █
```

OSSEC HIDS Menu

- Choose 'A'

Add a name for the agent and an IP address that should match the one the agent will be connecting from i.e. CALFORNIADC01 192.168.0.100

- Press 'Y'

```
- Adding a new agent (use '\q' to return to the main menu) .
Please provide the following:
* A name for the new agent: myagent
* The IP Address of the new agent: 192.168.0.100
* An ID for the new agent[001]:
Agent information:
ID:001
Name:myagent
IP Address:192.168.0.100
Confirm adding it?(y/n): █
```

Setting up the OSSEC agent IP and name

Retrieve the agent key information by entering 'E' for extract and the ID for the agent. Copy this key as it will be required for the remote agent install.

Example:

Agent key information for '002' is:

MDAxIFRlc3RBZ2V0biAxMTEuMTEeLjExMS4xMTEgY2MxZjA1Y2UxNWQyNzEyNjdIMmE3MTRIO
DIOMTA1YTgxNTM5ZDIiN2U2ZDQ5MwYyZBkOTU4MjRmNjU3ZmI2Zg==

Restart the OSSEC/Wazuh manager within the OSSEc container on Proteus:

- `var/ossec/bin/ossec-control restart`

```
manage_agents: Exiting.
root@siemonster-project-dev9-ossec-1:~# var/ossec/bin/ossec-control restart
Killing ossec-monitord ..
Killing ossec-logcollector ..
Killing ossec-remoted ..
Killing ossec-syscheckd ..
Killing ossec-analysisd ..
ossec-maild not running ..
Killing ossec-execd ..
OSSEC HIDS v2.9.0 Stopped
Starting OSSEC HIDS v2.9.0 (by Trend Micro Inc.)...
2016/12/19 21:58:55 ossec-maild: INFO: E-Mail notification disabled. Clean Exit.
Started ossec-maild...
Started ossec-execd...
Started ossec-analysisd...
Started ossec-logcollector...
Started ossec-remoted...
Started ossec-syscheckd...
Started ossec-monitord...
Completed.
root@siemonster-project-dev9-ossec-1:~# var/ossec/bin/list_agents -a
Test-01-172.31.45.51 is available.
root@siemonster-project-dev9-ossec-1:~#
```

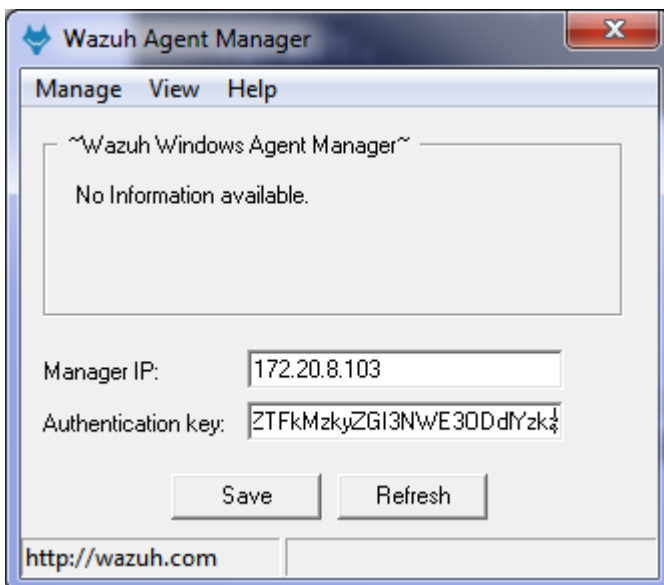
To install the remote agent on a windows machine, first download the agent install file <http://agents.siemonster.com/wazuh-agent-2.1.1-1.msi>

SHA256Checksum:

4e933484131b58d04bedeebafd93bc2d55fbf33faaf18956ab629a13bfaf4187a

Note. The agent must be installed with administrator privileges.

Launch the agent and enter the IP address of the Proteus appliance along with the key previously presented.



Proteus IP and Key

Back on the Proteus appliance check that the agent has connected correctly.

- `var/ossec/bin/list_agents -a`

```
[root@wazuh-manager /]# /var/ossec/bin/list_agents -a
SERVER9-172.20.8.1 is available.
[root@wazuh-manager /]#
```

6.5 SYSLOG

Network devices with remote syslog settings should be set to the Proteus appliance IP address. Syslogs are accepted on the ports

514 TCP	1516 TCP
514 UDP	1516 UDP

Parsing is handled by Logstash-Indexer before forwarding to the ES cluster. Syslog-NG is used to receive syslogs which are then converted to JSON and sent into the RabbitMQ message broker queue, from which they are input to the Logstash-Indexer.

7 INPUTS

7.1 LOGSTASH

All event data excepting syslog is initially received and processed by the Logstash-Collector before being sent on to the RabbitMQ message broker queue. The data is then input to the Logstash-Indexer where it is normalized and formatted for suitability for indexing into Elasticsearch.

Configuration files are located within the NFS shared folder /nfs on the Makara server.

```
makara nfs # ls -l
total 112
drwxr-xr-x. 2 root root 4096 Jan 14 00:55 siemonster-project-vagrant_alertmanager_c760b
drwxr-xr-x. 2 root root 4096 Jan 14 00:54 siemonster-project-vagrant_elastalert_rules_202ed
drwxr-xr-x. 4 102 102 4096 Jan 14 00:54 siemonster-project-vagrant_es-config_d5980
drwxr-xr-x. 2 33 33 4096 Jan 14 00:56 siemonster-project-vagrant_fouroneone-data_0bd87
drwxr-xr-x. 4 104 107 4096 Jan 14 01:15 siemonster-project-vagrant_grafana_data_feef1
drwxrwxr-x. 2 root root 4096 Jan 14 04:15 siemonster-project-vagrant_logstash-collector_52956
drwxrwxr-x. 2 root root 4096 Jan 14 20:25 siemonster-project-vagrant_logstash-indexer_6d728
drwxr-xr-x. 329 nobody nobody 20480 Jan 14 22:13 siemonster-project-vagrant_prometheus_data_e34ae
drwxr-xr-x. 2 nobody nobody 4096 Jan 14 00:55 siemonster-project-vagrant_prometheus_rules_3f47b
drwxr-xr-x. 3 root root 4096 Jan 14 01:31 siemonster-project-vagrant_reports_b0341
drwxrwxrwx. 2 122 129 4096 Jan 14 00:56 siemonster-project-vagrant_reports_config_f606a
drwxr-xr-x. 4 root root 4096 Jan 14 00:55 siemonster-project-vagrant_syslog-ng_094b6
```

Check out the SIEMonster logstash repo for the latest files - <https://github.com/siemonster>.

The layout of these files is set out in sections as follows: Input {} Filter {} Output {}

Multiple configuration files are processed in an alphanumeric sequence. For this reason, the most efficient method of deployment is to separate the input, filter and output into separate files.

Each input is given a tag and/or type for identification. This tag/type is used through the pipeline 'input-filter-output' to ensure that each data source is processed correctly. The following example illustrates how to configure Logstash-Collector to input Windows event logs:

From a terminal session on the Makara instance, make backups of any files pending edit, e.g. within the /nfs folder, cp xxx-logstash-collector_XXXXX/00-inputs.conf ~/

Edit the file / xxx-logstash-collector_XXXXX /00-inputs.conf to match the port setup to receive these logs from NXLOG.

```
makara nfs # ls -l
total 112
drwxr-xr-x. 2 root root 4096 Jan 14 00:55 siemonster-project-vagrant_alertmanager_c760b
drwxr-xr-x. 2 root root 4096 Jan 14 00:54 siemonster-project-vagrant_elastalert_rules_202ed
drwxr-xr-x. 4 102 102 4096 Jan 14 00:54 siemonster-project-vagrant_es-config_d5980
drwxr-xr-x. 2 33 33 4096 Jan 14 00:56 siemonster-project-vagrant_fouroneone-data_0bd87
drwxr-xr-x. 4 104 107 4096 Jan 14 01:15 siemonster-project-vagrant_grafana_data_feef1
drwxrwxr-x. 2 root root 4096 Jan 14 22:20 siemonster-project-vagrant_logstash-collector_52956
drwxrwxr-x. 2 root root 4096 Jan 14 22:18 siemonster-project-vagrant_logstash-indexer_6d728
drwxr-xr-x. 331 nobody nobody 20480 Jan 14 22:19 siemonster-project-vagrant_prometheus_data_e34ae
drwxr-xr-x. 2 nobody nobody 4096 Jan 14 00:55 siemonster-project-vagrant_prometheus_rules_3f47b
drwxr-xr-x. 3 root root 4096 Jan 14 01:31 siemonster-project-vagrant_reports_b0341
drwxrwxrwx. 2 122 129 4096 Jan 14 00:56 siemonster-project-vagrant_reports_config_f606a
drwxr-xr-x. 4 root root 4096 Jan 14 00:55 siemonster-project-vagrant_syslog-ng_094b6
makara nfs # vi siemonster-project-vagrant_logstash-collector_52956/00-inputs.conf
```

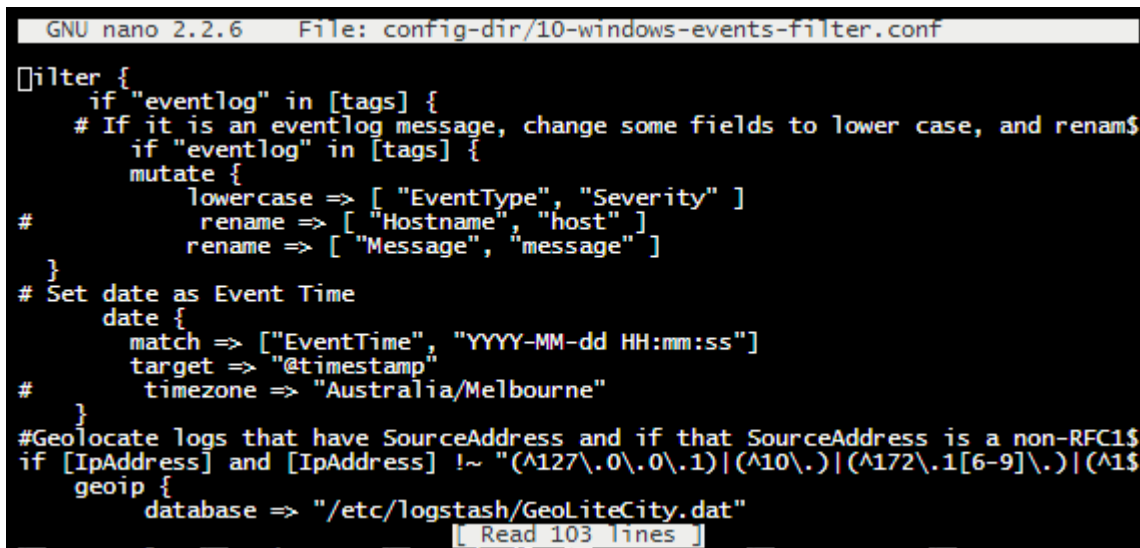
Match with NXlog configuration file – see 4.1

```

Input {
  tcp {
    type => "events"
    port => 3522
    ssl_enable => true
    ssl_cert => "/etc/logstash/logstash-forwarder.crt"
    ssl_key => "/etc/logstash/logstash-forwarder.key"
    ssl_verify => false
    codec => json_lines
    tags => ["windows", "eventlog"]
  }
}

```

Backup and then edit the file `/nfs/xxx-logstash-indexer_xxxxx/10-windows-events-filter.conf` for specific use cases/time zone changes etc.



```

GNU nano 2.2.6 File: config-dir/10-windows-events-filter.conf
filter {
  if "eventlog" in [tags] {
    # If it is an eventlog message, change some fields to lower case, and rename
    if "eventlog" in [tags] {
      mutate {
        lowercase => [ "EventType", "Severity" ]
        rename => [ "Hostname", "host" ]
        rename => [ "Message", "message" ]
      }
    }
    # Set date as Event Time
    date {
      match => [ "EventTime", "YYYY-MM-dd HH:mm:ss" ]
      target => "@timestamp"
      # timezone => "Australia/Melbourne"
    }
    #Geolocate logs that have SourceAddress and if that SourceAddress is a non-RFC15
    if [IpAddress] and [IpAddress] !~ "(^127\.0\.0\.1)|(^10\.)|(^172\.1[6-9]\.)|(^15
      geopip {
        database => "/etc/logstash/GeoLiteCity.dat"
      }
    }
  }
}

```

Save and exit

Restart the Logstash container and check the logs for errors, particularly 'Pipeline stopped' which indicates configuration file errors.

Active	logstash-collector ⓘ	Image: ikuturso/logstash-collector:1.1 Ports: 3520, 3521, 3522, 3524, 3525, 3526, 3527, 3528	Service	1 Container	⬆️ ⬇️ ⬇️
Active			Service	1 Cor	Upgrade ⬆️ Restart ⬇️
Active	logstash-indexer ⓘ	Image: ikuturso/logstash-indexer:1.0	Service	1 Container	⬆️ ⬇️ ⬇️
				1 Cor	Upgrade ⬆️ Restart ⬇️

Configuration files can be checked inside the containers, e.g.

```
/opt/logstash/bin/logstash --configtest -f /config-dir/00-inputs.conf
```

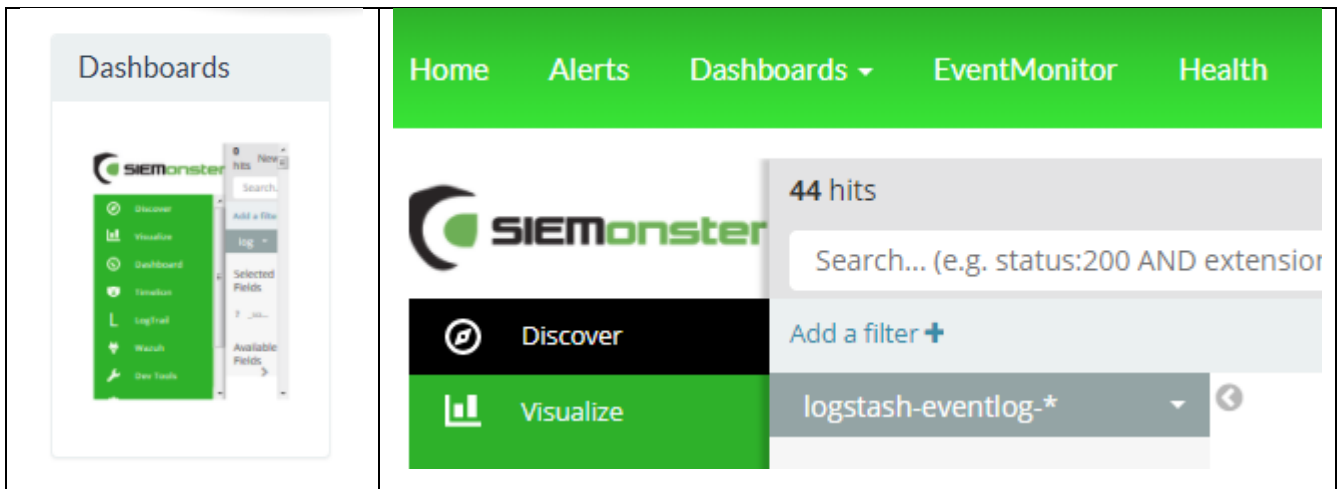
Correct response should be 'Configuration OK'. On error check the configuration files, edit, save and re-check.

Check the logs again for successful pipeline start.

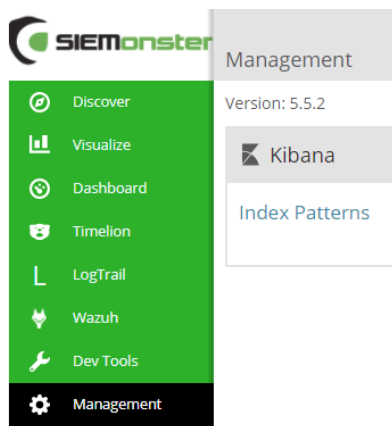
Check the connection from NXLOG: `netstat -ant |grep 3522` (or configured port)

The next step is to check for incoming events in Kibana. Assuming the index is named `logstash-eventlog-DATE` as preset in the `999-outputs.conf` of the Logstash Indexer then the events should be visible in the Discovery panel.

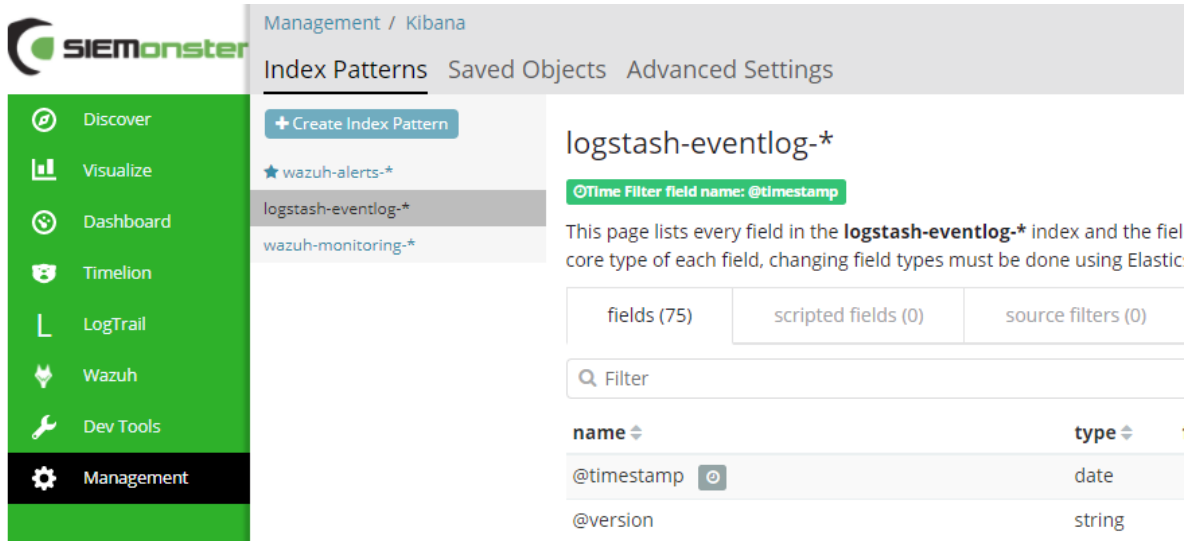
Access the Dashboards top menu or tile from the web application:



If the index has been renamed, then it should be first registered in the Management – Index Patterns panel:



Kibana Windows Events



Management / Kibana

Index Patterns Saved Objects Advanced Settings

+ Create Index Pattern

- wazuh-alerts-*
- logstash-eventlog-***
- wazuh-monitoring-*

logstash-eventlog-*

Time Filter field name: @timestamp

This page lists every field in the **logstash-eventlog-*** index and the field core type of each field, changing field types must be done using Elastic

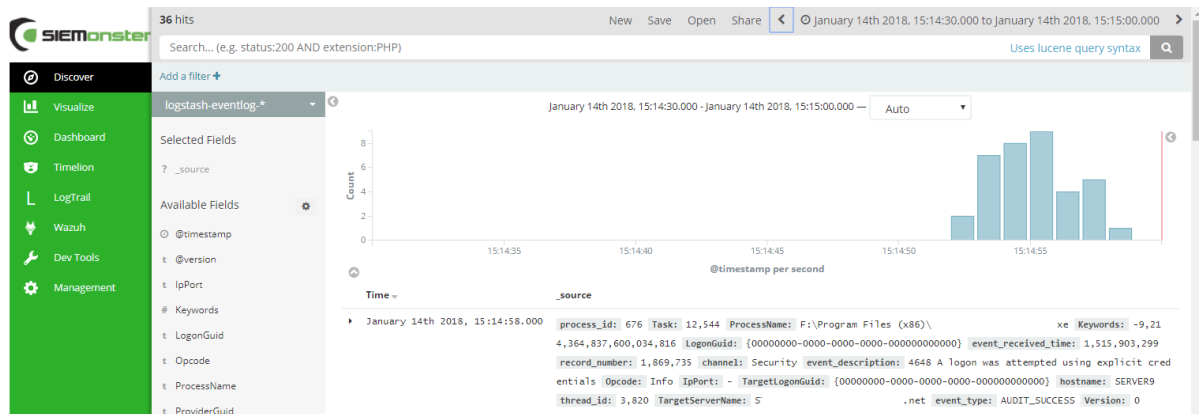
fields (75) scripted fields (0) source filters (0)

Filter

name	type
@timestamp	date
@version	string

Logstash Index

- Visit the Discovery menu and select the configured index



36 hits

Search... (e.g. status:200 AND extension:PHP)

logstash-eventlog-*

Selected Fields: ? _source

Available Fields: @timestamp, @version, IpPort, Keywords, LogonGuid, Opcode, ProcessName, ProviderGuid

January 14th 2018, 15:14:30.000 - January 14th 2018, 15:15:00.000

Count

Time

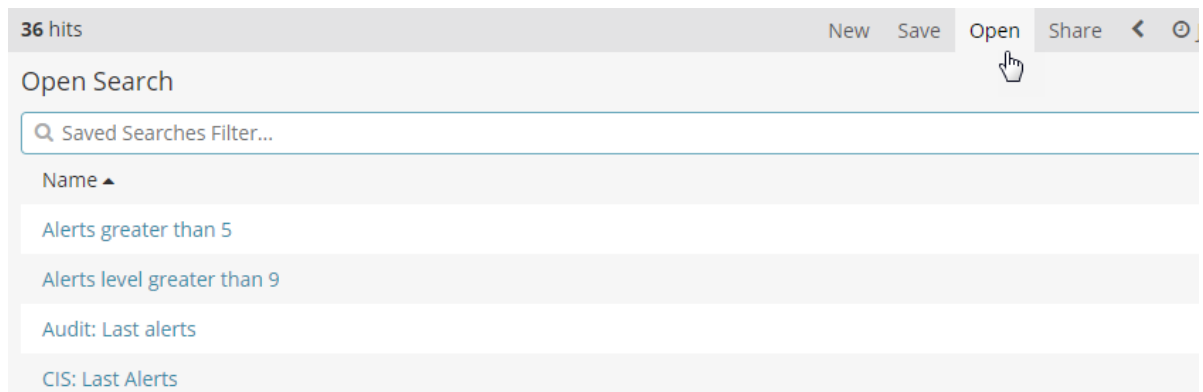
_source

```

process_id: 676 Task: 12,544 ProcessName: F:\Program Files (x86)\xe Keywords: -9,21
4,364,837,600,034,816 LogonGuid: {00000000-0000-0000-0000-000000000000} event_received_time: 1,515,903,299
record_number: 1,869,735 channel: Security event_description: 4648 A logon was attempted using explicit cred
entials Opcode: Info IpPort: - TargetLogonGuid: {00000000-0000-0000-0000-000000000000} hostname: SERVER9
thread_id: 3,820 TargetServerName: 5 .net_event_type: AUDIT_SUCCESS Version: 0
  
```

Visualization of the data

From here review some saved searches, visualizations and dashboards.



36 hits

New Save Open Share

Open Search

Search Saved Searches Filter...

Name

- Alerts greater than 5
- Alerts level greater than 9
- Audit: Last alerts
- CIS: Last Alerts

7.2 TROUBLESHOOTING SYSLOGS

If you're not sure whether there is a firewall in your way, or that the syslog conf is working there are a few things you can do.

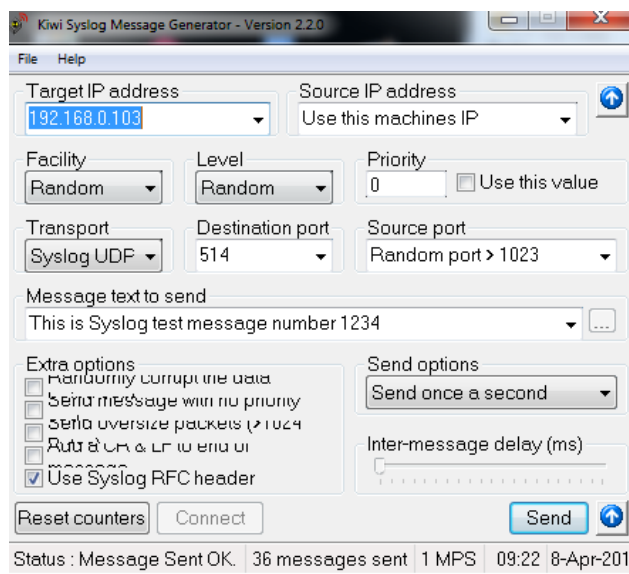
First telnet from the router/firewall subnet to Proteus on the port number i.e. telnet Proteus on the TCP port if it can see Proteus you're off to a good start for example

- telnet 192.168.0.103 514

To test syslogs, a test can be performed as follows, provided that the Syslog-ng changes were made as shown in section 7.4. This involves downloading a free tool that can be run on any Microsoft Windows box. The tool generates messages that get sent to Proteus and we can see if they are getting processed.

Download a syslog message generator on a windows machine.

<http://downloads.solarwinds.com/solarwinds/Release/FreeTool/Kiwi-SyslogGen-v2.zip>



Syslog Checker

Enter the Target IP address of the Proteus appliance and click Send.

Syslogs are logged within the Syslog container. Exec a shell from the Rancher UI and check `/var/log/syslog`

`> Shell: siemonster-project-vagrant-syslog-ng-1`

```
root@siemonster-project-vagrant-syslog-ng-1:~# tail /var/log/syslog
Jan 15 10:16:34 192.168.0.21 SERVER9 SyslogGen SIEMonster rocks
Jan 15 10:16:34 192.168.0.21 SERVER9 SyslogGen SIEMonster rocks
Jan 15 10:16:34 192.168.0.21 SERVER9 SyslogGen SIEMonster rocks
Jan 15 10:16:34 192.168.0.21 SERVER9 SyslogGen SIEMonster rocks
Jan 15 10:16:34 192.168.0.21 SERVER9 SyslogGen SIEMonster rocks
Jan 15 10:16:34 192.168.0.21 SERVER9 SyslogGen SIEMonster rocks
Jan 15 10:16:34 192.168.0.21 SERVER9 SyslogGen SIEMonster rocks
Jan 15 10:16:34 192.168.0.21 SERVER9 SyslogGen SIEMonster rocks
Jan 15 10:16:34 192.168.0.21 SERVER9 SyslogGen SIEMonster rocks
Jan 15 10:16:34 192.168.0.21 SERVER9 SyslogGen SIEMonster rocks
root@siemonster-project-vagrant-syslog-ng-1:~#
```


7.3 CATCH ALL SYSLOG FILTER

To set up a 'catch all' syslog filter within Logstash for testing purposes prior to deploying a complete filter. Open an SSH terminal on the Makara server. Locate the /nfs folder & list the Logstash-Indexer folder.

```
drwxr-xr-x. 2 root root 4096 Jan 14 00:55 siemmonster-project-vagrant_alertmanager_c760b
drwxr-xr-x. 2 root root 4096 Jan 14 00:54 siemmonster-project-vagrant_elastalert_rules_202ed
drwxr-xr-x. 4 102 102 4096 Jan 14 00:54 siemmonster-project-vagrant_es-config_d5980
drwxr-xr-x. 2 33 33 4096 Jan 14 00:56 siemmonster-project-vagrant_fouroneone-data_0bd87
drwxr-xr-x. 4 104 107 4096 Jan 14 01:15 siemmonster-project-vagrant_grafana_data_feef1
drwxrwxr-x. 2 root root 4096 Jan 14 23:23 siemmonster-project-vagrant_logstash-collector_52956
drwxrwxr-x. 2 root root 4096 Jan 14 22:18 siemmonster-project-vagrant_logstash-indexer_6d728
drwxr-xr-x. 361 nobody nobody 20480 Jan 14 23:43 siemmonster-project-vagrant_prometheus_data_e34ae
drwxr-xr-x. 2 nobody nobody 4096 Jan 14 00:55 siemmonster-project-vagrant_prometheus_rules_3f47b
drwxr-xr-x. 3 root root 4096 Jan 14 01:31 siemmonster-project-vagrant_reports_b0341
```

Backup the existing syslog filter and then delete:

```
cp /nfs/xxx_logstash-indexer_xxx/03-multisyslog-filter.conf ~/
rm /nfs/xxx_logstash-indexer_xxx/03-multisyslog-filter.conf
```

Download a basic syslog filter from SIEMonster Github:

```
wget https://raw.githubusercontent.com/siemonster/logstash/master/04-syslog-basic.conf
```

Copy over to the Logstash-Indexer configuration directory on Makara:

```
cp 04-syslog-basic.conf /nfs/xxx_logstash-indexer_xxx/
```

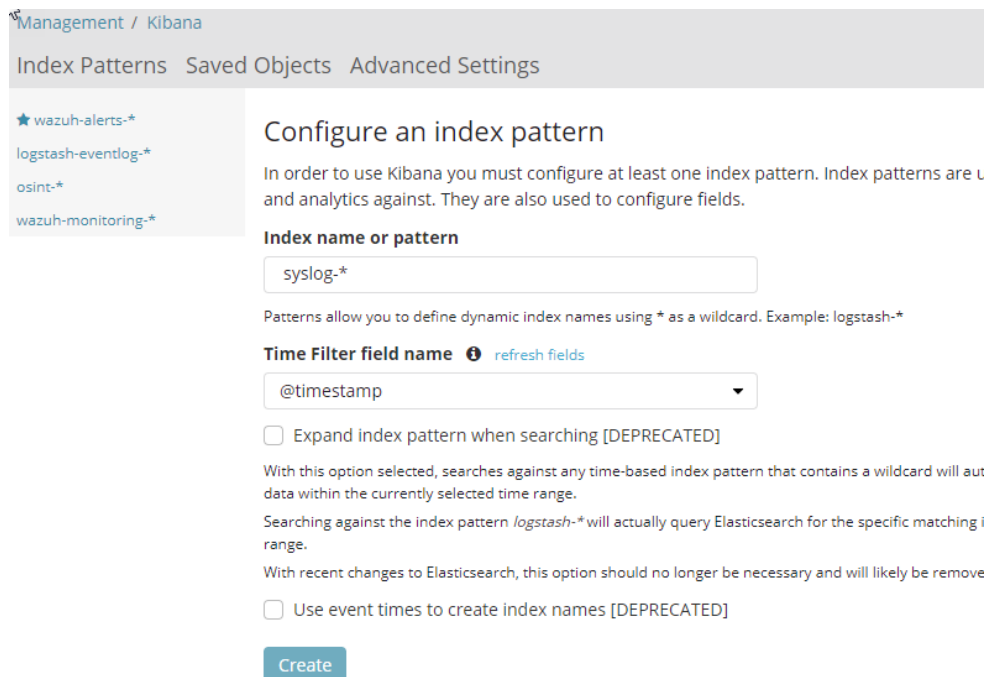
Restart the Logstash-Indexer container:

```
Docker restart <containerID>
```

Send some syslogs to Proteus on port 514 TCP/UDP

Check the logs inside the Syslog-NG container - /var/log/syslog

Configure a new index pattern:



The screenshot shows the Kibana interface for configuring an index pattern. The page title is 'Configure an index pattern'. Below the title, there is a description: 'In order to use Kibana you must configure at least one index pattern. Index patterns are used to filter data and analytics against. They are also used to configure fields.' The 'Index name or pattern' field contains 'syslog-*'. Below this, there is a 'Time Filter field name' dropdown menu set to '@timestamp'. There are two checkboxes: 'Expand index pattern when searching [DEPRECATED]' (unchecked) and 'Use event times to create index names [DEPRECATED]' (unchecked). A 'Create' button is at the bottom.

In the Discovery tab view the incoming logs:



7.4 TROUBLESHOOTING CISCO ASA SYSLOGS

You have completed all the steps above, and you can see traffic hitting Proteus, but you're not sure how to check whether its appearing in Logstash. Use the steps below.

Send some syslog to Proteus on UDP port 514 or 1514 from your ASA or other device. For example, log onto the device, or fail to log onto the device.

- Use the pre-configured cisco-fw index or register a syslog index in Kibana - Settings:

Notes:

If your endpoints have differing timestamps, to avoid a time travel paradox, edit the 03-multisyslog-filter.conf file and replace the timezone fields with your own timezone. <http://joda-time.sourceforge.net/timezones.html>

Otherwise events may appear in the future and will not be visible in Kibana.

In the Logstash-Indexer configuration file on the Makara server:

e.g. vi nfs/xxx_logstash-indexer_xx/03-multisyslog-filter.conf

```

}
syslog_pri { }
date {
  match => [ "syslog_timestamp", "MMM d HH:mm:ss",
  timezone => "Australia/Melbourne"
}

```

Time zone mods

Debugging:

Check the logs for the Logstash-Indexer container for any errors:

Logs: siemonster-project-siemonster-logstash-1

Note: Only combined stdout/stderr logs are available for this container because it was run with the TTY (-t) flag.

