VM Build Guide

January 2018

Doc Version 1.8

TABLE OF CONTENTS

1 Authors Preface 3
2 Introduction 4
3 Build Installation Architecture Overview 5
4 Version 3 Happy Snap Features 6
5 Provided OVA Image Builder Package 14
5.1 Image Creation Overview 15
5.2 Preparing your images – Windows 15
5.3 Preparing your images – MAC 17
6 Installation 18
6.1 VMware Workstation 18
6.2 VMware ESXI 19
6.3 Rancher 21
6.4 Stack Deployment 24
7 Web Application Setup 29
8 User Setup 31
8.1 User Roles 31
9 Site Administration 34
9.1 Site Email 34
9.2 LDAP Settings 34
10 Operational Overview 35
10.1 Log View 35
10.2 Shell Interaction 36
11 Skedler Licensing 37

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.

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

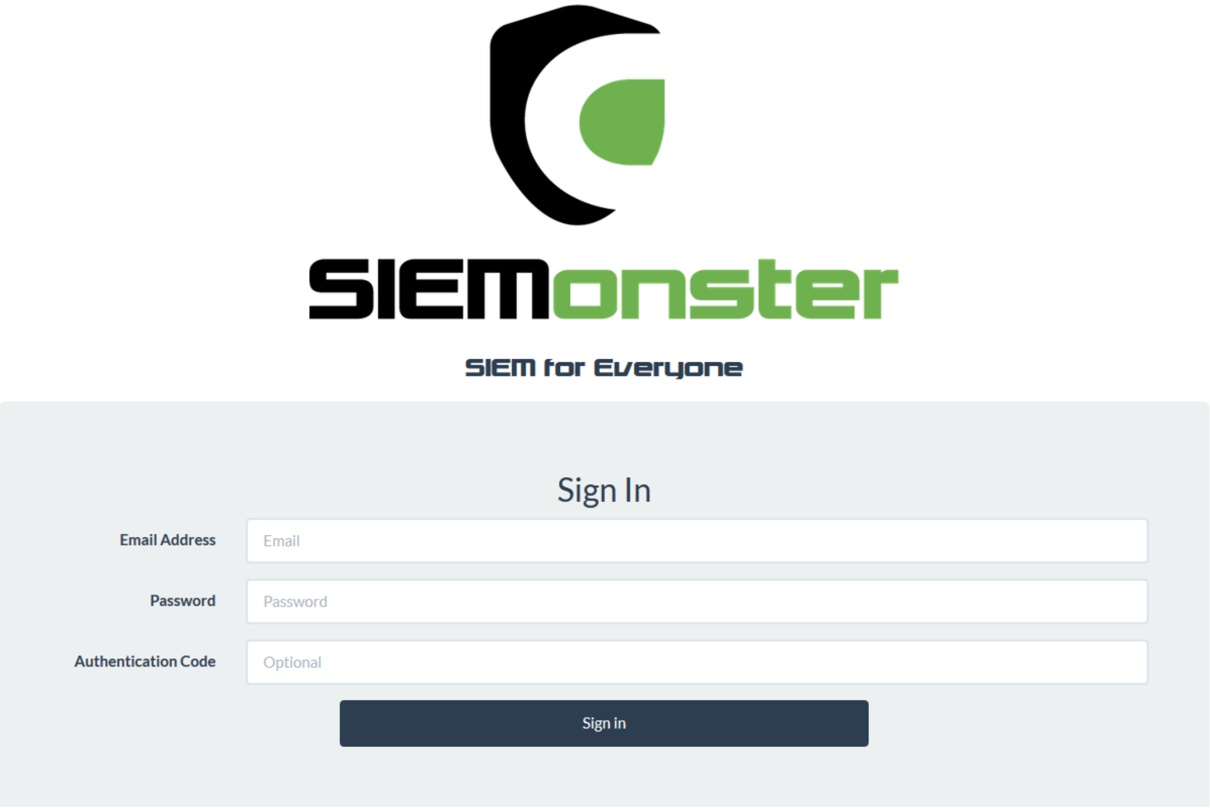
Rancher users can deploy an entire multi-container clustered application from the application catalog with one click of a button. Users can manage the deployed applications and perform fully automated upgrades when new versions of the application become available. Rancher maintains a public catalog consisting of popular applications contributed by the Rancher community. Rancher users can create their own private catalogs.W ith 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



SIEMonster

SIEM for Everyone

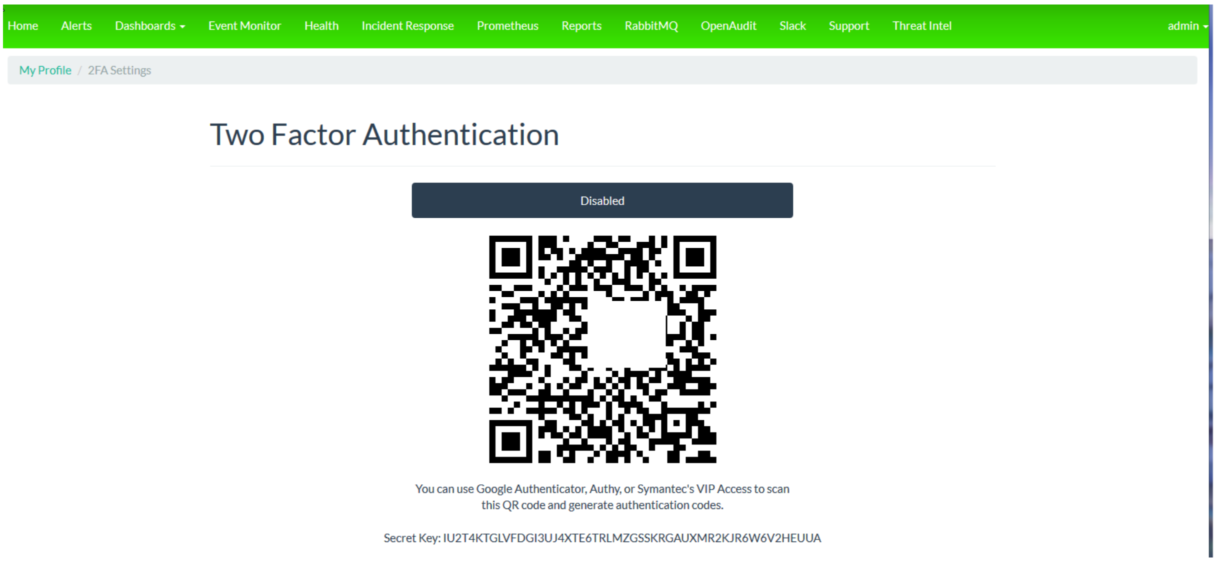
Sign In

Email Address: Email

Password: Password

Authentication Code: Optional

Sign in



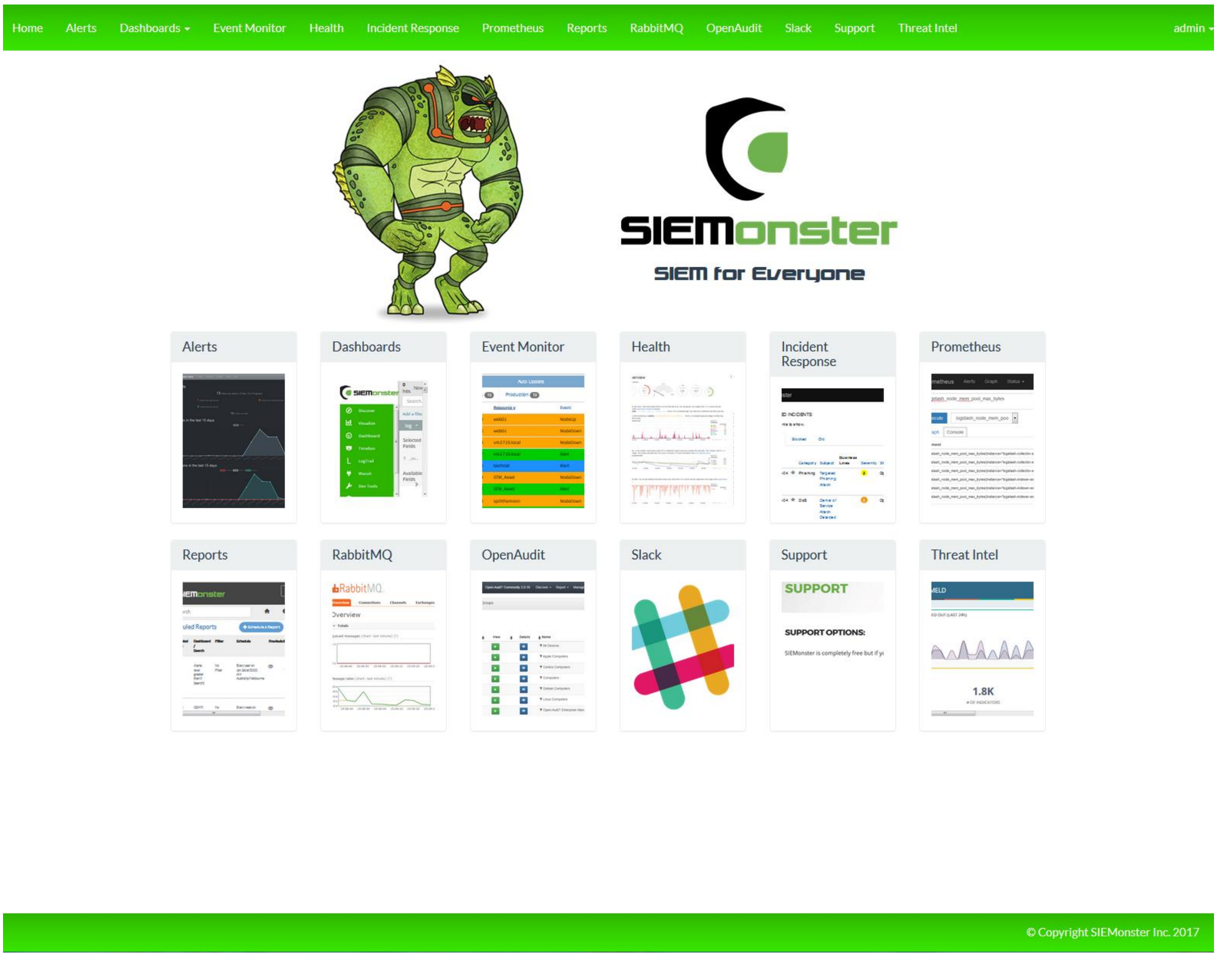
Two Factor Authentication

Disabled

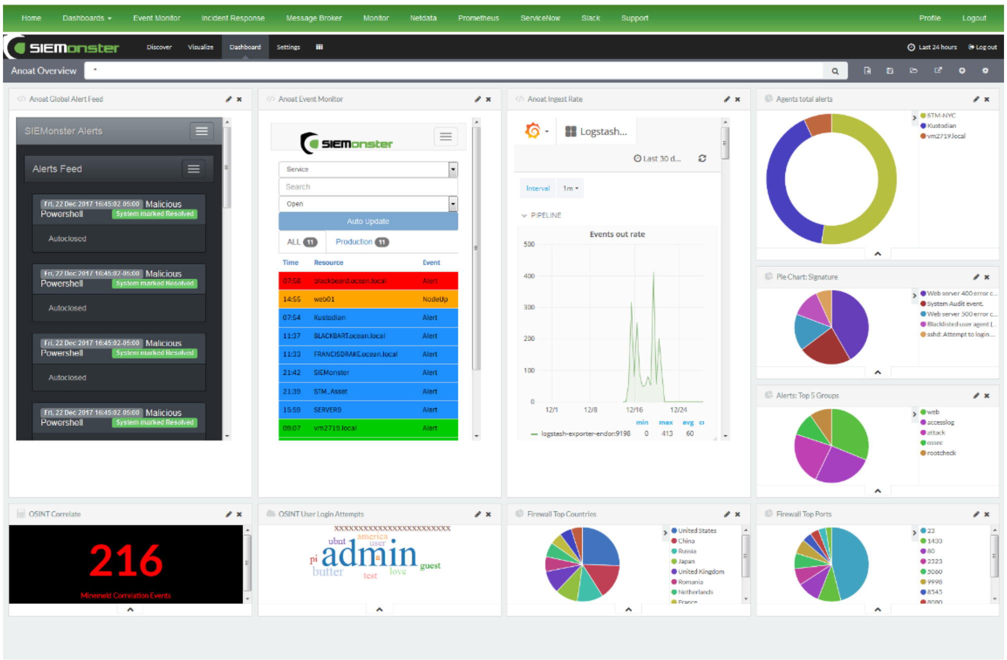
You can use Google Authenticator, Authy, or Symantec's VIP Access to scan this QR code and generate authentication codes.

Secret Key: IU2T4KTGLVFDGI3UJ4XTE6TRLMZGSSKRGAUXMR2KJR6W6V2HEUUA

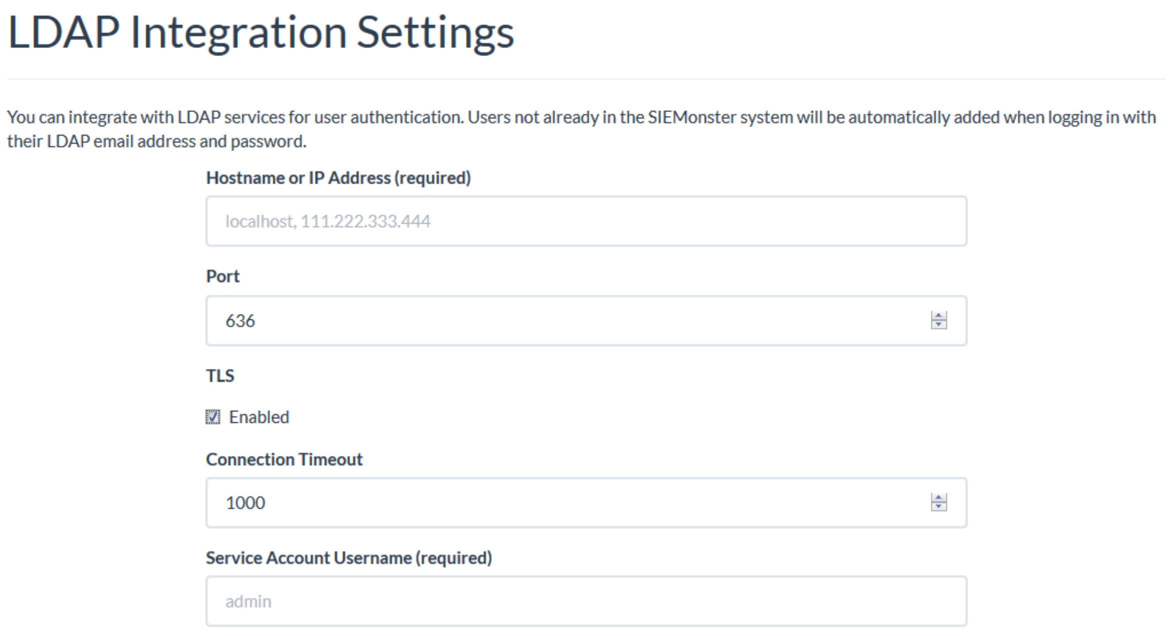
Updated fast loading dashboard



Pre-Configured Dashboards



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)

