clusterz.io

Cloud monitoring
using
CHR and Big-Data

Summary

- About Us
- General background on CHR
- CHR Amazon EC2 installing
- CHR Use cases
- Cloud monitoring elements
- Reporting , Alerting and Trigger

clusterz.io

>whoami

Shlomi Gutman

CTO of **Voicenter** *(Israel)*
VP of Cloud Products at **QXIP** *(Amsterdam)*

MikroTik MTCNA | MikroTik MTCTCE | MikroTik MTCRE | MikroTik MTCINE

KAMAILIO | opensips | Asterisk | elastic

VOICENTER

Let's talk business

Voicenter is A leading telecommunication technology company providing top-tier business telephony since 2007

We are delivering a ‘One-stop-shop’ solution for business all around the world

Telecom Services

PBX

Call Center Solution

QXIP - Voice Capture Engineering & Development

QXIP *{QuickSIP}* is an R&D Company specializing in Open-Source and Commercial Voice Technology Development.

What’s CHR?

Cloud Hosted Router (CHR) is a RouterOS version intended for running as a virtual machine.

It supports the x86 64-bit architecture and can be used on most of the popular hypervisors such as VMWare, Hyper-V, VirtualBox and others.

CHR has full RouterOS features enabled by default but has a different licensing model than other RouterOS versions.

CHR Licensing License

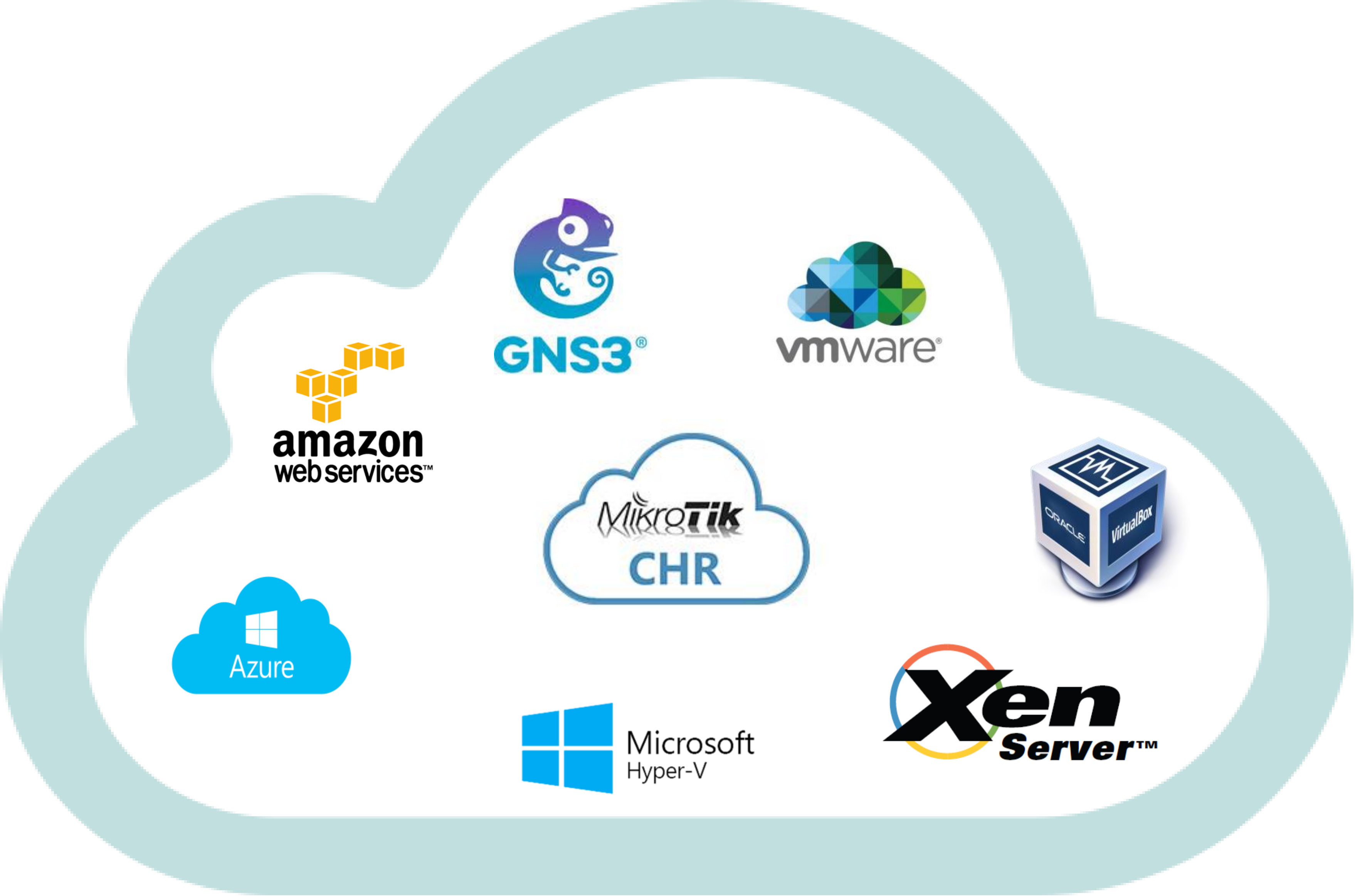
Perpetual is a lifetime license - buy once, use forever .

It is possible to transfer a perpetual license to another CHR instance.

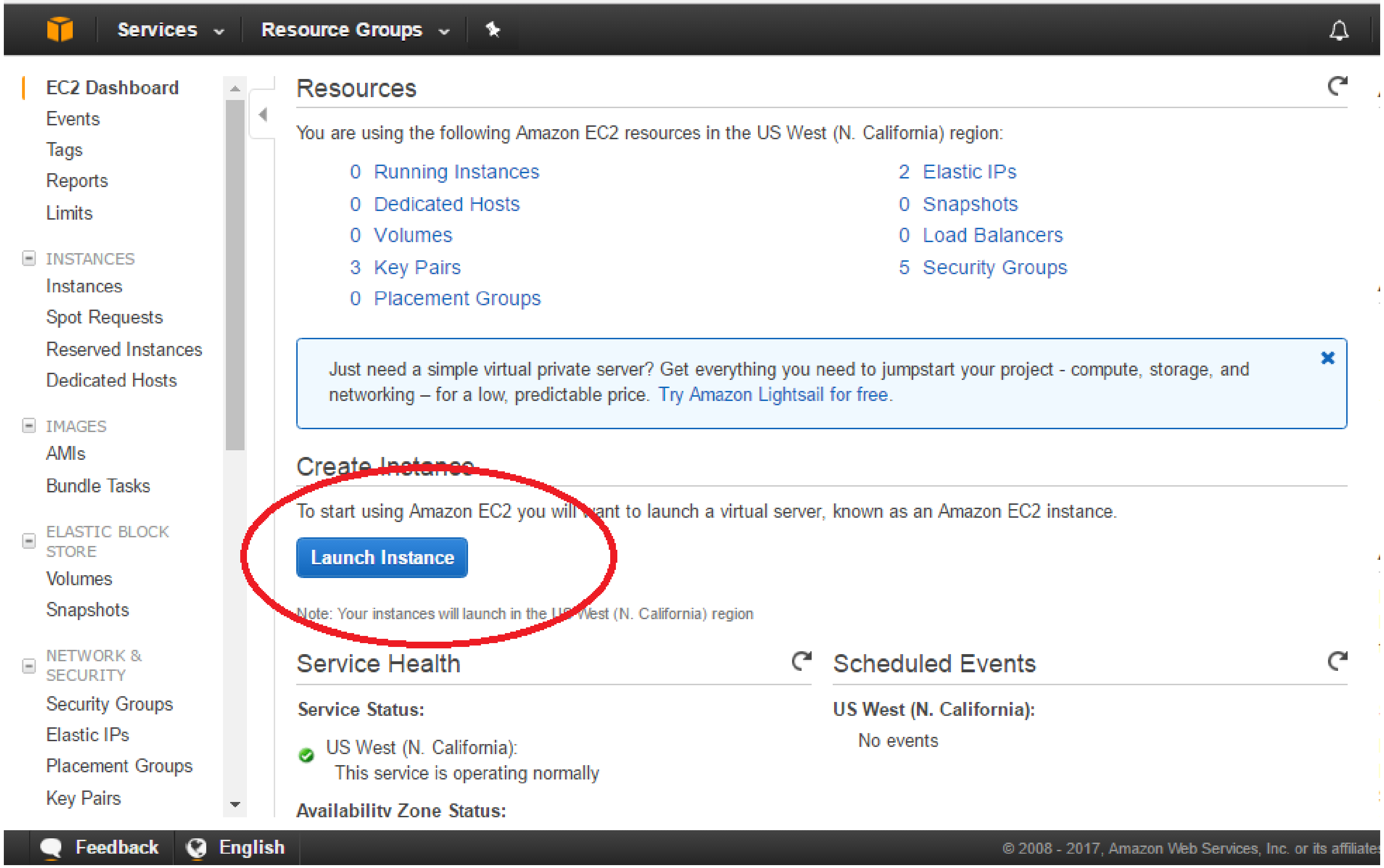
License	Speed limit	Price
Free	1Mbit	FREE
P1	1Gbit	45$
P10	10Gbit	95$
P-Unlimited	Unlimited	250$

If the CHR instance will not be able to access the account server to renew the license ,
it will behave as if the trial period has ran out and will not allow an upgrade of RouterOS to a newer version.

CHR hosting environment



Installing CHR on AWS – Step 1



Resources

You are using the following Amazon EC2 resources in the US West (N. California) region:

0 Running Instances	2 Elastic IPs
0 Dedicated Hosts	0 Snapshots
0 Volumes	0 Load Balancers
3 Key Pairs	5 Security Groups
0 Placement Groups	

Just need a simple virtual private server? Get everything you need to jumpstart your project - compute, storage, and networking – for a low, predictable price. Try Amazon Lightsail for free.

