.conf2015

Deploying A Splunk Cluster To The Cloud & Using Splunk To Improve Reliability Of A Fleet Of Mobile Devices

Rob Charlton

Cloud DevOps Architect, Vertu

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

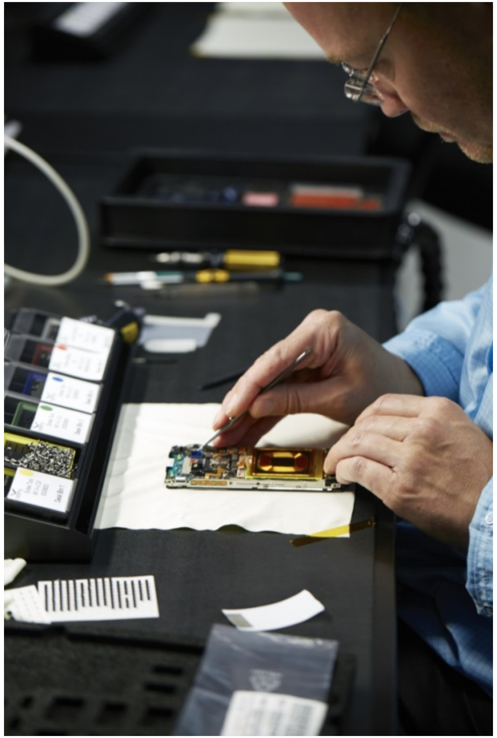
In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

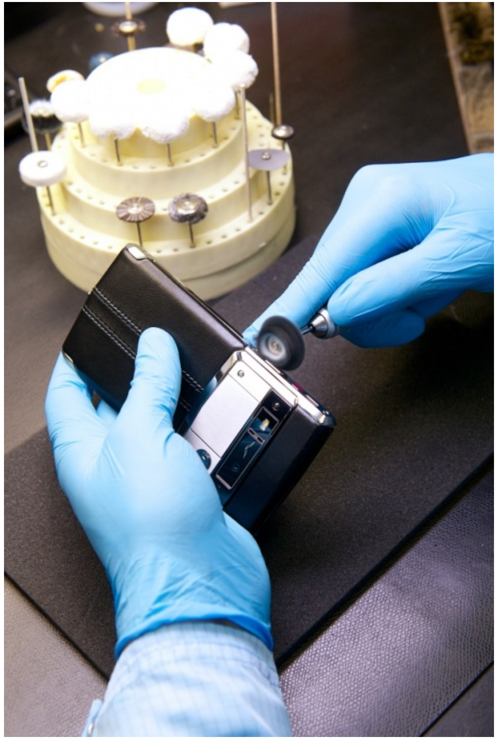
Agenda

- About Vertu
- Vertu's Digital Transformation
- Splunk @ Vertu
- Demo Environment
- Live Demo: Deploying a Splunk cluster using Ansible
- Live Demo: Crashing my phone!

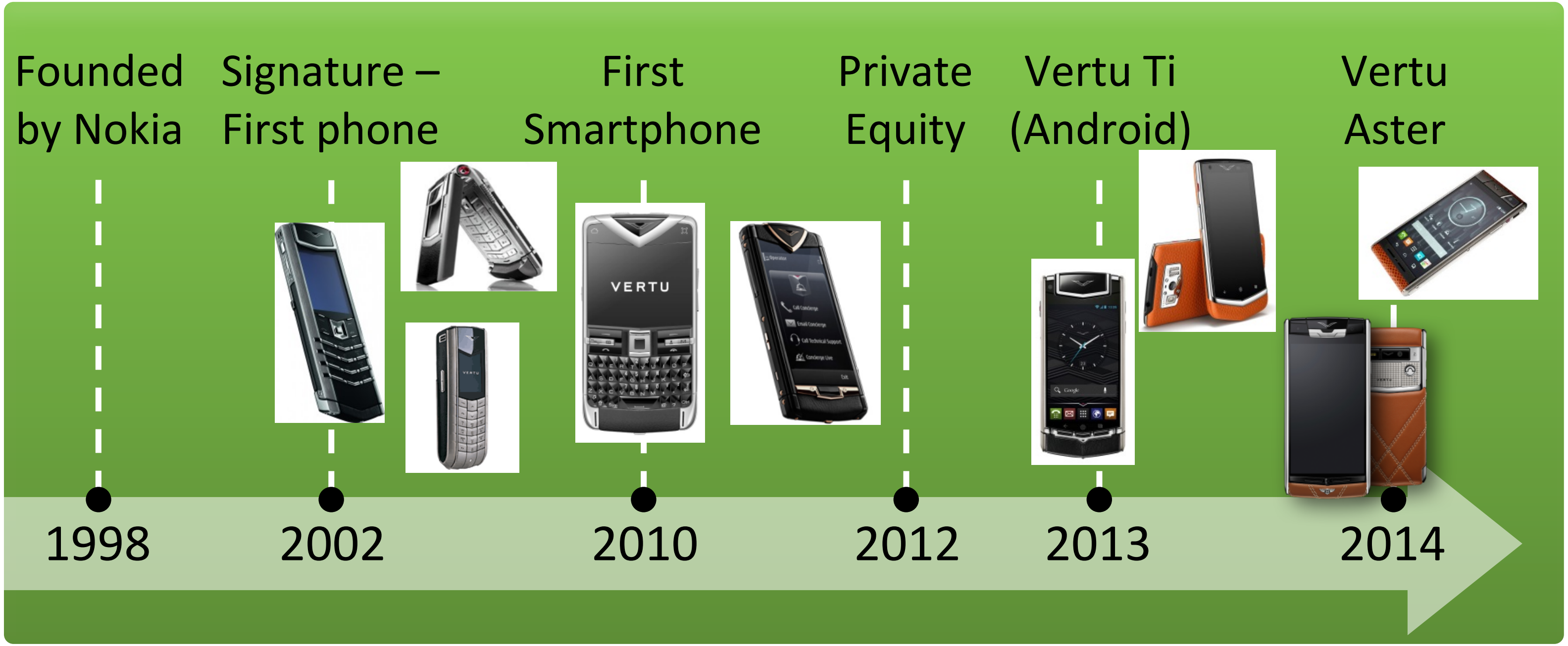
About Vertu Corporation

- British manufacturer and retailer of handmade luxury phones





Vertu Timeline



Founded by Nokia

1998

Signature – First phone

2002

First Smartphone

2010

Private Equity

2012

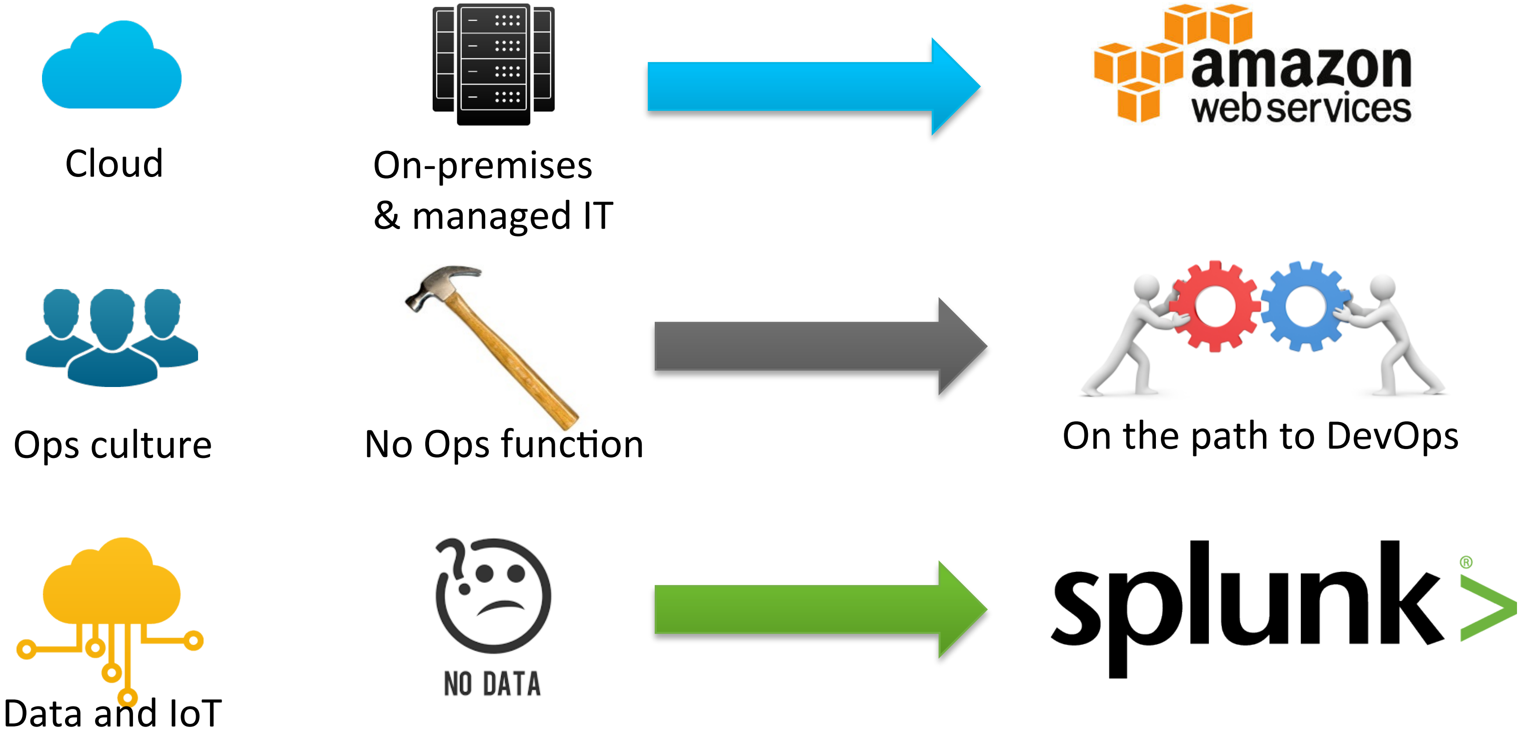
Vertu Ti (Android)

2013

Vertu Aster

2014

Vertu’s Digital Transformation



Cloud

On-premises & managed IT

Ops culture

No Ops function

On the path to DevOps

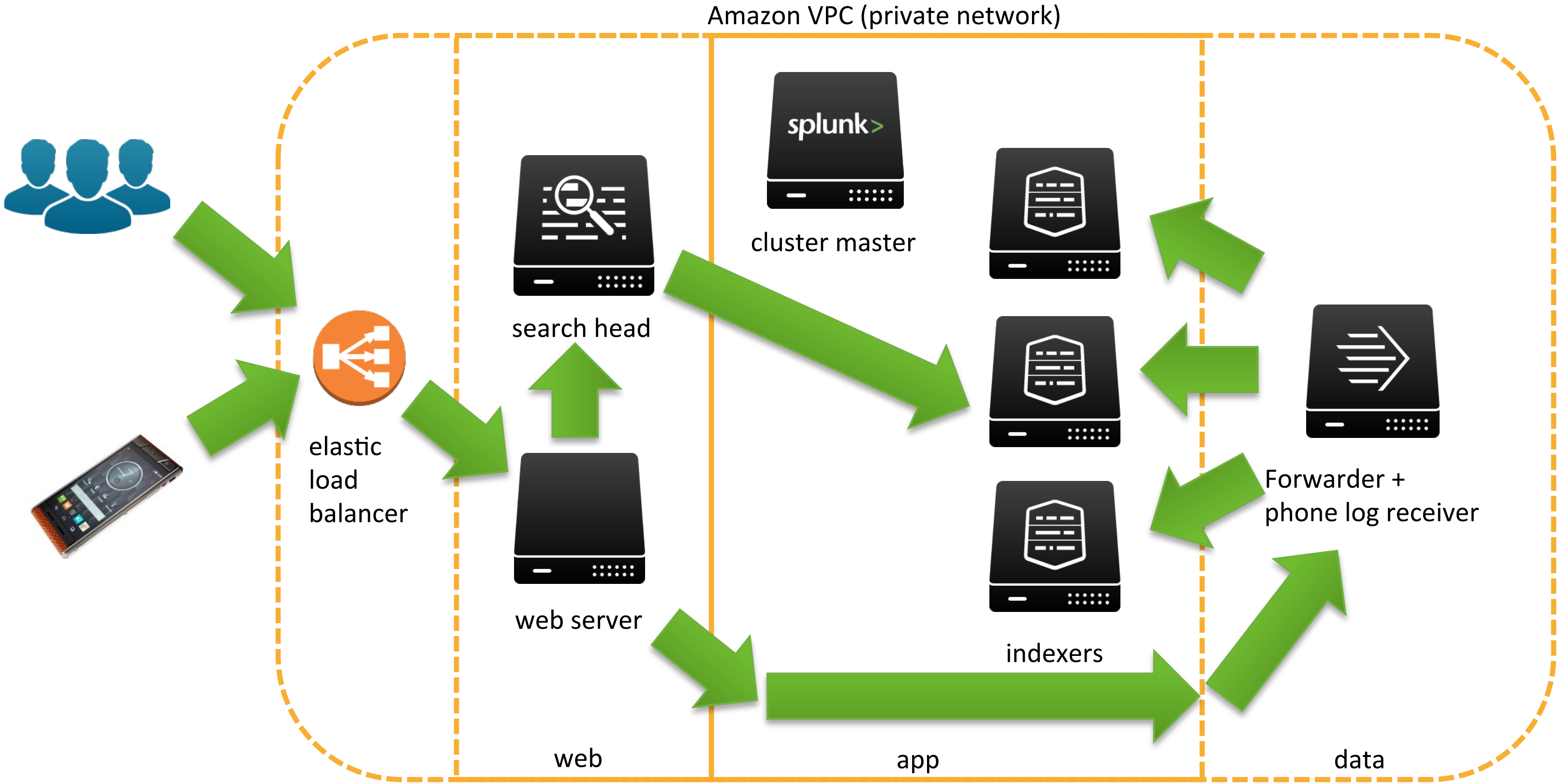
Data and IoT

Splunk @ Vertu

- Splunk Enterprise used since 2012
  - Gather diagnostics from phones being productised
  - Analyse using Splunk to give us insight into when to launch
- Today we'll see:
  - Live demo: Deploying a test Splunk cluster
  - Live demo: Capturing analytics from my phone as it crashes

Demo Setup

Simplified Demo Setup



Deployment Using Ansible

- Ansible is a configuration management tool, similar to Puppet, Chef or Saltstack
- You can automate the deployment and configuration of your infrastructure by writing Ansible playbooks
- We're going to use Ansible to deploy the whole demo setup
- But first, we need to break it…

Destroy!

- Chaos Monkey is a tool developed by Netflix to improve the resilience of their systems by randomly destroying machines.
- I feel Splunk should have a more appropriate animal…

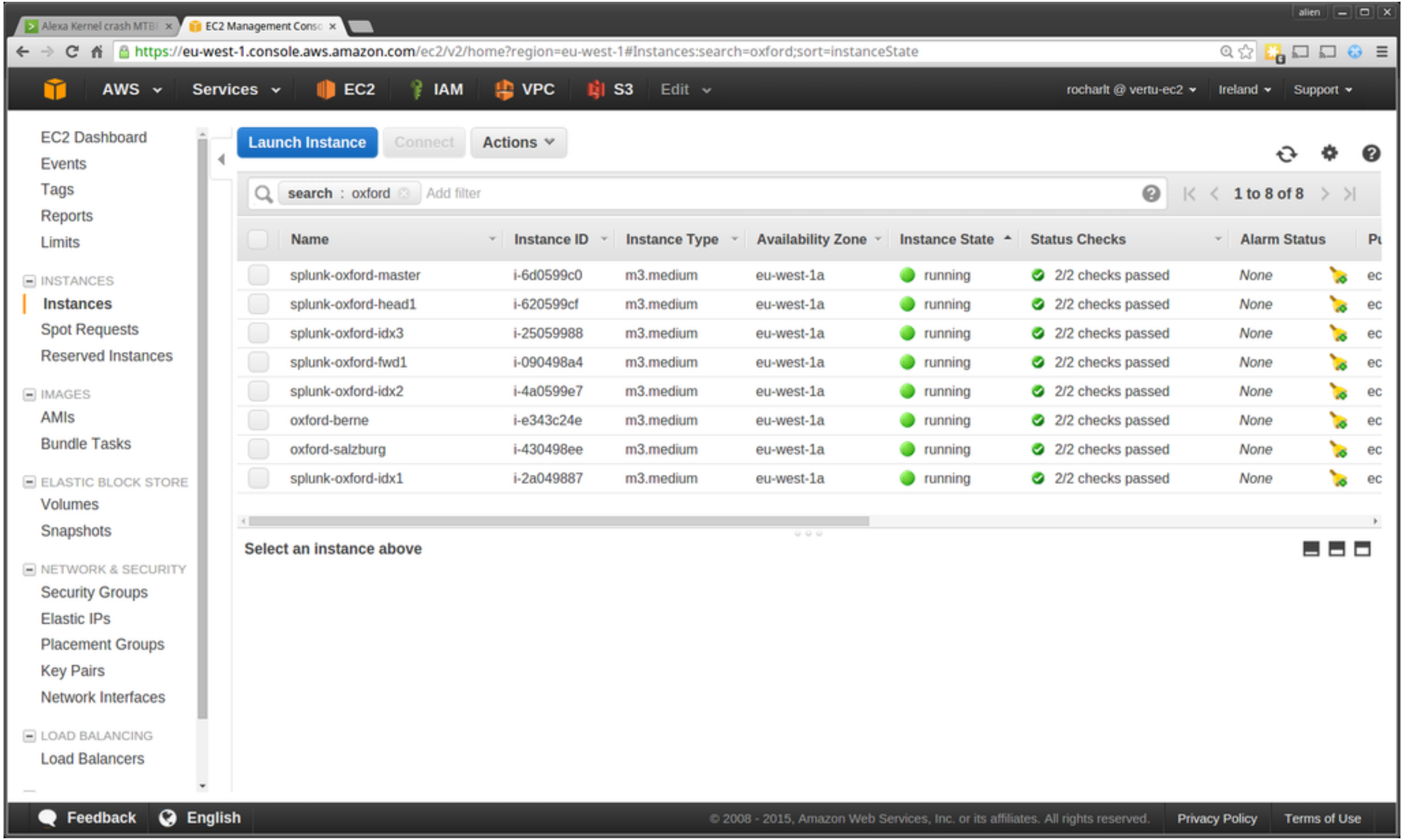
Live Demos:
First Up - Deploying Splunk Cluster With Ansible

(after the chaos pony breaks it)

Demonstration Overview

- Chaos Pony destroys the Splunk Cluster (<1 min)
- Run Ansible playbook to create empty machines (~4-5 min)
  - Blank Debian linux install from Amazon images
- Run Ansible playbook to deploy Splunk (~10 min)
  - Sets up complete OS, adds users, base APT packages etc. as well
  - I'll explain some of the playbook workings during this time
- Run Ansible playbook to deploy the log receiver application (~4 min)
  - Installs a lot of Python packages
- Demonstration of our Splunk alerts and Dashboards (~15 min)
  - Live phone crashing!