localhost, 111.222.333.444

Port

636

TLS

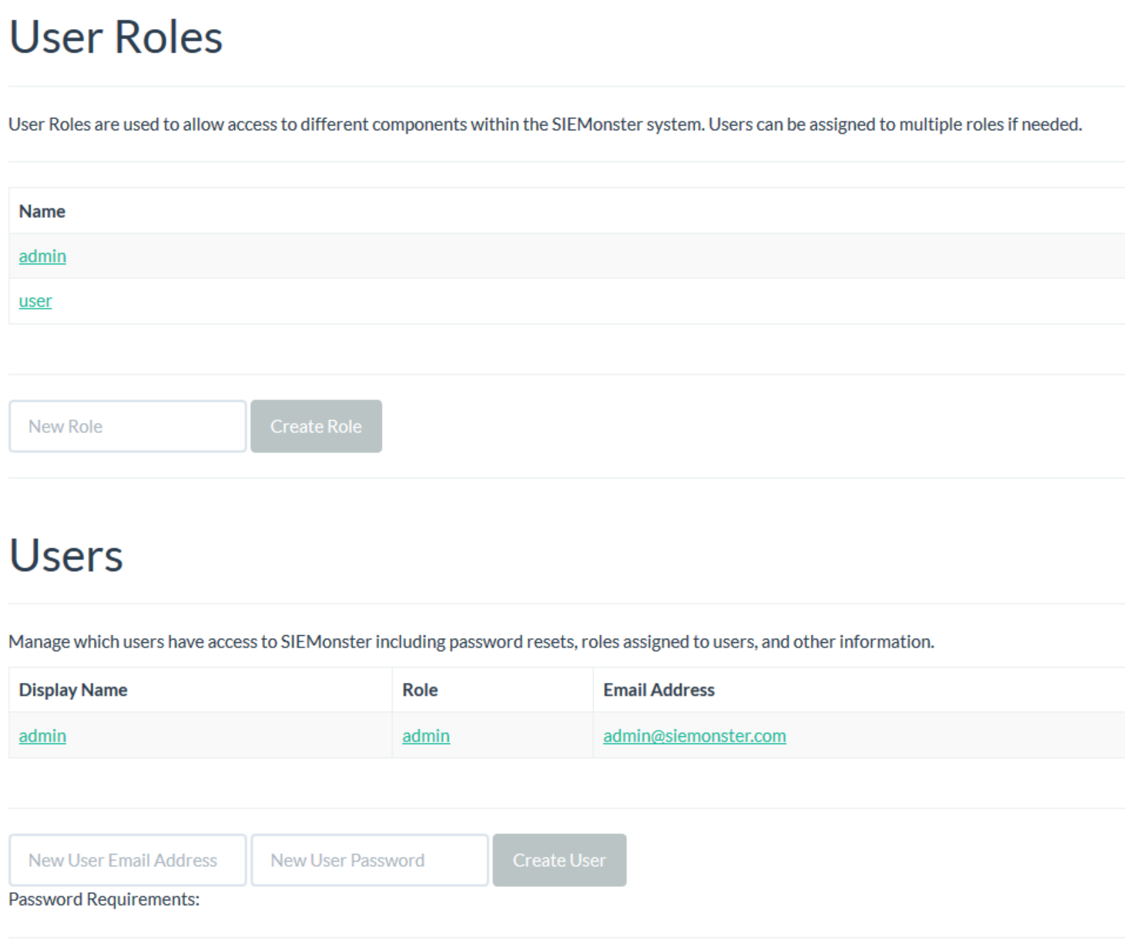
☑ Enabled

Connection Timeout

1000

Service Account Username (required)

admin



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
admin
user

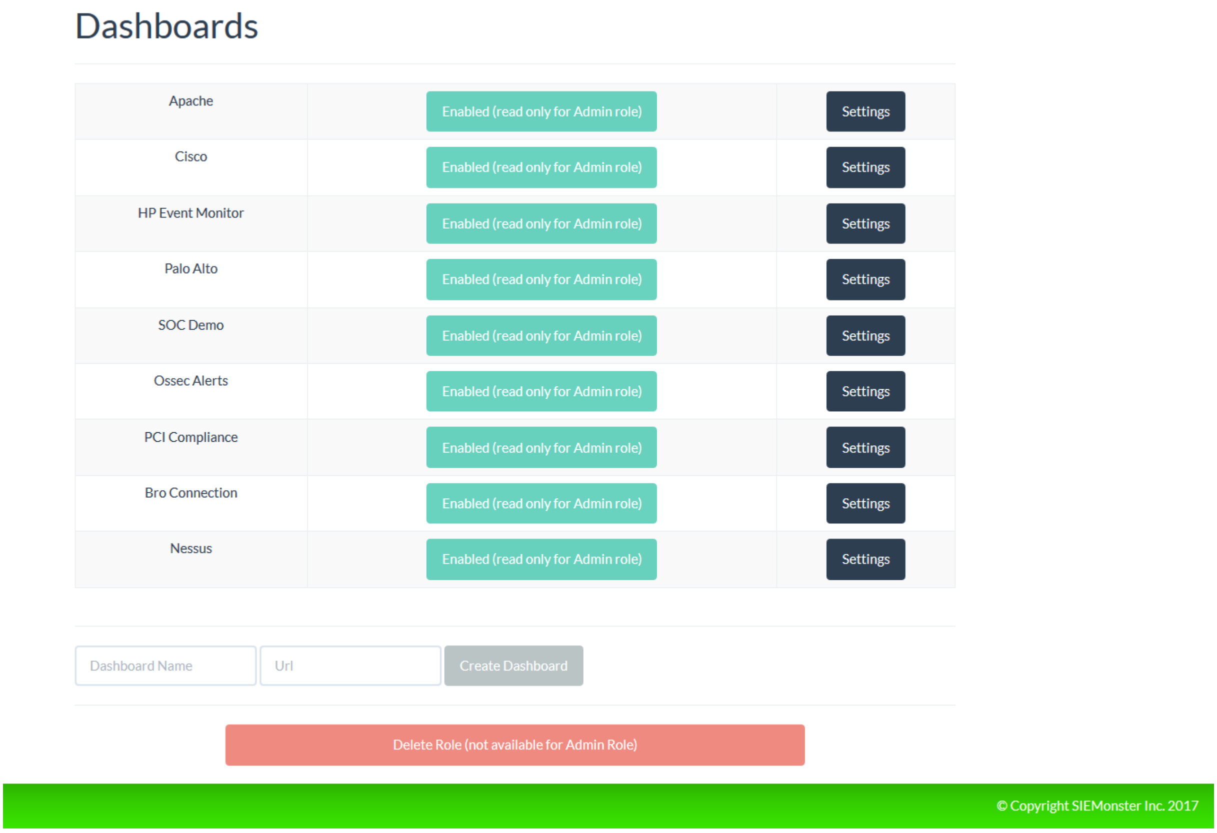
Users

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

Display Name	Role	Email Address
admin	admin	admin@siemonster.com

Password Requirements:

Customizable Dashboards

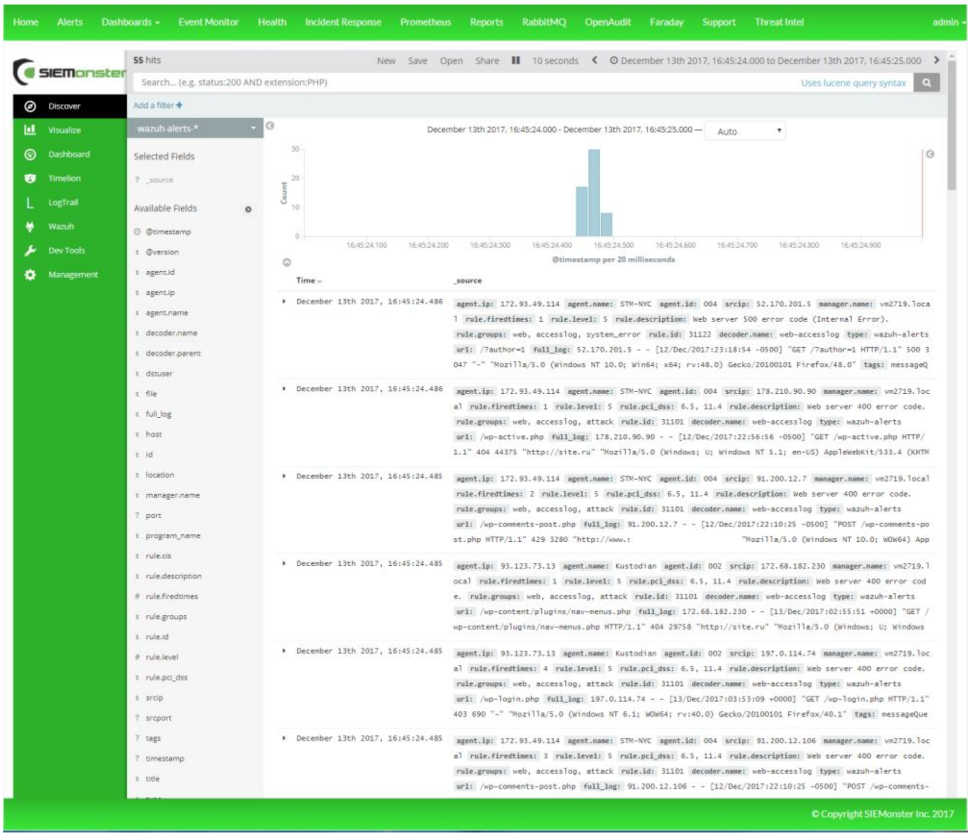


Dashboards

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

© Copyright SIEMonster Inc. 2017

Raw Log searches



55 hits

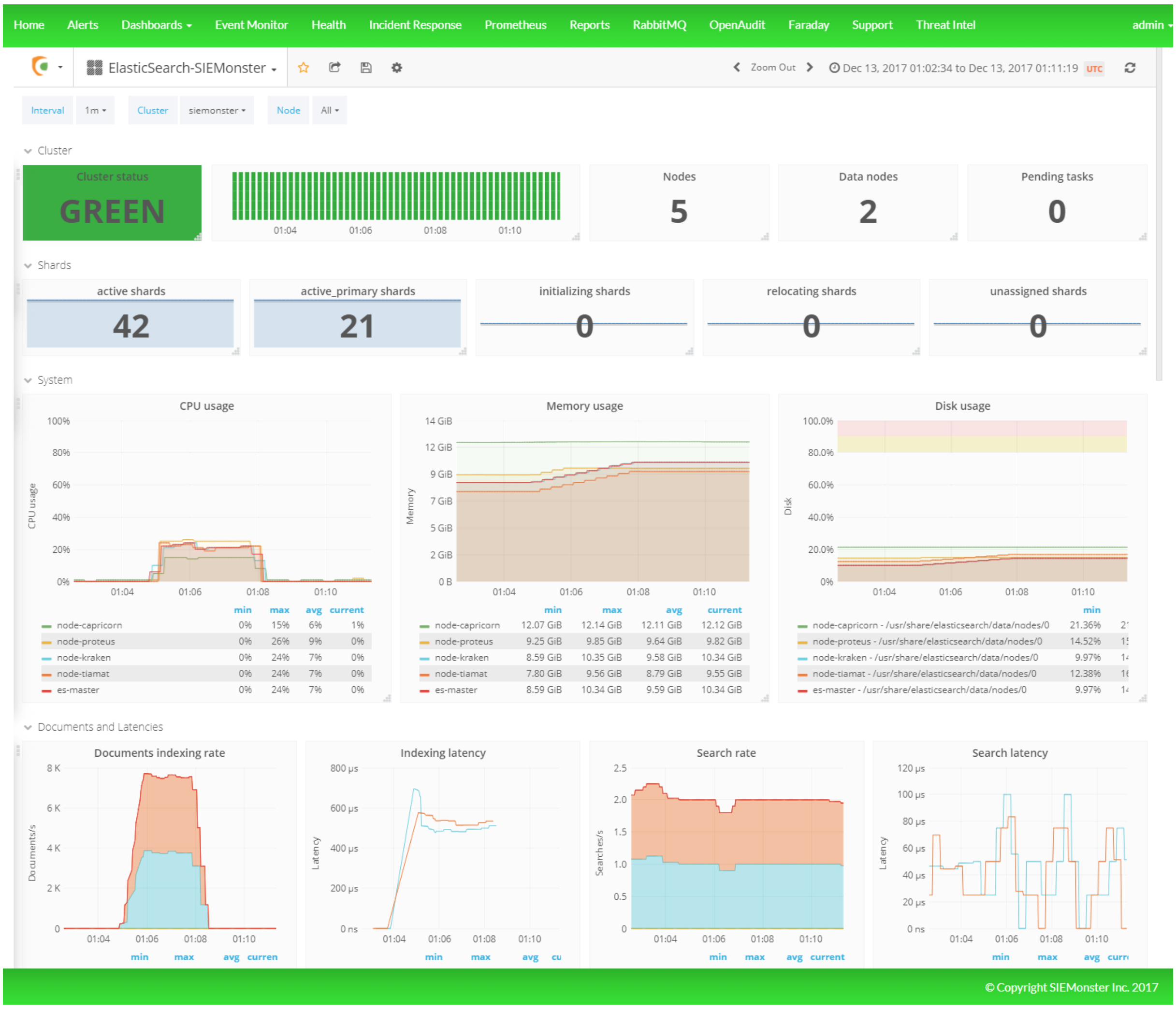
December 13th 2017, 16:45:24.000 to December 13th 2017, 16:45:25.000

December 13th 2017, 16:45:24.000 - December 13th 2017, 16:45:25.000 —

```
Time    _source
December 13th 2017, 16:45:24.486  agent.ip: 172.93.49.114 agent.name: STM-NYC agent.id: 004 srcip: 52.170.201.5 manager.name: vm2719.loca
                                  l rule.firedtimes: 1 rule.level: 5 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
                                  url: /?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/20100101 Firefox/48.0" tags: messageQ
December 13th 2017, 16:45:24.486  agent.ip: 172.93.49.114 agent.name: STM-NYC agent.id: 004 srcip: 178.210.90.90 manager.name: vm2719.loc
                                  al rule.firedtimes: 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
                                  url: /wp-active.php full_log: 178.210.90.90 - - [12/Dec/2017:22:56:56 -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 (KHTM
December 13th 2017, 16:45:24.485  agent.ip: 172.93.49.114 agent.name: STM-NYC agent.id: 004 srcip: 91.200.12.7 manager.name: vm2719.local
                                  rule.firedtimes: 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
                                  url: /wp-comments-post.php full_log: 91.200.12.7 - - [12/Dec/2017:22:10:25 -0500] "POST /wp-comments-po
                                  st.php HTTP/1.1" 429 3280 "http://www.:                  "Mozilla/5.0 (Windows NT 10.0; WOW64) App
December 13th 2017, 16:45:24.485  agent.ip: 93.123.73.13 agent.name: Kustodian agent.id: 002 srcip: 172.68.182.230 manager.name: vm2719.l
                                  ocal rule.firedtimes: 1 rule.level: 5 rule.pci_dss: 6.5, 11.4 rule.description: Web server 400 error cod
                                  e. rule.groups: web, accesslog, attack rule.id: 31101 decoder.name: web-accesslog type: wazuh-alerts
                                  url: /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
December 13th 2017, 16:45:24.485  agent.ip: 93.123.73.13 agent.name: Kustodian agent.id: 002 srcip: 197.0.114.74 manager.name: vm2719.loc
                                  al rule.firedtimes: 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
                                  url: /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
December 13th 2017, 16:45:24.485  agent.ip: 172.93.49.114 agent.name: STM-NYC agent.id: 004 srcip: 91.200.12.106 manager.name: vm2719.loc
                                  al rule.firedtimes: 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
                                  url: /wp-comments-post.php full_log: 91.200.12.106 - - [12/Dec/2017:22:10:25 -0500] "POST /wp-comments-
```

© Copyright SIEMonster Inc. 2017

Full Stack Monitoring



Cluster status: GREEN

Nodes: 5

Data nodes: 2

Pending tasks: 0

active shards: 42

active_primary shards: 21

initializing shards: 0

relocating shards: 0

unassigned shards: 0

CPU usage

	min	max	avg	current
node-capricorn	0%	15%	6%	1%
node-proteus	0%	26%	9%	0%
node-kraken	0%	24%	7%	0%
node-tiamat	0%	24%	7%	0%
es-master	0%	24%	7%	0%

