



Bare Metal **Build Guide**  
**January 2018**

Doc Version 1.8

## TABLE OF CONTENTS

|           |   |           |
|-----------|---|-----------|
| <b>1</b>  | <b>Authors Preface</b> .....                          | <b>3</b>  |
| <b>2</b>  | <b>Introduction</b> .....                             | <b>4</b>  |
| <b>3</b>  | <b>Build Installation Architecture Overview</b> ..... | <b>5</b>  |
| <b>4</b>  | <b>Version 3 Happy Snap Features</b> .....            | <b>6</b>  |
| <b>5</b>  | <b>ISO Image Builder Package</b> .....                | <b>14</b> |
|           | 5.1 ISO Image Creation Overview .....                 | 15        |
|           | 5.2 Preparing The ISO.....                            | 15        |
| <b>6</b>  | <b>Installation</b> .....                             | <b>17</b> |
|           | 6.1 CoreOS Install .....                              | 17        |
|           | 6.2 Rancher .....                                     | 18        |
|           | 6.3 Stack Deployment.....                             | 22        |
| <b>7</b>  | <b>Web Application Setup</b> .....                    | <b>26</b> |
| <b>8</b>  | <b>User Setup</b> .....                               | <b>28</b> |
|           | 8.1 User Roles .....                                  | 28        |
| <b>9</b>  | <b>Site Administration</b> .....                      | <b>31</b> |
|           | 9.1 Site Email .....                                  | 31        |
|           | 9.2 LDAP Settings.....                                | 31        |
| <b>10</b> | <b>Operational Overview</b> .....                     | <b>32</b> |
|           | 10.1 Log View.....                                    | 32        |
|           | 10.2 Shell Interaction .....                          | 33        |
| <b>11</b> | <b>Skedler Licensing</b> .....                        | <b>34</b> |

---

## 1 AUTHORS PREFACE

In 2015, one of our corporate clients told us of their frustrations with the exorbitant licensing costs of commercial Security Information and Events Management (SIEM) products. The customer light heartedly asked whether we could build them an open source SIEM to get rid of these annual license fees. We thought that was a great idea and set out so to develop a SIEM product for Managed Security Service Providers (MSSP's) and Security Professionals. This product is called SIEMonster.

SIEMonster Version 1 was released in late April of 2016 and a commercial release in November 2016. The release has been an astounding success without over 100,000 downloads of the product. We have assisted individuals and companies integrate SIEMonster into small medium and extra-large companies all around the world. SIEMonster with the help of the community and a team of developers have been working hard since the Version1 release incorporating what the community wanted to see in a SIEM as well as things we wanted to see in the next release.

Along the way we have signed up MSSP's from around the world who have contributed to the rollout of SIEMonster and in return they have assisted us with rollout scripts, ideas and things we hadn't even considered.

We are now proud to release the latest Version 3.0 Beta, and finalized in February 2018 for Alpha Release. We have added the following features to this release

- ELK Stack updated to version 5.5
- Built in Searchguard open source RBAC & encrypted node to node transport
- Wazuh HIDS system with Kibana plugin and OpenSCAP options & simplified agent registration process
- Simplified installation process for both Rancher Docker orchestration & SIEMonster web application
- All new dashboard with options for 2fa, site administration with user role based access and faster load times
- Built in parsers for most proprietary devices
- Preloaded Minemeld threat intel feeds integrated with log ingest out of the box.
- COREOS with NFS support

We have also automated correlation with Palo Alto MineMeld Open Source Threat Intelligence and added two factor authentication and easier rollouts.

The transition has now been completed to a full containerize all aspects of the SIEMonster application pool using the popular Docker system. This allows us to run on any hardware, cloud or operating system. It also provides the architecture for docker containers to be moved to other servers during downtime without affecting the SIEM.

We welcome you to try out our fully functional SIEM product, and if you wish to upgrade to our Premium version with Advanced Correlation, Reporting, Auditing and support please contact [sales@siemonster.com](mailto:sales@siemonster.com).

---

## 2 INTRODUCTION

SIEMonster Version 3 is built on the best open source components and custom develop from a wish list from the SIEMonster community. This document will cover the architecture, the features and the open source components that make up SIEMonster, so that all security professionals can run a SIEM in their organisations with no budget. If you would like more information about the architecture please see our High-Level Design.

SIEMonster is built on CoreOS, Docker with Rancher, Kubernetes orchestration. The product comes in Vbox, VMware, Bare-metal or Cloud install on AWS/Azure. SIEMonster can scale horizontally and vertically to support any enterprise client.

Some of these features include.

- OSINT from PaloAlto Minemeld.
- OSSEC Wazuh fork. Full integration with OSSEC Wazuh fork for Host Intrusion Detection and PCIDSS ruleset incorporated into Elastic.
- 411 demonstrated at DEFCON. Instant Incident Alerting via email or SMS or Console view via a secure portal and integration with “Slack”/“PagerDuty”/“Jira” using 411 Streams.
- Open Source AuditIT by Opmantek.
- Open Source Incident Response. Alerts maybe escalated as tickets to other operators or a whiteboard to show night shift analysts current issues.
- Elastalert, Event Monitor Alerting from the Guardian Newspaper.
- Data Correlation UI, community rulesets and dashboards, community and open source free plugins that make the SIEM.
- Incorporate your existing Vulnerability Scans into the Dashboard, (OpenVAS, McAfee, Nessus etc.)
- We have also developed and built in LDAP integration, advanced correlation and two factor authentication.

---

## 3 BUILD INSTALLATION ARCHITECTURE OVERVIEW

SIEMonster V3 cloud deployment is a modular Docker container system which will run on all operating systems supporting Docker. Architecturally this was chosen for portability across platforms, supporting not only most container platforms such as AWS ECS, Azure etc. but also VMWare, VirtualBox and bare metal installs used by our corporate customers. This will provide simplified upgrade paths and scaling potential as well as high availability.

Flexible deployment solutions include most cloud container platforms such as AWS, Azure, Digital Ocean etc. Also, options are available for VMware ESX and bare metal installs. For AWS deployment, the platform chosen is the open source container management system provided by Rancher Labs. Rancher supplies the entire software stack needed to manage containers in production. Rancher software consists of four major components:

### 1. INFRASTRUCTURE ORCHESTRATION

Rancher takes in raw computing resources from any public or private cloud in the form of Linux hosts. Each Linux host can be a virtual machine or physical machine. Rancher does not expect more from each host than CPU, memory, local disk storage, and network connectivity. From Rancher's perspective, a VM instance from a cloud provider and a bare metal server are indistinguishable.

Rancher implements a portable layer of infrastructure services designed specifically to power containerized applications. Rancher infrastructure services include networking, storage, load balancer, DNS, and security. Rancher infrastructure services are typically deployed as containers themselves, so that the same Rancher infrastructure service can run on any Linux hosts from any cloud.

### 2. CONTAINER ORCHESTRATION AND SCHEDULING

Many users choose to run containerized applications using a container orchestration and scheduling framework. Rancher includes a distribution of all popular container orchestration and scheduling frameworks today, including Docker Swarm, Kubernetes, and Mesos. The same user can create multiple Swarm or Kubernetes clusters. They can then use the native Swarm or Kubernetes tools to manage their applications.

In addition to Swarm, Kubernetes, and Mesos, Rancher supports its own container orchestration and scheduling framework called Cattle. Cattle was originally designed as an extension to Docker Swarm. As Docker Swarm continues to develop, Cattle and Swarm started to diverge. Rancher will therefore support Cattle and Swarm as separate frameworks going forward. Cattle is used extensively by Rancher itself to orchestrate infrastructure services as well as setting up, managing, and upgrading Swarm, Kubernetes, and Mesos clusters.

### 3. APPLICATION CATALOG

Rancher users can deploy an entire multi-container clustered application from the application catalog with one click of a button. Users can manage the deployed applications and perform fully automated upgrades when new versions of the application become available. Rancher maintains a public catalog consisting of popular applications contributed by the Rancher community. Rancher users can create their own private catalogs. With this deployment, custom Rancher catalog applications have been created for the SIEMonster stack. Using the Rancher network overlay, the SIEMonster container application loads have been evenly balanced across four nodes.

### 4. ENTERPRISE-GRADE CONTROL

Rancher supports flexible user authentication plugins and comes with pre-built user authentication integration with Active Directory, LDAP, and GitHub. Rancher supports Role-Based Access Control (RBAC) at the level of environments, allowing users and groups to share or deny access to, for example, development and production environments.

## 4 VERSION 3 HAPPY SNAP FEATURES

All new mobile friendly interface



Sign In

|                     |   |
|---------------------|---|
| Email Address       | <input type="text" value="Email"/>        |
| Password            | <input type="password" value="Password"/> |
| Authentication Code | <input type="text" value="Optional"/>     |

