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)*

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

clusterz.io

QXIP - Voice Capture Engineering & Development

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

clusterz.io

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.

clusterz.io

CHR Licensing License

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

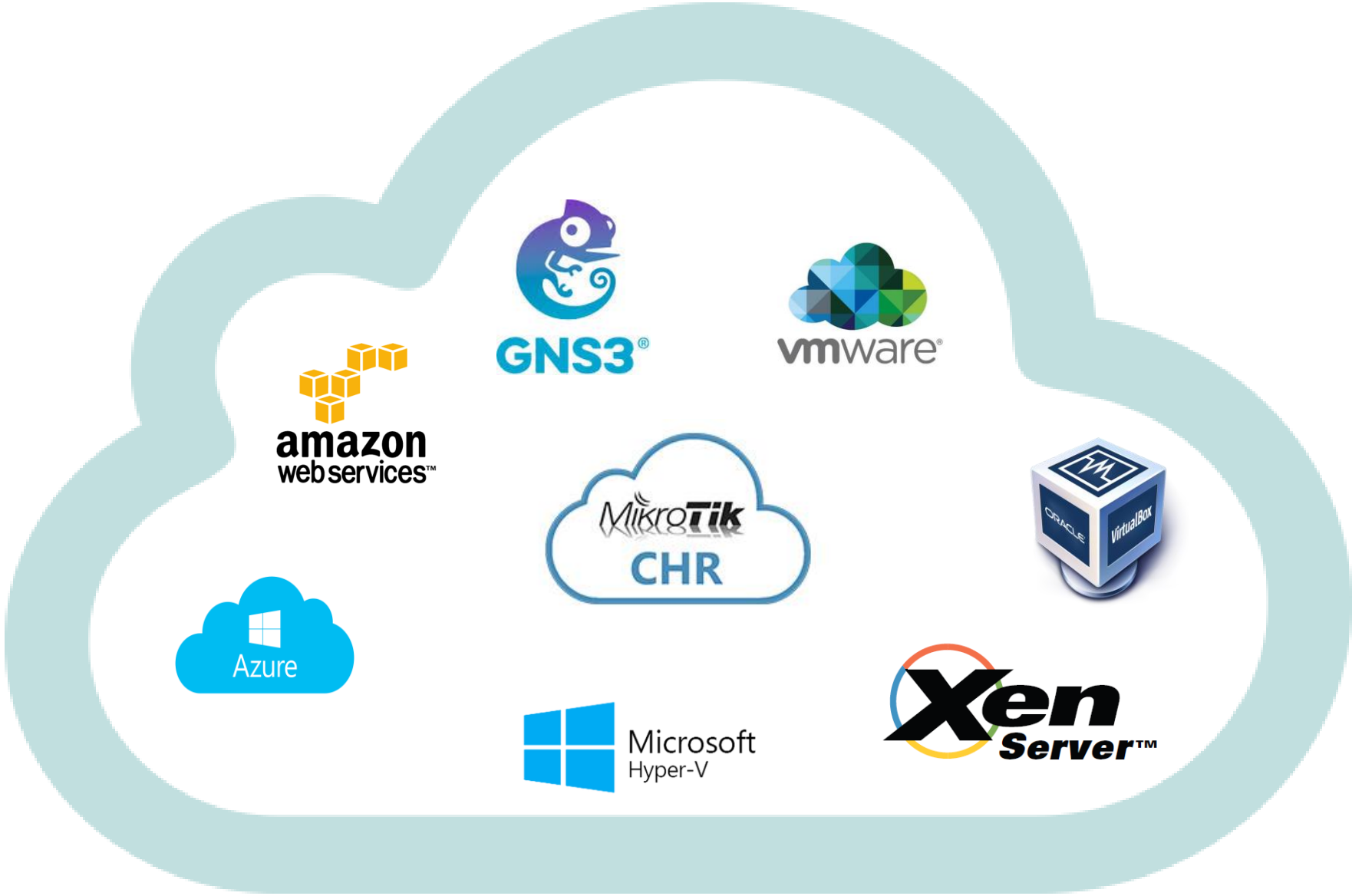
It is possible to transfer a perpetual license to another CHR instance.

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

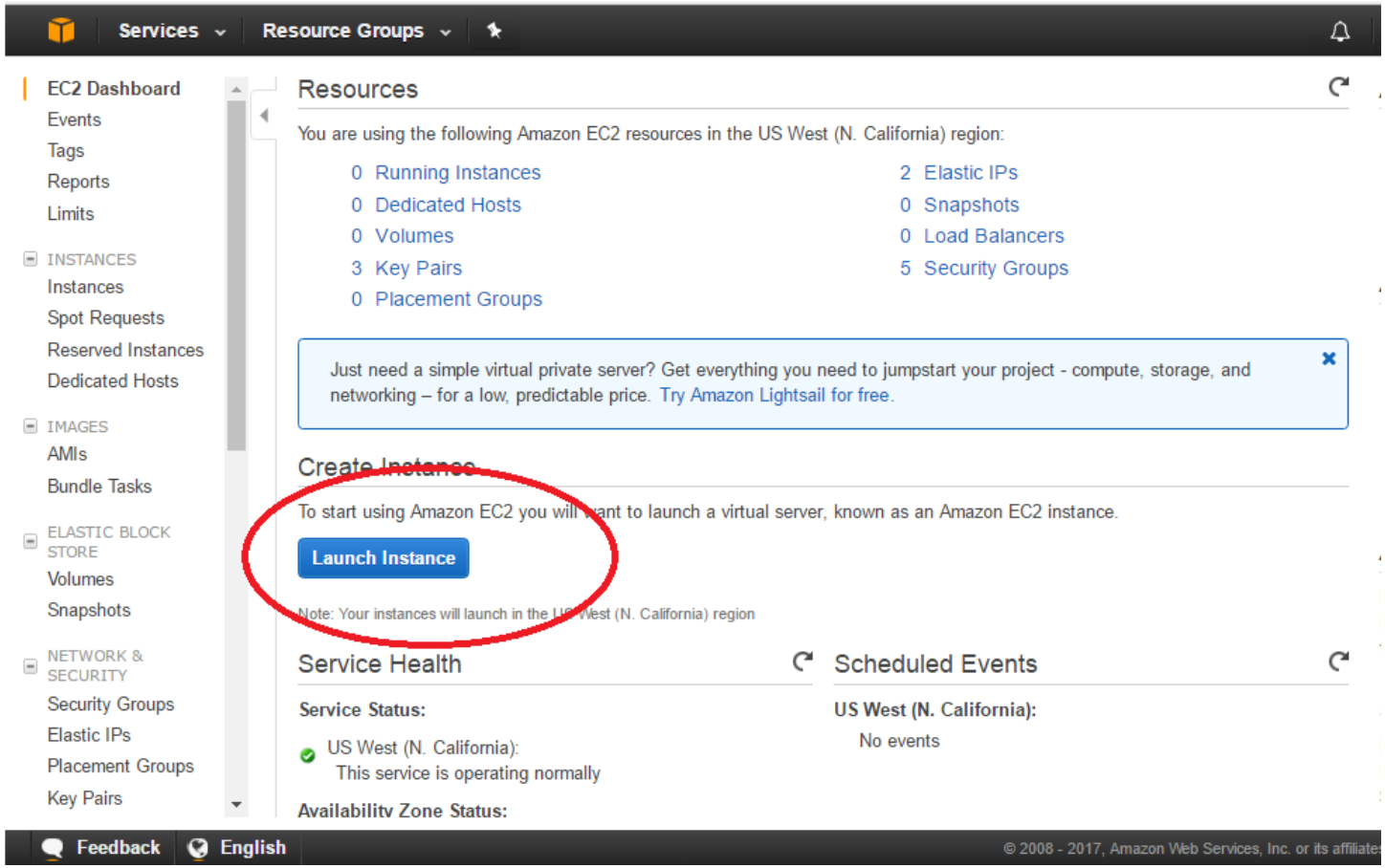
If the CHR instance will not be able to access the account server to renew the license ,
it will behave as if the trial period has ran out and will not allow an upgrade of RouterOS to a newer version.