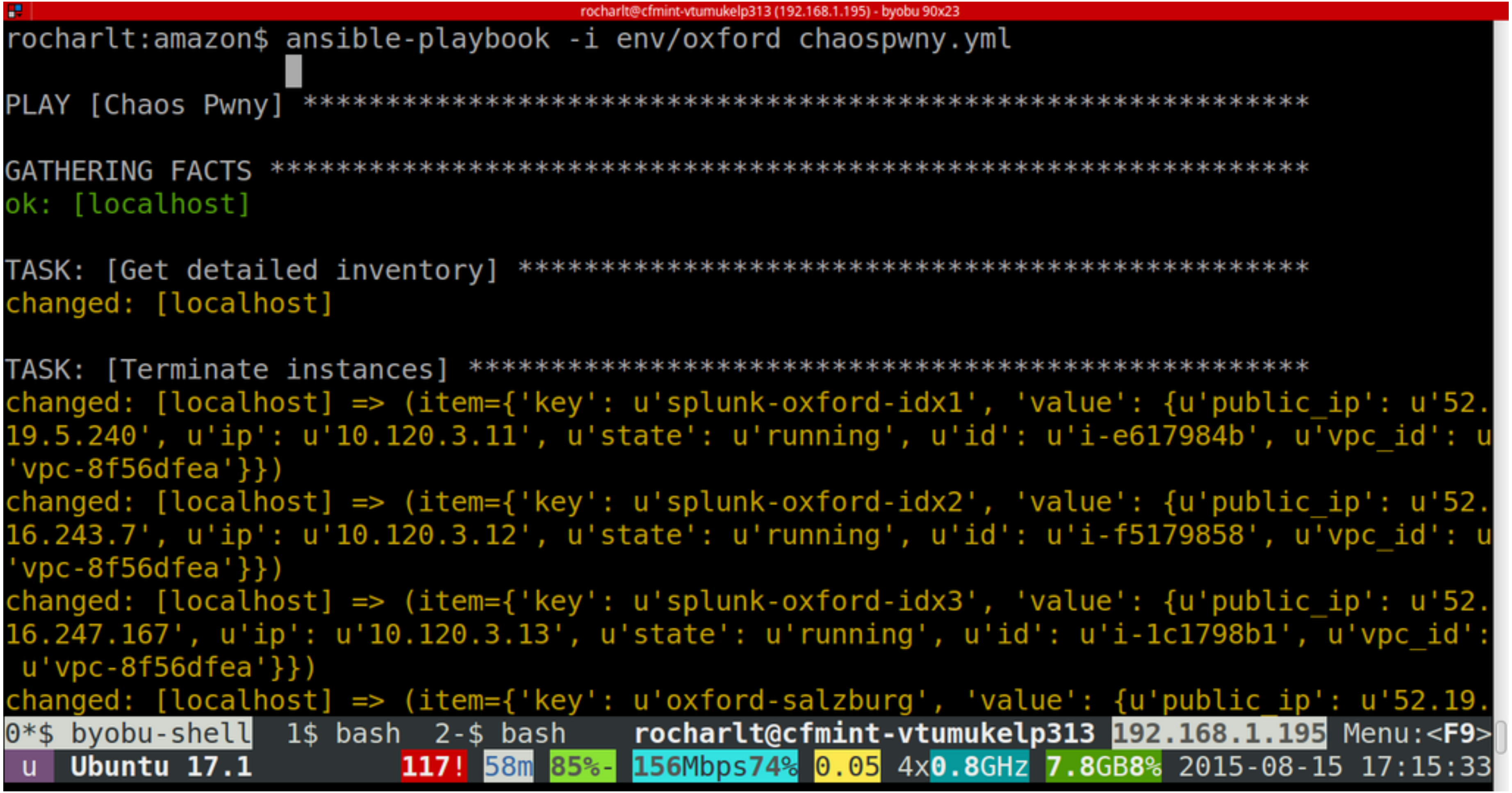
Demonstrations



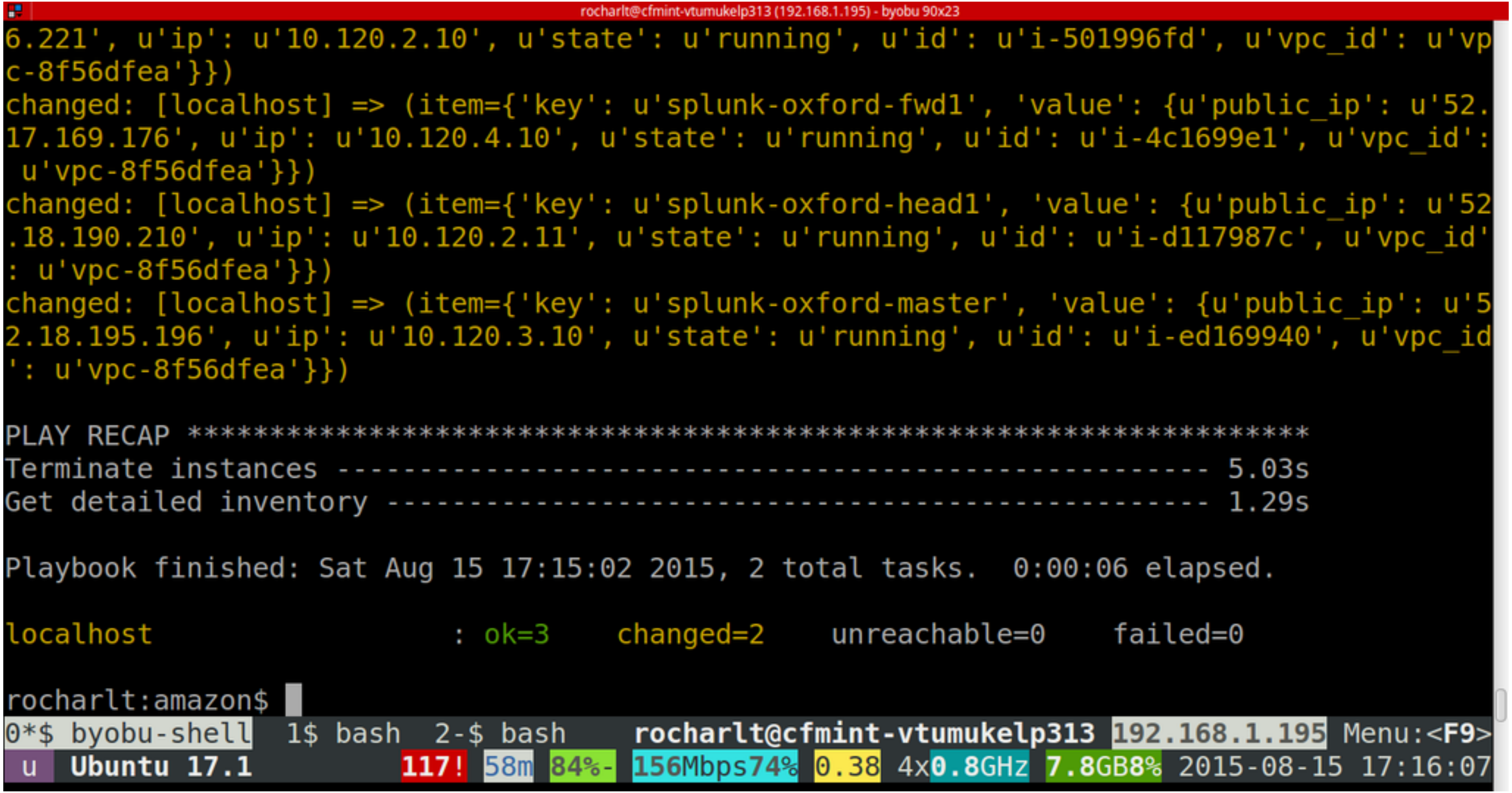
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status		Pu
splunk-oxford-master	i-6d0599c0	m3.medium	eu-west-1a	● running	✓ 2/2 checks passed	None		ec
splunk-oxford-head1	i-620599cf	m3.medium	eu-west-1a	● running	✓ 2/2 checks passed	None		ec
splunk-oxford-idx3	i-25059988	m3.medium	eu-west-1a	● running	✓ 2/2 checks passed	None		ec
splunk-oxford-fwd1	i-090498a4	m3.medium	eu-west-1a	● running	✓ 2/2 checks passed	None		ec
splunk-oxford-idx2	i-4a0599e7	m3.medium	eu-west-1a	● running	✓ 2/2 checks passed	None		ec
oxford-berne	i-e343c24e	m3.medium	eu-west-1a	● running	✓ 2/2 checks passed	None		ec
oxford-salzburg	i-430498ee	m3.medium	eu-west-1a	● running	✓ 2/2 checks passed	None		ec
splunk-oxford-idx1	i-2a049887	m3.medium	eu-west-1a	● running	✓ 2/2 checks passed	None		ec

Select an instance above

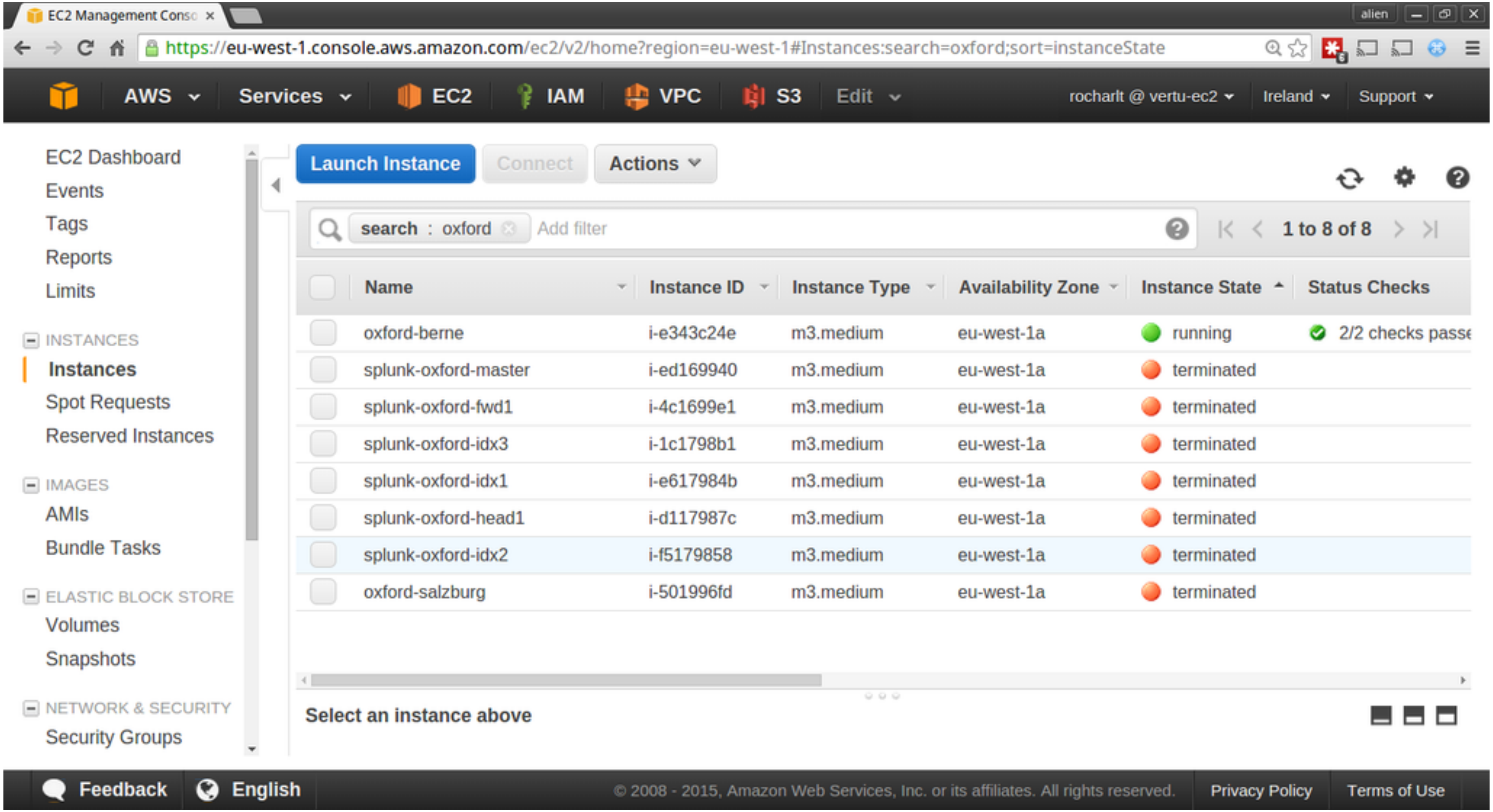
© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.



```
rocharlt:amazon$ ansible-playbook -i env/oxford chaospwny.yml


PLAY [Chaos Pwny] ************************************************************

GATHERING FACTS **************************************************************
ok: [localhost]

TASK: [Get detailed inventory] ***********************************************
changed: [localhost]

TASK: [Terminate instances] **************************************************
changed: [localhost] => (item={'key': u'splunk-oxford-idx1', 'value': {u'public_ip': u'52.
19.5.240', u'ip': u'10.120.3.11', u'state': u'running', u'id': u'i-e617984b', u'vpc_id': u
'vpc-8f56dfea'}})
changed: [localhost] => (item={'key': u'splunk-oxford-idx2', 'value': {u'public_ip': u'52.
16.243.7', u'ip': u'10.120.3.12', u'state': u'running', u'id': u'i-f5179858', u'vpc_id': u
'vpc-8f56dfea'}})
changed: [localhost] => (item={'key': u'splunk-oxford-idx3', 'value': {u'public_ip': u'52.
16.247.167', u'ip': u'10.120.3.13', u'state': u'running', u'id': u'i-1c1798b1', u'vpc_id':
 u'vpc-8f56dfea'}})
changed: [localhost] => (item={'key': u'oxford-salzburg', 'value': {u'public_ip': u'52.19.
0*$ byobu-shell  1$ bash  2-$ bash    rocharlt@cfmint-vtumukelp313 192.168.1.195 Menu:<F9>
 u  Ubuntu 17.1           117! 58m 85%- 156Mbps74% 0.05 4x0.8GHz 7.8GB8% 2015-08-15 17:15:33
```

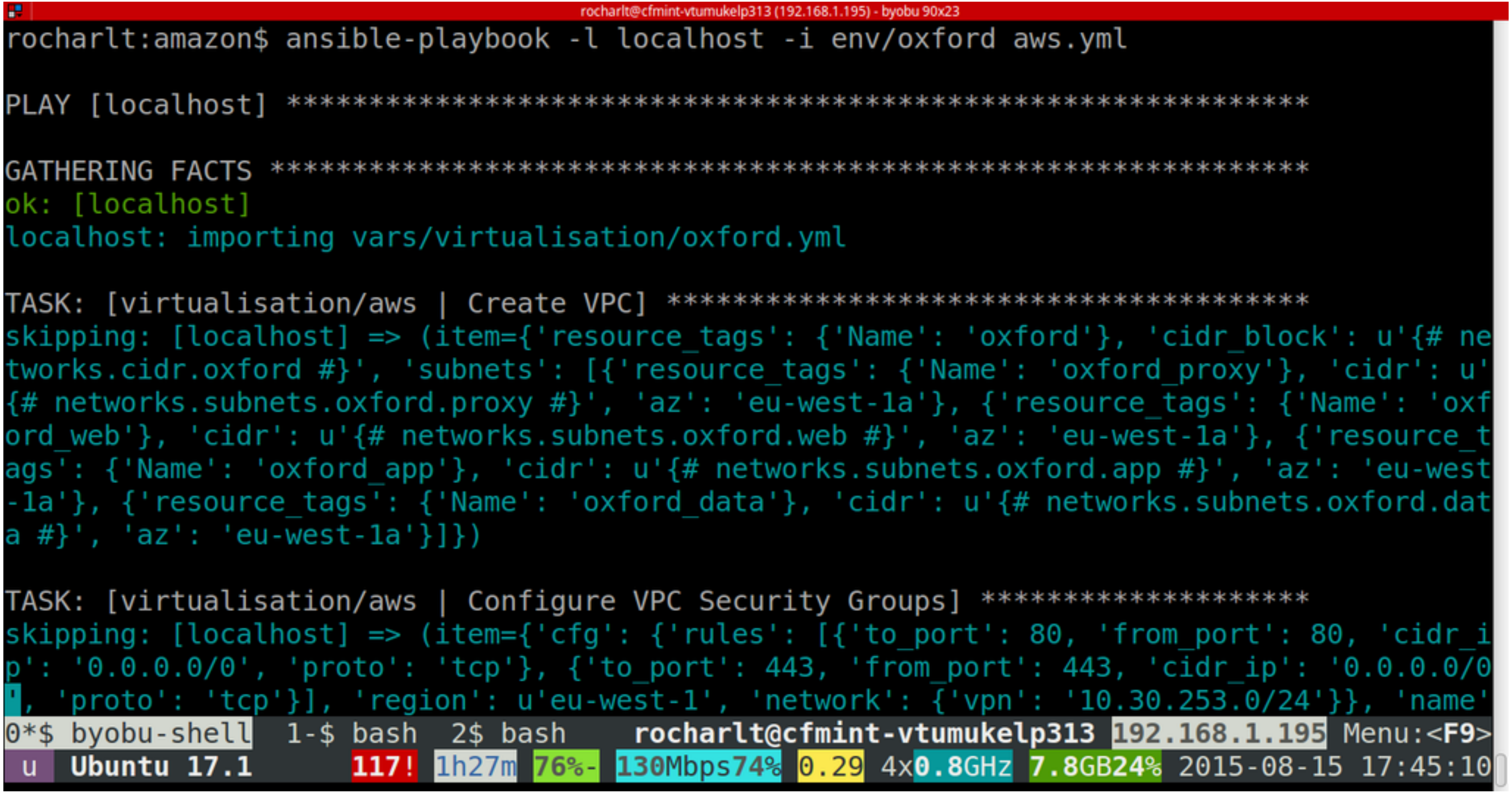


```
6.221', u'ip': u'10.120.2.10', u'state': u'running', u'id': u'i-501996fd', u'vpc_id': u'vp
c-8f56dfea'}})
changed: [localhost] => (item={'key': u'splunk-oxford-fwd1', 'value': {u'public_ip': u'52.
17.169.176', u'ip': u'10.120.4.10', u'state': u'running', u'id': u'i-4c1699e1', u'vpc_id':
 u'vpc-8f56dfea'}})
changed: [localhost] => (item={'key': u'splunk-oxford-head1', 'value': {u'public_ip': u'52
.18.190.210', u'ip': u'10.120.2.11', u'state': u'running', u'id': u'i-d117987c', u'vpc_id'
: u'vpc-8f56dfea'}})
changed: [localhost] => (item={'key': u'splunk-oxford-master', 'value': {u'public_ip': u'5
2.18.195.196', u'ip': u'10.120.3.10', u'state': u'running', u'id': u'i-ed169940', u'vpc_id
': u'vpc-8f56dfea'}})

PLAY RECAP ********************************************************************
Terminate instances ----------------------------------------------------- 5.03s
Get detailed inventory -------------------------------------------------- 1.29s

Playbook finished: Sat Aug 15 17:15:02 2015, 2 total tasks.  0:00:06 elapsed.

localhost                  : ok=3    changed=2    unreachable=0    failed=0

rocharlt:amazon$ 
0*$ byobu-shell  1$ bash  2-$ bash    rocharlt@cfmint-vtumukelp313 192.168.1.195 Menu:<F9>
 u  Ubuntu 17.1             117! 58m 84%- 156Mbps74% 0.38 4x0.8GHz 7.8GB8% 2015-08-15 17:16:07
```