My Profile / 2FA Settings

### Two Factor Authentication

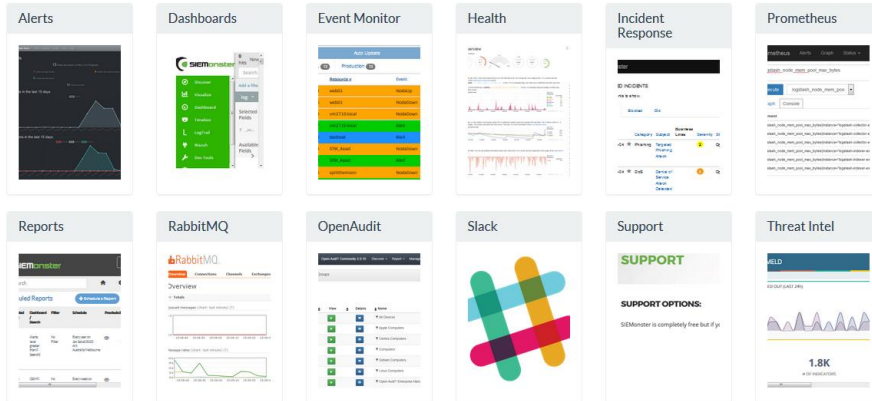
Disabled



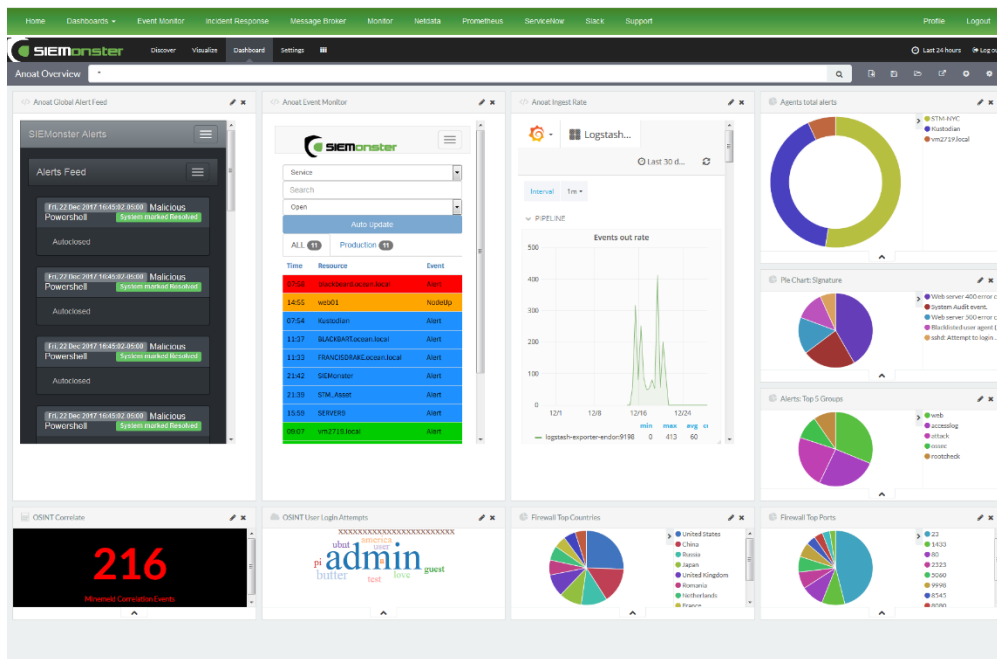
You can use Google Authenticator, Authy, or Symantec's VIP Access to scan this QR code and generate authentication codes.

Secret Key: IU2T4KTGLVFDGI3UJ4XTE6TRLMZGSSKRGAUXMR2KJR6W6V2HEUUA

## Updated fast loading dashboard

## Pre-Configured Dashboards



The dashboard displays several key components:

- Alerts Feed:** A list of alerts including 'Malicious Powershell' and 'System marked Restricted'.
- Global Alert Feed:** A large red number '216' indicating the total number of minimal correlation events.
- OSINT Correlator:** A visualization showing correlations between various entities.
- Event Monitor:** A table showing event details with columns for Time, Resource, and Event.
- Logstash Pipeline:** A line chart showing 'Events out rate' over time.
- Agents total alerts:** A donut chart showing the distribution of alerts across different agents.
- Alerts: Top 5 Groups:** A pie chart showing the top 5 groups of alerts.
- Firewall Top Countries:** A pie chart showing the top countries for firewall events.
- Firewall Top Ports:** A pie chart showing the top ports for firewall events.

## Role based access control with LDAP integration

# LDAP Integration Settings

You can integrate with LDAP services for user authentication. Users not already in the SIEMonster system will be automatically added when logging in with their LDAP email address and password.

Hostname or IP Address (required)

Port

TLS

Enabled

Connection Timeout

Service Account Username (required)

# User Roles

User Roles are used to allow access to different components within the SIEMonster system. Users can be assigned to multiple roles if needed.

| Name                  |
|-----------------------|
| <a href="#">admin</a> |
| <a href="#">user</a>  |

# Users

Manage which users have access to SIEMonster including password resets, roles assigned to users, and other information.

| Display Name          | Role                  | Email Address  |
|-----------------------|-----------------------|--|
| <a href="#">admin</a> | <a href="#">admin</a> | <a href="mailto:admin@siemonster.com">admin@siemonster.com</a> |

Password Requirements:



## Customizable Dashboards

### Dashboards

|                  |                                    |          |
|------------------|------------------------------------|----------|
| Apache           | Enabled (read only for Admin role) | Settings |
| Cisco            | Enabled (read only for Admin role) | Settings |
| HP Event Monitor | Enabled (read only for Admin role) | Settings |
| Palo Alto        | Enabled (read only for Admin role) | Settings |
| SOC Demo         | Enabled (read only for Admin role) | Settings |
| Ossec Alerts     | Enabled (read only for Admin role) | Settings |
| PCI Compliance   | Enabled (read only for Admin role) | Settings |
| Bro Connection   | Enabled (read only for Admin role) | Settings |
| Nessus           | Enabled (read only for Admin role) | Settings |

|                |     |                  |
|----------------|-----|------------------|
| Dashboard Name | Url | Create Dashboard |
|----------------|-----|------------------|

Delete Role (not available for Admin Role)

## Raw Log searches

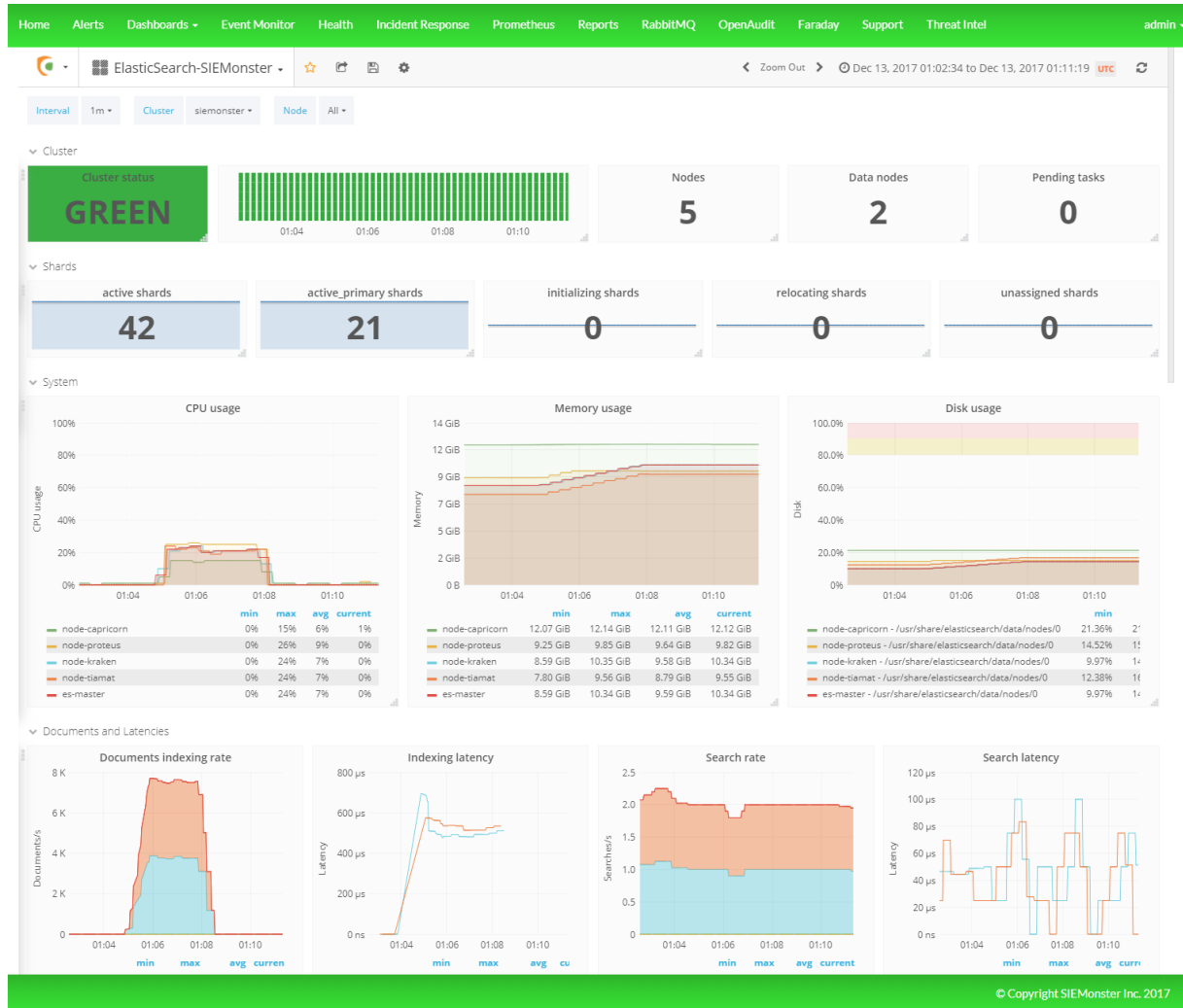
The screenshot shows the SIEMonster interface with a search for "wazuh-alerts\*" on December 13th, 2017. The search results are visualized as a histogram and a list of log entries. The histogram shows a peak in activity around 16:45:24.000. The log entries include details such as agent IP, rule ID, rule level, rule description, and the decoded message.

```

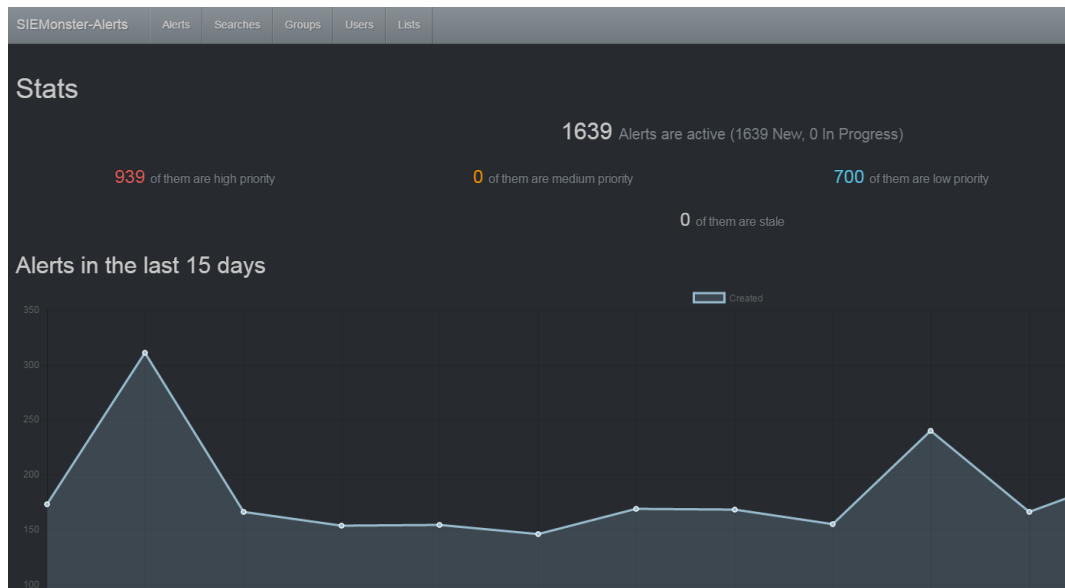
agent.ip: 172.93.49.114 agent.name: STM-NYC agent.id: 004 srcip: 52.170.201.5 manager.name: vn2719.local
rule.firetimes: 1 rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.description: web server 500 error code (Internal Error).
rule.groups: web, accesslog, system_error rule.id: 31122 decoder.name: web-accesslog type: wazuh-alerts
uri: /?author=1 full_log: 52.170.201.5 - - [12/Dec/2017:23:18:54 -0500] "GET /?author=1 HTTP/1.1" 500 3
047 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:48.0) Gecko/20101001 Firefox/48.0" tags: messageQ

agent.ip: 172.93.49.114 agent.name: STM-NYC agent.id: 004 srcip: 178.210.90.90 manager.name: vn2719.local
rule.firetimes: 1 rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.description: web server 400 error code.
rule.groups: web, accesslog, attack rule.id: 31101 decoder.name: web-accesslog type: wazuh-alerts
uri: /wp-active.php full_log: 178.210.90.90 - - [12/Dec/2017:22:56:16 -0500] "GET /wp-active.php HTTP/1.1" 404 44375 "http://site.ru" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; AppleWebKit/533.4 (KHTML
agent.ip: 172.93.49.114 agent.name: STM-NYC agent.id: 004 srcip: 91.200.12.7 manager.name: vn2719.local
rule.firetimes: 2 rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.description: web server 400 error code.
rule.groups: web, accesslog, attack rule.id: 31101 decoder.name: web-accesslog type: wazuh-alerts
uri: /wp-comments-post.php full_log: 91.200.12.7 - - [12/Dec/2017:22:10:25 -0500] "POST /wp-comments-post.php HTTP/1.1" 429 3280 "http://www.
agent.ip: 93.123.73.13 agent.name: Kustodian agent.id: 002 srcip: 172.68.182.230 manager.name: vn2719.local
rule.firetimes: 1 rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.description: web server 400 error code.
rule.groups: web, accesslog, attack rule.id: 31101 decoder.name: web-accesslog type: wazuh-alerts
uri: /wp-content/plugins/nav-menus.php full_log: 172.68.182.230 - - [13/Dec/2017:02:55:51 +0000] "GET /wp-content/plugins/nav-menus.php HTTP/1.1" 404 29758 "http://site.ru" "Mozilla/5.0 (Windows; U; Windows
agent.ip: 93.123.73.13 agent.name: Kustodian agent.id: 002 srcip: 197.0.114.74 manager.name: vn2719.local
rule.firetimes: 4 rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.description: web server 400 error code.
rule.groups: web, accesslog, attack rule.id: 31101 decoder.name: web-accesslog type: wazuh-alerts
uri: /wp-login.php full_log: 197.0.114.74 - - [13/Dec/2017:03:53:09 +0000] "GET /wp-login.php HTTP/1.1" 403 690 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1" tags: messageQue
agent.ip: 172.93.49.114 agent.name: STM-NYC agent.id: 004 srcip: 91.200.12.106 manager.name: vn2719.local
rule.firetimes: 3 rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.description: web server 400 error code.
rule.groups: web, accesslog, attack rule.id: 31101 decoder.name: web-accesslog type: wazuh-alerts
uri: /wp-comments-post.php full_log: 91.200.12.106 - - [12/Dec/2017:22:10:25 -0500] "POST /wp-comments-
  