Memory usage

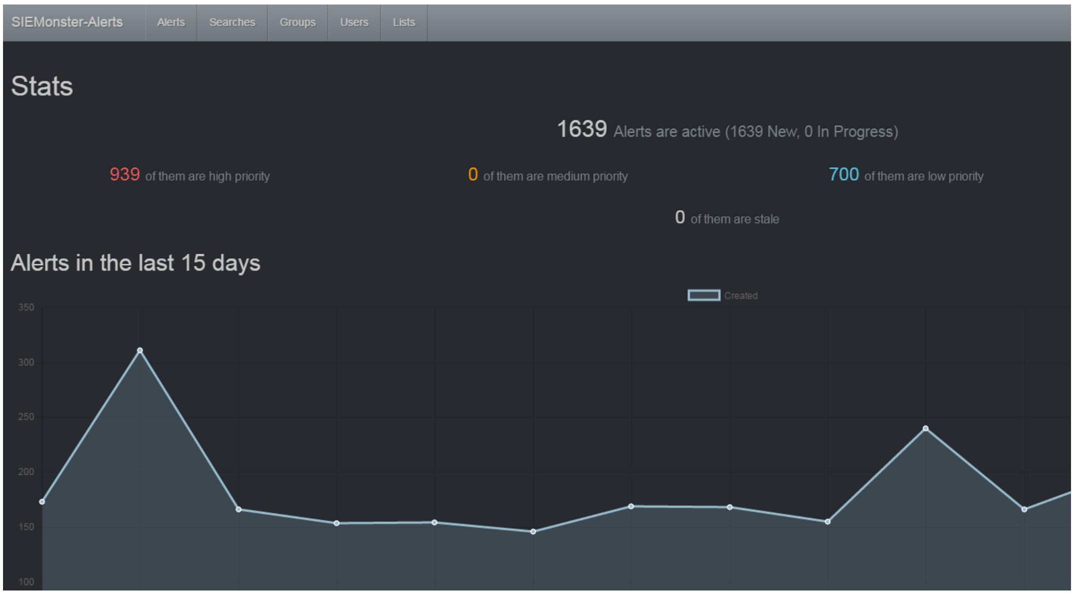
	min	max	avg	current
node-capricorn	12.07 GiB	12.14 GiB	12.11 GiB	12.12 GiB
node-proteus	9.25 GiB	9.85 GiB	9.64 GiB	9.82 GiB
node-kraken	8.59 GiB	10.35 GiB	9.58 GiB	10.34 GiB
node-tiamat	7.80 GiB	9.56 GiB	8.79 GiB	9.55 GiB
es-master	8.59 GiB	10.34 GiB	9.59 GiB	10.34 GiB

Disk usage

	min	
node-capricorn - /usr/share/elasticsearch/data/nodes/0	21.36%	2
node-proteus - /usr/share/elasticsearch/data/nodes/0	14.52%	15
node-kraken - /usr/share/elasticsearch/data/nodes/0	9.97%	14
node-tiamat - /usr/share/elasticsearch/data/nodes/0	12.38%	16
es-master - /usr/share/elasticsearch/data/nodes/0	9.97%	14

© Copyright SIEMonster Inc. 2017

Alerting



Stats

1639 Alerts are active (1639 New, 0 In Progress)

939 of them are high priority

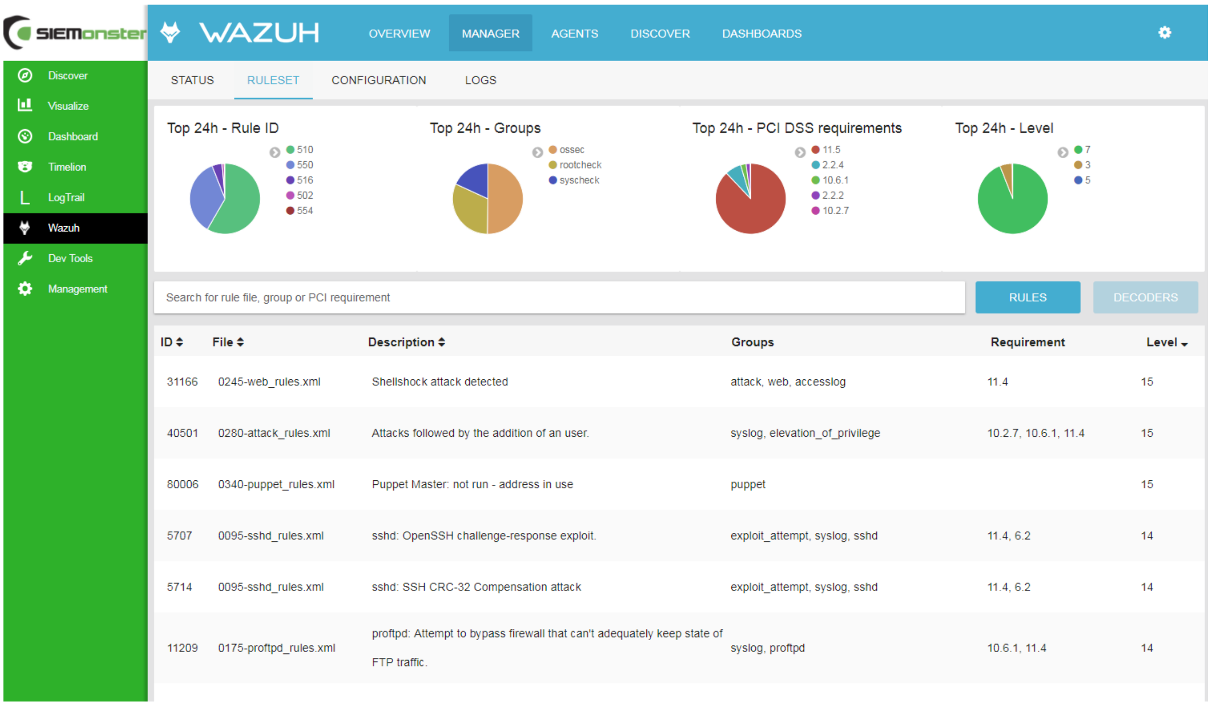
0 of them are medium priority

700 of them are low priority

0 of them are stale

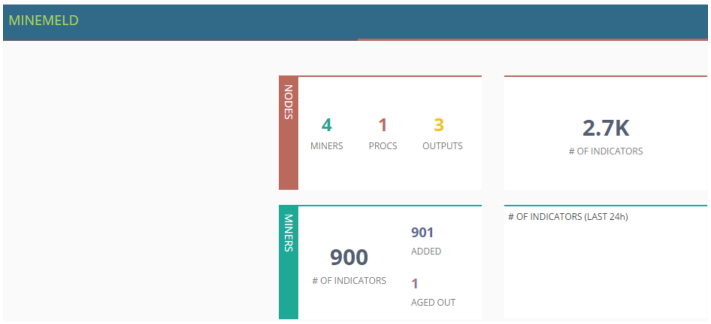
Alerts in the last 15 days

Wazuh HIDS Integration

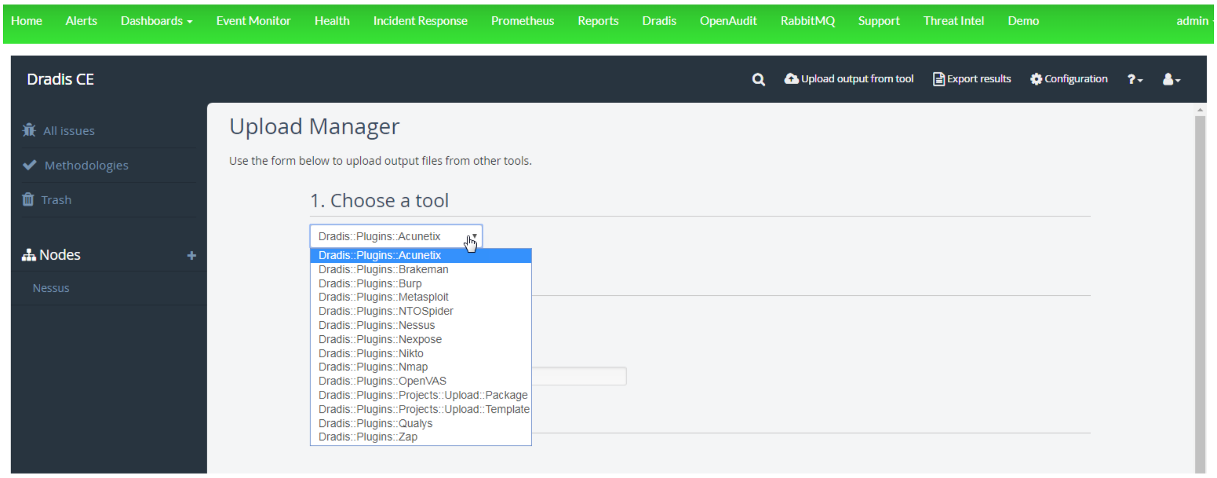


ID	File	Description	Groups	Requirement	Level
31166	0245-web_rules.xml	Shellshock attack detected	attack, web, accesslog	11.4	15
40501	0280-attack_rules.xml	Attacks followed by the addition of an user.	syslog, elevation_of_privilege	10.2.7, 10.6.1, 11.4	15
80006	0340-puppet_rules.xml	Puppet Master: not 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



Vulnerability Management

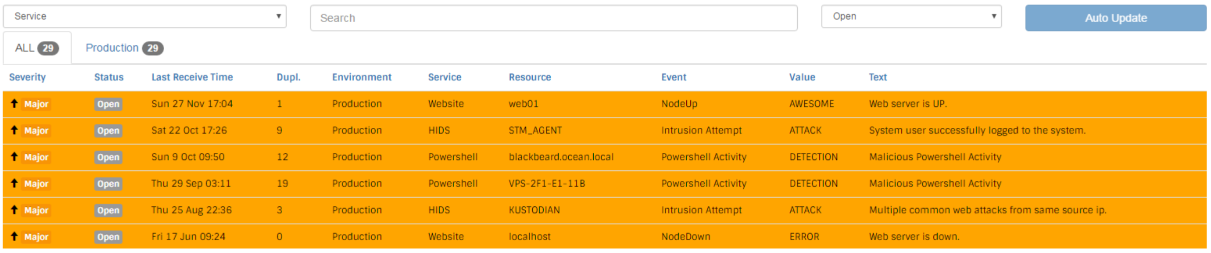


Upload Manager

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

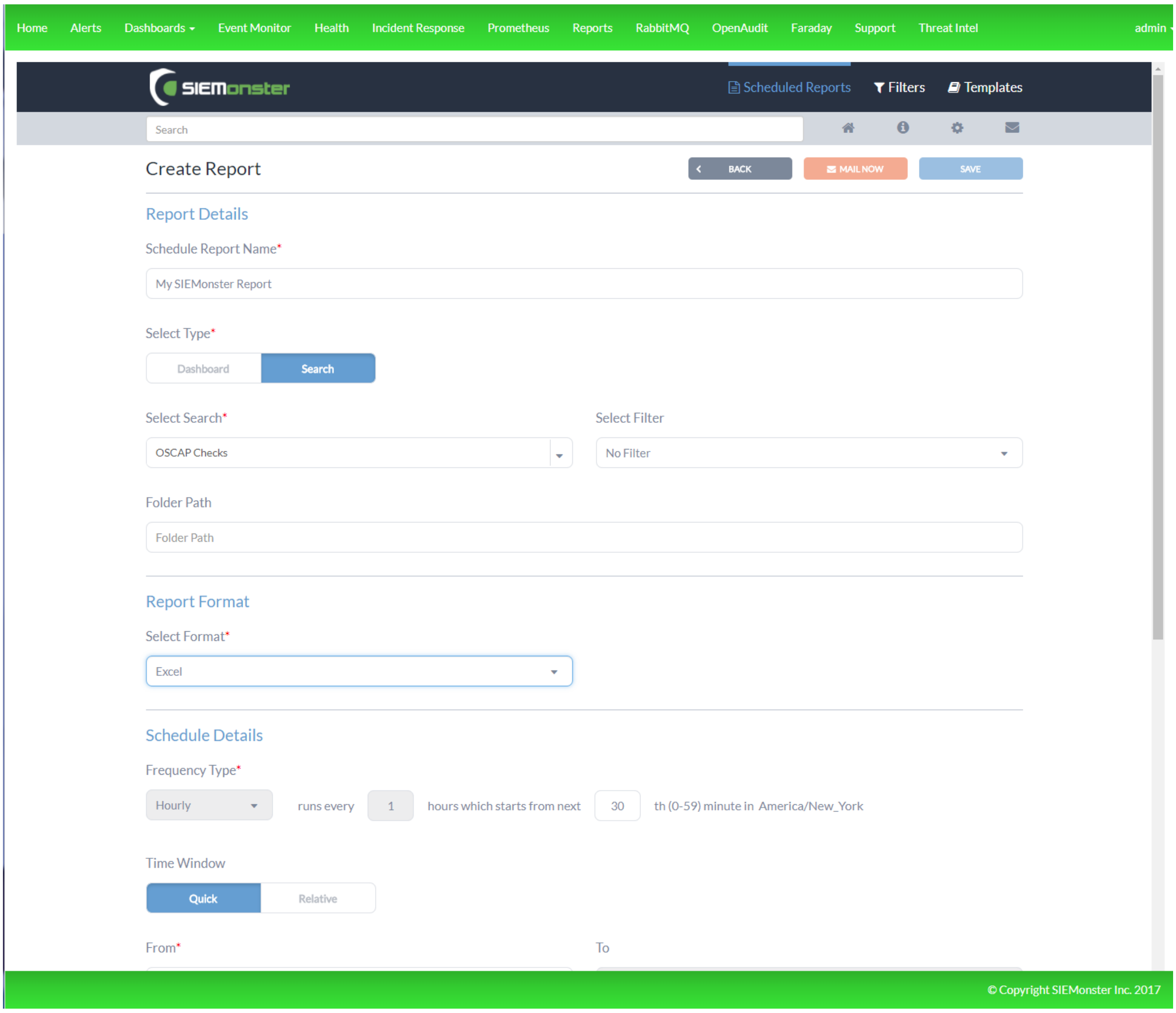
1. Choose a tool

Event Monitor



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



Create Report

Report Details

Schedule Report Name*

My SIEMonster Report

Select Type*

Dashboard | **Search**

Select Search*: OSCAP Checks

Select Filter: No Filter

Folder Path

Folder Path

Report Format

Select Format*: Excel

Schedule Details

Frequency Type*

Hourly ▾ runs every 1 hours which starts from next 30 th (0-59) minute in America/New_York

Time Window

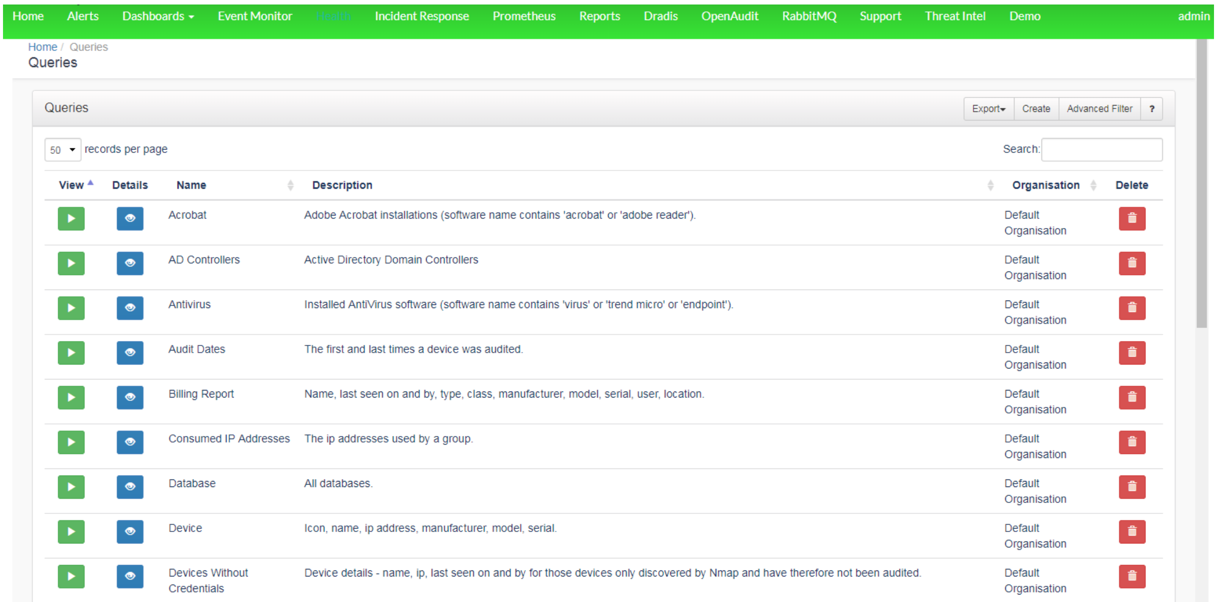
Quick | Relative

From*

To

© Copyright SIEMonster Inc. 2017

Audit and Discovery



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

5 PROVIDED OVA IMAGE BUILDER PACKAGE

The SIEMonster team have put together a package to allow for a fully customizable DIY VM installation.