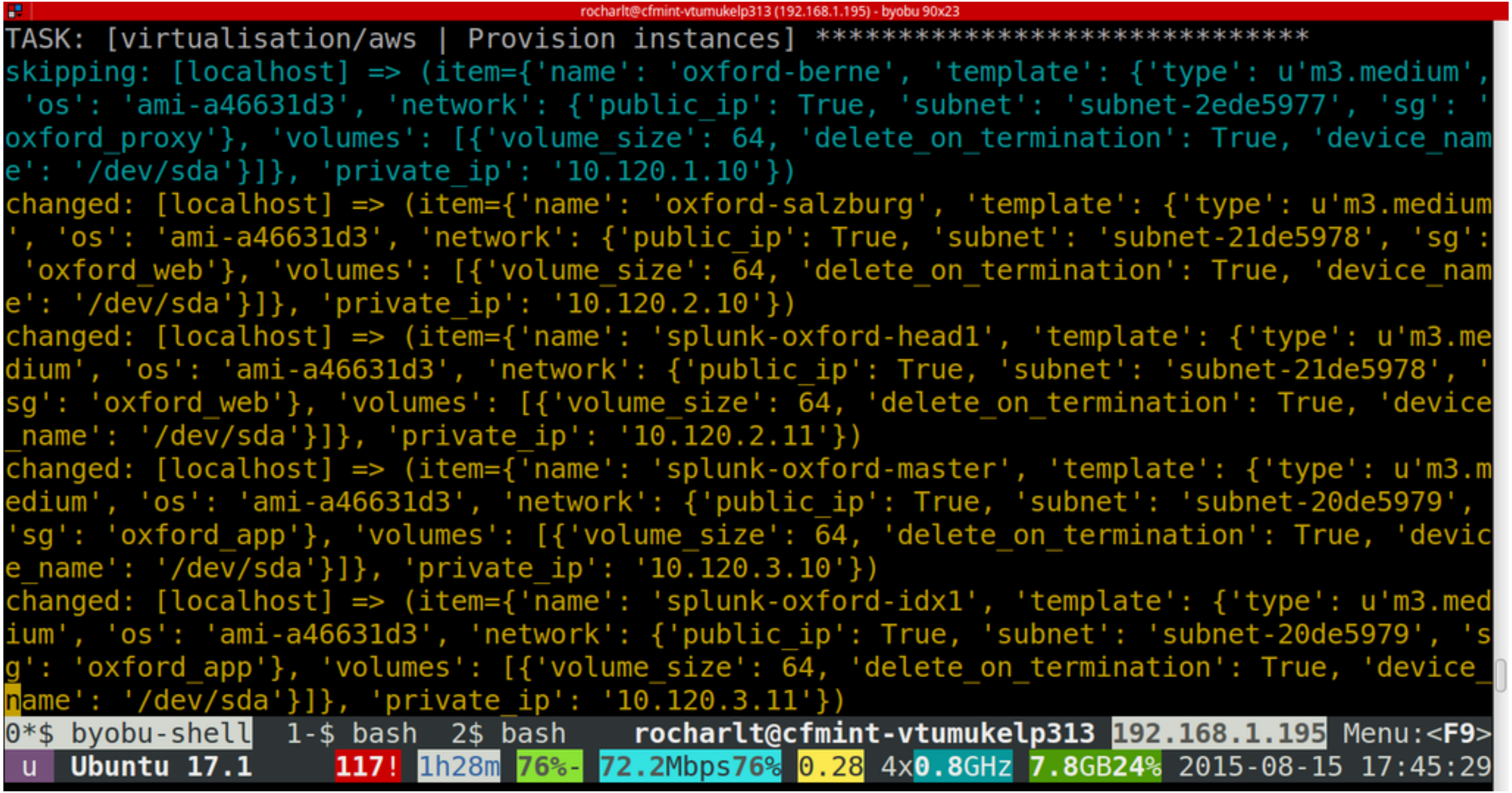


Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
oxford-berne	i-e343c24e	m3.medium	eu-west-1a	● running	✓ 2/2 checks passe
splunk-oxford-master	i-ed169940	m3.medium	eu-west-1a	● terminated	
splunk-oxford-fwd1	i-4c1699e1	m3.medium	eu-west-1a	● terminated	
splunk-oxford-idx3	i-1c1798b1	m3.medium	eu-west-1a	● terminated	
splunk-oxford-idx1	i-e617984b	m3.medium	eu-west-1a	● terminated	
splunk-oxford-head1	i-d117987c	m3.medium	eu-west-1a	● terminated	
splunk-oxford-idx2	i-f5179858	m3.medium	eu-west-1a	● terminated	
oxford-salzburg	i-501996fd	m3.medium	eu-west-1a	● terminated	

Select an instance above



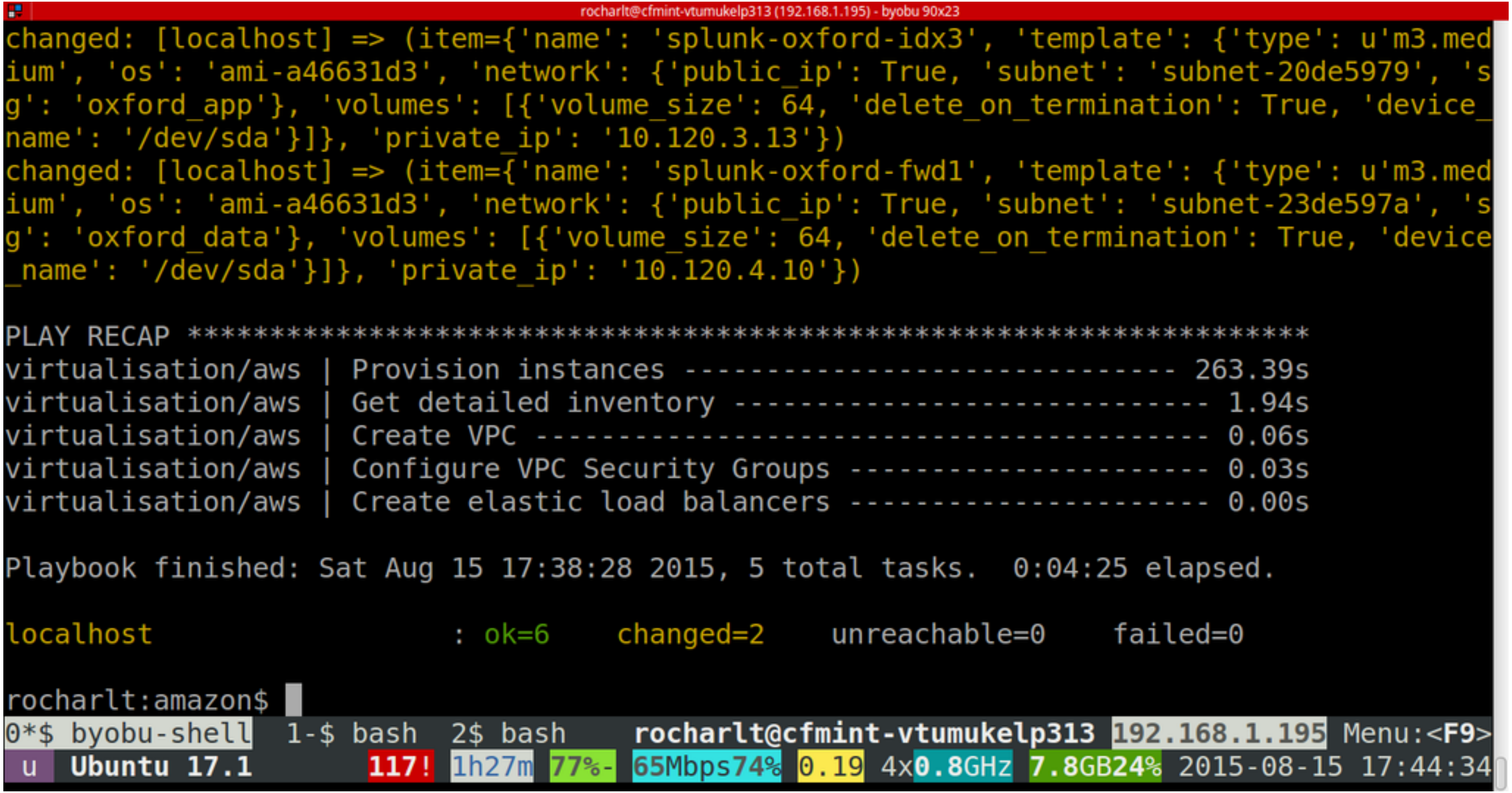
```
rocharlt:amazon$ ansible-playbook -l localhost -i env/oxford aws.yml

PLAY [localhost] **************************************************************

GATHERING FACTS ***************************************************************
ok: [localhost]
localhost: importing vars/virtualisation/oxford.yml

TASK: [virtualisation/aws | Create VPC] ***************************************
skipping: [localhost] => (item={'resource_tags': {'Name': 'oxford'}, 'cidr_block': u'{# ne
tworks.cidr.oxford #}', 'subnets': [{'resource_tags': {'Name': 'oxford_proxy'}, 'cidr': u'
{# networks.subnets.oxford.proxy #}', 'az': 'eu-west-1a'}, {'resource_tags': {'Name': 'oxf
ord_web'}, 'cidr': u'{# networks.subnets.oxford.web #}', 'az': 'eu-west-1a'}, {'resource_t
ags': {'Name': 'oxford_app'}, 'cidr': u'{# networks.subnets.oxford.app #}', 'az': 'eu-west
-1a'}, {'resource_tags': {'Name': 'oxford_data'}, 'cidr': u'{# networks.subnets.oxford.dat
a #}', 'az': 'eu-west-1a'}]})

TASK: [virtualisation/aws | Configure VPC Security Groups] ********************
skipping: [localhost] => (item={'cfg': {'rules': [{'to_port': 80, 'from_port': 80, 'cidr_i
p': '0.0.0.0/0', 'proto': 'tcp'}, {'to_port': 443, 'from_port': 443, 'cidr_ip': '0.0.0.0/0
', 'proto': 'tcp'}], 'region': u'eu-west-1', 'network': {'vpn': '10.30.253.0/24'}}, 'name'
0*$ byobu-shell  1-$ bash  2$ bash   rocharlt@cfmint-vtumukelp313 192.168.1.195 Menu:<F9>
 u  Ubuntu 17.1         117! 1h27m 76%- 130Mbps74% 0.29 4x0.8GHz 7.8GB24% 2015-08-15 17:45:10
```



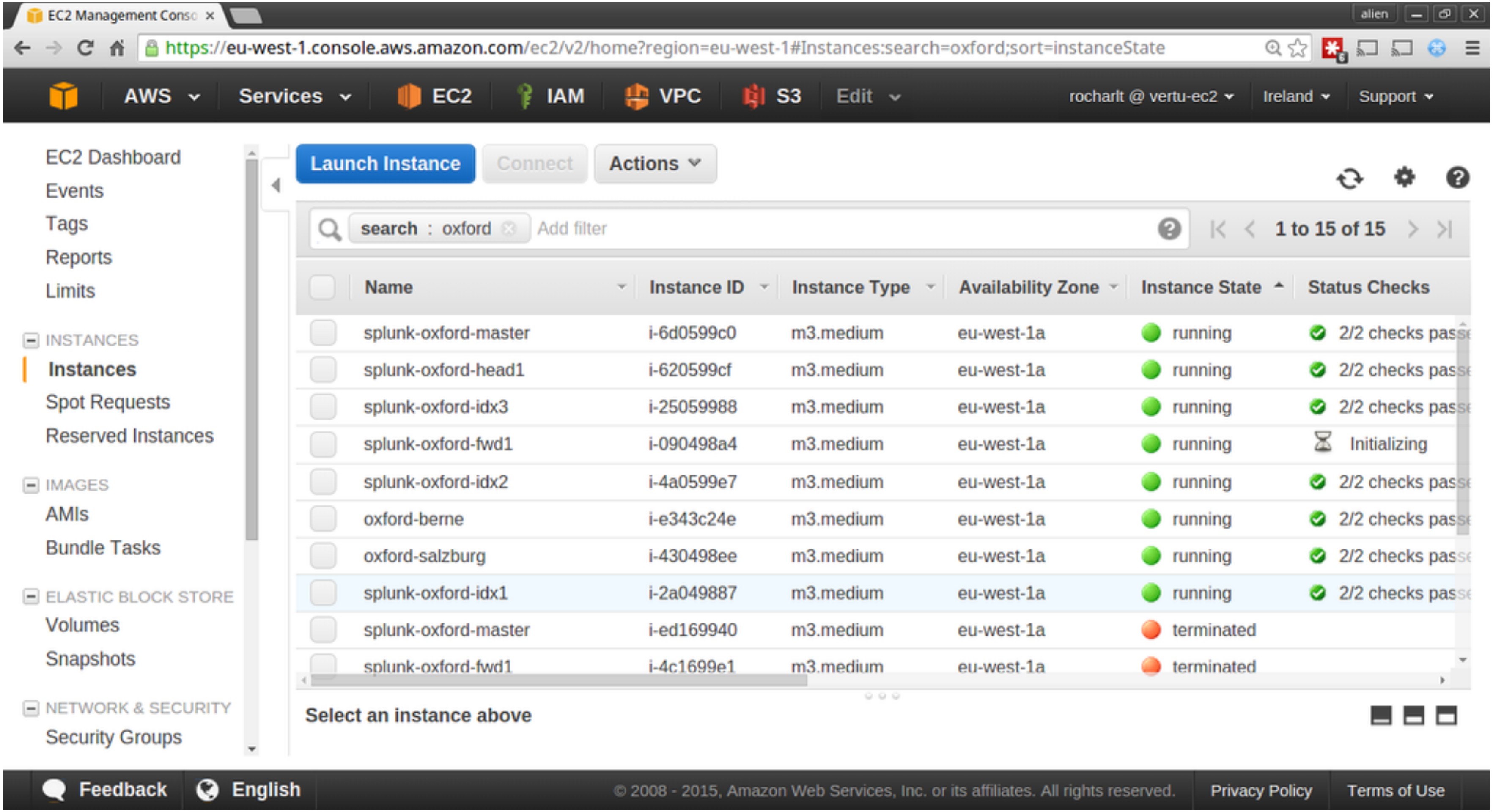
```
TASK: [virtualisation/aws | Provision instances] ******************************
skipping: [localhost] => (item={'name': 'oxford-berne', 'template': {'type': u'm3.medium',
 'os': 'ami-a46631d3', 'network': {'public_ip': True, 'subnet': 'subnet-2ede5977', 'sg': '
oxford_proxy'}, 'volumes': [{'volume_size': 64, 'delete_on_termination': True, 'device_nam
e': '/dev/sda'}]}, 'private_ip': '10.120.1.10'})
changed: [localhost] => (item={'name': 'oxford-salzburg', 'template': {'type': u'm3.medium
', 'os': 'ami-a46631d3', 'network': {'public_ip': True, 'subnet': 'subnet-21de5978', 'sg':
 'oxford_web'}, 'volumes': [{'volume_size': 64, 'delete_on_termination': True, 'device_nam
e': '/dev/sda'}]}, 'private_ip': '10.120.2.10'})
changed: [localhost] => (item={'name': 'splunk-oxford-head1', 'template': {'type': u'm3.me
dium', 'os': 'ami-a46631d3', 'network': {'public_ip': True, 'subnet': 'subnet-21de5978', '
sg': 'oxford_web'}, 'volumes': [{'volume_size': 64, 'delete_on_termination': True, 'device
_name': '/dev/sda'}]}, 'private_ip': '10.120.2.11'})
changed: [localhost] => (item={'name': 'splunk-oxford-master', 'template': {'type': u'm3.m
edium', 'os': 'ami-a46631d3', 'network': {'public_ip': True, 'subnet': 'subnet-20de5979',
'sg': 'oxford_app'}, 'volumes': [{'volume_size': 64, 'delete_on_termination': True, 'devic
e_name': '/dev/sda'}]}, 'private_ip': '10.120.3.10'})
changed: [localhost] => (item={'name': 'splunk-oxford-idx1', 'template': {'type': u'm3.med
ium', 'os': 'ami-a46631d3', 'network': {'public_ip': True, 'subnet': 'subnet-20de5979', 's
g': 'oxford_app'}, 'volumes': [{'volume_size': 64, 'delete_on_termination': True, 'device_
name': '/dev/sda'}]}, 'private_ip': '10.120.3.11'})
0*$ byobu-shell  1-$ bash  2$ bash   rocharlt@cfmint-vtumukelp313 192.168.1.195 Menu:<F9>
 u  Ubuntu 17.1      117! 1h28m 76%- 72.2Mbps76% 0.28 4x0.8GHz 7.8GB24% 2015-08-15 17:45:29
```