clusterz.io

CHR hosting environment

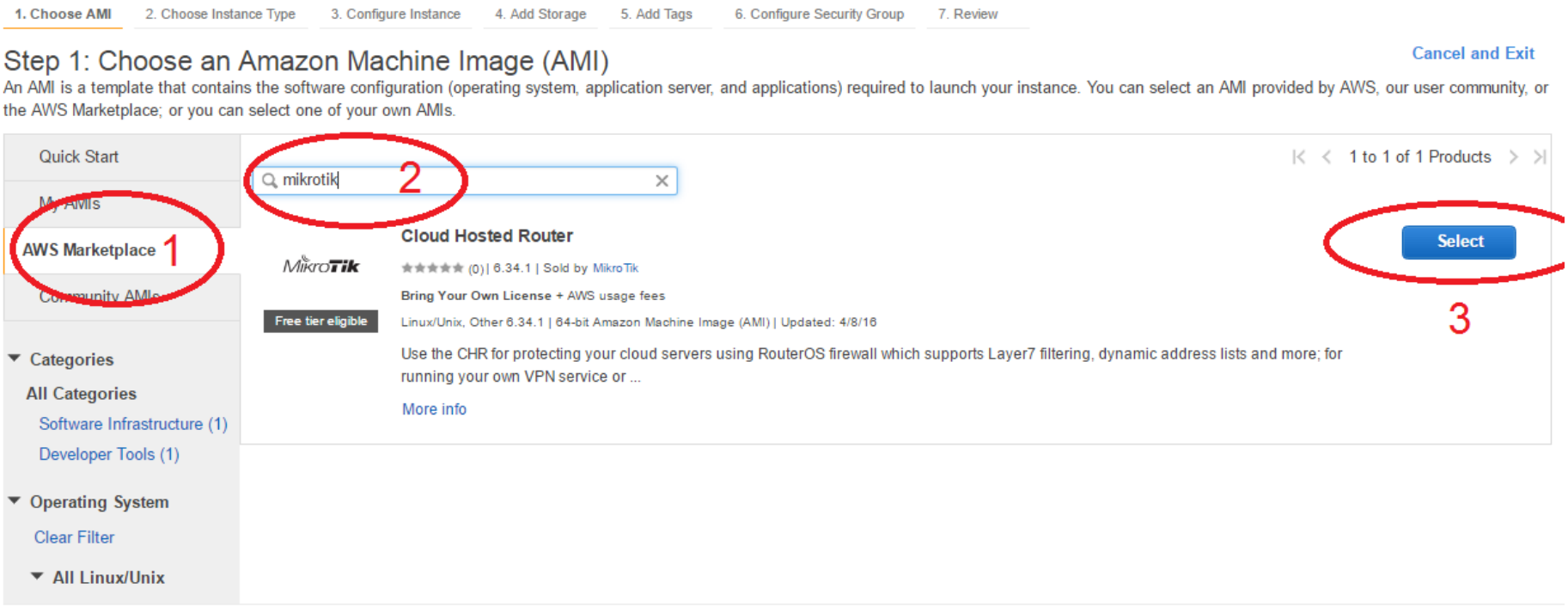


Installing CHR on AWS – Step 1



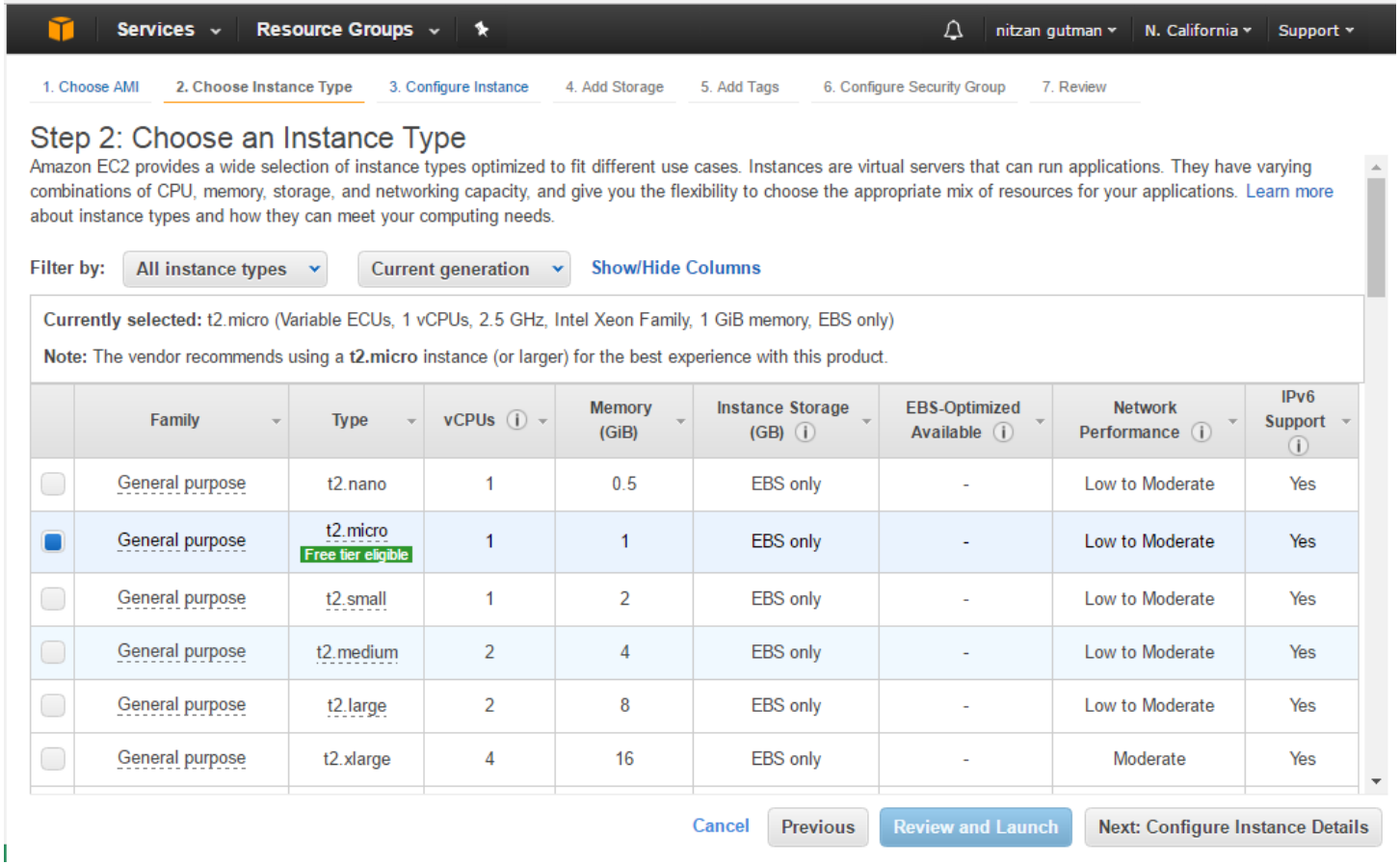
clusterz.io

Select CHR Image (AMI)– Step 2



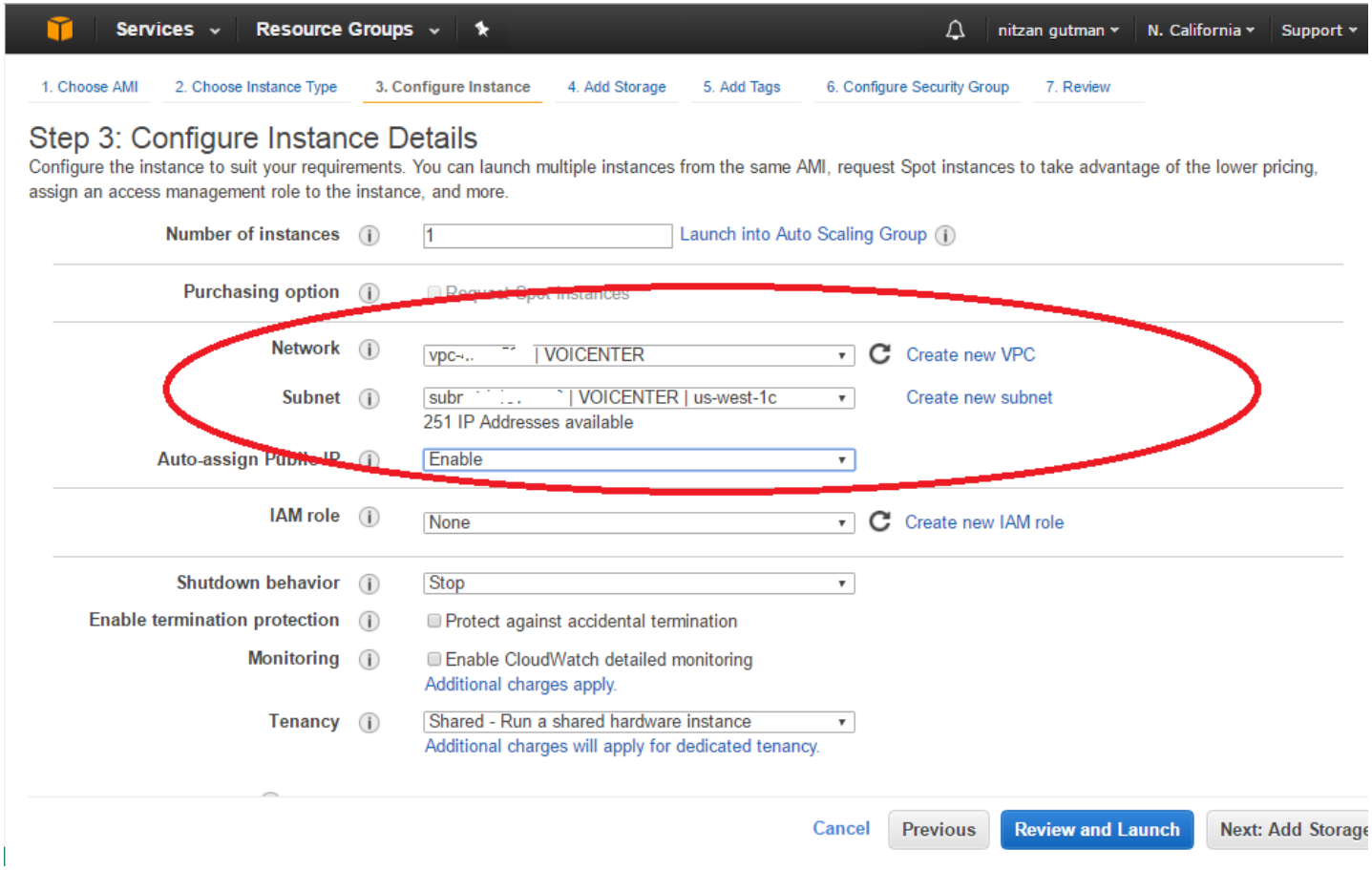