```

## Full Stack Monitoring



## Alerting



## Wazuh HIDS Integration

| ID    | File                   | Description  | Groups                         | Requirement          | Level |
|-------|------------------------|--|--------------------------------|----------------------|-------|
| 31166 | 0245-web_rules.xml     | Shellshock attack detected   | attack, web, accesslog         | 11.4                 | 15    |
| 40501 | 0280-attack_rules.xml  | Attacks followed by the addition of an user.   | syslog, elevation_of_privilege | 10.2.7, 10.6.1, 11.4 | 15    |
| 80006 | 0340-puppet_rules.xml  | Puppet Master: not run - address in use  | puppet                         |                      | 15    |
| 5707  | 0095-sshd_rules.xml    | sshd: OpenSSH challenge-response exploit.  | exploit_attempt, syslog, sshd  | 11.4, 6.2            | 14    |
| 5714  | 0095-sshd_rules.xml    | sshd: SSH CRC-32 Compensation attack   | exploit_attempt, syslog, sshd  | 11.4, 6.2            | 14    |
| 11209 | 0175-proftpd_rules.xml | proftpd: Attempt to bypass firewall that can't adequately keep state of FTP traffic. | syslog, proftpd                | 10.6.1, 11.4         | 14    |

## Threat Intel

**MINEMELD**

**SECTION**

- 4 MINERS
- 1 PROCS
- 3 OUTPUTS

**2.7K**  
# OF INDICATORS

**MINERS**

- 900 # OF INDICATORS
- 901 ADDED
- 1 AGED OUT

# OF INDICATORS (LAST 24h)

## Vulnerability Management

**Dradis CE**

Home Alerts Dashboards Event Monitor Health Incident Response Prometheus Reports Dradis OpenAudit RabbitMQ Support Threat Intel Demo admin

Upload Manager

Use the form below to upload output files from other tools.

1. Choose a tool

- Dradis:Plugins:Acunetix
- Dradis:Plugins:Acunetix
- Dradis:Plugins:Brakeman
- Dradis:Plugins:Burp
- Dradis:Plugins:Metasploit
- Dradis:Plugins:NTOSpider
- Dradis:Plugins:Nessus
- Dradis:Plugins:Nexpose
- Dradis:Plugins:Niko
- Dradis:Plugins:Nmap
- Dradis:Plugins:OpenVAS
- Dradis:Plugins:Projects:Upload:Package
- Dradis:Plugins:Projects:Upload:Template
- Dradis:Plugins:Qualys
- Dradis:Plugins:Zap

## Event Monitor

Service:  Search:  Open:  Auto Update

ALL 29 Production 29

| Severity | Status | Last Receive Time | Dupl. | Environment | Service    | Resource               | Event               | Value     | Text   |
|----------|--------|-------------------|-------|-------------|------------|------------------------|---------------------|-----------|--|
| Major    | Open   | Sun 27 Nov 17:04  | 1     | Production  | Website    | web01                  | NodeUp              | AWESOME   | Web server is UP.                                |
| Major    | Open   | Sat 22 Oct 17:26  | 9     | Production  | HIDS       | STM_AGENT              | Intrusion Attempt   | ATTACK    | System user successfully logged to the system.   |
| Major    | Open   | Sun 9 Oct 09:50   | 12    | Production  | Powershell | blackbeard.ocean.local | Powershell Activity | DETECTION | Malicious Powershell Activity                    |
| Major    | Open   | Thu 29 Sep 03:11  | 19    | Production  | Powershell | VPS-2F1-E1-11B         | Powershell Activity | DETECTION | Malicious Powershell Activity                    |
| Major    | Open   | Thu 25 Aug 22:36  | 3     | Production  | HIDS       | KUSTODIAN              | Intrusion Attempt   | ATTACK    | Multiple common web attacks from same source ip. |
| Major    | Open   | Fri 17 Jun 09:24  | 0     | Production  | Website    | localhost              | NodeDown            | ERROR     | Web server is down.                              |

## Reporting

Home Alerts Dashboards Event Monitor Health Incident Response Prometheus Reports RabbitMQ OpenAudit Faraday Support Threat Intel admin

SIEMonster Scheduled Reports Filters Templates

Search

BACK MAIL NOW SAVE

### Create Report

#### Report Details

Schedule Report Name\*

Select Type\*

Select Search\*  Select Filter

Folder Path

#### Report Format

Select Format\*

#### Schedule Details

Frequency Type\*  runs every  hours which starts from next  th (0-59) minute in America/New\_York

Time Window

From\*  To

© Copyright SIEMonster Inc. 2017

## Audit and Discovery

Home Alerts Dashboards ▾ Event Monitor **Queries** Incident Response Prometheus Reports Dradis OpenAudit RabbitMQ Support Threat Intel Demo admin

Home / Queries  
Queries

Queries Export▾ Create Advanced Filter ?

50 records per page Search:

| View ▲ | Details | Name                        | Description   | Organisation         | Delete |
|--------|---------|-----------------------------|---|----------------------|--------|
|        |         | Acrobat                     | Adobe Acrobat installations (software name contains 'acrobat' or 'adobe reader').   | Default Organisation |        |
|        |         | AD Controllers              | Active Directory Domain Controllers   | Default Organisation |        |
|        |         | Antivirus                   | Installed AntiVirus software (software name contains 'virus' or 'trend micro' or 'endpoint').                                 | Default Organisation |        |
|        |         | Audit Dates                 | The first and last times a device was audited.  | Default Organisation |        |
|        |         | Billing Report              | Name, last seen on and by, type, class, manufacturer, model, serial, user, location.  | Default Organisation |        |
|        |         | Consumed IP Addresses       | The ip addresses used by a group.   | Default Organisation |        |
|        |         | Database                    | All databases.  | Default Organisation |        |
|        |         | Device                      | Icon, name, ip address, manufacturer, model, serial.  | Default Organisation |        |
|        |         | Devices Without Credentials | Device details - name, ip, last seen on and by for those devices only discovered by Nmap and have therefore not been audited. | Default Organisation |        |

Upgrade to Premium for more advanced features including full reporting, customizations, upgrades and support – [sales@siemonster.com](mailto:sales@siemonster.com)

## 5 ISO IMAGE BUILDER PACKAGE

The SIEMonster team have put together a package to allow for a fully customizable ISO installation for use with bare metal deployments.