.conf2015

splunk>



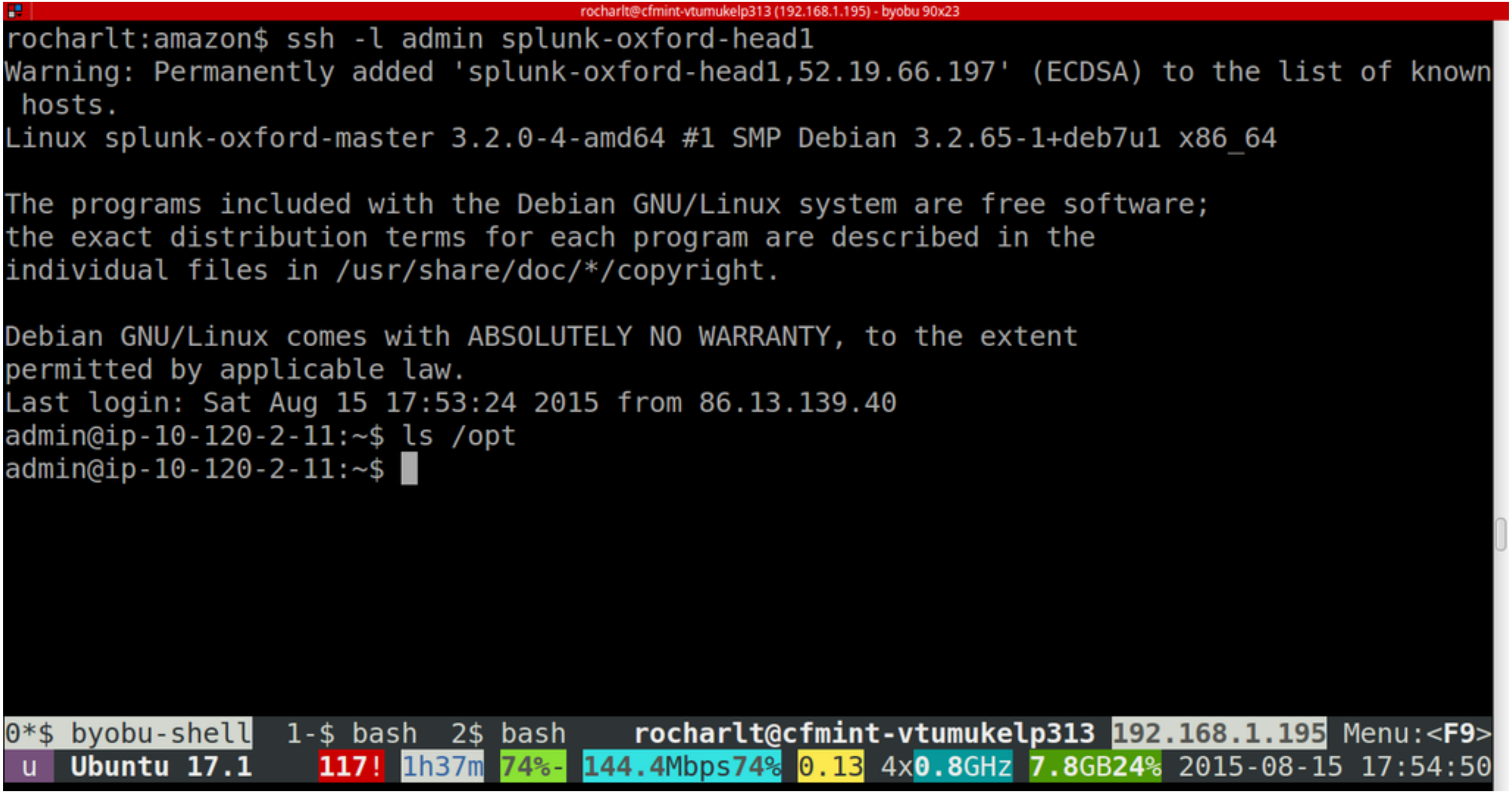
```
changed: [localhost] => (item={'name': 'splunk-oxford-idx3', 'template': {'type': u'm3.med
ium', 'os': 'ami-a46631d3', 'network': {'public_ip': True, 'subnet': 'subnet-20de5979', 's
g': 'oxford_app'}, 'volumes': [{'volume_size': 64, 'delete_on_termination': True, 'device_
name': '/dev/sda'}]}, 'private_ip': '10.120.3.13'})
changed: [localhost] => (item={'name': 'splunk-oxford-fwd1', 'template': {'type': u'm3.med
ium', 'os': 'ami-a46631d3', 'network': {'public_ip': True, 'subnet': 'subnet-23de597a', 's
g': 'oxford_data'}, 'volumes': [{'volume_size': 64, 'delete_on_termination': True, 'device
_name': '/dev/sda'}]}, 'private_ip': '10.120.4.10'})

PLAY RECAP ********************************************************************
virtualisation/aws | Provision instances ---------------------------- 263.39s
virtualisation/aws | Get detailed inventory ---------------------------- 1.94s
virtualisation/aws | Create VPC ---------------------------------------- 0.06s
virtualisation/aws | Configure VPC Security Groups --------------------- 0.03s
virtualisation/aws | Create elastic load balancers --------------------- 0.00s

Playbook finished: Sat Aug 15 17:38:28 2015, 5 total tasks.  0:04:25 elapsed.

localhost                  : ok=6    changed=2    unreachable=0    failed=0

rocharlt:amazon$ 
0*$ byobu-shell  1-$ bash  2$ bash   rocharlt@cfmint-vtumukelp313 192.168.1.195 Menu:<F9>
 u  Ubuntu 17.1          117! 1h27m 77%- 65Mbps74% 0.19 4x0.8GHz 7.8GB24% 2015-08-15 17:44:34
```



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks
splunk-oxford-master	i-6d0599c0	m3.medium	eu-west-1a	● running	✓ 2/2 checks pass
splunk-oxford-head1	i-620599cf	m3.medium	eu-west-1a	● running	✓ 2/2 checks pass
splunk-oxford-idx3	i-25059988	m3.medium	eu-west-1a	● running	✓ 2/2 checks pass
splunk-oxford-fwd1	i-090498a4	m3.medium	eu-west-1a	● running	⌛ Initializing
splunk-oxford-idx2	i-4a0599e7	m3.medium	eu-west-1a	● running	✓ 2/2 checks pass
oxford-berne	i-e343c24e	m3.medium	eu-west-1a	● running	✓ 2/2 checks pass
oxford-salzburg	i-430498ee	m3.medium	eu-west-1a	● running	✓ 2/2 checks pass
splunk-oxford-idx1	i-2a049887	m3.medium	eu-west-1a	● running	✓ 2/2 checks pass
splunk-oxford-master	i-ed169940	m3.medium	eu-west-1a	● terminated	
splunk-oxford-fwd1	i-4c1699e1	m3.medium	eu-west-1a	● terminated	

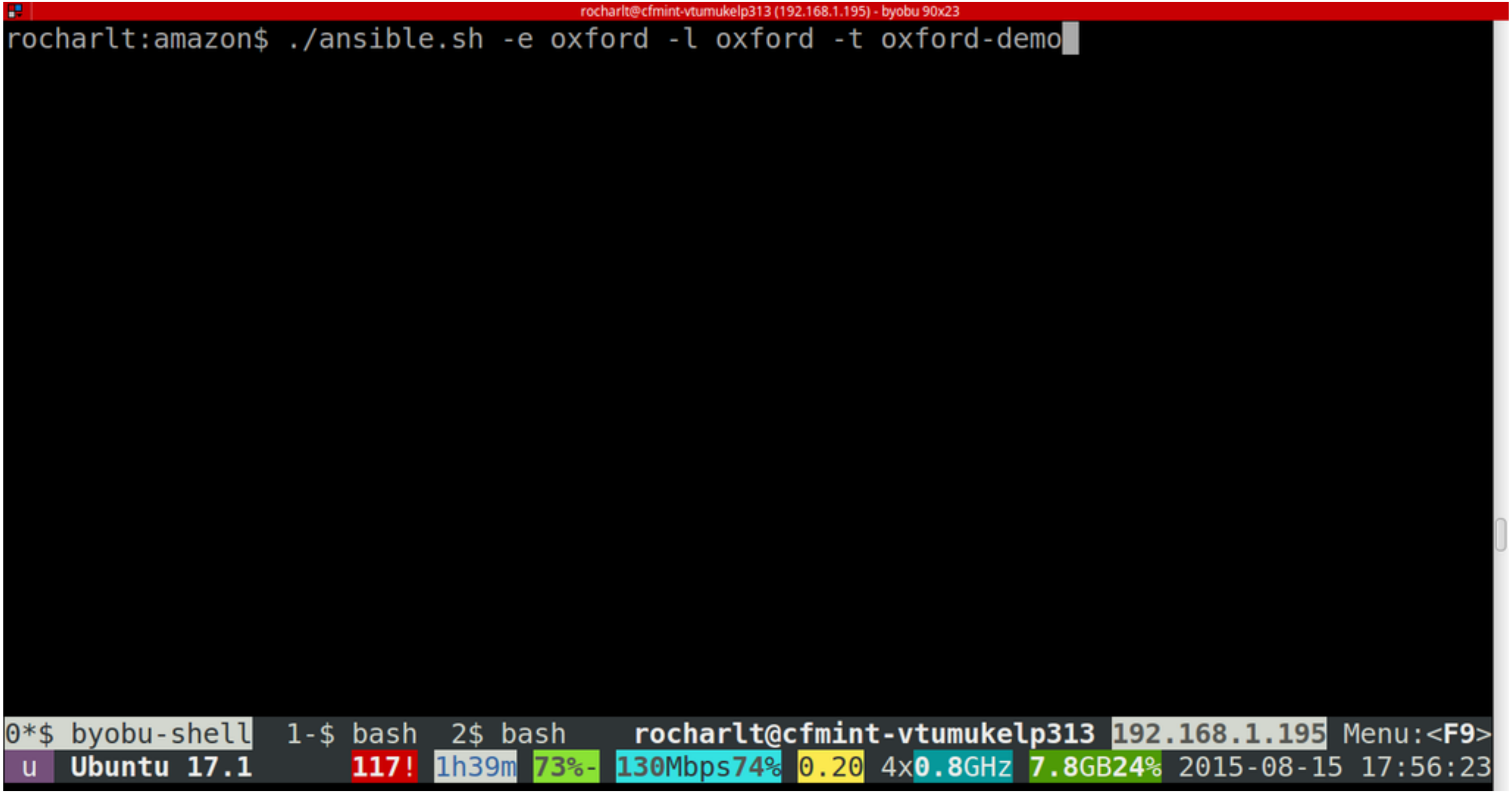
Select an instance above

© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved.



```
rocharlt:amazon$ ssh -l admin splunk-oxford-head1
Warning: Permanently added 'splunk-oxford-head1,52.19.66.197' (ECDSA) to the list of known
 hosts.
Linux splunk-oxford-master 3.2.0-4-amd64 #1 SMP Debian 3.2.65-1+deb7u1 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Aug 15 17:53:24 2015 from 86.13.139.40
admin@ip-10-120-2-11:~$ ls /opt
admin@ip-10-120-2-11:~$ 
```

```
0*$ byobu-shell   1-$ bash   2$ bash     rocharlt@cfmint-vtumukelp313 192.168.1.195 Menu:<F9>
 u  Ubuntu 17.1      117! 1h37m 74%- 144.4Mbps74% 0.13 4x0.8GHz 7.8GB24% 2015-08-15 17:54:50
```

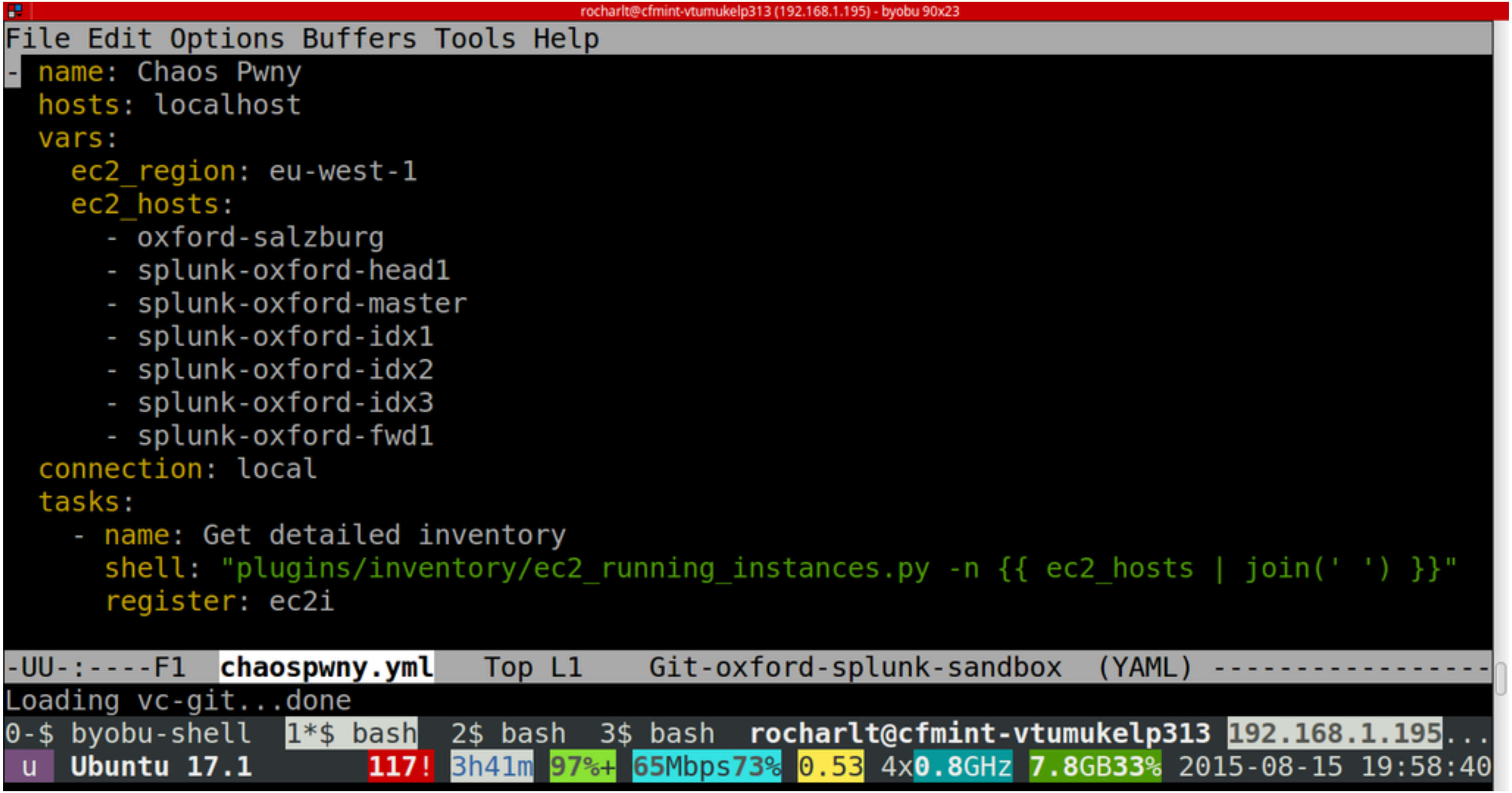


```
rocharlt:amazon$ ./ansible.sh -e oxford -l oxford -t oxford-demo
```

```
0*$ byobu-shell  1-$ bash  2$ bash   rocharlt@cfmint-vtumukelp313 192.168.1.195 Menu:<F9>
 u  Ubuntu 17.1      117! 1h39m 73%- 130Mbps74% 0.20 4x0.8GHz 7.8GB24% 2015-08-15 17:56:23
```