clusterz.io

Select Instance Tab – Step 3



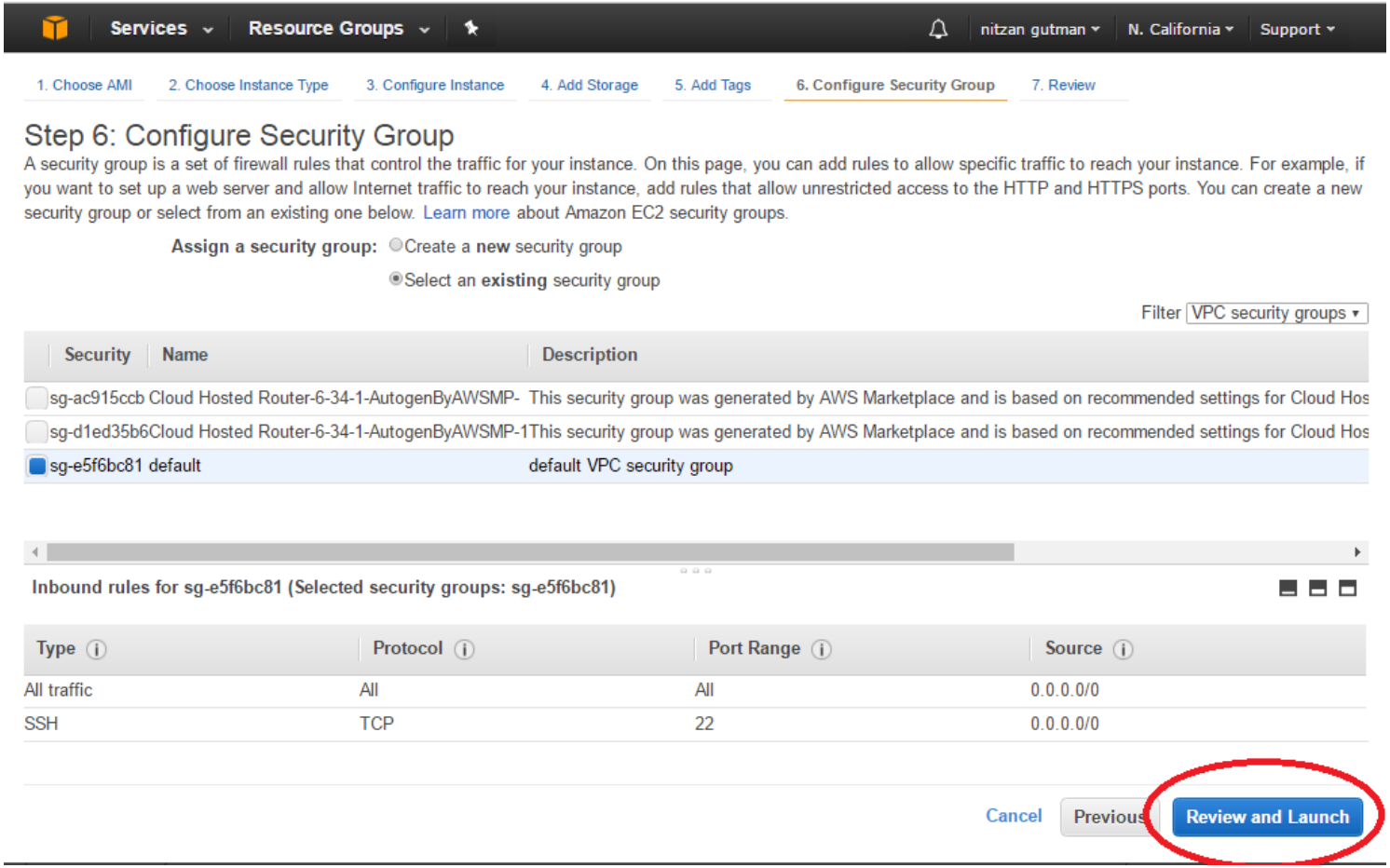
clusterz.io

Setup your network – Step 4



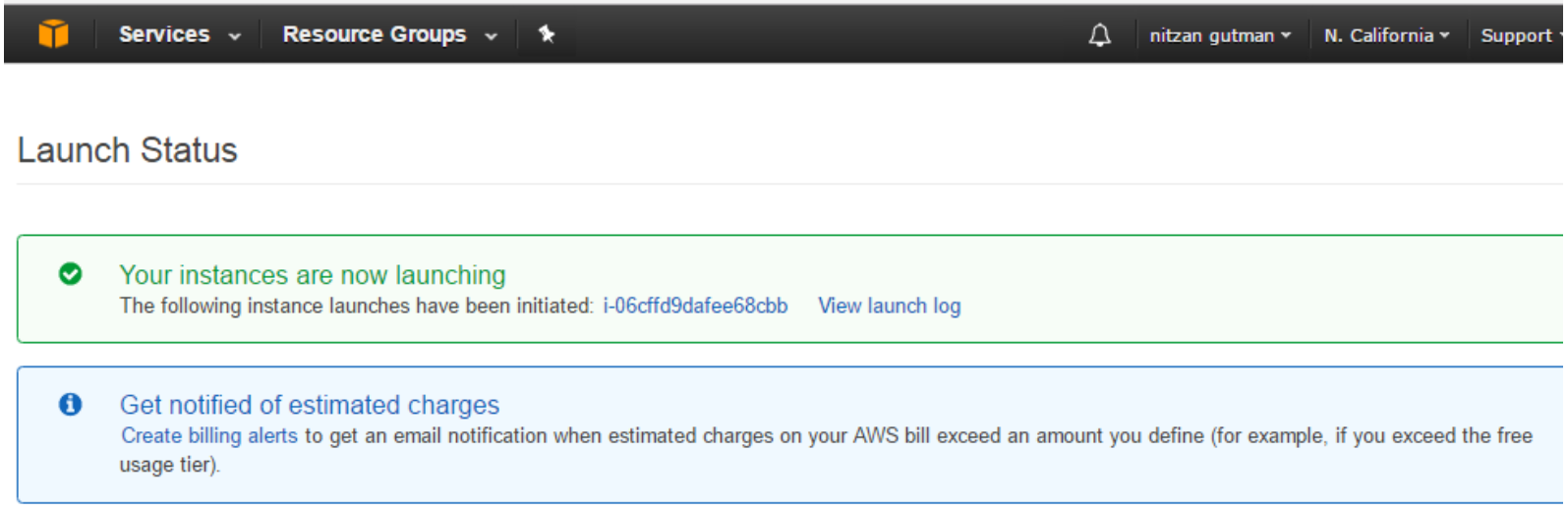
clusterz.io

Configure – Step 5



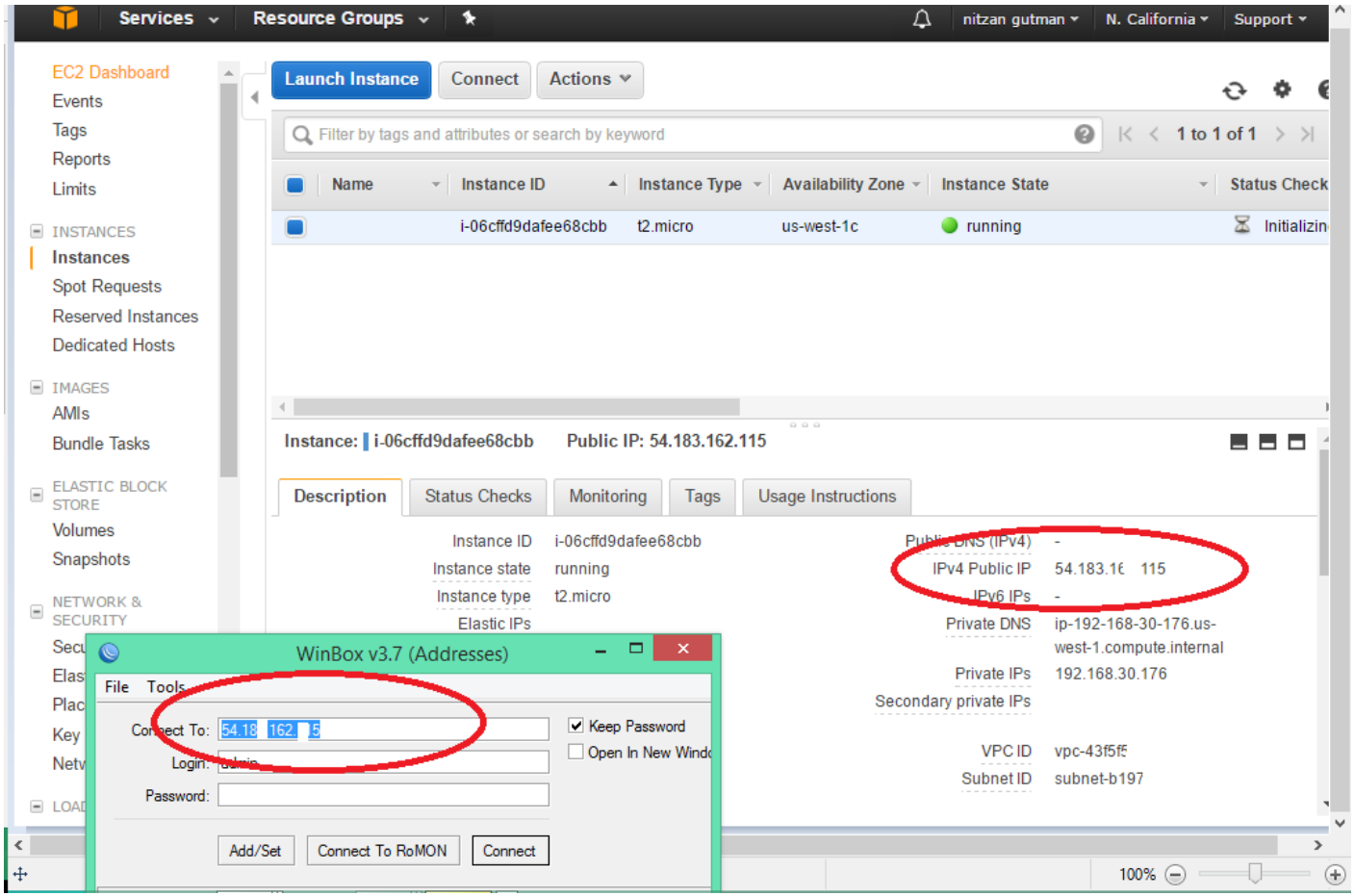