The DIY option allows you to build your own images, this will allow you to hard set IP addresses, proxies, disk size before you build. This is the best option for most corporate environments.

Building the image using the default settings will build a DHCP based cluster, perfect for a quick POC deployment without customization.

The SIEMonster VM Image provides the means to quickly rollout a cluster using VMWare Workstation or VMWare ESXi 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 platforms:

- Mac OS X
- Debian
- Windows
- CentOS

Supported platforms are VMware Workstation and VMware ESXi

5.1 IMAGE CREATION OVERVIEW

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

- Download the package from the website using the Image Builder VM link
- Install Packer
- Install the OVF Tool (Windows)
- Edit the config file for static IP range, Proxy and Disk Size, Memory & Credentials
- Run the image builder script to create the VM files/OVA
- Run the OVFtool to create OVA or OVF images. (Windows)

The goal of this project is to create an image of a virtual machine, through which a user can deploy a 5-node Rancher SIEMonster cluster. This can be achieved by creating a virtual machine template in the OVA/OVF format. Customizations:

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

5.2 PREPARING YOUR IMAGES – WINDOWS

1. Click on Download on the SIEMonster website, register and Download the latest SIEMonster ImageBuilder Configuration file.
   SHA256 3b3bd1d6b0371bceef916b11196af97bd8095299159013c519d33108fcd1e9d1

2. Download and install the latest version of Packer https://www.packer.io/downloads.html

3. Download and the latest version of VMware OVF tool. The tool is free but requires an VMware registration account, https://www.vmware.com/support/developer/ovf/

4. Prepare the installation on a Linux machine, e.g. you can use an Ubuntu virtual machine.

   Prerequisites:
   sudo apt install python-pip
   pip install j2cli
   pip install cot

   Configure:
   cp ova_params.sh.example ova_params.sh
   Edit ova_params.sh – see example below
   chmod +x *.sh
   Edit core-ova-npp.json to change disk or memory size (optional)
   Edit win-var-template.json and modify the COREOS_PASSWORD to match that in ova_params.sh, if changed in core-ova-npp.json.

   Build:
   ./build_install_only.sh

5. Copy the entire ImageBuilder folder from Linux over to Windows, use WinSCP or similar.

6. Open a command prompt within the copied directory and run the following command:

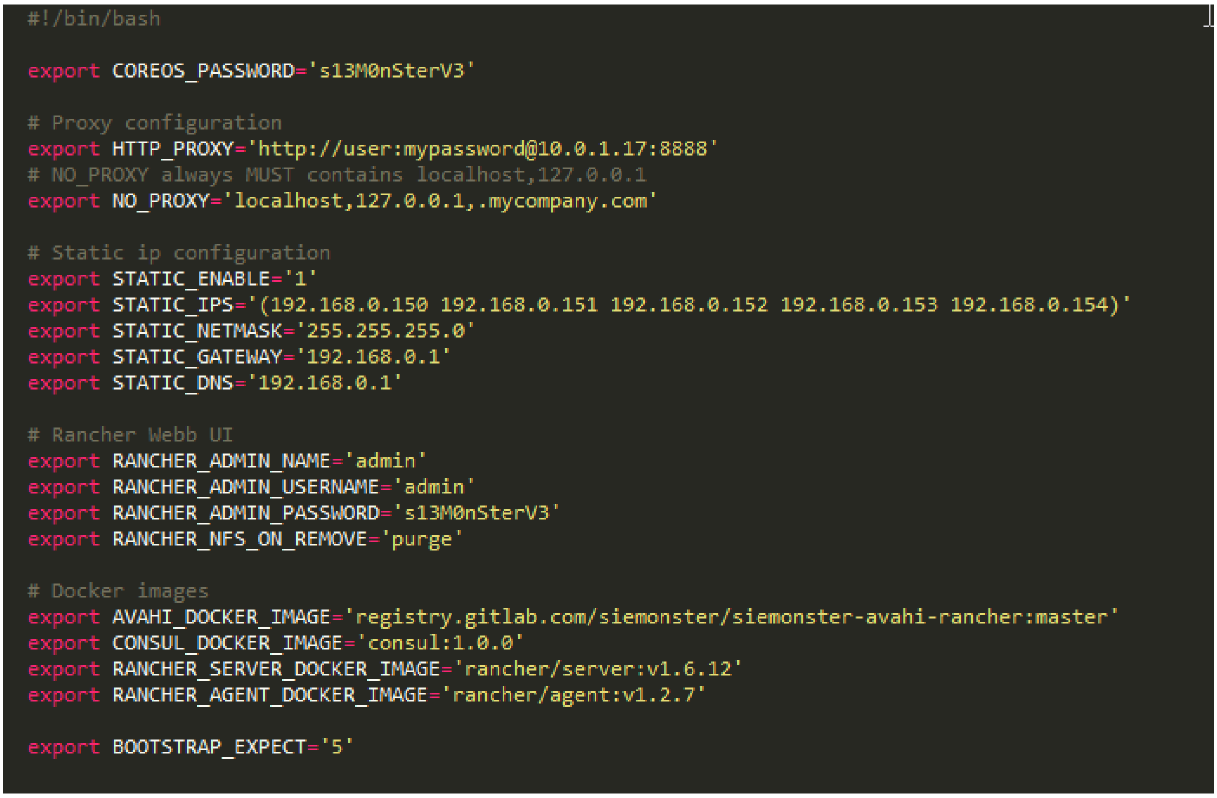
   packer build -var-file=win-var-template.json coreos-ova-npp.json

   This will create the required VMware machine in the build directory.

7. Convert to an OVA/OVF using OVFTool:
   e.g. ovftool.exe --shaAlgorithm=SHA1 g:\ImageBuilder\build\coreos.vmx f:\siemonster-v3.ova

8. You now have your custom image and can proceed to Chapter 6 Installation

   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'
```

5.3 PREPARING YOUR IMAGES – MAC

1. Click on Download on the SIEMonster website, register and Download the latest SIEMonster ImageBuilder Configuration file.
   SHA256 3b3bd1d6b0371bceef916b11196af97bd8095299159013c519d33108fcd1e9d1

2. Prerequisites:
   pip install j2cli
   pip install cot
   brew install packer
   Installed VMWare Fusion – Note: Use 2048 as minimum VM RAM setting

3. cp ova_params.sh.example ova_params.sh
   Edit ova_params.sh (see above for example).
   chmod +x *.sh
   Edit core-ova.json to change disk or memory size (optional)

4. Build:
   ./build_ova.sh

5. You now have your custom image and can proceed to Chapter 6 Installation skipping the download the latest ova section as you have your own now.

6 INSTALLATION

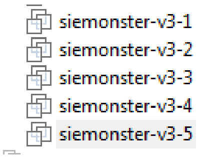
The VM Image deployment overview contains the following steps.

- Creation of SIEMonster OVA Image
- Automatic Rancher cluster deployment with credentialed access
- NFS creation for configuration centralization
- SSL certificate insertion
- SIEMonster Catalog item for one click install

6.1 VMWARE WORKSTATION

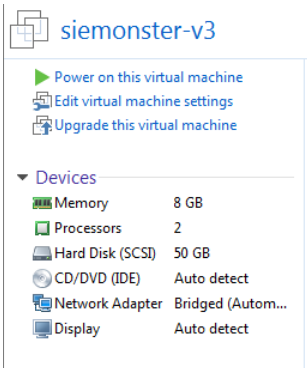
1. Create the OVA image file as shown in Section 5.

2. Import the image 5 times into VMWare, naming each instance sequentially. The hostnames for each instance are allocated automatically, so the naming is only so that each instance has a unique label.



siemonster-v3-1
siemonster-v3-2
siemonster-v3-3
siemonster-v3-4
siemonster-v3-5

3. The default Networking option is NAT, this should be changed to Bridged to allow incoming network connections from the local LAN. Ensure the Memory allocation is a minimum of 8GB. Make these changes on each instance.



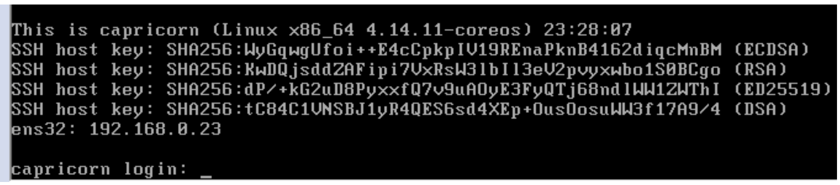
siemonster-v3

Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine

Devices

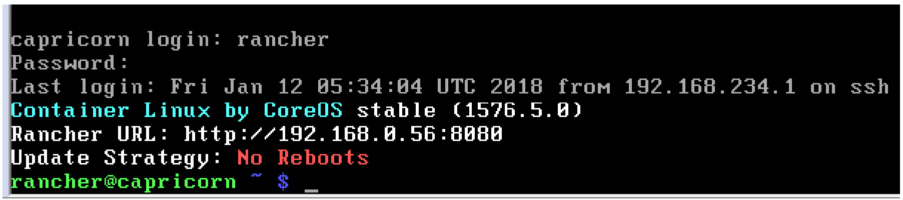
Memory	8 GB
Processors	2
Hard Disk (SCSI)	50 GB
CD/DVD (IDE)	Auto detect
Network Adapter	Bridged (Autom...
Display	Auto detect

4. Power on each virtual machine in turn and allow 10-30 minutes or so for the automatic stack build to complete. When ready, a specific hostname is allocated and shown in the terminal. If it still says localhost, it’s still building.



```
This is capricorn (Linux x86_64 4.14.11-coreos) 23:28:07
SSH host key: SHA256:WyGqwgUfoi++E4cCpkpIV19REnaPknB4162diqcMnBM (ECDSA)
SSH host key: SHA256:KwDQjsddZAFipi7VxRsW3lbIl3eV2pvyxwbo1S0BCgo (RSA)
SSH host key: SHA256:dP/+kG2uD8PyxxfQ7v9uAOyE3FyQTj68ndlWW1ZWThI (ED25519)
SSH host key: SHA256:tC84C1VNSBJ1yR4QES6sd4XEp+OusOosuWW3f17A9/4 (DSA)
ens32: 192.168.0.23

capricorn login: _
```

5. Within VMWare, logon to any of the instances with the default credentials (rancher/ s13M0nSterV3), if they were not changed during OVA creation.



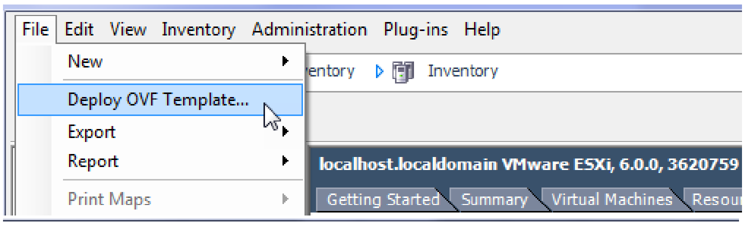
```
capricorn login: rancher
Password:
Last login: Fri Jan 12 05:34:04 UTC 2018 from 192.168.234.1 on ssh
Container Linux by CoreOS stable (1576.5.0)
Rancher URL: http://192.168.0.56:8080
Update Strategy: No Reboots
rancher@capricorn ~ $ _
```

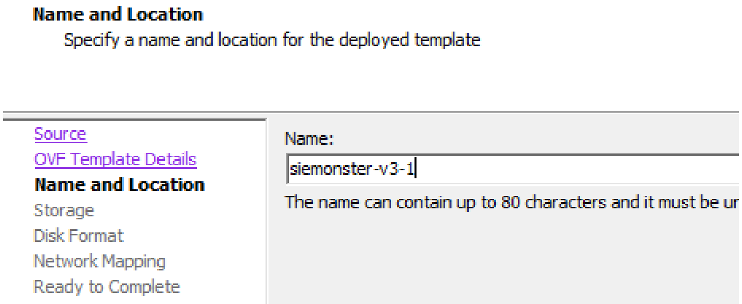
6. The Rancher URL will be shown in the terminal. The credentials are admin/s13M0nSterV3 if they were not changed during OVA creation.

6.2 VMWARE ESXI

1. Create the OVA image file as shown in Section 5.

2. Use the ‘Deploy Template’ option to import the image 5 times into ESXi, naming each instance sequentially. The hostnames for each instance are allocated automatically, so the naming is only so that each instance has a unique label.





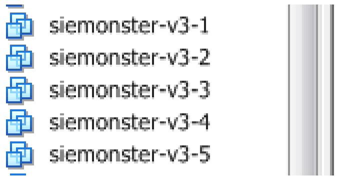
Name and Location

Specify a name and location for the deployed template

Name: siemonster-v3-1

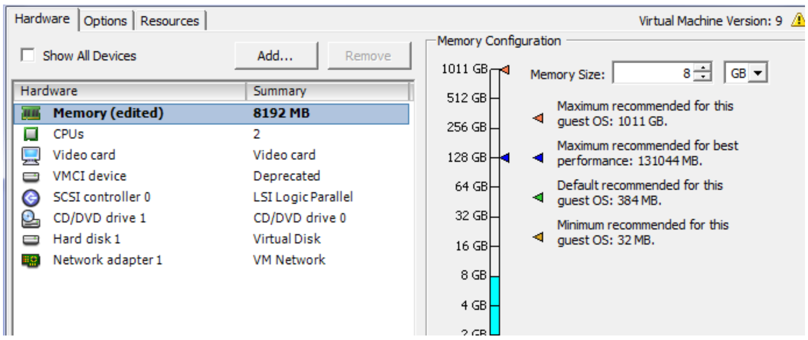
The name can contain up to 80 characters and it must be ur

3. Accept the defaults for each step.



siemonster-v3-1
siemonster-v3-2
siemonster-v3-3
siemonster-v3-4
siemonster-v3-5

4. Ensure that the minimum memory allocation for each instance is 8GB



Hardware	Summary
Memory (edited)	**8192 MB**
CPUs	2
Video card	Video card
VMCI device	Deprecated
SCSI controller 0	LSI Logic Parallel
CD/DVD drive 1	CD/DVD drive 0
Hard disk 1	Virtual Disk
Network adapter 1	VM Network

Memory Size: 8 GB

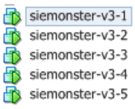
Maximum recommended for this guest OS: 1011 GB.

Maximum recommended for best performance: 131044 MB.

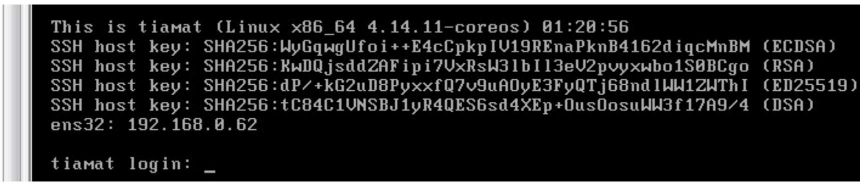
Default recommended for this guest OS: 384 MB.

Minimum recommended for this guest OS: 32 MB.

5. Power on each virtual machine in turn and allow 10 minutes or so for the automatic stack build to complete. When ready, a specific hostname is allocated and shown in the Console view within ESXi.

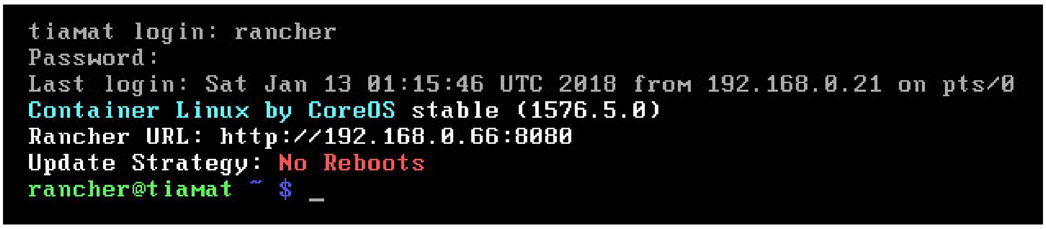


siemonster-v3-1
siemonster-v3-2
siemonster-v3-3
siemonster-v3-4
siemonster-v3-5