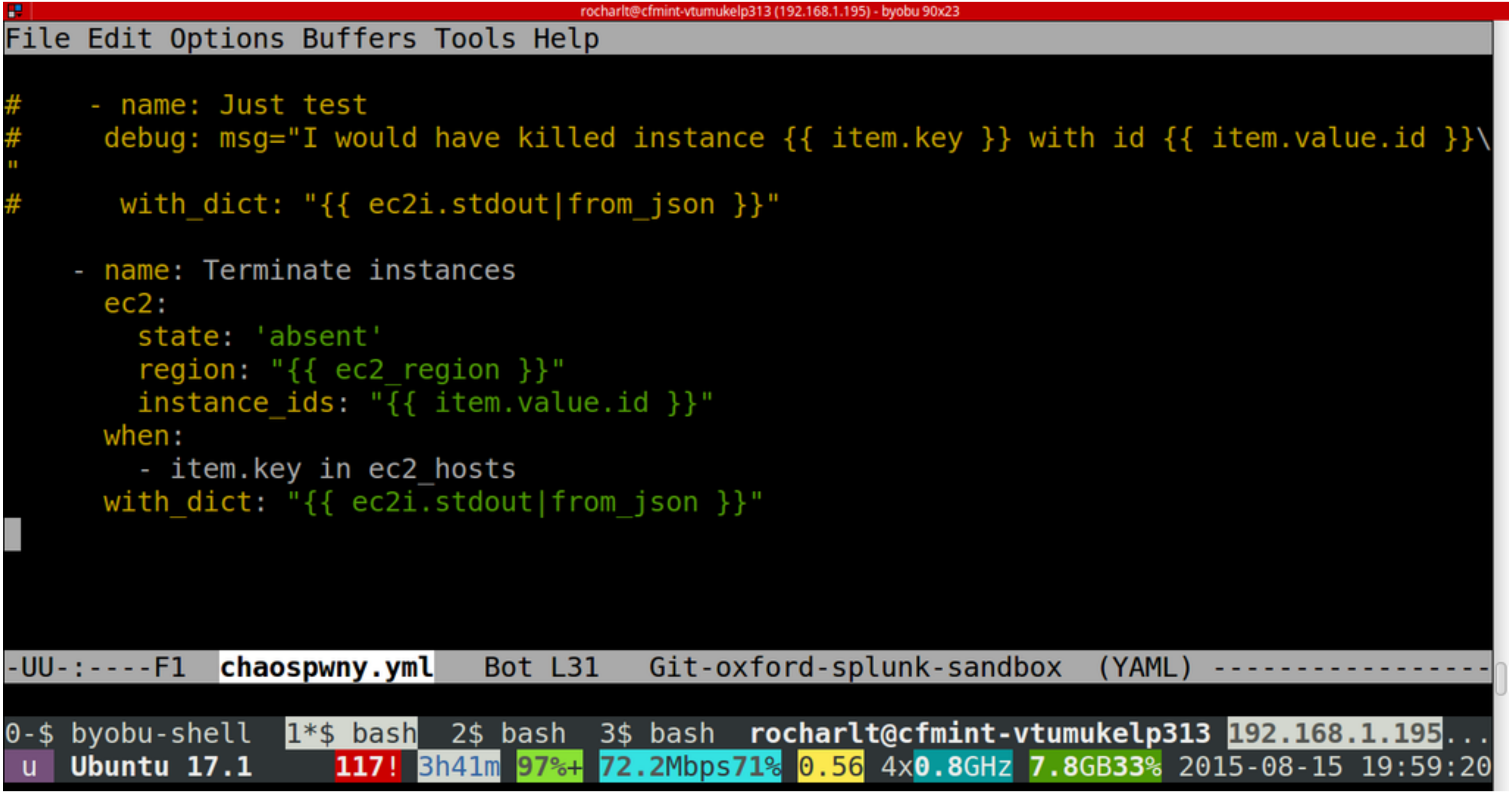
Pause While Main Play Runs

- Lets examine what’s in the Ansible code

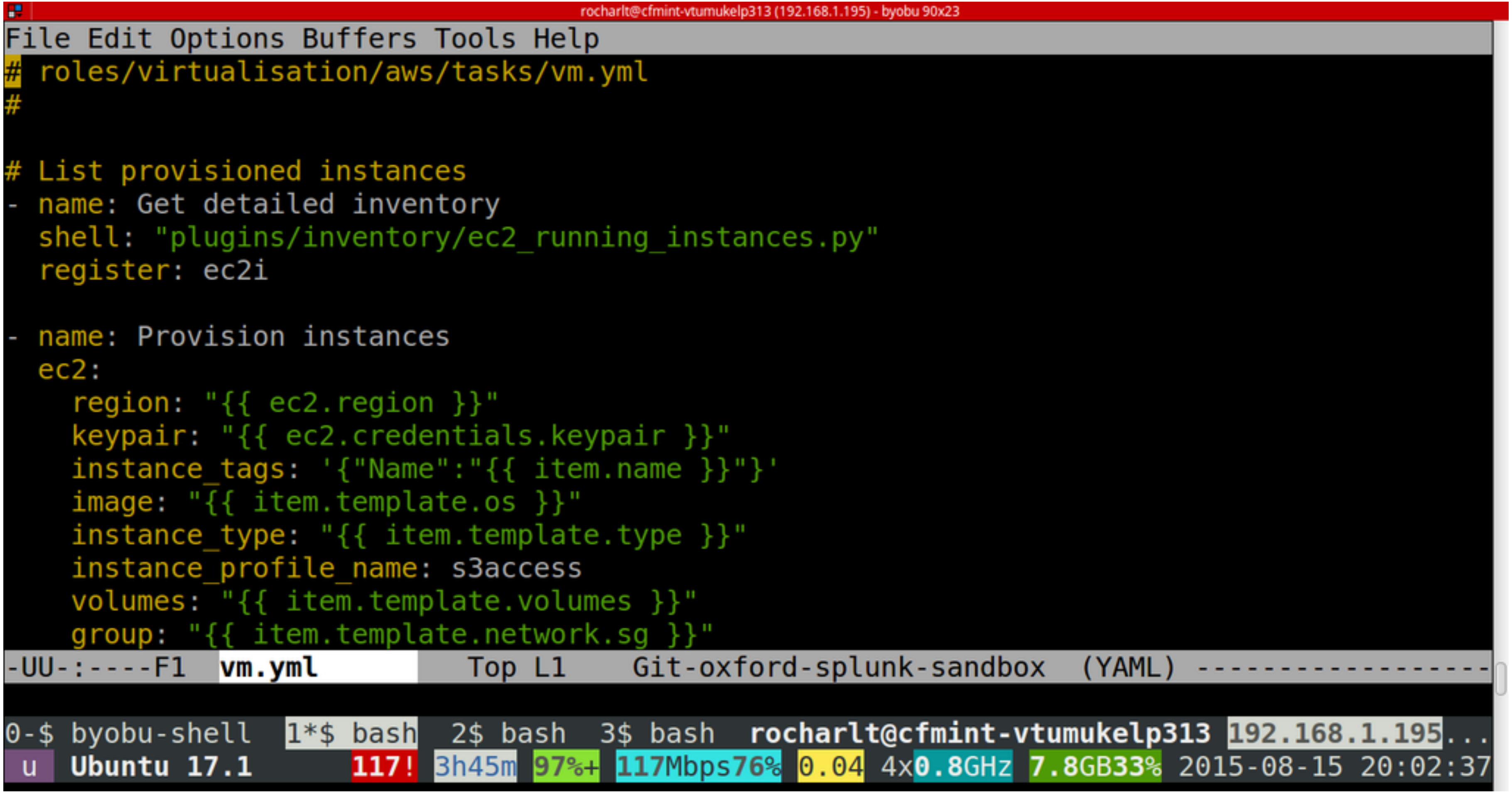


rocharlt@cfmint-vtumukelp313 (192.168.1.195) - byobu 90x23
File Edit Options Buffers Tools Help

```
- name: Chaos Pwny
  hosts: localhost
  vars:
    ec2_region: eu-west-1
    ec2_hosts:
      - oxford-salzburg
      - splunk-oxford-head1
      - splunk-oxford-master
      - splunk-oxford-idx1
      - splunk-oxford-idx2
      - splunk-oxford-idx3
      - splunk-oxford-fwd1
  connection: local
  tasks:
    - name: Get detailed inventory
      shell: "plugins/inventory/ec2_running_instances.py -n {{ ec2_hosts | join(' ') }}"
      register: ec2i

-UU-:----F1  chaospwny.yml   Top L1    Git-oxford-splunk-sandbox  (YAML) -----------------
Loading vc-git...done
0-$ byobu-shell  1*$ bash  2$ bash  3$ bash  rocharlt@cfmint-vtumukelp313 192.168.1.195...
 u  Ubuntu 17.1          117! 3h41m 97%+ 65Mbps73% 0.53 4x0.8GHz 7.8GB33% 2015-08-15 19:58:40
```

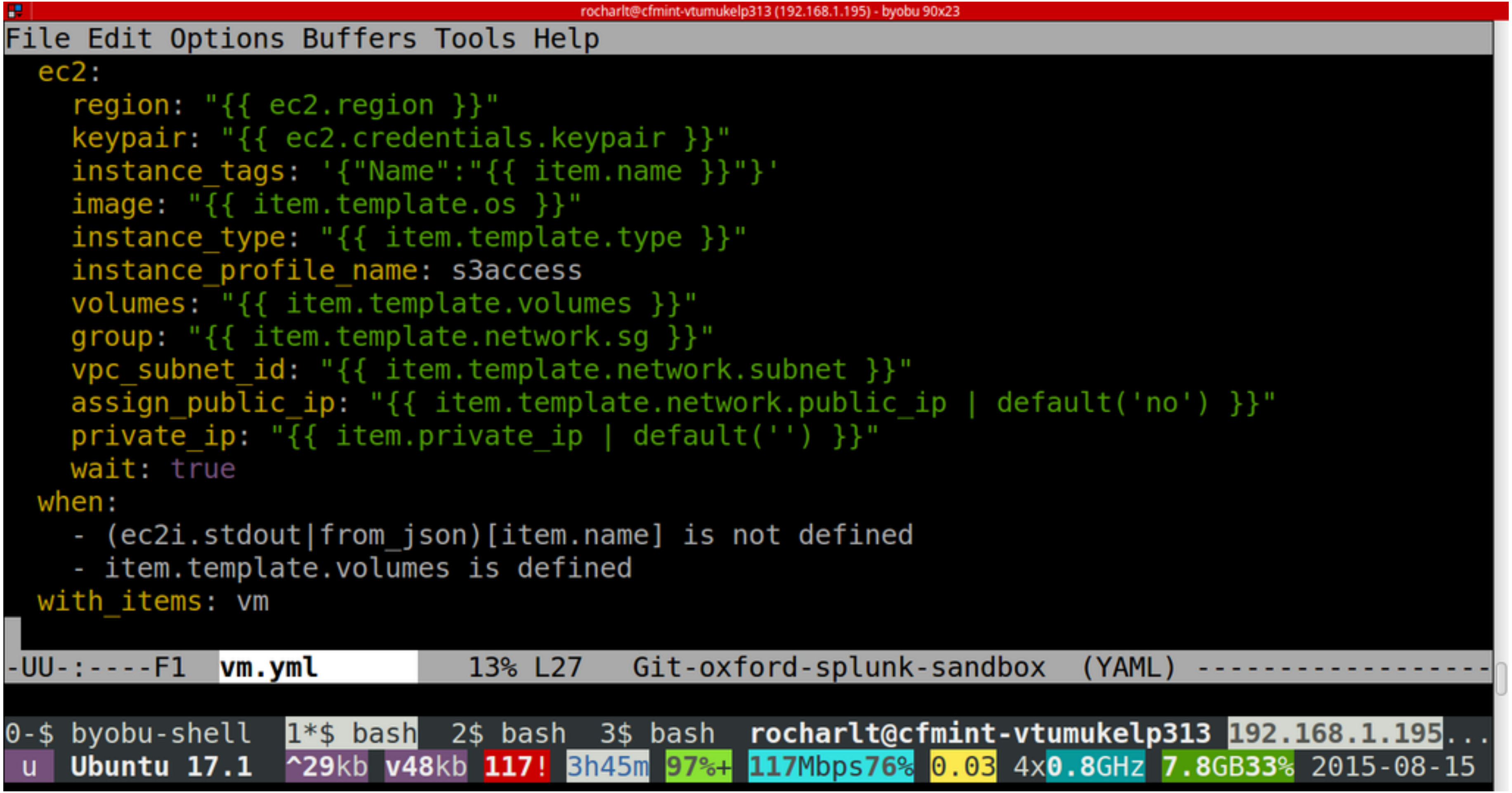

rocharlt@cfmint-vtumukelp313 (192.168.1.195) - byobu 90x23
File Edit Options Buffers Tools Help

```
#    - name: Just test
#     debug: msg="I would have killed instance {{ item.key }} with id {{ item.value.id }}\
"
#      with_dict: "{{ ec2i.stdout|from_json }}"

    - name: Terminate instances
      ec2:
        state: 'absent'
        region: "{{ ec2_region }}"
        instance_ids: "{{ item.value.id }}"
      when:
        - item.key in ec2_hosts
      with_dict: "{{ ec2i.stdout|from_json }}"

-UU-:----F1  chaospwny.yml   Bot L31   Git-oxford-splunk-sandbox  (YAML) -----------------

0-$ byobu-shell  1*$ bash  2$ bash  3$ bash  rocharlt@cfmint-vtumukelp313 192.168.1.195...
 u  Ubuntu 17.1      117! 3h41m 97%+ 72.2Mbps71% 0.56 4x0.8GHz 7.8GB33% 2015-08-15 19:59:20
```

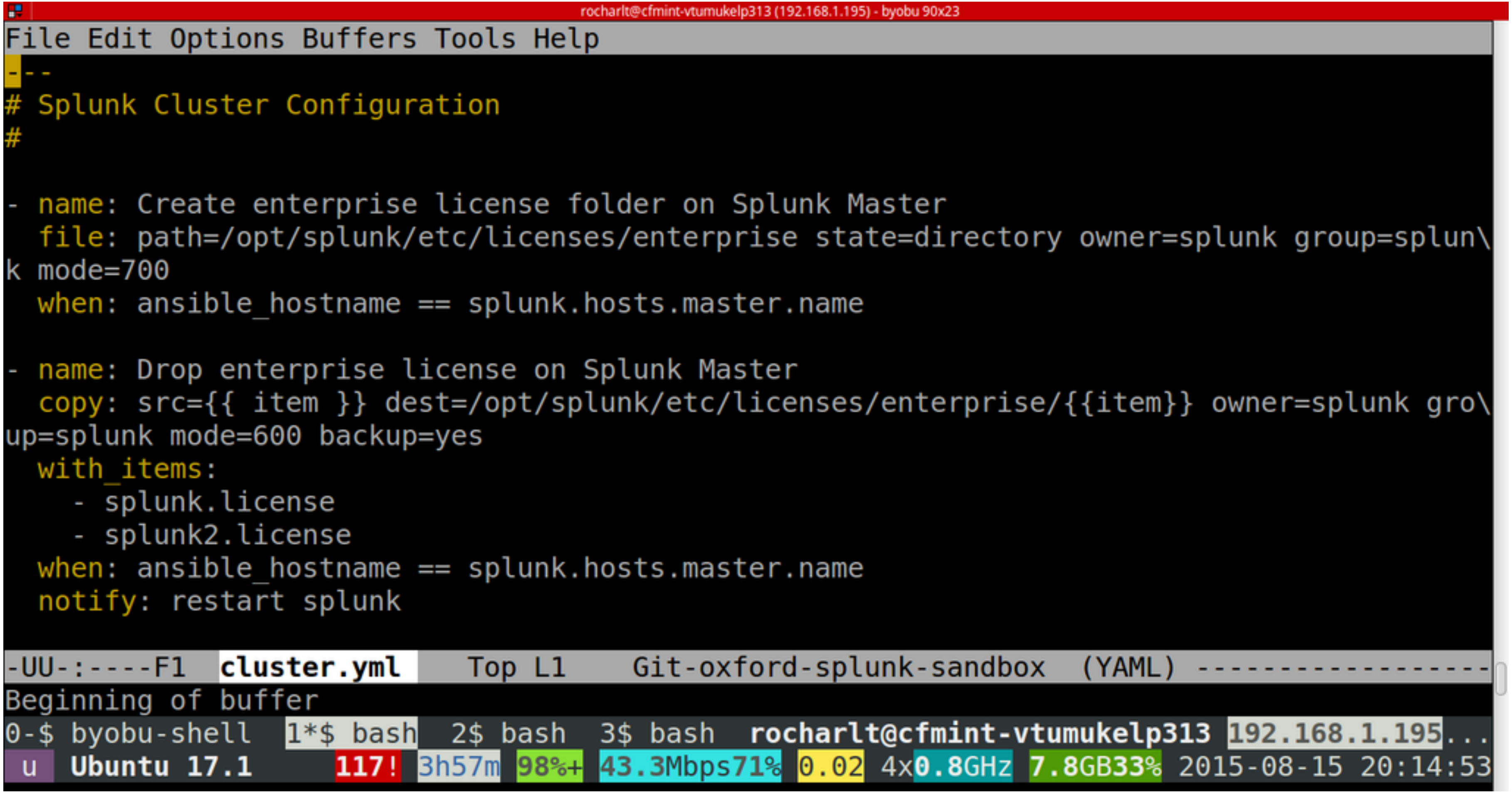


rocharlt@cfmint-vtumukelp313 (192.168.1.195) - byobu 90x23

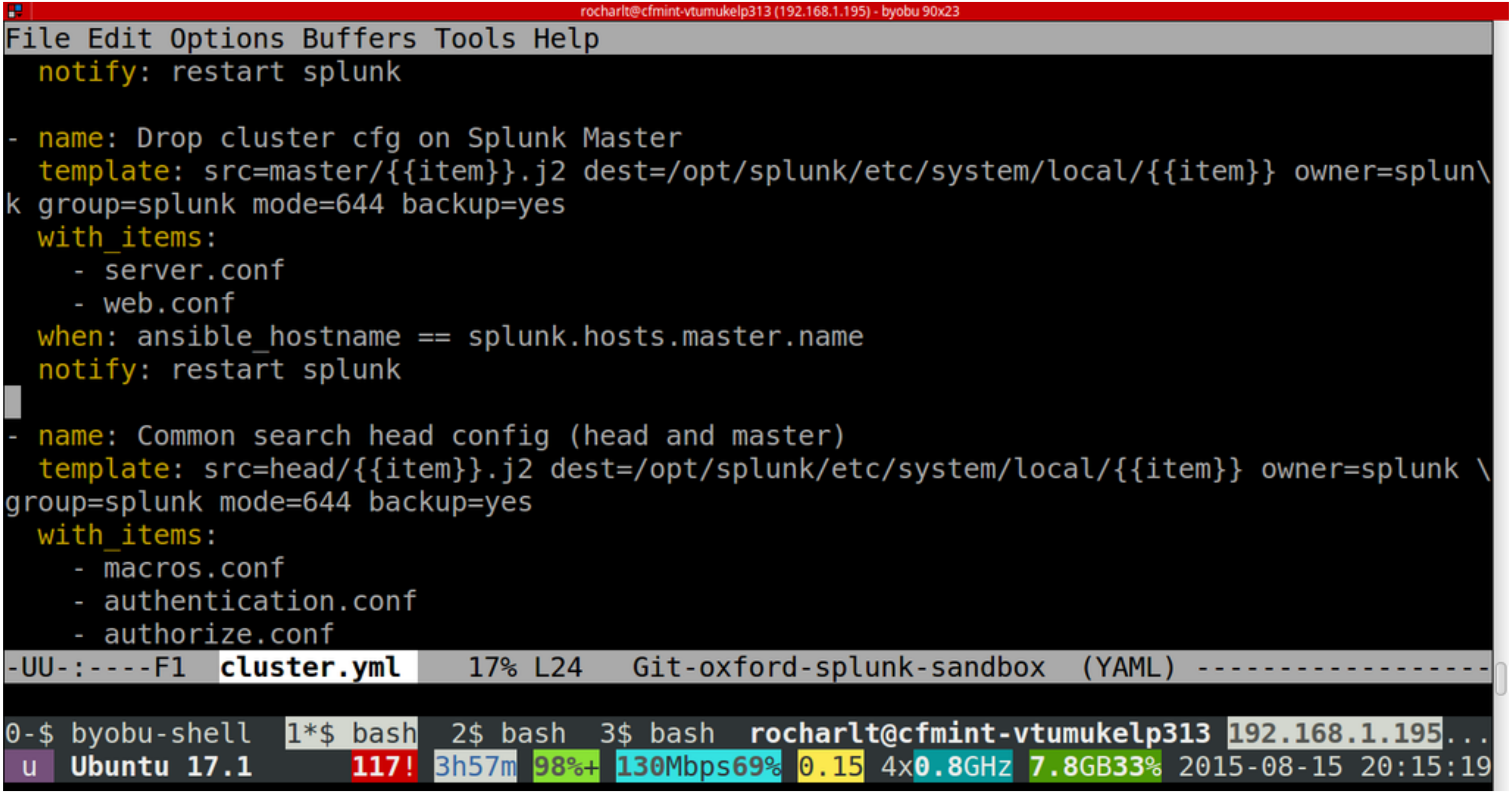
```
# roles/virtualisation/aws/tasks/vm.yml
#

# List provisioned instances
- name: Get detailed inventory
  shell: "plugins/inventory/ec2_running_instances.py"
  register: ec2i

- name: Provision instances
  ec2:
    region: "{{ ec2.region }}"
    keypair: "{{ ec2.credentials.keypair }}"
    instance_tags: '{"Name":"{{ item.name }}"}'
    image: "{{ item.template.os }}"
    instance_type: "{{ item.template.type }}"
    instance_profile_name: s3access
    volumes: "{{ item.template.volumes }}"
    group: "{{ item.template.network.sg }}"
-UU-:----F1  vm.yml         Top L1     Git-oxford-splunk-sandbox  (YAML) ------------------

0-$ byobu-shell  1*$ bash  2$ bash  3$ bash  rocharlt@cfmint-vtumukelp313 192.168.1.195...
 u  Ubuntu 17.1        117! 3h45m 97%+ 117Mbps76% 0.04 4x0.8GHz 7.8GB33% 2015-08-15 20:02:37
```


rocharlt@cfmint-vtumukelp313 (192.168.1.195) - byobu 90x23
File Edit Options Buffers Tools Help