clusterz.io

Installing CHR on AWS – Step 6



clusterz.io

Finally… Winbox … IP… Connect …



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

clusterz.io

CHR - Use case Types

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

clusterz.io

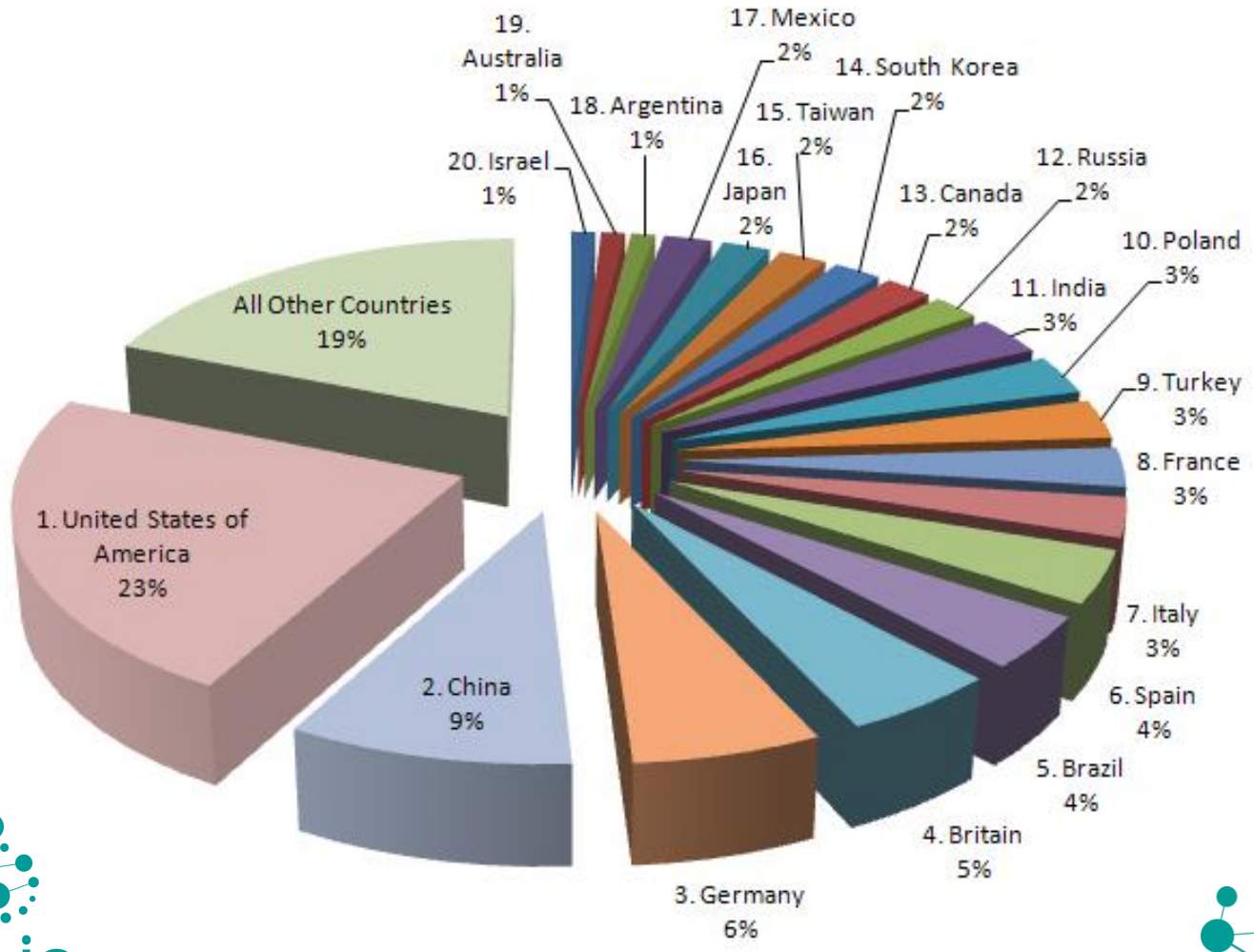
CHR - Use case Types

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

clusterz.io

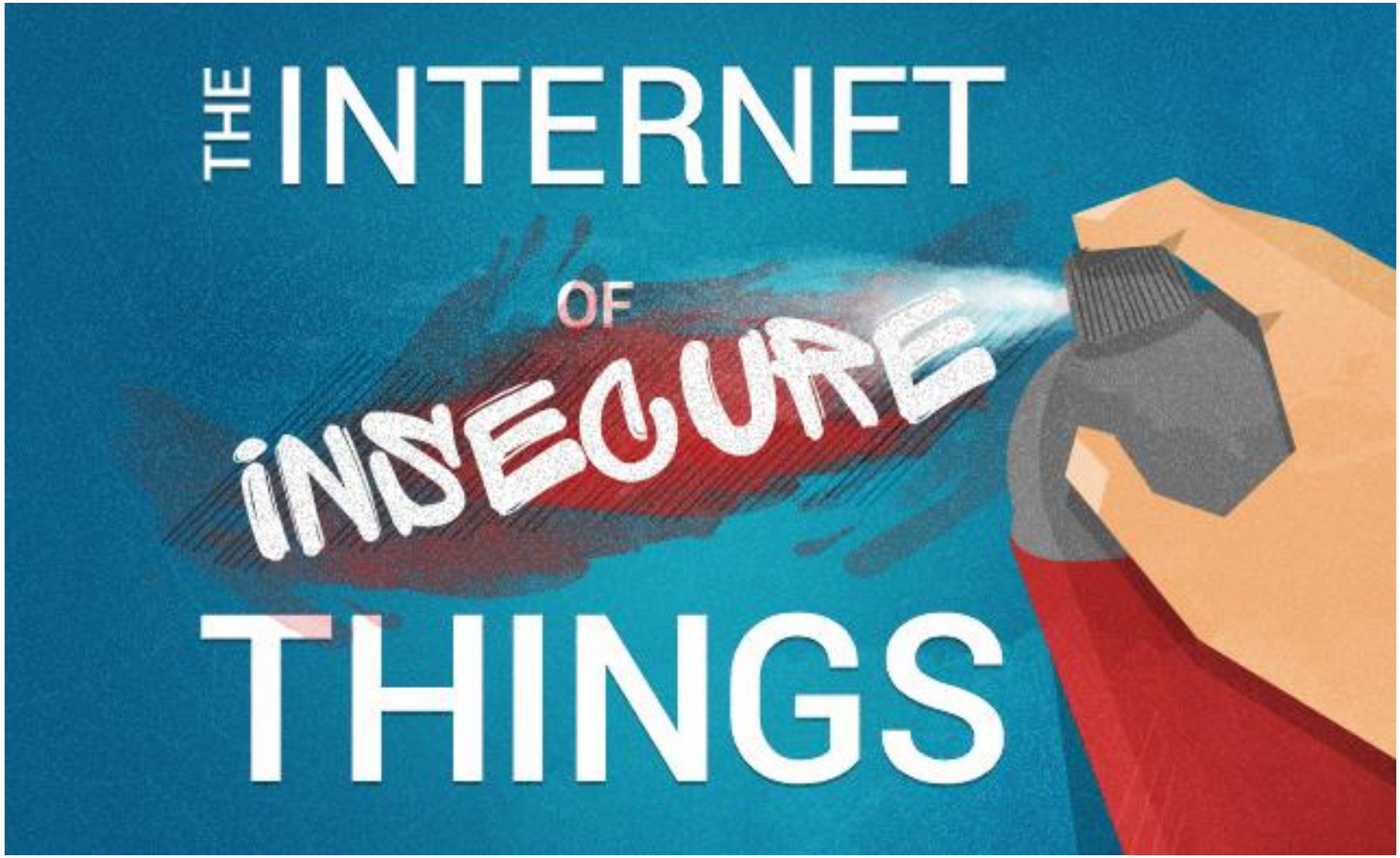

CYBERWAR
END OF
THE
WORLD
(AS WE KNOW IT)