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

Launch Instance

Note: Your instances will launch in the US West (N. California) region

Service Health

Service Status:

US West (N. California):
This service is operating normally

Availability Zone Status:

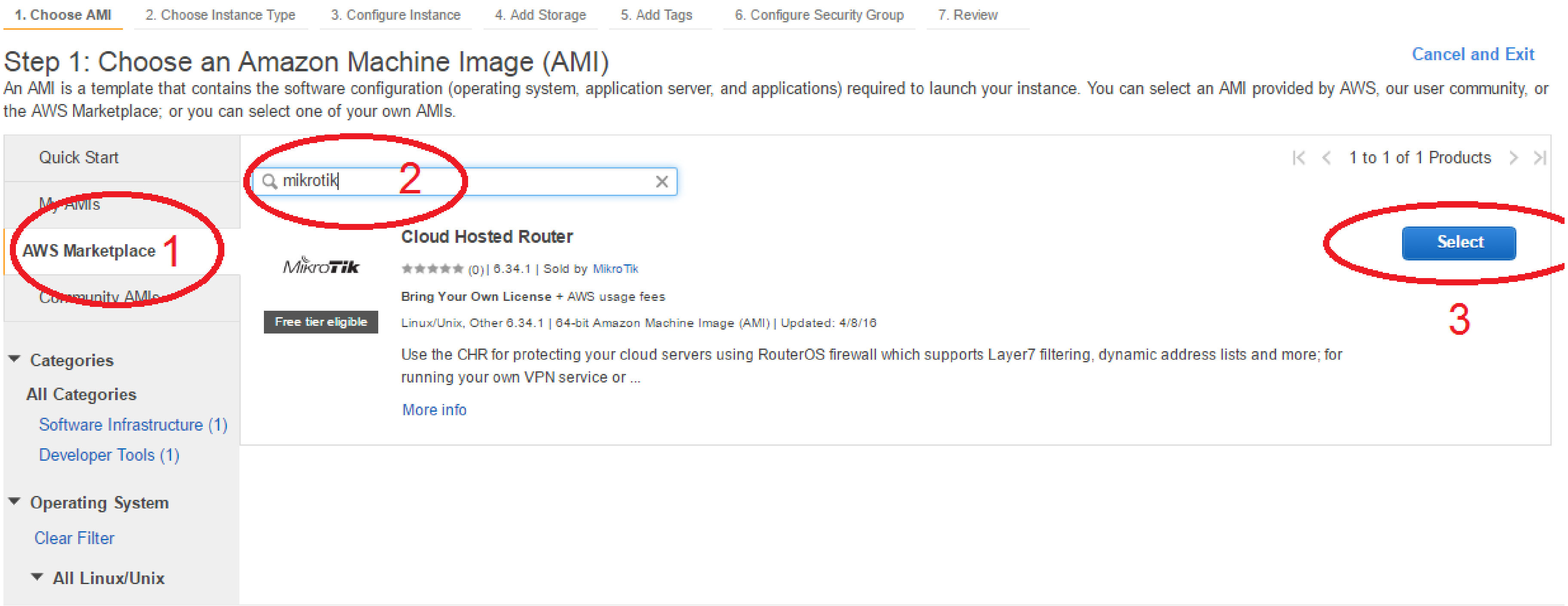
Scheduled Events

US West (N. California):
No events

© 2008 - 2017, Amazon Web Services, Inc. or its affiliates

clusterz.io

Select CHR Image (AMI)– Step 2



1. Choose AMI | 2. Choose Instance Type | 3. Configure Instance | 4. Add Storage | 5. Add Tags | 6. Configure Security Group | 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Cloud Hosted Router

★★★★★ (0) | 6.34.1 | Sold by MikroTik

Bring Your Own License + AWS usage fees

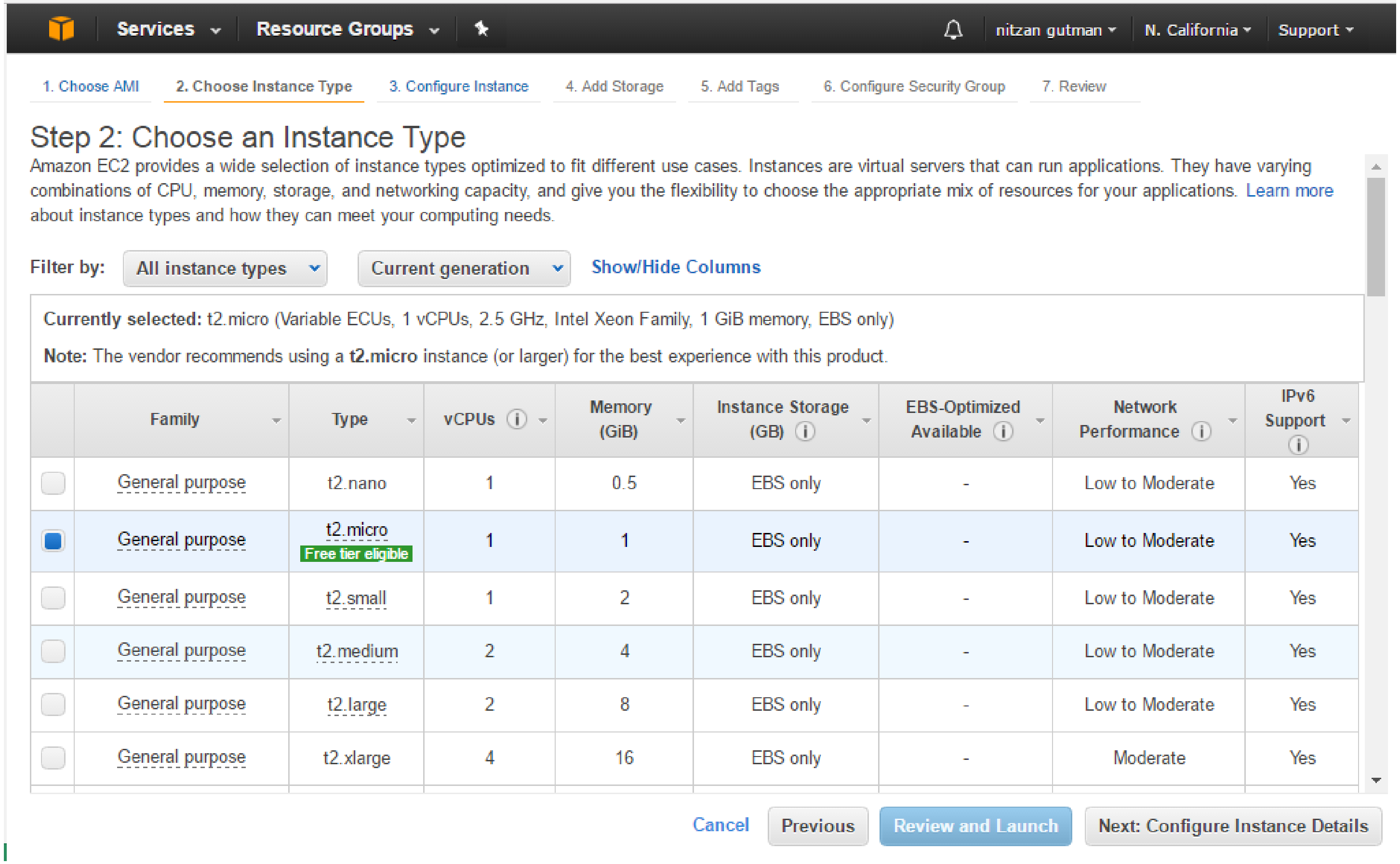
Linux/Unix, Other 6.34.1 | 64-bit Amazon Machine Image (AMI) | Updated: 4/8/16

Use the CHR for protecting your cloud servers using RouterOS firewall which supports Layer7 filtering, dynamic address lists and more; for running your own VPN service or ...

More info

clusterz.io

Select Instance Tab – Step 3



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types | Current generation | Show/Hide Columns

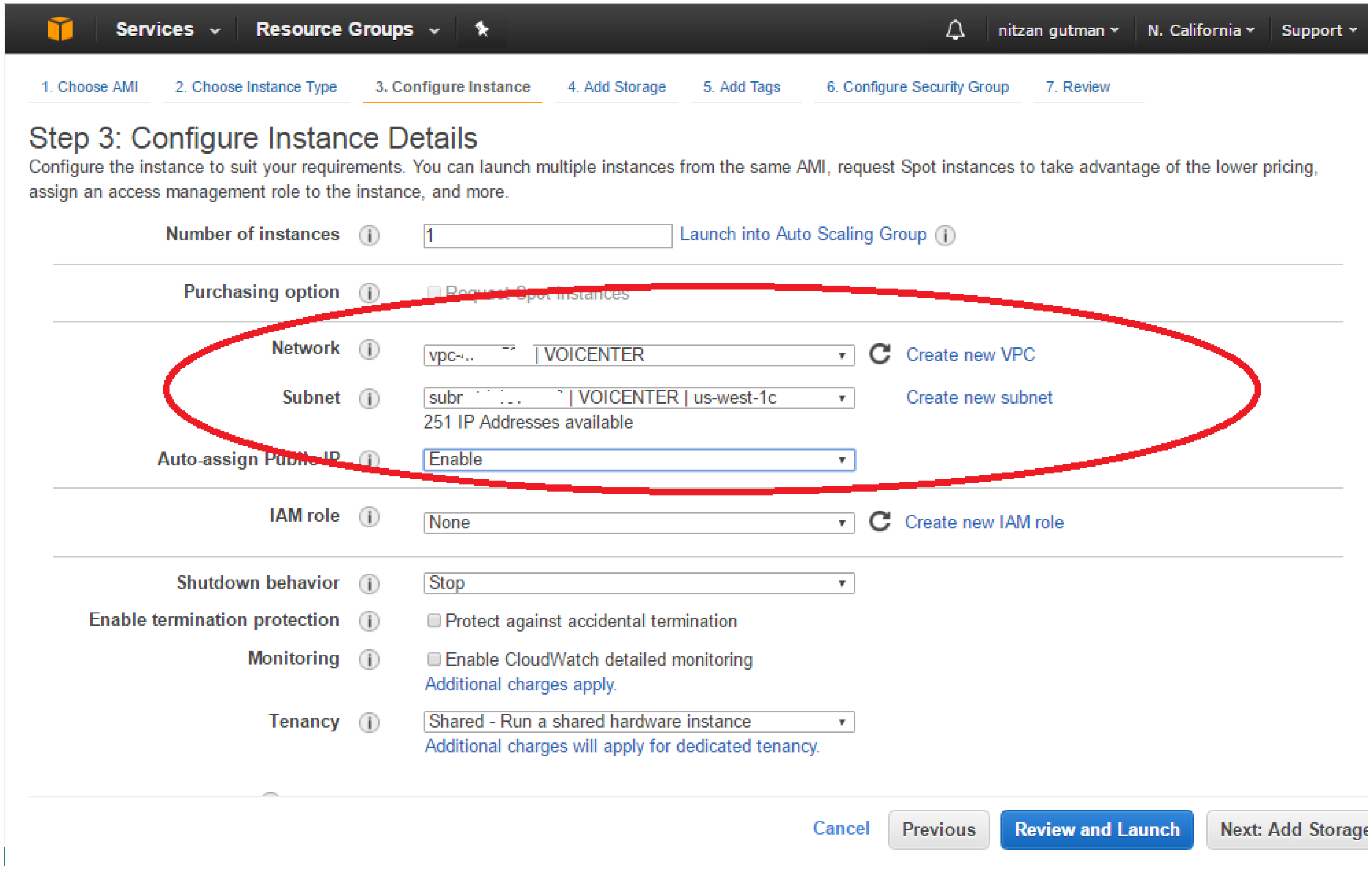
Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