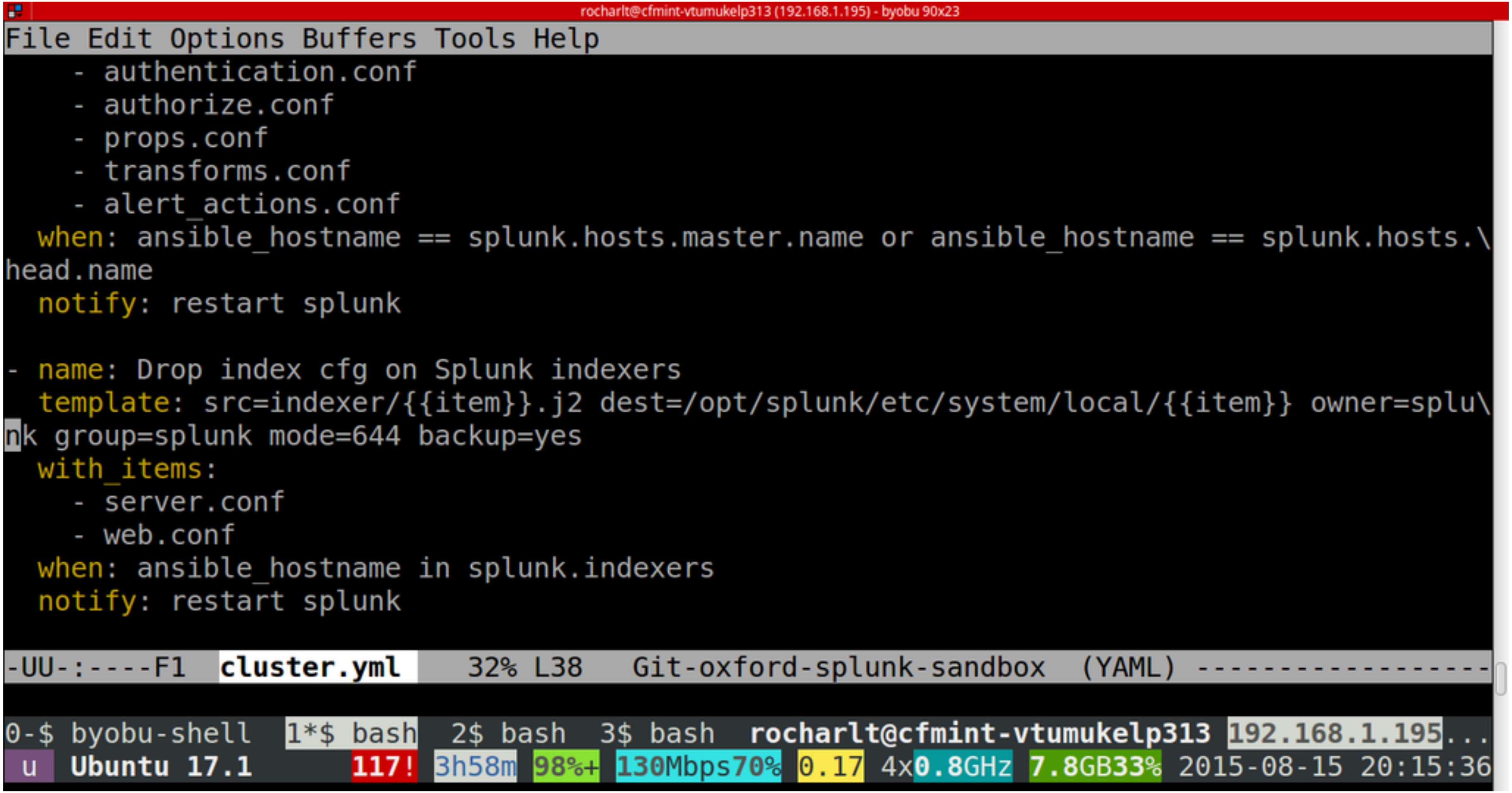
```
  ec2:
    region: "{{ ec2.region }}"
    keypair: "{{ ec2.credentials.keypair }}"
    instance_tags: '{"Name":"{{ item.name }}"}'
    image: "{{ item.template.os }}"
    instance_type: "{{ item.template.type }}"
    instance_profile_name: s3access
    volumes: "{{ item.template.volumes }}"
    group: "{{ item.template.network.sg }}"
    vpc_subnet_id: "{{ item.template.network.subnet }}"
    assign_public_ip: "{{ item.template.network.public_ip | default('no') }}"
    private_ip: "{{ item.private_ip | default('') }}"
    wait: true
  when:
    - (ec2i.stdout|from_json)[item.name] is not defined
    - item.template.volumes is defined
  with_items: vm

-UU-:----F1  vm.yml        13% L27   Git-oxford-splunk-sandbox  (YAML) -----------------

0-$ byobu-shell  1*$ bash  2$ bash  3$ bash  rocharlt@cfmint-vtumukelp313 192.168.1.195...
 u  Ubuntu 17.1  ^29kb v48kb 117! 3h45m 97%+ 117Mbps76% 0.03 4x0.8GHz 7.8GB33% 2015-08-15
```


rocharlt@cfmint-vtumukelp313 (192.168.1.195) - byobu 90x23
File Edit Options Buffers Tools Help

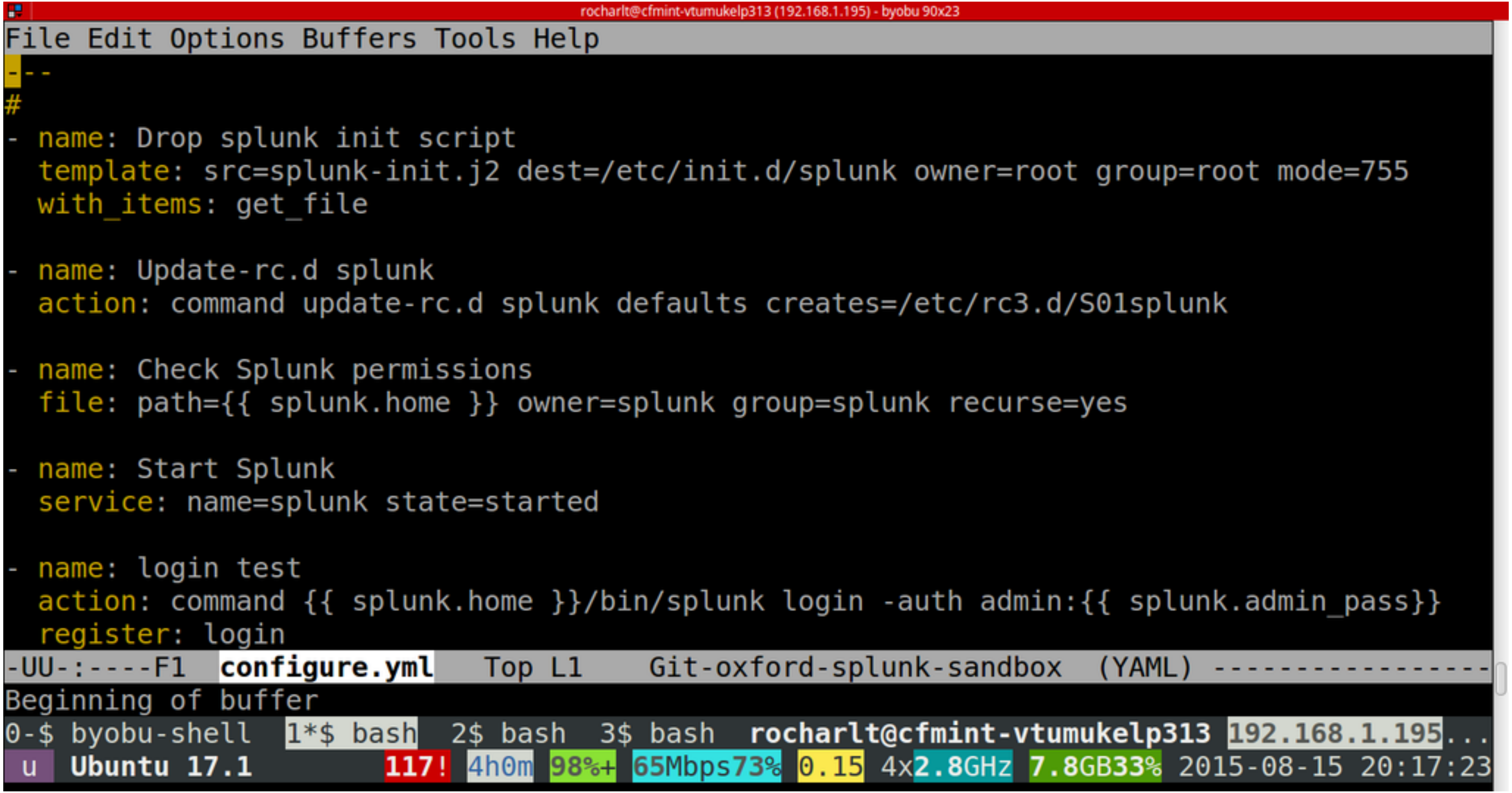
```
---
# Splunk Cluster Configuration
#

- name: Create enterprise license folder on Splunk Master
  file: path=/opt/splunk/etc/licenses/enterprise state=directory owner=splunk group=splun\
k mode=700
  when: ansible_hostname == splunk.hosts.master.name

- name: Drop enterprise license on Splunk Master
  copy: src={{ item }} dest=/opt/splunk/etc/licenses/enterprise/{{item}} owner=splunk gro\
up=splunk mode=600 backup=yes
  with_items:
    - splunk.license
    - splunk2.license
  when: ansible_hostname == splunk.hosts.master.name
  notify: restart splunk

-UU-:----F1  cluster.yml    Top L1    Git-oxford-splunk-sandbox  (YAML) -------------------
Beginning of buffer
0-$ byobu-shell  1*$ bash  2$ bash  3$ bash  rocharlt@cfmint-vtumukelp313 192.168.1.195...
 u  Ubuntu 17.1       117! 3h57m 98%+ 43.3Mbps71% 0.02 4x0.8GHz 7.8GB33% 2015-08-15 20:14:53
```


rocharlt@cfmint-vtumukelp313 (192.168.1.195) - byobu 90x23
File Edit Options Buffers Tools Help

```
  notify: restart splunk

- name: Drop cluster cfg on Splunk Master
  template: src=master/{{item}}.j2 dest=/opt/splunk/etc/system/local/{{item}} owner=splun\
k group=splunk mode=644 backup=yes
  with_items:
    - server.conf
    - web.conf
  when: ansible_hostname == splunk.hosts.master.name
  notify: restart splunk

- name: Common search head config (head and master)
  template: src=head/{{item}}.j2 dest=/opt/splunk/etc/system/local/{{item}} owner=splunk \
group=splunk mode=644 backup=yes
  with_items:
    - macros.conf
    - authentication.conf
    - authorize.conf
-UU-:----F1  cluster.yml    17% L24    Git-oxford-splunk-sandbox  (YAML) -----------------

0-$ byobu-shell  1*$ bash  2$ bash  3$ bash  rocharlt@cfmint-vtumukelp313 192.168.1.195...
 u  Ubuntu 17.1        117! 3h57m 98%+ 130Mbps69% 0.15 4x0.8GHz 7.8GB33% 2015-08-15 20:15:19
```


rocharlt@cfmint-vtumukelp313 (192.168.1.195) - byobu 90x23
File Edit Options Buffers Tools Help

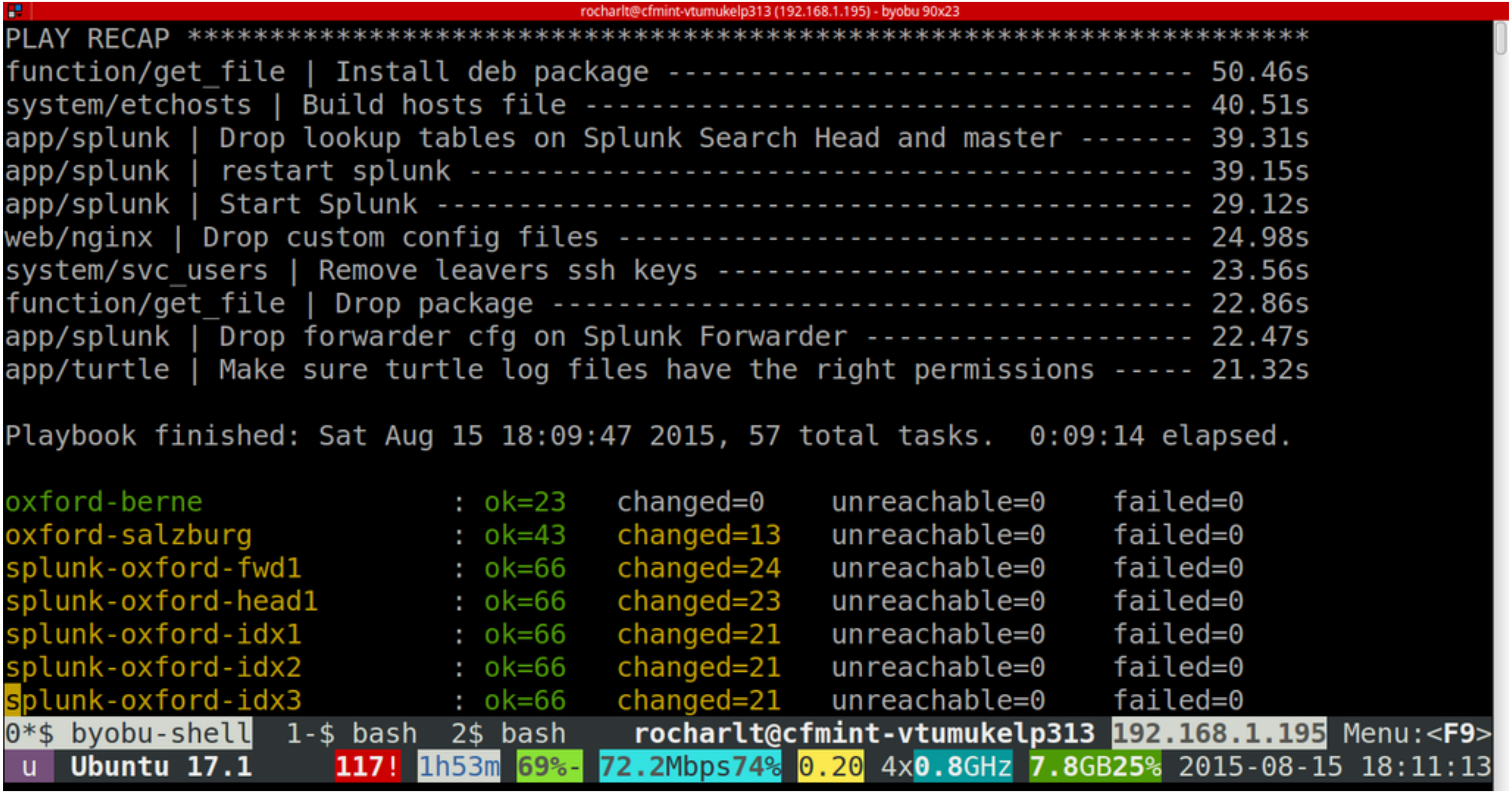
```
    - authentication.conf
    - authorize.conf
    - props.conf
    - transforms.conf
    - alert_actions.conf
  when: ansible_hostname == splunk.hosts.master.name or ansible_hostname == splunk.hosts.\
head.name
  notify: restart splunk

- name: Drop index cfg on Splunk indexers
  template: src=indexer/{{item}}.j2 dest=/opt/splunk/etc/system/local/{{item}} owner=splu\
nk group=splunk mode=644 backup=yes
  with_items:
    - server.conf
    - web.conf
  when: ansible_hostname in splunk.indexers
  notify: restart splunk

-UU-:----F1  cluster.yml    32% L38   Git-oxford-splunk-sandbox  (YAML) ------------------

0-$ byobu-shell  1*$ bash  2$ bash  3$ bash  rocharlt@cfmint-vtumukelp313 192.168.1.195...
 u  Ubuntu 17.1         117! 3h58m 98%+ 130Mbps70% 0.17 4x0.8GHz 7.8GB33% 2015-08-15 20:15:36
```


rocharlt@cfmint-vtumukelp313 (192.168.1.195) - byobu 90x23
File Edit Options Buffers Tools Help

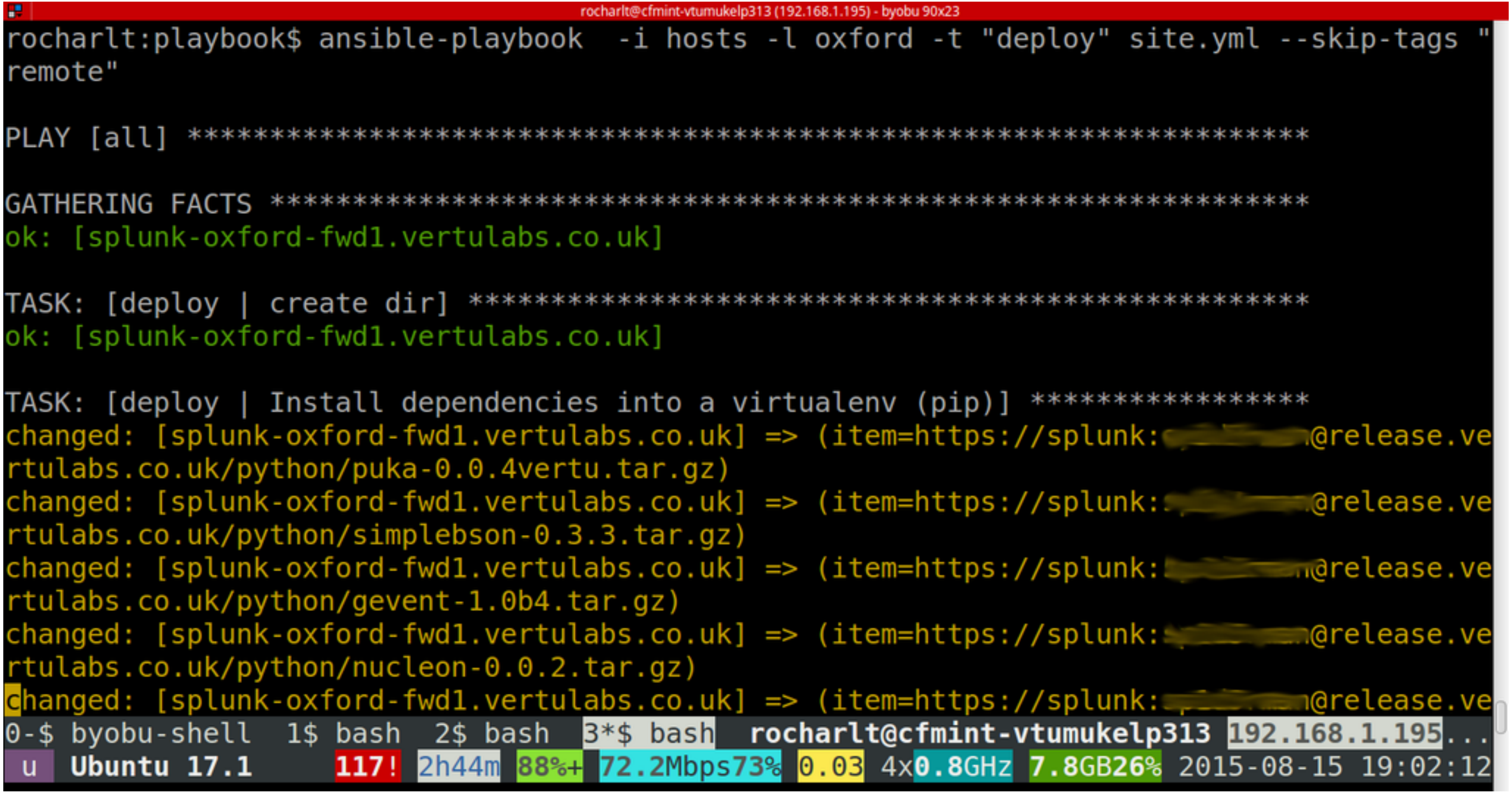
```
---
#
- name: Drop splunk init script
  template: src=splunk-init.j2 dest=/etc/init.d/splunk owner=root group=root mode=755
  with_items: get_file

- name: Update-rc.d splunk
  action: command update-rc.d splunk defaults creates=/etc/rc3.d/S01splunk

- name: Check Splunk permissions
  file: path={{ splunk.home }} owner=splunk group=splunk recurse=yes

- name: Start Splunk
  service: name=splunk state=started

- name: login test
  action: command {{ splunk.home }}/bin/splunk login -auth admin:{{ splunk.admin_pass}}
  register: login
-UU-:----F1  configure.yml   Top L1   Git-oxford-splunk-sandbox  (YAML) ------------------
Beginning of buffer
0-$ byobu-shell  1*$ bash  2$ bash  3$ bash  rocharlt@cfmint-vtumukelp313 192.168.1.195...
 u  Ubuntu 17.1          117! 4h0m 98%+ 65Mbps73% 0.15 4x2.8GHz 7.8GB33% 2015-08-15 20:17:23
```