This option allows you to build your own ISO installers, this will allow you to hard set IP addresses, proxies, disk size before you build. This is a good option for most corporate environments.

Building the ISO using the default settings will build a DHCP based cluster, perfect for a quick POC deployment.

The SIEMonster ISO Image provides the means to quickly rollout a cluster using bare metal servers of your choice comprising the base build for all 5 servers required.

The five servers are comprised of

- Proteus (Application Server/Ingestion Server)
- Capricorn (Application Server)
- Kraken (Elasticsearch)
- Tiamat (Elasticsearch)
- Makara (Rancher / Orchestration Server / Ingestion Server)

System requirements should allow for 8GB RAM for each instance and minimum 250GB free disk space, (50GB per instance). Supported build platforms:

- Mac OS X
- Ubuntu
- Debian
- CentOS

## 5.1 ISO IMAGE CREATION OVERVIEW

The high-level overview of the image building process is set out below.

- Download the package from the SIEMonster website using the ImageBuilder link
- Edit the config file for static IP range, Proxy and Disk Size, Memory & Credentials
- Run the ISO builder script to create the ISO file

The goal of this project is to create an ISO image, through which a user can deploy a 5-node Rancher SIEMonster cluster. Customizations:

- Static IP Range Assignment
- Proxy
- Gateway
- DNS
- SSH Password
- Rancher Username
- Rancher Password

## 5.2 PREPARING THE ISO

1. Click on Download on the SIEMonster website, register and Download the latest SIEMonster ImageBuilder package.  
SHA256 3b3bd1d6b0371bceef916b11196af97bd8095299159013c519d33108fcd1e9d1
2. Target system Ubuntu/Debian.

**Prerequisites:**

```
sudo apt install python-pip
pip install j2cli
sudo apt-get install genisoimage
```

Target system MAC OSX.

**Prerequisites:**

```
sudo apt install python-pip
pip install j2cli
brew install cdrtools
```

Target System CentOS

**Prerequisites:**

```
yum install python-pip
pip install j2cli
```

**Configure:**

```
cp ova_params.sh.example ova_params.sh
Edit ova_params.sh – see example below
chmod +x *.sh
```

**Build:**

```
./build_iso.sh
```

Example ova\_params.sh template: Note – Setting STATIC\_ENABLE to 0 will build DHCP based image.

```
#!/bin/bash

export COREOS_PASSWORD='s13M0nSterV3'

# Proxy configuration
export HTTP_PROXY='http://user:mypassword@10.0.1.17:8888'
# NO_PROXY always MUST contains localhost,127.0.0.1
export NO_PROXY='localhost,127.0.0.1,.mycompany.com'

# Static ip configuration
export STATIC_ENABLE='1'
export STATIC_IPS='(192.168.0.150 192.168.0.151 192.168.0.152 192.168.0.153 192.168.0.154)'
export STATIC_NETMASK='255.255.255.0'
export STATIC_GATEWAY='192.168.0.1'
export STATIC_DNS='192.168.0.1'

# Rancher Webb UI
export RANCHER_ADMIN_NAME='admin'
export RANCHER_ADMIN_USERNAME='admin'
export RANCHER_ADMIN_PASSWORD='s13M0nSterV3'
export RANCHER_NFS_ON_REMOVE='purge'

# Docker images
export AVAHI_DOCKER_IMAGE='registry.gitlab.com/siemonster/siemonster-avahi-rancher:master'
export CONSUL_DOCKER_IMAGE='consul:1.0.0'
export RANCHER_SERVER_DOCKER_IMAGE='rancher/server:v1.6.12'
export RANCHER_AGENT_DOCKER_IMAGE='rancher/agent:v1.2.7'

export BOOTSTRAP_EXPECT='5'
```



## 6 INSTALLATION

The ISO Image deployment overview contains the following steps.

- Creation of SIEMonster ISO Image and transfer to disk
- Install CoreOS, then deploy using ISO configdrive option
- Automatic Rancher cluster deployment with credentialed access
- NFS creation for configuration centralization
- SSL certificate insertion
- SIEMonster Catalog item for one click install

### 6.1 COREOS INSTALL

First download the latest stable bootable CoreOS ISO file:

<https://coreos.com/os/docs/1662.0.0/booting-with-iso.html>

Burn the image to disk or transfer to bootable USB and boot the server from this image.

Once loaded the system will auto login:

```
This is localhost (Linux x86_64 4.14.11-coreos) 08:28:36
SSH host key: SHA256:Fh4f2jgWJ31ZaXIPi7x67zrZz7817qtgWRv5eiDRyxY (ED25519)
SSH host key: SHA256:Vpi6q0g9GtWR1PhFjBBgqQRp5MUMJZoJPYnCKtzF2eA (ECDSA)
SSH host key: SHA256:BUzh8CAX5sR1g7zjFdhZQv+BnRkLq+Unmb01UJUHTaQ (DSA)
SSH host key: SHA256:5ep1GxJKX1oyDrIjodU779bUD9h/itEjkzWqGcLwkW4 (RSA)
ens33: fe80::20c:29ff:fef8:9c26

localhost login: core (automatic login)
Container Linux by CoreOS stable (1576.5.0)
Update Strategy: No Reboots
core@localhost ~$ _
```

To ensure network connectivity, internet access, and for any troubleshooting purposes it is recommended to configure networking and access settings.

Copy a pre-configured cloud-config.yaml using SCP from a server accessible to the CoreOS install.

An example file can be found here:

<https://raw.githubusercontent.com/siemonster/misc/master/cloud-config.yaml>

Username is 'core', password is 'coreos' – adjust network settings to suit environment.

E.g. `scp siemonster@10.0.0.100:/home/siemonster/cloud-config.yaml .`  
(Notice the final .)

Run the CoreOS installer:

`coreos-install -d /dev/sda -C stable -c cloud-config.yaml`

Successful completion:

```
[ 190.264945] GPT:9289727 != 33554431
[ 190.264990] GPT:Alternate GPT header not at the end of the disk.
[ 190.265053] GPT:9289727 != 33554431
[ 190.265097] GPT: Use GNU Parted to correct GPT errors.
[ 190.265165] sda: sda1 sda2 sda3 sda4 sda6 sda7 sda9
Success! CoreOS Container Linux stable 1576.5.0 is installed on /dev/sda
core@localhost ~ $ _
```

Shutdown the server.

Remove the CoreOS install media and replace with the SIEMonster ISO image created in section 5.

Get to this stage with the remaining 4 servers, ensuring each server has a unique IP address set in the cloud-config file.

Start each server in turn and then wait for 20-30 minutes for the cluster to be built.

To monitor progress, SSH to any server and run 'docker ps' to show running containers. The first container will be the AVAHI image which detects and configures all nodes.

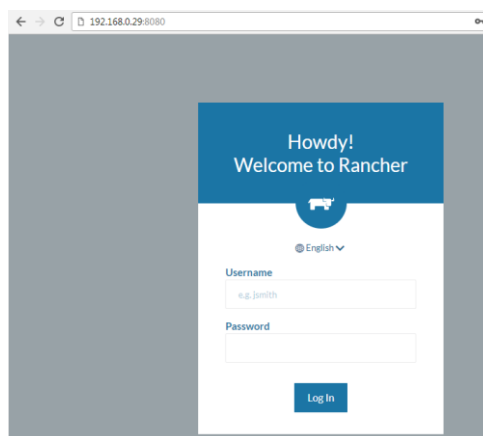
The next container to run will be the Consul image, which sets up the Rancher cluster.

Running 'docker logs -f <containerID>' will show the container activity.

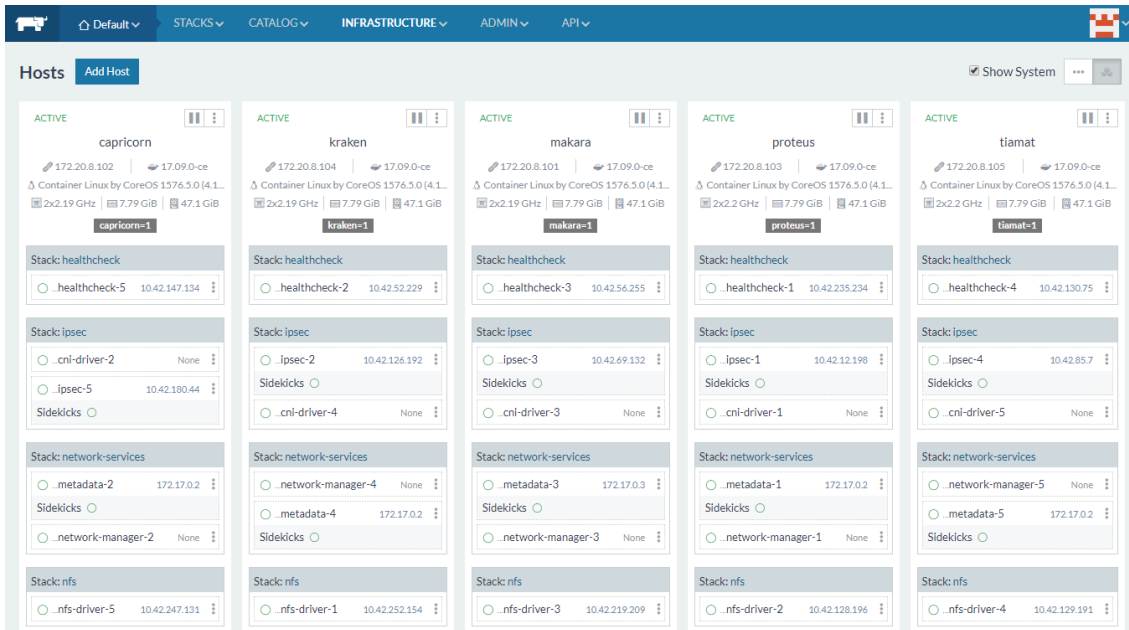
Once completed, the new hostnames will appear in a terminal session. Locate the host 'Makara' and identify the IP address. This will be the URL for the Rancher Server. SSH login to these hosts will now be with the credentials configured during the ISO build creation.