Note: The vendor recommends using a **t2.micro** instance (or larger) for the best experience with this product.

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
□	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
■	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes

clusterz.io

Setup your network – Step 4



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-[redacted] | VOICENTER — Create new VPC

Subnet: subr[redacted] | VOICENTER | us-west-1c — Create new subnet
251 IP Addresses available

Auto-assign Public IP: Enable

IAM role: None — Create new IAM role

Shutdown behavior: Stop

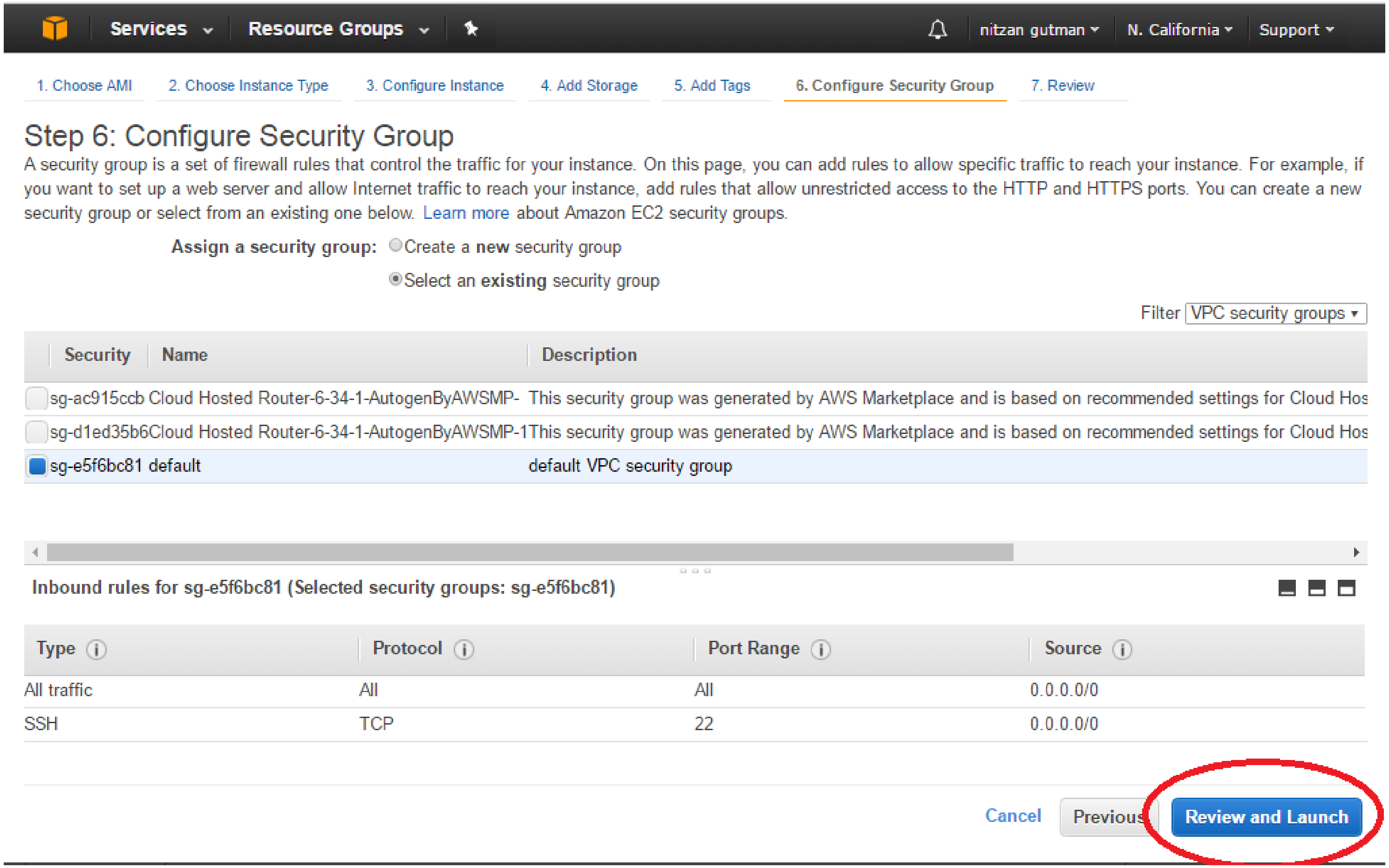
Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

clusterz.io

Configure – Step 5



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group

● Select an **existing** security group

Filter VPC security groups ▾

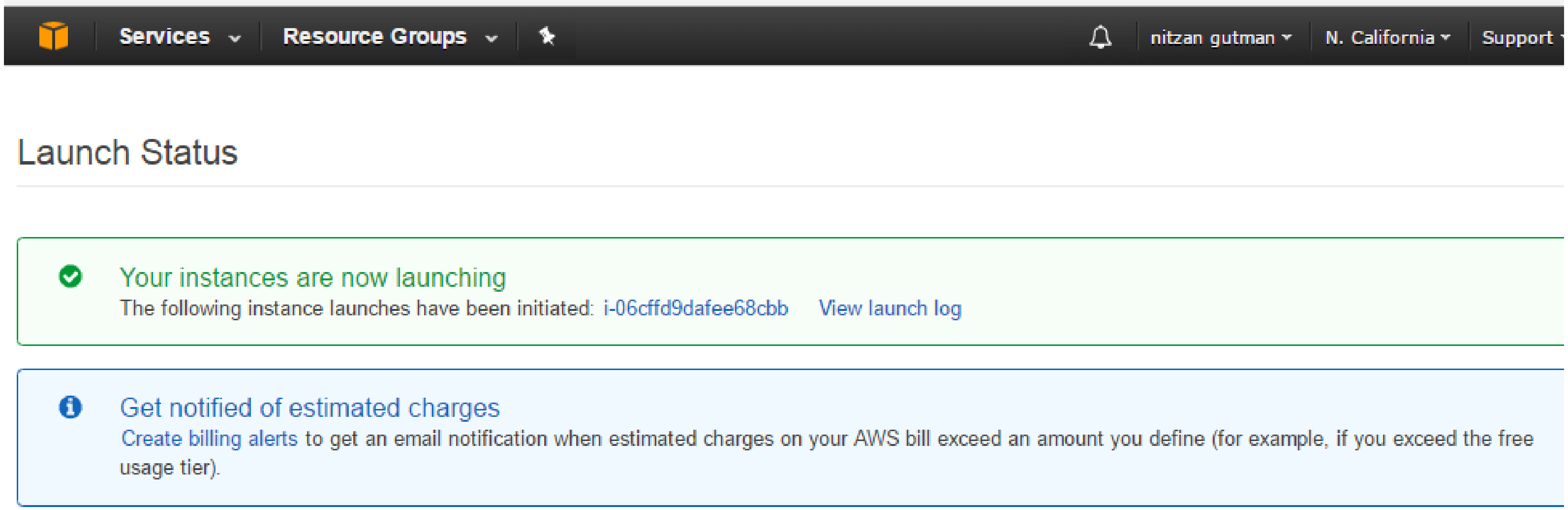
	Security	Name	Description
□	sg-ac915ccb	Cloud Hosted Router-6-34-1-AutogenByAWSMP-	This security group was generated by AWS Marketplace and is based on recommended settings for Cloud Hos
□	sg-d1ed35b6	Cloud Hosted Router-6-34-1-AutogenByAWSMP-1	This security group was generated by AWS Marketplace and is based on recommended settings for Cloud Hos
■	sg-e5f6bc81	default	default VPC security group

Inbound rules for sg-e5f6bc81 (Selected security groups: sg-e5f6bc81)