Back To The Deployment…

- Now it is finished



```
PLAY RECAP ********************************************************************
function/get_file | Install deb package -------------------------------- 50.46s
system/etchosts | Build hosts file ------------------------------------- 40.51s
app/splunk | Drop lookup tables on Splunk Search Head and master ------- 39.31s
app/splunk | restart splunk -------------------------------------------- 39.15s
app/splunk | Start Splunk ---------------------------------------------- 29.12s
web/nginx | Drop custom config files ----------------------------------- 24.98s
system/svc_users | Remove leavers ssh keys ----------------------------- 23.56s
function/get_file | Drop package --------------------------------------- 22.86s
app/splunk | Drop forwarder cfg on Splunk Forwarder -------------------- 22.47s
app/turtle | Make sure turtle log files have the right permissions ----- 21.32s

Playbook finished: Sat Aug 15 18:09:47 2015, 57 total tasks.  0:09:14 elapsed.

oxford-berne               : ok=23   changed=0    unreachable=0    failed=0
oxford-salzburg            : ok=43   changed=13   unreachable=0    failed=0
splunk-oxford-fwd1         : ok=66   changed=24   unreachable=0    failed=0
splunk-oxford-head1        : ok=66   changed=23   unreachable=0    failed=0
splunk-oxford-idx1         : ok=66   changed=21   unreachable=0    failed=0
splunk-oxford-idx2         : ok=66   changed=21   unreachable=0    failed=0
splunk-oxford-idx3         : ok=66   changed=21   unreachable=0    failed=0
0*$ byobu-shell  1-$ bash  2$ bash   rocharlt@cfmint-vtumukelp313 192.168.1.195 Menu:<F9>
 u  Ubuntu 17.1      117! 1h53m 69%- 72.2Mbps74% 0.20 4x0.8GHz 7.8GB25% 2015-08-15 18:11:13
```

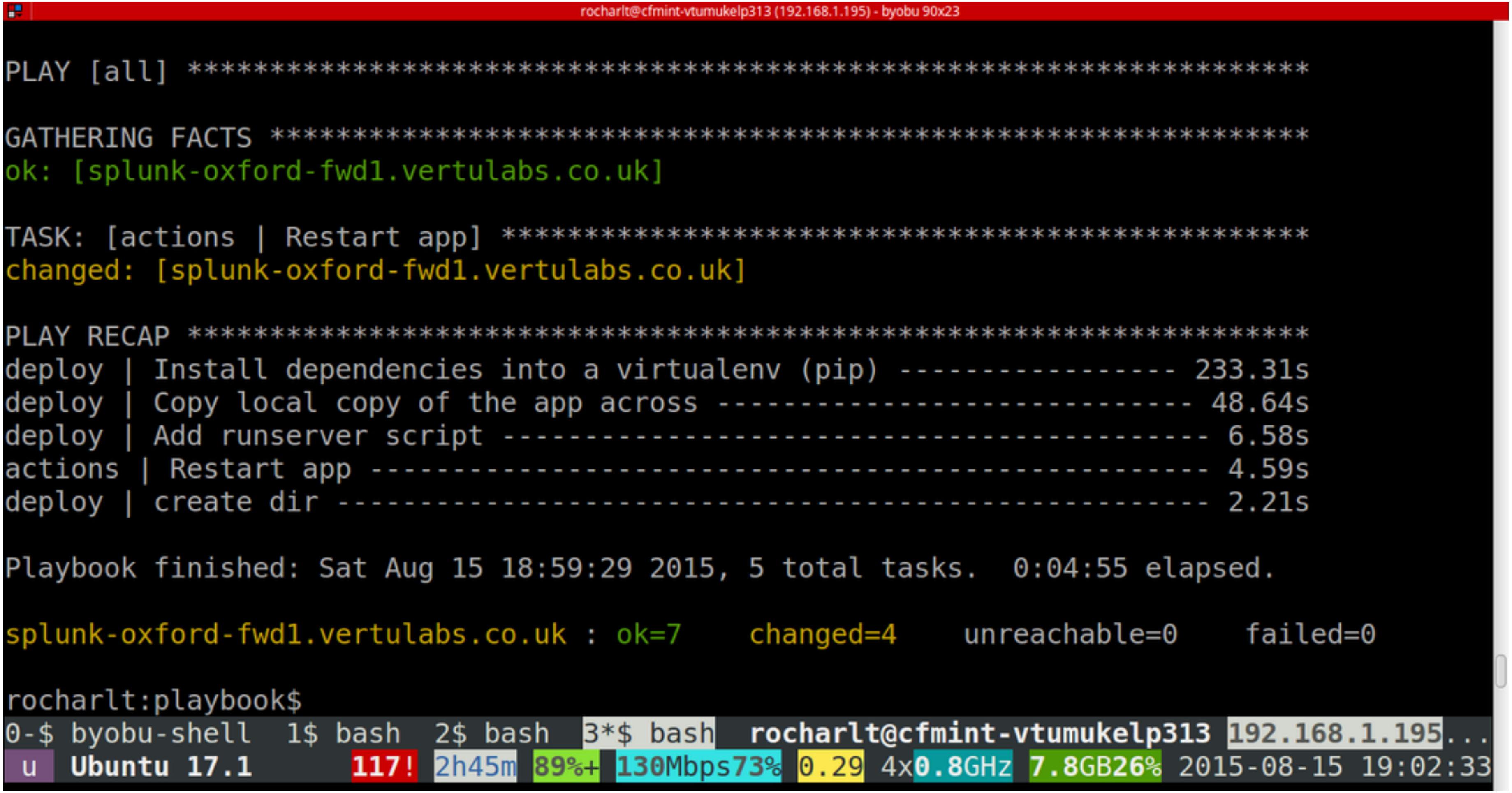


rocharlt@cfmint-vtumukelp313 (192.168.1.195) - byobu 90x23

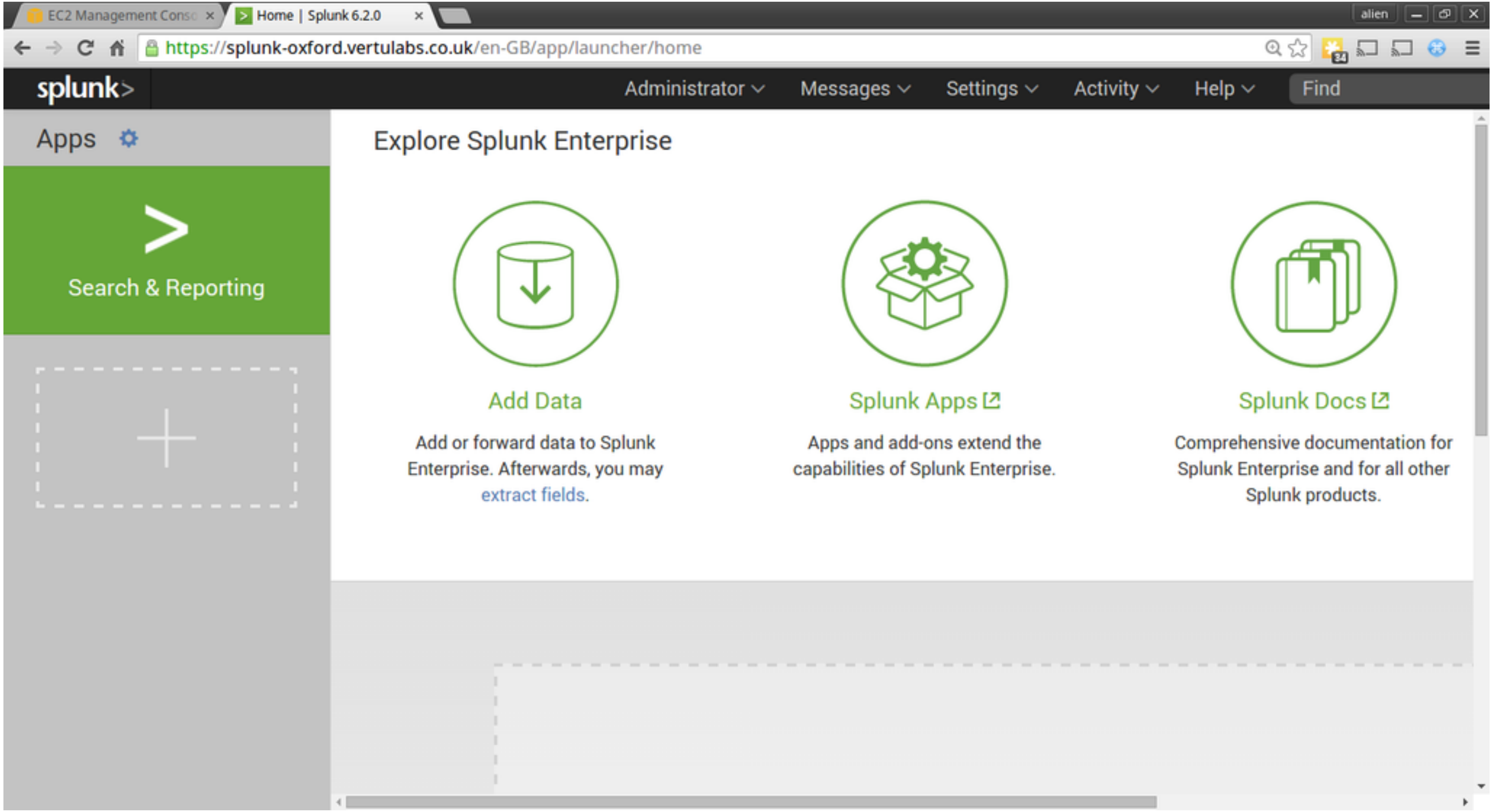
```
rocharlt:playbook$ ansible-playbook  -i hosts -l oxford -t "deploy" site.yml --skip-tags "
remote"

PLAY [all] *********************************************************************

GATHERING FACTS ****************************************************************
ok: [splunk-oxford-fwd1.vertulabs.co.uk]

TASK: [deploy | create dir] ****************************************************
ok: [splunk-oxford-fwd1.vertulabs.co.uk]

TASK: [deploy | Install dependencies into a virtualenv (pip)] *****************
changed: [splunk-oxford-fwd1.vertulabs.co.uk] => (item=https://splunk:[redacted]@release.ve
rtulabs.co.uk/python/puka-0.0.4vertu.tar.gz)
changed: [splunk-oxford-fwd1.vertulabs.co.uk] => (item=https://splunk:[redacted]@release.ve
rtulabs.co.uk/python/simplebson-0.3.3.tar.gz)
changed: [splunk-oxford-fwd1.vertulabs.co.uk] => (item=https://splunk:[redacted]@release.ve
rtulabs.co.uk/python/gevent-1.0b4.tar.gz)
changed: [splunk-oxford-fwd1.vertulabs.co.uk] => (item=https://splunk:[redacted]@release.ve
rtulabs.co.uk/python/nucleon-0.0.2.tar.gz)
changed: [splunk-oxford-fwd1.vertulabs.co.uk] => (item=https://splunk:[redacted]@release.ve
0-$ byobu-shell  1$ bash  2$ bash  3*$ bash  rocharlt@cfmint-vtumukelp313 192.168.1.195...
 u  Ubuntu 17.1      117! 2h44m 88%+ 72.2Mbps73% 0.03 4x0.8GHz 7.8GB26% 2015-08-15 19:02:12
```

.conf2015

splunk>



```
PLAY [all] **********************************************************************

GATHERING FACTS *****************************************************************
ok: [splunk-oxford-fwd1.vertulabs.co.uk]

TASK: [actions | Restart app] ***************************************************
changed: [splunk-oxford-fwd1.vertulabs.co.uk]

PLAY RECAP **********************************************************************
deploy | Install dependencies into a virtualenv (pip) ----------------- 233.31s
deploy | Copy local copy of the app across --------------------------- 48.64s
deploy | Add runserver script ---------------------------------------- 6.58s
actions | Restart app ----------------------------------------------- 4.59s
deploy | create dir ------------------------------------------------- 2.21s

Playbook finished: Sat Aug 15 18:59:29 2015, 5 total tasks.  0:04:55 elapsed.

splunk-oxford-fwd1.vertulabs.co.uk : ok=7    changed=4    unreachable=0    failed=0

rocharlt:playbook$
0-$ byobu-shell  1$ bash  2$ bash  3*$ bash  rocharlt@cfmint-vtumukelp313 192.168.1.195...
 u  Ubuntu 17.1       117! 2h45m 89%+ 130Mbps73% 0.29 4x0.8GHz 7.8GB26% 2015-08-15 19:02:33
```



Explore Splunk Enterprise

Add Data

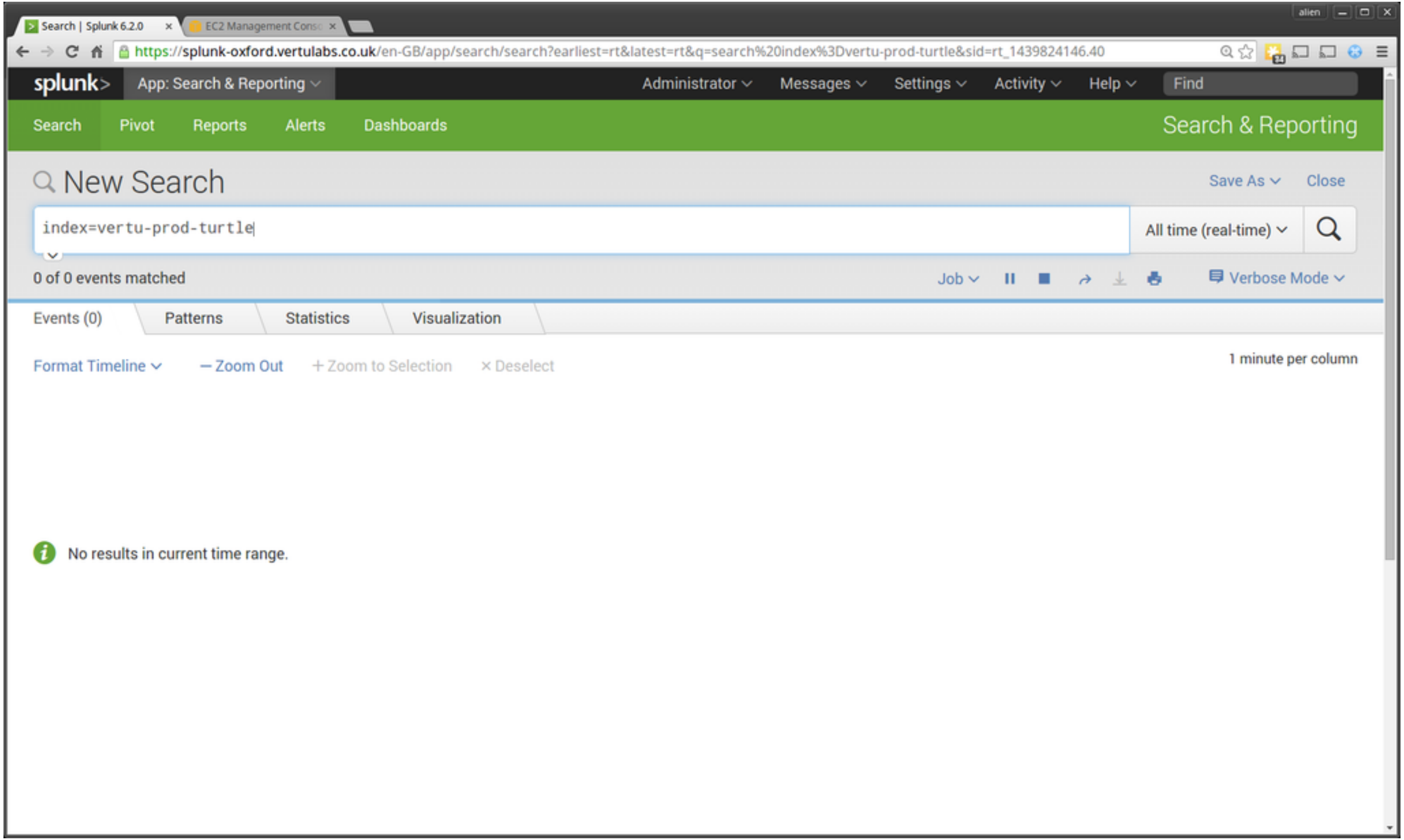
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

Splunk Apps

Apps and add-ons extend the capabilities of Splunk Enterprise.