```
This is tiamat (Linux x86_64 4.14.11-coreos) 01:20:56
SSH host key: SHA256:WyGqwgUfoi++E4cCpkpIV19REnaPknB4162diqcMnBM (ECDSA)
SSH host key: SHA256:KwDQjsddZAFipi7VxRsW3lbIl3eV2pvyxwbo1S0BCgo (RSA)
SSH host key: SHA256:dP/+kG2uD8PyxxfQ7v9uA0yE3FyQTj68ndlWW1ZWThI (ED25519)
SSH host key: SHA256:tC84C1VNSBJ1yR4QES6sd4XEp+OusOosuWW3f17A9/4 (DSA)
ens32: 192.168.0.62

tiamat login: _
```

6. Within the ESXi Console view, logon to any of the instances with the default credentials (rancher/ s13M0nSterV3).

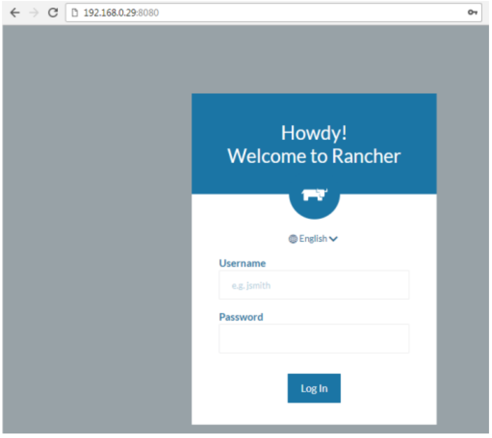


```
tiamat login: rancher
Password:
Last login: Sat Jan 13 01:15:46 UTC 2018 from 192.168.0.21 on pts/0
Container Linux by CoreOS stable (1576.5.0)
Rancher URL: http://192.168.0.66:8080
Update Strategy: No Reboots
rancher@tiamat ~ $ _
```

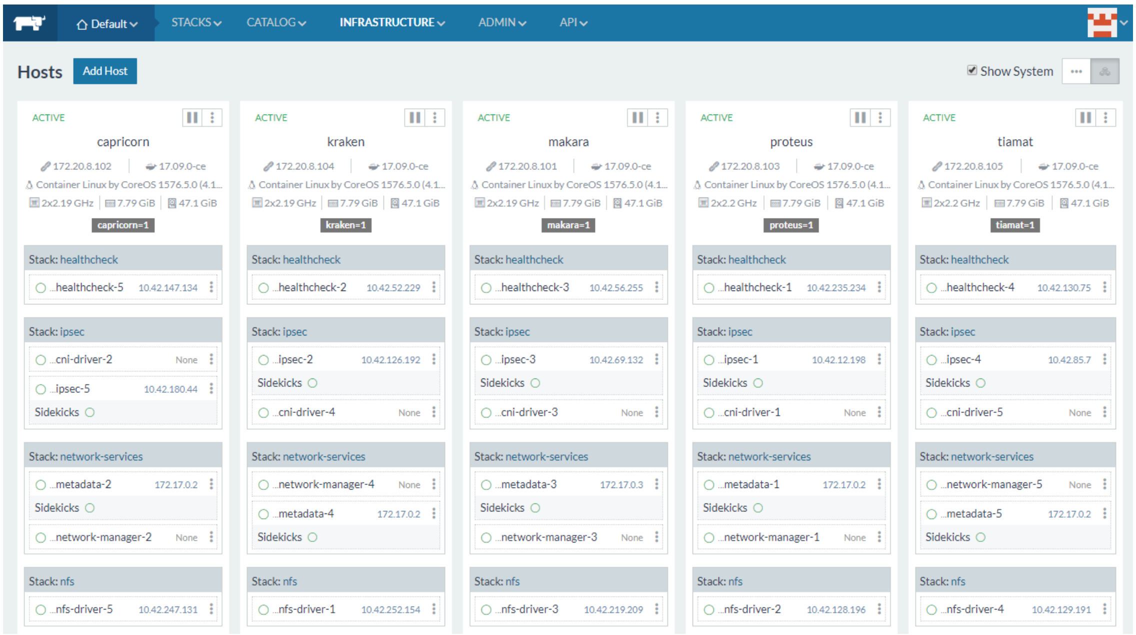
7. The Rancher URL will be shown in the Console.

6.3 RANCHER

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



9. Login with the configured credentials (default admin/siemonster), and navigate to Infrastructure – Hosts



ACTIVE
capricorn
172.20.8.102 | 17.09.0-ce
Container Linux by CoreOS 1576.5.0 (4.1...
2x2.19 GHz | 7.79 GiB | 47.1 GiB
capricorn=1

Stack: healthcheck
○ ...healthcheck-5 10.42.147.134

Stack: ipsec
○ ...cni-driver-2 None
○ ...ipsec-5 10.42.180.44
Sidekicks ○

Stack: network-services
○ ...metadata-2 172.17.0.2
Sidekicks ○
○ ...network-manager-2 None

Stack: nfs
○ ...nfs-driver-5 10.42.247.131

ACTIVE
kraken
172.20.8.104 | 17.09.0-ce
Container Linux by CoreOS 1576.5.0 (4.1...
2x2.19 GHz | 7.79 GiB | 47.1 GiB
kraken=1

Stack: healthcheck
○ ...healthcheck-2 10.42.52.229

Stack: ipsec
○ ...ipsec-2 10.42.126.192
Sidekicks ○
○ ...cni-driver-4 None

Stack: network-services
○ ...network-manager-4 None
○ ...metadata-4 172.17.0.2
Sidekicks ○

Stack: nfs
○ ...nfs-driver-1 10.42.252.154

ACTIVE
makara
172.20.8.101 | 17.09.0-ce
Container Linux by CoreOS 1576.5.0 (4.1...
2x2.19 GHz | 7.79 GiB | 47.1 GiB
makara=1

Stack: healthcheck
○ ...healthcheck-3 10.42.56.255

Stack: ipsec
○ ...ipsec-3 10.42.69.132
Sidekicks ○
○ ...cni-driver-3 None

Stack: network-services
○ ...metadata-3 172.17.0.3
Sidekicks ○
○ ...network-manager-3 None

Stack: nfs
○ ...nfs-driver-3 10.42.219.209

ACTIVE
proteus
172.20.8.103 | 17.09.0-ce
Container Linux by CoreOS 1576.5.0 (4.1...
2x2.2 GHz | 7.79 GiB | 47.1 GiB
proteus=1

Stack: healthcheck
○ ...healthcheck-1 10.42.235.234

Stack: ipsec
○ ...ipsec-1 10.42.12.198
Sidekicks ○
○ ...cni-driver-1 None

Stack: network-services
○ ...metadata-1 172.17.0.2
Sidekicks ○
○ ...network-manager-1 None

Stack: nfs
○ ...nfs-driver-2 10.42.128.196

ACTIVE
tiamat
172.20.8.105 | 17.09.0-ce
Container Linux by CoreOS 1576.5.0 (4.1...
2x2.2 GHz | 7.79 GiB | 47.1 GiB
tiamat=1

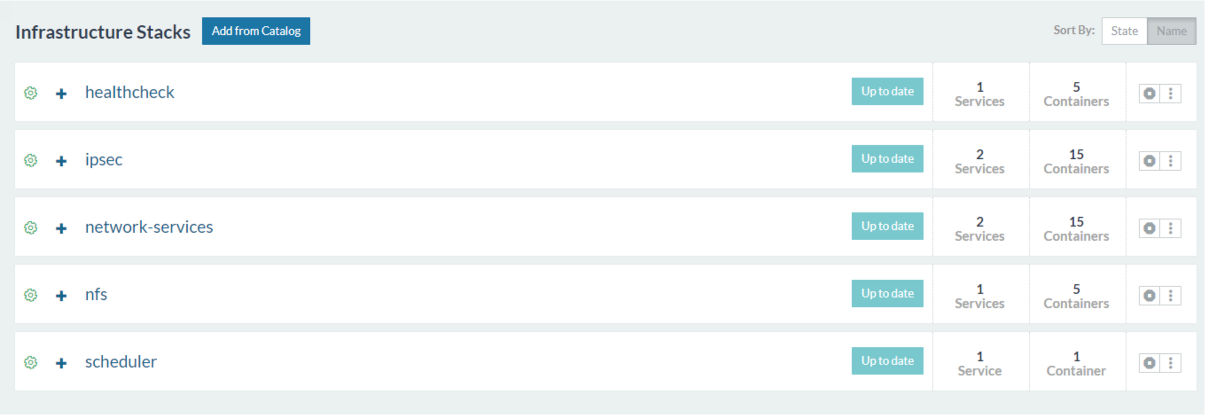
Stack: healthcheck
○ ...healthcheck-4 10.42.130.75

Stack: ipsec
○ ...ipsec-4 10.42.85.7
Sidekicks ○
○ ...cni-driver-5 None

Stack: network-services
○ ...network-manager-5 None
○ ...metadata-5 172.17.0.2
Sidekicks ○

Stack: nfs
○ ...nfs-driver-4 10.42.129.191

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

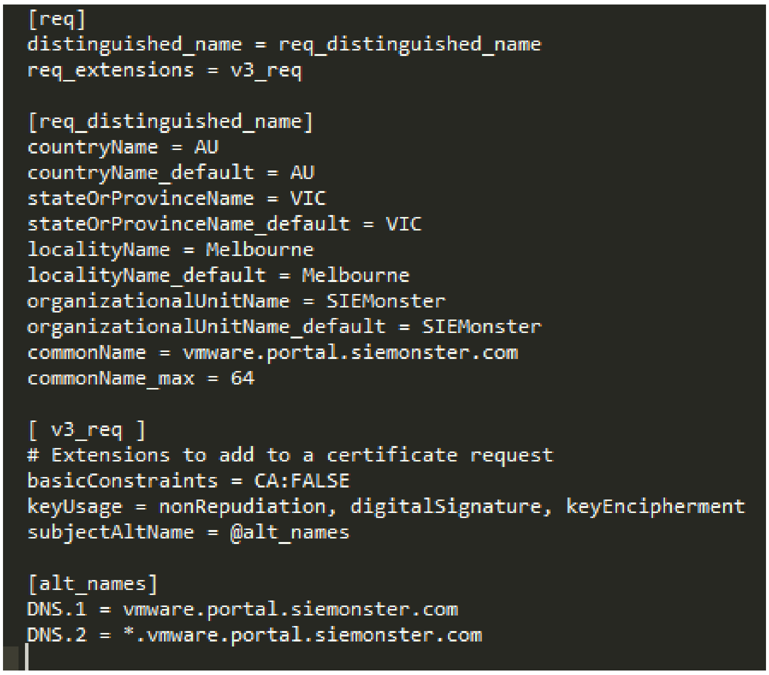


Infrastructure Stacks

Stack	State	Services	Containers
healthcheck	Up to date	1 Services	5 Containers
ipsec	Up to date	2 Services	15 Containers
network-services	Up to date	2 Services	15 Containers
nfs	Up to date	1 Services	5 Containers
scheduler	Up to date	1 Service	1 Container

11. 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.

12. 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:

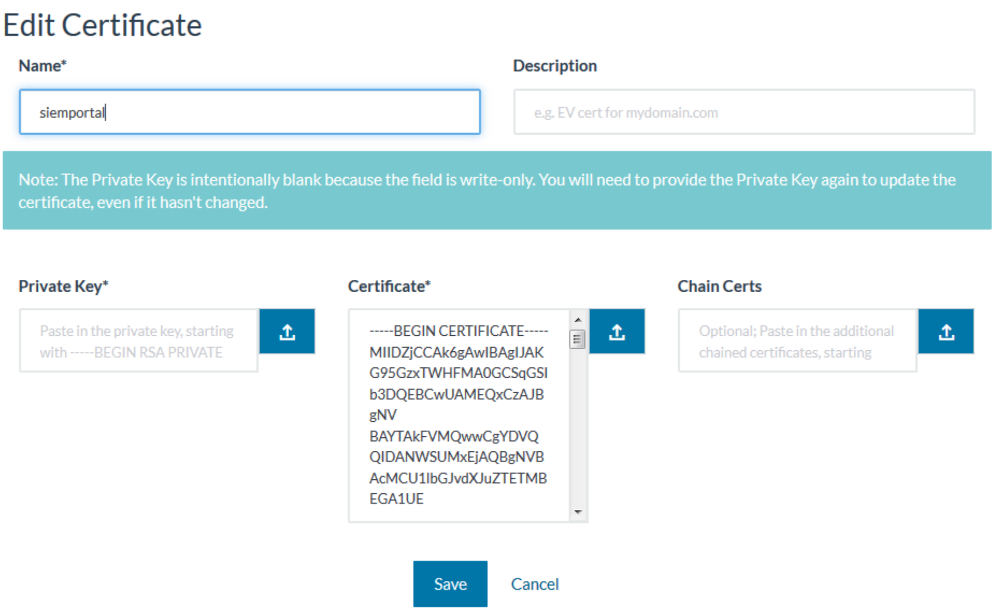


```
[req]
distinguished_name = req_distinguished_name
req_extensions = v3_req

[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
```

13. Next make the script 'generate_certs.sh' executable (chmod +x generate_certs.sh), and run to produce the certificates and .p12 keystore.

14. In the Rancher UI, navigate to Infrastructure – Certificates, edit the existing siemportal certificate, updating the private key and certificate.

15. 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*: siemportal

Description: 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*: Paste in the private key, starting with -----BEGIN RSA PRIVATE

Certificate*:

```
-----BEGIN CERTIFICATE-----
MIIDZjCCAk6gAwIBAgIJAK
G95GzxTWHFMA0GCSqGSI
b3DQEBCwUAMEQxCzAJB
gNV
BAYTAkFVMQwwCgYDVQ
QIDANWSUMxEjAQBgNVB
AcMCU1lbGJvdXJuZTETMB
EGA1UE
```

Chain Certs: Optional; Paste in the additional chained certificates, starting

16. The ‘Name’ field must be set to ‘siemportal’ this is mandatory for the Load Balancer.

17. 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

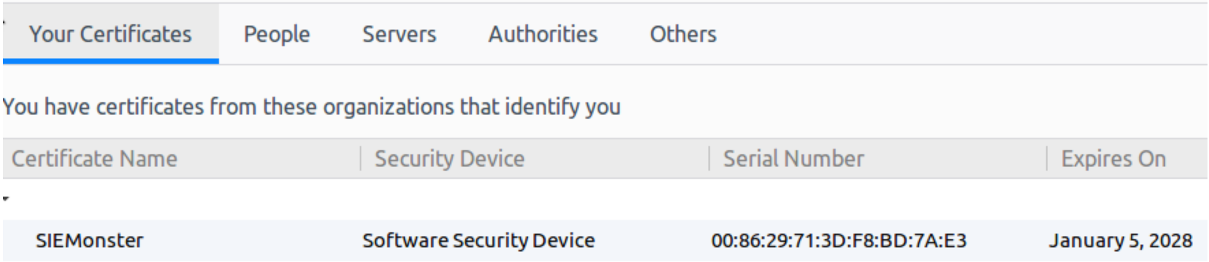
- Click Start, click Start Search, type mmc, and then press ENTER.
- On the File menu, click Add/Remove Snap-in.
- Under Available snap-ins, click Certificates,and then click Add.
- Under This snap-in will always manage certificates for, click Computer account, and then click Next.
- Click Local computer, 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’.

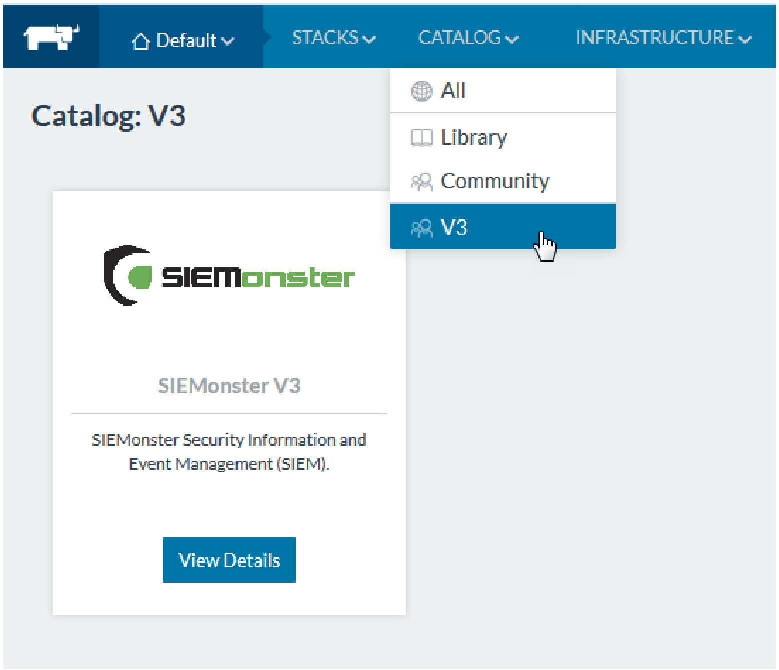


You have certificates from these organizations that identify you

Certificate Name	Security Device	Serial Number	Expires On
SIEMonster	Software Security Device	00:86:29:71:3D:F8:BD:7A:E3	January 5, 2028

6.4 STACK DEPLOYMENT

The SIEMonster V3 application catalog item is pre-loaded.



Catalog: V3

SIEMonster V3

SIEMonster Security Information and Event Management (SIEM).

18. Navigate to the V3 catalog and click ‘View Details’ for the SIEMonster V3 App.

19. 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

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

    For example

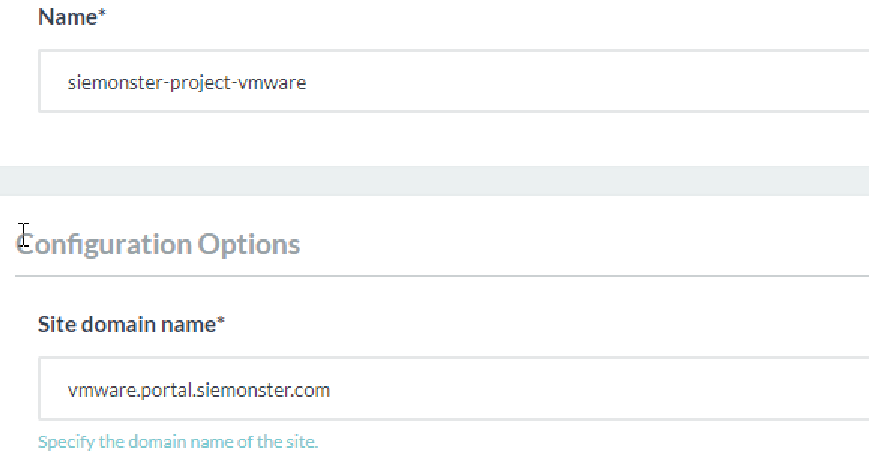
    Name:

    siemonster-project-siemportal will become

    Site domain name:

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

Before



Name*

siemonster-project-vmware

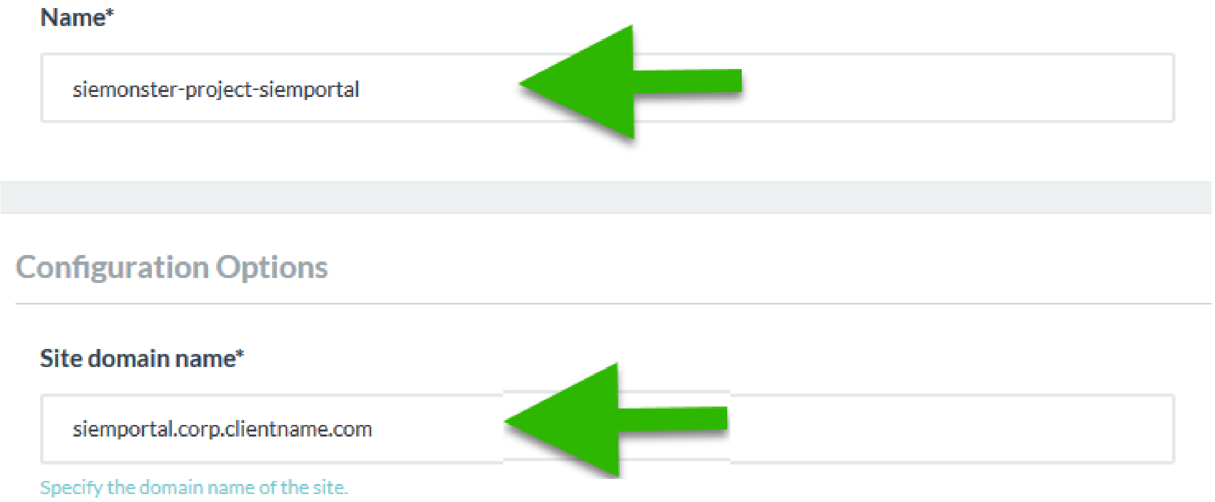
Configuration Options

Site domain name*

vmware.portal.siemonster.com

Specify the domain name of the site.

After



Name*

siemonster-project-siemportal

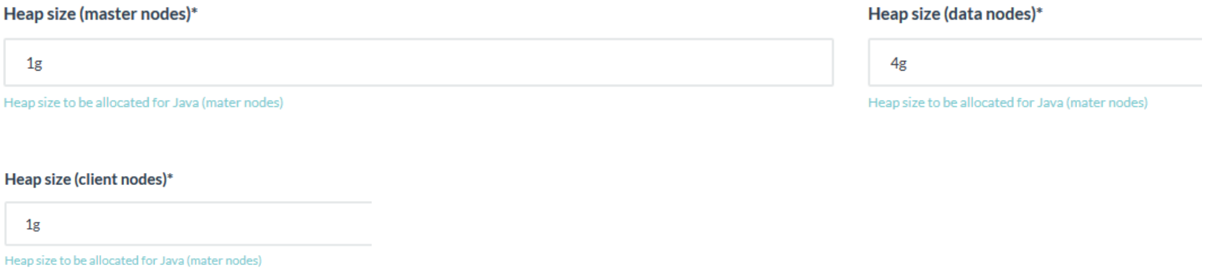
Configuration Options

Site domain name*

siemportal.corp.clientname.com

Specify the domain name of the site.

21. 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)*

1g

Heap size to be allocated for Java (mater nodes)

Heap size (data nodes)*

4g

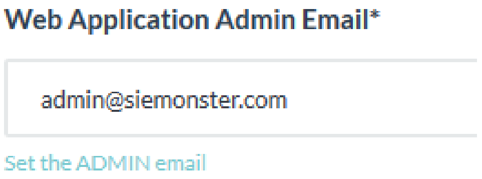
Heap size to be allocated for Java (mater nodes)

Heap size (client nodes)*

1g

Heap size to be allocated for Java (mater nodes)

22. 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

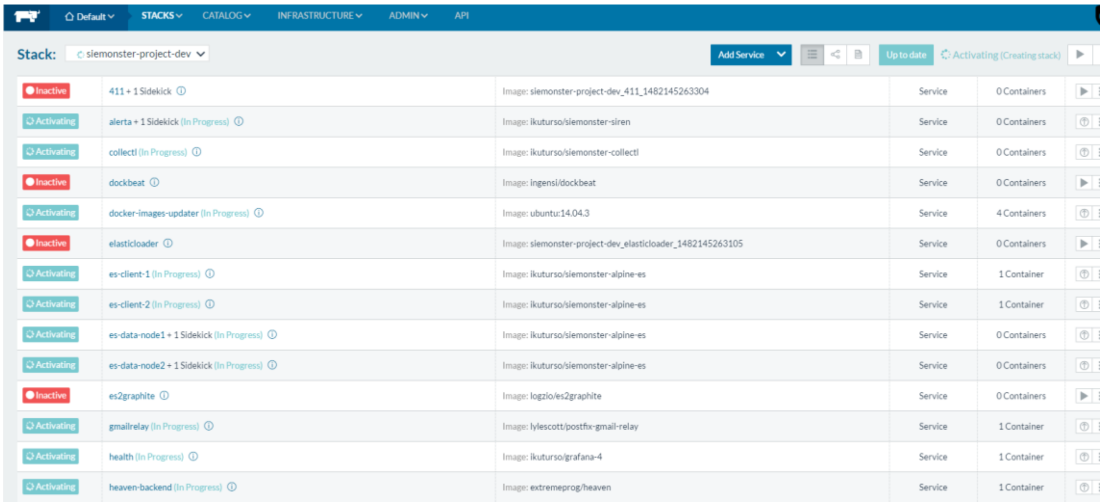
23. The remaining application passwords should be changed from the defaults, see Appendix A for change management table. Aside from the CertAuth, Truststore & KeyStore passwords, all passwords can be changed post-install if required.

24. The SITE_ID option should be left at default, as initially the Logstash Heap Size

25. If Gmail alert relaying is required set the appropriate values. It is recommended to setup a Gmail account specifically for this purpose.

26. Finally, click on ‘Launch’.

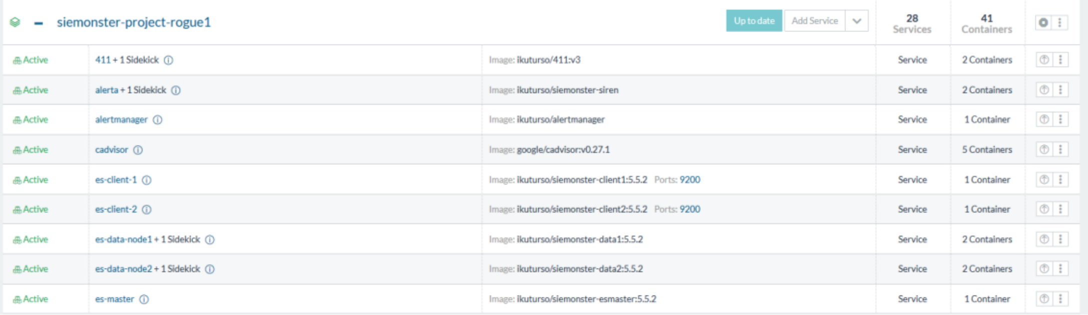
27. The stack will take around 5 - 60 minutes to build, depending on internet connection speed. The status can be viewed under Stacks – User



Stack: siemonster-project-dev

Inactive	411 + 1 Sidekick	Image: siemonster-project-dev_411_1482145263304	Service	0 Containers
Activating	alerta + 1 Sidekick (In Progress)	Image: ikuturso/siemonster-siren	Service	0 Containers
Activating	collectl (In Progress)	Image: ikuturso/siemonster-collectl	Service	0 Containers
Inactive	dockbeat	Image: ingensi/dockbeat	Service	0 Containers
Activating	docker-images-updater (In Progress)	Image: ubuntu:14.04.3	Service	4 Containers
Inactive	elasticloader	Image: siemonster-project-dev_elasticloader_1482145263105	Service	0 Containers
Activating	es-client-1 (In Progress)	Image: ikuturso/siemonster-alpine-es	Service	1 Container
Activating	es-client-2 (In Progress)	Image: ikuturso/siemonster-alpine-es	Service	1 Container
Activating	es-data-node1 + 1 Sidekick (In Progress)	Image: ikuturso/siemonster-alpine-es	Service	0 Containers
Activating	es-data-node2 + 1 Sidekick (In Progress)	Image: ikuturso/siemonster-alpine-es	Service	0 Containers
Inactive	es2graphite	Image: logzio/es2graphite	Service	0 Containers
Activating	gmailrelay (In Progress)	Image: lylescott/postfix-gmail-relay	Service	1 Container
Activating	health (In Progress)	Image: ikuturso/grafana-4	Service	1 Container
Activating	heaven-backend (In Progress)	Image: extremeprog/heaven	Service	1 Container

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



			28 Services	41 Containers
Active	411 + 1 Sidekick	Image: ikuturso/411:v3	Service	2 Containers
Active	alerta + 1 Sidekick	Image: ikuturso/siemonster-siren	Service	2 Containers
Active	alertmanager	Image: ikuturso/alertmanager	Service	1 Container
Active	cadvisor	Image: google/cadvisor:v0.27.1	Service	5 Containers
Active	es-client-1	Image: ikuturso/siemonster-client1:5.5.2 Ports: 9200	Service	1 Container
Active	es-client-2	Image: ikuturso/siemonster-client2:5.5.2 Ports: 9200	Service	1 Container
Active	es-data-node1 + 1 Sidekick	Image: ikuturso/siemonster-data1:5.5.2	Service	2 Containers
Active	es-data-node2 + 1 Sidekick	Image: ikuturso/siemonster-data2:5.5.2	Service	2 Containers
Active	es-master	Image: ikuturso/siemonster-esmaster:5.5.2	Service	1 Container

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.

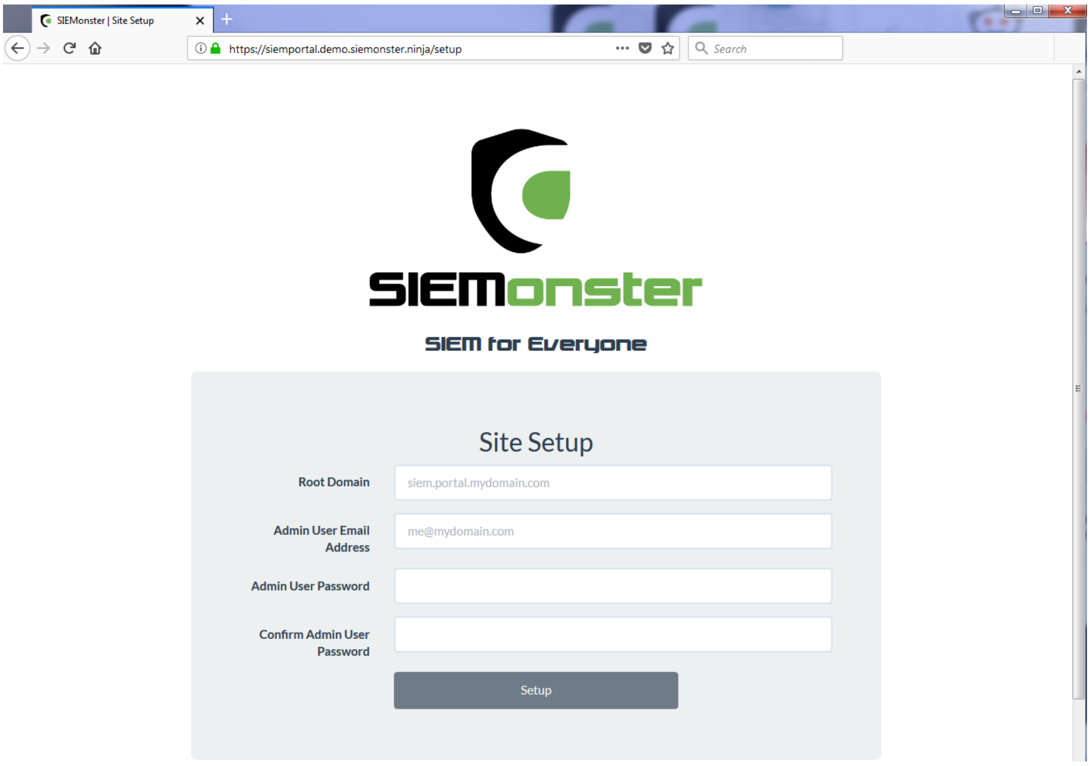
Using a local DNS server, zone entries are required for site.dname.com and *.site.dname.com, e.g.
siemportal.corp.clientname.com
*. siemportal.corp.clientname.com

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



SIEMonster | Site Setup

https://siemportal.demo.siemonster.ninja/setup

SIEM for Everyone

Site Setup

Root Domain: siem.portal.mydomain.com

Admin User Email Address: me@mydomain.com

Admin User Password:

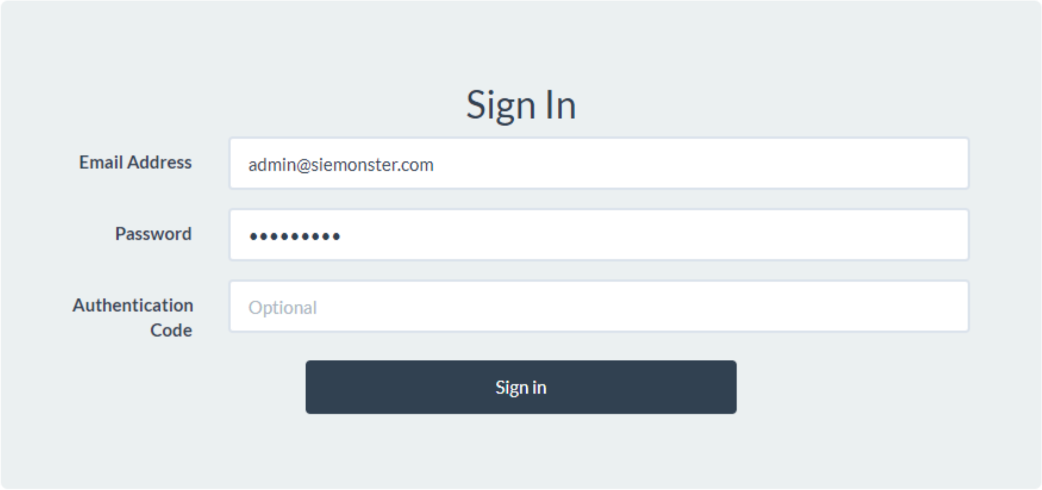
Confirm Admin User Password:

- 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:



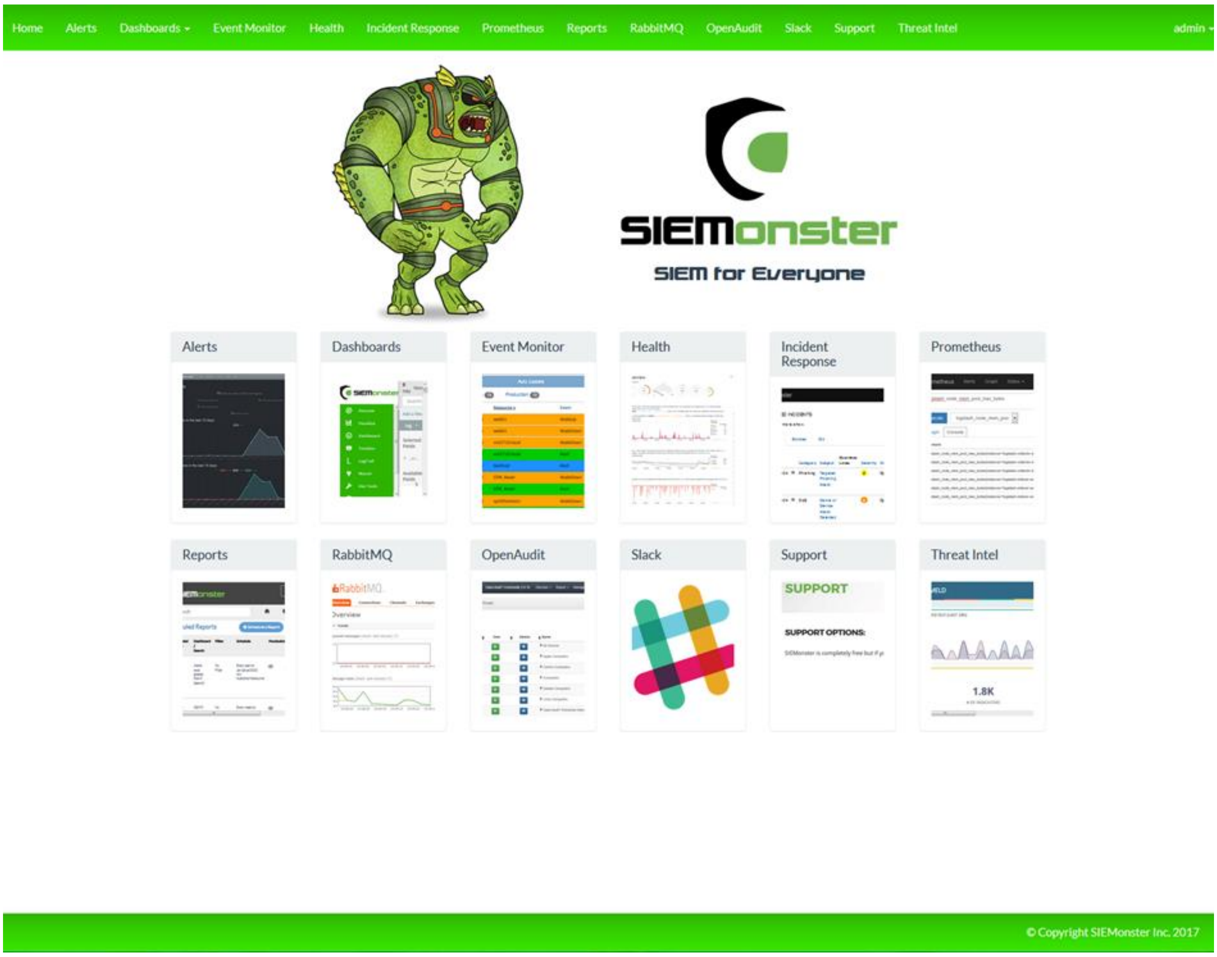
Sign In

Email Address: admin@siemonster.com

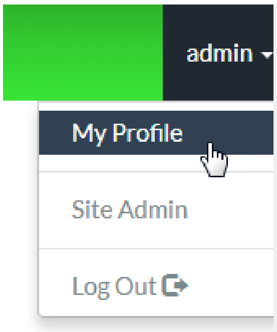
Password: •••••••••

Authentication Code: Optional

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.



8 USER SETUP



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

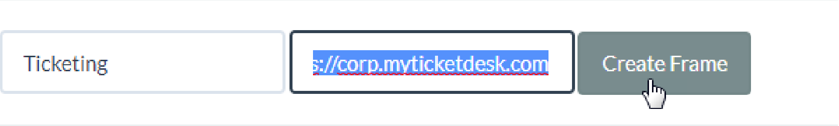
This includes changing the display name, changing the password or adding two factor authentication.

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).

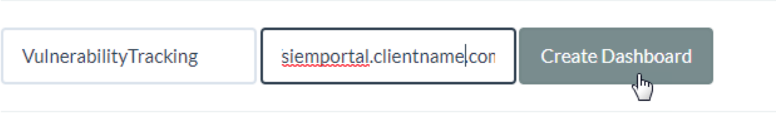
New frames may also be added using the ‘Create Frame’ option:



Ticketing

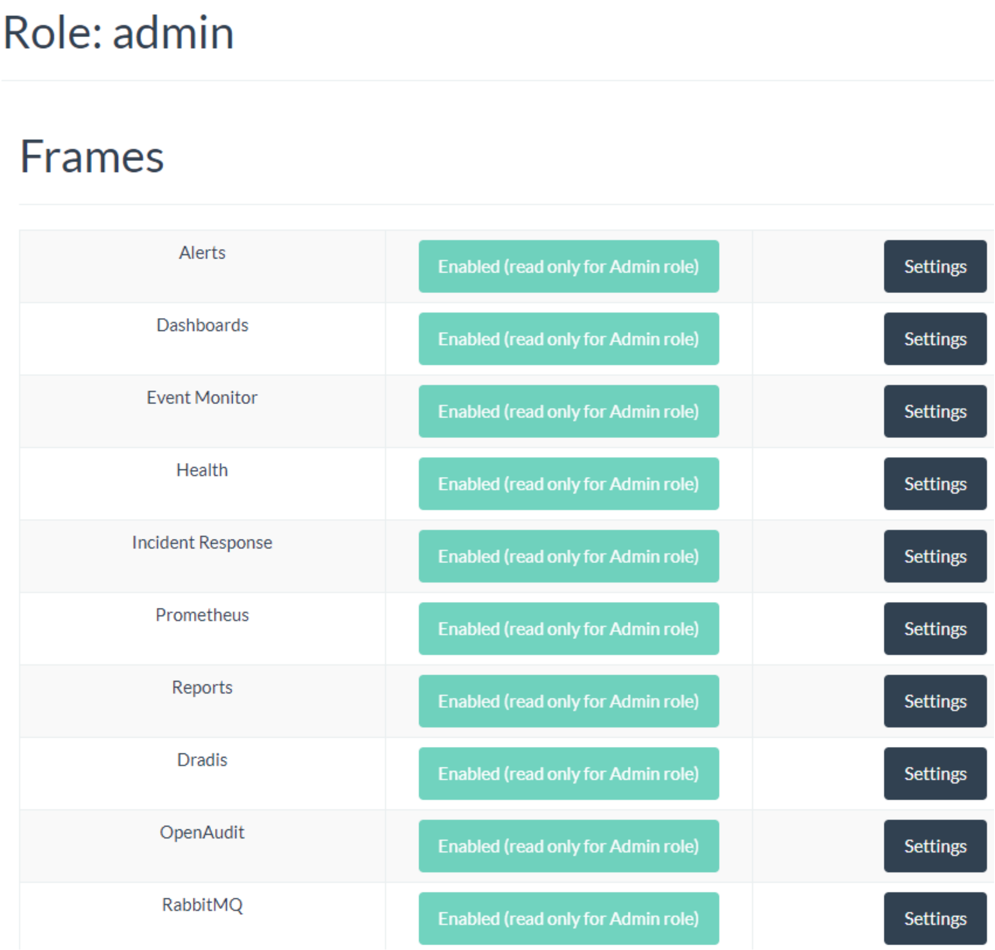
s://corp.myticketdesk.com

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



VulnerabilityTracking

siemportal.clientname.con

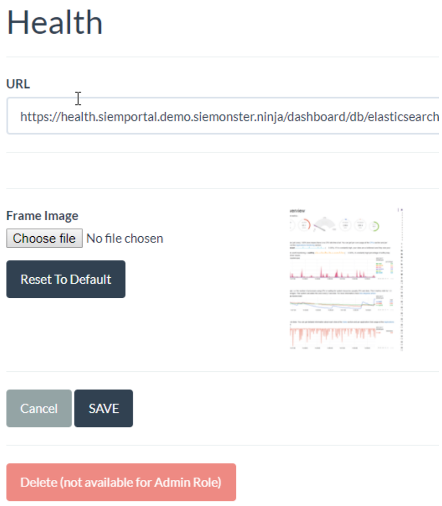


Role: admin

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.

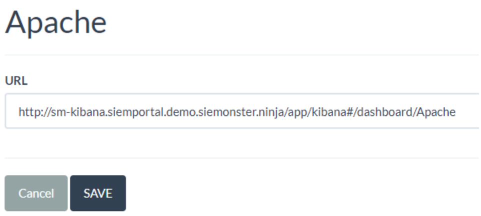


Health

URL: https://health.siemportal.demo.siemonster.ninja/dashboard/db/elasticsearch

Frame Image: Choose file No file chosen

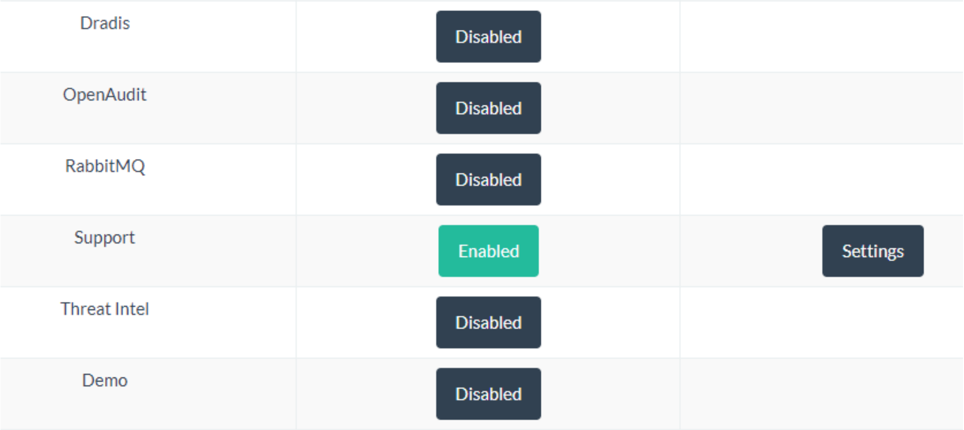
Similarly, the default Dashboard URLs may be modified to suit if required.



Apache

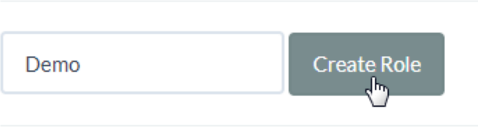
URL: http://sm-kibana.siemportal.demo.siemonster.ninja/app/kibana#/dashboard/Apache

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.



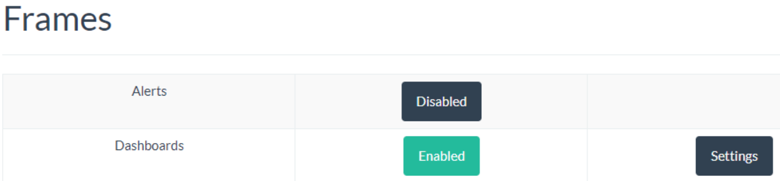
Dradis	Disabled	
OpenAudit	Disabled	
RabbitMQ	Disabled	
Support	Enabled	Settings
Threat Intel	Disabled	
Demo	Disabled	

New roles may be added using the ‘Create Role’ option.



Demo

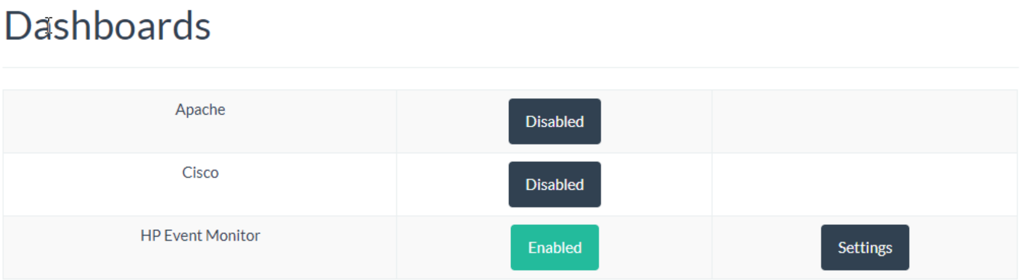
Access to relevant frames can be enabled and settings modified if required.



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.

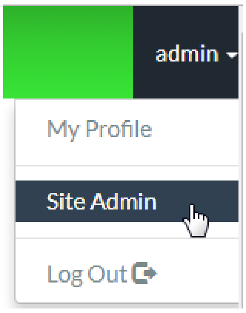


Dashboards

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

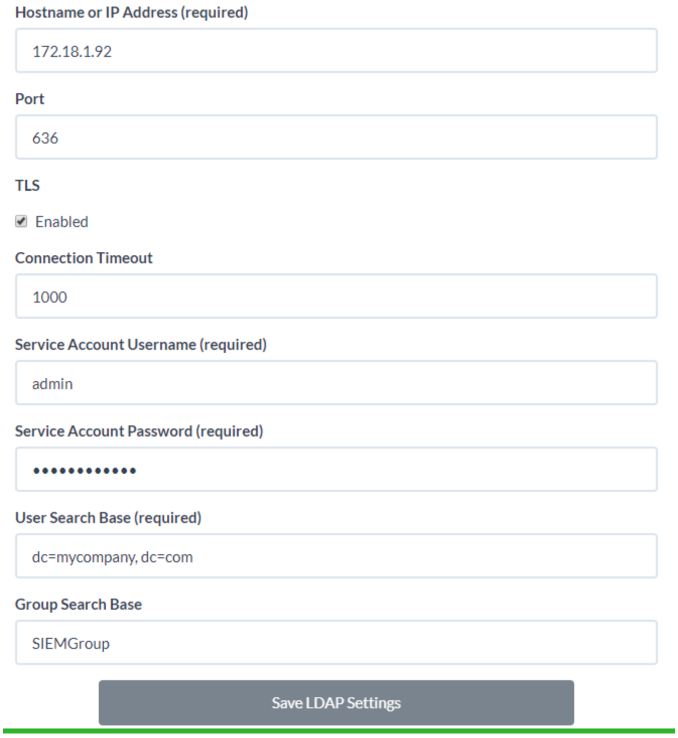
Email settings are configured to use Mailgun, for which a free account can be setup at https://www.mailgun.com/ This mail account is for the web application only, which will send out notifications when a user logs on to the SIEM.

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)
172.18.1.92

Port
636

TLS
☑ Enabled

Connection Timeout
1000

Service Account Username (required)
admin

Service Account Password (required)
••••••••••••

User Search Base (required)
dc=mycompany, dc=com

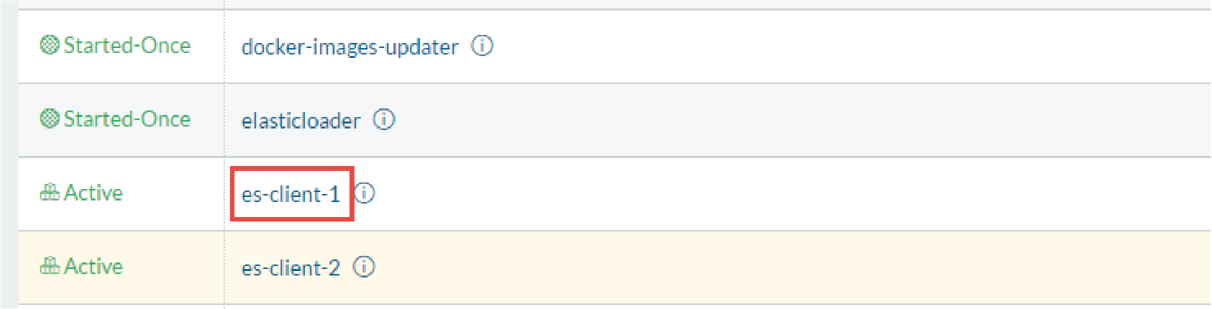
Group Search Base
SIEMGroup

10 OPERATIONAL OVERVIEW

10.1 LOG VIEW

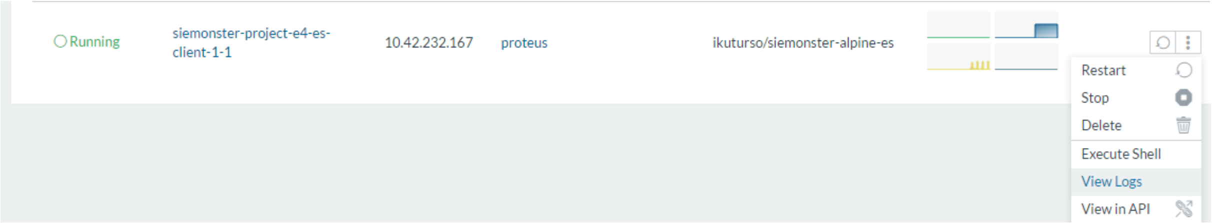
The logs for each container can be viewed within the Rancher Server UI as follows:

First click on a container

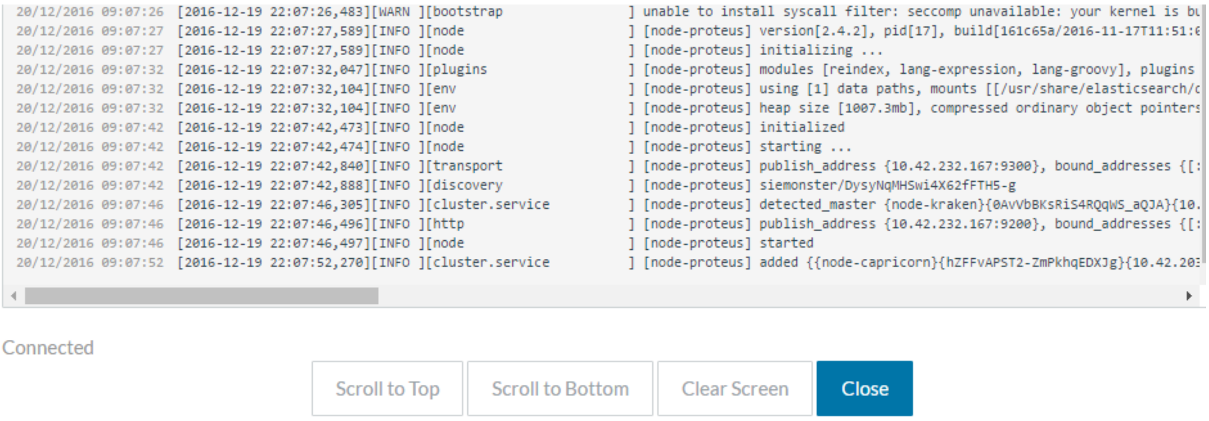


Started-Once	docker-images-updater ⓘ
Started-Once	elasticloader ⓘ
Active	es-client-1 ⓘ
Active	es-client-2 ⓘ

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



○ Running siemonster-project-e4-es-client-1-1 10.42.232.167 proteus ikuturso/siemonster-alpine-es



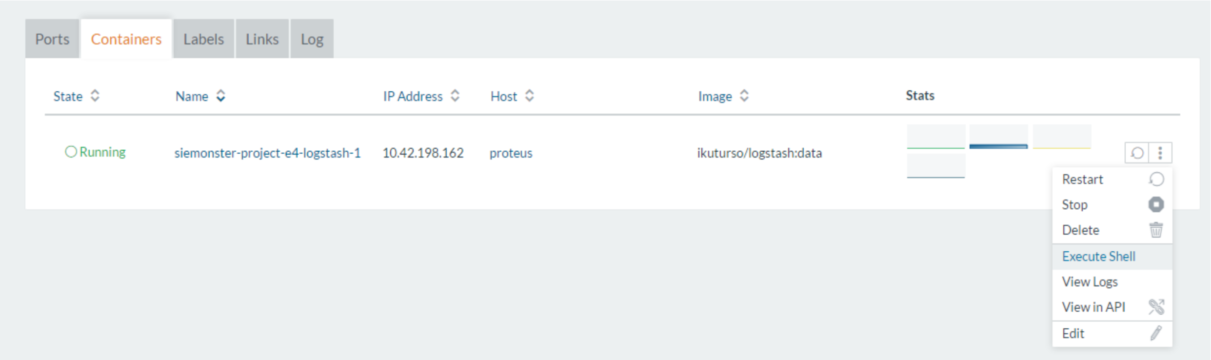
```
20/12/2016 09:07:26  [2016-12-19 22:07:26,483][WARN ][bootstrap                ] unable to install syscall filter: seccomp unavailable: your kernel is bu
20/12/2016 09:07:27  [2016-12-19 22:07:27,589][INFO ][node                     ] [node-proteus] version[2.4.2], pid[17], build[161c65a/2016-11-17T11:51:
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/
20/12/2016 09:07:32  [2016-12-19 22:07:32,104][INFO ][env                      ] [node-proteus] heap size [1007.3mb], compressed ordinary object pointer
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] siemonster/DysyNqMHSwi4X62fFTH5-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