```
07/02/2017 06:37:16 log4j:WARN No appenders could be found for logger (io.netty.util.internal.logging.InternalLoggerFactory).
07/02/2017 06:37:16 log4j:WARN Please initialize the log4j system properly.
07/02/2017 06:37:16 log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
07/02/2017 06:37:18 Settings: Default pipeline workers: 4
07/02/2017 06:37:22 Pipeline main started
07/02/2017 12:00:05 SIGTERM received. Shutting down the agent. {:level=>:warn}
07/02/2017 12:00:05 stopping pipeline {:id=>"main"}
07/02/2017 12:00:29 log4j:WARN No appenders could be found for logger (io.netty.util.internal.logging.InternalLoggerFactory).
07/02/2017 12:00:29 log4j:WARN Please initialize the log4j system properly.
07/02/2017 12:00:29 log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more info.
07/02/2017 12:00:30 Settings: Default pipeline workers: 4
07/02/2017 12:00:33 Pipeline main started
```

8 ALERTING

8.1 411

The primary alerting system for V3, configured with many index interfaces to provide a feature rich method of event log analysis and outputs for email, Slack, Pager Duty, and webhooks to send to custom applications.

Configure Searches to periodically run against a variety of data sources. You can define a custom pipeline of Filters to manipulate any generated Alerts and forward them to multiple Targets.

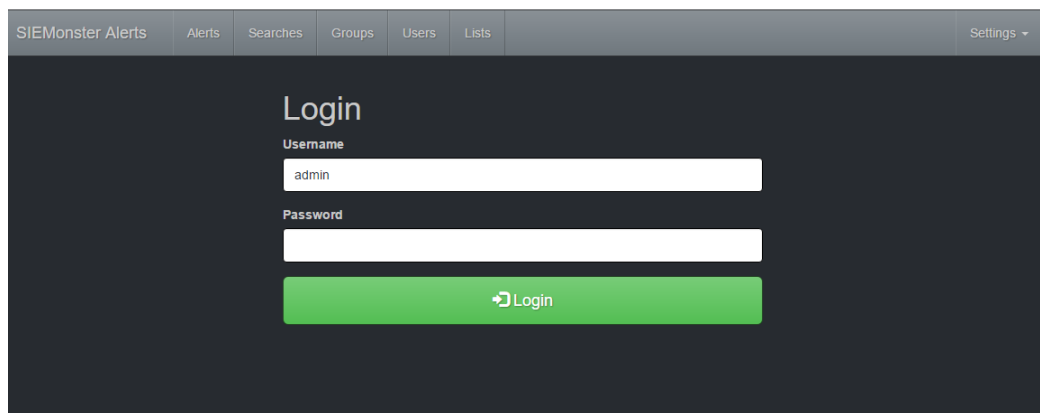
Use Cases:

- You want to detect when certain log lines show up in ES.
- You want to detect when a Graphite metric changes.
- You want to detect when a server stops responding
- You want to manage alerts through a simple workflow.

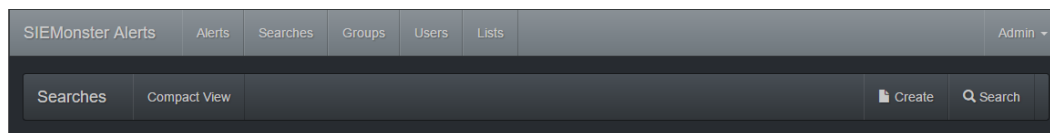
SIEMonster includes the 411 Alert management suite similar to Graylog that offers configurable search scheduling to query ES to detect security related events and then through alert management, send alerts to the users required to be notified.

8.2 ADDING A SEARCH

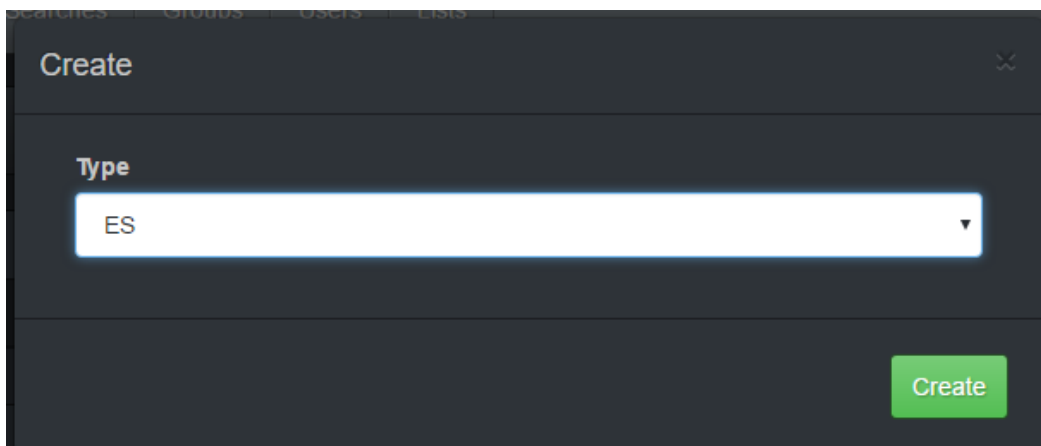
1. Login to the 411 web console by clicking on Alerts in the SIEMonster main menu.



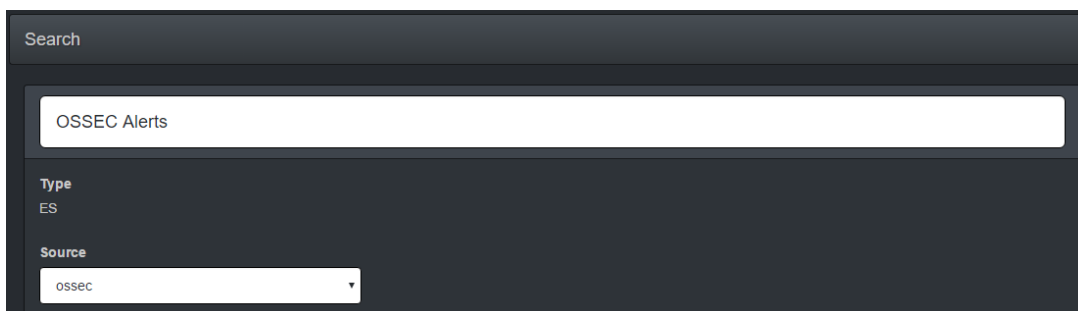
2. Click searches, then Create.



3. Type ES.



4. For this example, set up the search for high severity level OSSEC events, set Name of the search as appropriate, set the source to the index required to search from, for this example source will be set to 'ossec' to detect high severity level security events on OSSEC agents in the system.



5. Enter the search query to be executed on the data source, for this example find alert levels greater than 9 only, eg using the table below

10 - Multiple user generated errors - They include multiple bad passwords, multiple failed logins, etc. They may indicate an attack or may just be that a user just forgot his credentials.

11 - Integrity checking warning - They include messages regarding the modification of binaries or the presence of rootkits (by rootcheck). If you just modified your system configuration you should be fine regarding the "syscheck" messages. They may indicate a successful attack. Also included IDS events that will be ignored (high number of repetitions).

12 - High impotency event - They include error or warning messages from the system, kernel, etc. They may indicate an attack against a specific application.

13 - Unusual error (high importance) - Most of the times it matches a common attack pattern.

14 - High importance security event. Most of the times done with correlation and it indicates an attack.

15 - Severe attack - No chances of false positives. Immediate attention is necessary.

Basic Notifications Advanced

Query

rule.AlertLevel:>9

The search query to execute against the data source.

- Set the result to return, either return the fields and data of resulting search with a filter of limited or unlimited amount of results returned, or can specify to return a count of result entries found. Specify the fields that need to be displayed in the result in the fields dialog, eg. AgentName, description, etc. Lastly give an appropriate Description of what the search does.

Result Type Result Filter

Fields Count No results

At least -inf At most inf results

Fields

AgentName rule.firedtimes rule.description GeoLocation.country_name

Description

Ossec Alerts greater than 9

A description of what this Search does.

- Set Category as appropriate, for OSSEC it will be security, set the Tags, Priority of the search, and both the frequency of the search which is how often the search will be executed and the time range of events to be searched, so if its 30 minutes, when the search is run it will search for events that occurred with 30 minutes prior to the current time of search.

- Make sure that status is enabled.

Category Tags Priority

Security HIDS Medium

Frequency Time Range

Cron? 1 minute 30 minutes

Status

Enable

Test Create

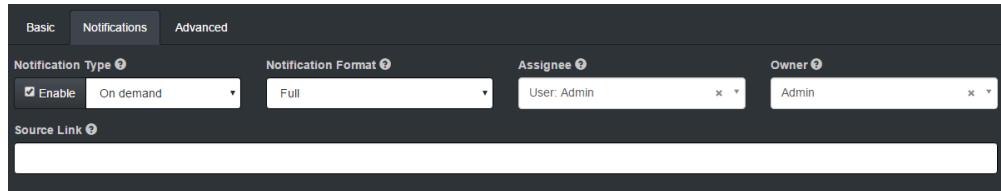
- Click Test if required, then click Create.
- (Optional) if you are modifying an existing search, add a Description of changes made and click Update.

Description of changes

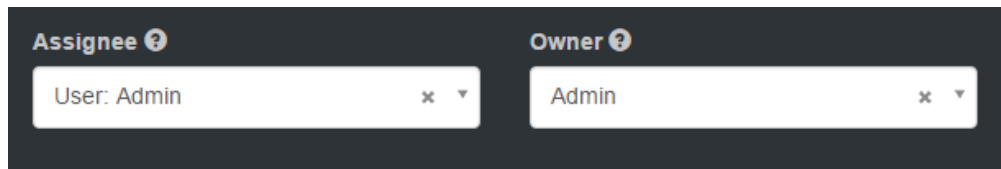
Test Execute Update Delete

8.3 SETTING NOTIFICATIONS

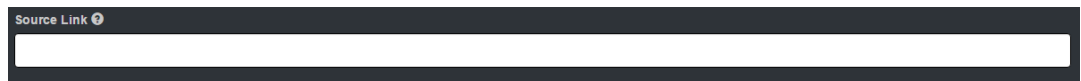
1. Click on the notifications tab in the search settings page. Click the checkbox to enable and set the type to On demand, Hourly, or Daily to choose how often notifications are sent. Choose format to be Full or Content only of search.



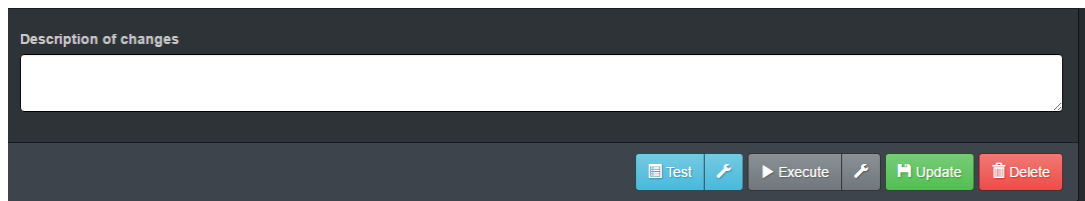
2. Set the Assignee which is the user or group of users that the notification will be sent to, and the Owner the user that maintains and administers the search itself.



3. If required set the source link of the search to be sent in the notification.

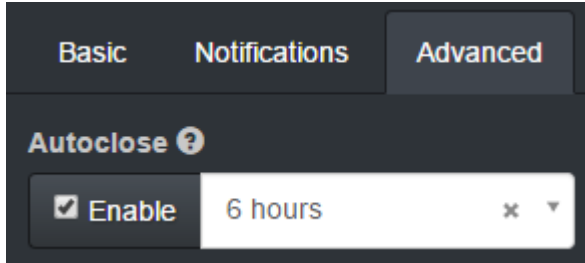


4. Click Test if required and then click Create.
5. (Optional) if you are modifying an existing search notification settings, add a Description of changes made and click Update.

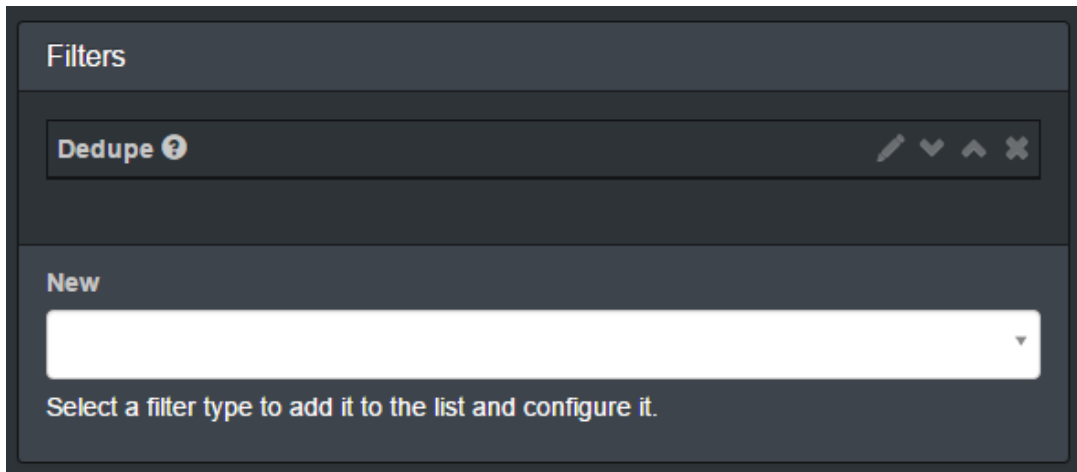


8.4 ADVANCED

1. Autoclose: enable and set a time to define how long before the alert is automatically closed after there has been no activity.

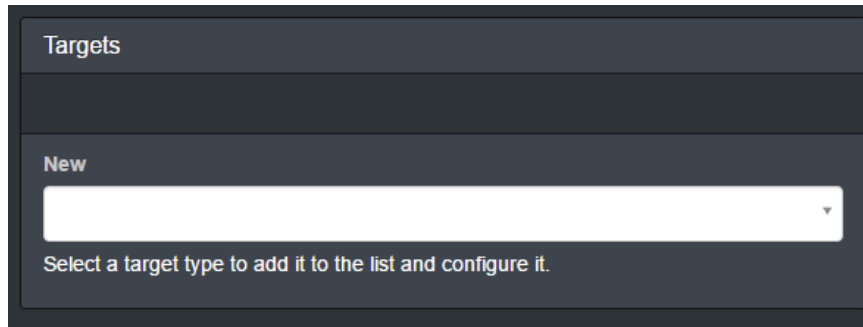


2. Filters: Enable filters by clicking the New dropdown dialog, for example the Dedupe filter removes duplicates of alerts, which is important if your search is set to repeat frequently through a range of time in which a particular alert could appear in multiple occurrence of this search.



There are many filters that can be applied, to find out what each filter does, simply hover the mouse over the question mark icon next to the filter name.

3. Targets: Set targets to where notifications get sent to by the search, to add a target click the New dropdown menu and click either WebHook or PagerDuty.



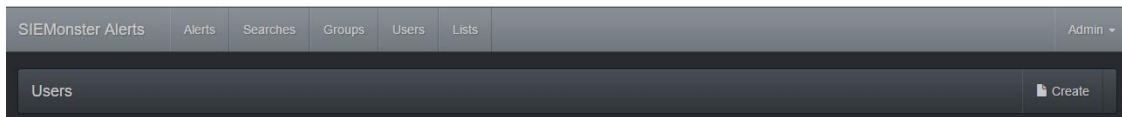
WebHook – sends alerts off to a remote server using the HTTP POST method.

PagerDuty – sends alert to a Pager system.

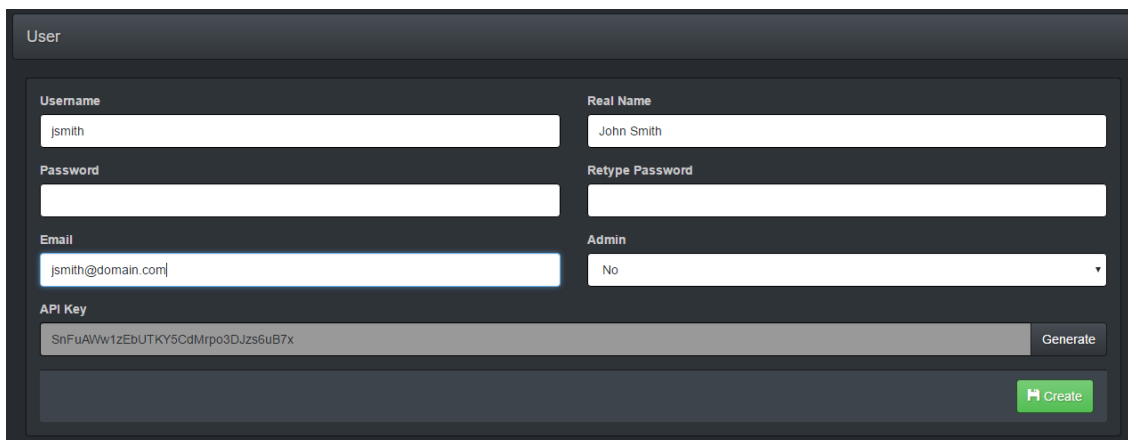
4. Once all filters and targets have been set and configured, click Save Filters and Targets.
5. Add Description of changes, click Test if required and then click Update.

8.5 USERS AND GROUPS

1. Creating users: Click Users in the top menu, then click create on the right-hand side.



2. Fill in the required user details. including email in which notifications will be sent to depending on what searches the user is an assignee of.

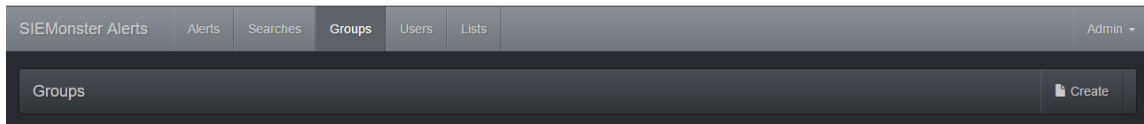


The form contains the following fields and values:

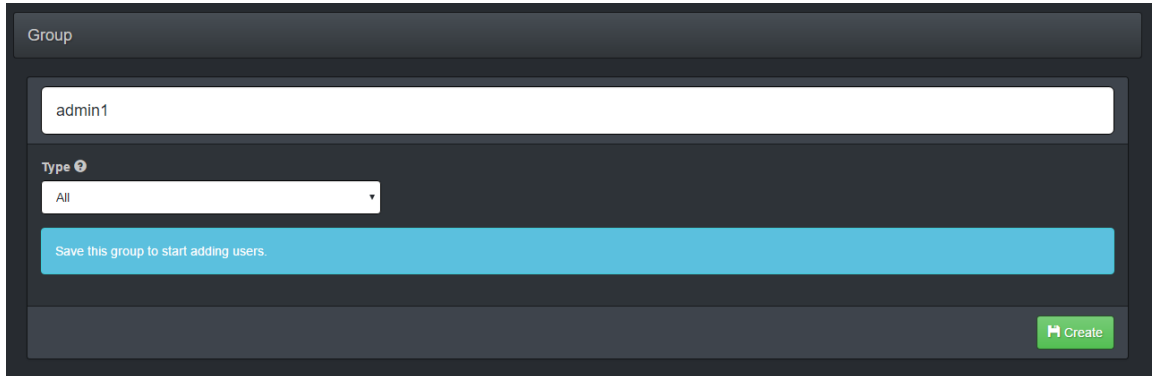
- Username: jsmith
- Real Name: John Smith
- Password: (empty)
- Retype Password: (empty)
- Email: jsmith@domain.com
- Admin: No
- API Key: SnFuAWw1zEbUTKY5CdMrpo3DJzs6uB7x

Then click Create.

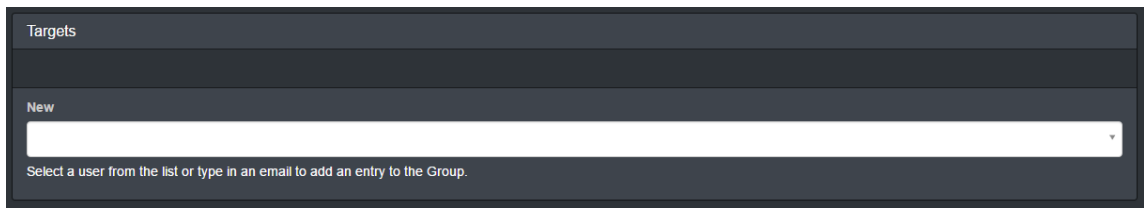
3. Groups: Click Groups in the top menu, then click create on the right-hand side.



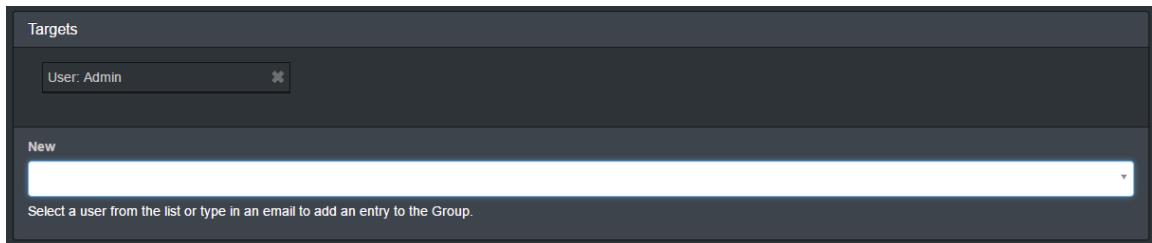
Give the Group a Name and Type, then click Create.



4. Add members to this group by clicking the New dropdown menu in the targets section.



Then click the user to add in the dropdown menu.



The user will now display in the targets section and is now a member of the group.

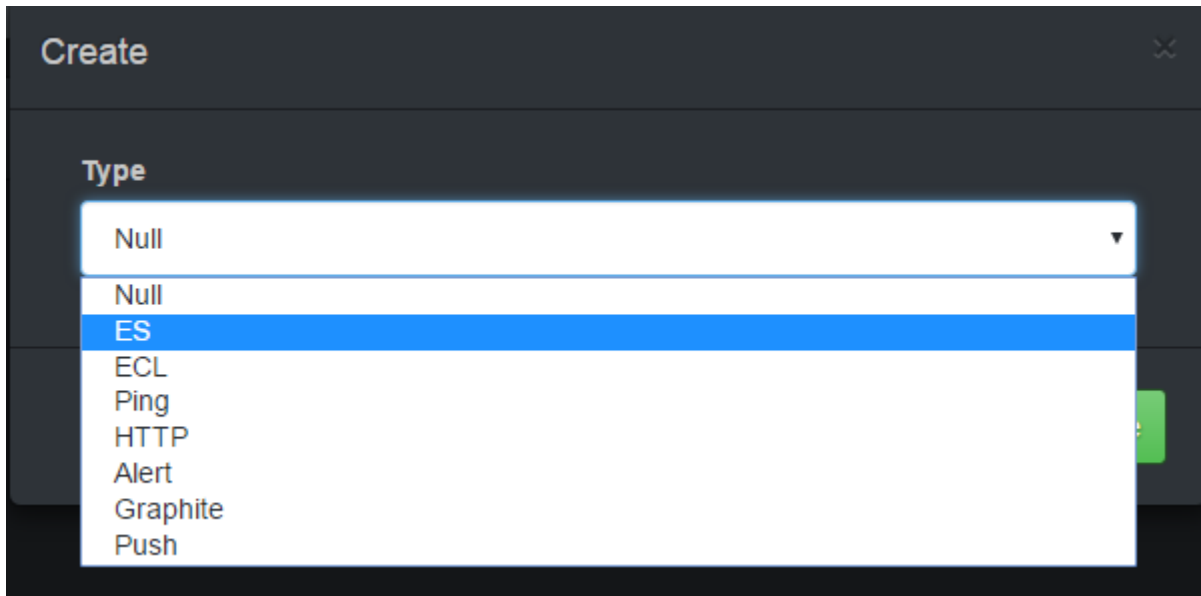
5. Click Update when finished to save the group and exit the group editor menu.

8.6 INDEX OVERVIEW

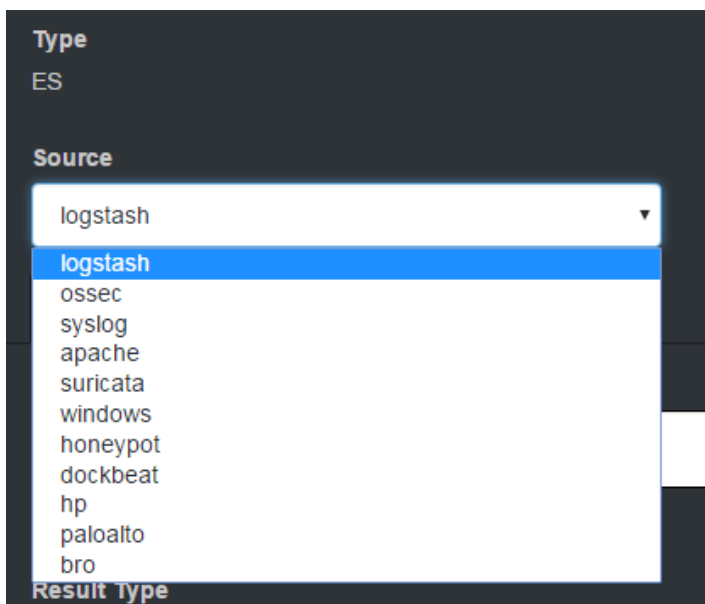
411 Alert Management Web Application offers new features for multiple index searching via the generic ES search option. This can be accessed when creating new searches.

8.7 ADD INDEX

1. Check the ES option is available in Searches – Create Search



2. Access index type under Source



- To create a new search, open a terminal session to Makara and locate the 411-configuration folder within the /nfs folder

```
drwxr-xr-x. 2 root root 4096 Jan 14 00:55 siemonster-project-vagrant_alertmanager_c760b
drwxr-xr-x. 2 root root 4096 Jan 14 00:54 siemonster-project-vagrant_elastalert_rules_202ed
drwxr-xr-x. 4 102 102 4096 Jan 14 00:54 siemonster-project-vagrant_es-config_d5980
drwxr-xr-x. 2 33 33 4096 Jan 14 00:56 siemonster-project-vagrant_fouroneone-data_0bd87
drwxr-xr-x. 4 104 107 4096 Jan 14 01:15 siemonster-project-vagrant_grafana_data_reer1
drwxrwxr-x. 2 root root 4096 Jan 14 23:23 siemonster-project-vagrant_logstash-collector_52956
drwxrwxr-x. 2 root root 4096 Jan 14 22:18 siemonster-project-vagrant_logstash-indexer_6d728
drwxr-xr-x. 361 nobody nobody 20480 Jan 14 23:43 siemonster-project-vagrant_prometheus_data_e34ae
drwxr-xr-x. 2 nobody nobody 4096 Jan 14 00:55 siemonster-project-vagrant_prometheus_rules_3f47b
drwxr-xr-x. 3 root root 4096 Jan 14 01:31 siemonster-project-vagrant_reports_b0341
```

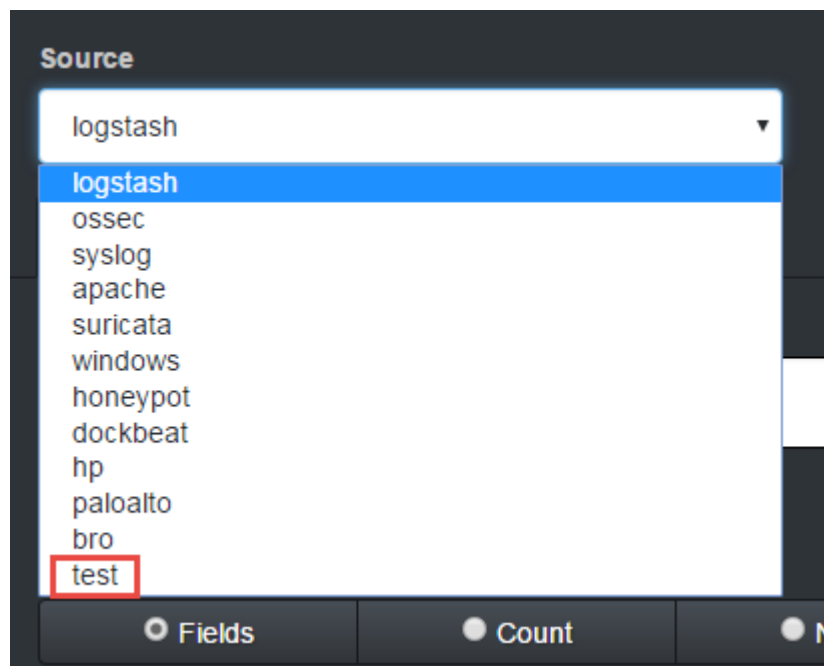
Edit the config.php file within, copy an existing stanza and append.

Change the required index name/type

```
# Configuration for the bro index that 411 queries.
'bro' => [
  'hosts' => ['https://elastic:s13M0nSterV3@es-master:9200'],
  'index_hosts' => [],
  'ssl_cert' => '/usr/share/elasticsearch/config/searchguard/ssl/elastic.crtfull.pem',
  'index' => '[bro-]Y.m.d',
  'date_based' => true,
  'date_field' => '@timestamp',
  'src_url' => null,
],
```

Save this file and exit

- There is no need to restart any containers, simply reload the 411 web page to see the new index type.

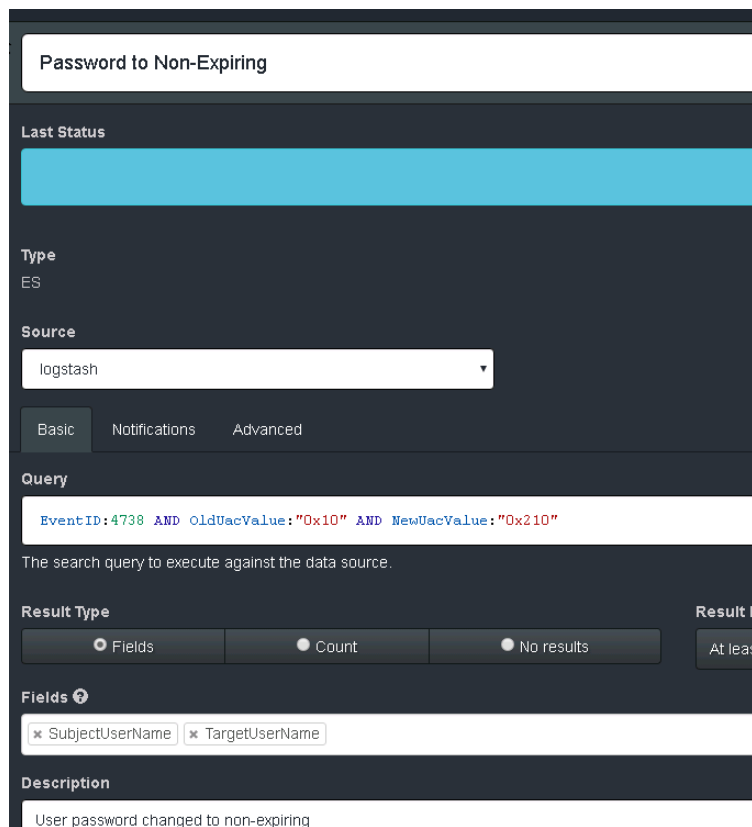


8.8 HOW TO SETUP ALERTS EXAMPLES IN 411

Listed below are some examples of possible configurations of searches and use cases that are a capability of 411.

8.9 WINDOWS USER ACCOUNT PASSWORD SET TO NON-EXPIRING ALERT

- The following search settings are to search the logstash data source in Elastic Search.
- The Query uses **EventID:4738, A user account was changed**, which refers to unique security log event in windows.
- The **OldUacValue** and **NewUacValue**, which are the User Account Control flags for this particular event, using this in the query will ensure that only the event of a password being set to not expire.
- The fields returned are **SubjectUserName** and **TargetUserName**, being the requester of the action and the user account affected.
- This alert is triggered when a user accounts password is set not to expire.

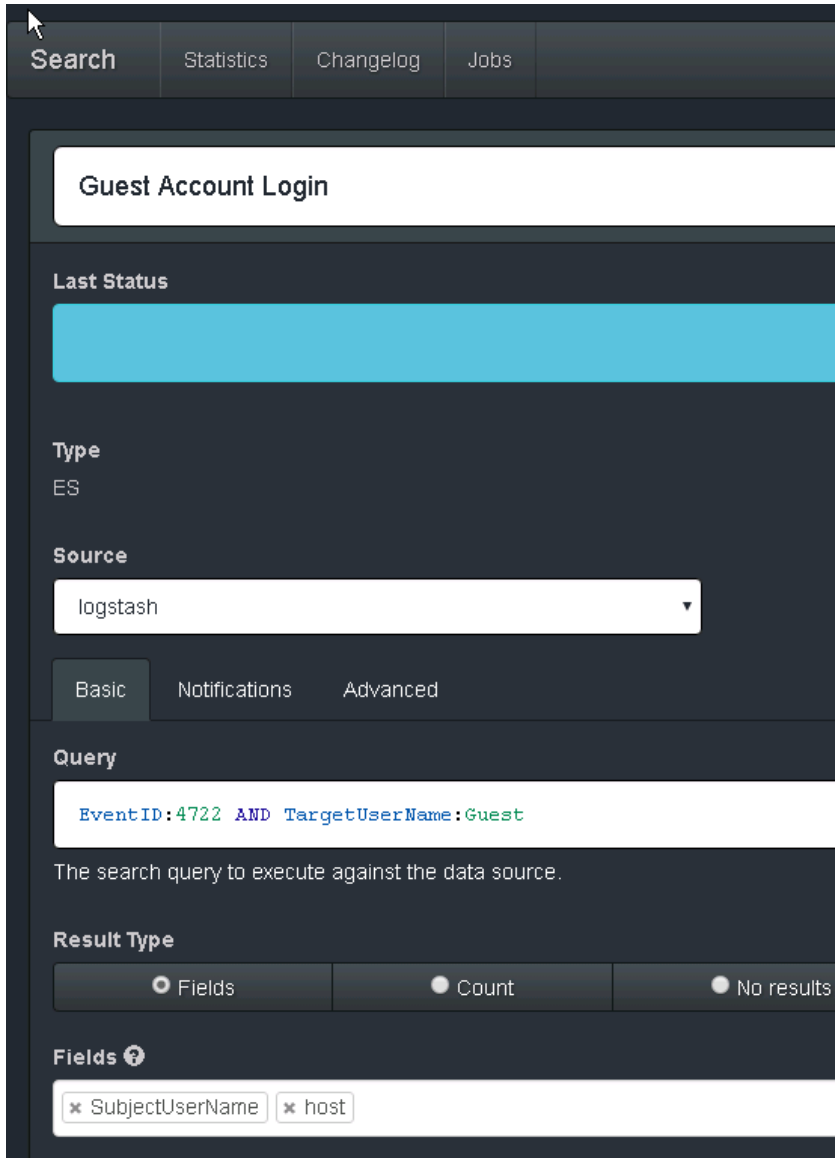


The screenshot shows the configuration interface for an alert titled "Password to Non-Expiring". The interface includes the following sections:

- Last Status:** A blue bar indicating the current status.
- Type:** Set to "ES".
- Source:** A dropdown menu set to "logstash".
- Query:** The query is `EventID:4738 AND OldUacValue:"0x10" AND NewUacValue:"0x210"`. Below the query, it states "The search query to execute against the data source."
- Result Type:** Three radio buttons are present: "Fields" (selected), "Count", and "No results". A "Result F" button is partially visible on the right.
- Fields:** Two fields are selected: "SubjectUserName" and "TargetUserName".
- Description:** The description is "User password changed to non-expiring".

8.10 GUEST ACCOUNT LOGIN ALERT

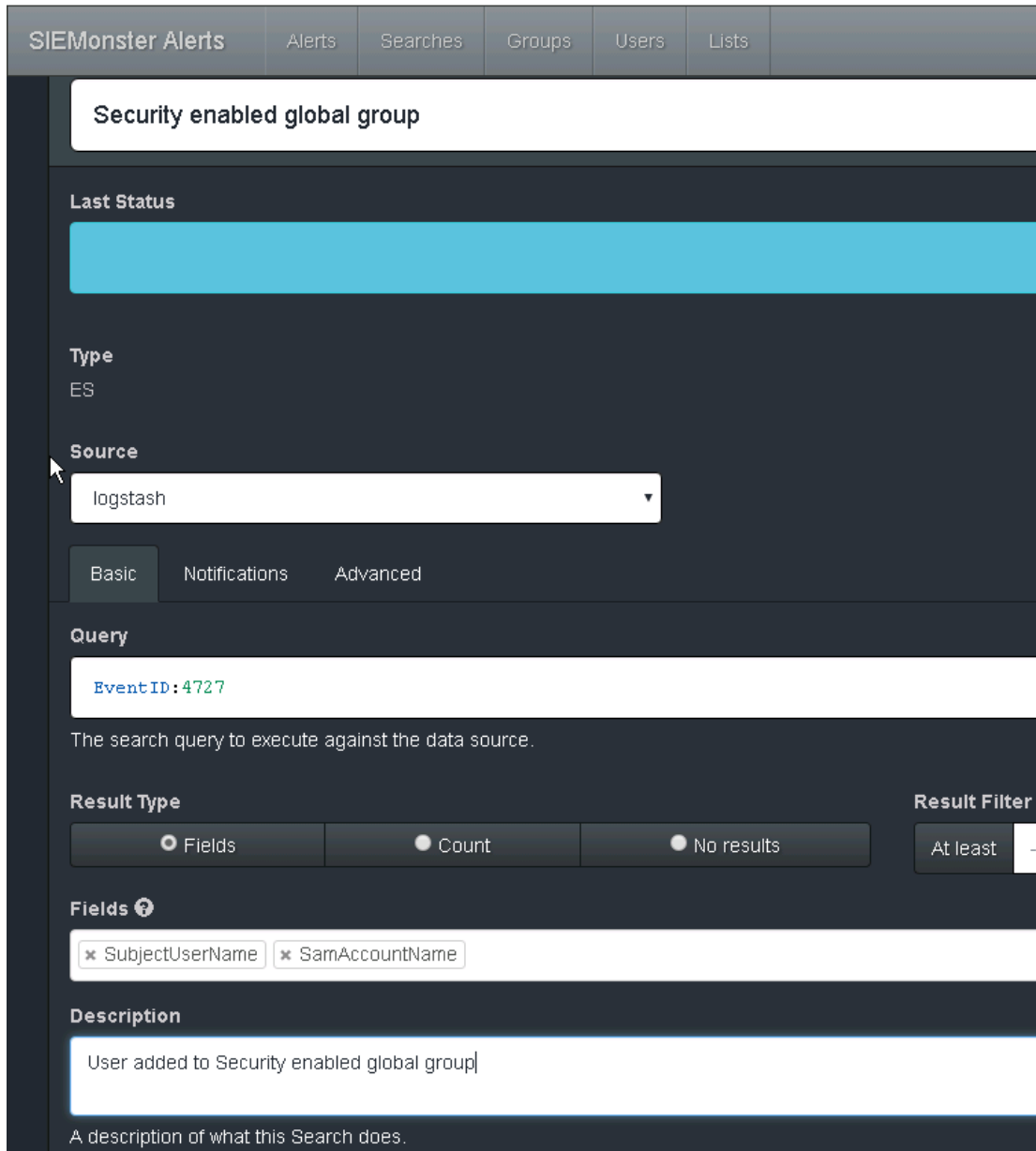
- Data source: **logstash**.
- Query selects **EventID:4722, A user account was enabled**.
- And **TargetUserName:Guest** which specifies the user account affected, being **Guest**.
- Returns the **SubjectUserName** and **host**, being the user that performed the action and the host machine the action was performed on.
- This alert is triggered when the Guest account on windows is used.



The screenshot shows the configuration interface for an alert named "Guest Account Login". At the top, there are navigation tabs: "Search" (selected), "Statistics", "Changelog", and "Jobs". Below the title, there is a "Last Status" section with a blue bar. The "Type" is set to "ES". The "Source" is a dropdown menu set to "logstash". There are three tabs for configuration: "Basic" (selected), "Notifications", and "Advanced". The "Query" field contains the text: `EventID:4722 AND TargetUserName:Guest`. Below the query, it says "The search query to execute against the data source." The "Result Type" section has three radio buttons: "Fields" (selected), "Count", and "No results". The "Fields" section shows two fields: "SubjectUserName" and "host", each with a close button (x).

8.11 WINDOWS USER ACCOUNT ADDED TO SECURITY GROUP ALERT

- Data source: **logstash**.
- Query selects **EventID:4727, A security-enabled global group was created**.
- Returns the **SubjectUserName** and **SamAccountName** which is the User that performed the action and the Group name affected.
- A Security group is a local group on a windows system that delegates permissions to users within that group.

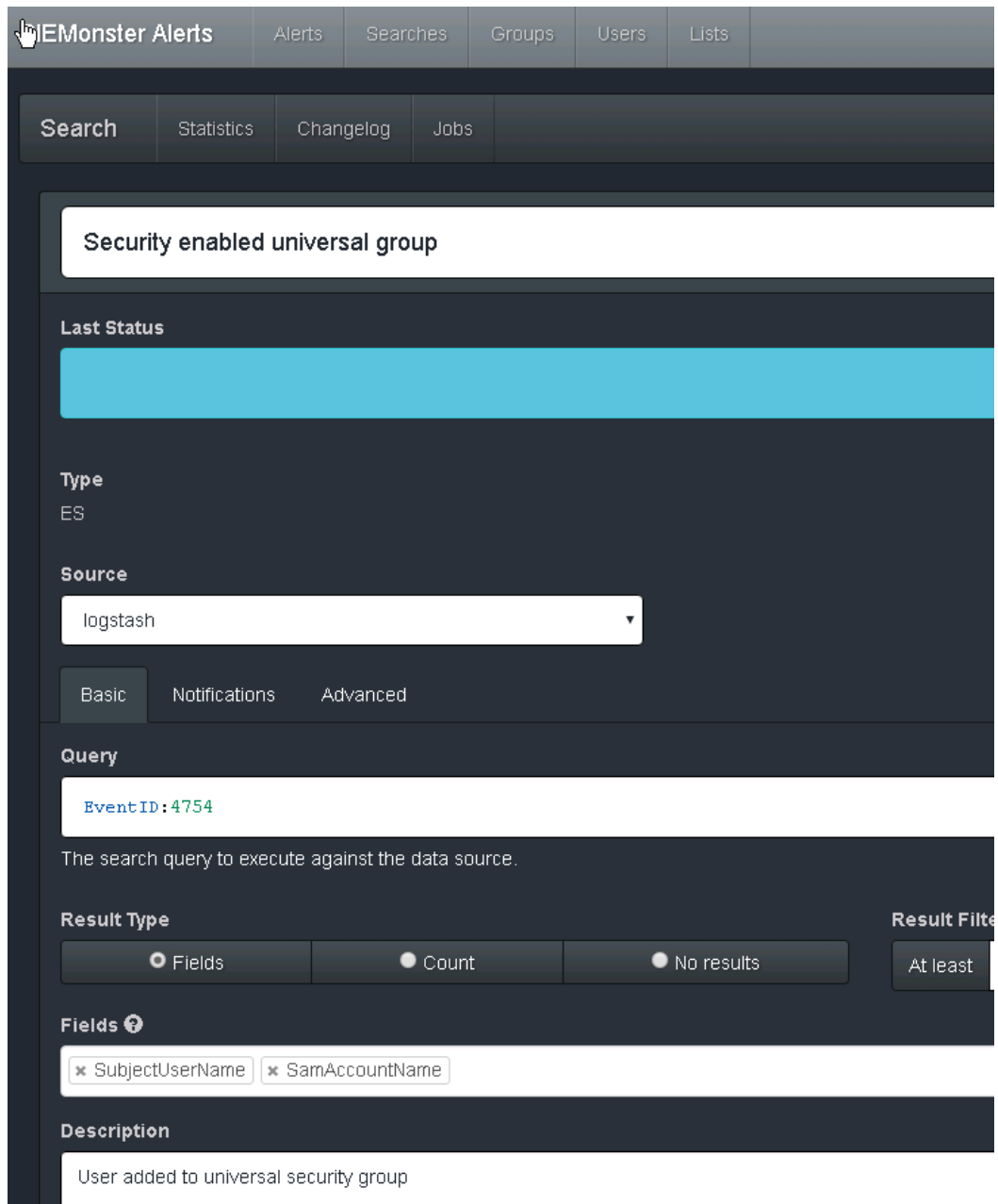


The screenshot shows the configuration interface for an alert in SIEMonster. The top navigation bar includes 'SIEMonster Alerts', 'Alerts', 'Searches', 'Groups', 'Users', and 'Lists'. The main content area is titled 'Security enabled global group' and contains several sections:

- Last Status:** A blue bar indicating the alert's current state.
- Type:** Set to 'ES'.
- Source:** A dropdown menu set to 'logstash'.
- Basic / Notifications / Advanced:** Tabs for configuring the alert's behavior.
- Query:** A text box containing the query 'EventID:4727'. Below it, a note states: 'The search query to execute against the data source.'
- Result Type:** Radio buttons for 'Fields' (selected), 'Count', and 'No results'.
- Result Filter:** A dropdown menu set to 'At least'.
- Fields:** A list of selected fields: 'SubjectUserName' and 'SamAccountName'.
- Description:** A text box containing the description 'User added to Security enabled global group'. Below it, a note states: 'A description of what this Search does.'

8.12 WINDOWS USER ACCOUNT ADDED TO UNIVERSAL SECURITY GROUP ALERT

- Data source: logstash.
- Query selects EventID:4754, A security-enabled universal group was created.
- Returns the SubjectUserName and SamAccountName which is the User that performed the action and the Group name affected.
- A Security group is a cross-domain group on a windows system that delegates permissions to users within that group and those permissions span across different domains.



The screenshot displays the SIEMonster Alerts interface. At the top, there is a navigation bar with tabs for Alerts, Searches, Groups, Users, and Lists. Below this is a secondary navigation bar with Search, Statistics, Changelog, and Jobs. The main content area shows an alert titled "Security enabled universal group".

Last Status

Type
ES

Source
logstash

Basic | Notifications | Advanced

Query
EventID:4754
The search query to execute against the data source.

Result Type
 Fields | Count | No results

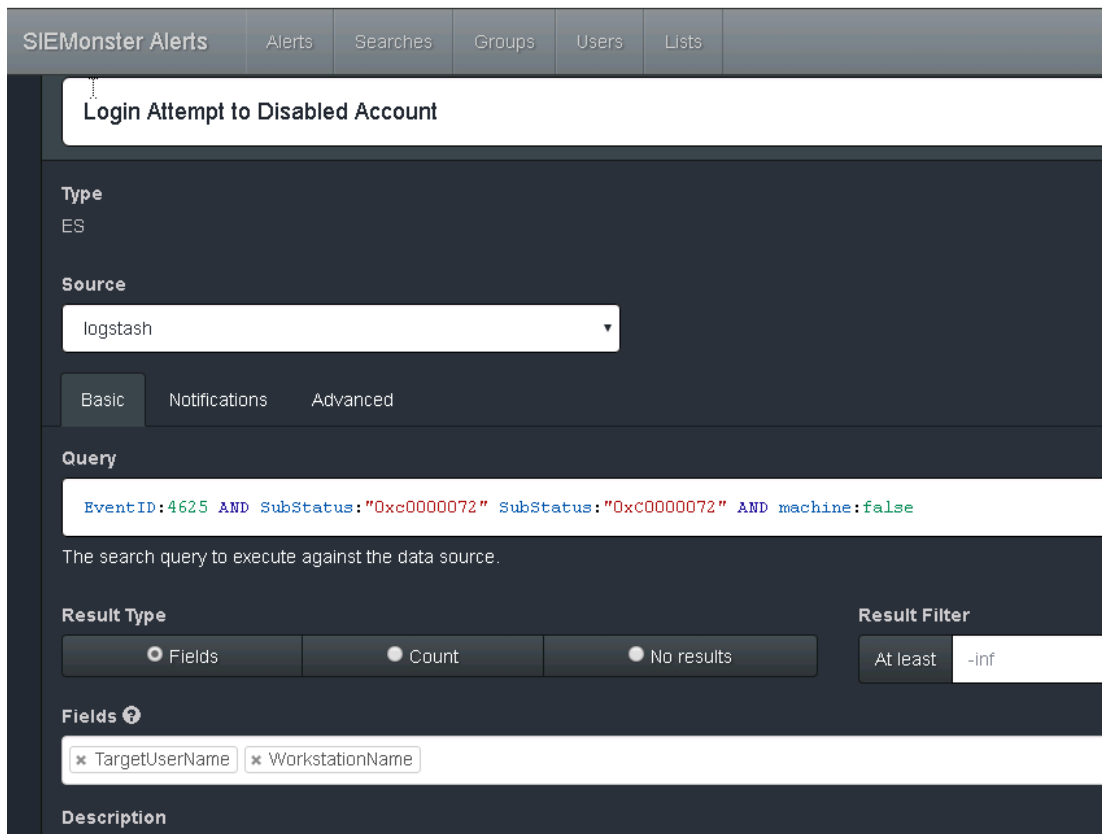
Result Filter
At least

Fields ⓘ
x SubjectUserName | x SamAccountName

Description
User added to universal security group

8.13 LOGIN ATTEMPT TO DISABLED WINDOWS USER ACCOUNT ALERT

- Data source: logstash.
- Query selects EventID:4625, An account failed to log on.
- SubStatus and machine, which substatus is the code signifying the logon failure reason, and machine, a true or false value.
- Returns the TargetUserName and WorkstationName, which is the user name that was used in the logon attempt and the name of the workstation the logon attempt was made on.
- This alert is triggered when someone tries to logon to an account that is disable.




The screenshot shows the configuration interface for an alert in SIEMonster. The alert is titled "Login Attempt to Disabled Account".

- Alerts:** Login Attempt to Disabled Account
- Type:** ES
- Source:** logstash
- Query:** `EventID:4625 AND SubStatus:"0xc0000072" SubStatus:"0xc0000072" AND machine:false`
- Result Type:** Fields (selected), Count, No results
- Result Filter:** At least -inf
- Fields:** TargetUserName, WorkstationName
- Description:** (empty)

8.14 SLACK

- Create a slack channel by going to; <https://slack.com/>
And create a new team by following the prompts on the website.
- Once the slack team is created, install the incoming-webhook application into the channel required to receive notifications from 411.



Incoming WebHooks

Incoming Webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details described later.

[Message Attachments](#) can also be used in Incoming Webhooks to display richly-formatted messages that stand out from regular chat messages.

1. Take note of the Webhook URL field of the configuration.

Webhook URL

Send your JSON payloads to this URL.
[Show setup instructions](#)

<https://hooks.slack.com/services/T4LBYQU91/B4LF41PGC/bMhyuLAJeXqKHF>

[Regenerate](#)

2. On the Makara server, navigate to the /nfs folder and locate the 411 configuration folder:

```
drwxr-xr-x. 2 root root 4096 Jan 14 00:55 siemmonster-project-vagrant_alertmanager_c760b
drwxr-xr-x. 2 root root 4096 Jan 14 00:54 siemmonster-project-vagrant_elastalert_rules_202ed
drwxr-xr-x. 4 102 102 4096 Jan 14 00:54 siemmonster-project-vagrant_es-config_d5980
drwxr-xr-x. 2 33 33 4096 Jan 14 00:56 siemmonster-project-vagrant_fouroneone-data_0bd87
drwxr-xr-x. 4 104 107 4096 Jan 14 01:15 siemmonster-project-vagrant_grafana_data_reer1
drwxrwxr-x. 2 root root 4096 Jan 14 23:23 siemmonster-project-vagrant_logstash-collector_52956
drwxrwxr-x. 2 root root 4096 Jan 14 22:18 siemmonster-project-vagrant_logstash-indexer_6d728
drwxr-xr-x. 361 nobody nobody 20480 Jan 14 23:43 siemmonster-project-vagrant_prometheus_data_e34ae
drwxr-xr-x. 2 nobody nobody 4096 Jan 14 00:55 siemmonster-project-vagrant_prometheus_rules_3f47b
drwxr-xr-x. 3 root root 4096 Jan 14 01:31 siemmonster-project-vagrant_reports_b0341
```

3. Edit the config.php file, and add the Webhook URL from the slack configuration to the required field below.

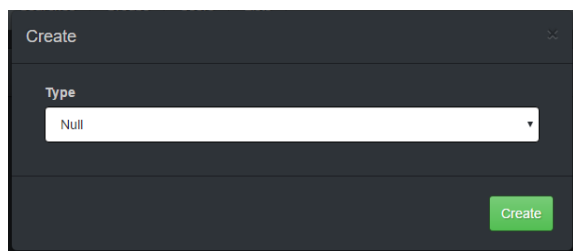
```
# Slack integration
# Fill in to allow 411 to send messages to Slack.
$config['slack'] = [
    'webhook_url' => 'https://hooks.slack.com/services/T4LBYQU91/B4LF41PGC/bMhyuLAJeXqXXXXXXXXX'
];
```

4. Save the configuration & restart the 411 container in the rancher stack menu.

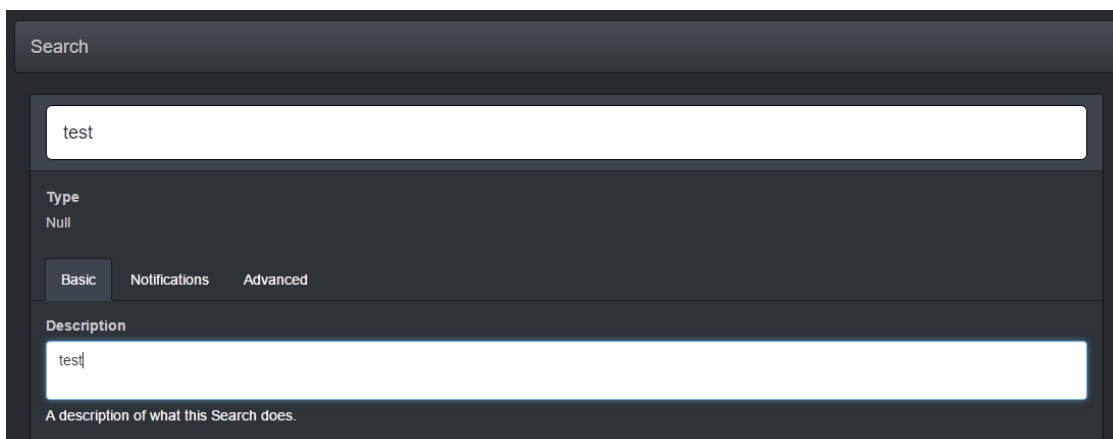
Active	411+1 Sidekick	Image: siemmonster-project-siemapp_411_1490013514654	Service	2 Containers	Upgrade Restart
Active	admin	Image: ikuturso/msa-free	Service	1 Cont	

5. To test slack notifications, go to the 411 console in the SIEMonster main menu.

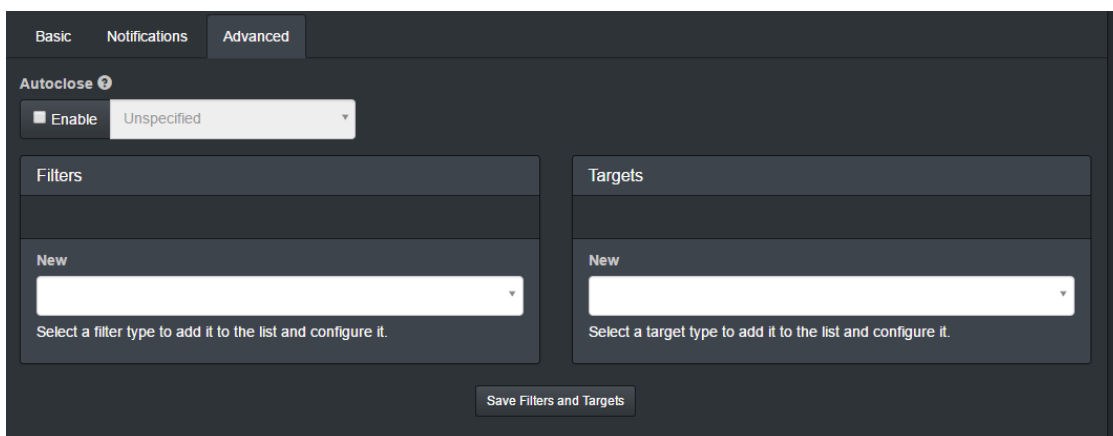
6. Create a new search, set Type to Null.

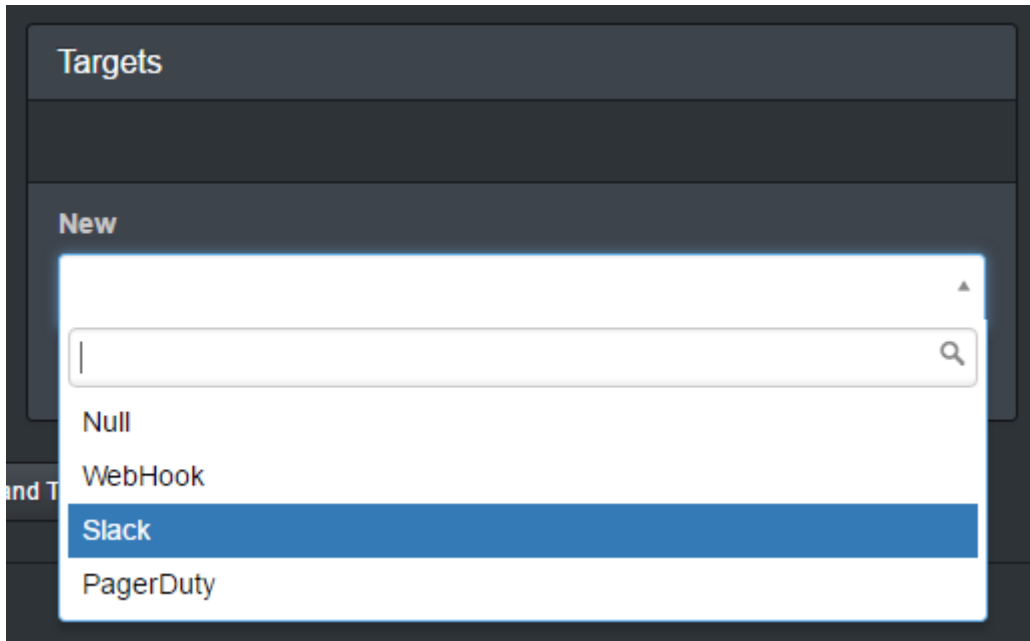


7. Set a Name and Description and click Create.

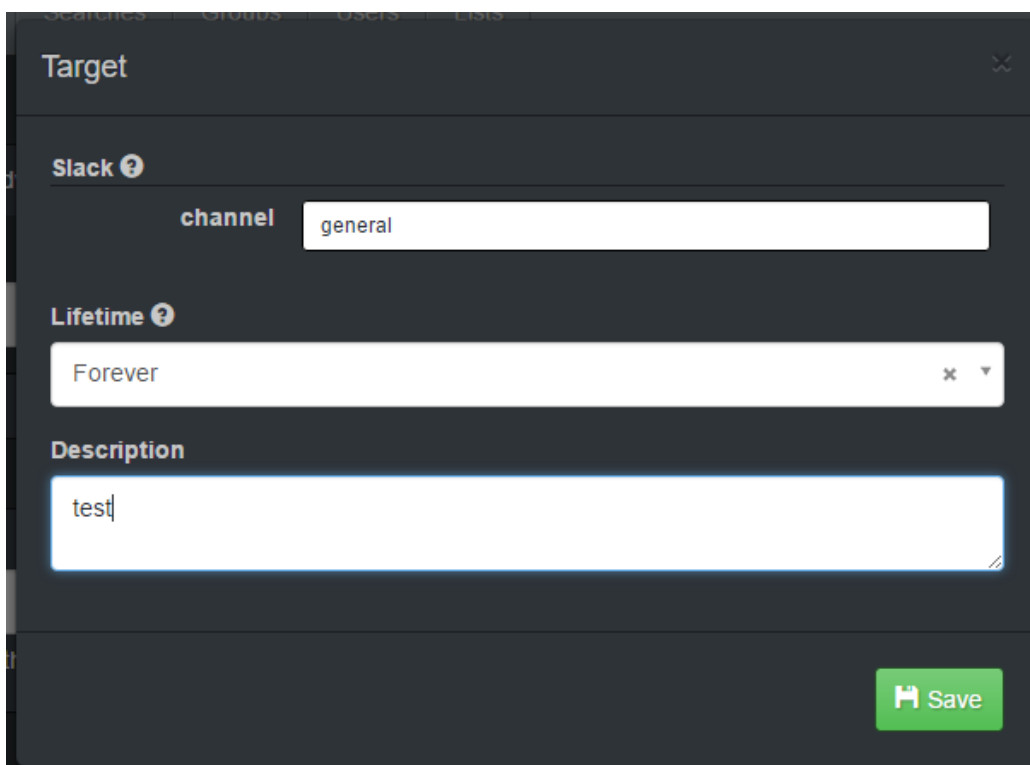


8. Go to the Advanced tab, click the Targets dropdown menu and click Slack.

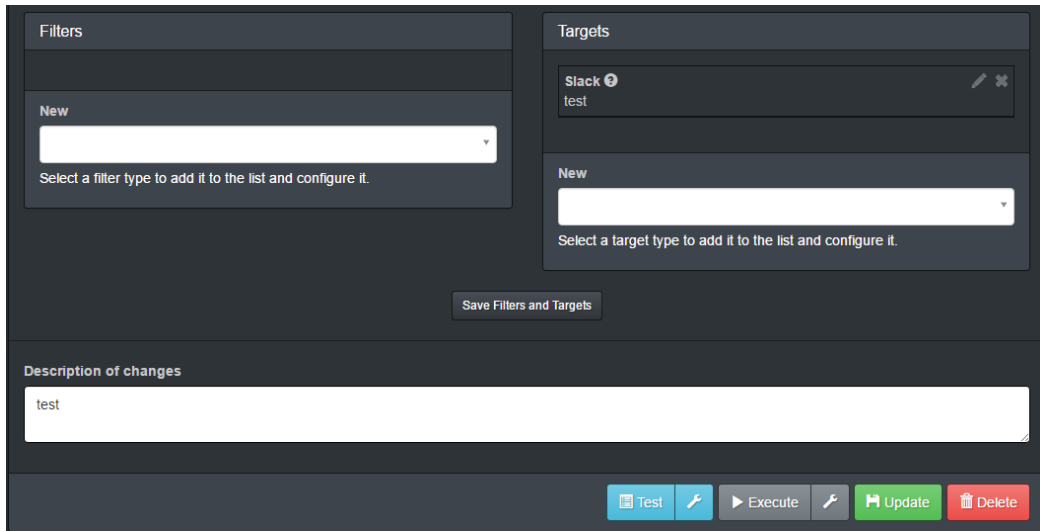




9. Set the Channel and Description and click Save.



- Click Save Filters and Targets, add a Description of changes and click Update.

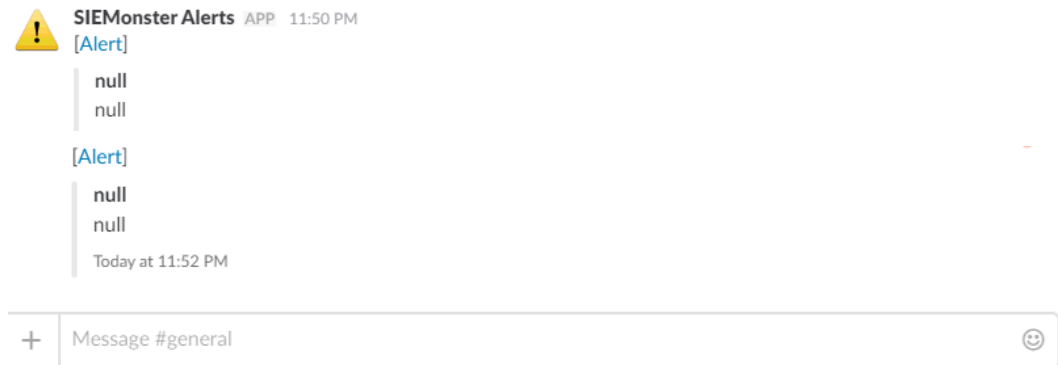


The screenshot shows a configuration interface with three main sections:

- Filters:** A 'New' dropdown menu with the text 'Select a filter type to add it to the list and configure it.'
- Targets:** A 'Slack' target with the name 'test', and another 'New' dropdown menu with the text 'Select a target type to add it to the list and configure it.'
- Description of changes:** A text input field containing the word 'test'.

At the bottom, there is a 'Save Filters and Targets' button and a row of action buttons: 'Test', 'Execute', 'Update', and 'Delete'.

- Click **Execute** and the slack channel configured will display notifications as shown below.



8.15 LOGSTASH

The 3rd alerting option is the Logstash system which can be useful for monitoring specific events. As an example, adding the following to the output section of a the Logstash Windows event configuration file will alert on a new security enabled group being created:

```
if [EventID] == 4727 {
  email {
    from => "siem@siemonster.com"
    subject => "%{EventDesc}"
    to => "alerts@siemonster.com"
    cc => "tickets@siemonster.com"
    via => "sendmail"
    body => "Alert - %{SubjectUserName} has created a new security enabled global group
    %{SamAccountName} %{message}"
    options => { "location" => "/sbin/sendmail" }
  }
}
```

9 OSINT

9.1 MINEMELD

As a part of the SIEMonster toolset, MineMeld is a Threat intelligence processing framework that can be used to collect, aggregate and filter indicators from a variety of sources and intelligence feeds.

Providing vectors for translation tables in the form of known malicious domains used for Phishing, C&C hosts, TOR endpoints and known compromised hosts. This open source intelligence is then used to identify/detect such hosts contained within incoming security log data.

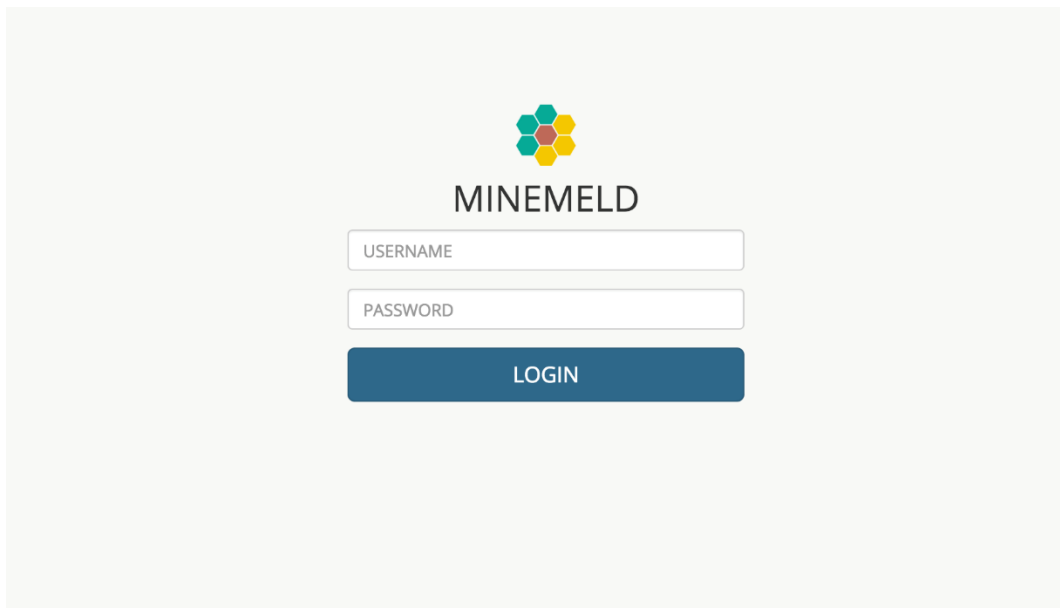
The Palo Alto Minemeld client application has been pre-installed to setup appropriate feeds

Check under Threat Intel on the web application menu .Login admin/minemeld if no auto login configured.

9.2 MINEMELD INTERFACE

From the SIEMonster main menu select Threat Intel.

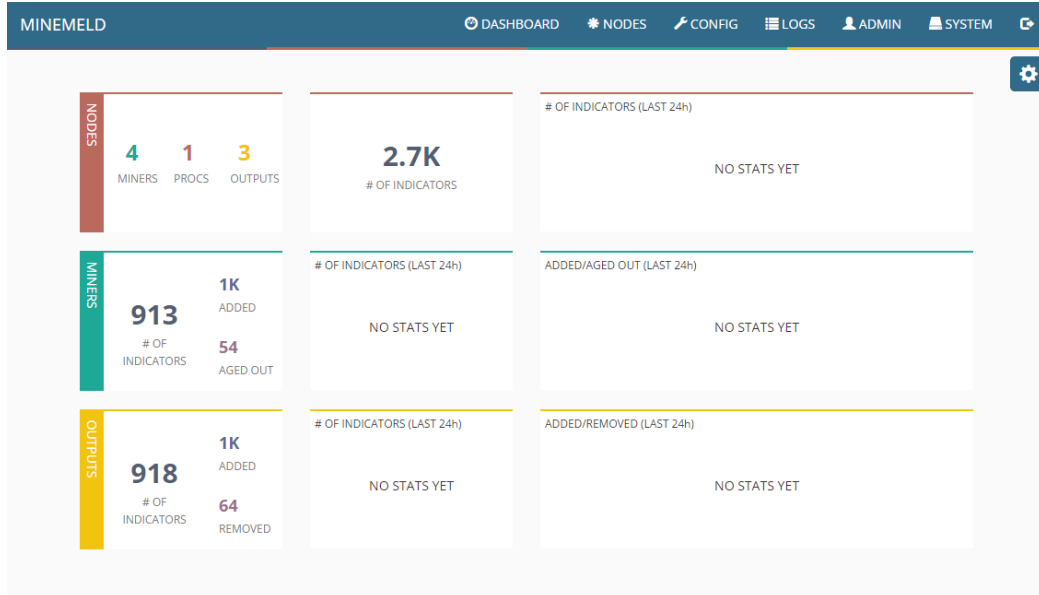
The default credentials for MineMeld are admin/minemeld.



The screenshot shows the login page for MINEMELD. At the top center is a logo consisting of six hexagons in teal, yellow, and orange. Below the logo is the text "MINEMELD". Underneath, there are two input fields: "USERNAME" and "PASSWORD". At the bottom of the form is a blue button labeled "LOGIN".

9.3 DASHBOARD

The dashboard is the main page displayed after login and is used to check the overall status of MineMeld.



- **First Row**, in the first row the number of nodes active per type, the current total numbers of indicators, and a graph of the total number of indicators over the last 24 hours.
- **Second Row**, The second row is for Miners, displaying the total number of indicators stored in the miner nodes, and the number of indicators added and aged out since MineMeld has been running. Charts on the right display number of indicators within the last out, and indicators added and aged out in the last hour.
- **Third Row**, The third row shows the same information as the second but for the Output nodes.

9.4 NODES

The Nodes page displays information and the status of all the nodes in the system.

Types of Nodes;

- **Miners**, responsible for periodically retrieving indicators from feeds, and pushing them to connected nodes with *Update* messages. They are also responsible for aging out indicators when they disappear from the original feed or when an indicator is considered dead, the Miner for that feed instructs the other nodes to remove the indicator via a *Withdraw* message.
- **Processor**, aggregates indicators received by multiple Miner nodes and forwards them to the appropriate output nodes.
- **Output**, receives indicators from the processor node and transforms them into a format that could be parsed to external entities.

MINEMELD DASHBOARD NODES CONFIG LOGS ADMIN SYSTEM

ADD INDICATOR

Show All entries Search:

NAME	TYPE	STATE	INDICATORS	ADD/REM/AO	UPDATES	WITHDRAWS
dshield_blocklist	MINER	STARTED	20	ADDED: 71 AGED OUT: 51	RX: 0 PROCESSED: 0 TX: 1076	RX: 0 PROCESSED: 0 TX: 51
spamhaus_DROP	MINER	STARTED	839	ADDED: 842 AGED OUT: 3	RX: 0 PROCESSED: 0 TX: 842	RX: 0 PROCESSED: 0 TX: 3
spamhaus_EDROP	MINER	STARTED	54	ADDED: 54 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 54	RX: 0 PROCESSED: 0 TX: 0
wlWhiteListIPv4	MINER	STARTED	0	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 0	RX: 0 PROCESSED: 0 TX: 0
inboundfeedhc	OUTPUT	STARTED	918	ADDED: 982 REMOVED: 64	RX: 1992 PROCESSED: 1992 TX: 0	RX: 64 PROCESSED: 64 TX: 0
inboundfeedlc	OUTPUT	STARTED	0	ADDED: 0 REMOVED: 0	RX: 1992 PROCESSED: 0 TX: 0	RX: 64 PROCESSED: 2056 TX: 0
inboundfeedmc	OUTPUT	STARTED	0	ADDED: 0 REMOVED: 0	RX: 1992 PROCESSED: 0 TX: 0	RX: 64 PROCESSED: 2056 TX: 0
inboundagggregator	PROCESSOR	STARTED	913	ADDED: 967 REMOVED: 54	RX: 1972 PROCESSED: 1972 TX: 1992	RX: 54 PROCESSED: 54 TX: 64

Showing 1 to 8 of 8 entries < 1 >

- **Name**, name of the node.
- **Position**, type of node eg, (Miner, Processor, Output).
- **State**, current functional state of the individual node.
- **Indicators**, number of indicators stored in node.
- **Add/Rem/AO**, Number of indicators added, Removed or Aged Out.
- **Updates**, Updates received, processed and transmitted.
- **Withdraws**, Withdraws received, processed and transmitted.

Clicking on one of the nodes displays a page with more information on that particular node.

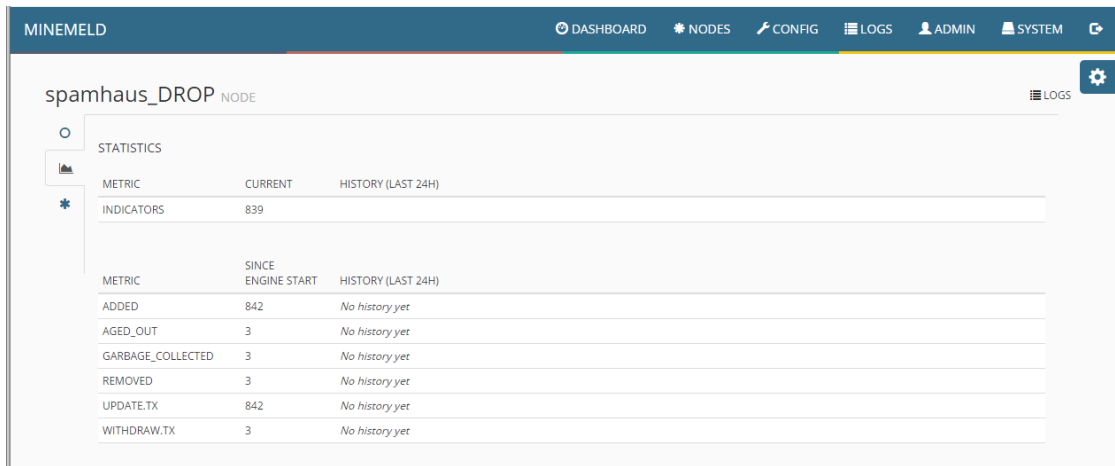
MINEMELD DASHBOARD NODES CONFIG LOGS ADMIN SYSTEM

spamhaus_DROP NODE LOGS

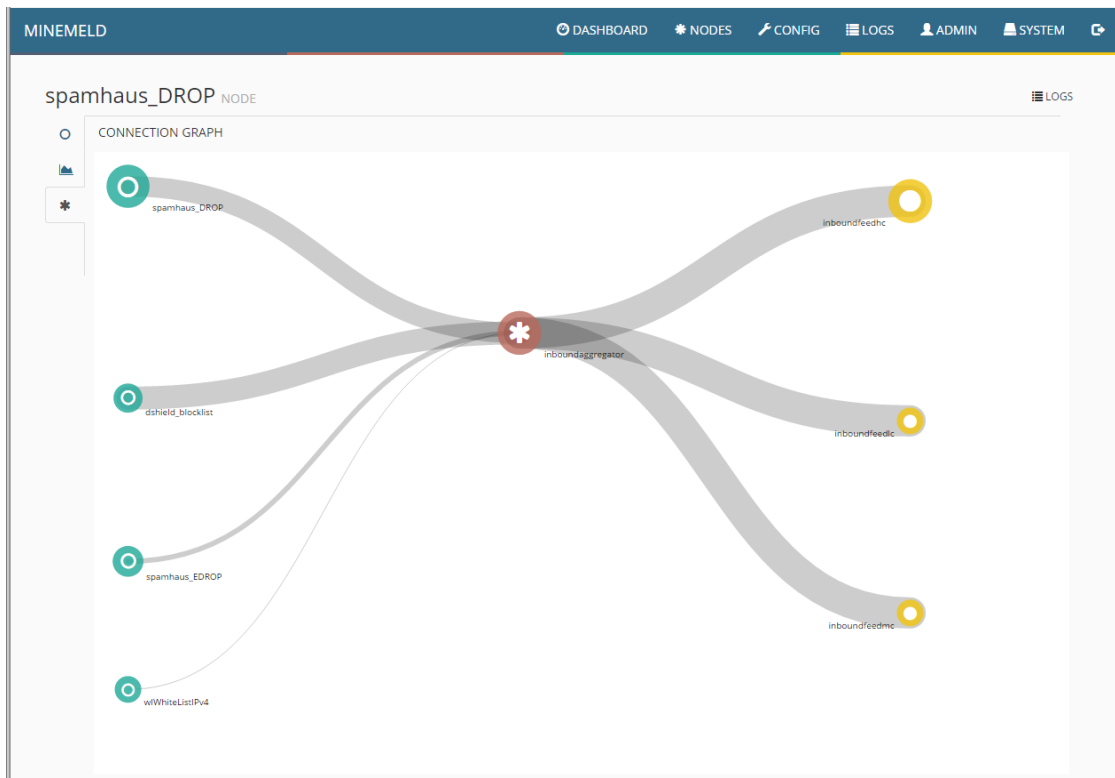
STATUS

CLASS	minemeld.ft.http.HttpFT	OUTPUT	ENABLED
STATE	STARTED	INPUTS	none
LAST RUN	2017-03-23 21:59:14 +1100 SUCCESS		
# INDICATORS	839		

Clicking through the tab menu on the left displays further statistics on that particular node.



The bottom tab displays a live diagram of how that node interconnects with the other nodes, and how each of the other nodes interconnects. This includes statistics of each connection between nodes.

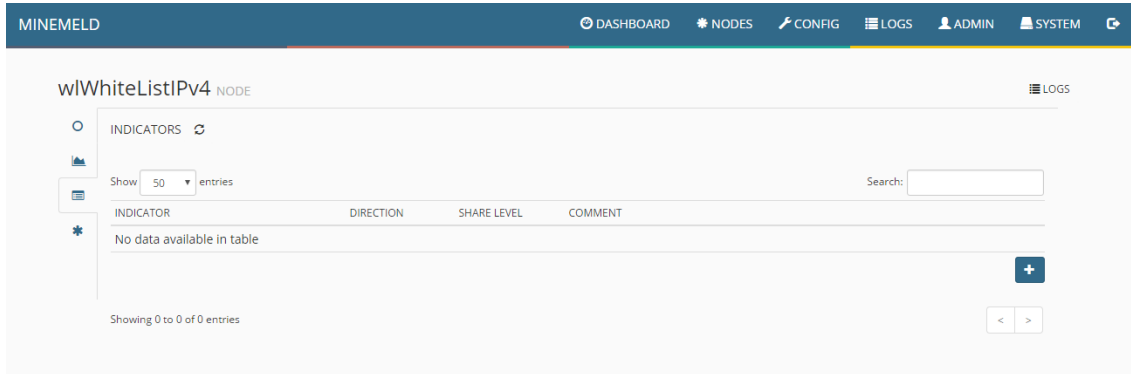


9.5 ADDING A WHITELIST/NODAL INDICATOR

1. Click on **wlWhiteListIPv4** miner node.

wlWhiteListIPv4	MINER	STARTED	0	ADDED: 1 AGED OUT: 1	RX: 0 PROCESSED: 0 TX: 1	RX: 0 PROCESSED: 0 TX: 1
-----------------	--------------	----------------	---	-------------------------	--------------------------------	--------------------------------

2. In the information page click on the indicators tab, and click on the add button in the bottom right of the page.



3. Add the **IP** of the whitelisted host, the **Direction**, which is in relation to traffic travelling out of and into the local network. **Share Level**, refers to the tag associated with that particular indicator and signifies the confidentiality of that indicator and also of the source that the indicator came from. Add details in the **Comment** section, and click OK.

ADD IPv4 INDICATOR

INDICATOR

DIRECTION ✕ ▼

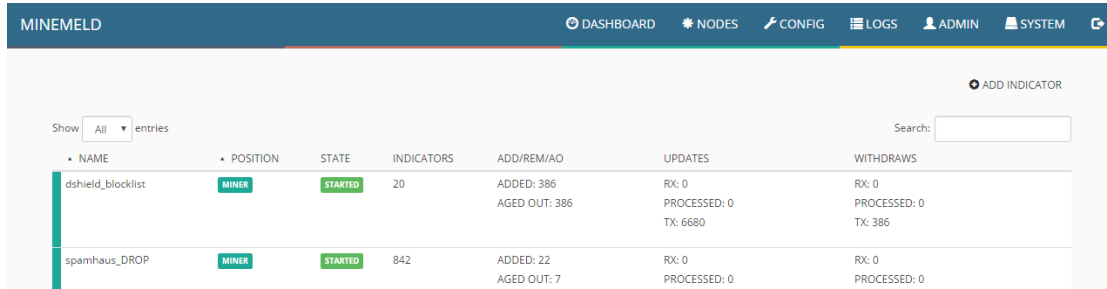
SHARE LEVEL RED

COMMENT

OK
CANCEL

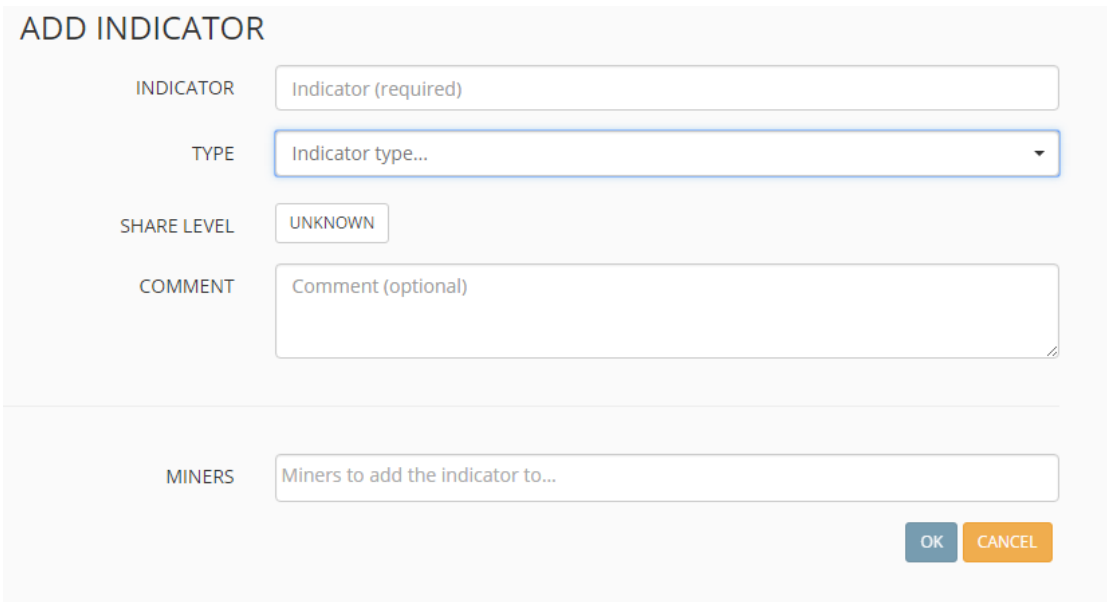
9.6 ADDING A GENERIC INDICATOR

1. From the Nodes page, click **Add Indicator**.



NAME	POSITION	STATE	INDICATORS	ADD/REM/AO	UPDATES	WITHDRAWS
dshield_blocklist	MINER	STARTED	20	ADDED: 386 AGED OUT: 386	RX: 0 PROCESSED: 0 TX: 6680	RX: 0 PROCESSED: 0 TX: 386
spamhaus_DROP	MINER	STARTED	842	ADDED: 22 AGED OUT: 7	RX: 0 PROCESSED: 0	RX: 0 PROCESSED: 0

2. Fill in indicator details, including the **indicator** itself, which could be an IP address, URL or a domain. The **Type**, eg. (IPv4, IPv6, URL, domain), the **Share Level**, which is the confidentiality of the indicator and possibly the source of the indicator.



ADD INDICATOR

INDICATOR:

TYPE:

SHARE LEVEL:

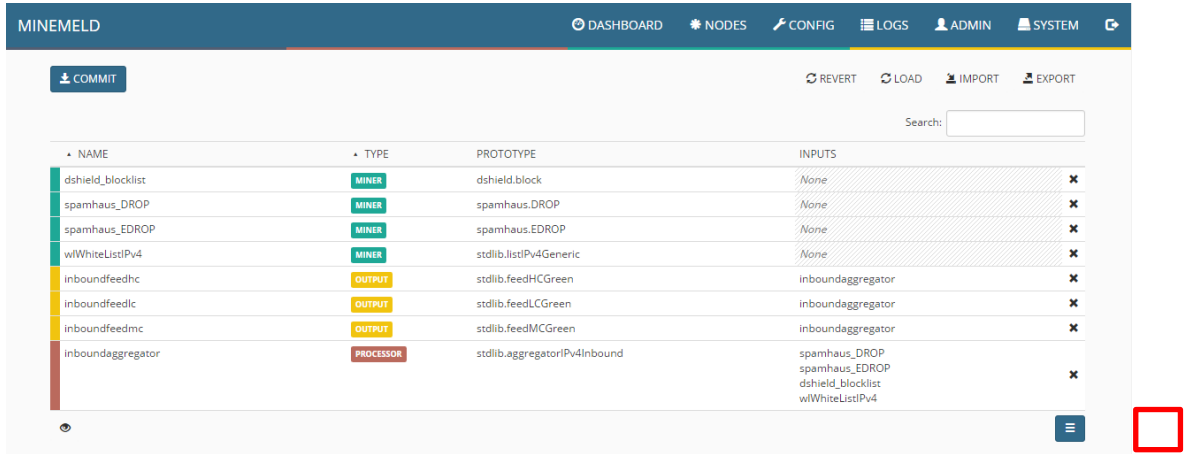
COMMENT:

MINERS:

3. Add a **Comment** to signify the description of the indicator, then select the **Miner** that the indicator will be allocated to. And click OK.

9.7 ADDING A NODE

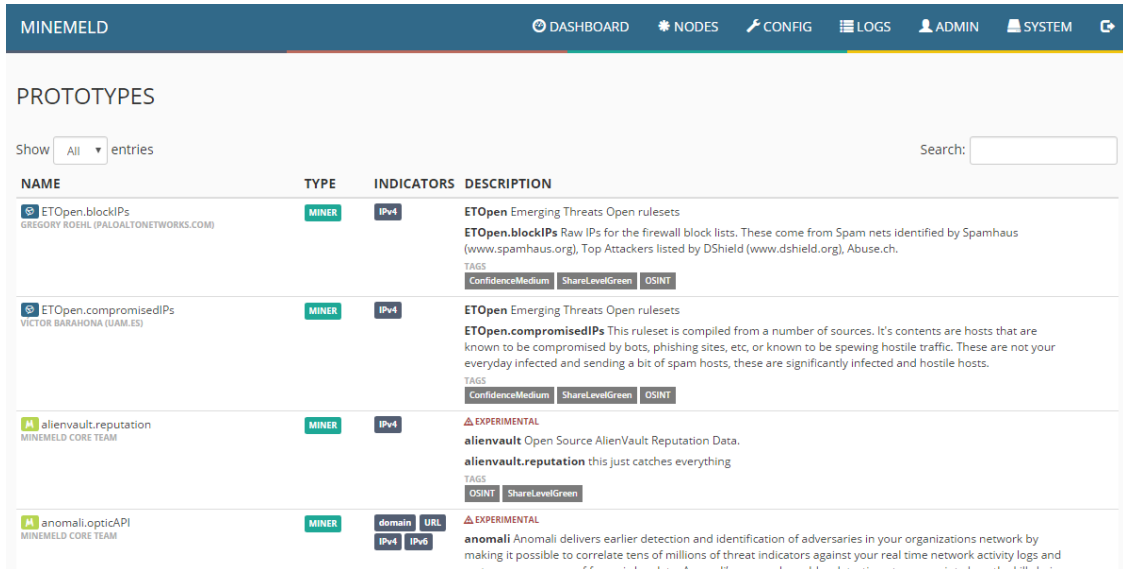
1. Go to the **Config** page, and click the button in the bottom right corner.



The screenshot shows the MINEMELD Config page. At the top, there are navigation tabs: DASHBOARD, NODES, CONFIG, LOGS, ADMIN, and SYSTEM. Below the navigation, there are buttons for COMMIT, REVERT, LOAD, IMPORT, and EXPORT. A search bar is present. The main content is a table with columns: NAME, TYPE, PROTOTYPE, and INPUTS. The table lists several node prototypes, including dshield_blocklist, spamhaus_DROP, spamhaus_EDROP, wlWhiteListIPv4, inboundfeedhc, inboundfeedlc, inboundfeedmc, and inboundagggregator. A red box highlights a button in the bottom right corner of the table area.

NAME	TYPE	PROTOTYPE	INPUTS
dshield_blocklist	MINER	dshield.block	None
spamhaus_DROP	MINER	spamhaus.DROP	None
spamhaus_EDROP	MINER	spamhaus.EDROP	None
wlWhiteListIPv4	MINER	stdlib.listIPv4Generic	None
inboundfeedhc	OUTPUT	stdlib.feedHCGreen	inboundagggregator
inboundfeedlc	OUTPUT	stdlib.feedLCGreen	inboundagggregator
inboundfeedmc	OUTPUT	stdlib.feedMCGreen	inboundagggregator
inboundagggregator	PROCESSOR	stdlib.aggregatorIPv4Inbound	spamhaus_DROP spamhaus_EDROP dshield_blocklist wlWhiteListIPv4

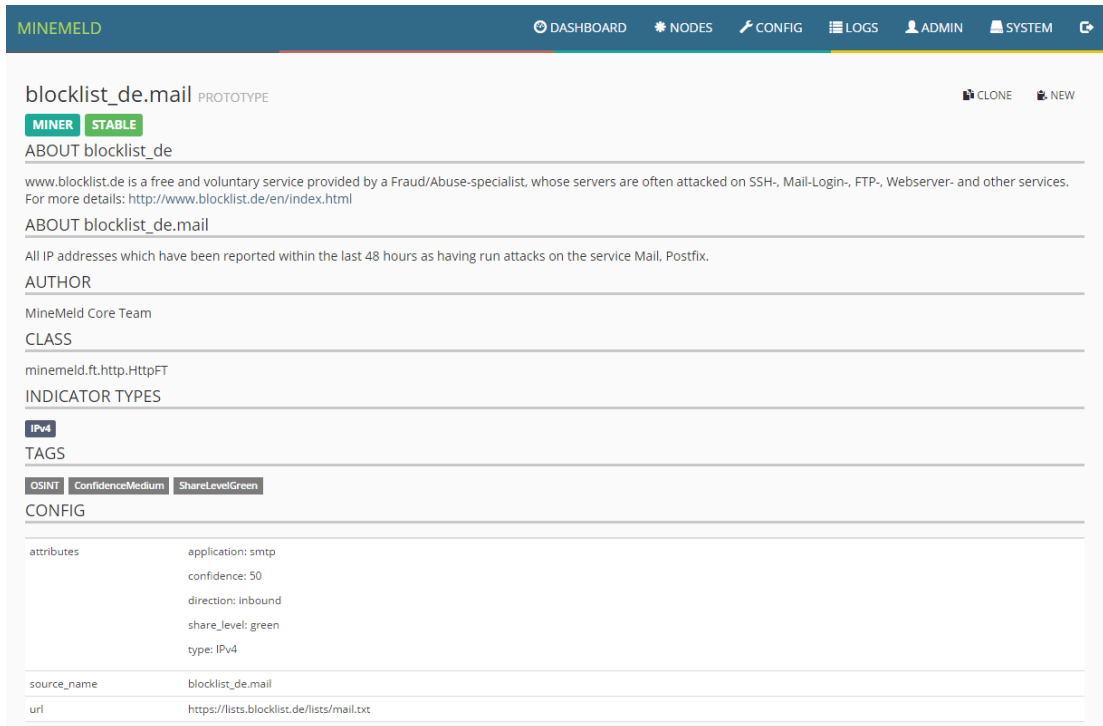
2. Listed below will be all the possible preset node prototypes that can be implemented.



The screenshot shows the MINEMELD Prototypes page. At the top, there are navigation tabs: DASHBOARD, NODES, CONFIG, LOGS, ADMIN, and SYSTEM. Below the navigation, there is a search bar and a dropdown menu to show all entries. The main content is a table with columns: NAME, TYPE, INDICATORS, and DESCRIPTION. The table lists several preset node prototypes, including ETOpen.blockIPs, ETOpen.compromisedIPs, alienvault.reputation, and anomali.opticAPI.

NAME	TYPE	INDICATORS	DESCRIPTION
ETOpen.blockIPs GREGORY ROEHL (PALOALTONETWORKS.COM)	MINER	IPv4	ETOpen Emerging Threats Open rulesets ETOpen.blockIPs Raw IPs for the firewall block lists. These come from Spam nets identified by Spamhaus (www.spamhaus.org), Top Attackers listed by DShield (www.dshield.org), Abuse.ch. TAGS: ConfidenceMedium, ShareLevelGreen, OSINT
ETOpen.compromisedIPs VICTOR BARAHONA (UAM.ES)	MINER	IPv4	ETOpen Emerging Threats Open rulesets ETOpen.compromisedIPs This ruleset is compiled from a number of sources. It's contents are hosts that are known to be compromised by bots, phishing sites, etc, or known to be spewing hostile traffic. These are not your everyday infected and sending a bit of spam hosts, these are significantly infected and hostile hosts. TAGS: ConfidenceMedium, ShareLevelGreen, OSINT
alienvault.reputation MINEMELD CORE TEAM	MINER	IPv4	EXPERIMENTAL alienvault Open Source AlienVault Reputation Data. alienvault.reputation this just catches everything TAGS: OSINT, ShareLevelGreen
anomali.opticAPI MINEMELD CORE TEAM	MINER	domain, URL, IPv4, IPv6	EXPERIMENTAL anomali Anomali delivers earlier detection and identification of adversaries in your organizations network by making it possible to correlate tens of millions of threat indicators against your real time network activity logs and up to a year or more of forensic log data. Anomali's approach enables detection at every point along the kill chain

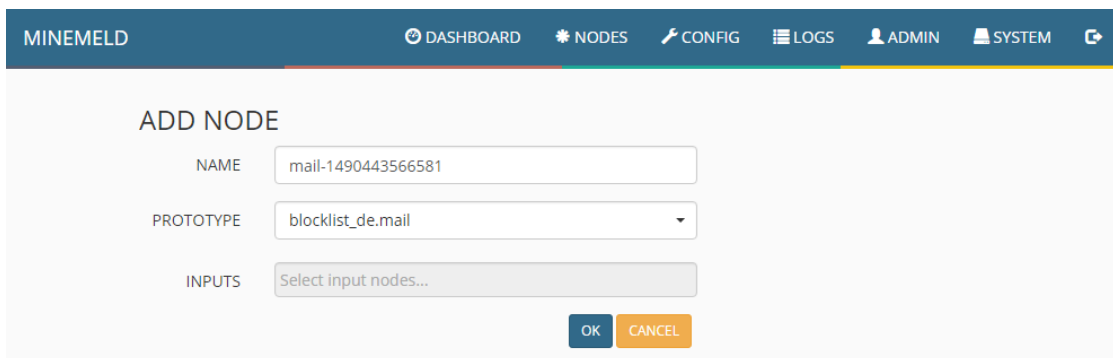
3. To add a new node, click a node in the list.



The screenshot shows the configuration page for a node named 'blocklist_de.mail' in the MINEMELD interface. The page includes a navigation bar with 'DASHBOARD', 'NODES', 'CONFIG', 'LOGS', 'ADMIN', and 'SYSTEM'. The main content area displays the node's details, including its status (MINER, STABLE), a description of the service, author information (MineMeld Core Team), and configuration attributes. The configuration table is as follows:

attributes	value
application	smtp
confidence	50
direction	inbound
share_level	green
type	IPv4
source_name	blocklist_de.mail
url	https://lists.blocklist.de/lists/mail.txt

4. Click **Clone**, then click OK.

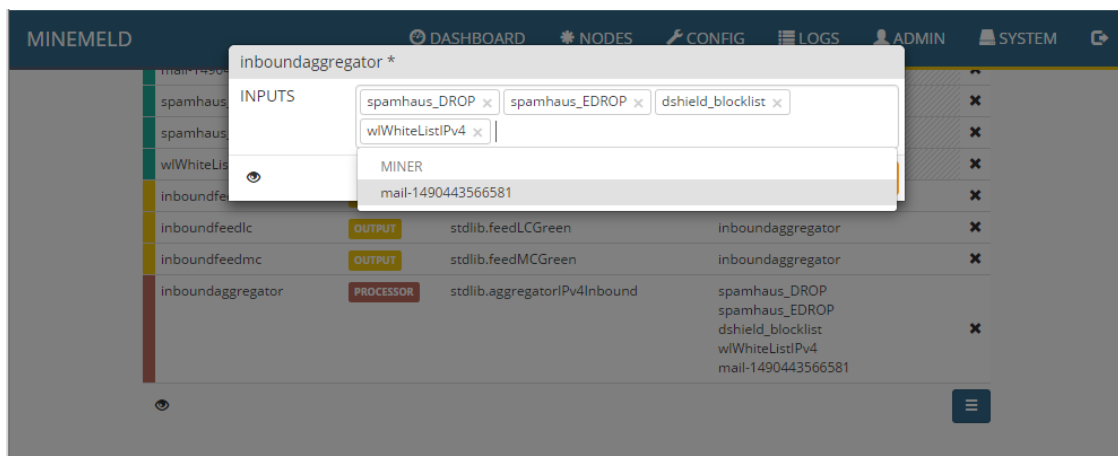


The screenshot shows the 'ADD NODE' form in the MINEMELD interface. The form has the following fields:

- NAME:** mail-1490443566581
- PROTOTYPE:** blocklist_de.mail
- INPUTS:** Select input nodes...

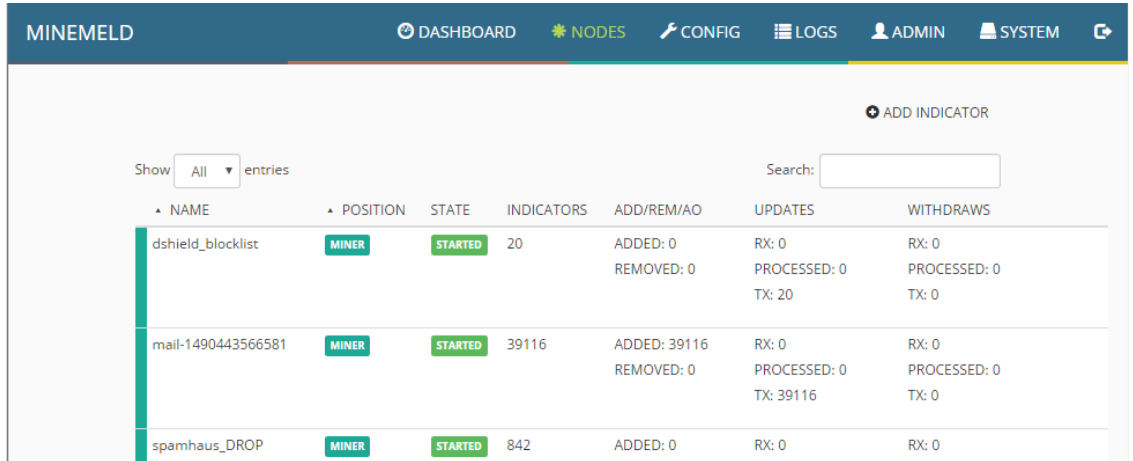
At the bottom of the form, there are 'OK' and 'CANCEL' buttons.

5. Click on the inputs area of the appropriate processor for the newly added node, then add the new node to the list of inputs.



The screenshot shows the 'inboundagggregator' processor configuration in the MINEMELD interface. The processor is currently set to 'MINER' and has the name 'mail-1490443566581'. The 'INPUTS' section is open, showing a list of selected input nodes: spamhaus_DROP, spamhaus_EDROP, dshield_blocklist, and wiWhiteListIPv4. The processor is currently connected to 'stdlib.feedLCGreen' and 'stdlib.feedMCGreen' as output nodes, and 'stdlib.agggregatorIPv4Inbound' as a processor node. The output nodes are connected to 'inboundagggregator'.

- Click **Commit** and wait for the system to refresh.
- Go to the Nodes page to view the statistics of the new node.



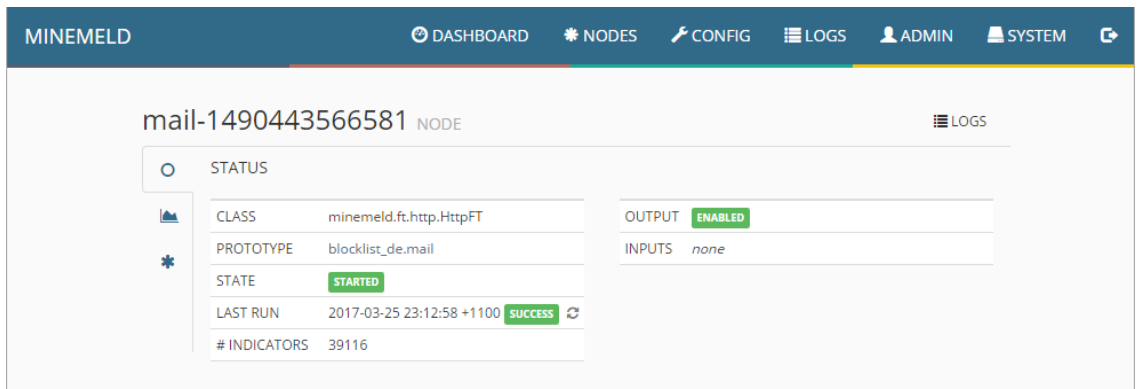
MINEMELD DASHBOARD NODES CONFIG LOGS ADMIN SYSTEM

ADD INDICATOR

Show All entries Search:

NAME	POSITION	STATE	INDICATORS	ADD/REM/AO	UPDATES	WITHDRAWS
dshield_blocklist	MINER	STARTED	20	ADDED: 0 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 20	RX: 0 PROCESSED: 0 TX: 0
mail-1490443566581	MINER	STARTED	39116	ADDED: 39116 REMOVED: 0	RX: 0 PROCESSED: 0 TX: 39116	RX: 0 PROCESSED: 0 TX: 0
spamhaus_DROP	MINER	STARTED	842	ADDED: 0	RX: 0	RX: 0

- Click the node to view extended information and the full connectivity map including the new node.

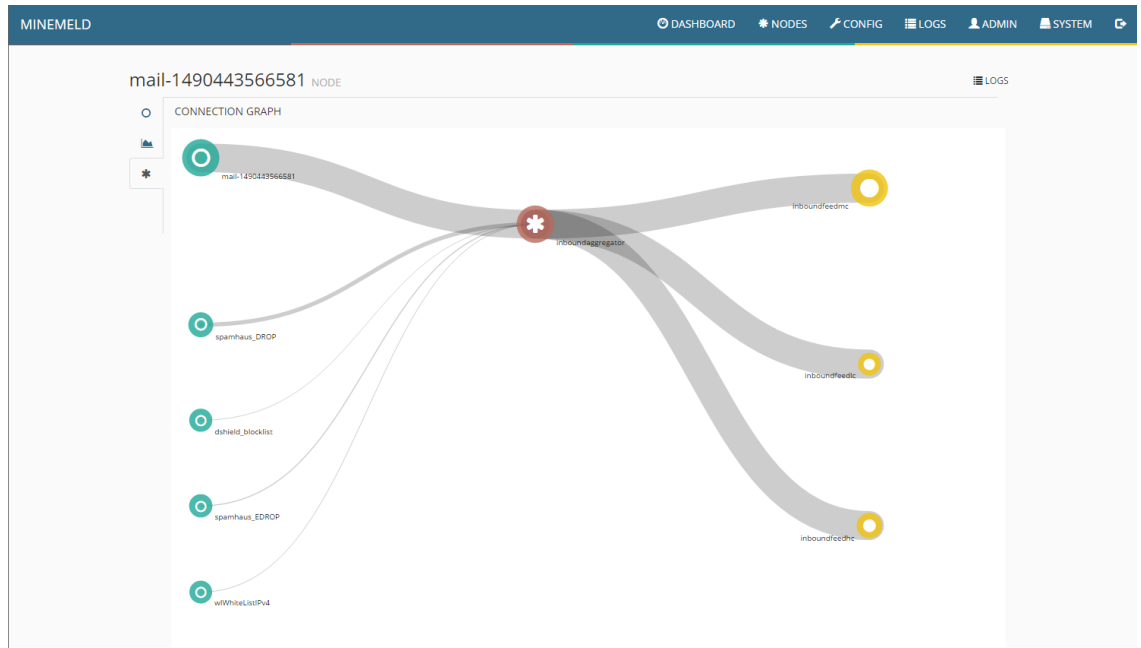


MINEMELD DASHBOARD NODES CONFIG LOGS ADMIN SYSTEM

mail-1490443566581 NODE LOGS

STATUS

CLASS	minemeld.ft.http.HttpFT	OUTPUT	ENABLED
PROTOTYPE	blocklist_de.mail	INPUTS	none
STATE	STARTED		
LAST RUN	2017-03-25 23:12:58 +1100 SUCCESS		
# INDICATORS	39116		



9.8 SUPPORTED NODES

Below is a non-exhaustive list of supported nodes in MineMeld.

9.9 MINERS

OSINT

- AlienVault Reputation
- Bambenekconsulting
- DShield
- Emerging Threats Open rulesets
- badips.com
- Binary Defense Systems Artillery
- blocklist.de
- BruteForceBlocker
- hailataxii.com
- Malware Domain List
- OpenBL
- OpenPhish
- Ransomware Tracker
- sslbl.abuse.ch
- Virbl
- ZeuS Tracker
- Feodo Tracker

Commercial

- Anomali
- Palo Alto Networks AutoFocus
- PhishMe
- Proofpoint ET Intelligence
- Recorded Future
- Soltra
- Spamhaus Project
- The Media Trust
- ThreatQ
- Virustotal Private API

Organizations

- AUS-CERT

Cloud services

- AWS Public IPs
- Microsoft Azure Public IPs
- Google NetBlocks
- Google GCE NetBlocks
- Microsoft Office365 IPs and URLs

Threat Intelligence Platforms

- CIF

Various

- Tor Exit Nodes
- PAN-OS Syslog messages
- Cisco ISE
- Youtube Channel (as external extension)

Processors

- IPv4 Aggregator
- IPv6 Aggregator
- Generic Aggregator
- Syslog Matcher for PAN-OS syslog messages

Outputs

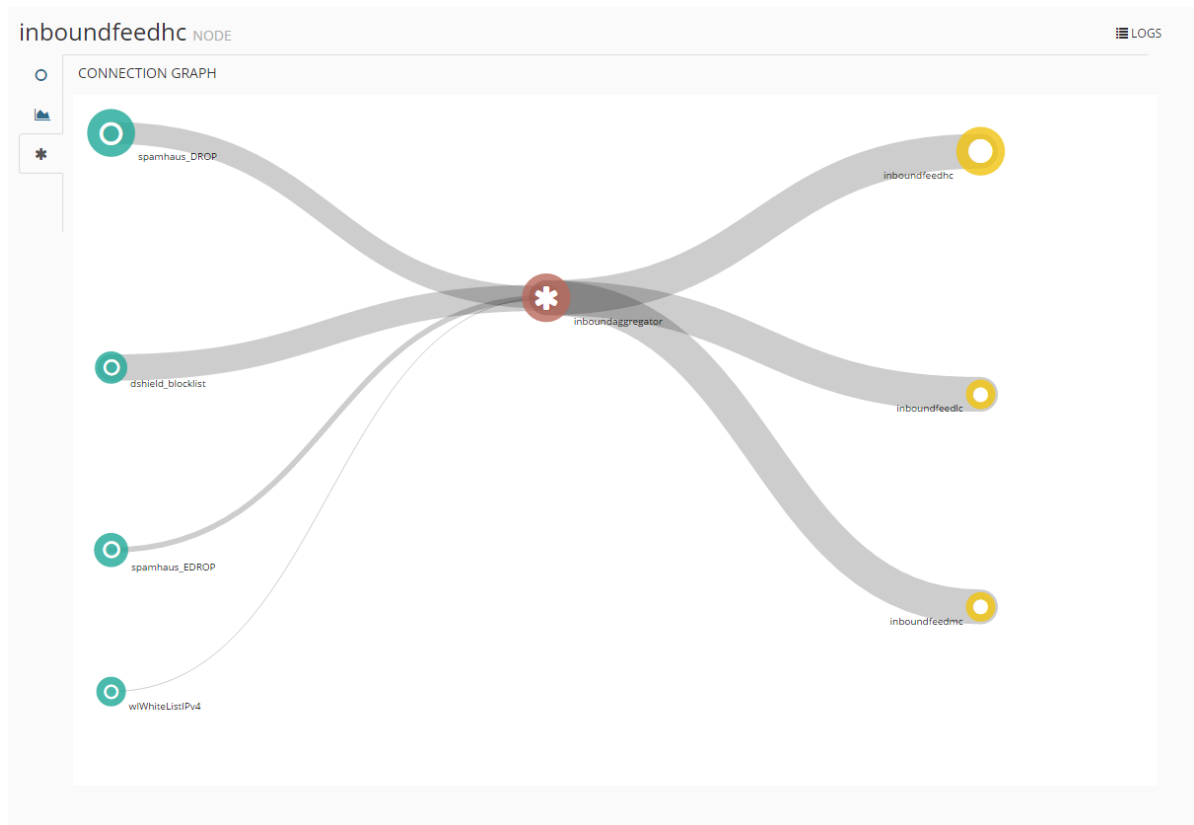
- JSON
- JSON-SEQ
- STIX/TAXII
- PAN-OS EDL
- PAN-OS DAG API
- Elastic Logstash
- Arcsight CEF (as external extension)

10 ACTIVE THREAT DETECTION PFSENSE/APACHE

SIEMonster, through the method of live MineMeld output feeds and customized configuration of Logstash, is able to perform active threat detection. This works by taking logs from PfSense and/or Apache and matching the IP addresses from source, destination (PfSense) and client (apache) data fields being input into Elastic, and then matches them with any malicious addresses found by the live MineMeld threat intelligence feed.

10.1 MINEMELD

Set up the threat feed miners to get the list of malicious IP ranges. Then output them to the IPv4 aggregator node, which then outputs to the **inboundfeedhc**, **mc**, **lc** nodes, indicating the level severity.



10.2 LOGSTASH

Within the Logstash-Indexer configuration files is an OSINT filter which gathers key fields from existing indices and creates a new index named 'osint-DATE'. As a default, this extracts key data from Wazuh/Ossec and Windows event log data, but can easily be extended for other indices using the 90-osint-filter.conf as a template. Having key data from multiple endpoints such as firewalls, VPN devices, Active Directory in a single index allows for easy threat intel correlation in a single index. The OSINT index has a field 'threatnet' added which is assigned different values depending on risk level. The OSINT index is activated by adding as a new index in Management – Index Patterns once there is sufficient incoming data to extract from:

Configure an index pattern

In order to use Kibana you must configure at least one index pattern. Index patterns are also used to configure fields.

Index name or pattern

Patterns allow you to define dynamic index names using * as a wildcard. Example: logstash-*

Time Filter field name ? refresh fields

 Expand index pattern when searching [DEPRECATED]

With this option selected, searches against any time-based index pattern that contains a wildcard selected time range.

Searching against the index pattern /logstash-* will actually query Elasticsearch for the specific time range. With recent changes to Elasticsearch, this option should no longer be necessary and will likely be removed.

 Use event times to create index names [DEPRECATED]

SSH/shell exec to the Logstash-Indexer container on proteus, in the /run/miscellaneous directory the updatefeed.sh script required to maintain an up to date threat intelligence feed integrated into the logstash configuration.

In this script shown below, the latest output feed node is retrieved using wget, from the **inboundfeedhc** output node, note that the **?tr=1** expression at the end of the feed URL, which converts the IPv4 list into CIDR format. This threat feed URL is interchangeable with any other output node.

The following lines after implement the latest list of malicious IPs into the logstash configuration OSINT filter

```

firoot@siemonster-project-vagrant-logstash-indexer-1:/run/miscellaneous# cat updatefeed.sh
#!/bin/bash
# Copyright SIEMonster 2017
# Maintained by jim@siemonster.com
# Dynamic Logstash intel feed insertion
cd /tmp
cp /etc/logstash/conf.d/90-osint-filter.conf .
wget -O minemeldsource http://minemeld/feeds/inboundfeedhc?tr=1
if [ ! -s minemeldsource ]
then
    exit 1
else
    # Convert list to comma delimited
    awk -vORS=, '{ print "\""$0"\"" }' minemeldsource | sed 's/,,$/\n/' > cidrs.txt
    read feedupdate < cidrs.txt
    # Insert update
    sed -i "/^\\s*network/ s/[\\.\\*]\\|\\[${feedupdate}\\]|g" 90-osint-filter.conf
    rsync -vh 90-osint-filter.conf /etc/logstash/conf.d/90-osint-filter.conf

```

In the following file, **90-osint-filter.conf**, the tag **minemeld_trigger** is added to any incoming log entries that contain the source and/or destination field IP addresses that correlate with any of the IP address ranges in the **network** list. In this case the threatnet field value is assigned the value 'minemeld_correlation'.

```

cidr {
  add_tag => [ "minemeld_trigger", "tor-exit-node" ]
  address => [ "%{client_ip}", "%{dest_ip}" ]
  network => [ "109.248.9.0/24", "141.212.122.0/24", "181.214.87.0/24", "191.101.168.62.0/24", "5.188.86.0/24", "77.72.82.0/24", "80.82.77.0/24", "85.93.20.0/24", "93.174.120.128.0/18", "120.128.192.0/18", "120.129.0.0/17", "120.129.128.0/17", "120.130.120.64.0.0/16", "120.67.0.0/16", "149.109.0.0/21", "152.136.0.0/21", "153.85.0.0/16", "188.247.232.0/24", "196.196.8.0/22", "203.119.116.0/22", "208.12.64.0/19", "208.12.64.0/22", "24.233.0.0/21", "27.112.32.0/19", "37.9.53.0/24", "41.138.164.0/22", "41.138.168.0/22", "41.71.171.0/24", "41.71.176.0/23", "41.71.178.0/24", "41.71.184.0/22", "41.71.188.0/23", "43.57.0.0/16", "46.8.255.0/24", "58.2.0.0/17", "62.112.16.0/21", "81.94.43.0/24", "85.93.212.217.0/24", "211.154.137.0/24", "45.55.7.0/24", "93.115.26.0/24", "95.215.60.0/24" ]
}

if "minemeld_trigger" in [tags] {
  mutate {
    replace => { "threatnet" => "minemeld_correlation" }
    replace => { "risk_level" => "security" }
  }
}

```

These triggers are also used in the Logstash-Indexer 999-outputs.conf file to send live updates to the Event Viewer:

```

} else if [type] == "osint" {
  elasticsearch {
    index => "osint-%{+YYYY.MM.dd}"
    hosts => ["${ELASTICSEARCH_HOST}:9200"]
    user => "logstash"
    password => "${LOGSTASH_PWD}"
    ssl => true
    ssl_certificate_verification => false
    truststore => "/usr/share/elasticsearch/config/searchguard/ssl/truststore.jks"
    truststore_password => "${TS_PWD}"
  }
  if [threatnet] == "minemeld_correlation" {
    exec {
      command => "/usr/bin/alerta --endpoint-url http://alerta/api send -r %{hostname} -t '%{event_description}' -T '%{tags}' -v OSINT-MINEMELD"
    }
  } else {
    exec {
      command => "/usr/bin/alerta --endpoint-url http://alerta/api send -r %{hostname} -t '%{event_description}' -T '%{tags}' -v OSINT"
    }
  }
}