Splunk Docs

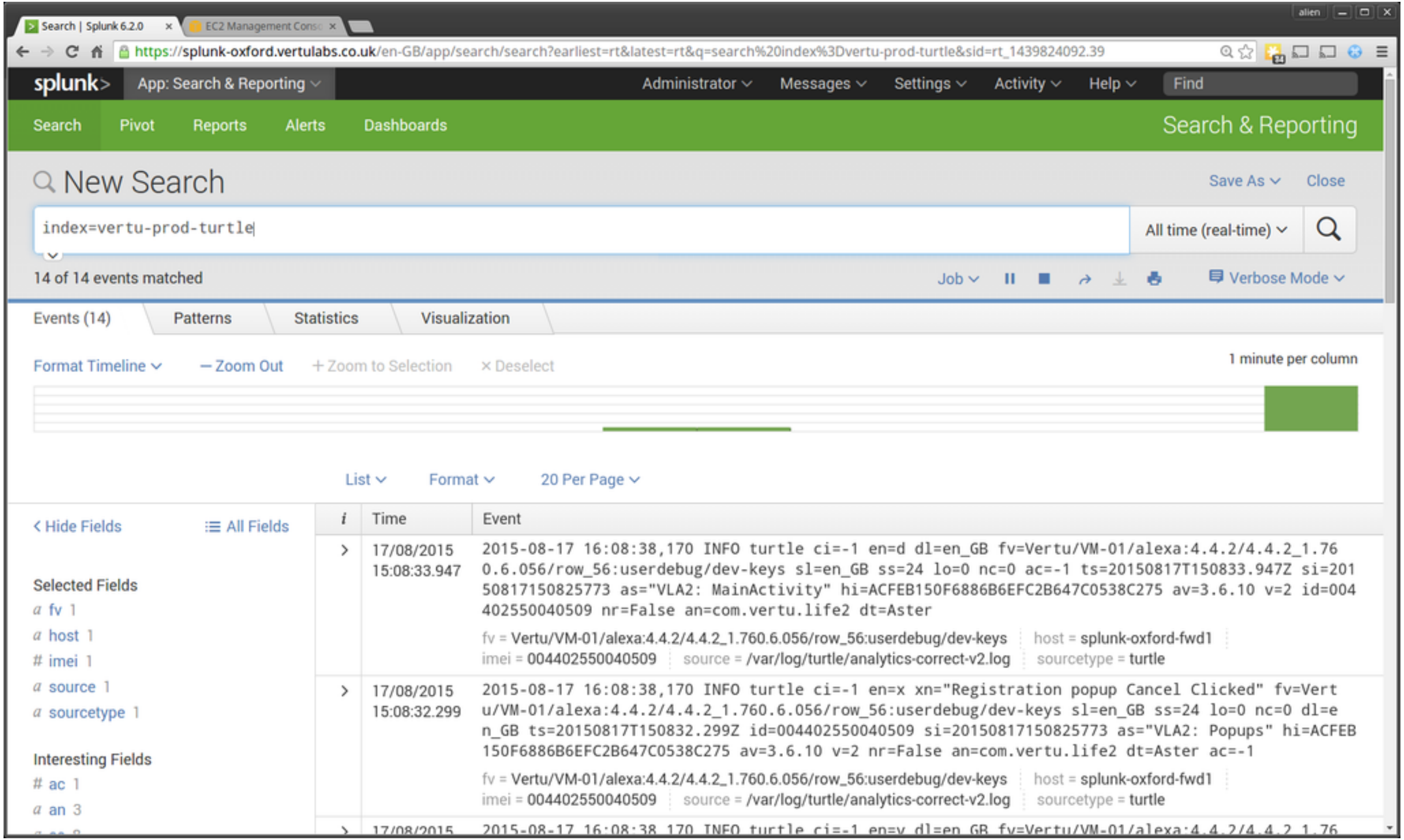
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.



```
index=vertu-prod-turtle
```

0 of 0 events matched

No results in current time range.



```
index=vertu-prod-turtle
```

14 of 14 events matched

Selected Fields

- a fv 1
- a host 1
- # imei 1
- a source 1
- a sourcetype 1

Interesting Fields

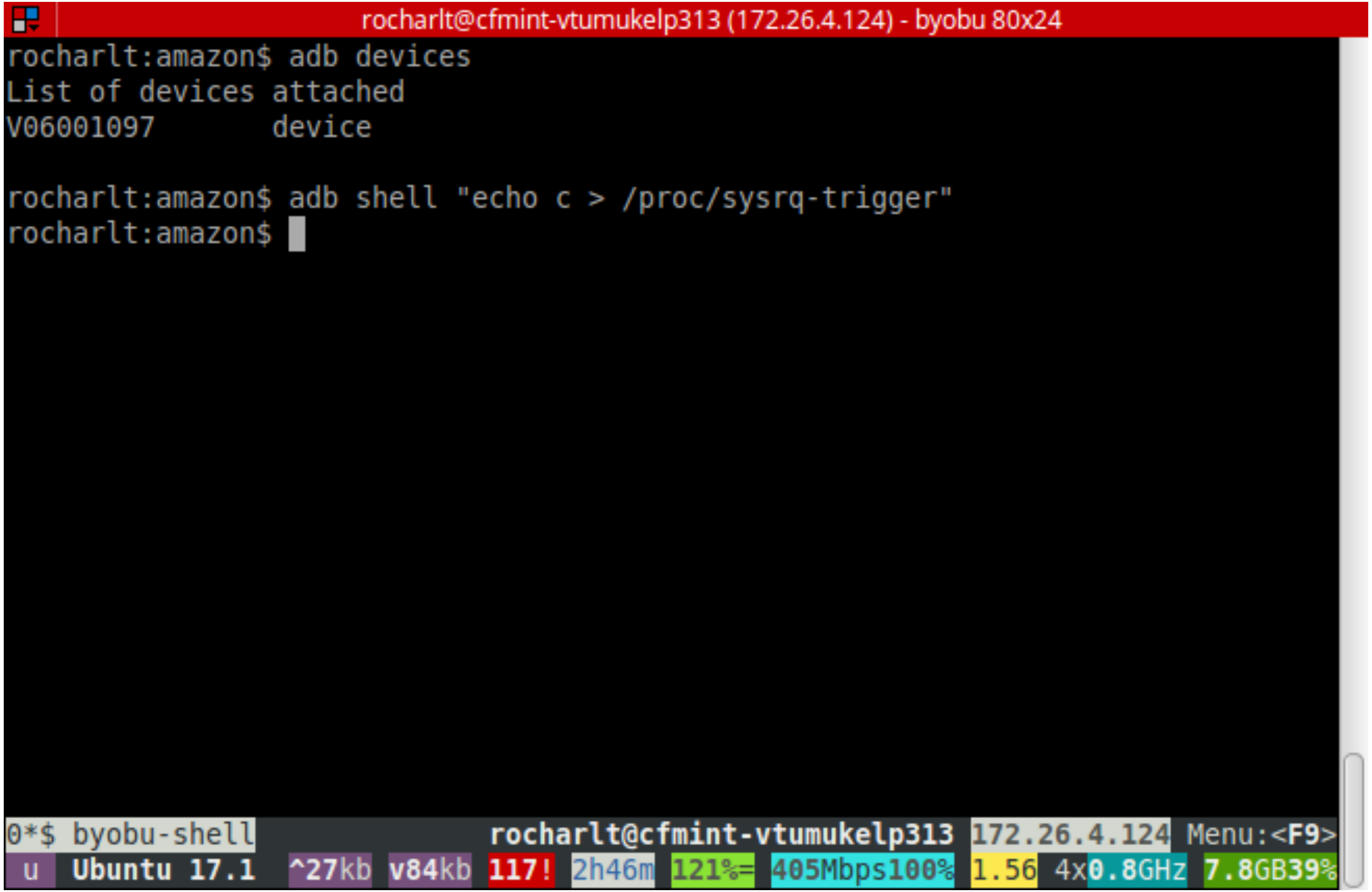
- # ac 1
- a an 3

Time	Event

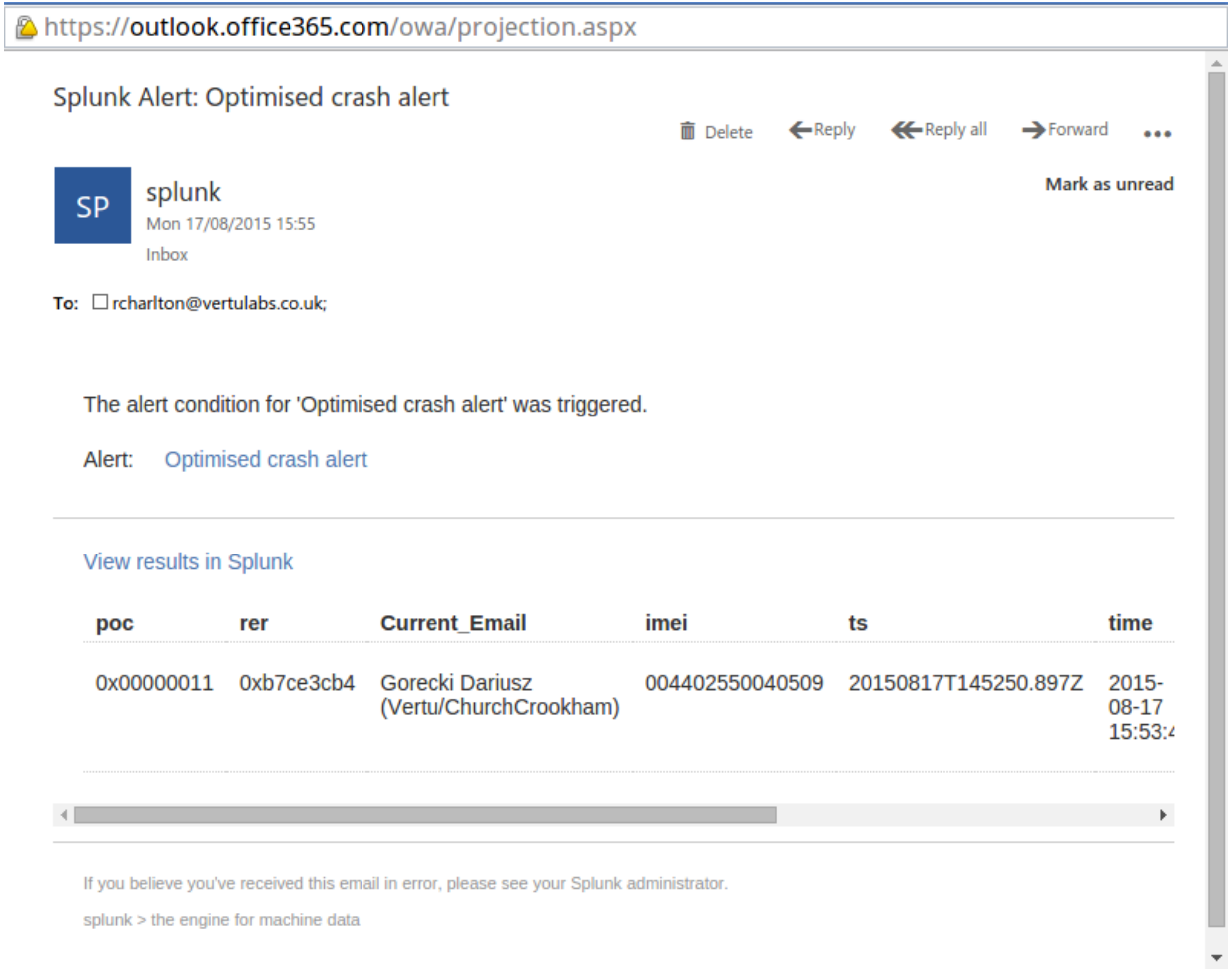
17/08/2015
15:08:33.947
	2015-08-17 16:08:38,170 INFO turtle ci=-1 en=d dl=en_GB fv=Vertu/VM-01/alexa:4.4.2/4.4.2_1.760.6.056/row_56:userdebug/dev-keys sl=en_GB ss=24 lo=0 nc=0 ac=-1 ts=20150817T150833.947Z si=20150817150825773 as="VLA2: MainActivity" hi=ACFEB150F6886B6EFC2B647C0538C275 av=3.6.10 v=2 id=004402550040509 nr=False an=com.vertu.life2 dt=Aster
	fv = Vertu/VM-01/alexa:4.4.2/4.4.2_1.760.6.056/row_56:userdebug/dev-keys host = splunk-oxford-fwd1
	imei = 004402550040509 source = /var/log/turtle/analytics-correct-v2.log sourcetype = turtle

17/08/2015
15:08:32.299
	2015-08-17 16:08:38,170 INFO turtle ci=-1 en=x xn="Registration popup Cancel Clicked" fv=Vertu/VM-01/alexa:4.4.2/4.4.2_1.760.6.056/row_56:userdebug/dev-keys sl=en_GB ss=24 lo=0 nc=0 dl=en_GB ts=20150817T150832.299Z id=004402550040509 si=20150817150825773 as="VLA2: Popups" hi=ACFEB150F6886B6EFC2B647C0538C275 av=3.6.10 v=2 nr=False an=com.vertu.life2 dt=Aster ac=-1
	fv = Vertu/VM-01/alexa:4.4.2/4.4.2_1.760.6.056/row_56:userdebug/dev-keys host = splunk-oxford-fwd1
	imei = 004402550040509 source = /var/log/turtle/analytics-correct-v2.log sourcetype = turtle

17/08/2015	2015-08-17 16:08:38,170 INFO turtle ci=-1 en=v dl=en_GB fv=Vertu/VM-01/alexa:4.4.2/4.4.2_1.76



```
rocharlt:amazon$ adb devices
List of devices attached
V06001097       device

rocharlt:amazon$ adb shell "echo c > /proc/sysrq-trigger"
rocharlt:amazon$
```



Splunk Alert: Optimised crash alert

splunk
Mon 17/08/2015 15:55
Inbox

To: □ rcharlton@vertulabs.co.uk;

The alert condition for 'Optimised crash alert' was triggered.

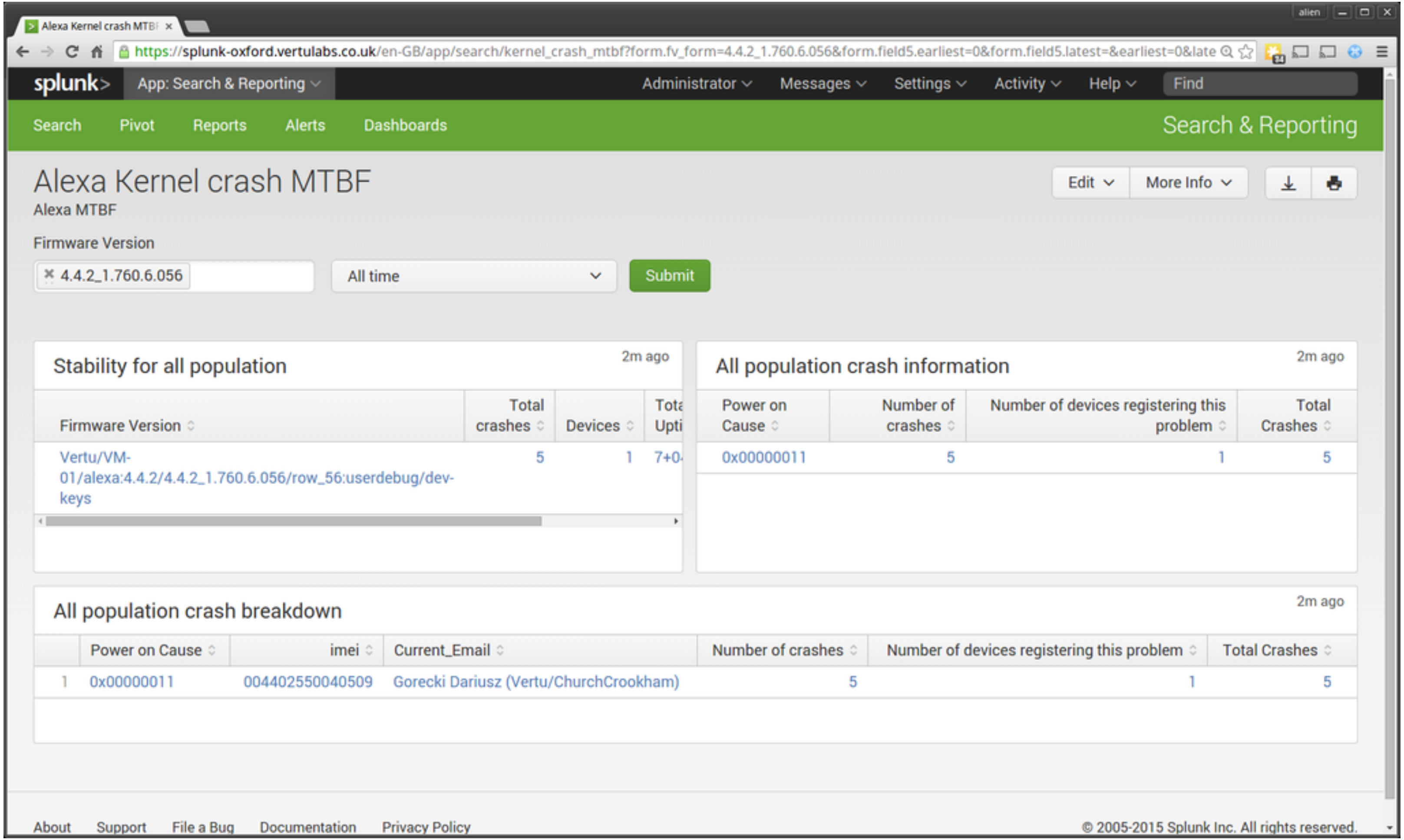
Alert: Optimised crash alert

View results in Splunk

poc	rer	Current_Email	imei	ts	time
0x00000011	0xb7ce3cb4	Gorecki Dariusz (Vertu/ChurchCrookham)	004402550040509	20150817T145250.897Z	2015-08-17 15:53:4

If you believe you've received this email in error, please see your Splunk administrator.

splunk > the engine for machine data



Alexa Kernel crash MTBF

Alexa MTBF

Firmware Version: 4.4.2_1.760.6.056 | All time | Submit

Stability for all population

2m ago

Firmware Version	Total crashes	Devices	Tota Upti
Vertu/VM-01/alexa:4.4.2/4.4.2_1.760.6.056/row_56:userdebug/dev-keys	5	1	7+0

All population crash information

2m ago

Power on Cause	Number of crashes	Number of devices registering this problem	Total Crashes
0x00000011	5	1	5

All population crash breakdown

2m ago

	Power on Cause	imei	Current_Email	Number of crashes	Number of devices registering this problem	Total Crashes
1	0x00000011	004402550040509	Gorecki Dariusz (Vertu/ChurchCrookham)	5	1	5

.conf2015

THANK YOU

splunk>