Type	Protocol	Port Range	Source
All traffic	All	All	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0

clusterz.io

Installing CHR on AWS – Step 6



Launch Status

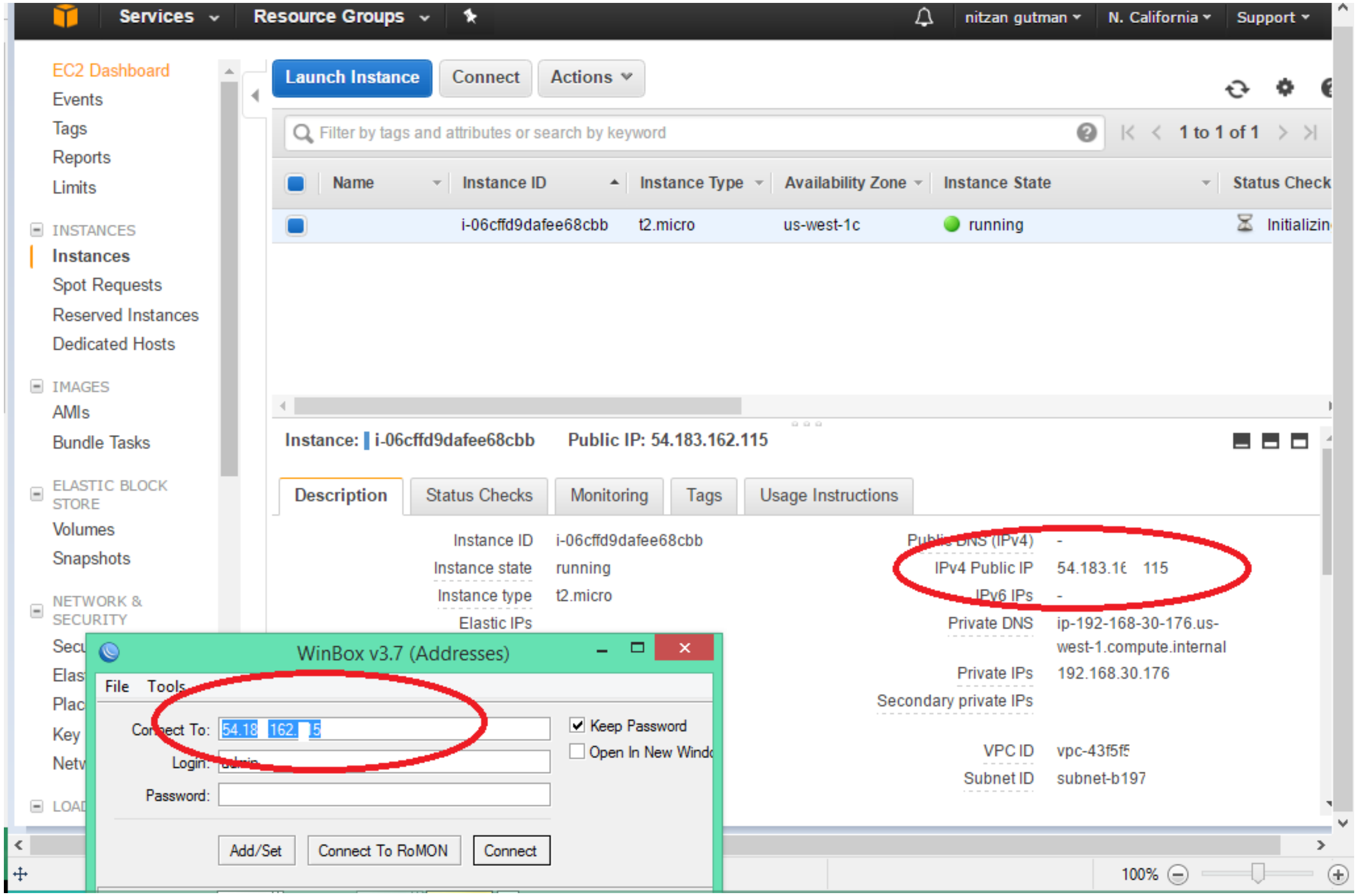
Your instances are now launching

The following instance launches have been initiated: i-06cffd9dafee68cbb View launch log

Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

Finally... Winbox ... IP... Connect ...



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Check
	i-06cffd9dafee68cbb	t2.micro	us-west-1c	● running	Initializin

Instance: i-06cffd9dafee68cbb   Public IP: 54.183.162.115

Instance ID i-06cffd9dafee68cbb
Instance state running
Instance type t2.micro
Elastic IPs

Public DNS (IPv4) -
IPv4 Public IP 54.183.16   115
IPv6 IPs -
Private DNS ip-192-168-30-176.us-west-1.compute.internal
Private IPs 192.168.30.176
Secondary private IPs
VPC ID vpc-43f5f5
Subnet ID subnet-b197

Connect To: 54.18 162. 5
Login: admin
Password:
☑ Keep Password
□ Open In New Windo

clusterz.io

Change Password !!!

CHR - Use case Types

- Virtual Instance
  - ✓ Custom hardware
  - ✓ Management - Dude ,RADIUS
  - ✓ Labs setup

clusterz.io

Virtualization – CHR vs x86

Why use the CHR instead of the traditional x86 VM?

- Optimized for Virtualization

  64 bit support
  Fastpath support
  Driver support

- Paravirtualized NIC –

  Using the CHR allows us to use the a paravirtualized NIC which is capable of speeds beyond 10 Gbps.
  The E1000 NIC used in the x86 VM is only capable of 1Gbps.

- Future proof – The CHR will continue to be developed

CHR - Use case Types

- Cloud Connectivity
  - ✓ VPN cloud - **Road Warrior**
  - ✓ Direct Connect alternative
  - ✓ Secure distributed cloud environment

clusterz.io

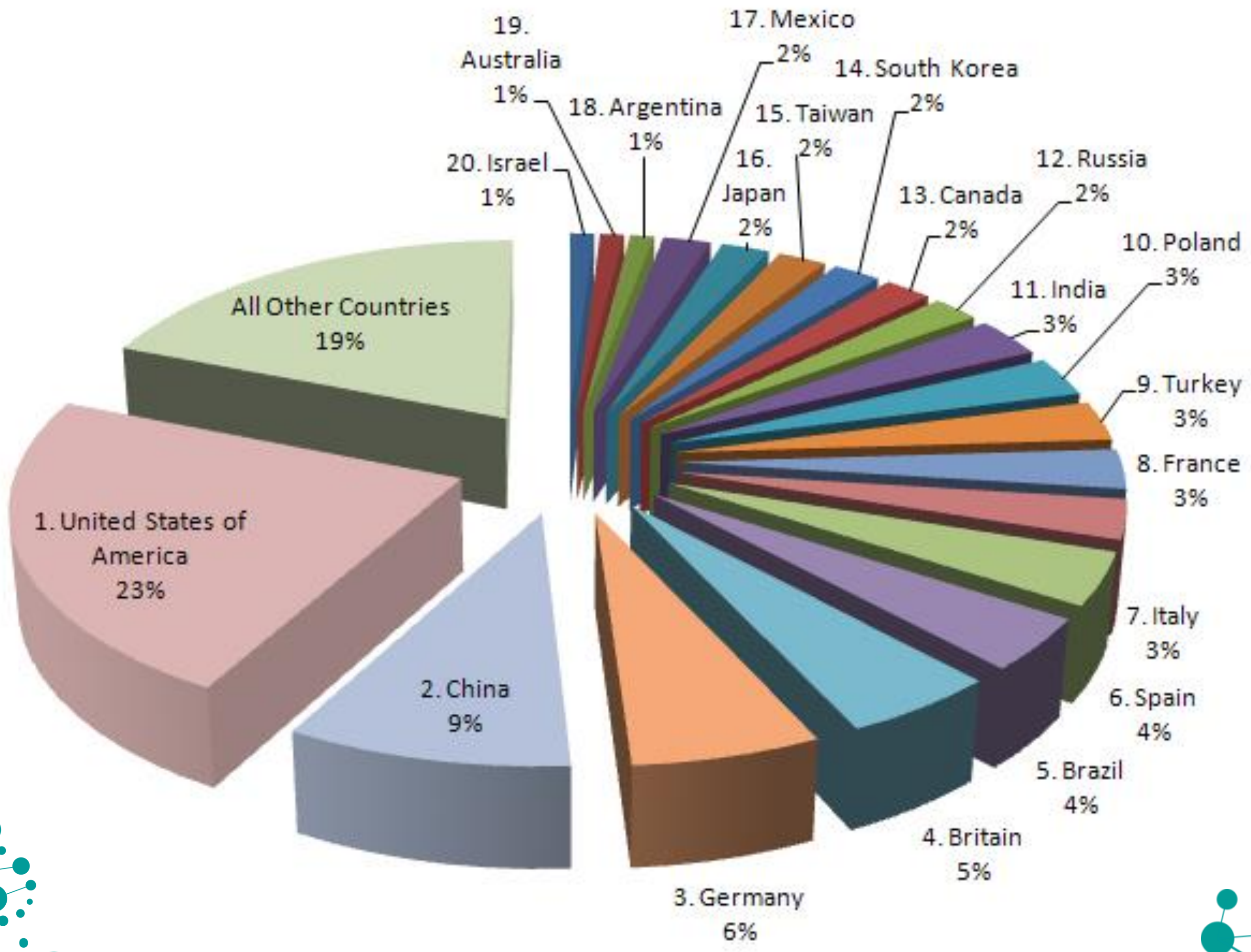
CHR - Use case Types

- Cloud monitoring
  - ✓ Cyber Defense
  - ✓ Billing Logic on Steroids
  - ✓ Centralized Log Analyze