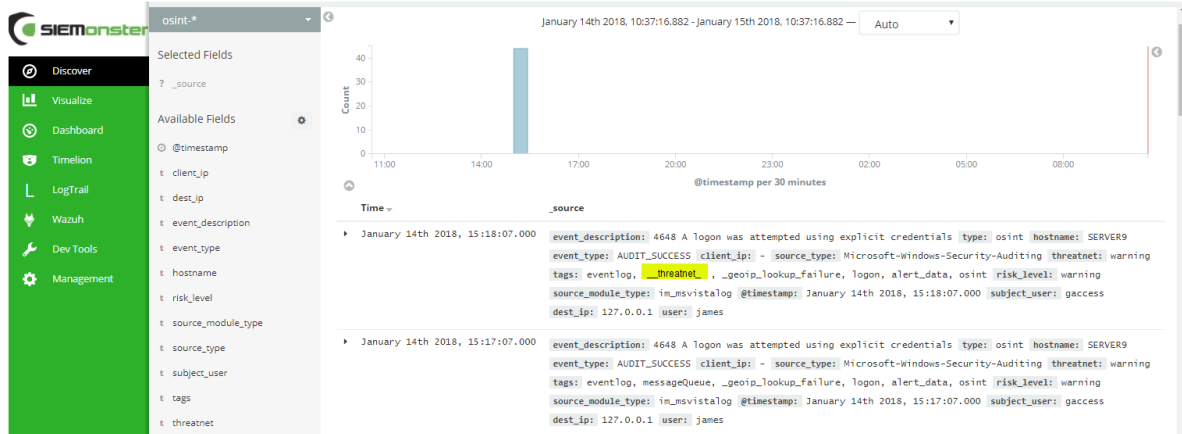
```

Warning	Open	Thu 11 Jan 09:53	39	Production	PowerShell	blackbeard.ocean.local	Alert	OSINT	4624 An account was successfully logged on
Minor	Open	Fri 12 Jan 12:05	0	Production	HIDS	Ku	Alert	OSINT	Maximum authentication attempts exceeded.
Warning	Open	Fri 12 Jan 12:21	6	Production	HIDS	NYC	Alert	OSINT	Web server 503 error code (Service unavailable).
Informational	Open	Fri 12 Jan 12:24	5	Production	firewall	vm27 al	Alert	OSINT	Blocked access to port 9000

10.3 ELASTIC SEARCH/KIBANA

In the Elastic/Kibana view, the “**threatnet**” tags can be seen added to entries with malicious IP addresses associated with them.

The following is of the **osint** logs index.



Note the **threatnet** tag in each view, which can be searched for in the search bar.

10.4 SYSMON/WINDOWS EXE DETECTION

System Monitor (Sysmon) is a Windows system service and device driver that, once installed on a system, remains resident across system reboots to monitor and log system activity to the Windows event log. It provides detailed information about process creations, network connections, and changes to file creation time.

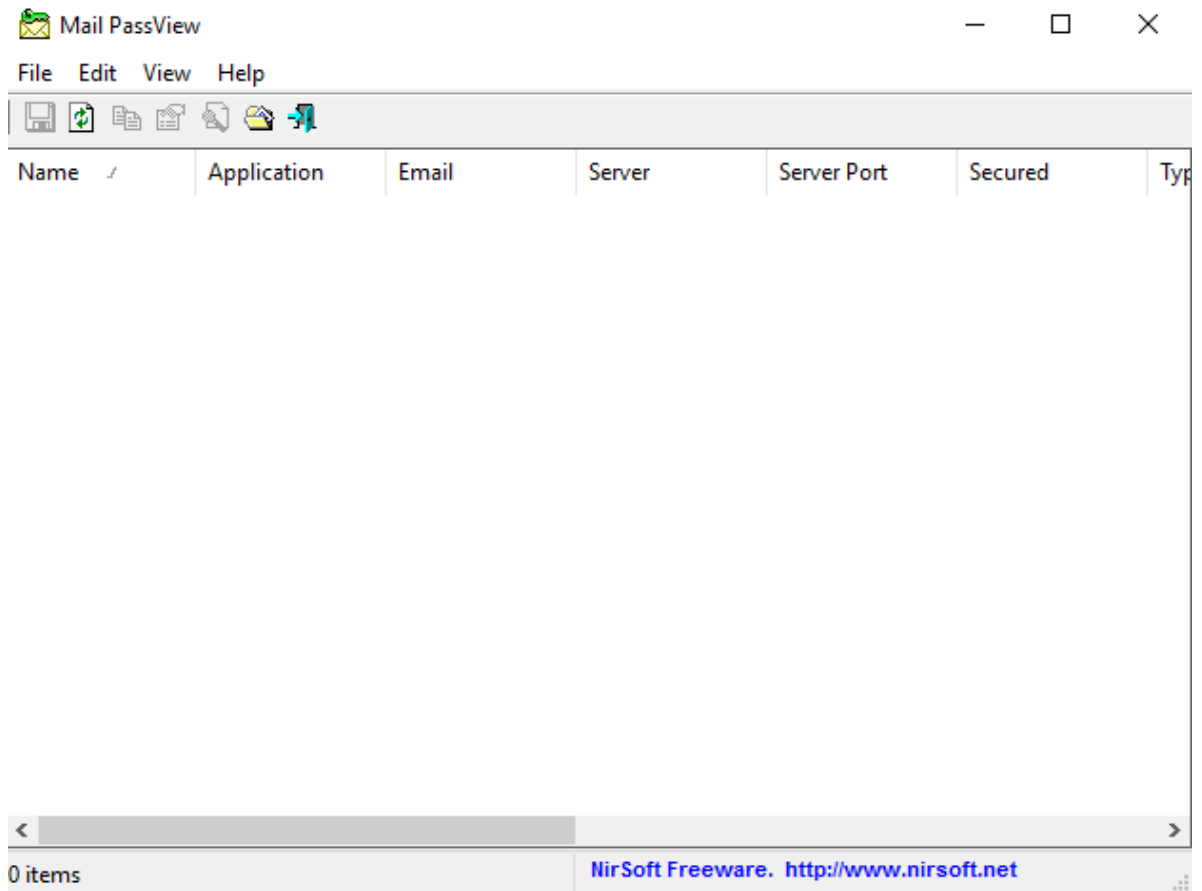
Sysmon is integrated with SIEMonster using the following steps.

1. Download, Extract and install Sysmon, install with the command **sysmon64 -accepteula -l**, link to download page: <https://technet.microsoft.com/en-us/sysinternals/sysmon>.
2. Add the following to the NXLog Input configuration, for detailed instructions on NXLog implementation refer to section 4.1,

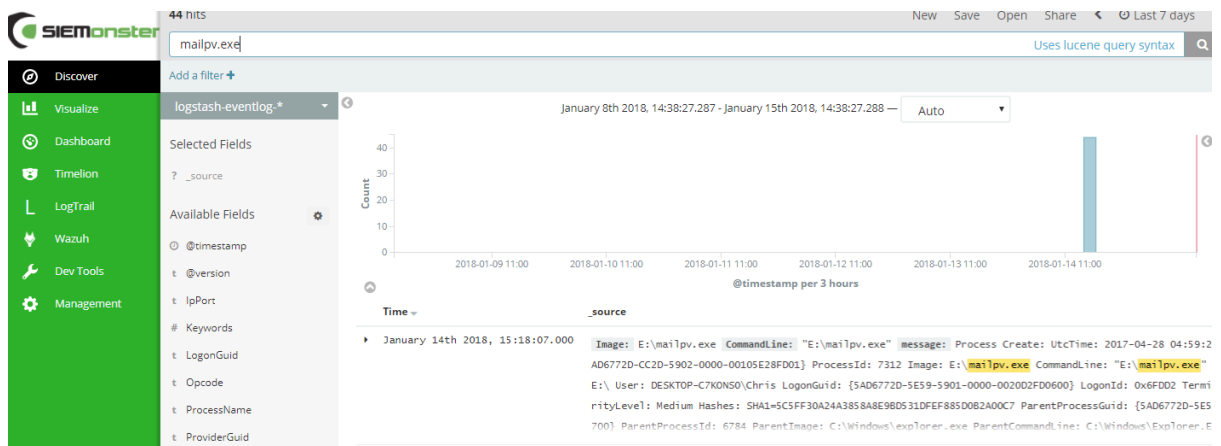
```
<Select Path="Windows PowerShell">*</Select>\
<Select Path="Microsoft-Windows-Sysmon/Operational">*</Select>\</Query>\
```

3. Check Elasticsearch/kibana on index logstash-win-* that the new logs are being input into SIEMonster.
4. Malicious executables being run on end hosts can now be searched for in Elasticsearch, for example.

Mail PassView a program end users may not be allowed to run in written security policy.



This executable can be searched for just by using "mailpv.exe" as the criteria.



11 HIDS

11.1 RULESETS

Wazuh/OSSEC rulesets can be updated manually, but running on a weekly schedule via a cronjob is recommended.

To perform a manual update, issue the following command within the Wazuh container on the Proteus appliance:

- `/var/ossec/bin/update_ruleset.py -s`

> Shell: siemonster-project-vagrant-wazuh-1

```
[root@wazuh-manager /]# /var/ossec/bin/update_ruleset.py -r
### Wazuh ruleset ###
-
Creating a backup for folders '/var/ossec/etc' and '/var/ossec/rules'.
Backup folder: /var/ossec/update/ruleset/backups/20170207_002
[Done]

Checking directory structure.
[Done]

Downloading new ruleset.
[Done]

Checking new ruleset.
[Done]

Cleaning directory.
[Done]

*Your ruleset is up to date.*
```

Automatic updates are performed weekly inside the Docker container.

11.2 MANAGEMENT

Wazuh/OSSEC management is handled by the `ossec-control` feature: `/var/ossec/bin/ossec-control`

Usage: `/var/ossec/bin/ossec-control {start|stop|restart|status|enable|disable}`