Cyber crime top 20 countries attracts



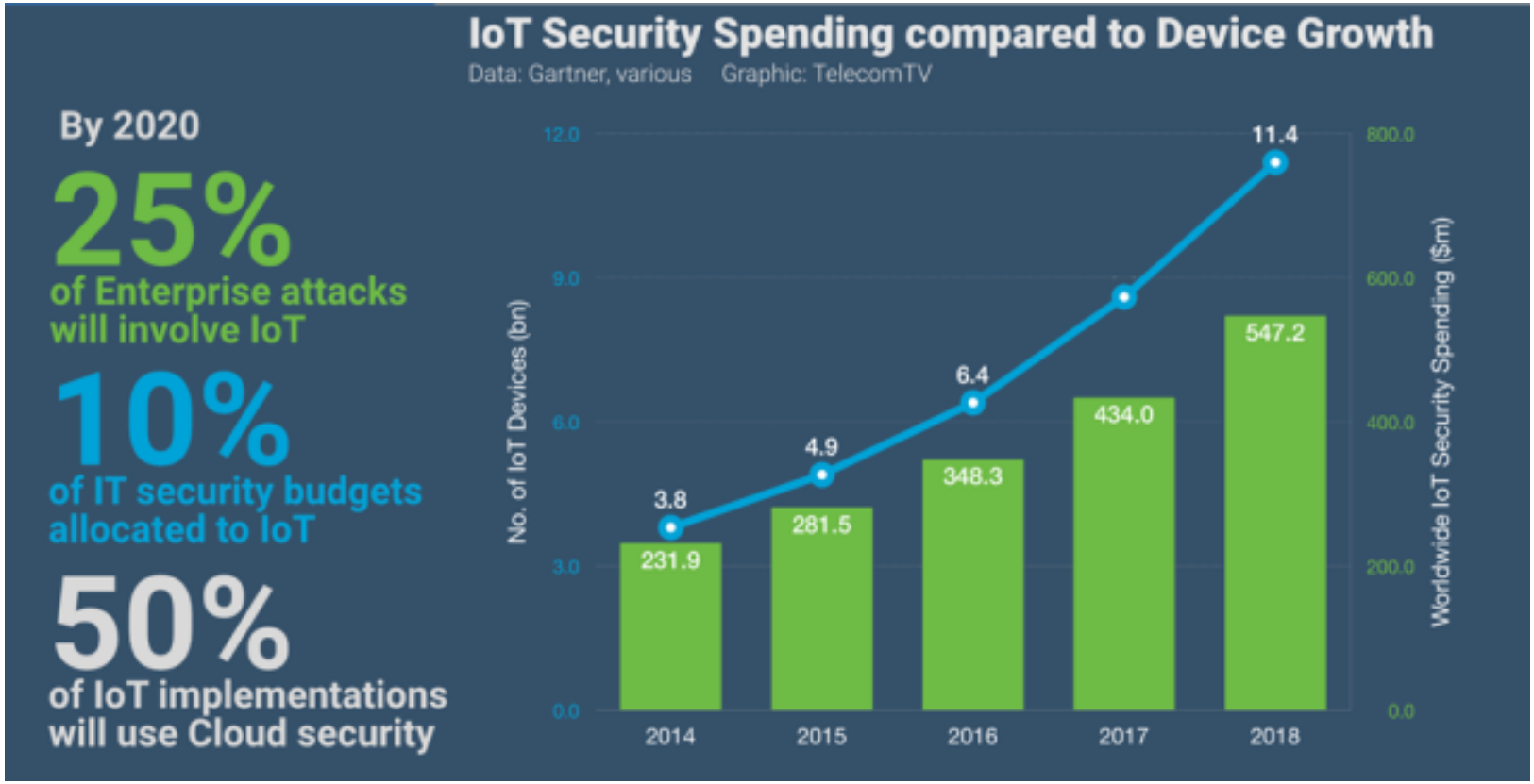
clusterz.io

IOT – the missing S



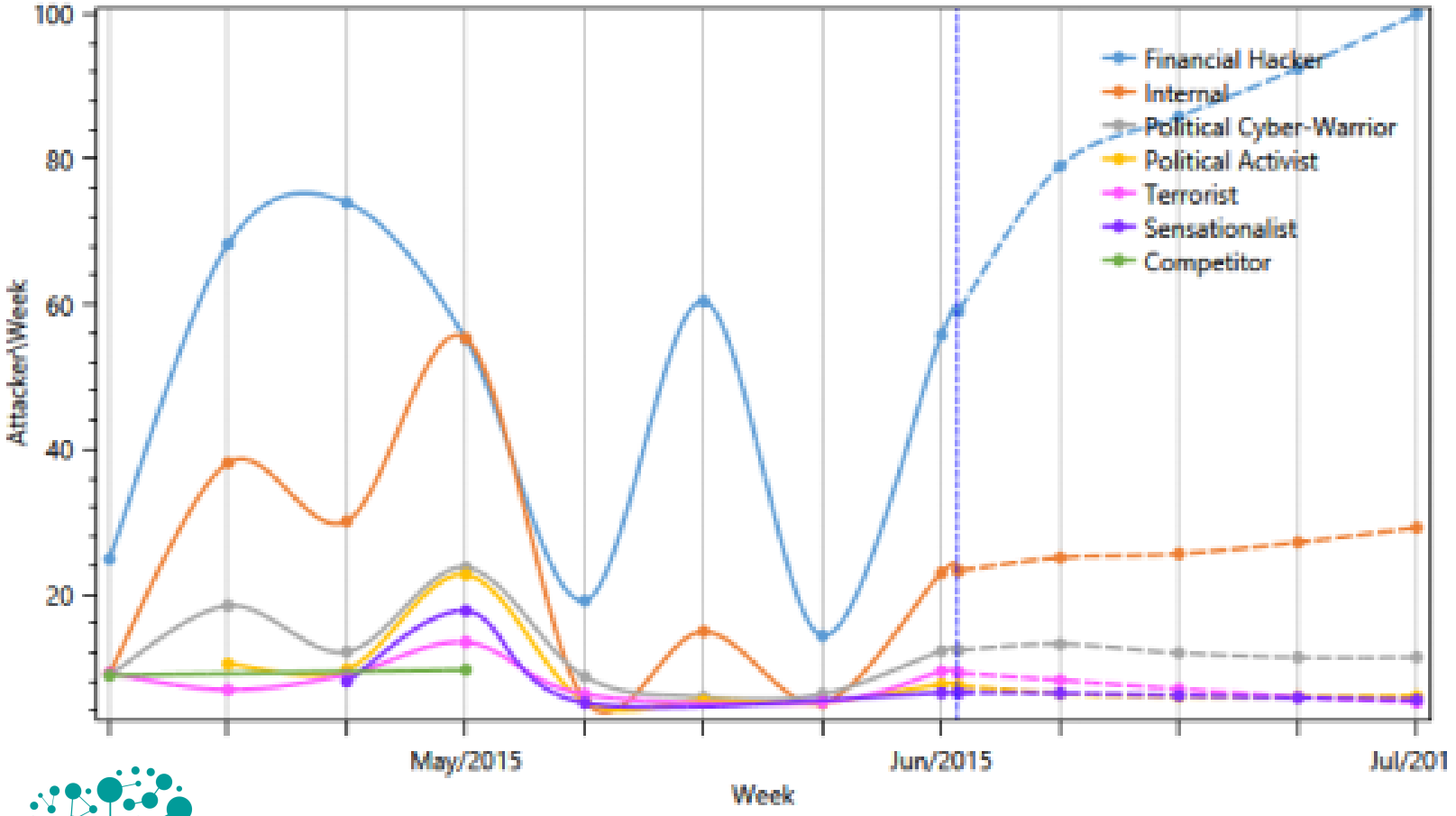
clusterz.io

General background on cyber attracts



clusterz.io

Who is behind cyber crime ?