clusterz.io

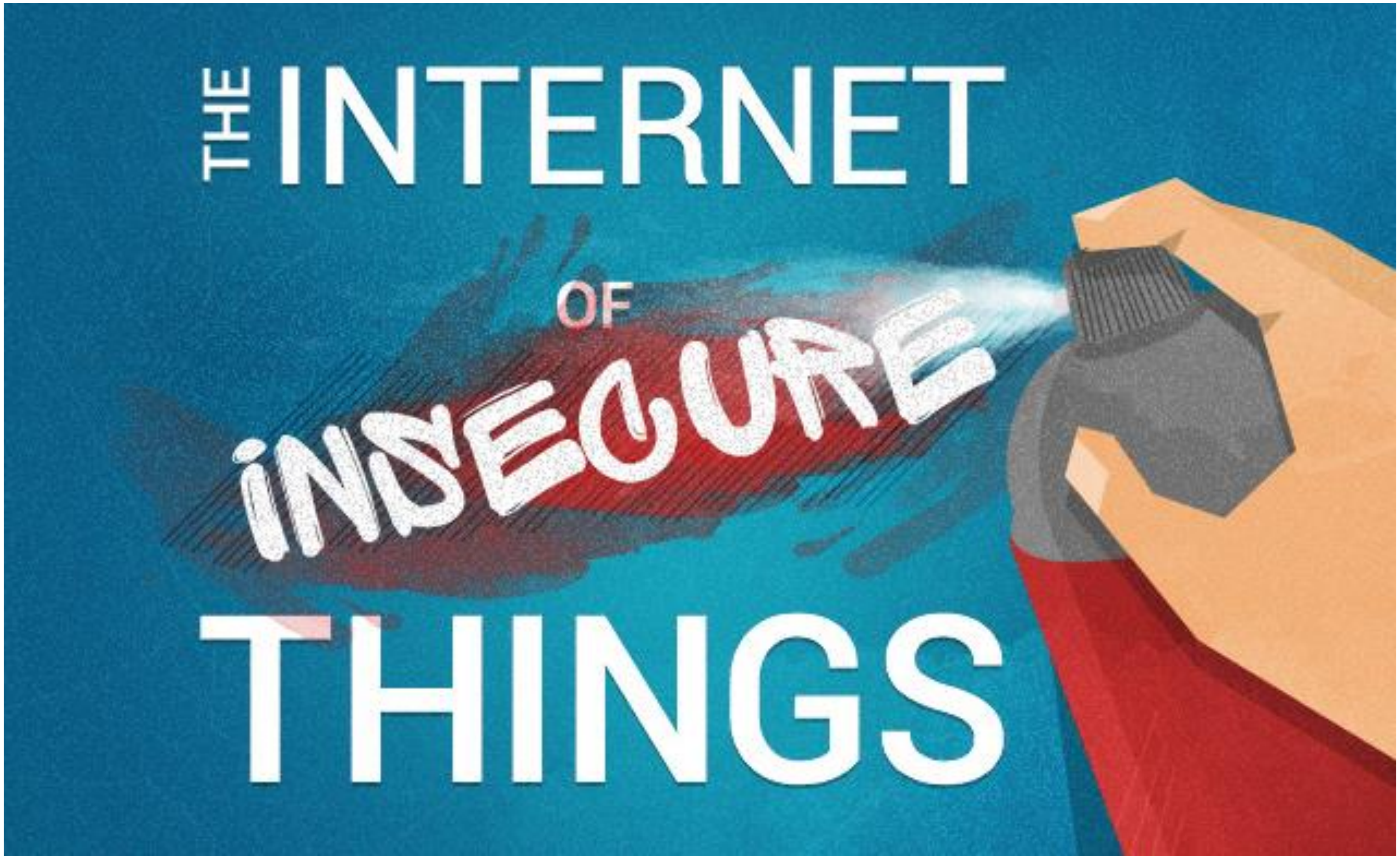
CYBERWAR
END OF THE WORLD
(AS WE KNOW IT)
YOURWALLPAPER.COM

Cyber crime top 20 countries attracts



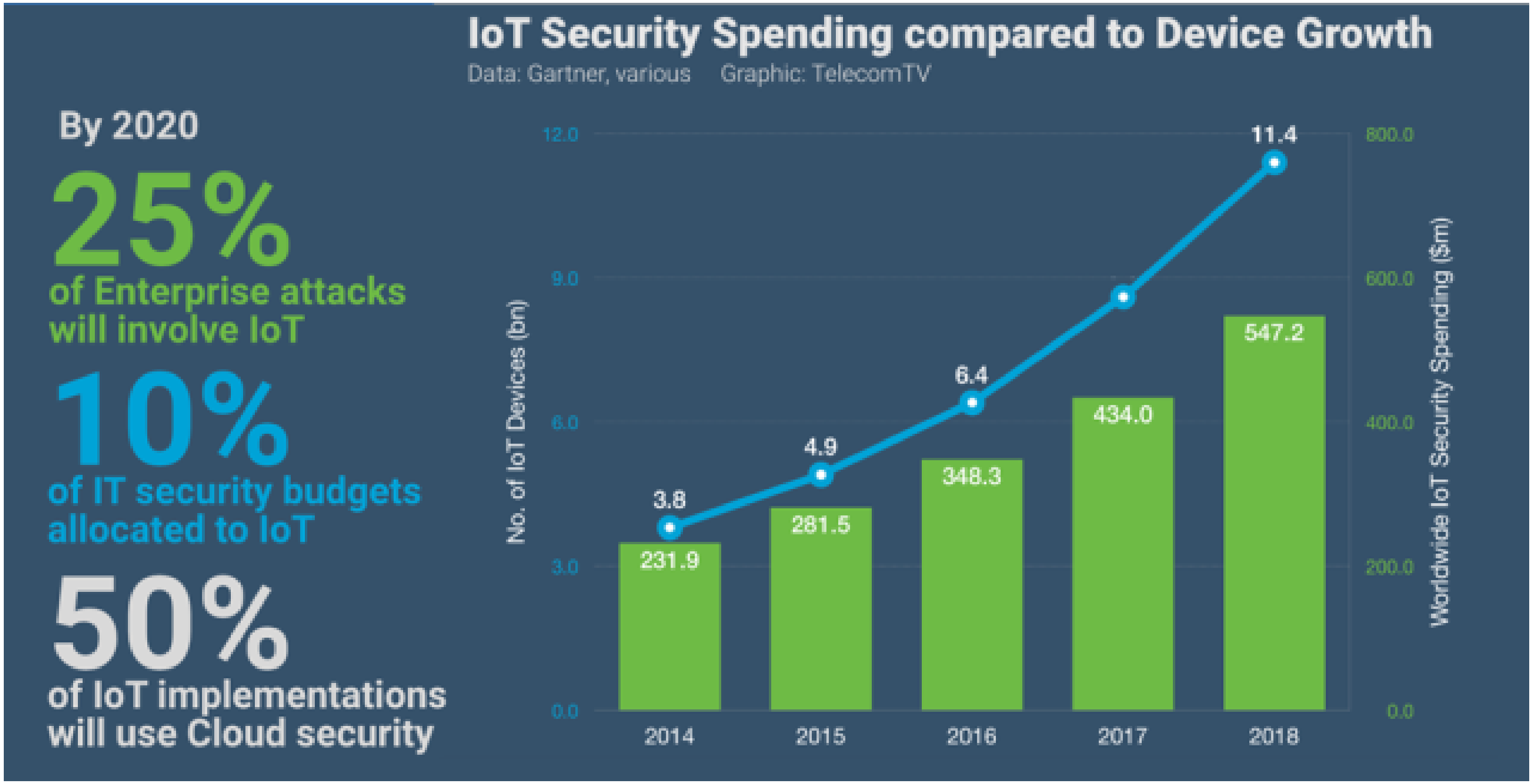
clusterz.io

IOT – the missing S



clusterz.io

General background on cyber attracts



By 2020

25%
of Enterprise attacks will involve IoT

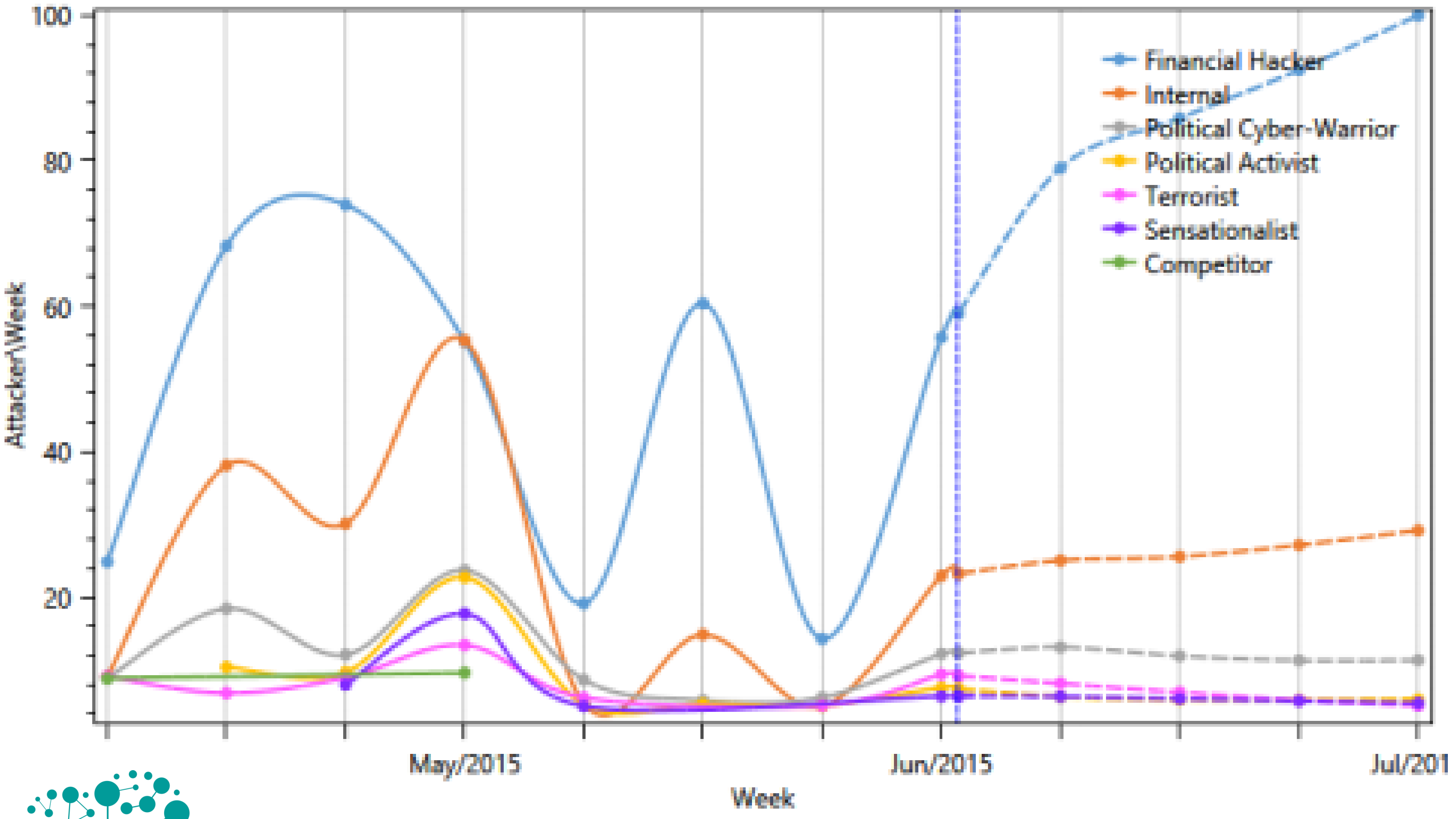
10%
of IT security budgets allocated to IoT

50%
of IoT implementations will use Cloud security

IoT Security Spending compared to Device Growth

Data: Gartner, various Graphic: TelecomTV

Who is behind cyber crime ?