```
root@siemonster-project-siemonster-ossec-1:/# /var/ossec/bin/ossec-control statu
s
ossec-monitor is running...
ossec-logcollector is running...
ossec-remoted is running...
ossec-syscheckd is running...
ossec-analysisd is running...
ossec-maild not running...
ossec-execd is running...
root@siemonster-project-siemonster-ossec-1:/#
```

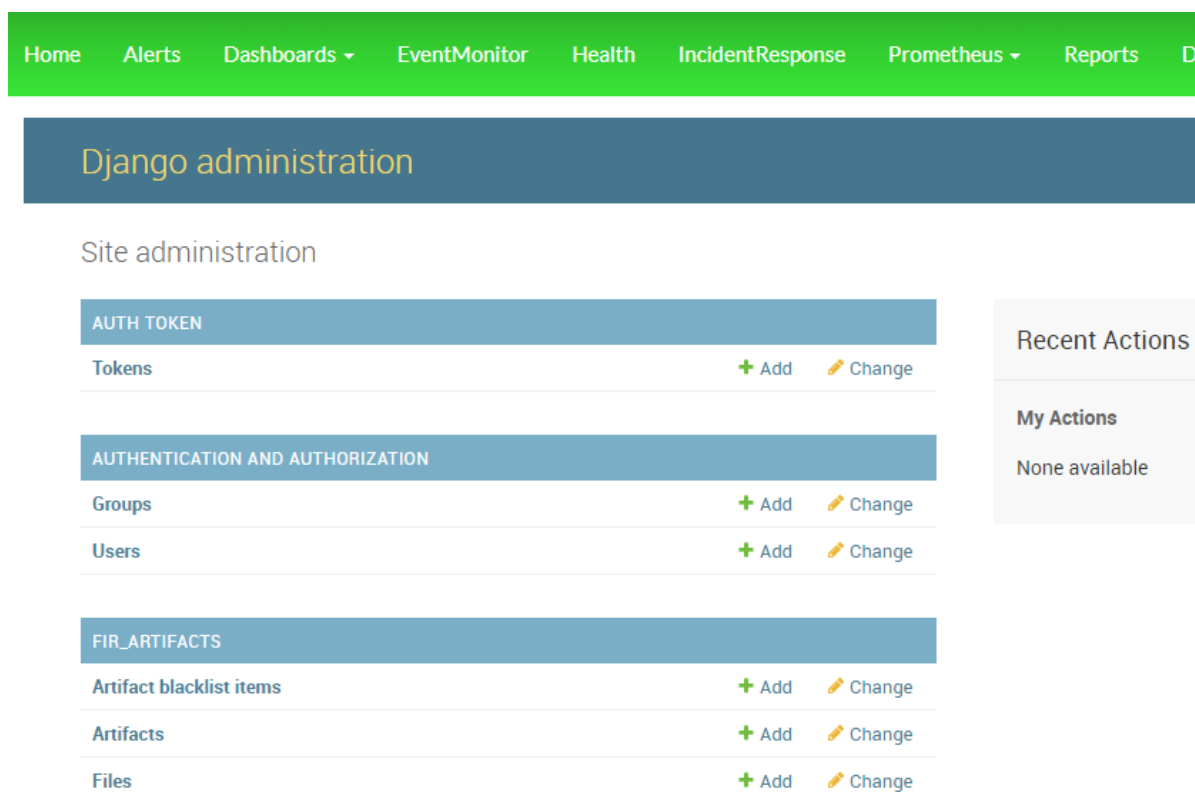
Close

12 INCIDENT RESPONSE

FIR (Fast Incident Response) is a cybersecurity incident management platform designed with agility and speed in mind. It allows for easy creation, tracking, and reporting of cybersecurity incidents. For those companies that do not have Incident Response Software or ticketing system, this is an ideal system. For those that do this feature can be turned off. However, consider using this tool for its automated ticketing of alerts and forwarders into your existing ticketing system.

12.1 ADMINISTRATION

From the main menu – Incident Response drop down menu - IR Admin (default login admin/admin)



The screenshot shows the Django administration interface. The top navigation bar is green and contains the following items: Home, Alerts, Dashboards, EventMonitor, Health, IncidentResponse, Prometheus, and Reports. Below the navigation bar is a dark blue header with the text 'Django administration'. The main content area is titled 'Site administration' and contains three sections:

- AUTH TOKEN**: Tokens (Add, Change)
- AUTHENTICATION AND AUTHORIZATION**: Groups (Add, Change), Users (Add, Change)
- FIR_ARTIFACTS**: Artifact blacklist items (Add, Change), Artifacts (Add, Change), Files (Add, Change)

On the right side, there is a sidebar with 'Recent Actions' and 'My Actions' (None available).

Once you're logged in

- Click on the Add button in the Users row. Fill-in the fields and click on save. On the next screen, go to the Groups section, click on "incident handlers", and on the arrow to add it to the column "Chosen groups". Click on Save at the bottom of the screen.

A standard user 'dev' has already been created with a password of 'dev'.

Next, you need to add a profile to the user. Still logged in as the super-user,

- Click on "Add" in the "Profiles" row of the admin panel. Select the created user and chose the number of incidents they will see in their view. Click "Save", and log out.

Creating labels: (Sample labels have already been created).

Labels are used to populate choices in some incident fields:

Detection source

Actions taken

Actor

Plan

FIR uses these "label groups" to know how where to map the labels.

The four mandatory label groups are detection, action, actor, and plan. You can add these through the admin interface in the "Label groups" section.

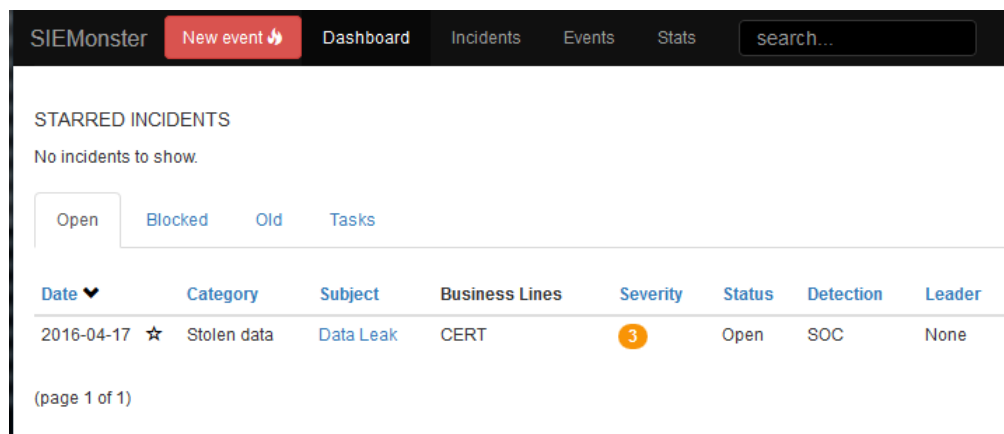
You should then specify options for each of the labels. Remember that an incident has a mandatory detection field, and comments have a mandatory action field; You'll need to populate at least those two.

12.2 USAGE

New Event:

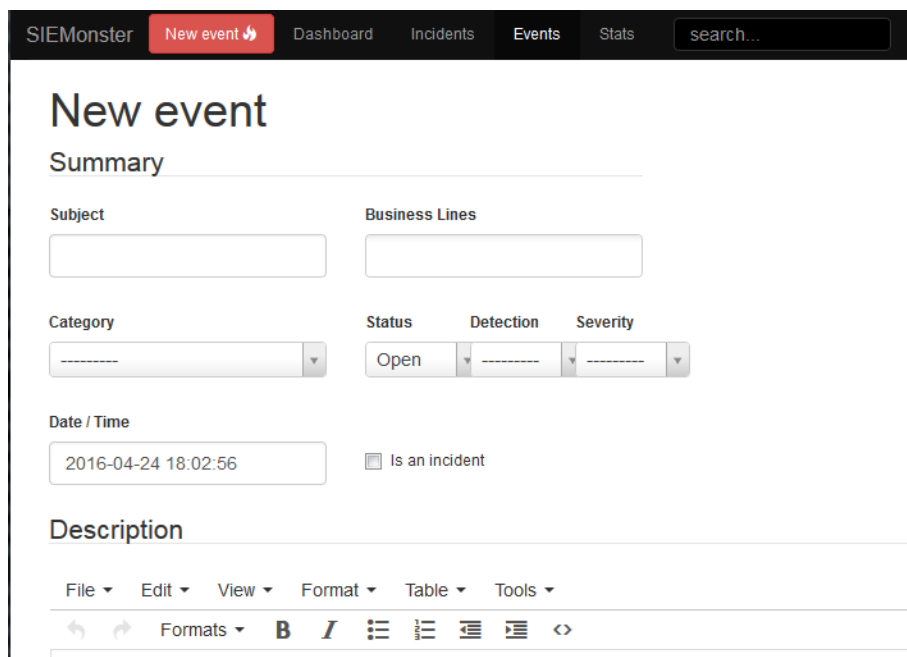
Login as a standard user, you can start off with user 'dev', password 'dev'.

Click on the New event button to go to the event creation form:



The screenshot shows the SIEMonster dashboard. At the top, there is a navigation bar with the SIEMonster logo, a 'New event' button with a flame icon, and links for 'Dashboard', 'Incidents', 'Events', and 'Stats'. A search bar is also present. Below the navigation bar, the 'STARRED INCIDENTS' section is displayed, indicating 'No incidents to show.' There are four tabs: 'Open', 'Blocked', 'Old', and 'Tasks'. Below the tabs is a table with the following columns: Date, Category, Subject, Business Lines, Severity, Status, Detection, and Leader. The table contains one row of data: 2016-04-17, Stolen data, Data Leak, CERT, 3 (in a yellow circle), Open, SOC, and None. At the bottom of the table, it says '(page 1 of 1)'.

FIR New event creation



FIR Events

Here is the description of the available fields:

Subject: short description of your incident. The one that will appear on event tables.

Business Lines: entities concerned by this incident. You choose what you make of business lines: internal department, customers, etc.

Category: category of the incident (ex: phishing, malware). Categories are also customizable in the admin panel.

Status: can take three values: Open, Closed and Blocked. These are all labels defined in the admin panel

Detection: how the incident was detected. Default values: CERT, External. These values can be changed in the admin panel in the labels section

Severity: from 1 to 4.

Date / Time: date and time of the incident

Is an incident: differentiates between an event and an incident

Description: free-form text describing the event

When you are dealing with an incident, the following additional fields are available. These fields are only used for display and statistics:

Actor: who is the leader on this incident management? Default values are CERT and Entity

Plan: what is the named remediation plan used?

Confidentiality: from C0 to C3

Click on Save, and you will be redirected to the incident details page.

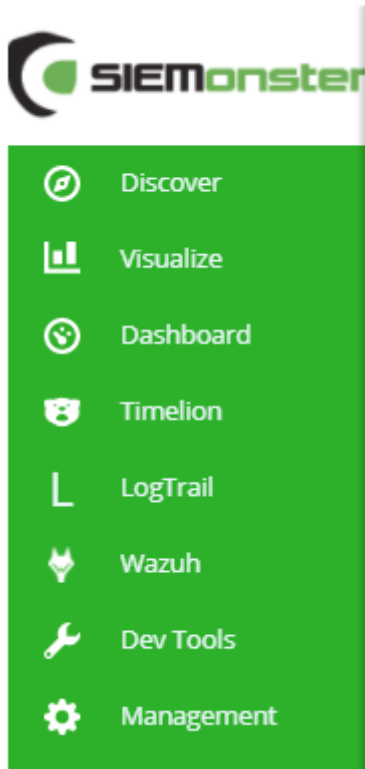
13 THE HOW TO OF SIEMONSTER DASHBOARDS

13.1 INTRODUCTION

The SIEMonster Kibana Dashboards give you full flexibility and functionality on how you want your dashboards to appear for different users. This chapter gives you a good guide on how to use the dashboards and customize them to your own organization.

13.2 OVERVIEW

At the top of the SIEMonster Dashboard page, Kibana shows the main navigation, which will give you access to the 4 main pages in Kibana: Discover, Visualize, Dashboard and Management.



Discover

The discover page displays all documents from a selected timespan (if the index contains time-based events) in a table. If you index doesn't contain time based data, it will just list all data.

Visualize

In Kibana 5 a visualization is a graph, map, table or other visualization of a special aspect of your data. On this tab, you will create or modify your visualizations. It's where most of the "producer" action happens in Kibana.

Dashboard

Several visualizations can be placed on one dashboard. A dashboard is not restricted to one index but can contain visualizations of any indexes you wish. This is mostly what "consumers" of Kibana will use, to look at all the visualizations that you created.

Management

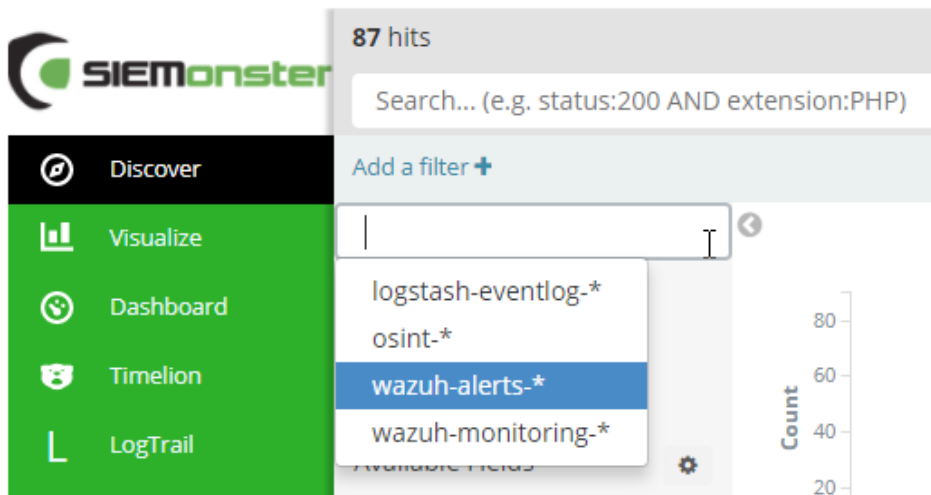
The settings page does pretty much what the name promises. You can change your settings there, like adding indexes to or removing them from your Kibana instance

13.3 DISCOVERY

The Discover view presents all the data in your index as a table of documents.

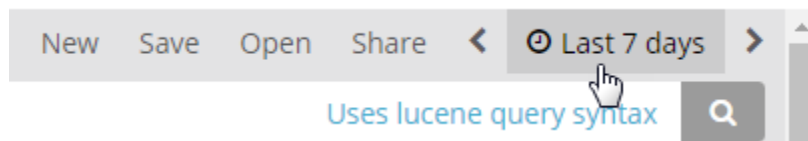
Changing the index

To change the index, you want to see the data from, you can press arrow to the right side of the current index.



Select the time

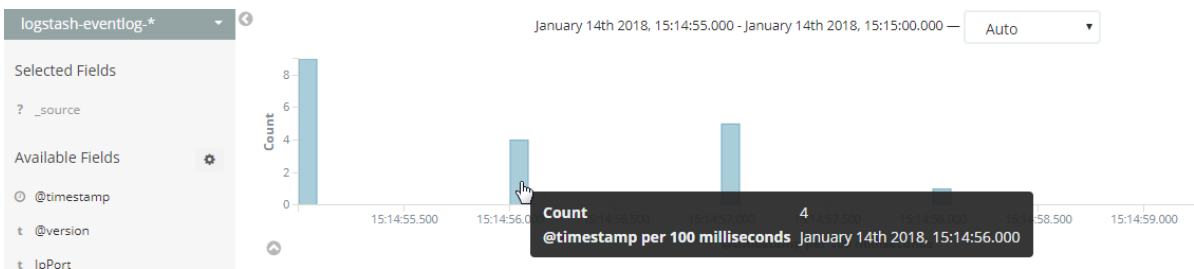
For all time-based data you can select the time span, that you want to analyze in the current view at the top right of the window. There are multiple ways to get to the documents you are interested in. Either use the Quick tab to quickly select a date range like today or Last 1 hour or use the relative and absolute tabs to specify which time spans you want to look at.



Time Range

Quick	Today	Yesterday	Last 15 minutes	Last 30 days
Relative	This week	Day before yesterday	Last 30 minutes	Last 60 days
Absolute	This month	This day last week	Last 1 hour	Last 90 days
	This year	Previous week	Last 4 hours	Last 6 months
	The day so far	Previous month	Last 12 hours	Last 1 year
	Week to date	Previous year	Last 24 hours	Last 2 years
	Month to date		Last 7 days	Last 5 years
	Year to date			

After you selected a time range which contains data, you will see a histogram at the top of the screen, which will show the distribution of events over time. You can select a range in there if you want to "zoom into" a specific time span. You can "zoom out" again by just pressing back in your browser.



The time you select will apply to any screen you visit (dashboards, visualize, etc.) and these screens offer you the possibility to change the time at the top right of the page. You also have the possibility to set a refresh rate there. This will allow you to automatically refresh a dashboard e.g. every minute. This might be useful, if you use Kibana to monitor some of the underlying data.

New Save Open Share **Auto-refresh** <

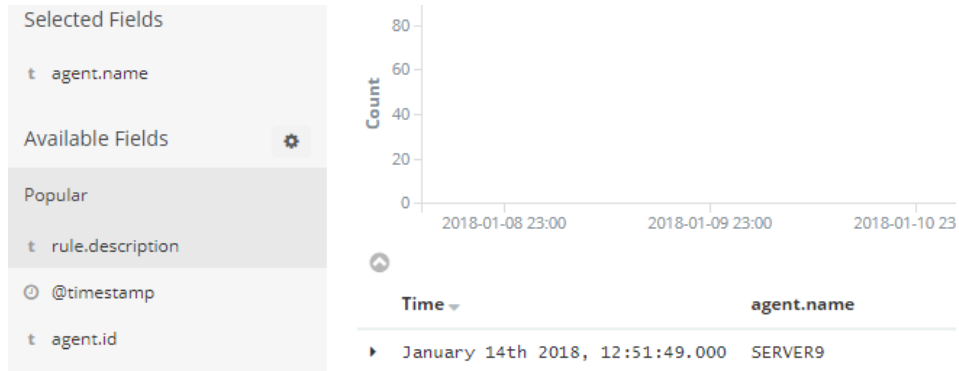
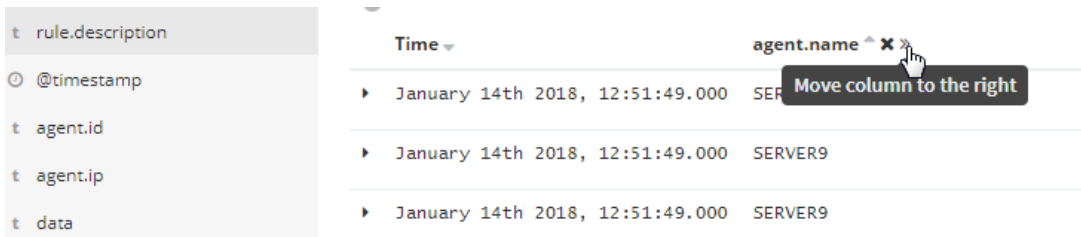
Refresh Interval

Off

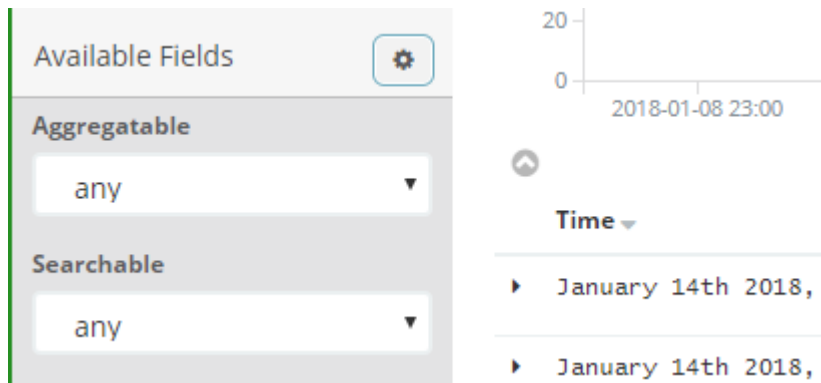
5 seconds	1 minute	1 hour
10 seconds	5 minutes	2 hour
30 seconds	15 minutes	12 hour
45 seconds	30 minutes	1 day

Fields

On the left side of the page you have a list of the fields (with their data type indicated by an icon), that exist in the documents. If you hover over a field, you have the possibility to click add which will add a column containing the contents of this field to the table. As soon as you added your first field, the output of whole documents in the list will vanish. No matter what fields you have added as columns, you can always expand a row on the caret in the front. You can also remove fields, that you don't want to see as columns anymore in the section Selected Fields above the field list on the left.

You can also move columns to the right or left for viewing. If your data has a lot of fields, you can also use the small gear icon below the Fields title on the left side, to filter the fields for some information (like whether they are aggregatable, indexed, their type or just search for a name).

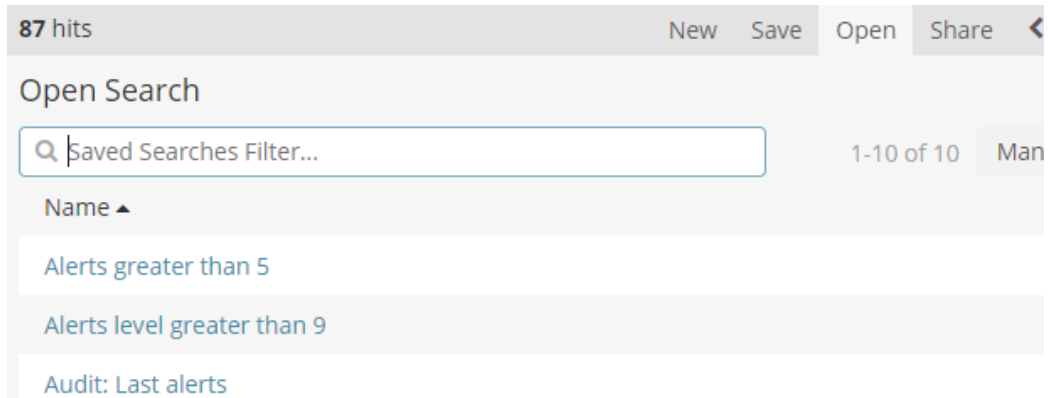


Saving and Loading

If you want to store your field list (and the queries, that we will write in a moment), you can press the Save Search icon beside the search box at the top. You must specify a name.



You can press the Open icon at any time and you will get a list of all saved searches. If you have a lot of saved searches the filter box might be useful, which lets you search in all names.

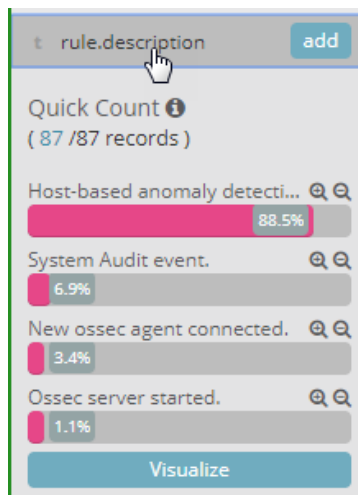


To start over a complete new view, press the New button. Never forget to save your views with the already mentioned save button, otherwise they won't be persisted. It is easy to forget that, since you can surf around between the different tabs (dashboard, discover, etc.) and on return Kibana will automatically show the last table with the fields you have selected.

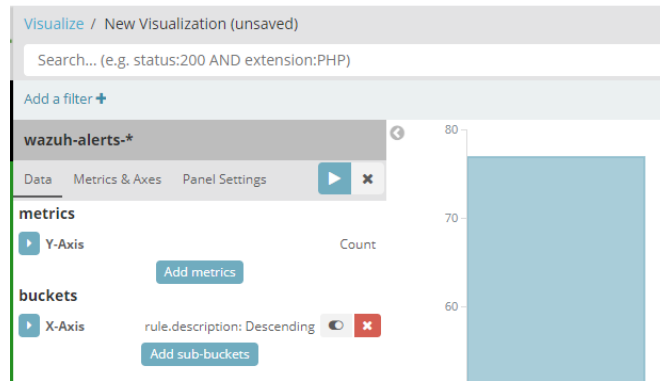
The save/load/new buttons are also available for Dashboards and Visualizations with the same functions and the same warning!

Filter for documents

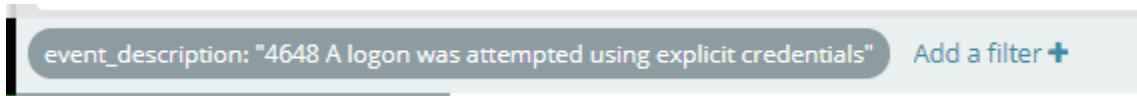
You can expand any field in the fields list on the left by clicking on it. It will reveal the list of the most common values for that field. Use the – and + magnifier icons to quickly add a filter for to show only documents having that value (+) or to exclude all documents with that value (-).



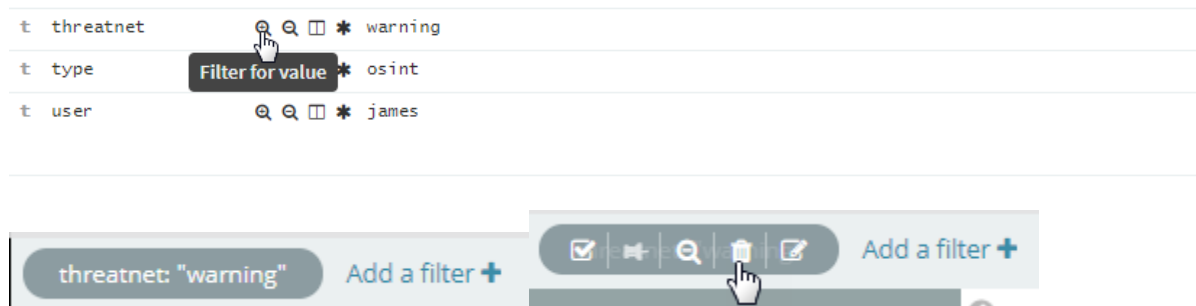
Also, the current field may be instantly visualized for its values:



If you add filters that way, a bar will appear on the top below the search bar. Each filter will be displayed as a tag, that you can disable temporary or remove completely.



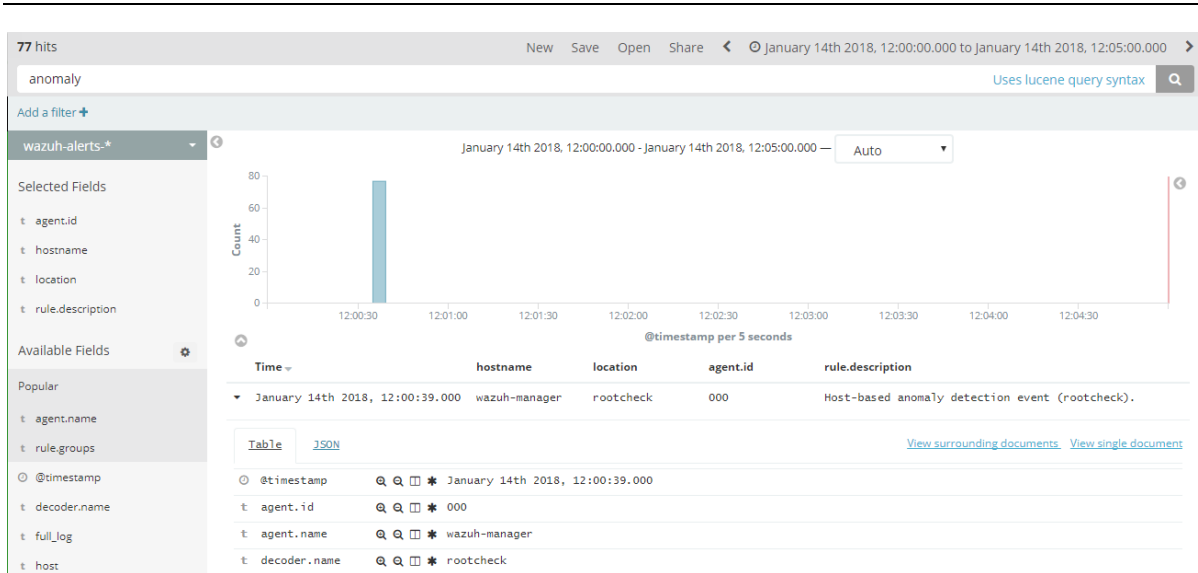
Filters can also be set by expanding the table rows on the right which show the document contents and using the filter buttons which are shown there. Note that documents may contain fields which are not indexed and can thus not be used for filtering. You won't find any filter buttons for those.



Search for documents

To search and filter the documents shown in the list, you can use the large Search box at the top of the page. The search box accepts query strings in a special syntax.

If you want to search content in any field, just type in the content, that you want to search. Entering 'anomaly' in the search box and pressing enter will show you only events that contain the term 'anomaly'.



The query language allows also some more fine-grained search queries, like:

SEARCH TERM

lang:en
 lang:e?
 lang:(en OR es)
 user.listed_count:[0 TO 10]

DESCRIPTION

to just search inside a field named "lang"
 wildcard expressions
 OR queries on fields
 range search on numeric fields

13.4 VISUALIZATIONS

Visualizations are the heart of Kibana 5. They are used to aggregate and visualize your data in different ways. To understand visualizations, we must look at Elasticsearch aggregations first, since they are the basis. If you are familiar with Elasticsearch's aggregations, you can skip the next paragraphs.

Aggregations

The aggregation of our data is not done by Kibana, but by the underlying Elasticsearch. We can distinguish two types of aggregations: bucket and metric aggregations. To get a good grip on visualizations with Kibana 5, it is essential to understand how those aggregations work, so don't be discouraged by the wall of text coming up.

Bucket aggregations

A bucket aggregation, groups all documents into several buckets, each containing a subset of the indexed documents. The decision which bucket to sort a specific document into can be based on the value of a specific field, a custom filter or other parameters. Currently, Kibana 5 supports 7 bucket aggregations, which will be described in the following paragraphs. For each aggregation, an example for the sample twitter data is given. Later in this tutorial we will see some complete examples for several of them:

Date Histogram

The date histogram aggregation requires a field of type date and an interval. It will then put all the documents into one bucket, whose value of the specified date field lies within the same interval.

Example: You can construct a Date Histogram on @timestamp field of all messages with the interval minute. In this case, there will be a bucket for each minute and each bucket will hold all messages that have been written in that minute.

Besides common interval values like minutes, hourly, daily, etc. there is the special value auto. When you select this interval, the actual time interval will be determined by Kibana depending on how large you want to draw this graph, so that a respectable number of buckets will be created (not too many to pollute the graph, nor too few so the graph would become irrelevant).

Histogram

A histogram is pretty much like a date histogram, except that you can use it on every number field. Same as with date histogram, you specify a number field and an interval (which in this case is any number). The aggregation then builds a bucket for each interval and puts in all documents, whose value falls inside this interval.

Range

The range aggregation is like a manual histogram aggregation. You also need to specify a field of type number, but you must specify each interval manually. This is useful if you either want differently sized intervals or intervals that overlap. Whenever you enter a range in Kibana, you can leave the upper or lower bound empty to create an open range (like the above 1000-*).

Terms

A terms aggregation creates buckets by the values of a field. This is much like a classical SQL GROUP BY. You specify a field (which can be of any type) and it will create a bucket for each of the values that exist in that field, and put all documents in that field that have the value.

Example: You can run a terms aggregation on the field `geoip.country_name` which holds the country name. After that you will have a bucket for each country and in each bucket the documents of all events from that country.

The aggregation doesn't always need to match the whole field value. If you let Elasticsearch analyze a string field, it will by default split its value up by spaces, punctuation marks and the like, and each part will be an own term, and as such would get an own bucket. If you do a term aggregation on the rule. Description, you might assume that you would get nearly one bucket per event, because two messages rarely are exactly the same. But this field is analysed in our sample data, so you would get buckets for e.g. `ssh`, `syslog`, `failure` and so on and in each of these buckets all documents, that had that term in the text field (even though it doesn't need to match the text field exactly).

Elasticsearch can be configured not to analyze fields or you can configure the analyzer that is used to match the behaviour of a terms aggregation to your actual needs. E.g. you could let the text field be analysed so that colons (`:`) and slashes (`/`) won't be split separators. That way, an URL would be a single term and not split up into `http`, the domain, the ending and so on. More information on analyzers can be found in the Elasticsearch documentation. For the most part SIEMonster presents fields with the `.raw` suffix which are not analyzed

Filters

A filter aggregation is a completely flexible (but therefore maybe slower than the others) aggregation. You just specify a filter for each bucket and all documents, that match the filter will be in that bucket. Each filter is just a query as described previously in section *Search for documents*. The filter you specify for each bucket can be whatever you like, meaning there doesn't need to be any relation between these filters (though most likely for a useful graph there is a connection between them).

Example: Create a filter aggregation with one query being `"geoip.country_name:(Ukraine or China)"` and the second filter being `"rule.firedtimes:[100 TO *]"`. That way the aggregation creates two buckets, one containing all the events from Ukraine & China, and one bucket with all the events with 100 or more rule fired times. It is up to you, to decide what kind of analysis you would do with these two buckets.. as already mentioned, completely unrelated queries in the filters aggregation rarely make sense.

Significant Terms

The significant terms aggregation can be used to find "uncommonly common" terms in a set of documents (cf. Elasticsearch Guide). Given a subset of documents, this aggregation finds all the terms which appear in this subset more often than could be expected from term occurrences in the whole document set. It then builds a bucket for each of the significant terms which contains all documents of the subset in which this term appears. The size parameter controls how many buckets are constructed, i. e. how many significant terms are calculated.

The subset on which to operate the significant terms aggregation can be constructed by a filter or you can use another bucket aggregation first on all documents and then choose significant terms as a sub-aggregation which is computed for the documents in each bucket.

Example: We use the search field at the top to filter our documents for those with `geop.country_name:China` and then select significant terms as a bucket aggregation. For our purpose of getting to know Kibana and playing around with the visualizations the corresponding results would be adequate. Note however, that in order to deliver relevant results that really give insight into trends and anomalies in your data, the significant terms aggregation needs sufficiently sized subsets of documents to work on. And a further side note: That our significant terms don't tell us much about the contents of the events has to do with the fact that we are looking for terms that are significant for higher risk security events.

Geohash

Elasticsearch can store coordinates in a special type `geo_point` field. That way the geohash aggregation can create buckets for values close to each other. You have to specify a field of type `geo_point` and a precision. The smaller the precision, the larger area the buckets will cover.

Example: You can create a geohash aggregation on the coordinates field in the event data. This will create a bucket each containing events close to each other (how close [and therefore how many buckets you need for all data] will be specified by the precision).

Hint: This kind of aggregation makes mostly sense, if you use a Tile Map visualization (will be covered later). In all other aggregations you will just see a cryptic geohash string, which doesn't make much sense, if not shown on a map.

Metric Aggregations

After you have run a bucket aggregation on your data, you will have several buckets with documents in them. You now specify one metric aggregation to calculate a single value for each bucket. The metric aggregation will be run on every bucket and result in one value per bucket.

In the visualizations the bucket aggregation usually will be used to determine the "first dimension" of the chart (e.g. for a pie chart, each bucket is one pie slice; for a bar chart each bucket will get its own bar). The value calculated by the metric aggregation will then be displayed as the "second dimension" (e.g. for a pie chart, the percentage it has in the whole pie; for a bar chart the actual high of the bar on the y-axis).

Since metric aggregations mostly makes sense, when they run on buckets, the examples of metric aggregations will always contain a bucket aggregation as a sample too. But of course, you could also use the metric aggregation on any other bucket aggregation; a bucket stays a bucket.

Count

This is not really an aggregation. It just returns the number of documents that are in each bucket as a value for that bucket. Sounds pretty simple, but is often enough for many kinds of analysis.

Example: If you want to know, how many events are from which country, you can use a term aggregation on the field `geop.country_name` (which will create one bucket per country code) and afterwards run a count metric aggregation. Every country bucket will have the number of events as a result.

Average/Sum

For the average and sum aggregations you need to specify a numeric field. The result for each bucket will be the sum of all values in that field or the average of all values in that field respectively.

Example: You can have the same country buckets as above again and use an average aggregation on the rule fired times count field to get a result of how many rule fired times events in that country have in average.

Max/Min: Like the average and sum aggregation, this aggregation needs a numeric field to run on. It will return the minimum value or maximum value that can be found in any document in the bucket for that field.

Example: If we use the country buckets again and run a maximum aggregation on the rule fired times we would get for each country the highest amount of rule triggers an event had in the selected time period.

Unique count

The unique count will require a field and count how many different / unique values exist in documents for that bucket.

Example: This time we will use range buckets on the rule.firedtimes field, meaning we will have buckets for e.g. users with 1-50, 50-100 and 100- rule fired times. If we now run a unique count aggregation on the geoip.country_name field, we will get for each rule fired times range the number of how many different countries users with so many rule fired times would come. In the sample data that would show us, that there are attackers from 8 different countries with 1 to 50 rule fired times, from 30 for 50 to 100 rule fired times and from 4 different countries for 100+ rule fired times and above.

Percentiles: A percentiles aggregation is a bit different, since it won't result in one value for each bucket, but in multiple values per bucket. These can be shown as e.g. different colored lines in a line graph.

When specifying a percentile aggregation, you have to specify a number value field and multiple percentage values. The result of the aggregation will be the value for which the specified percentage of documents will be inside (lower) as this value. Confused? Let's do this as an example:

You specify a percentiles aggregation on the field user.rule fired times_count and specify the percentile values 1, 50 and 99. This will result in three aggregated values for each bucket. Let's assume we have just one bucket with events in it (doesn't matter where this bucket came from). The 1 percentile result (and e.g. the line in a line graph) will have the value 7. This means that 1% of all the events in this bucket have a rule fired times count with 7 or below. The 50 percentile result is 276, meaning that 50% of all the events in this bucket have a rule fired times count of 276 or below. The 99 percentile have a value of 17000, meaning that 99% of the events in the bucket have a rule fired times count of 17000 or below. If you want to read more on percentile aggregations, you can read the Elasticsearch documentation.

Visualizations

Now that you've got an idea about what the available aggregations do, we will look at how to use them with visualizations. The different visualizations and what they do in short:

CHART TYPE	DESCRIPTION
Area Chart	Displays a line chart with filled areas below the lines. The areas can be displayed stacked, overlapped, or some other variations.
Data Table	Displays a table of aggregated data.
Line Chart	Displays aggregated data as lines.
Markdown Widget	A simple widget, that can display some markdown text. Can be used to add help boxes or links to dashboards.
Metric	Displays one the result of a metric aggregation without buckets as a single large number.

Pie Chart	Displays data as a pie with different slices for each bucket or as a donut (depending on your taste).
Tile Map	Displays a map for results of a geohash aggregation.
Vertical bar chart	A chart with vertical bars for each bucket.

Saving and Loading

While editing a visualization you will see the same New, Save and Load icons beside the search bar, as known from the Discover screen. The same rules apply there: When switching to another tab (e.g. Dashboard) and back again to the Visualize tab, Kibana will return to the very same visualization that you just edited. But unless you save this visualization it is not really persisted! So, if you don't want your visualization to be lost, always save it! This is easy to forget, especially once you saved it and edit it afterwards. These edits will be stored temporary when you switch tab, but they are not persisted at all in Kibana, unless you press save again.

Starting your first visualization

When you go to the Visualize tab, you will see a list of visualizations you can create and below a list of all saved visualizations, that you can open for editing.

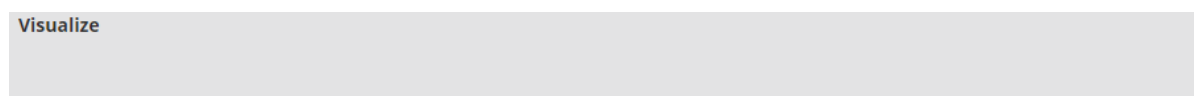
Once you clicked a visualization type to create you have two options:

- From a new search
- From a saved search

You can use From a saved search to link a visualization to a query that you have save on the Discover page. If you don't want to link it, just click From a new search to visualize on all of your data.

Sidenote: If you have added multiple indexes to your Kibana, you will be asked for which of the indexes you want to generate a visualization at this point. Unless you use From a new search in which case the visualization will be linked to the same index than the search.

In the following all the visualizations are described in detail with some example. The order is not alphabetically, but an order that should be more intuitive to understand the visualizations. All are based on the Wazuh/OSSEC alerts index. A lot of the logic that applies to all charts will be explained in the Pie Charts section, so you should read this one before the others.

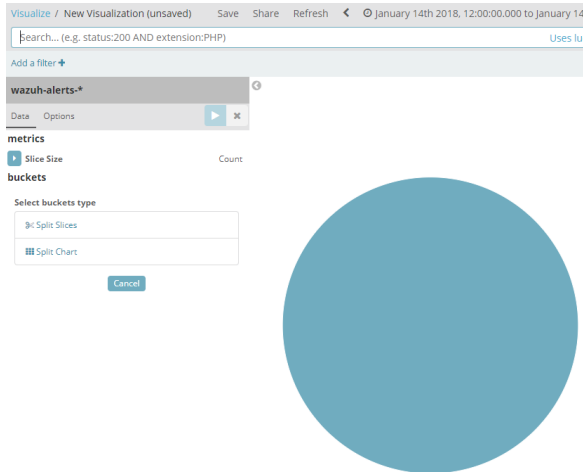


Pie chart

Basic Charts



Once you selected the Pie Chart you will come to the 'choose source' options for which 'wazuh-alerts' is used in this example and will then be taken to the visualization editor. This screen has a preview of your visualization on the right, and the edit options in the sidebar on the left.



Visualization editor for a Pie Chart

There are two icon buttons on top right of the panel. Apply is a play icon and discard a cancel cross beside it. If you make changes in the editor, you must press Apply to see them in the preview on the right side, or press Discard to throw them away and reset the editor to the state, that is currently shown in the preview (i.e. the last state you applied).



View options

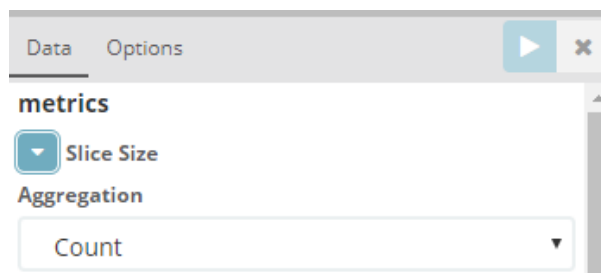
Every visualization has the expandable view options where you can change some options about the visualization. For the pie chart, there exist three different options:

Donut checks whether the diagram should be displayed as a donut instead of a pie.

Show Tooltip exist on most of the visualizations and allow to enable or disable tooltips on the diagram. When they are enabled and the user hover over a slice of the pie chart (or bar in a bar diagram, etc.), a tooltip will appear showing some data about that slice, e.g. which field and value this belongs to and the value that the metrics aggregation calculated.

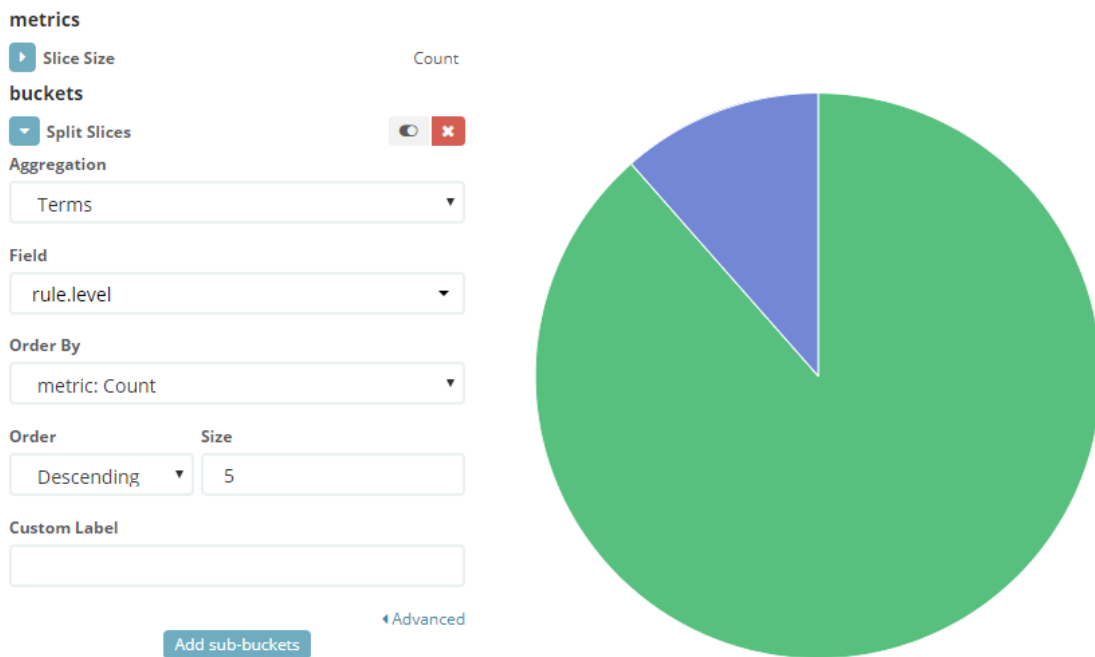
Aggregations

Above the view options visualizations have the list of their bucket aggregations applied (if the visualization supports bucket aggregations). You can add a new bucket aggregation by pressing Add Aggregation in the buckets section.



Kibana asks you now to specify in which way the different buckets of these aggregations should be shown. A common option, that exists for most of the visualizations is the Split Chart option. That way each bucket that will be created by the bucket aggregation gets an own chart. All the charts will be placed beside and below each other and make up the whole visualization.

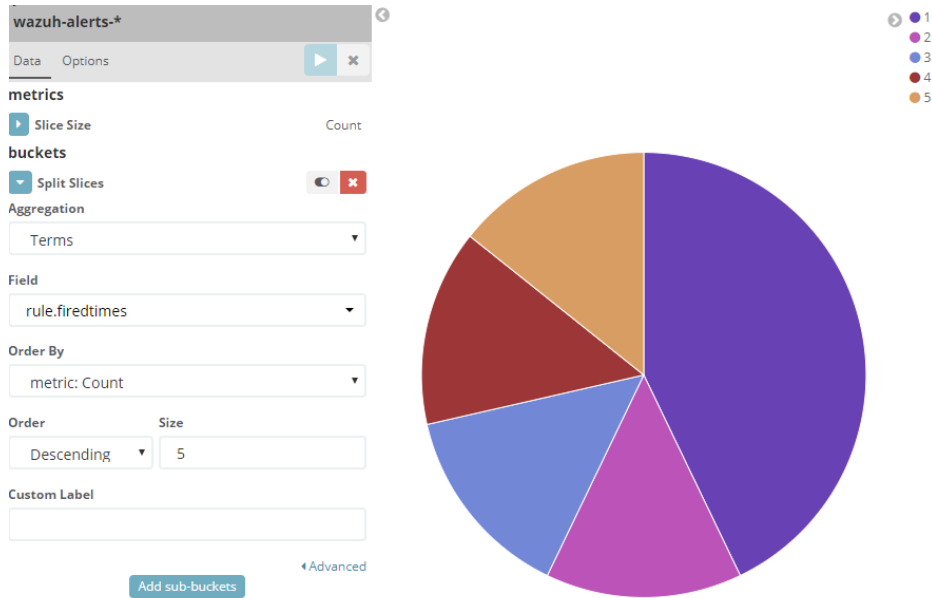
The other option for pie charts is Split Slices, which will generate a slice for each bucket. Let's add a Split Slices type. Kibana now asks you for the aggregation and its parameters. Let's say we want to see how the rule levels are distributed. We will select a terms aggregation, select the field rule.level and hit Apply.



The screenshot shows the Kibana visualization configuration interface. Under the 'metrics' section, 'Slice Size' is selected with a value of 'Count'. Under the 'buckets' section, 'Split Slices' is selected. The 'Aggregation' is set to 'Terms', the 'Field' is 'rule.level', and the 'Order By' is 'metric: Count'. The 'Order' is 'Descending' and the 'Size' is '5'. There is an 'Add sub-buckets' button and an 'Advanced' link. To the right of the configuration is a pie chart with two slices: a large green slice and a smaller blue slice.

The result should look like the screenshot above. We got one pie slice per bucket (i.e. per rule level). But how is the size of the slice in the pie determined? This will be done by the metric aggregation, which by default is set to Count of documents. So, the pie now shows one slice per rule.level bucket and its percentage depends on the number of events, that came from this event.

Pie chart with a sum metric aggregation across the ruled count but, why are there only shown two slices? This is determined by the Order and Size option in the bucket aggregation. You can specify how many buckets you want to see in the diagram, and if you would like to see the ones with the least (bottom) or the highest (top) values. What might be a bit confusing is, that these order and size actually is linked to the metric aggregation on the top. To demonstrate this, we will switch the metric aggregation on the top. When you expand it you can switch the type to Sum and the field to rule.firedtimes You will now get a slice for each level and its size will be determined, by the sum of the triggers per rule, that fired in our time range.

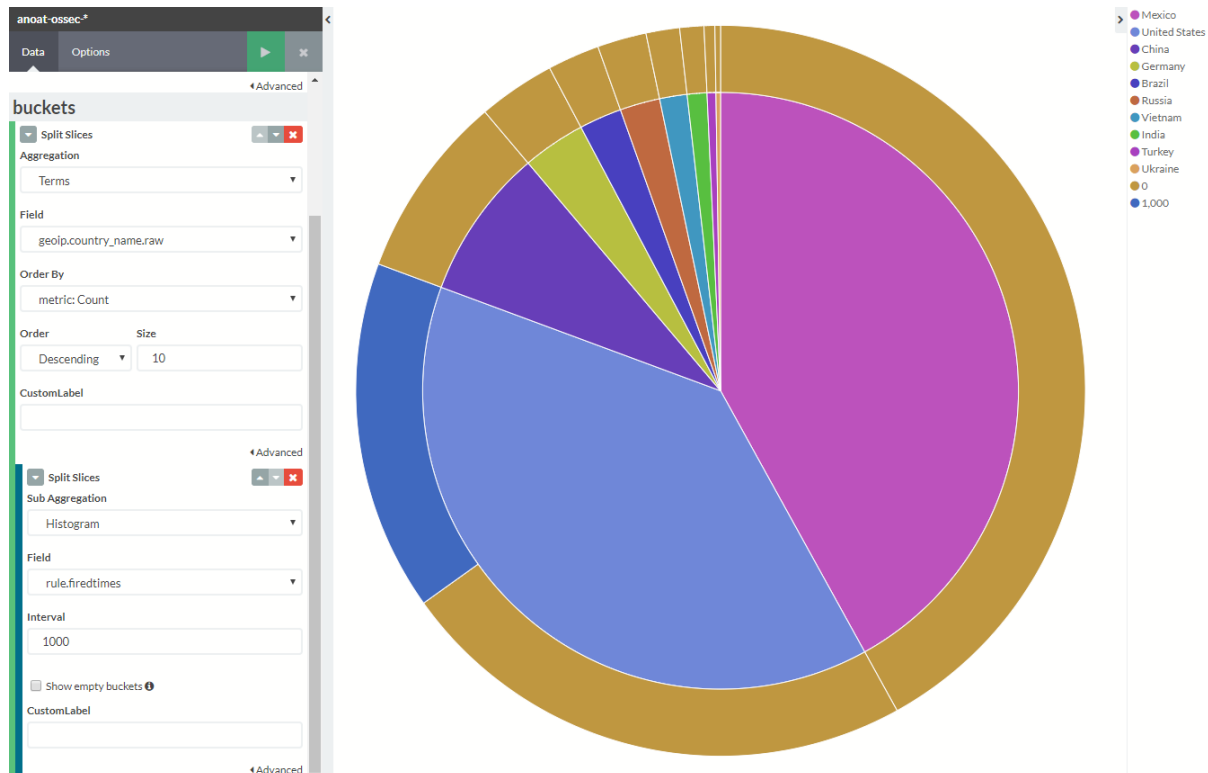


By using the Size option you can restrict results to only show the top n results. The order settings depend on the metric aggregation, that you have selected at the top of the editor. With the Order by select box you can also specify another metrics aggregation, that you want to use for ordering. Some graph types support multiple metric aggregations. If you add multiple metrics aggregations you will also be able to select in the order by box, which of these you want to use for ordering.

A lot of diagrams can use nested bucketing, so does the pie chart. You can click the Add Sub Aggregation button to add another level of bucketing. You cannot nest the different types how the chart should display this in any order you want. For example, the pie chart will complain, if you try to add now a Split Chart type, because it would like to first split charts, then use the sub aggregation on each chart.

Nested aggregations on a pie chart

Adding a sub aggregation of type Split Slices will cause a second ring of slices around the first ring.



What does happen here? Kibana first aggregate via a terms aggregation on the country code field, so we have one bucket for each country code with all the events from that country in it. These buckets are shown as the inner pie and their size is determined by the selected metric aggregation (count of documents in each bucket).

Inside each bucket Kibana now use the nested aggregation to group by the rule fired times count in a thousand interval. The result will be a bucket for each country code and inside each of these buckets, are buckets for each rule fired interval. The size of the inside buckets is again determined by the selected metric aggregation, meaning also the size of documents will be counted. In the pie chart you will see this nested aggregation as more slices in the second ring.

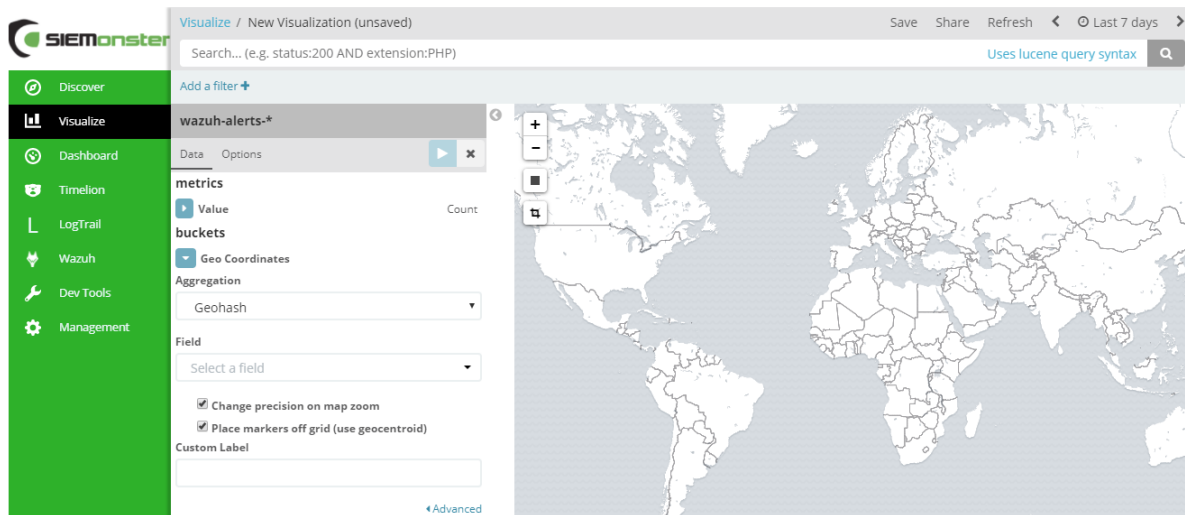
If you want to change the bucketing order, meaning in this case, you first want to bucket the events by their rule fired times and then you want to have buckets inside these follower buckets for each country, you can just use the arrows beside the aggregation to move it to an outer or inner level.

There are some options to the Histogram aggregation. You can set if empty buckets (buckets in which interval no documents lie) should be shown. This doesn't make any sense for pie charts, since they will just appear in the legend, but due to the nature of the pie chart, their slice will be 0% large, so you cannot see it. You can also set a limit for the minimum and maximum field value, that you want to use.

Before we look at the next type of visualization, we should save this one for later usage. Press the Save button on the top right and give your visualization a name. To create a new visualization just hit the new button beside the save button.

Tile Map

A tile map is most likely the only useful way to display a geohash aggregation. When you create a new one, you can again use the Split Chart to create one map per bucket, and the other option is the Geo coordinates type. That way you have to select a field that contains geo coordinates and a precision. The visualization will show a circle on the map for each bucket. The circle (and bucket) size depends on the precision you choose. The color of the circle will indicate the actual value calculated by the metric aggregation.

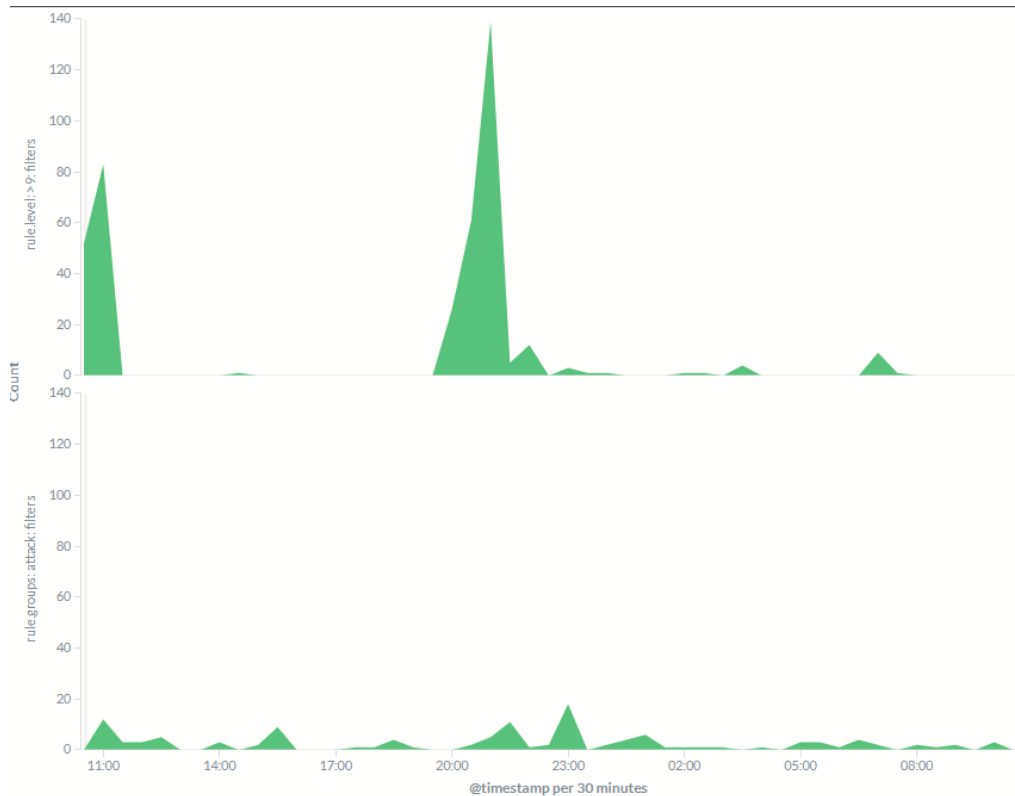


Tile map with rules triggered per location

Area/Line Chart

The Area Chart and Line Chart are very similar, except for the Area Chart painting the area below the line, and so it supports different methods of overlapping and stacking for the different areas. Both kind of charts are often used to display data over time.

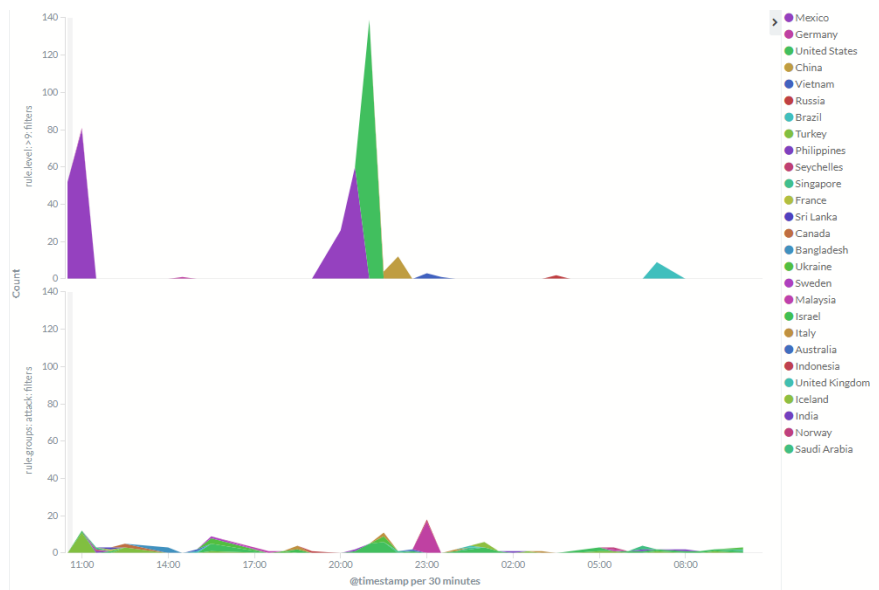
The chart that we want to create, should compare HIDS rule levels greater than 9 with attack signatures. We want to split up the graph for the two options.



Area chart with split chart aggregation

First we add a new bucket aggregation with type Split Chart with a filters aggregation and one filter for rule.level: >9 and another for rule.groups: attack. As mentioned the x-axis will often be used to display a time value (so data will be displayed over time), but it is not limited to that. You can use any other aggregation if you like, but take care, that the line (or area) will be interpolated between two points on the x-axis. Which doesn't make much sense, if the values you choose aren't anyhow consecutive.

Add now another sub aggregation of type Split Area which will cause to create multiple colored areas in the graph. To add geo positions, we will do a terms aggregation on the field `geoip.country_name.raw`. Now you have graphs showing the events by country.



In the Metric & Axes options you can change the Chart Mode which is currently set to stacked. This option only applies to the area chart, since in a line chart there is no need for stacking or overlapping areas. For area charts, there exist five different types of Chart Mode:

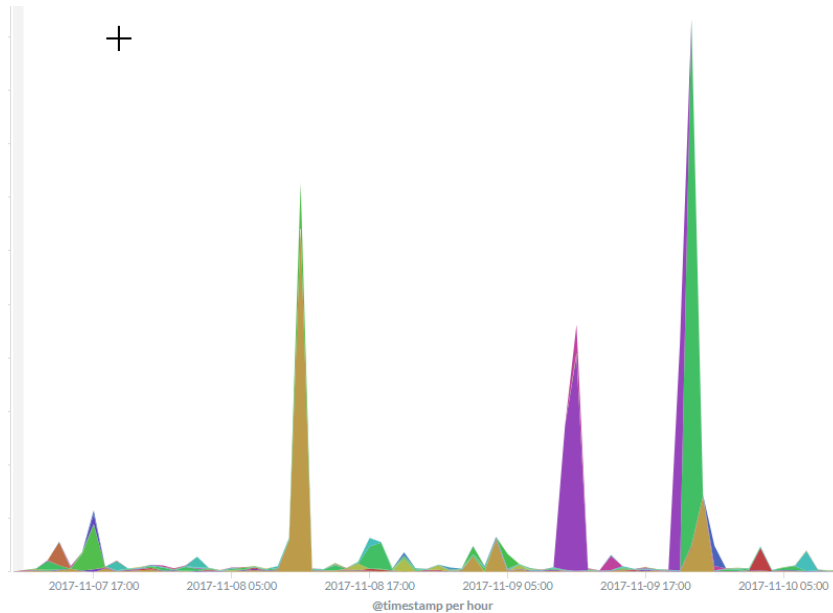
- *Stacked*: Stacks the aggregations on top of each other.
- *Overlap*: The aggregations overlap, with translucency indicating areas of overlap.
- *Wiggle*: Displays the aggregations as a streamgraph.
- *Percentage*: Displays each aggregation as a proportion of the total.
- *Silhouette*: Displays each aggregation as variance from a central line.

Checkboxes are available to enable and disable the following behaviours:

- **Smooth Lines**: Check this box to curve the top boundary of the area from point to point.
- **Set Y-Axis Extents**: Check this box and enter values in the y-max and y-min fields to set the Y axis to specific values.
- **Scale Y-Axis to Data Bounds**: The default Y axis bounds are zero and the maximum value returned in the data. Check this box to change both upper and lower bounds to match the values returned in the data.
- **Order buckets by descending sum**: Check this box to enforce sorting of buckets by descending sum in the visualization
- **Show Tooltip**: Check this box to enable the display of tooltips.

1. Stacked

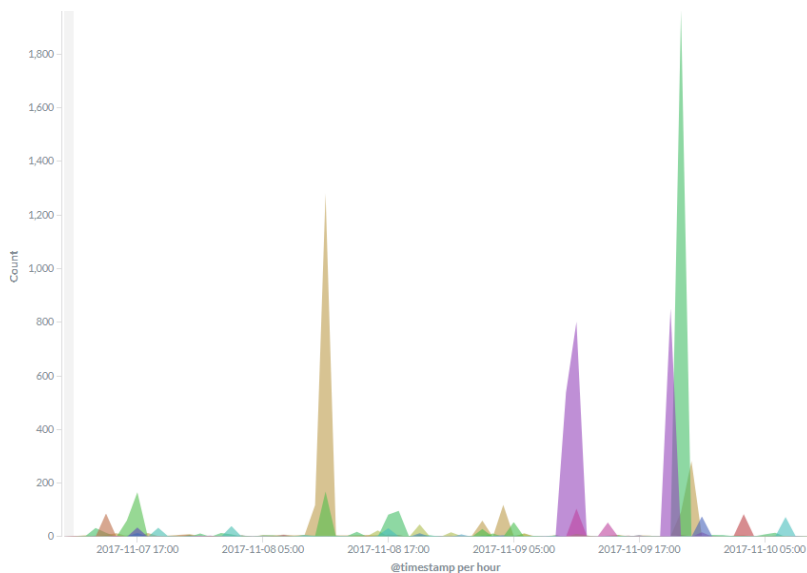
The area for each bucket will be stacked upon the area below. The total documents across all buckets can be directly seen from the height, of all stacked elements.



Stacked mode of area chart

2. Normal

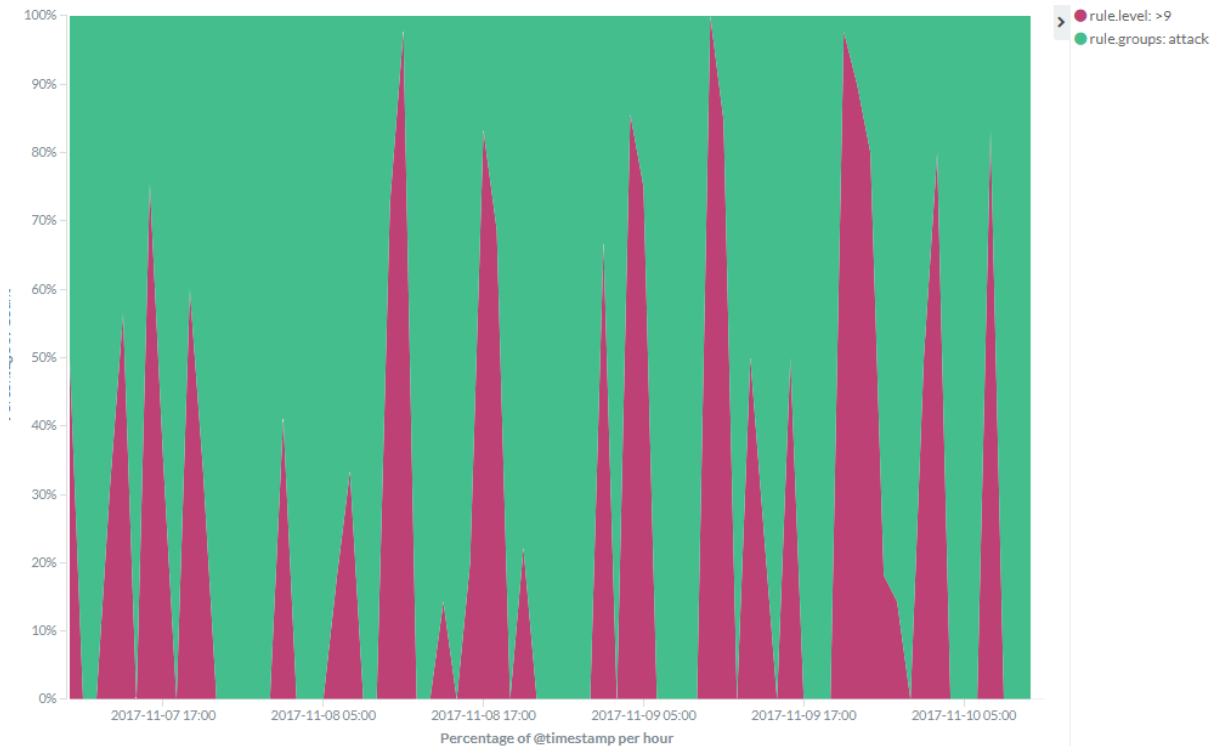
In the overlap view, areas won't be stacked upon each other. Every area will begin at the x-axis and will be displayed semi-transparent, so all areas overlap each other. You can easily compare the values of the different buckets against each other that way, but it is harder to get the total value of all buckets in that mode.



Overlap mode of area chart

3. Percentage

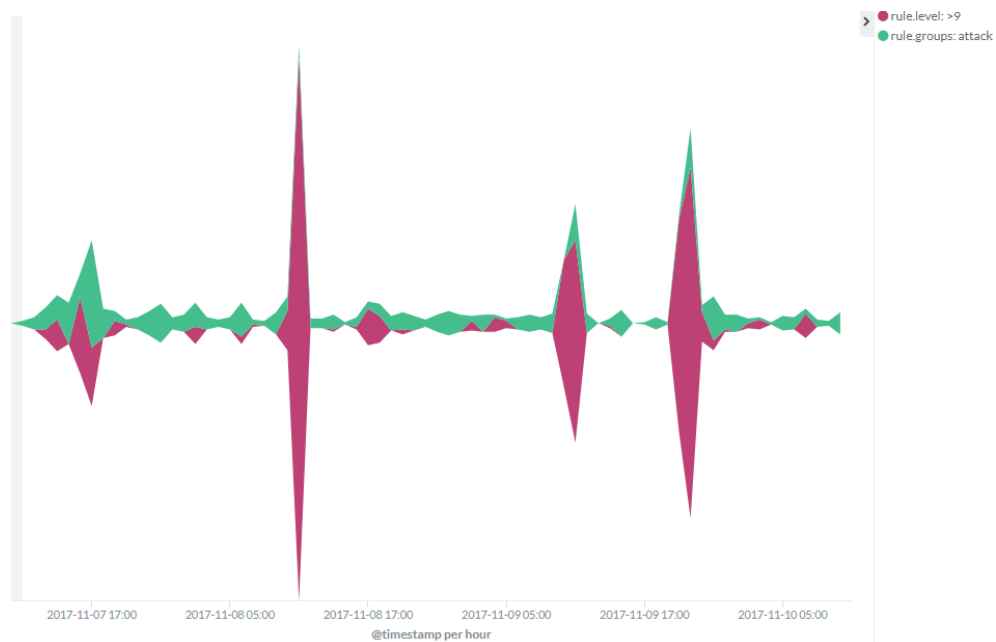
The height of the chart will always be 100% for the whole x-axis and only the percentage between the different buckets will be shown.



Percentage mode of area chart

4. Silhouette

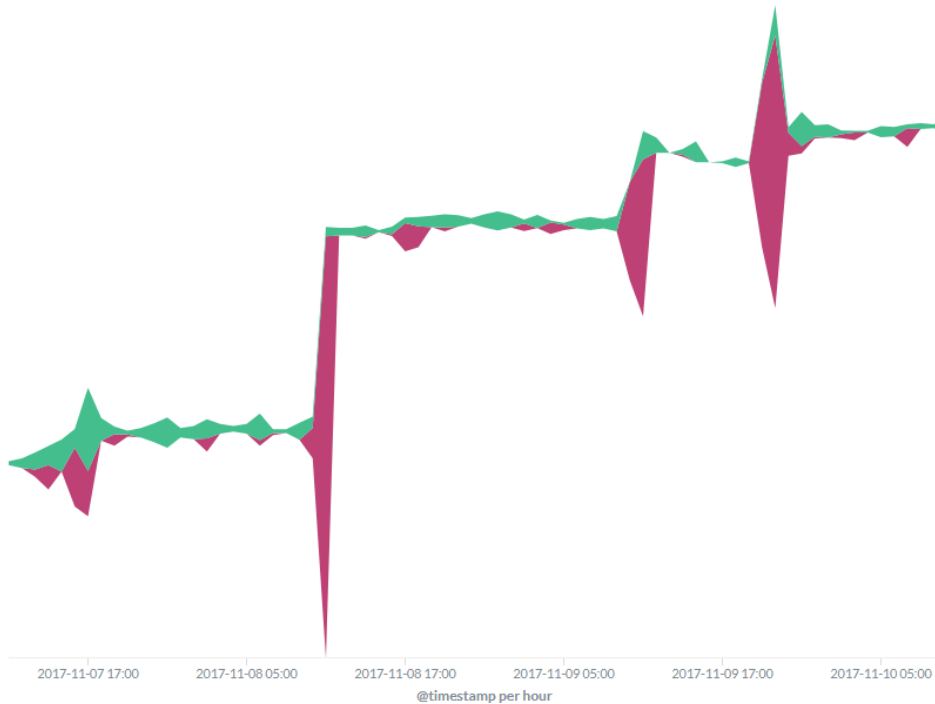
In this chart mode, a line somewhere in the middle of the diagram is chosen and all charts evolve from that line to both directions.



Silhouette mode of area chart

5. Wiggle

This is much like the silhouette mode, but it doesn't keep a static baseline from which the areas evolve in both directions. Instead it tries to calculate the baseline for each value again, so that change in slope is minimized. It's hardly ever found that useful in a diagram, since it makes seeing relations between area sizes and reading the total value more difficult than the other modes.

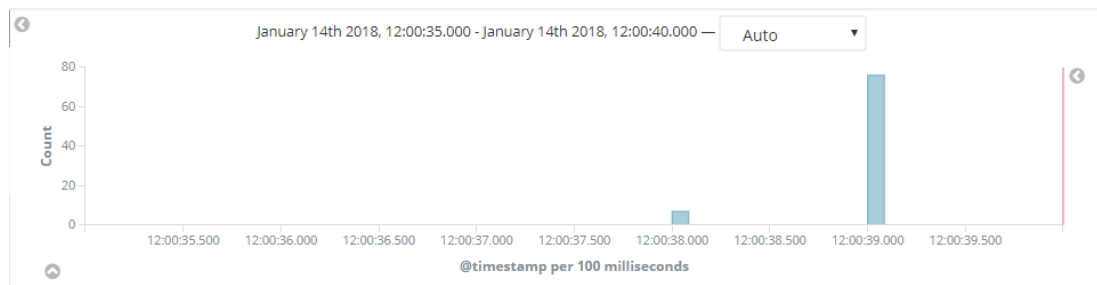


Wiggle mode in area chart

Multiple Y-Axes

Beside changing the view mode, you also have the possibility to add another metric aggregation to either line or area charts. That metric aggregation will be shown with its own color in the same diagrams. Unfortunately, all metric aggregations you add, will share the same scale on the y-axis. That's why this makes most sense, if your metric aggregations return values in the same dimension (e.g. one metric that will result in values from up to 100 and another that result in values from 1 million to 10 million, won't be displayed very well, since the first metric will barely be visible in the graph).

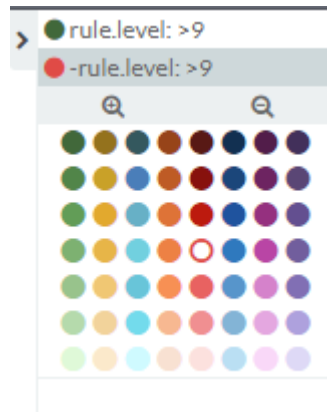
Vertical Bar



A bar chart example

The vertical bar visualization is much like the area visualization, but more suited if the data on your x-axis isn't consecutive, because each x-axis value will get its own bar(s) and there won't be any interpolation done between the values of these bars.

Changing bar colors: To the right of the visualization the colors for each filter/query can be changed by expanding the filter and picking required color.



You only have three bar modes available: stacked, which behave the same like in area chart, it just stack the bars onto each other. percentage use 100% height bars, and only shows the distribution between the different buckets. Grouped is the only different mode compared to area charts. It will place the bars for each x-axis value beside each other as shown in the screenshot on the right.

Metric

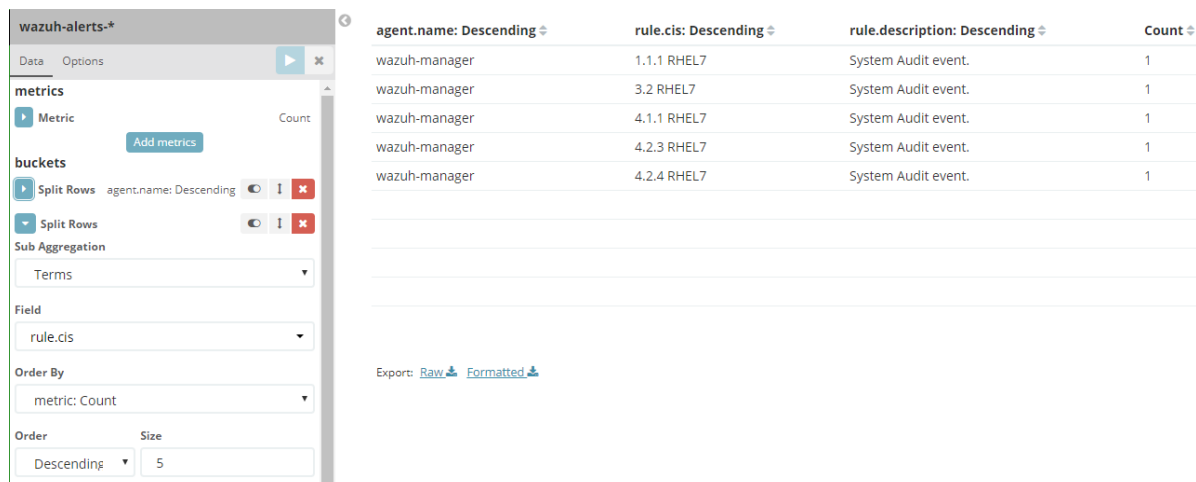
A metric visualization can just display the result of a metrics aggregation. There is no bucketing done. It will always apply to the whole data set, that is currently taken into account (you can change the data set by typing queries in the top box). The only view option, that exists is the font size of the displayed number.

Markdown widget

This is a very simple widget, which doesn't do anything with your data. You only have the view options where you can specify some markdown. The markdown will be rendered in the visualization. This can be very useful to add help texts or links to other pages to your dashboards. The markdown you can enter is GitHub flavoured markdown.

Data table

A data table is a tabular output of aggregation results. It's basically the raw data, that in other visualizations would be rendered into some graphs. And as we will cover in the paragraph *Debugging visualizations* you can get the table of every visualization.



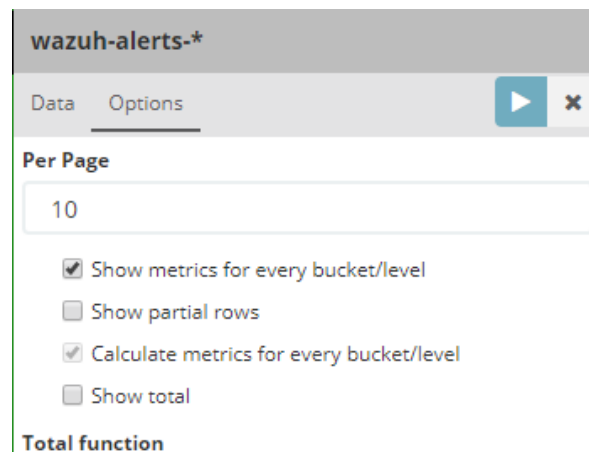
agent.name: Descending	rule.cis: Descending	rule.description: Descending	Count
wazuh-manager	1.1.1 RHEL7	System Audit event.	1
wazuh-manager	3.2 RHEL7	System Audit event.	1
wazuh-manager	4.1.1 RHEL7	System Audit event.	1
wazuh-manager	4.2.3 RHEL7	System Audit event.	1
wazuh-manager	4.2.4 RHEL7	System Audit event.	1

A sample data table

Let's create a table that uses the Split Rows type to aggregate the top 5 countries. and a sub aggregation with some ranges on the rule level field. In the screenshot above, you can see what the aggregations should look like and the result of the table.

We will get all the country buckets on the top level. They will be presented in the first column of the table. Since each of these rule level buckets contains multiple buckets for the rule levels nested aggregation, there are 2 rows for each country, i.e. there is one row with the country in the front for every bucket in the nested aggregation. The first two rows are both for United States, and each row for one sub bucket of the nested aggregation. The result of the metrics aggregation will be shown in the last column. If you add another nested aggregation you will see, that those tables easily get pretty large and confusing.

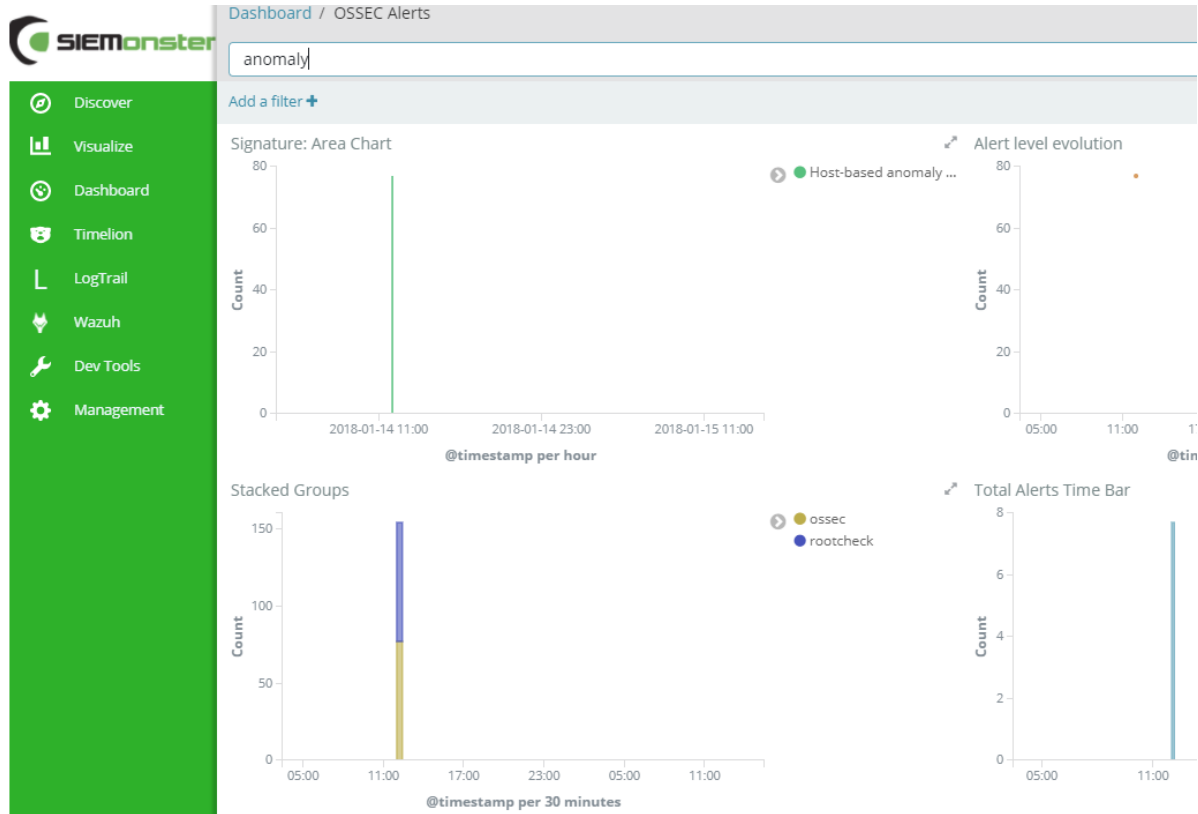
If you would now like to see the result of the metrics aggregation for the terms aggregation on the countries, you would have to sum up all the values in the last column, that belongs to rows beginning with United States. This is some work to do, and wouldn't work very well for average metrics aggregations for example. In the view options you can enable Show metrics for every bucket/level, which will show the result of the metrics aggregation after every column, for that level of aggregation. If you switch it on, after the United States column should appear another column, which says 3989, meaning there are 3989 documents in the United States bucket. This will be shown in every row, though it will always be the same for all rows with United States in it. You can also set the size of how many rows should be shown in one page of the table in the view options.



Queries in visualizations

After we learned about all the visualizations there are just some small features we should talk about, before continuing to dashboards. Perhaps the most important one is queries in visualizations.

As you remember from the Discover section, you can enter queries in a specific query language in the search box at the top of the page. This also works for visualizations. You can just enter any query there, and it will use this as a filter on the data, before the aggregation runs on the data. You can just try this out on our data table we generated in the last paragraph, by e.g. entering 'anomaly' to the search box and press enter. You will see that only panes relating to anomaly.



This filtering is very handy, because it will be stored with the visualization when you save it, meaning if you place the visualization on a dashboard the query that you stored with the visualization will still apply.

Debugging Visualizations

If you are more known to Elasticsearch or interested in the raw data of your visualizations, it might come handy to take a deeper look into them. Kibana offers you some debugging output for your visualizations. If you are in the Visualize screen, you can see a small up pointing arrow below the visualization preview (you will also see this on dashboards below the visualizations). Hitting this will reveal the debug panel with several tabs on the top.

Table

Will show the results of the aggregation as a data table visualization, i.e. it's the raw data the way Kibana sees it.

Request

The request tab shows the raw JSON of the request, that has been sent to Elasticsearch for this aggregation. This can get handy if you are common to Elasticsearch and its behaviour.

Response

Shows the raw JSON response body, that Elasticsearch returned for the request.

Statistics

Show some statistics about the call, like the duration of the request and the query, the number of documents, that where hit, and the index that was queried.

13.5 DASHBOARDS

A dashboard is just a place to put several of these visualizations and arrange them. This has many advantages, e.g. you can easily use a visualization on multiple dashboard, without the need to copy code around. If you edit the visualization it will be changing automatically on every dashboard you use it. When opening the Dashboard tab, the first time we will have an empty dashboard, ready to be arranged with our visualizations.

Placing visualizations

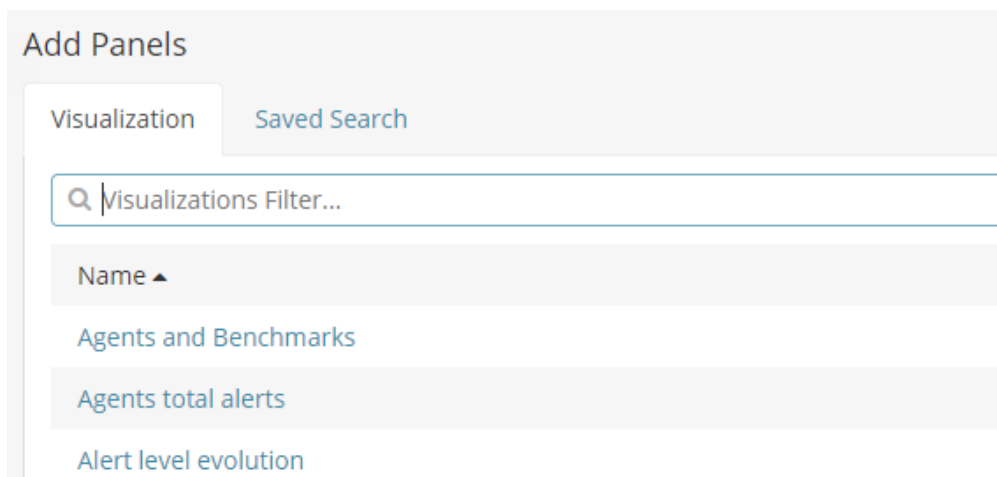
To add a new visualization, press the Add button over to the right. A panel with a list of all your visualizations will be expanded.



This dashboard is empty. Let's fill it up!

Click the **Add** button in the menu bar above to add a visualization to the dashboard.

If you haven't set up any visualizations yet, [visit the Visualize app](#) to create your first visualization.



You can use the filter on the top to search for a special one, or just browse through the list until you found one. Let's choose any of them and click on it, to add it to the dashboard. You will see a box with that visualization appearing on the dashboard. You can use the top right corner of the box to resize the box to the desired size. You can also move around the box by grabbing it at the title bar. If you want to remove the box again (this won't delete the visualization itself) just press the small x in the upper right corner. By hitting the pencil beside the x, you will jump to the visualize editor for this visualization. Try to place several of your visualizations on the dashboard and arrange them in a way you like. You will quickly notice, that some of the visualizations need some space to display their content, and will just display a warning, when you resize them too small.

Placing Searches

Besides adding visualizations, you can also place the tabular output for a specific filter (i.e. what you saved under Discover) to the dashboard. After clicking the add button you can switch to the tab Searches. Just select any search you saved on the Discover page and it will be added to the dashboard as well.

Saving/Loading dashboards

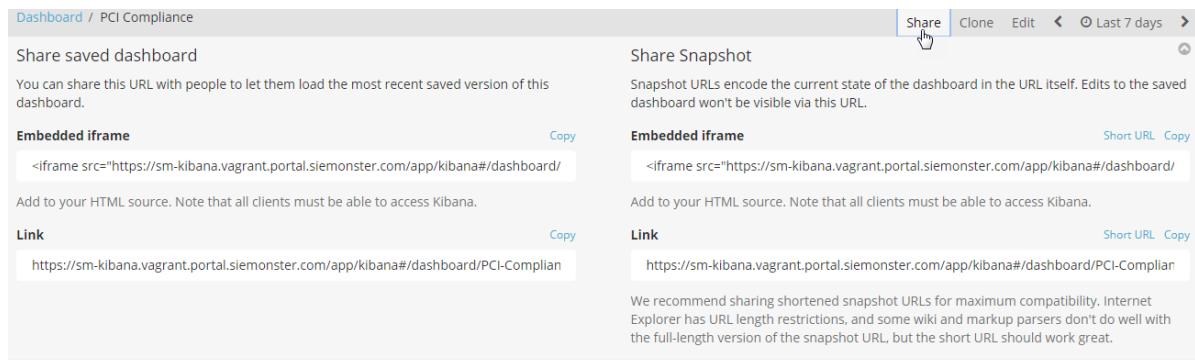
Once you finished arranging all the visualizations, you can use the save button on the top right to give the dashboard a name and store it. Same with visualizations and the discover tab: when you make changes to the dashboard, you need to press save again to store these changes permanently. You can load dashboards by pressing the loading button and select the desired dashboard.

Queries in dashboards

Same as with all other screens, you can use the query language to enter queries in the top search box. The data for all visualizations placed in the dashboard will be filtered by this query before aggregation. If you have stored a query with a visualization (as described in the previously), both queries will apply. So, you can use the dashboard search box to quickly filter out data you want to aggregate, without destroying any filter logic inside the visualization. If you change the time interval on your dashboard (on the top right side) this will of course also apply to every visualization on the dashboard.

Sharing Dashboards

You can press the share link (beside the Add Visualizations) to get some links that you can share around. There is an embed html snippet available at the top. If you copy out the link written in the `src=".."` attribute and share this, your users won't have the option to modify the dashboard. This is not a security feature, since a user can just remove the embed from the URL. But it might be handy, if you want to share links to people, that should not modify the dashboards by accident. There is also a URL shortener to enable easier share links.



The screenshot shows the 'Share' menu for a dashboard titled 'PCI Compliance'. The menu is open, displaying two main options: 'Share saved dashboard' and 'Share Snapshot'. Each option provides an 'Embedded iframe' and a 'Link' with a 'Copy' button. The 'Share saved dashboard' option provides a link to the dashboard's current state, while the 'Share Snapshot' option provides a link to a snapshot of the dashboard's state. A note at the bottom of the 'Share Snapshot' section recommends using shortened snapshot URLs for maximum compatibility.

Dashboard / PCI Compliance

Share saved dashboard

You can share this URL with people to let them load the most recent saved version of this dashboard.

Embedded iframe [Copy](#)