## 6.2 RANCHER


1. Using Firefox/Chrome/Safari open the Rancher server URL using port 8080, e.g. <http://192.168.0.29:8080>



2. Login with the configured credentials (default admin/s13M0nSterV3 if not changed during the ISO creation process), and navigate to Infrastructure – Hosts



- Next navigate to Stacks – Infrastructure and ensure that all services are green before proceeding.



| Stack Name       | Status     | Services | Containers | Actions |
|------------------|------------|----------|------------|---------|
| healthcheck      | Up to date | 1        | 5          | ⚙️      |
| ipsec            | Up to date | 2        | 15         | ⚙️      |
| network-services | Up to date | 2        | 15         | ⚙️      |
| nfs              | Up to date | 1        | 5          | ⚙️      |
| scheduler        | Up to date | 1        | 1          | ⚙️      |

- As the access to the web application is via SSL only, certificates are required to be generated for the chosen local domain. A sample template, 'openssl.cnf' and script (generate\_certs.sh) to generate certificates can be found at <https://github.com/siemonster/misc>. If using Windows, copy these files to a Linux/Mac virtual or physical machine to proceed.

- Modify the openssl.cnf template to match the required local domain. For example, if the chosen domain is 'vmware.portal.siemonster.com' (Must be a domain with 4 names) then make the changes as follows:

```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req

[req_distinguished_name]
countryName = AU
countryName_default = AU
stateOrProvinceName = VIC
stateOrProvinceName_default = VIC
localityName = Melbourne
localityName_default = Melbourne
organizationalUnitName = SIEMonster
organizationalUnitName_default = SIEMonster
commonName = vmware.portal.siemonster.com
commonName_max = 64

[ v3_req ]
# Extensions to add to a certificate request
basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = vmware.portal.siemonster.com
DNS.2 = *.vmware.portal.siemonster.com
```

- Next make the script 'generate\_certs.sh' executable ( chmod +x generate\_certs.sh), and run to produce the certificates and .p12 keystore.
- In the Rancher UI, navigate to Infrastructure – Certificates, edit the existing siemportal certificate, updating the private key and certificate.
- Copy and paste the contents of the server.key and server.crt, or upload to the Private Key and Certificate fields and save:

### Edit Certificate

| Name*      | Description                   |
|------------|-------------------------------|
| siemportal | e.g. EV cert for mydomain.com |

Note: The Private Key is intentionally blank because the field is write-only. You will need to provide the Private Key again to update the certificate, even if it hasn't changed.

| Private Key*   | Certificate*   | Chain Certs  |
|--|--|--|
| Paste in the private key, starting with -----BEGIN RSA PRIVATE | -----BEGIN CERTIFICATE-----<br>MIIDZJCCAk6gAwIBAgUAK<br>G95GzxTWHFMA0GCSqGSI<br>b3DQEBCwUAMEQx CzA JB<br>gNV<br>BAYTAKFVMQwwCgYDVQ<br>QIDANWSUMxEJAJAQBGNVB<br>AcMCU1IbGJvdXJlZTETMB<br>EGA1UE | Optional: Paste in the additional chained certificates, starting |

Save Cancel

- The 'Name' field must be set to 'siemportal' this is mandatory for the Load Balancer.

10. As the SIEMonster application uses multiple subdomains, it is necessary to import the keyStore.p12 cert into the local trusted certificate authorities for clean SSL sessions. This is so your browser doesn't keep popping up do you trust this connection. To do this follow the operating system below.

#### For Windows:

Administrators is the minimum group membership required to complete this procedure. To add certificates to the Trusted Root Certification Authorities store for a local computer

- Click Start, click Start Search, type mmc, and then press ENTER.
- On the File menu, click Add/Remove Snap-in.
- Under Available snap-ins, click Certificates, and then click Add.
- Under This snap-in will always manage certificates for, click Computer account, and then click Next.
- Click Local computer, and click Finish.
- If you have no more snap-ins to add to the console, click OK.
- In the console tree, double-click Certificates.
- Right-click the Trusted Root Certification Authorities store.
- Click Import to import the keystore.p12 certificate and follow the steps in the Certificate Import Wizard.

#### For Mac OS X

- To open Keychain Access, start by clicking on Go in the Finder menu and the select Utilities.
- When the Utilities window opens up, look for and click on the icon named Keychain Access.
- Note: Alternatively, you can open the Keychain Access by typing "Keychain Access" in the Spotlight search field at the top.
- Within the Keychain Access menu select File > click Import Items
- Browse to the .p12 or .pfx file that you want to import and open it.
- In the Add Certificates window select **System** in the Keychain drop-down and click **Add**
- Enter your admin password to authorize the changes and click **Modify Keychain**
- Leave the password field blank and click 'OK'.

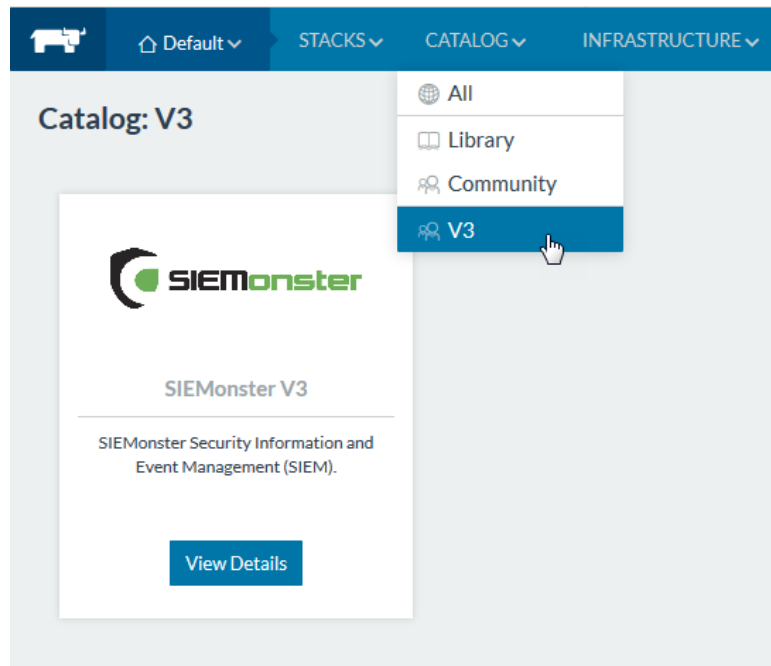
#### For Linux using Firefox

- Open Firefox. Click Edit > Preferences.
- Privacy & Security – scroll to bottom, View Certificates
- Your Certificates – Import keystore.p12
- Leave the password field blank and click 'OK'.

| Your Certificates  | People                   | Servers                    | Authorities     | Others |
|--|--------------------------|----------------------------|-----------------|--------|
| You have certificates from these organizations that identify you |                          |                            |                 |        |
| Certificate Name   | Security Device          | Serial Number              | Expires On      |        |
| SIEMonster   | Software Security Device | 00:86:29:71:3D:F8:BD:7A:E3 | January 5, 2028 |        |

## 6.3 STACK DEPLOYMENT

The SIEMonster V3 application catalog item is pre-loaded.



11. Navigate to the V3 catalog and click 'View Details' for the SIEMonster V3 App.

12. Under 'New Stack', substitute projectname for the required application name. This name will be used for your site domain in the next step.

Example:

siemonster-project-vmware change this to siemportal

siemonster-project-siemportal

13. Under Configuration Options, substitute projectname for the name chosen

*For example*

*Name:*

*siemonster-project-siemportal will become*

*Site domain name:*

*siemportal.corp.clientname.com (domain name must have 4 names)*

### Before

Name\*

### Configuration Options

Site domain name\*

Specify the domain name of the site.

### After

Name\*

### Configuration Options

Site domain name\*

Specify the domain name of the site.

14. Set the Elasticsearch JAVA HEAP SIZE per the machine specifications. For Elasticsearch Data Nodes, this should be set to a value half of the available system RAM. For the Master & Client nodes, the heap sizes can be left as default as these can be modified to suit at any time post install.

Heap size (master nodes)\*

Heap size to be allocated for Java (mater nodes)

Heap size (data nodes)\*

Heap size to be allocated for Java (mater nodes)

Heap size (client nodes)\*

Heap size to be allocated for Java (mater nodes)

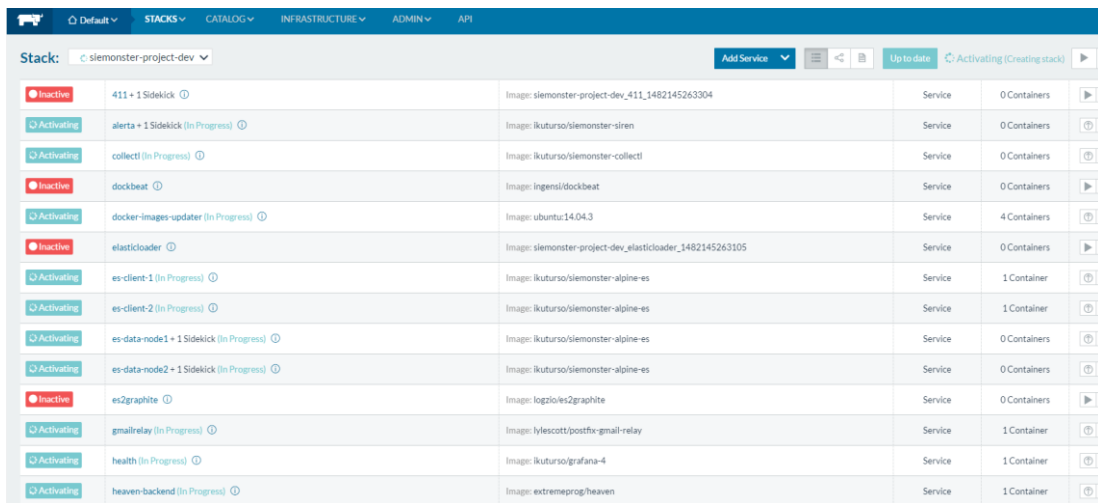
15. Set the administrator email address for the SIEMonster Web interface. **This will be the same email** that will be used in Chapter 7 – Web Application Setup.

## Web Application Admin Email\*

admin@siemonster.com

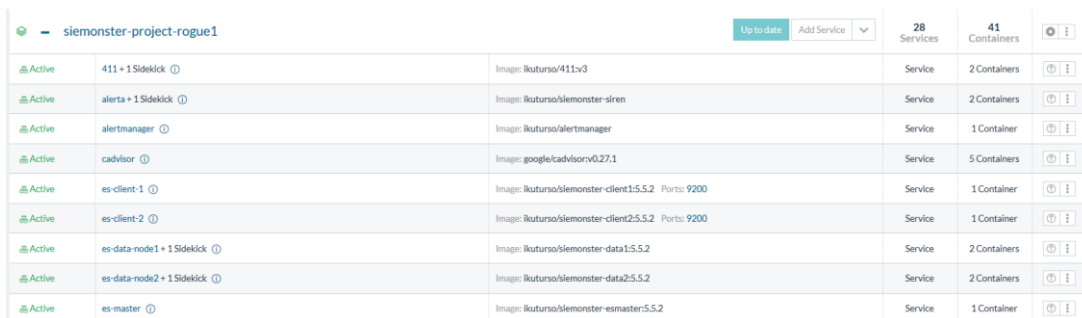
Set the ADMIN email

16. The remaining application passwords should be changed from the defaults, see Appendix A for change management table. Aside from the CertAuth, Truststore & KeyStore passwords, all passwords can be changed post-install if required.
17. The SITE\_ID option should be left at default, as initially the Logstash Heap Size
18. If Gmail alert relaying is required set the appropriate values. It is recommended to setup a Gmail account specifically for this purpose.
19. Finally, click on 'Launch'.
20. The stack will take around 5 - 60 minutes to build, depending on internet connection speed. The status can be viewed under Stacks – User



| Stack: siemonster-project-dev            | Services | Containers   | Status     |
|--|----------|--------------|------------|
| 411 + 1 Sidekick                         | Service  | 0 Containers | Inactive   |
| alerta + 1 Sidekick (In Progress)        | Service  | 0 Containers | Activating |
| collectl (In Progress)                   | Service  | 0 Containers | Activating |
| dockbeat                                 | Service  | 0 Containers | Inactive   |
| docker-images-updater (In Progress)      | Service  | 4 Containers | Activating |
| elasticsearch                            | Service  | 0 Containers | Inactive   |
| es-client-1 (In Progress)                | Service  | 1 Container  | Activating |
| es-client-2 (In Progress)                | Service  | 1 Container  | Activating |
| es-data-node1 + 1 Sidekick (In Progress) | Service  | 0 Containers | Activating |
| es-data-node2 + 1 Sidekick (In Progress) | Service  | 0 Containers | Activating |
| es2graphite                              | Service  | 0 Containers | Inactive   |
| gmailrelay (In Progress)                 | Service  | 1 Container  | Activating |
| health (In Progress)                     | Service  | 1 Container  | Activating |
| heaven-backend (In Progress)             | Service  | 1 Container  | Activating |

On completion, the status will turn to green for all items:



| Stack: siemonster-project-rogue1 | Services | Containers   | Status |
|----------------------------------|----------|--------------|--------|
| 411 + 1 Sidekick                 | Service  | 2 Containers | Active |
| alerta + 1 Sidekick              | Service  | 2 Containers | Active |
| alertmanager                     | Service  | 1 Container  | Active |
| cadvisor                         | Service  | 5 Containers | Active |
| es-client-1                      | Service  | 1 Container  | Active |
| es-client-2                      | Service  | 1 Container  | Active |
| es-data-node1 + 1 Sidekick       | Service  | 2 Containers | Active |
| es-data-node2 + 1 Sidekick       | Service  | 2 Containers | Active |
| es-master                        | Service  | 1 Container  | Active |



If using a local DNS entry for example a hosts file. You will need to add your entries to a host file.

### Local DNS Settings

The Makara server is the endpoint used by the load balancer.  
This will be the IP address used for the Rancher Server.

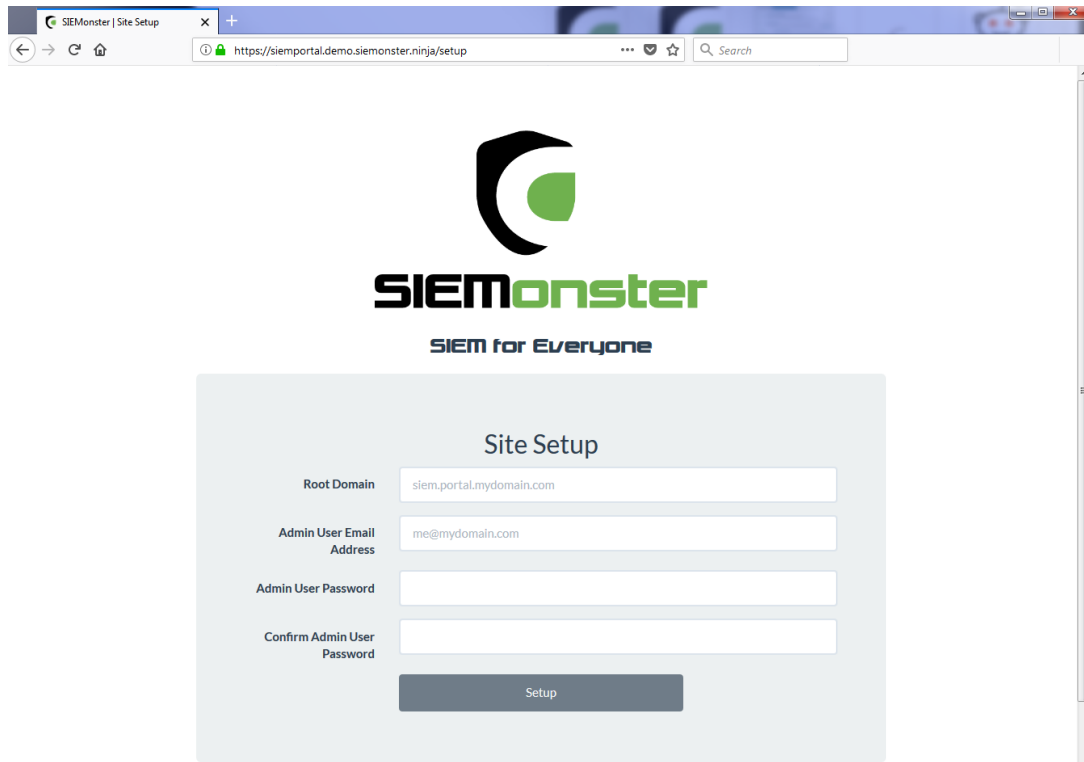
Using a local DNS server, zone entries are required for site.dname.com and \*.site.dname.com, e.g.  
siemportal.corp.clientname.com  
\*. siemportal.corp.clientname.com

Where there is no DNS server, the following entries can simply be added to the local hosts file using the Makara IP address

```
192.168.0.29 vmware.portal.siemonster.com
192.168.0.29 prometheus.vmware.portal.siemonster.com
192.168.0.29 alertmanager.vmware.portal.siemonster.com
192.168.0.29 dradis.vmware.portal.siemonster.com
192.168.0.29 ir.vmware.portal.siemonster.com
192.168.0.29 411.vmware.portal.siemonster.com
192.168.0.29 reporting.vmware.portal.siemonster.com
192.168.0.29 minemeld.vmware.portal.siemonster.com
192.168.0.29 health.vmware.portal.siemonster.com
192.168.0.29 sm-kibana.vmware.portal.siemonster.com
192.168.0.29 openaudit.vmware.portal.siemonster.com
192.168.0.29 rabbitmq.vmware.portal.siemonster.com
192.168.0.29 alerta.vmware.portal.siemonster.com
```

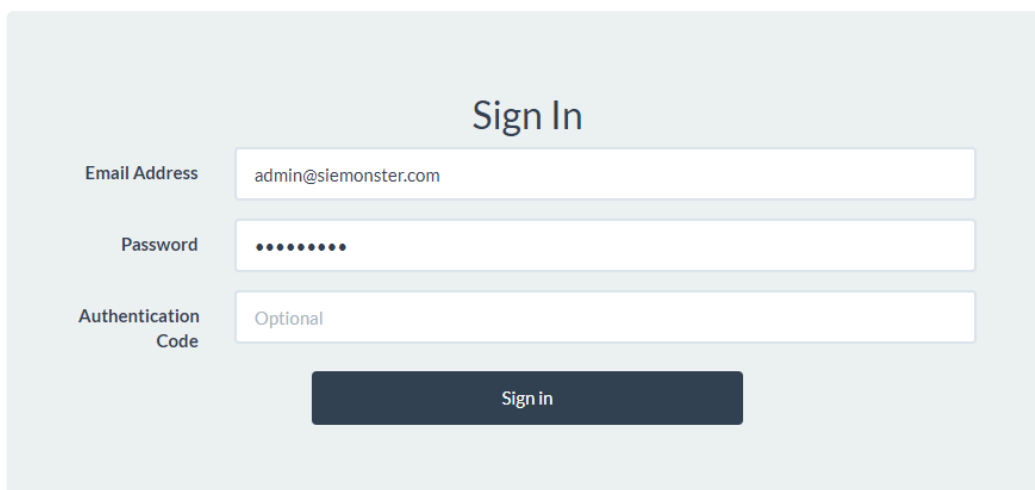
Leave a few minutes for the DNS to propagate if using a DNS server and the system health checks to complete before opening the web application URL, e.g. <https://siemportal.corp.clientname.com> from the example shown previously.

## 7 WEB APPLICATION SETUP

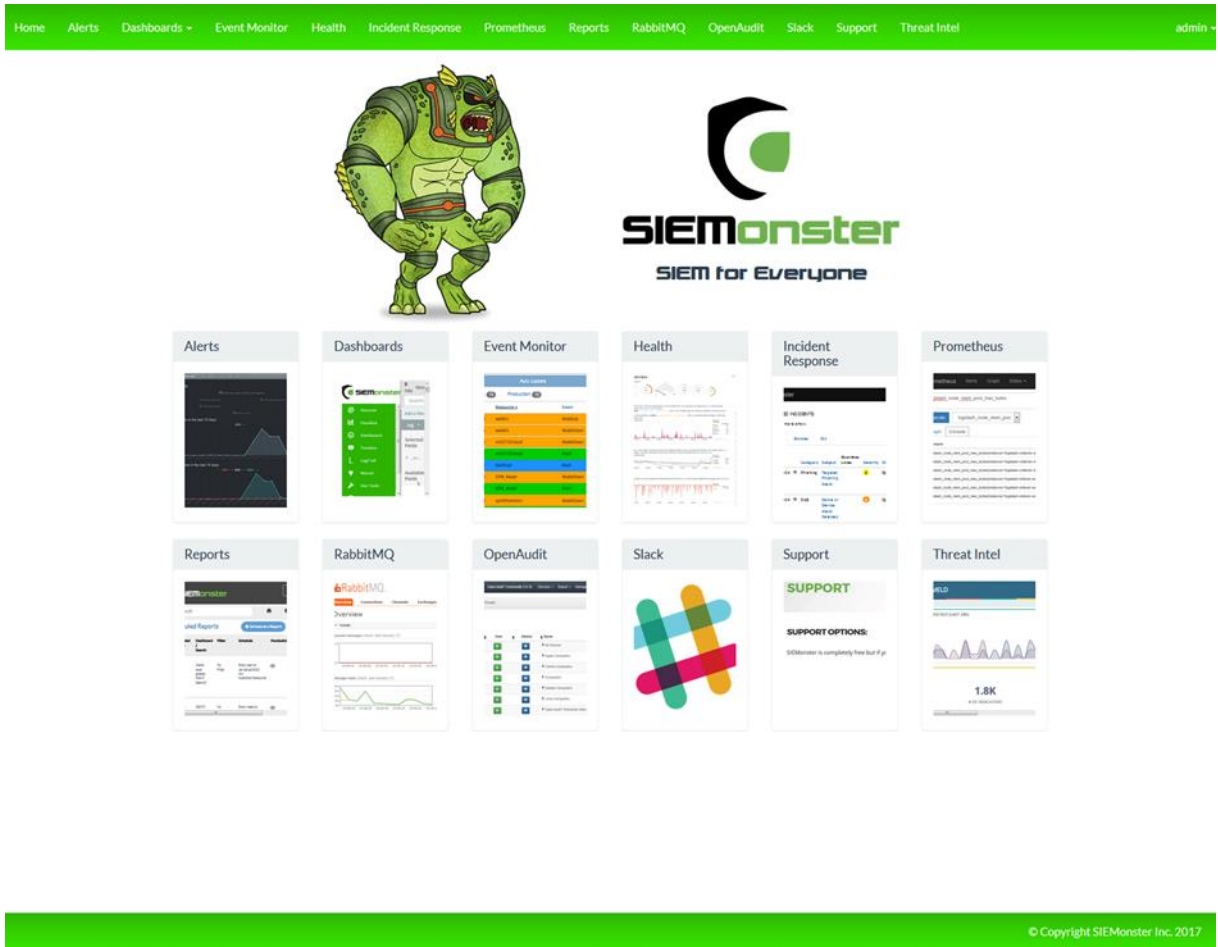


- For the Root Domain, enter the domain name used in Section 6.  
e.g. siemportal.corp.clientname.com
- The Admin User email address should be the same as that entered in section 6.3 Stack Deployment
- Strong passwords are enforced and must be 8 Characters in Length, upper and lower-case letters, at least 1 number, at least 1 symbol  
Click 'Setup' on completion.

On successful setup, a sign in page will appear:

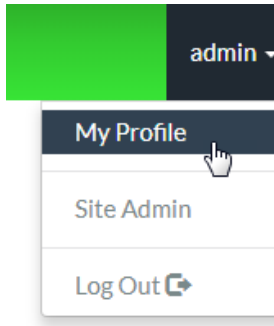


Sign in with the credentials entered during the above Setup phase. Note that the Authentication Code for 2FA if required, can be setup after initial login.



The screenshot displays the SIEMonster dashboard interface. At the top, a green navigation bar contains the following menu items: Home, Alerts, Dashboards, Event Monitor, Health, Incident Response, Prometheus, Reports, RabbitMQ, OpenAudit, Slack, Support, Threat Intel, and an admin user profile. Below the navigation bar, the dashboard features a central area with the SIEMonster logo and the tagline "SIEM for Everyone". To the left of the logo is a green cartoon monster character. Below the logo and character, there is a grid of 12 dashboard tiles, each representing a different feature: Alerts, Dashboards, Event Monitor, Health, Incident Response, Prometheus, Reports, RabbitMQ, OpenAudit, Slack, Support, and Threat Intel. Each tile contains a small preview of the corresponding dashboard's content. At the bottom of the page, a green footer bar contains the copyright notice: "© Copyright SIEMonster Inc. 2017".

## 8 USER SETUP



For each logged on user there is an option available under the user menu, top right, to modify the users profile.

This includes changing the display name, changing the password or adding two factor authentication.

### 8.1 USER ROLES

User Roles are used to allow access to different components within the SIEM. Two roles are preconfigured during deployment – admin and user.

The admin role contains all default role options for frames (home page tiles) and dashboards (Kibana).

New frames may also be added using the 'Create Frame' option:



Similarly, after creating new dashboards within Kibana, menu links to these items may be added using the 'Create Dashboard' option.



## Role: admin

### Frames

|                   |                                    |          |
|-------------------|------------------------------------|----------|
| Alerts            | Enabled (read only for Admin role) | Settings |
| Dashboards        | Enabled (read only for Admin role) | Settings |
| Event Monitor     | Enabled (read only for Admin role) | Settings |
| Health            | Enabled (read only for Admin role) | Settings |
| Incident Response | Enabled (read only for Admin role) | Settings |
| Prometheus        | Enabled (read only for Admin role) | Settings |
| Reports           | Enabled (read only for Admin role) | Settings |
| Dradis            | Enabled (read only for Admin role) | Settings |
| OpenAudit         | Enabled (read only for Admin role) | Settings |
| RabbitMQ          | Enabled (read only for Admin role) | Settings |

Using the 'Settings' option, the frame can be modified if required and an image used to reflect the properties of the frame.

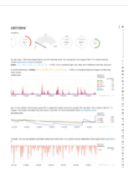
### Health

URL

---

Frame Image

No file chosen



Similarly, the default Dashboard URLs may be modified to suit if required.

### Apache

URL

The 'users' role is designed for new users who have been allocated login credentials without a specific role. This is useful when allocating members of an LDAP group. A single support access tile is provided.

|              |          |          |
|--------------|----------|----------|
| Dradis       | Disabled |          |
| OpenAudit    | Disabled |          |
| RabbitMQ     | Disabled |          |
| Support      | Enabled  | Settings |
| Threat Intel | Disabled |          |
| Demo         | Disabled |          |

New roles may be added using the 'Create Role' option.

Access to relevant frames can be enabled and settings modified if required.

## Frames

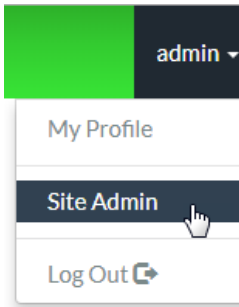
|            |          |          |
|------------|----------|----------|
| Alerts     | Disabled |          |
| Dashboards | Enabled  | Settings |

If the Dashboards frame is enabled, a Dashboard settings section will appear, providing options to enable or disable dashboards specific to the role.

## Dashboards

|                  |          |          |
|------------------|----------|----------|
| Apache           | Disabled |          |
| Cisco            | Disabled |          |
| HP Event Monitor | Enabled  | Settings |

## 9 SITE ADMINISTRATION



Under the Profile option is the Site Administration option.

This is used to setup site email settings, new local or LDAP users, roles and custom dashboard setup for each user.

### 9.1 SITE EMAIL

Email settings are configured to use Mailgun, for which a free account can be setup at <https://www.mailgun.com/>. This mail account is for the web application only, which will send out notifications when a user logs on to the SIEM.

### 9.2 LDAP SETTINGS

LDAP settings can be used to setup Active Directory users. It is recommended to create a group within the AD and then add users to this group who will require access.

Once completed, click on 'Save LDAP Settings'. The entered details will first be confirmed correct before being saved.

LDAP users in the chosen group will now be able to login using their corporate email address and active directory password.

|   |   |
|---|---|
| Hostname or IP Address (required)                 | <input type="text" value="172.18.1.92"/>          |
| Port  | <input type="text" value="636"/>                  |
| TLS   | <input checked="" type="checkbox"/> Enabled       |
| Connection Timeout                                | <input type="text" value="1000"/>                 |
| Service Account Username (required)               | <input type="text" value="admin"/>                |
| Service Account Password (required)               | <input type="password" value="....."/>            |
| User Search Base (required)                       | <input type="text" value="dc=mycompany, dc=com"/> |
| Group Search Base                                 | <input type="text" value="SIEMGroup"/>            |
| <input type="button" value="Save LDAP Settings"/> |   |

## 10 OPERATIONAL OVERVIEW

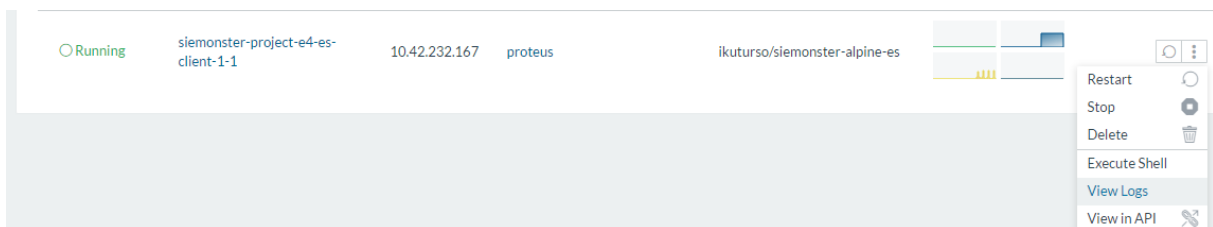
### 10.1 LOG VIEW

The logs for each container can be viewed within the Rancher Server UI as follows:

First click on a container

|              |                         |
|--------------|-------------------------|
| Started-Once | docker-images-updater ⓘ |
| Started-Once | elasticloader ⓘ         |
| Active       | <b>es-client-1</b> ⓘ    |
| Active       | es-client-2 ⓘ           |

Next click on the menu to the right and choose View Logs:



Running siemmonster-project-e4-es-client-1 10.42.232.167 proteus ikurturso/siemmonster-alpine-es

- Restart
- Stop
- Delete
- Execute Shell
- View Logs**
- View in API

```

20/12/2016 09:07:26 [2016-12-19 22:07:26,483][WARN ][bootstrap ] unable to install syscall filter: seccomp unavailable: your kernel is bu
20/12/2016 09:07:27 [2016-12-19 22:07:27,589][INFO ][node ] [node-proteus] version[2.4.2], pid[17], build[161c65a/2016-11-17T11:51:6
20/12/2016 09:07:27 [2016-12-19 22:07:27,589][INFO ][node ] [node-proteus] initializing ...
20/12/2016 09:07:32 [2016-12-19 22:07:32,047][INFO ][plugins ] [node-proteus] modules [reindex, lang-expression, lang-groovy], plugins
20/12/2016 09:07:32 [2016-12-19 22:07:32,104][INFO ][env ] [node-proteus] using [1] data paths, mounts [[/usr/share/elasticsearch/c
20/12/2016 09:07:32 [2016-12-19 22:07:32,104][INFO ][env ] [node-proteus] heap size [1007.3mb], compressed ordinary object pointers
20/12/2016 09:07:42 [2016-12-19 22:07:42,473][INFO ][node ] [node-proteus] initialized
20/12/2016 09:07:42 [2016-12-19 22:07:42,474][INFO ][node ] [node-proteus] starting ...
20/12/2016 09:07:42 [2016-12-19 22:07:42,840][INFO ][transport ] [node-proteus] publish_address {10.42.232.167:9300}, bound_addresses {[
20/12/2016 09:07:42 [2016-12-19 22:07:42,888][INFO ][discovery ] [node-proteus] siemmonster/DysyNqMHSwi4XG2FFTH5-g
20/12/2016 09:07:46 [2016-12-19 22:07:46,305][INFO ][cluster.service ] [node-proteus] detected_master {node-kraken}{0AVvBBksRiS4RQqWS_aQJA}{10.
20/12/2016 09:07:46 [2016-12-19 22:07:46,496][INFO ][http ] [node-proteus] publish_address {10.42.232.167:9200}, bound_addresses {[
20/12/2016 09:07:46 [2016-12-19 22:07:46,497][INFO ][node ] [node-proteus] started
20/12/2016 09:07:52 [2016-12-19 22:07:52,270][INFO ][cluster.service ] [node-proteus] added {{node-capricorn}{hZFFvAPST2-ZmPKhqEDXJg}{10.42.20:

```

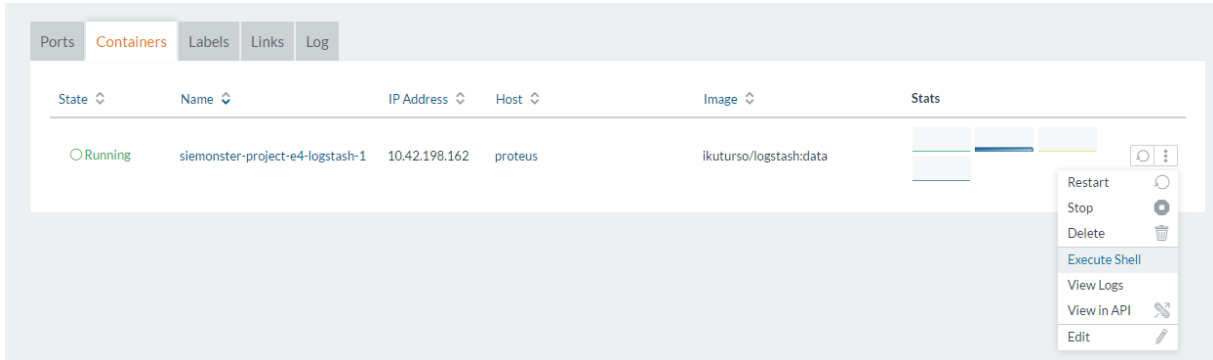
Connected

Useful for diagnostics and maintenance, the logs for any container can be viewed in this manner.



## 10.2 SHELL INTERACTION

Following the above steps and choosing the 'Execute Shell' option, a terminal may be opened to each container if any maintenance is required. For access to the configuration files, rules, etc. see the following section – VPN access.



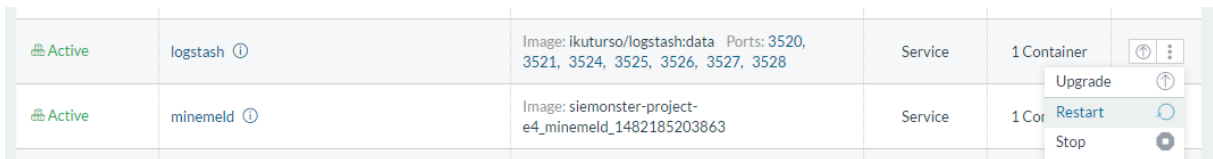
```

root@siemonster-project-e4-logstash-1:~# cd config-dir/
root@siemonster-project-e4-logstash-1:/config-dir# ls -l
total 64
-rw-r--r-- 1 root root 1105 Dec 18 01:12 00-inputs.conf
-rw-r--r-- 1 root root 1038 Dec 18 01:12 01-ossec-filter.conf
-rw-r--r-- 1 root root 9337 Dec 18 01:12 03-multisyslog-filter.conf
-rw-r--r-- 1 root root 500 Dec 18 01:12 05-osint-filter.conf
-rw-r--r-- 1 root root 1600 Dec 18 01:12 07-hp-printer-filter.conf
-rw-r--r-- 1 root root 3023 Dec 18 01:12 10-windows-events-filter.conf
-rw-r--r-- 1 root root 1067 Dec 18 01:12 15-suricata.conf
-rw-r--r-- 1 root root 1077 Dec 18 01:12 20-pfsense-filter.conf
-rw-r--r-- 1 root root 4814 Dec 18 01:12 25-paloalto-filter.conf
-rw-r--r-- 1 root root 4225 Dec 18 01:12 30-apache-filter.conf
-rw-r--r-- 1 root root 116 Dec 18 01:12 95-metrics-filter.conf
-rw-r--r-- 1 root root 2407 Dec 18 01:13 99-outputs.conf
root@siemonster-project-e4-logstash-1:/config-dir#

```

Close

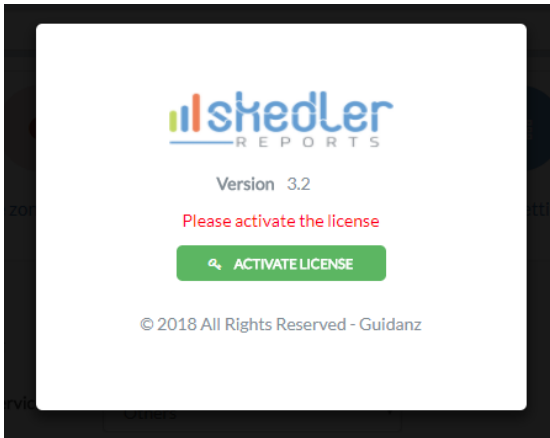
If any changes have been made, the container can be restarted on the main screen:




## 11 SKEDLER LICENSING

Reports - Menu

Click on 'Activate License'



License Activation

Proxy Setting 

Name\*

Email\*

Company Name\*

License Key\*

I agree to the [terms and conditions](#)






ONLINE ACTIVATION

Use the provided trial license key fill out the details to activate the license.

Configure the Email and Time Zone settings as appropriate.

Options are also available for setting a proxy, Slack messages and uploading a custom logo.

Search 🏠

-   
Email Settings
-   
Time zone Settings
-   
Slack Settings
-   
Proxy Settings
-   
Ot

**Email Setting**  On

**Supported Service\***

Gmail

Select Service

Others

Gmail

SES

SES-US-EAST-1

SES-US-WEST-2

SES-EU-WEST-1

**Sender's Email\***

**Password\***

**Admin Email\***

## Appendix A: Change Management for password.

Use only Alphanumeric passwords, e.g. Ys3CretpAss624

| Application      | Username   | Password                         |
|------------------|------------|----------------------------------|
| Grafana (Health) | admin      | admin                            |
| Web App Mongo    | siemuser01 | s13M0nSterV3                     |
| Mongo Hash Salt  | N/A        | 6b44d8edb86b4ca8bb8f3aaa35ddaf7d |
| RabbitMQ         | admin      | s13M0nSterV3                     |
| Wazuh API        | siemonster | s13M0nSterV3                     |
| Logstash         | logstash   | s13M0nSterV3                     |
| CA               | N/A        | s13M0nSterV3                     |
| 411              | admin      | admin                            |
| IR               | admin      | admin                            |
| Minemeld         | admin      | minemeld                         |
| Truststore       | N/A        | s13M0nSterV3                     |
| Keystore         | N/A        | s13M0nSterV3                     |
| Elastic          | elastic    | s13M0nSterV3                     |
| Beats            | beats      | s13M0nSterV3                     |
| Skedler          | skedler    | s13M0nSterV3                     |
| MySQL            | fouronone  | s13M0nSterV3                     |
| MySQL Root       | root       | s13M0nSterV3                     |
| Rancher          | admin      | s13M0nSterV3                     |
| SSH              | rancher    | s13M0nSterV3                     |