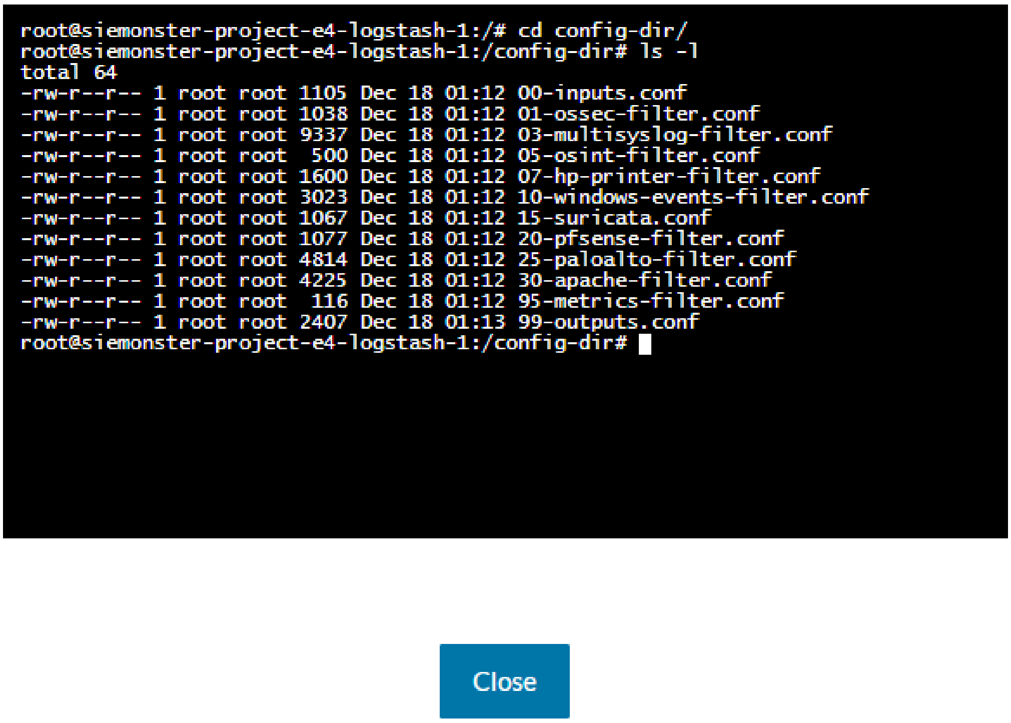
Useful for diagnostics and maintenance, the logs for any container can be viewed in this manner.