```
<iframe src="https://sm-kibana.vagrant.portal.siemonster.com/app/kibana#/dashboard/"
```

Add to your HTML source. Note that all clients must be able to access Kibana.

Link [Copy](#)

```
https://sm-kibana.vagrant.portal.siemonster.com/app/kibana#/dashboard/PCI-Complian
```

Share Snapshot

Snapshot URLs encode the current state of the dashboard in the URL itself. Edits to the saved dashboard won't be visible via this URL.

Embedded iframe [Short URL](#) [Copy](#)

```
<iframe src="https://sm-kibana.vagrant.portal.siemonster.com/app/kibana#/dashboard/"
```

Add to your HTML source. Note that all clients must be able to access Kibana.

Link [Short URL](#) [Copy](#)

```
https://sm-kibana.vagrant.portal.siemonster.com/app/kibana#/dashboard/PCI-Complian
```

We recommend sharing shortened snapshot URLs for maximum compatibility. Internet Explorer has URL length restrictions, and some wiki and markup parsers don't do well with the full-length version of the snapshot URL, but the short URL should work great.

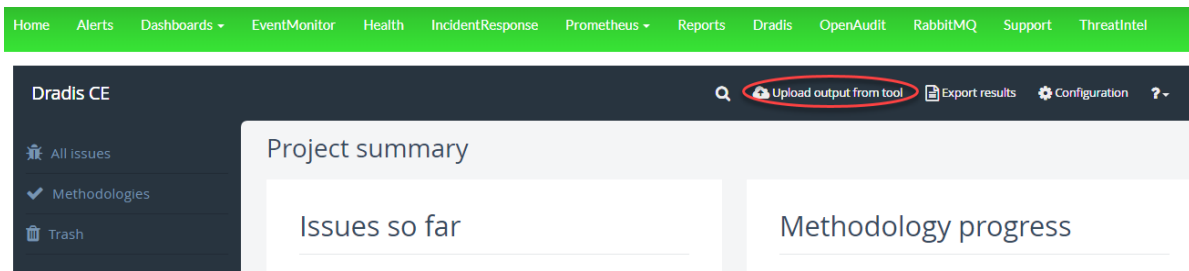
14 DRADIS INTEGRATION

To integrate Commercial & Open Source vulnerability reports into the SIEMonster dashboard.

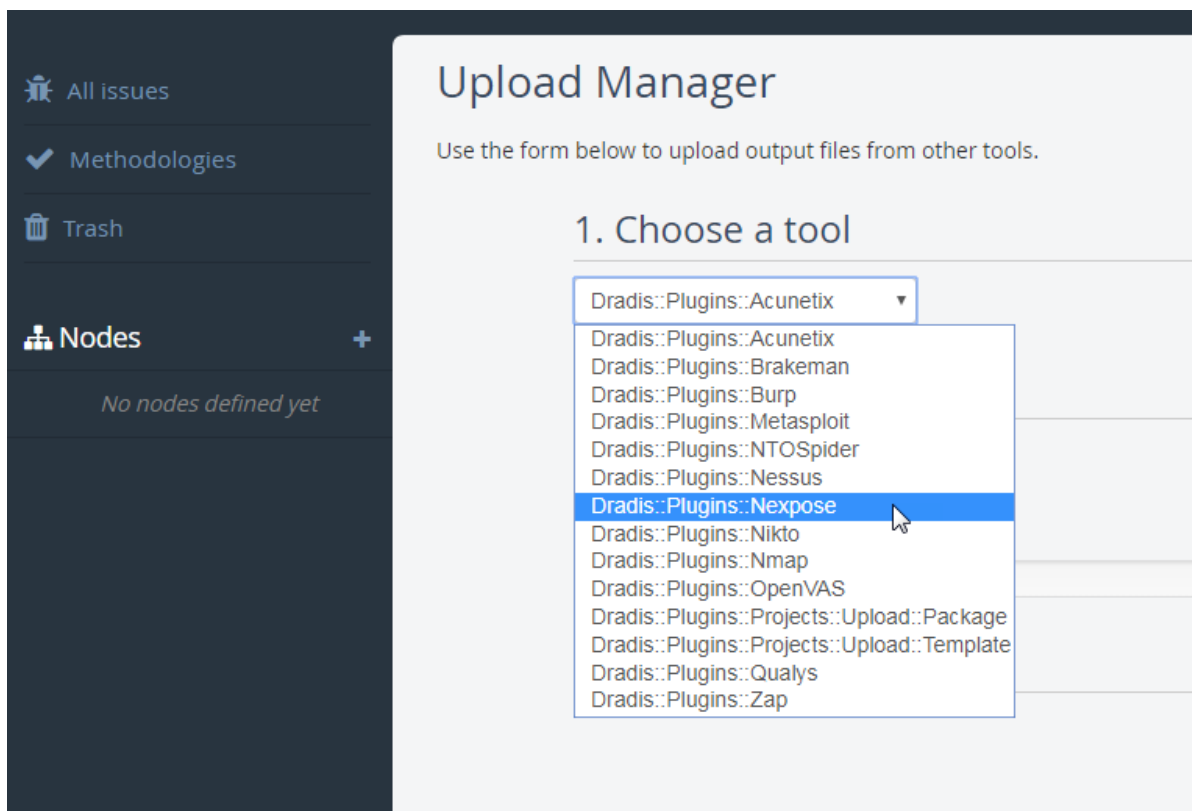
Dradis is an open source framework to enable effective sharing of information among participants in a penetration test. It is a self-contained web application that provides a centralised repository of information to keep track of what has been done so far, and what is still ahead. It has plugins to read and collect the output of a variety of network scanning tools, like Qualys, Accunetix, Nessus, Burp Suite & OpenVAS

Upload and convert Nessus File

From the main screen, choose the 'Upload output from tool' options



Choose the tool for which you have the output export file:



The scan results will be processed over a few minutes before being displayed as issues to be reviewed and collaborated on.

More information can be found at <https://dradisframework.com/ce/>

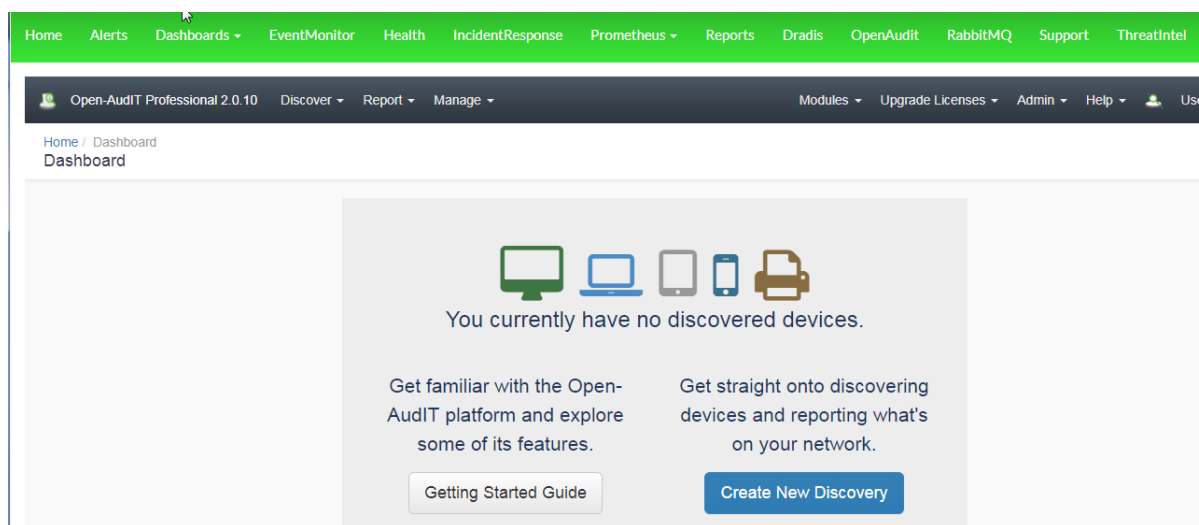
15 OPENAUDIT – ASSET DISCOVERY

Open-Audit is an application to tell you exactly what is on your network, how it is configured and when it changes. Open-Audit will run on Windows and Linux systems. Essentially, Open-Audit is a database of information, that can be queried via a web interface. Data about the network is inserted via a Bash Script (Linux) or VBScript (Windows). The entire application is written in php, bash and vbscript. These are all 'scripting' languages - no compiling and human readable source code. Making changes and customisations is both quick and easy.

Windows PCs can be queried for hardware, software, operating system settings, security settings, IIS settings, services, users & groups and much more. Linux systems can be queried for a similar amount of information. Network devices (printers, switches, routers, etc) can have data recorded such as IP-Address, MAC Address, open ports, serial number, etc, etc. Output is available in PDF, CSV and webpages. There are export options for Dia and Inkscape.

Open-Audit can be configured to scan your network and devices automatically. A daily scan is recommended for systems, with network scans every couple of hours. That way, you can be assured of being notified if something changes (day to day) on a PC, or even sooner, if something "new" appears on your network.

Once activated, (Community Edition), review the 'Getting Started' guide and when ready go ahead to 'Create New Discovery'



Enter credentials for network devices and then the required subnet for discovery:

Discoveries

Name ?

Subnet ?

Check the Discovery details, then Execute.

SIEMonster LAN
List Discoveries ?

ID 1	Subnet 192.168.0.0/24 ✎
Name SIEMonster LAN ✎	Execute Execute
Organisation Default Organisation ✎	
Description Subnet - 192.168.0.0/24	
Network Address http://10.42.237.159/open-audit/ ✎	
Type subnet	
Assign Devices to Org ✎	
Assign Devices to Location ✎	
Edited By Administrator	
Edited Date 2018-01-15 04:58:13	
Complete y	

Logs

Found Devices
All IPs
Debug

Discoveries

Discovery 'SIEMonster LAN' is running.

Results will be shown in the logs below:

Found Devices
All IPs
Debug

50 records per page

Timestamp	▲ Message
2018-01-15 05:00:49	Discovery found an unknown device at IP address 192.168.0.1.
2018-01-15 05:02:10	Discovery found an unknown device at IP address 192.168.0.3.
2018-01-15 05:02:27	Discovery found an unknown device at IP address 192.168.0.4.
2018-01-15 05:03:42	Discovery found an unknown device at IP address 192.168.0.7.

16 FREQUENTLY ASKED QUESTIONS

16.1 CONFIGURATION / INSTALLATION

Is there a license requirement for SIEMonster?

There is no license needed, you can have as many nodes and ingest as much data as you want. SIEMonster is a collection of tools licensed under the [GNU General Public License](#).

Where is the latest FAQ's?

www.siemonster.com and Click on Resources or support.

16.2 BACKUP/SCALING

Backup to Amazon S3 storage is available. The Elasticsearch Cloud AWS plugin is preinstalled.

16.3 BACKUP

SIEMonster Rancher Server – Makara runs a self-contained MySQL database which contains data for the current install. This includes Stack/User/Network/Catalog data. In the event of Docker container loss or server failure it is recommended to backup this database on a regular basis.

The Rancher Server container can also be linked to an external database for more resilience.

16.4 RANCHER SERVER MYSQL BACKUP/MIGRATION

The following examples illustrate a backup strategy and a migration example.

Backup

1. First, identify the ContainerID:

```
$ docker ps
```

```
CONTAINER ID   IMAGE
d10efd4d77c3   rancher/server
```

2. Run a scheduled backup via a Docker container, where DB_DUMP_FREQ is in minutes.

```
docker run -d --restart=always -e DB_DUMP_FREQ=1440 -e DB_DUMP_BEGIN=+0 -e DB_DUMP_TARGET=/db --link d10efd4d77c3:db -v "$PWD":/db deitch/mysql-backup
```

This will start straight away, run every 24 hours and drop a compressed dump file into the current folder, e.g. db_backup_20170113025536.gz

Full details at <https://github.com/deitch/mysql-backup>

Migrate DB for resilience

1. First backup the current database to file as shown above.
2. Download the latest Rancher Server image:

```
$ docker pull rancher/server:latest
```
3. Setup an external MySQL database such as AWS RDS.

http://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_GettingStarted.CreatingConnecting.MySQL.html#CHAP_GettingStarted.Creating.MySQL

4. Extract the backup dump file from step 1, e.g.

```
$ gunzip db_backup_20170113025536.gz
```
5. Restore to remote MySQL:

```
$ mysql -h mysql-db.us-west-2.rds.amazonaws.com -P 3306 -u dbuser -p <db_backup_20170113025536
```
6. Stop the current Rancher Server container:

```
$ docker ps  
$ docker stop <ContainerID>
```
7. Using the IP address of the remote DB, run a new instance of Rancher Server with remote database connection details:

```
$ docker run -d --restart=unless-stopped -p 8080:8080 rancher/server --db-host 172.1.1.100 --db-port 3306 --db-user dbuser --db-pass mypassword --db-name cattle
```
8. Check the logs:

```
$ docker logs -f <ContainerID>
```
9. Remove the old Rancher Server container