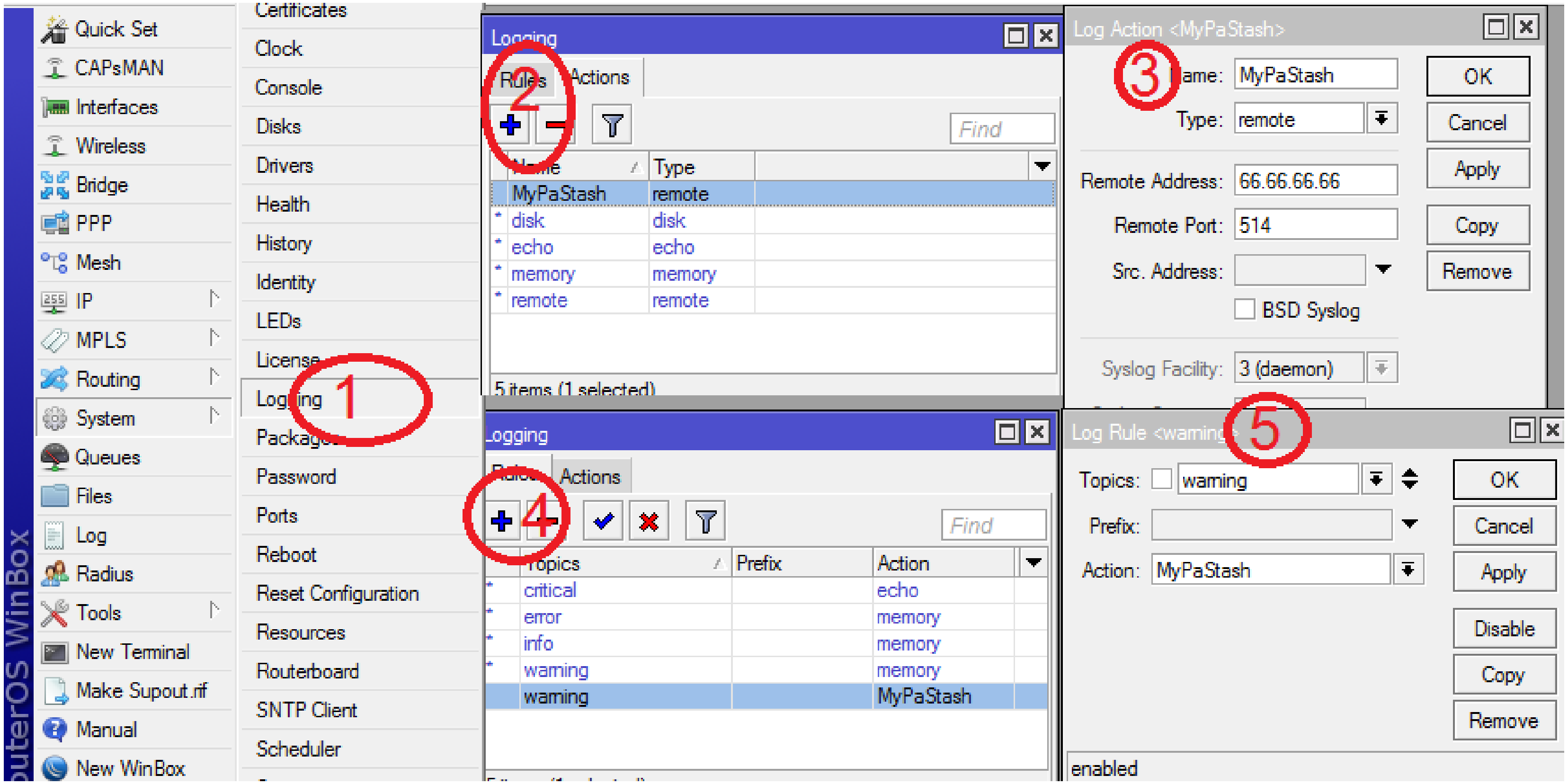


clusterz.io

CALVIN DIDN'T REALISE THAT IN JUST 3 SECONDS HE'D HAVE A 2ND CHANCE TO MAKE A 1ST IMPRESSION...

Big Data

How to ship your data(Syslog) .....



Name	Type
MyPaStash	remote
disk	disk
echo	echo
memory	memory
remote	remote

5 items (1 selected)

Name: MyPaStash

Type: remote

Remote Address: 66.66.66.66

Remote Port: 514

Src. Address:

□ BSD Syslog

Syslog Facility: 3 (daemon)

Topics	Prefix	Action
critical		echo
error		memory
info		memory
warning		memory
warning		MyPaStash

Topics: □ warning

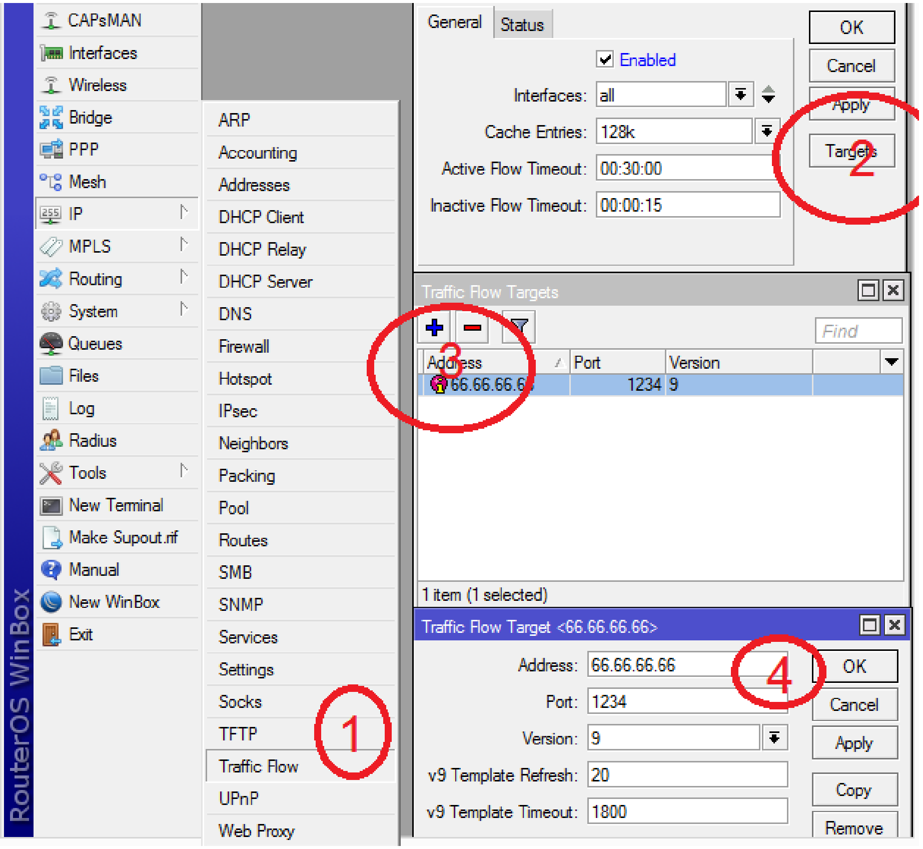
Prefix:

Action: MyPaStash

enabled

clusterz.io

How to ship your data (NetFlow)



☑ Enabled

Interfaces: all

Cache Entries: 128k

Active Flow Timeout: 00:30:00

Inactive Flow Timeout: 00:00:15

Address	Port	Version
66.66.66.6	1234	9

1 item (1 selected)

Traffic Flow Target <66.66.66.66>

Address: 66.66.66.66

Port: 1234

Version: 9

v9 Template Refresh: 20

v9 Template Timeout: 1800

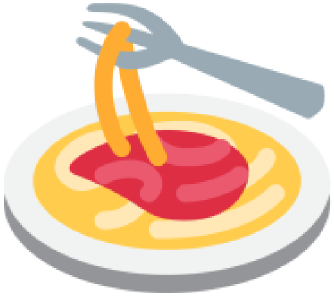
```
/ip traffic-flow
set cache-entries=4M enabled=yes
                interfaces=BRIDGE

/ip traffic-flow target
 add dst-address=66.66.66.66
                port=1234     version=5
```

clusterz.io

Shipping Big Data Log

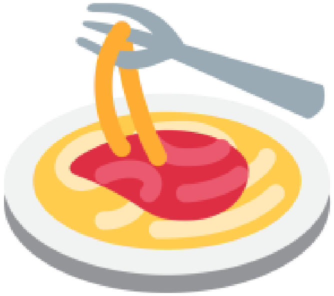
- **paStash** is a tool to manage spaghetti I/O with input, processors and output.
- modules for all seasons and protocols.



https://**github.com/sipcapture/paStash**

clusterz.io

PaStash Config



```
input {
  udp {
    host => 0.0.0.0
    port => 514
    type => syslog
  }
}

filter {
  regex {
    regex => /^(\S)/+/
    fields => [toto]
  }
}


output {
  elasticsearch {
    host => localhost
    port => 9200
  }
}
```

Input plugins

- File
- Syslog
- ZeroMQ
- Redis
- HTTP
- Websocket
- TCP / TLS
- Google app engine
- AMQP
- SQS
- NetFlow
- Freeswitch ESL
- Asterisk AMI

Filter plugins

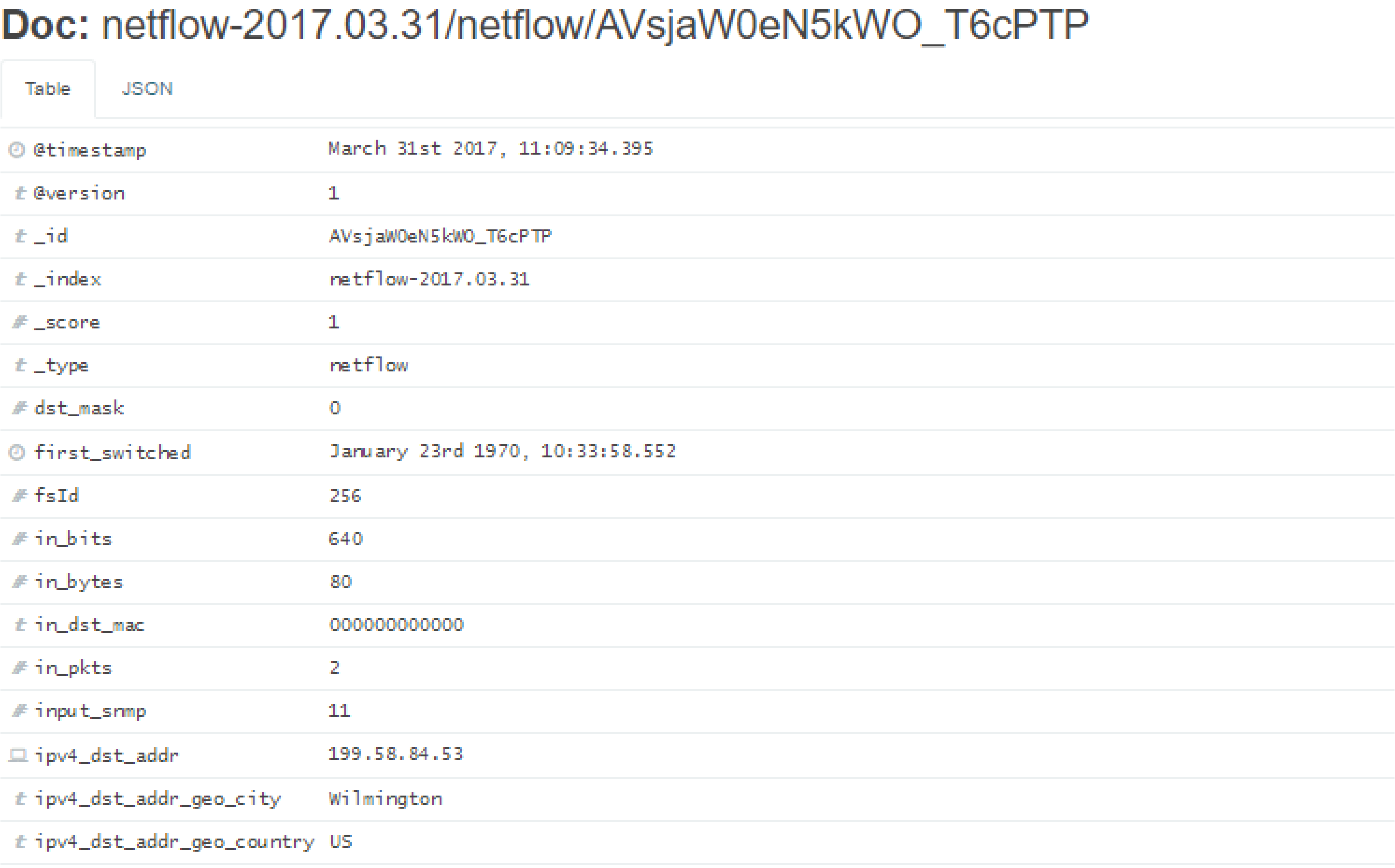
- Regex
- Grok
- Mutate Replace
- Grep
- Reverse DNS
- Compute field
- Compute hash
- Compute date field
- Split
- Rename
- Multiline
- Json fields
- Geoip
- Eval
- Bunyan
- HTTP Status Classifier

Outputs

- ZeroMQ
- ElasticSearch
- Statsd
- Gelf
- File
- HTTP Post
- Websocket
- Redis
- Logio
- TCP / TLS
- AMQP
- SQS
- HEP

clusterz.io

Parsing Mikrotik Netflow



Doc: netflow-2017.03.31/netflow/AVsjaW0eN5kWO_T6cPTP

@timestamp	March 31st 2017, 11:09:34.395
@version	1
_id	AVsjaW0eN5kWO_T6cPTP
_index	netflow-2017.03.31
_score	1
_type	netflow
dst_mask	0
first_switched	January 23rd 1970, 10:33:58.552
fsId	256
in_bits	640
in_bytes	80
in_dst_mac	000000000000
in_pkts	2
input_snmp	11
ipv4_dst_addr	199.58.84.53
ipv4_dst_addr_geo_city	Wilmington
ipv4_dst_addr_geo_country	US

Parsing Mikrotik Log

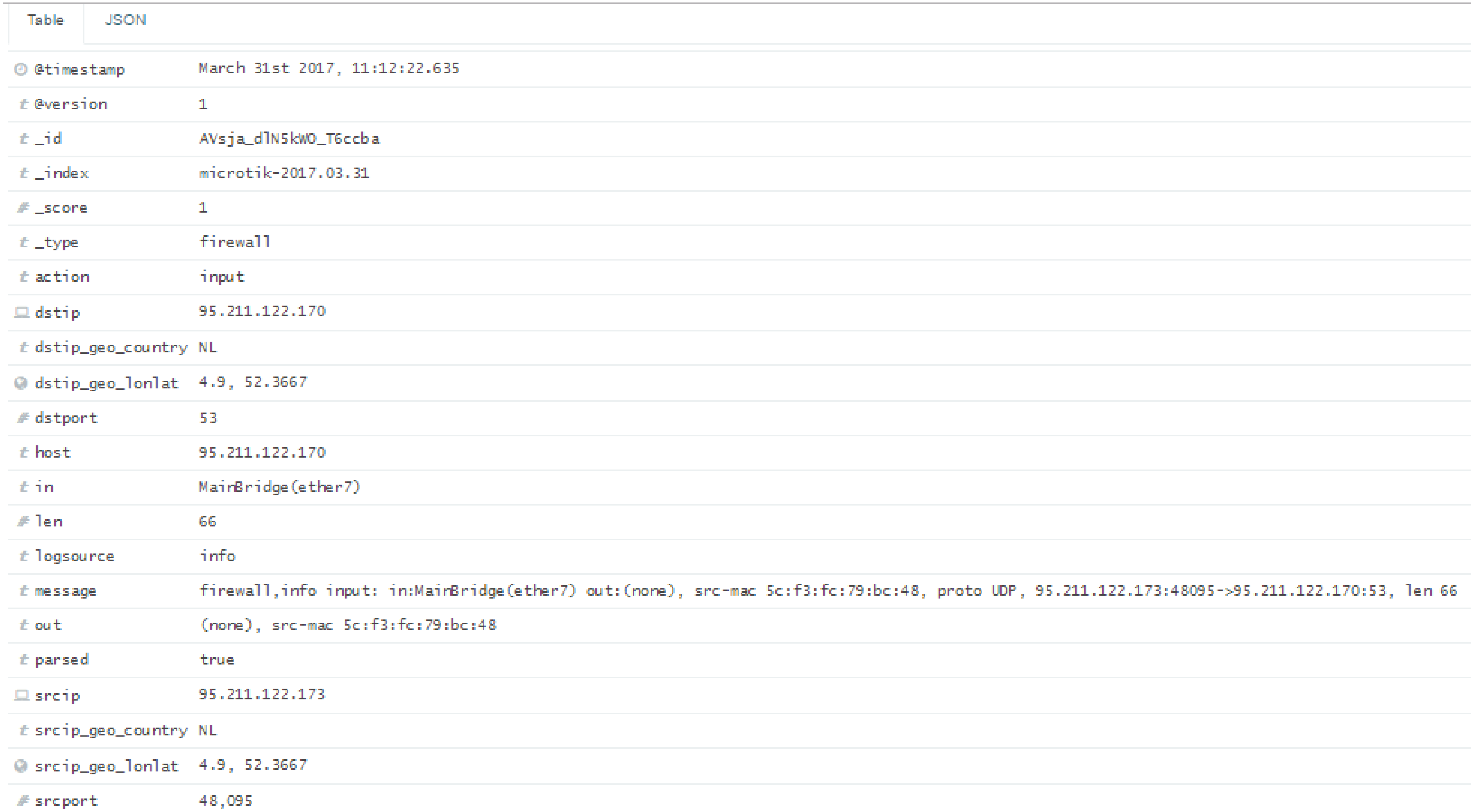
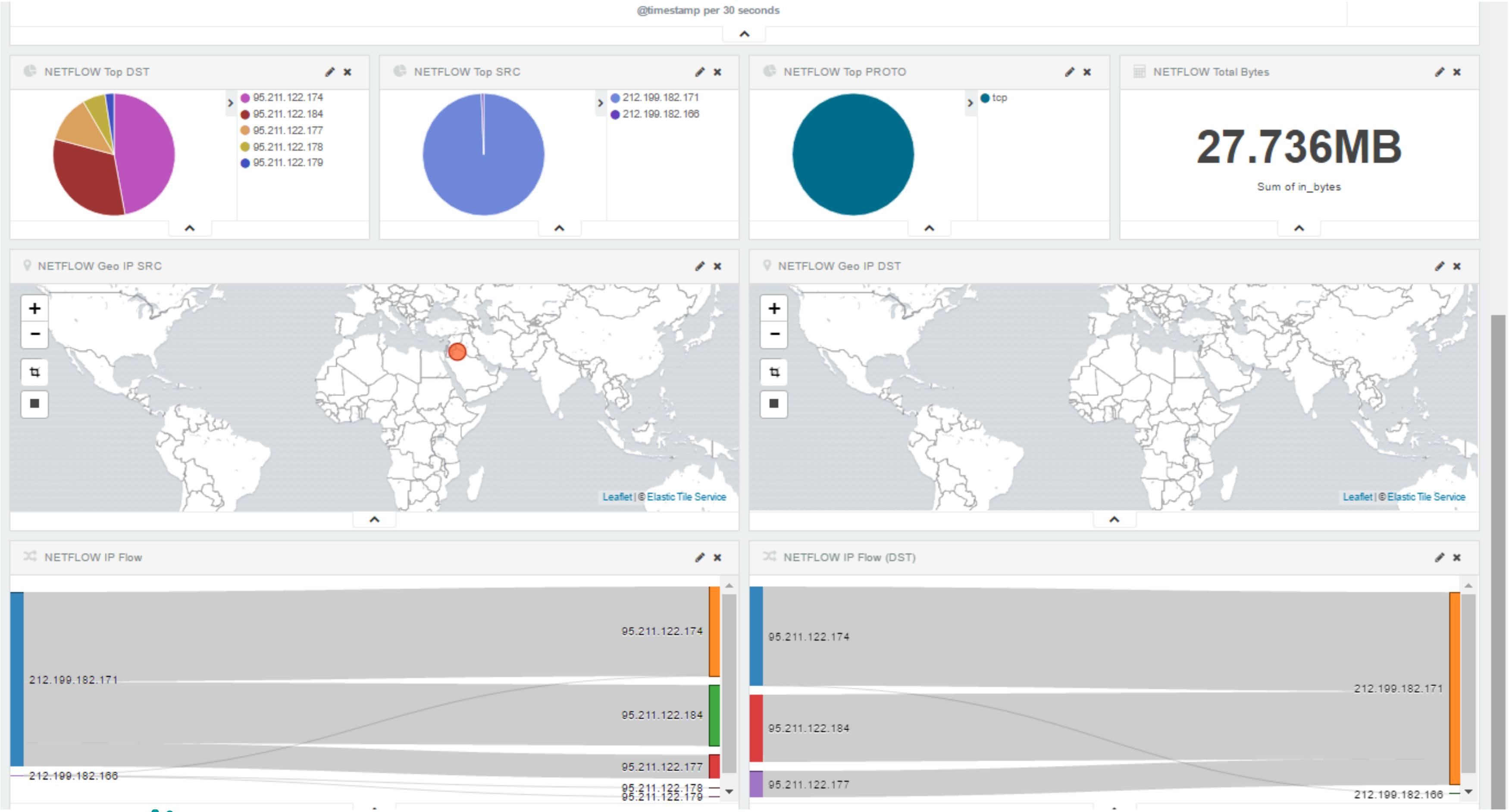


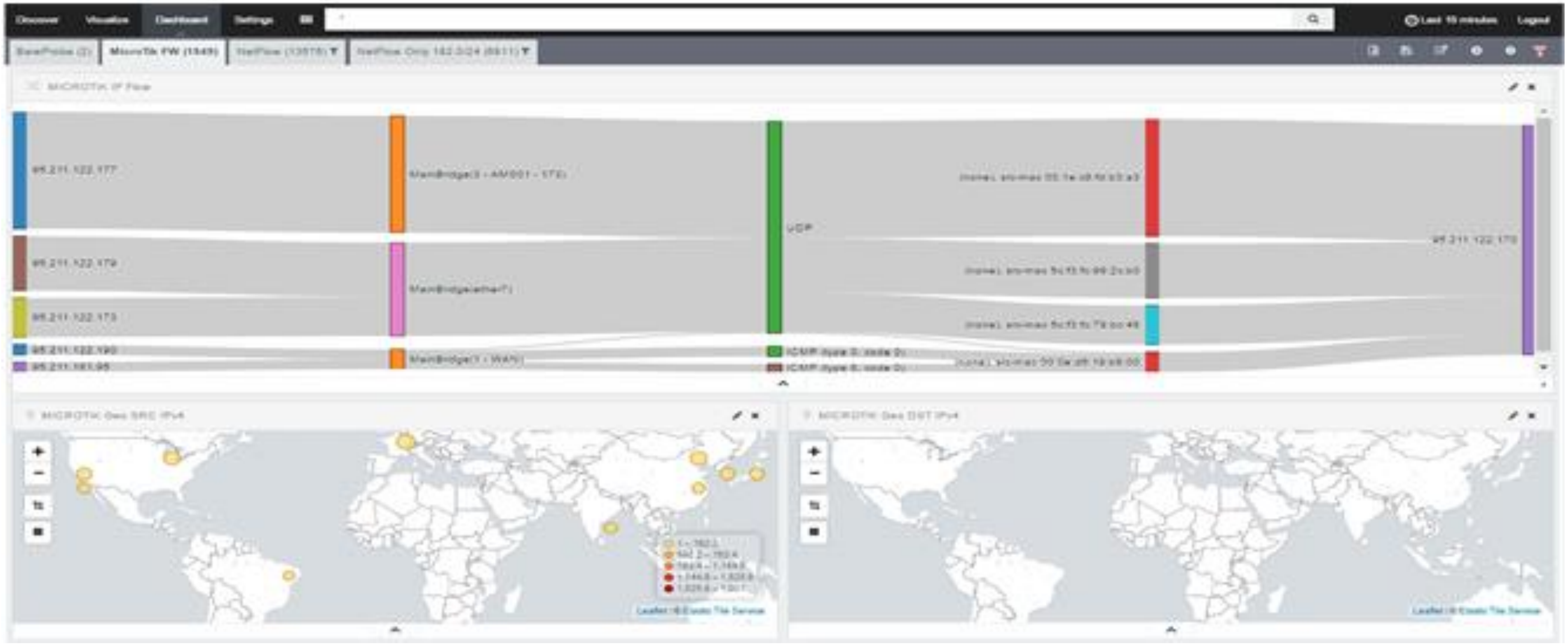
Table JSON

@timestamp	March 31st 2017, 11:12:22.635
@version	1
_id	AVsja_dlN5kWO_T6ccba
_index	microtik-2017.03.31
_score	1
_type	firewall
action	input
dstip	95.211.122.170
dstip_geo_country	NL
dstip_geo_lonlat	4.9, 52.3667
dstport	53
host	95.211.122.170
in	MainBridge(ether7)
len	66
logsource	info
message	firewall,info input: in:MainBridge(ether7) out:(none), src-mac 5c:f3:fc:79:bc:48, proto UDP, 95.211.122.173:48095->95.211.122.170:53, len 66
out	(none), src-mac 5c:f3:fc:79:bc:48
parsed	true
srcip	95.211.122.173
srcip_geo_country	NL
srcip_geo_lonlat	4.9, 52.3667
srcport	48,095

Mikrotik Netflow Dashboards



Mikrotik Logs Dashboards



Elasticsearch

Elasticsearch is a search engine based on Lucene. It provides a distributed, multitenant-capable full-text search engine with an HTTP web interface and schema-free JSON documents.

clusterz.io

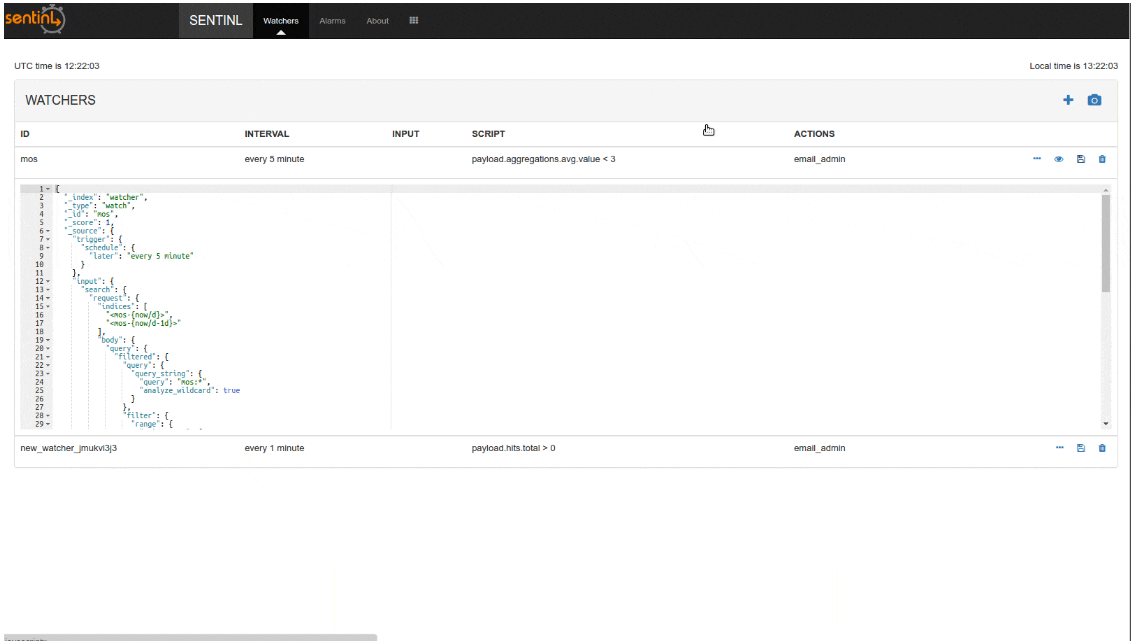
Siren alerting & reporting application

SENTINL extends Siren with Alerting and Reporting functionality to monitor, validate and inform users and administrators on data series changes using standard queries or join queries, programmable validators, transformers and messages to send out using a variety of configurable actions including sending action to the Mikrotik API as well as sending Emails, Slack Messages, API Webhooks, PDF Snapshots of Charts, creating new Documents and much more.

Siren Alerting & Reporting App

Siren

Enterprise provides many unique features and enables integrators to realize unique Business Intelligence creatures. With such power, automating workflows and being able to get notified with data detections quickly becomes a key requirement.



UTC time is 12:22:03

Local time is 13:22:03

WATCHERS

ID	INTERVAL	INPUT	SCRIPT	ACTIONS
mos	every 5 minute		payload.aggregations.avg.value < 3	email_admin
new_watcher_jmukvi3j3	every 1 minute		payload.hits.total > 0	email_admin

```
{
  "_index": "watcher",
  "_type": "watch",
  "_id": "mos",
  "_score": 1,
  "_source": {
    "trigger": {
      "schedule": {
        "later": "every 5 minute"
      }
    },
    "input": {
      "search": {
        "request": {
          "indices": [
            "<mos-{now/d}>",
            "<mos-{now/d-1d}>"
          ],
          "body": {
            "query": {
              "filtered": {
                "query": {
                  "query_string": {
                    "query": "mos:*",
                    "analyze_wildcard": true
                  }
                },
                "filter": {
                  "range": {
```

THANK YOU!