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.

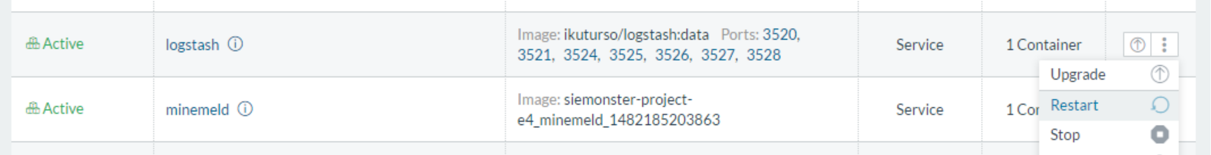


State	Name	IP Address	Host	Image	Stats
○ Running	siemonster-project-e4-logstash-1	10.42.198.162	proteus	ikuturso/logstash:data	



```
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# 
```

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

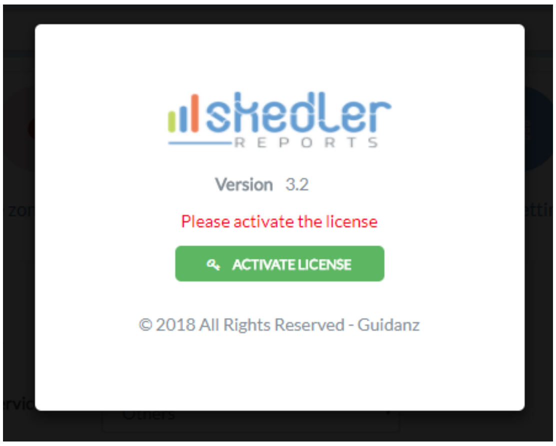


Active	logstash ⓘ	Image: ikuturso/logstash:data Ports: 3520, 3521, 3524, 3525, 3526, 3527, 3528	Service	1 Container
Active	minemeld ⓘ	Image: siemonster-project-e4_minemeld_1482185203863	Service	1 Cor

11 SKEDLER LICENSING

Reports - Menu

Click on ‘Activate License’



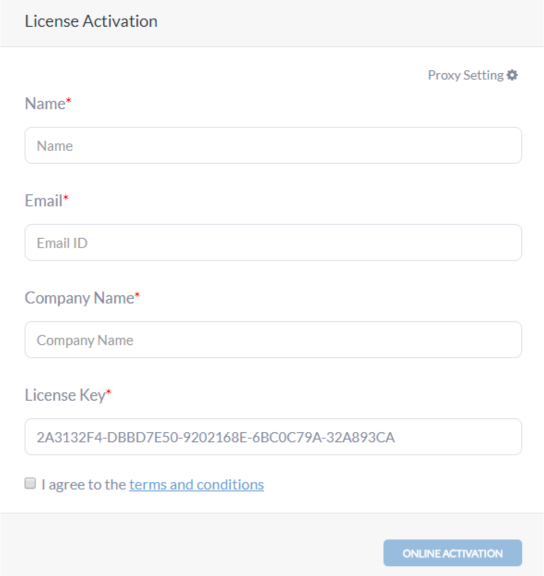
skedler REPORTS

Version 3.2

Please activate the license

ACTIVATE LICENSE

© 2018 All Rights Reserved - Guidanz



License Activation

Proxy Setting ⚙

Name*

Name

Email*

Email ID

Company Name*

Company Name

License Key*

2A3132F4-DBBD7E50-9202168E-6BC0C79A-32A893CA

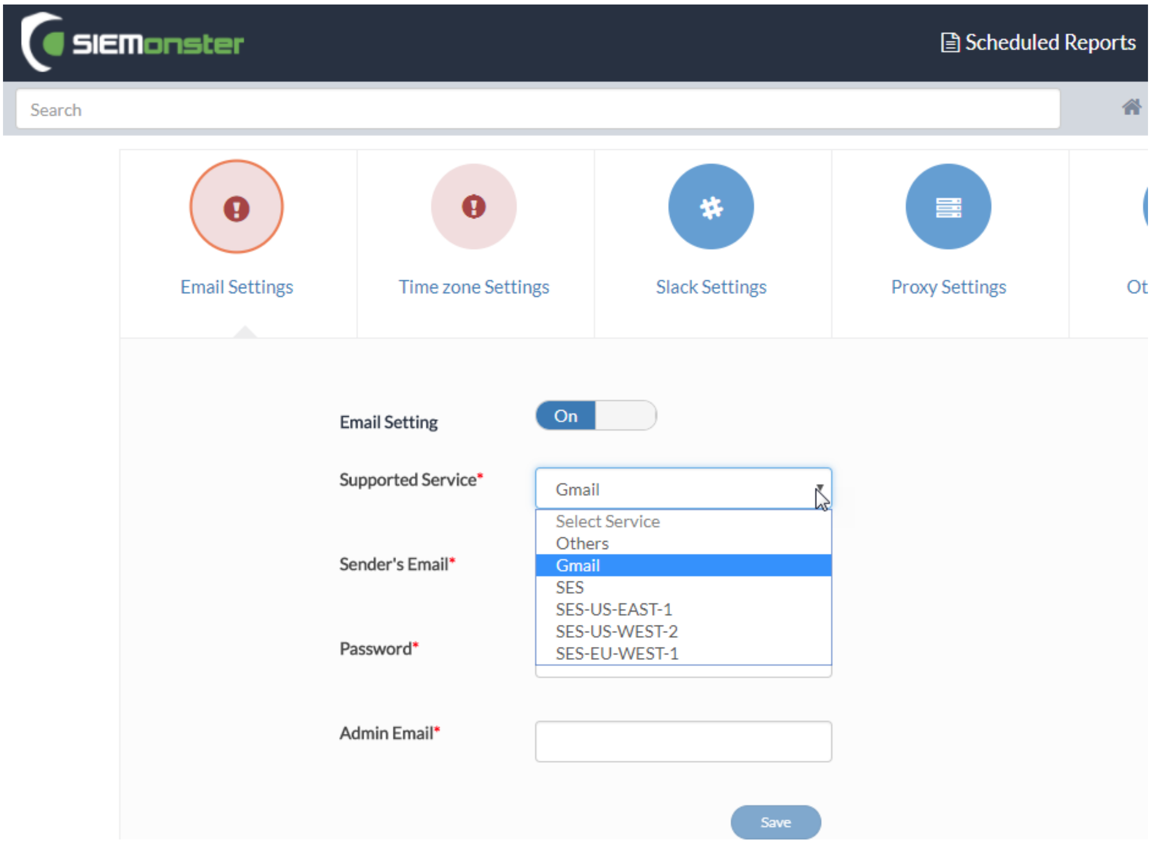
□ I agree to the terms and conditions

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.



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	mimemeld
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