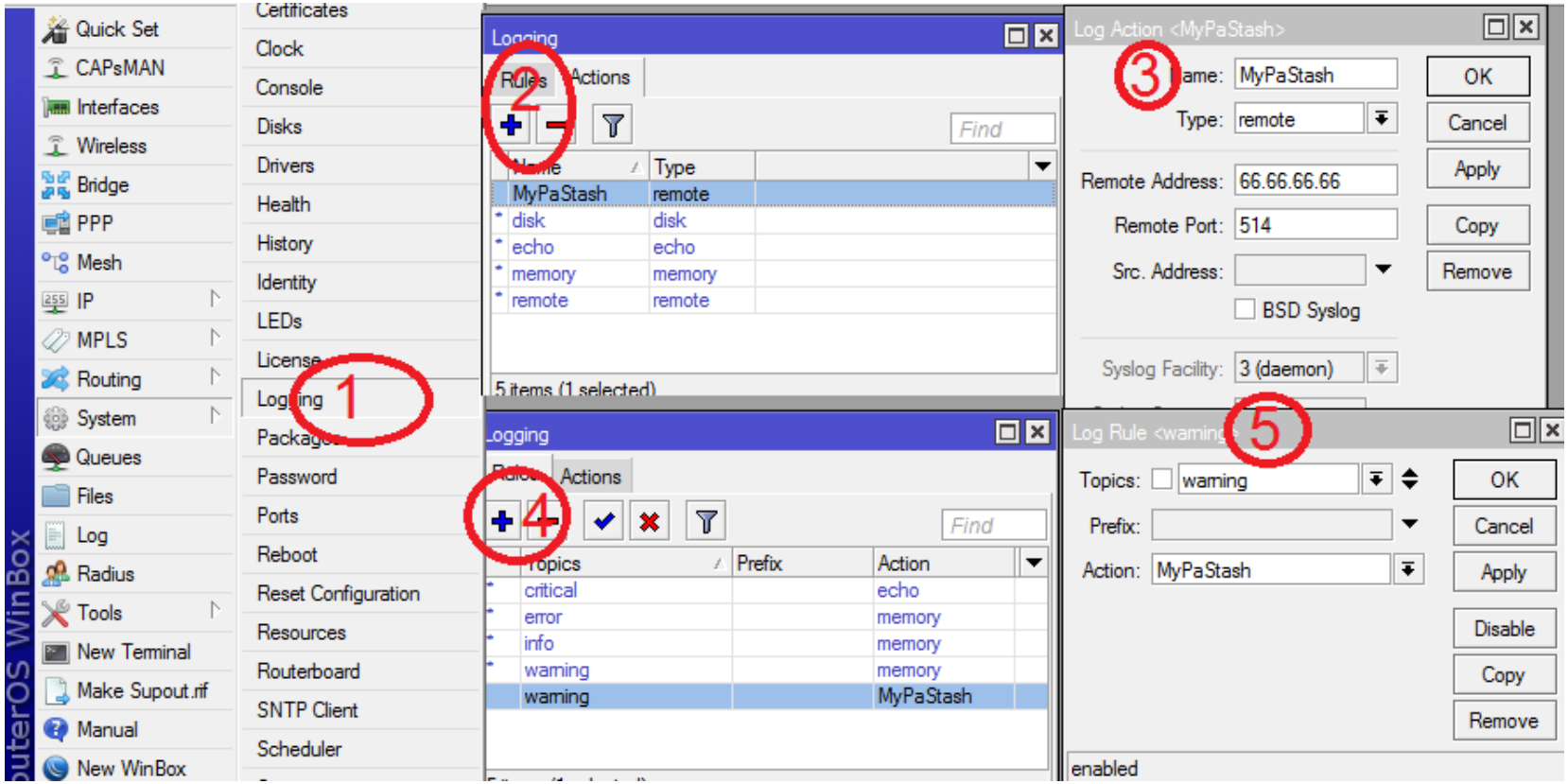
clusterz.io

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

clusterz.io

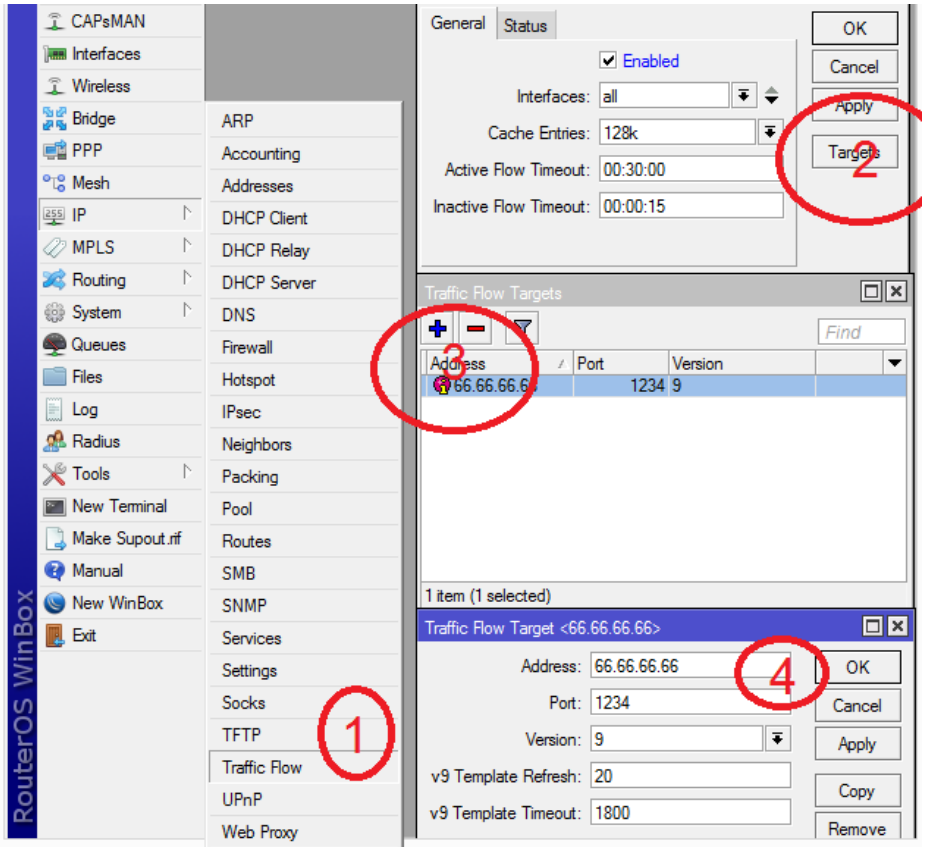
clusterz.io

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



clusterz.io

How to ship your data (NetFlow)




```
/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

Table | JSON

@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

clusterz.io

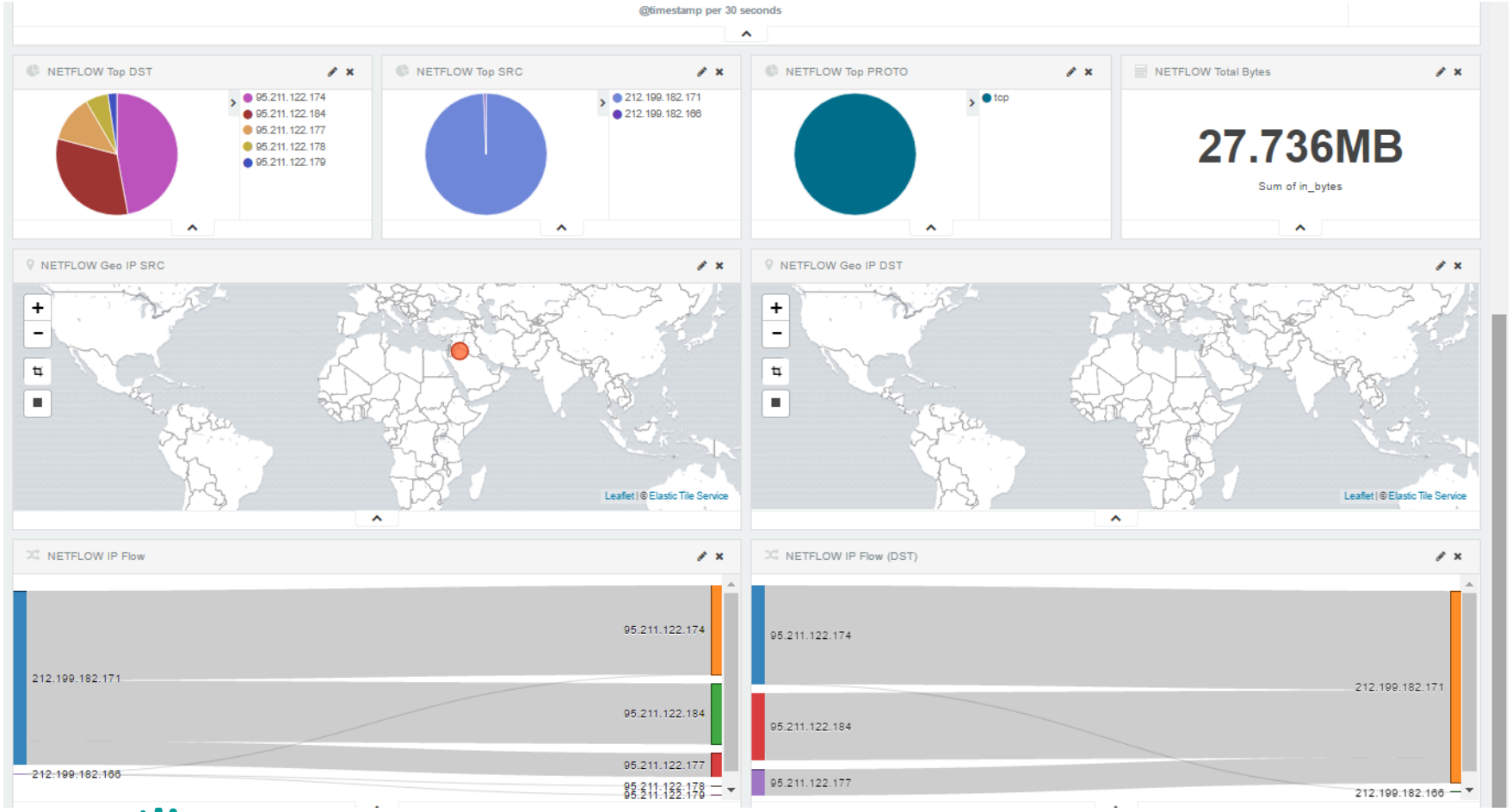
Parsing Mikrotik Log

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

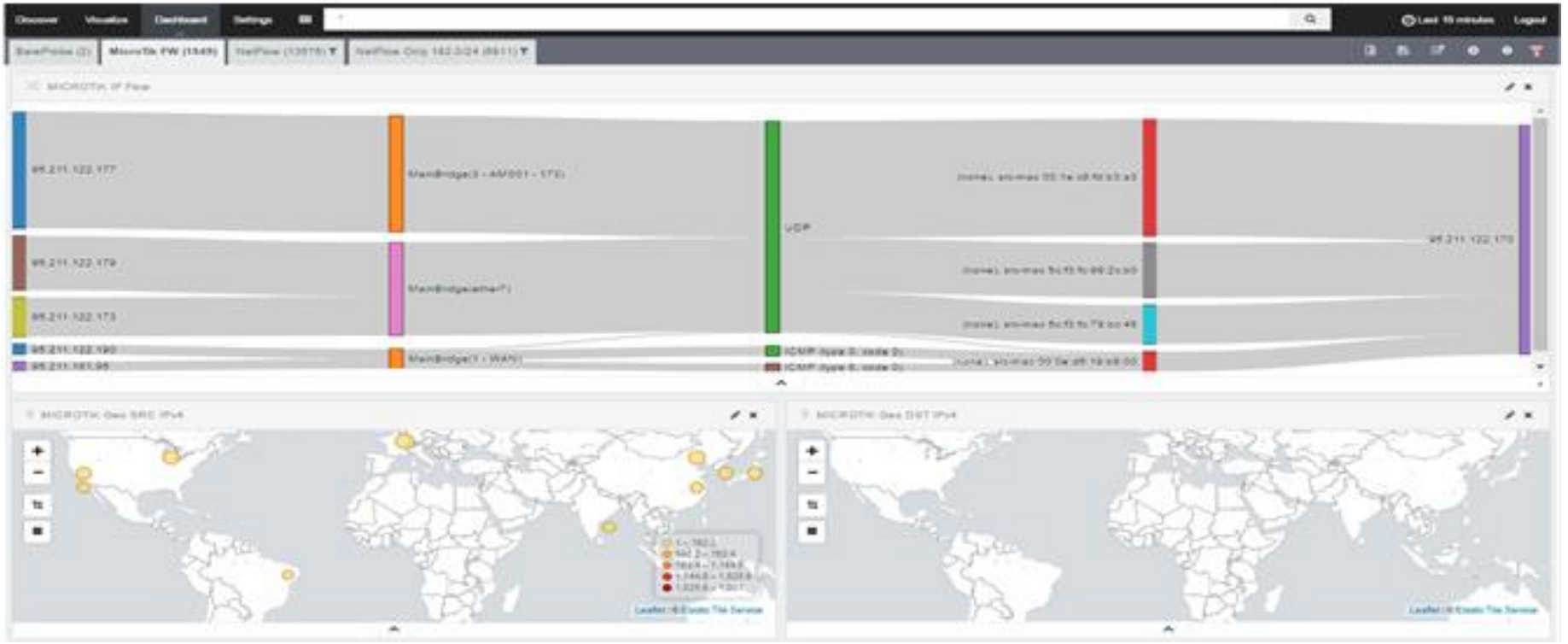
clusterz.io

Mikrotik Netflow Dashboards



clusterz.io

Mikrotik Logs Dashboards



clusterz.io

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

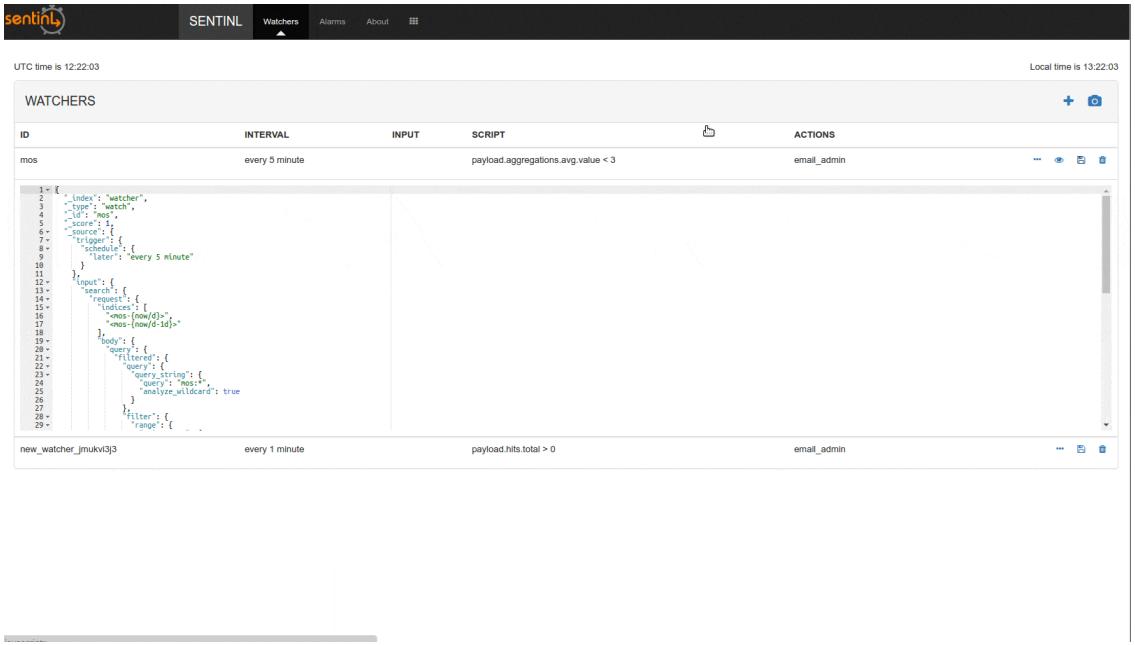
SENTINL extends Siren with Alerting and Reporting functionality to monitor, validate and inform users and administrators on data series changes using standard queries or join queries, programmable validators, transformers and messages to send out using a variety of configurable actions including sending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

clusterz.io

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.



clusterz.io

Pushing your data out of the box

clusterz.io

Contact us today for a month free trial

info@clusterz.io

THANK YOU!