```
$ docker rm <ContainerID>
```


16.5 PHYSICAL DISK EXPANSION

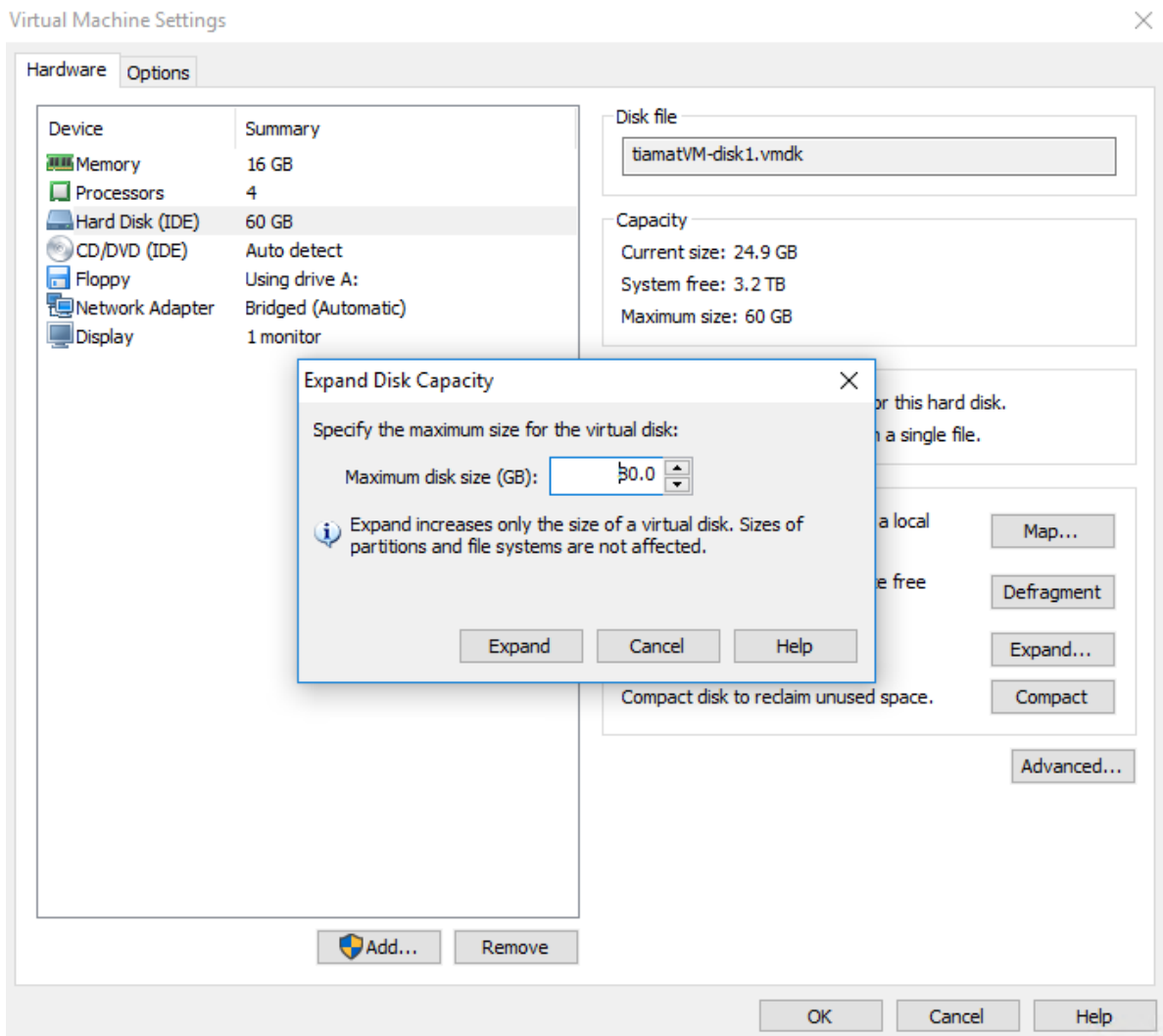
The following details how to expand the physical partition size of any of the SIEMonster hosts.

Note: Please back up any data of the SIEMonster host to be modified in the event of failure or data loss during the modification of the partitions.

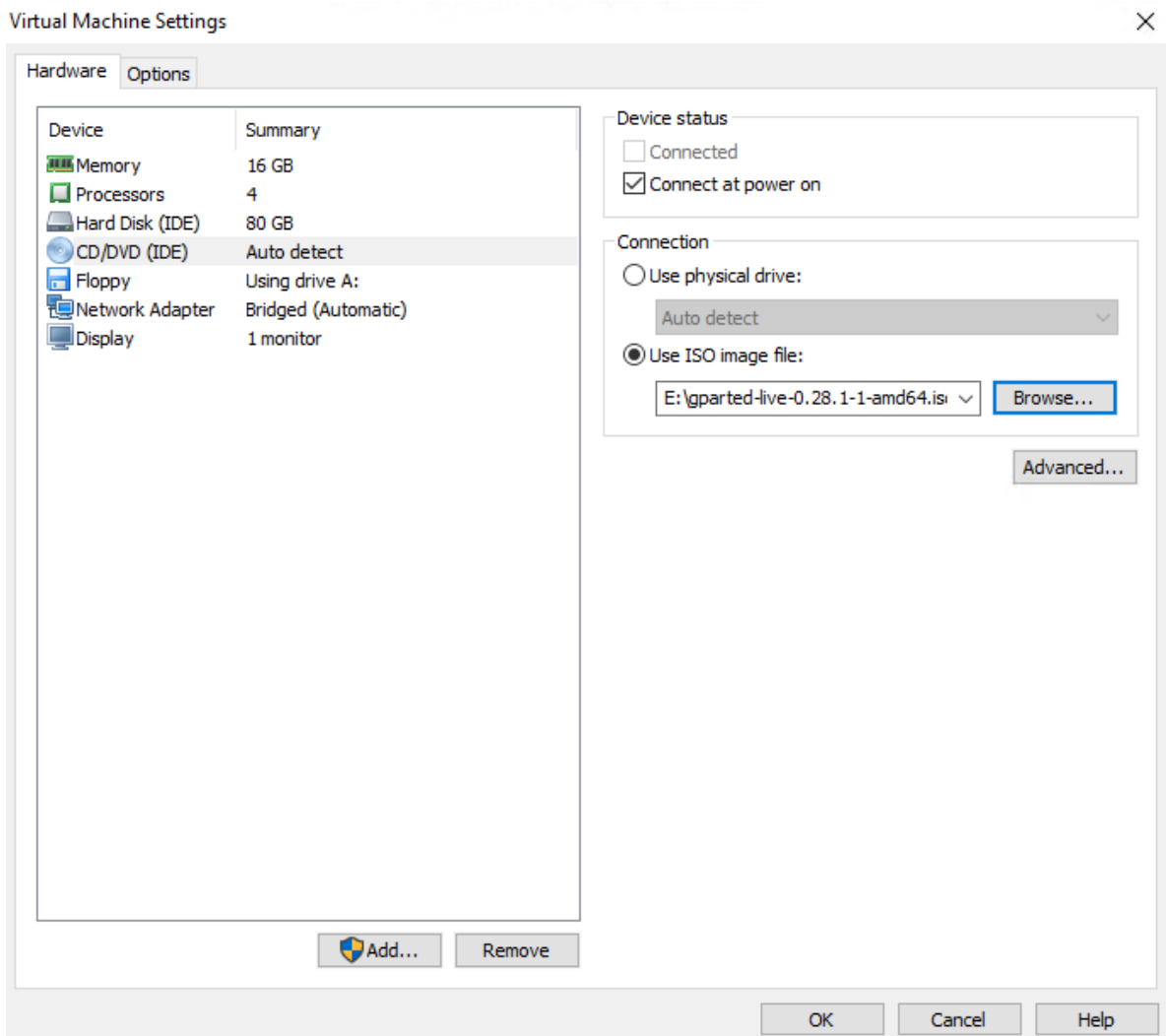
Download the Gparted Live CD from,

<http://gparted.org/livecd.php>

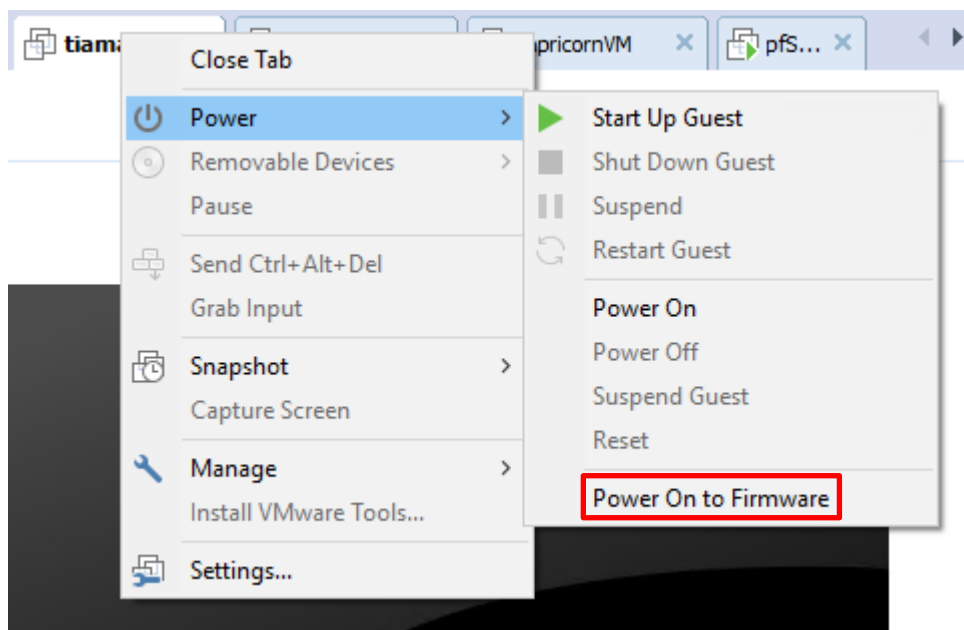
Expand the space allocated in VMware/ESXi



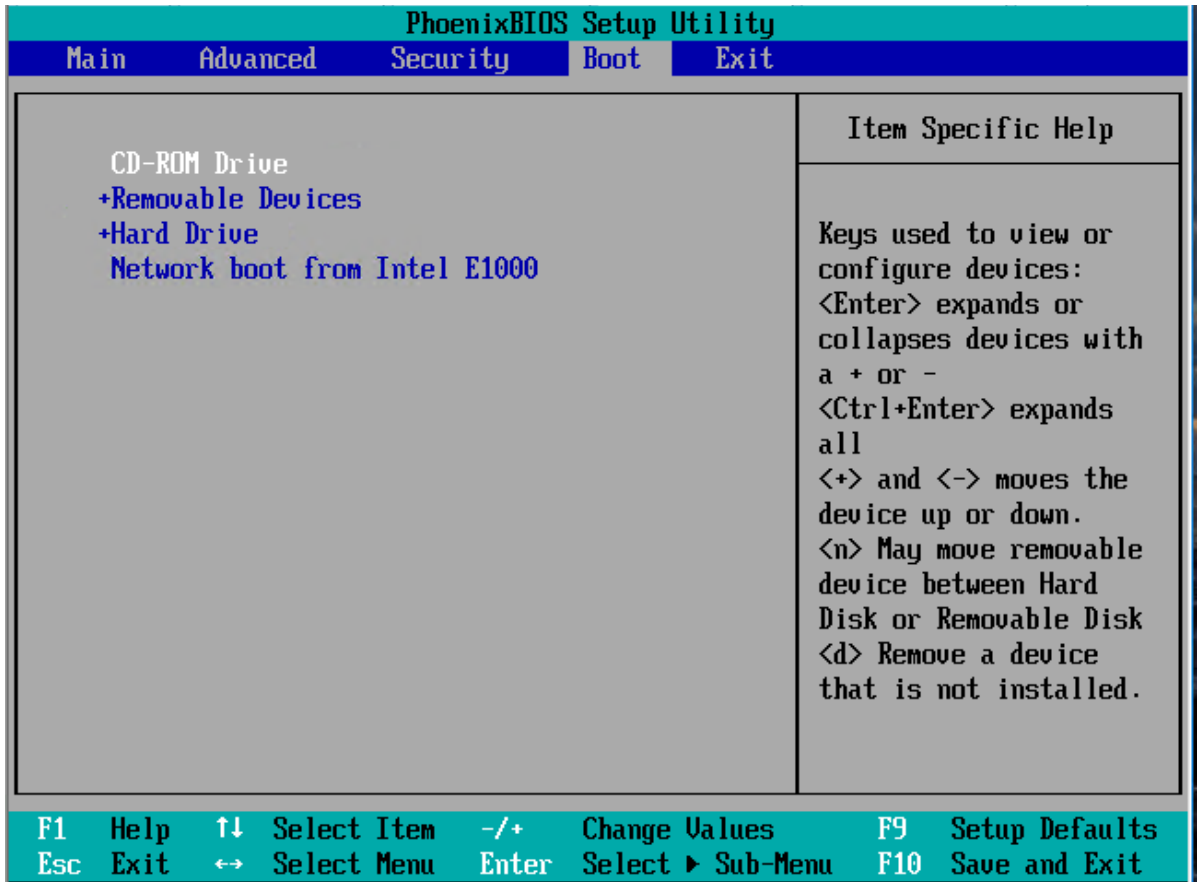
Attach the Gparted boot media to the VM CD/DVD drive.



Boot into the firmware interface of the VM



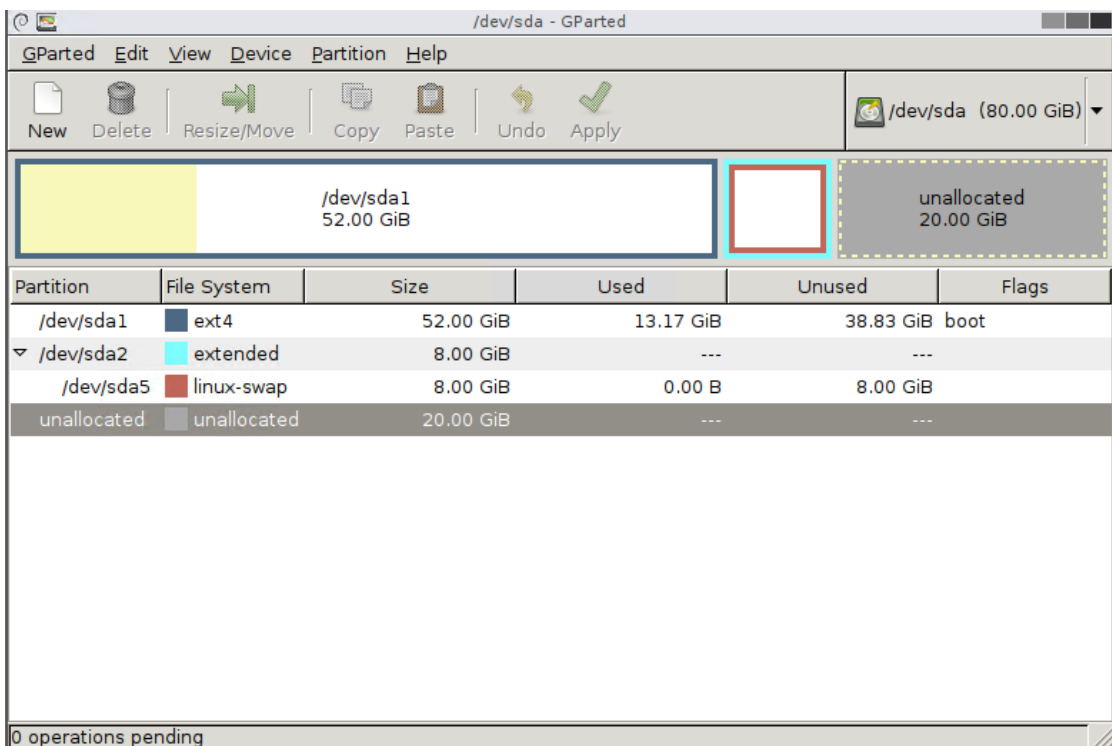
Change the boot order to prioritize the CD-ROM Drive containing Gparted, then Save and Exit.



The screenshot shows the PhoenixBIOS Setup Utility interface. The 'Boot' tab is selected, showing the boot order: CD-ROM Drive, +Removable Devices, +Hard Drive, and Network boot from Intel E1000. A help window on the right lists keys for navigating and configuring devices. The bottom of the screen contains a legend for keyboard shortcuts.

PhoenixBIOS Setup Utility			
Main	Advanced	Security	Boot
CD-ROM Drive +Removable Devices +Hard Drive Network boot from Intel E1000			Item Specific Help Keys used to view or configure devices: <Enter> expands or collapses devices with a + or - <Ctrl+Enter> expands all <+> and <-> moves the device up or down. <n> May move removable device between Hard Disk or Removable Disk <d> Remove a device that is not installed.
F1	Help	↑↓	Select Item
Esc	Exit	↔	Select Menu
-/+	Change Values		
Enter	Select	▶	Sub-Menu
F9	Setup Defaults		
F10	Save and Exit		

Press enter to ALL prompts accepting the default settings, and the following Gparted console will display after system has fully loaded.

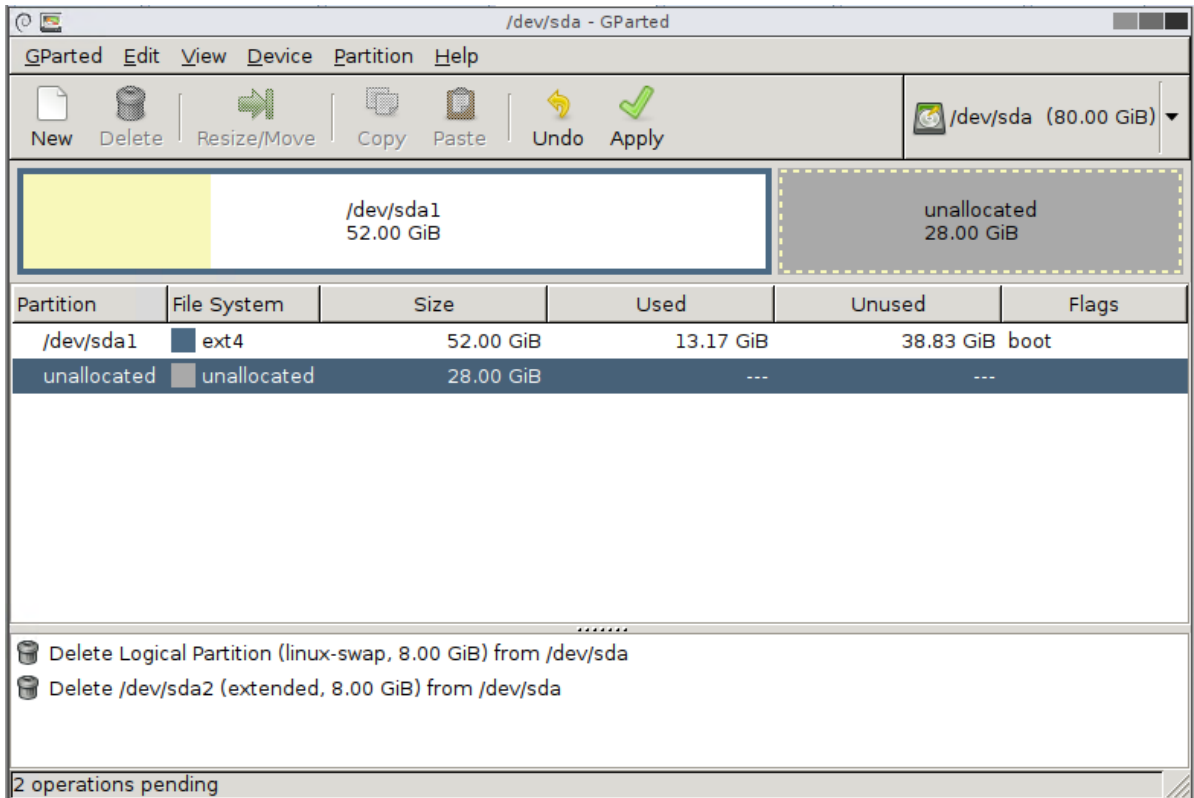


The screenshot shows the GParted application window. The main display shows a disk layout with a yellow partition (/dev/sda1, 52.00 GiB) and a grey unallocated area (20.00 GiB). A table below provides details for each partition.

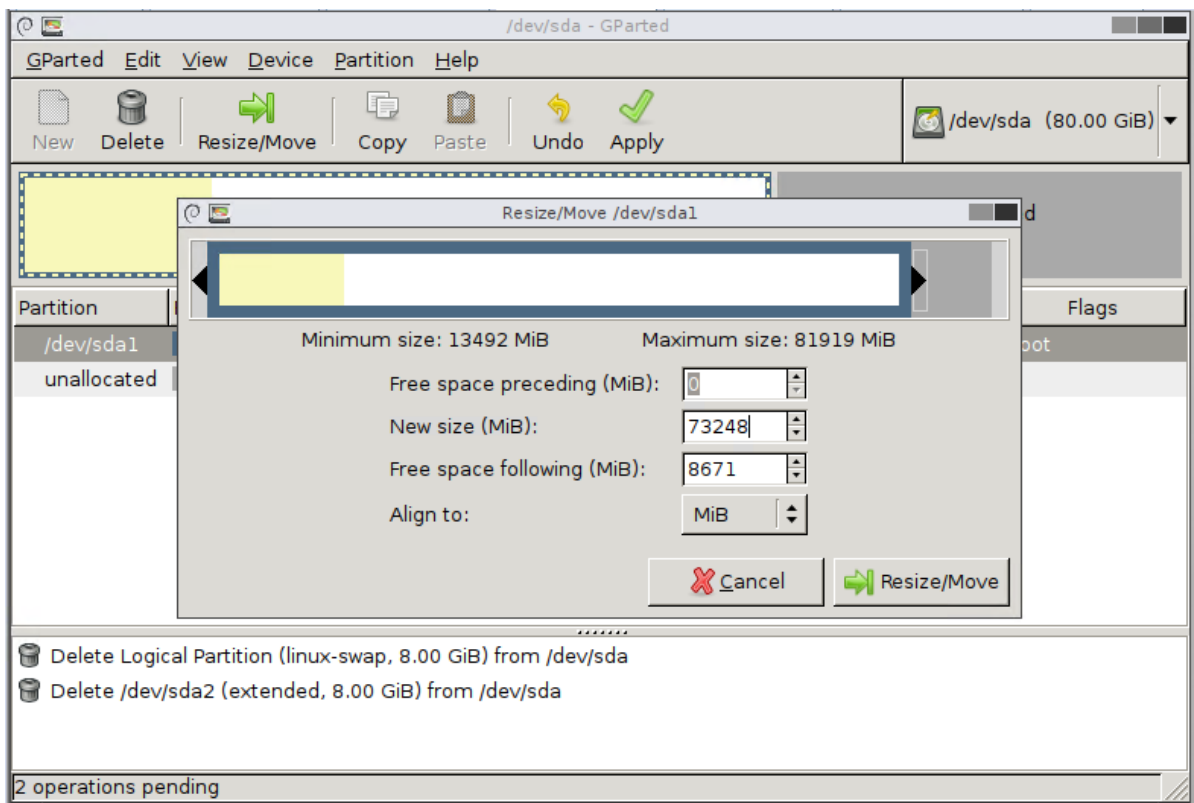
Partition	File System	Size	Used	Unused	Flags
/dev/sda1	ext4	52.00 GiB	13.17 GiB	38.83 GiB	boot
▼ /dev/sda2	extended	8.00 GiB	---	---	
/dev/sda5	linux-swap	8.00 GiB	0.00 B	8.00 GiB	
unallocated	unallocated	20.00 GiB	---	---	

0 operations pending

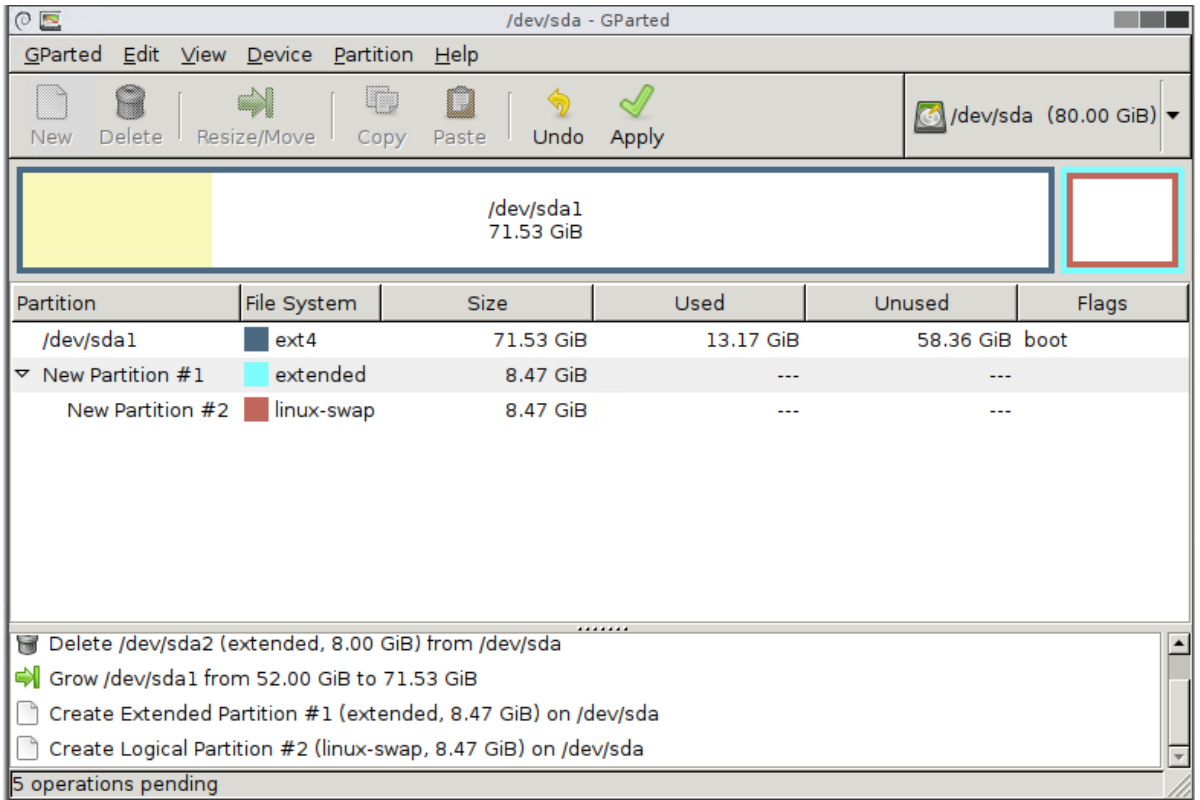
Delete the Swap and extended partitions (sda5 and sda2).



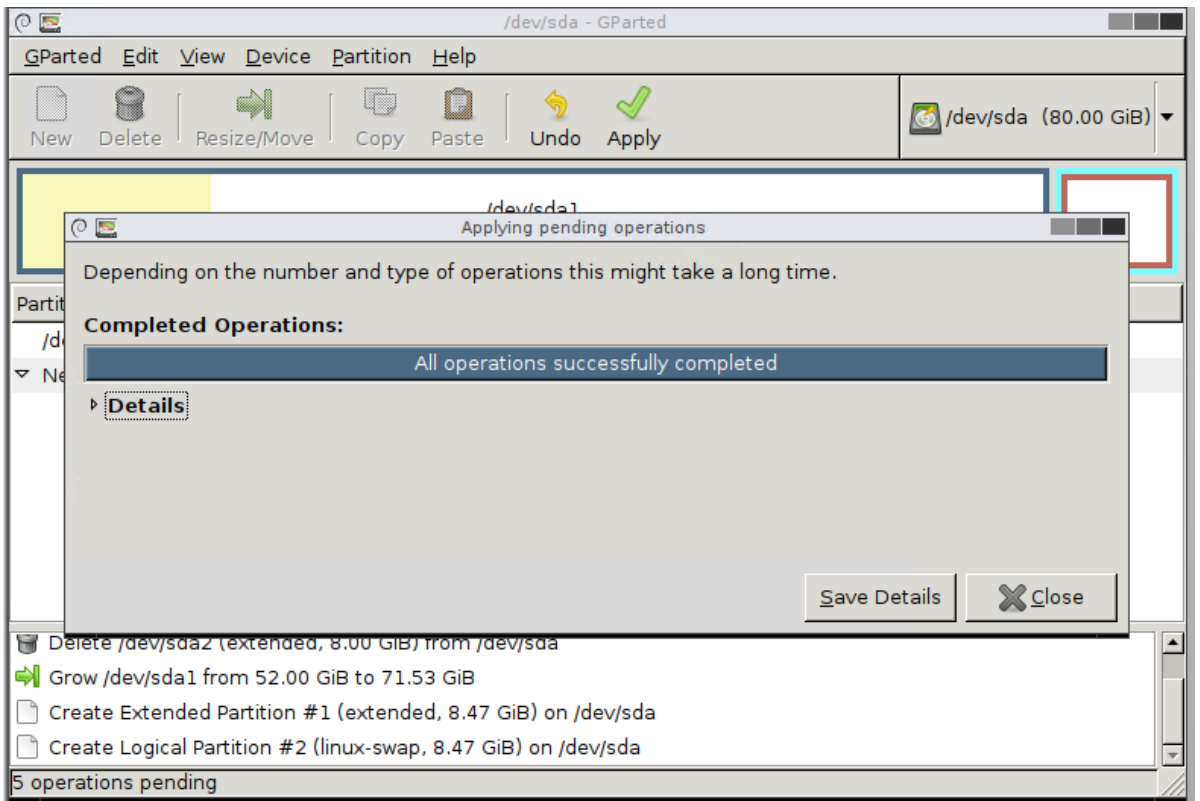
Resize the main partition ext4 (sda1) and expand it to the new size including the space made available when expanding the allocated size in VMware/ESXi.



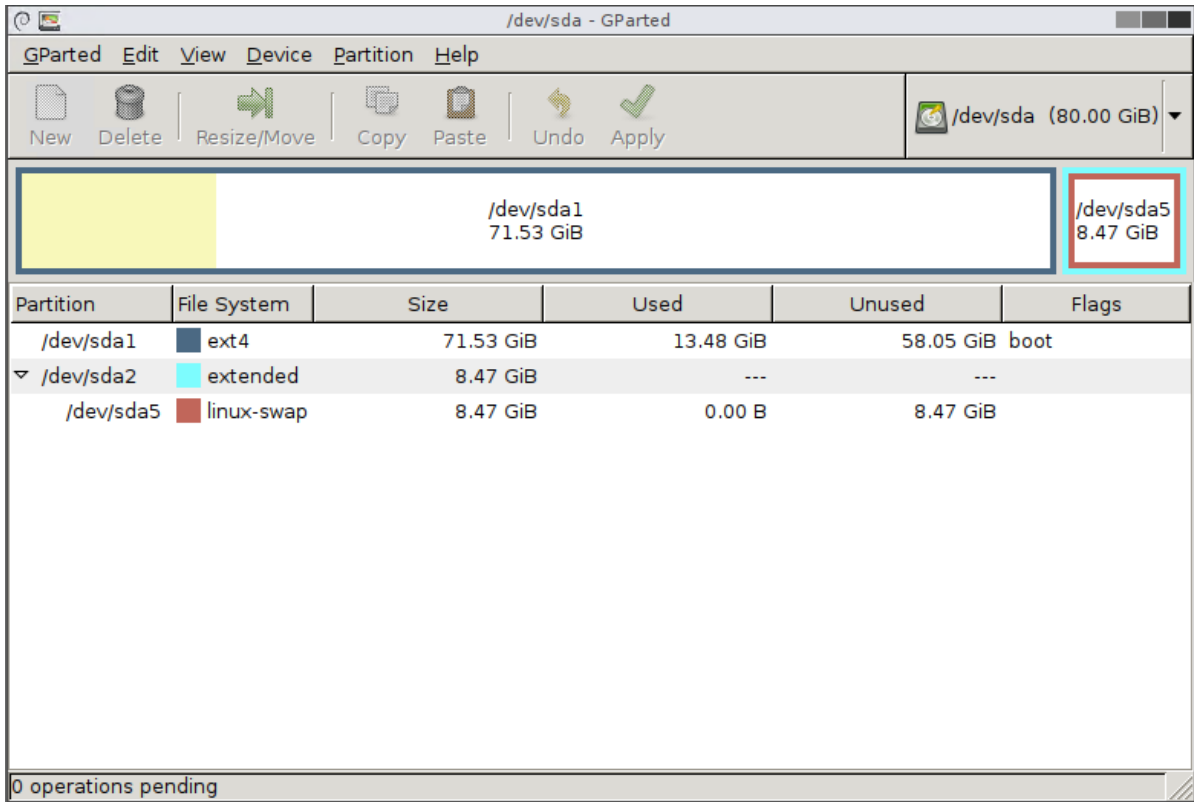
Remake the extended and linux-swap partitions with the remaining space.



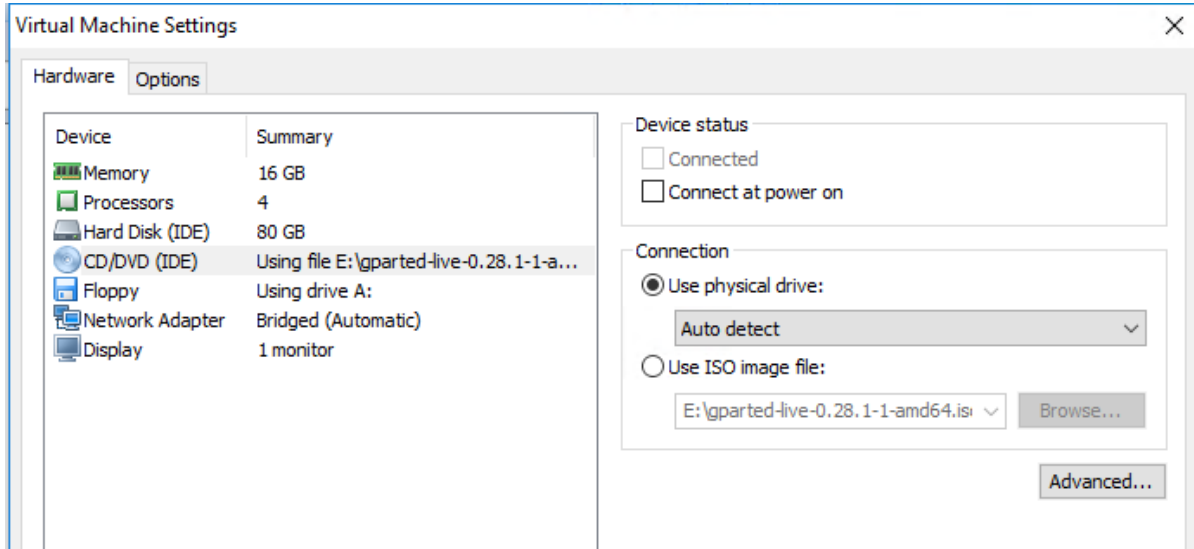
Click apply, then apply again and waiting for all operations to complete.



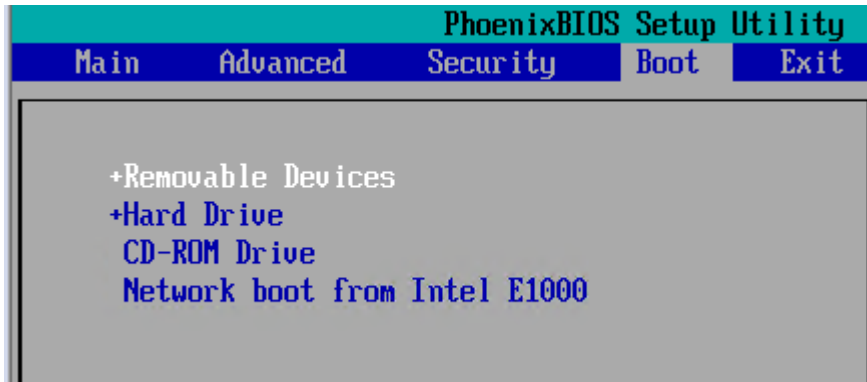
Now the partitions should look similar to the following.



Quit Gparted, shut down and remove the Gparted media from the machine.



Change the firmware settings boot options back to default settings, then save and exit.



Machine will reboot and start normally, double check rancher stack to make sure all containers started up and are running as expected.

ACTIVE ⏸ ⋮

makara

🔧 172.20.8.101 | 📡 17.09.0-ce

📦 Container Linux by CoreOS 1576.5.0 (4.14.11)

📊 2x2.2 GHz | 📦 7.79 GiB | 📦 47.1 GiB

makara=1

🏠 - siemonster-project-vagrant

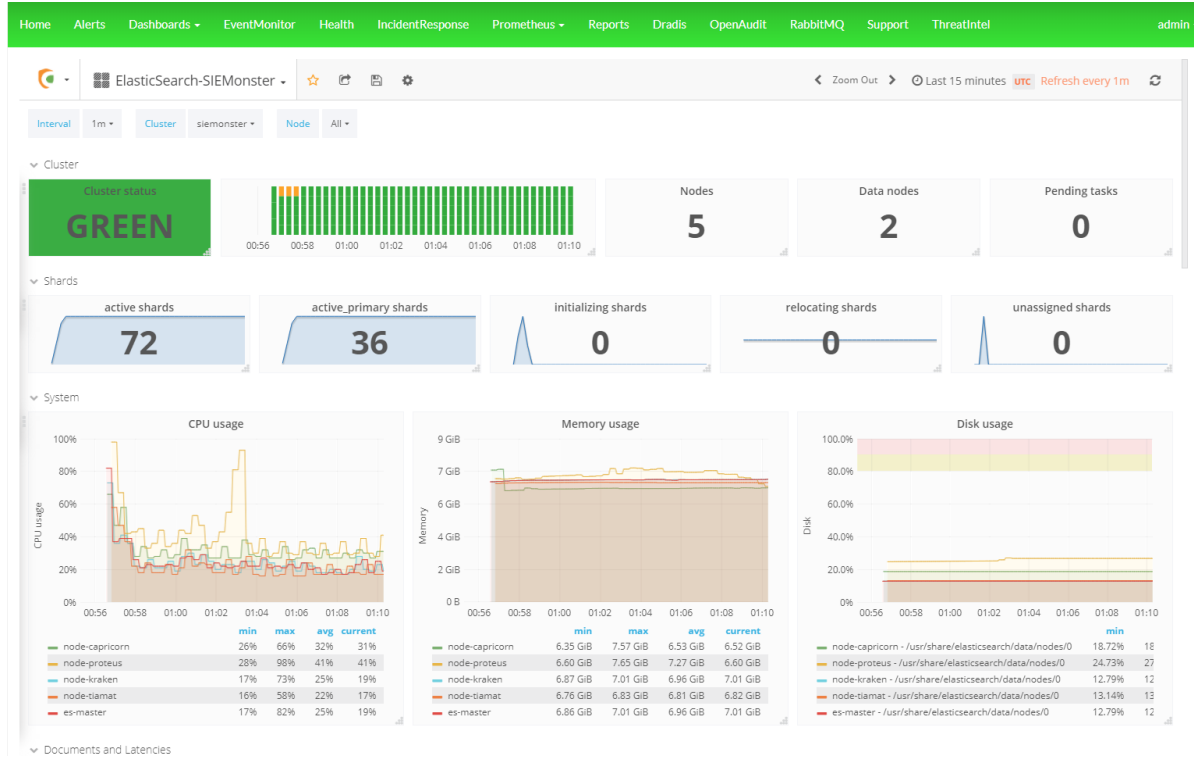
🟢 Active	411 + 1 Sidekick ⓘ
🟢 Active	alerta + 1 Sidekick ⓘ
🟢 Active	alertmanager ⓘ
🟢 Active	cadvisor ⓘ
🟢 Active	dradis ⓘ
🟢 Active	elastalert ⓘ
🟢 Active	es-client-1 ⓘ
🟢 Active	es-client-2 ⓘ
🟢 Active	es-data-node1 + 1 Sidekick ⓘ
🟢 Active	es-data-node2 + 1 Sidekick ⓘ
🟢 Active	es-master ⓘ
🟡 Started-Once	event ⓘ
🟢 Active	gmailrelay ⓘ
🟢 Active	grafana ⓘ
🟢 Active	ir ⓘ
🟢 Active	kibana ⓘ
🟢 Active	logstash-collector ⓘ
🟢 Active	logstash-collector-exporter ⓘ
🟢 Active	logstash-indexer ⓘ
🟢 Active	logstash-indexer-exporter ⓘ

17 TROUBLESHOOTING

How do I know if my ELK stack is up and running?

A health check dashboard is available to monitor stack health and detailed statistics.

Using the web interface, this is available on the health dashboard.



Health Check view

On the command line at the Proteus appliance cluster health may be found using the command:

- `curl -k https://elastic:elastic-password@localhost:9200/_cluster/health?pretty`

Where 'elastic-password' is the password allocated during deployment.

```
rancher@proteus ~ $ curl -k https://elastic:s13M0nSterV3@localhost:9200/_cluster/health?pretty
{
  "cluster_name" : "siemonster",
  "status" : "green",
  "timed_out" : false,
  "number_of_nodes" : 5,
  "number_of_data_nodes" : 2,
  "active_primary_shards" : 26,
  "active_shards" : 52,
  "relocating_shards" : 0,
  "initializing_shards" : 0,
  "unassigned_shards" : 0,
  "delayed_unassigned_shards" : 0,
  "number_of_pending_tasks" : 0,
  "number_of_in_flight_fetch" : 0,
  "task_max_waiting_in_queue_millis" : 0,
  "active_shards_percent_as_number" : 100.0
}
```

Curl output

I cannot see any incoming event logs/messages.

This issue usually arises when the message timestamp is incorrect or the remote device has the wrong time set. If you adjust the range back to 7 days, the messages might be visible.

18 CHANGING PASSWORDS

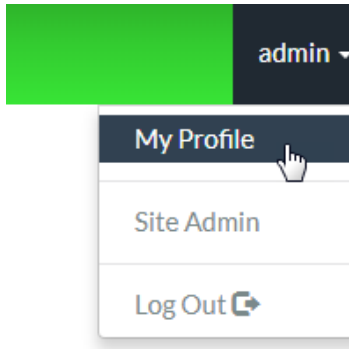
Once you are happy with your SIEM and it's in production it's time to lockdown the system. This includes changing all the default passwords not included at launch time. Below is a simple guide on changing the passwords on all the systems. Place these passwords in a safe place.

Linux passwords for root & rancher on all servers:

- sudo passwd root – sudo passwd rancher

Web Interface

- Go the My Profile option and enter new password twice to confirm



Security

Password

Requirements: 8 Characters in Length, upper and lower case letters, at least 1 number, at least 1 symbol

Current Password



New Password

Confirm Password

SAVE

FIR password: Login as admin to the FIR web interface and change within the user section

411: Once logged in go to the Users section:

SIEMonster-Alerts	Alerts	Searches	Groups	Users	Lists
Users					
Name					
	admin				
	demo				

Click on edit next to the user

SIEMonster-Alerts	Alerts	Searches	Groups	Users	Lists
User					
Username			Real Name		
<input type="text" value="admin"/>			<input type="text" value="Admin"/>		
New Password			Retype Password		
<input type="text"/>			<input type="text"/>		
Email			Admin		
<input type="text" value="demo@siemonster.com"/>			<input type="text" value="Yes"/>		
API Key					

Enter the new password twice.

Incident Response:

Navigate to IR Admin under the Incident Response menu and click the change password option to the right

Django administration
WELCOME, ADMIN. [VIEW SITE](#) / [CHANGE PASSWORD](#) / [LOG OUT](#)

Django administration

Home » Password change

Password change

Please enter your old password, for security's sake, and then enter

Old password:	<input style="width: 80%;" type="password"/>
New password:	<input style="width: 80%;" type="password"/>
New password confirmation:	<input style="width: 80%;" type="password"/>

Minemeld:

Click on the Admin menu item and then the password object:

