KubeCon | CloudNativeCon

North America 2017

Deploying Kubernetes

without scaring away your security team

Paul Czarkowski, Pivotal Software *(@pczarkowsi)*
Major Hayden, Rackspace *(@majorhayden)*

Deploying Kubernetes
Without Scaring Away Your Security Team

Principal Technologist @ Pivotal

Always doing things and promoting agile synergistic principles that resonate down the value chain

Principal Architect @ Rackspace

Secures OpenStack/Kubernetes clouds and owns far too many domain names *(including icanhazip.com)*

Photo credit: Pixabay

Photo credit: Pixabay

Your first day back at the office talking about Kubernetes feels like this

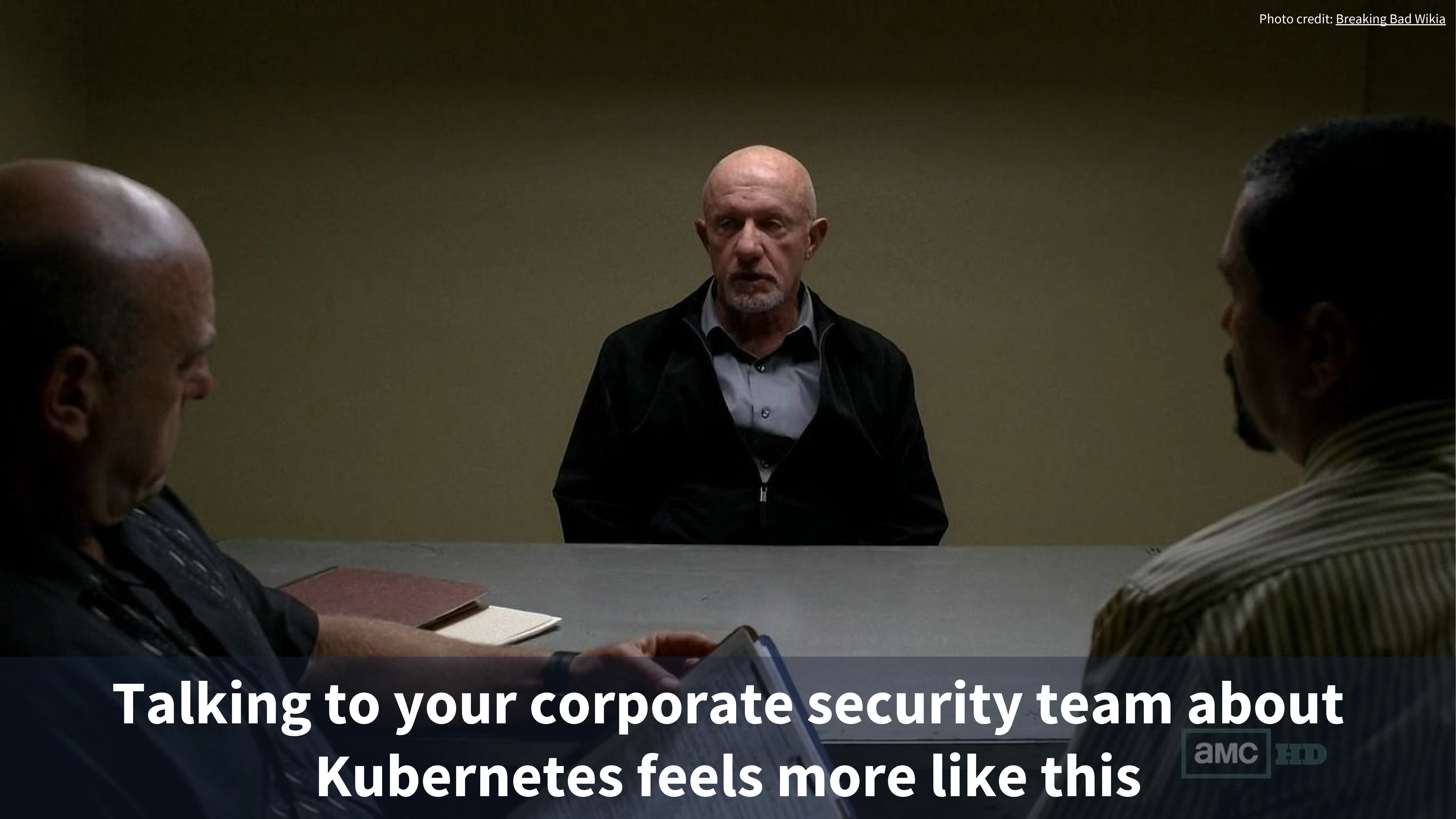


Photo credit: Breaking Bad Wikia

Talking to your corporate security team about Kubernetes feels more like this

Deploying Kubernetes
Without Scaring Away Your Security Team

Enterprise security teams **demand** security layers that are:

- Valuable
- Non-disruptive
- Documented
- Auditable
- Easily understood

Deploying Kubernetes Without Scaring Away Your Security Team

Find a way to get here

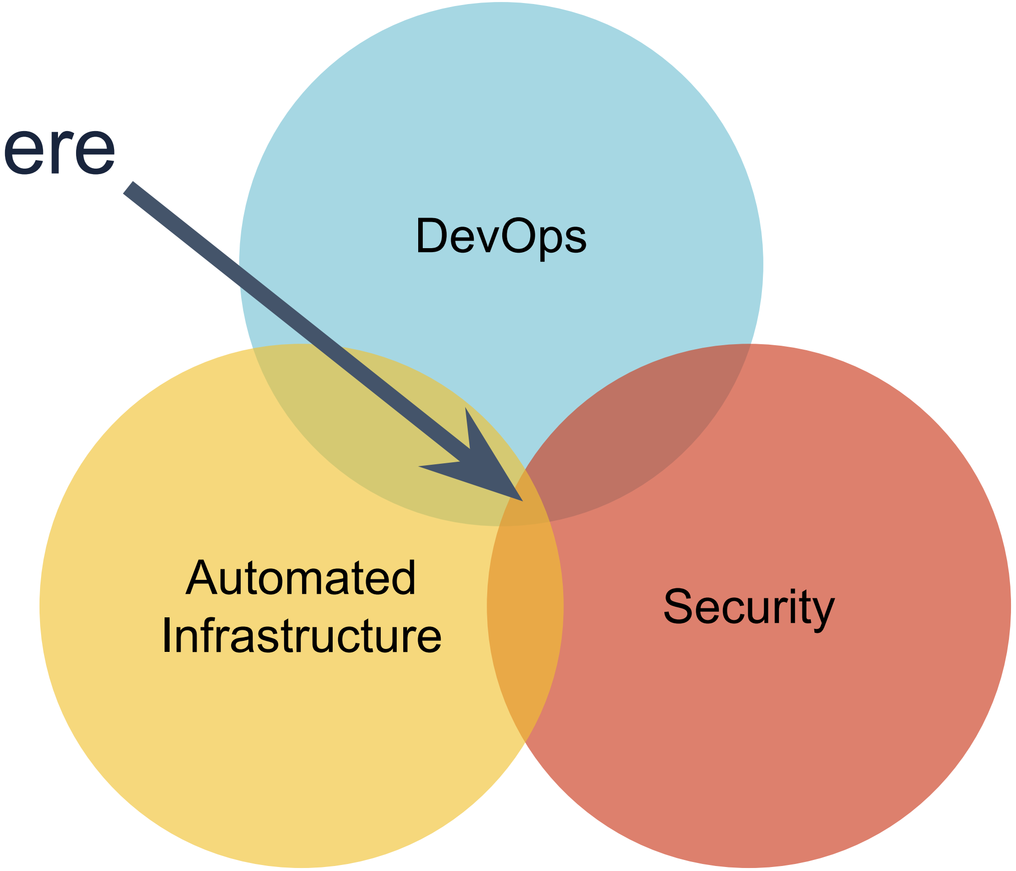


Photo credit: Wikipedia

Security requirements and restrictions should be guardrails, not roadblocks

PUBLIC SERVICE ANNOUNCEMENT:

Always enable Linux Security Modules in your container deployments.

(like SELinux or AppArmor)

SERIOUSLY.
STOP DISABLING SELINUX.

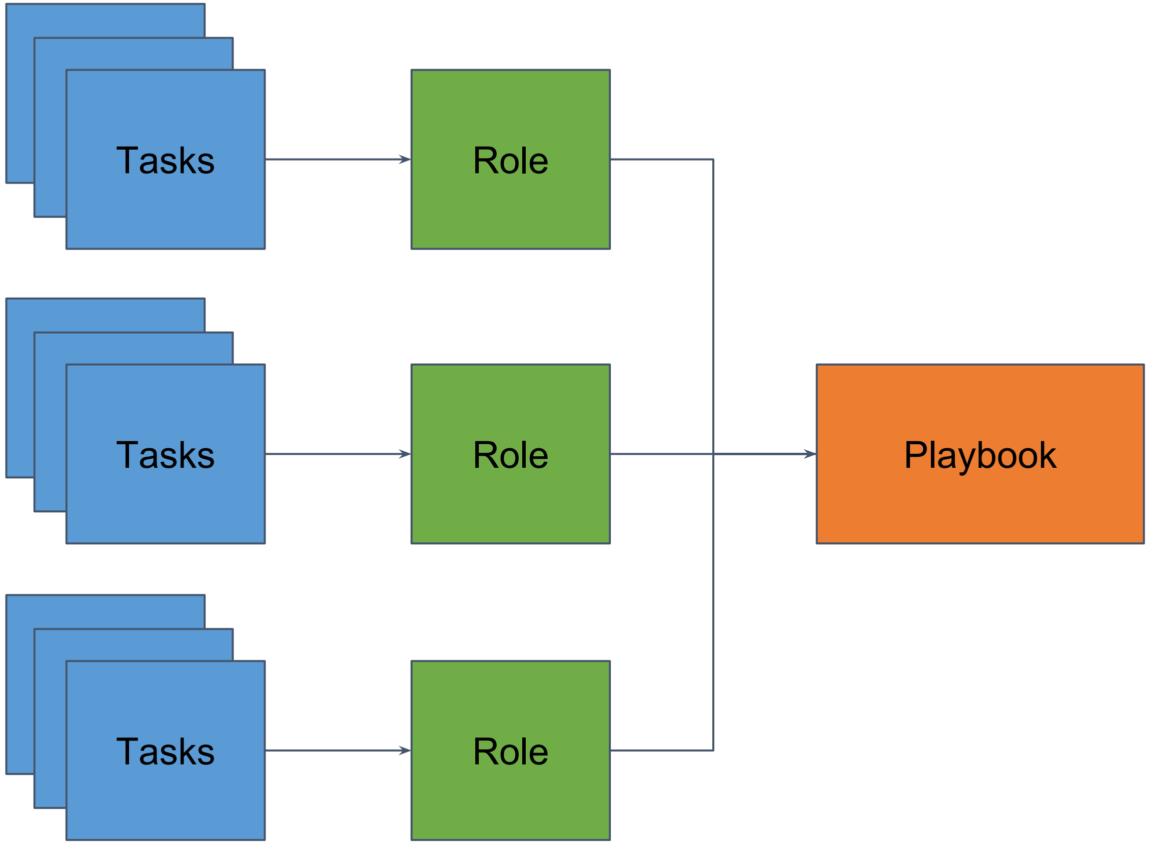
Luckily, there are tools that help with many of these challenges.

Deploying Kubernetes Without Scaring Away Your Security Team

https://www.ansible.com/

- Orchestration
- Configuration management
- Software deployment
- Stackable building blocks
- Everything as code

Deploying Kubernetes
Without Scaring Away Your Security Team



Ansible explained in three bullets:

- Each task does one thing
- Tasks are grouped into roles
- Playbooks apply one or more roles to one or more servers

Deploying Kubernetes Without Scaring Away Your Security Team

Ansible is **simple**

- Tasks are read one at a time, top-down
- Tasks are written in YAML
- No need for dependency chaining or complex ordering
- Simple inventory system

Deploying Kubernetes Without Scaring Away Your Security Team

Ansible is **versatile**

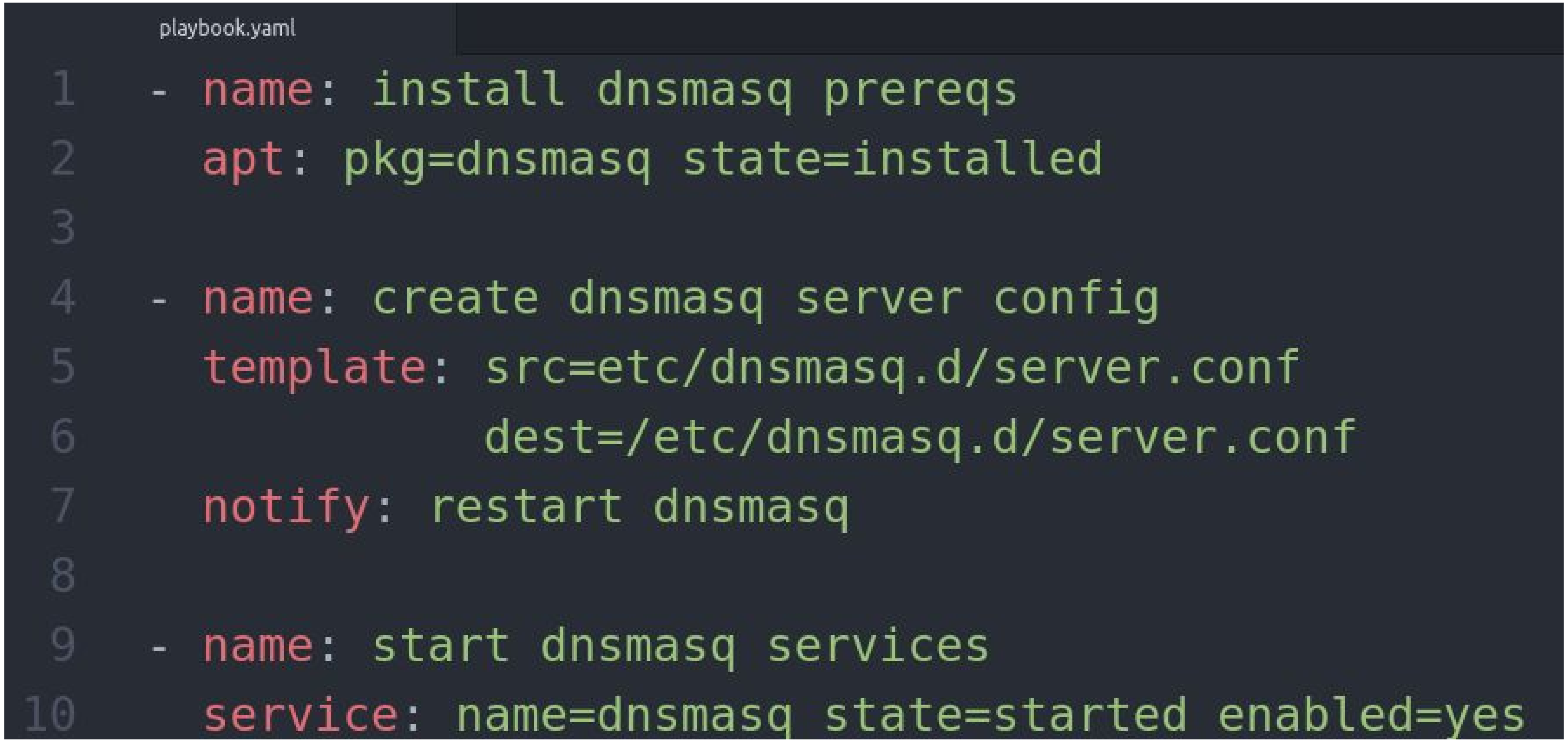
- Automates containers, virtual machines, servers, network devices, clouds, laptops
- No daemons or complex dependencies
- Got Python installed on your nodes? You’re ready.

Deploying Kubernetes Without Scaring Away Your Security Team

Ansible is **repeatable**

- A playbook can be run repeatedly with the same results
- Ansible can audit a system and show potential changes before making them

Ansible playbook

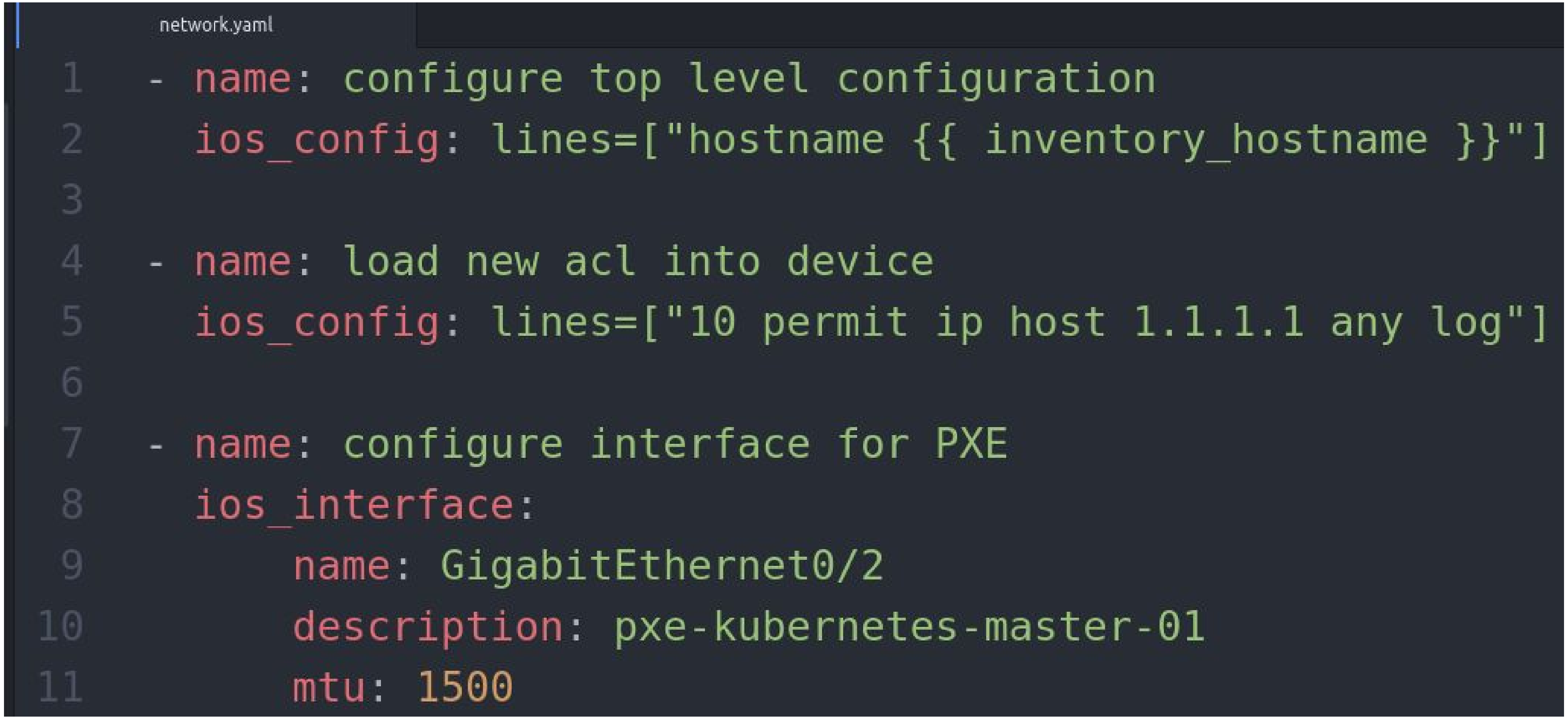


```yaml
- name: install dnsmasq prereqs
  apt: pkg=dnsmasq state=installed

- name: create dnsmasq server config
  template: src=etc/dnsmasq.d/server.conf
            dest=/etc/dnsmasq.d/server.conf
  notify: restart dnsmasq

- name: start dnsmasq services
  service: name=dnsmasq state=started enabled=yes
```

Networking as code

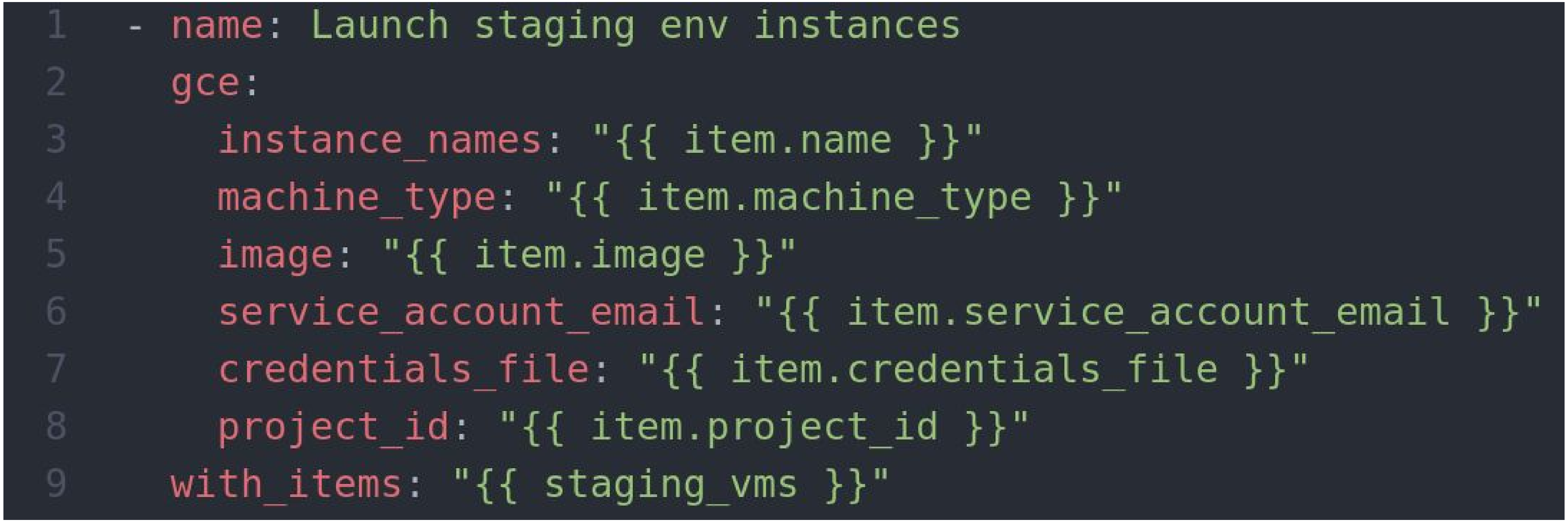


```yaml
- name: configure top level configuration
  ios_config: lines=["hostname {{ inventory_hostname }}"]

- name: load new acl into device
  ios_config: lines=["10 permit ip host 1.1.1.1 any log"]

- name: configure interface for PXE
  ios_interface:
      name: GigabitEthernet0/2
      description: pxe-kubernetes-master-01
      mtu: 1500
```

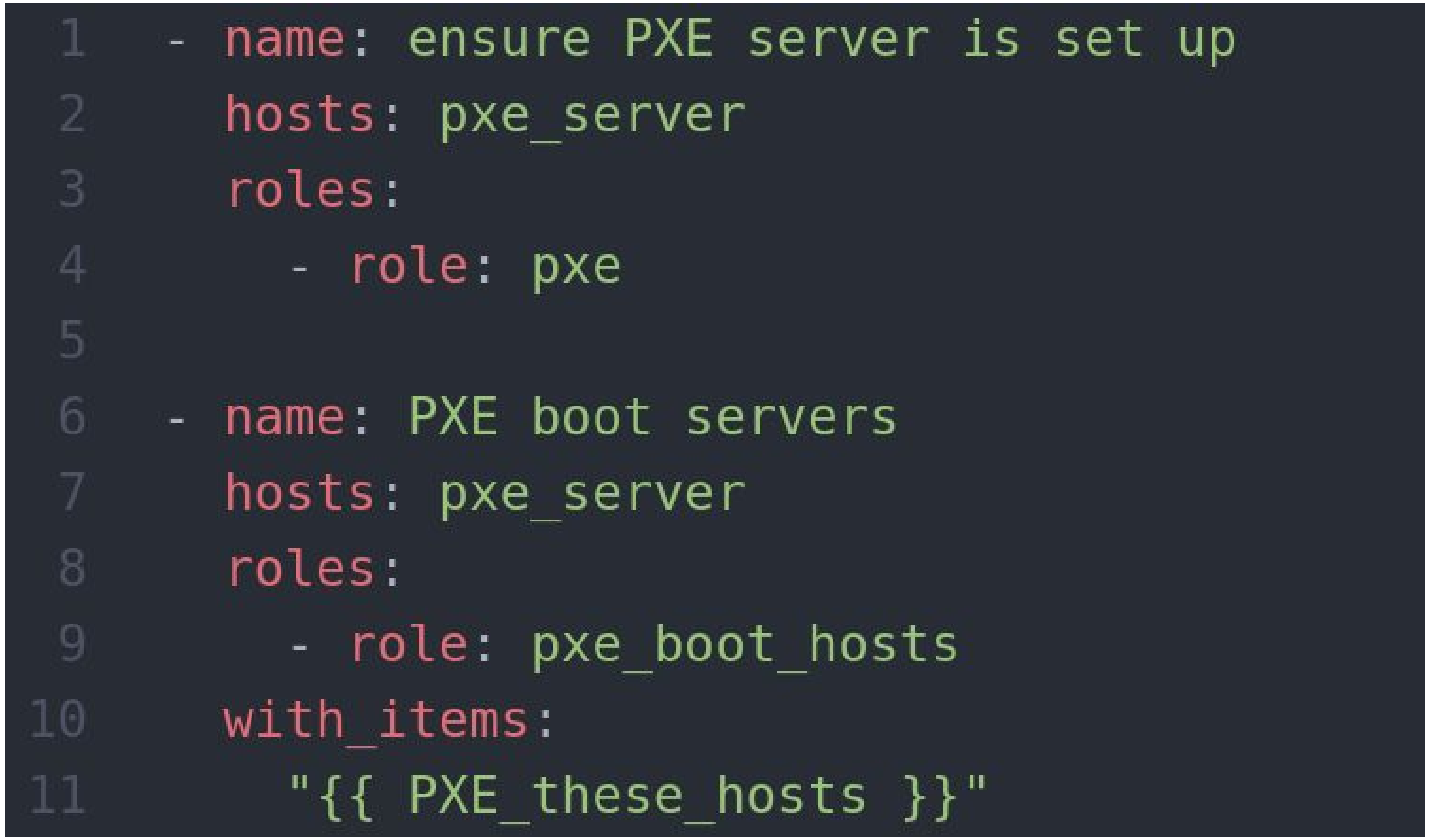
Infrastructure as code



```
- name: Launch staging env instances
  gce:
    instance_names: "{{ item.name }}"
    machine_type: "{{ item.machine_type }}"
    image: "{{ item.image }}"
    service_account_email: "{{ item.service_account_email }}"
    credentials_file: "{{ item.credentials_file }}"
    project_id: "{{ item.project_id }}"
  with_items: "{{ staging_vms }}"
```

Deploying Kubernetes
Without Scaring Away Your Security Team

Infrastructure as Code



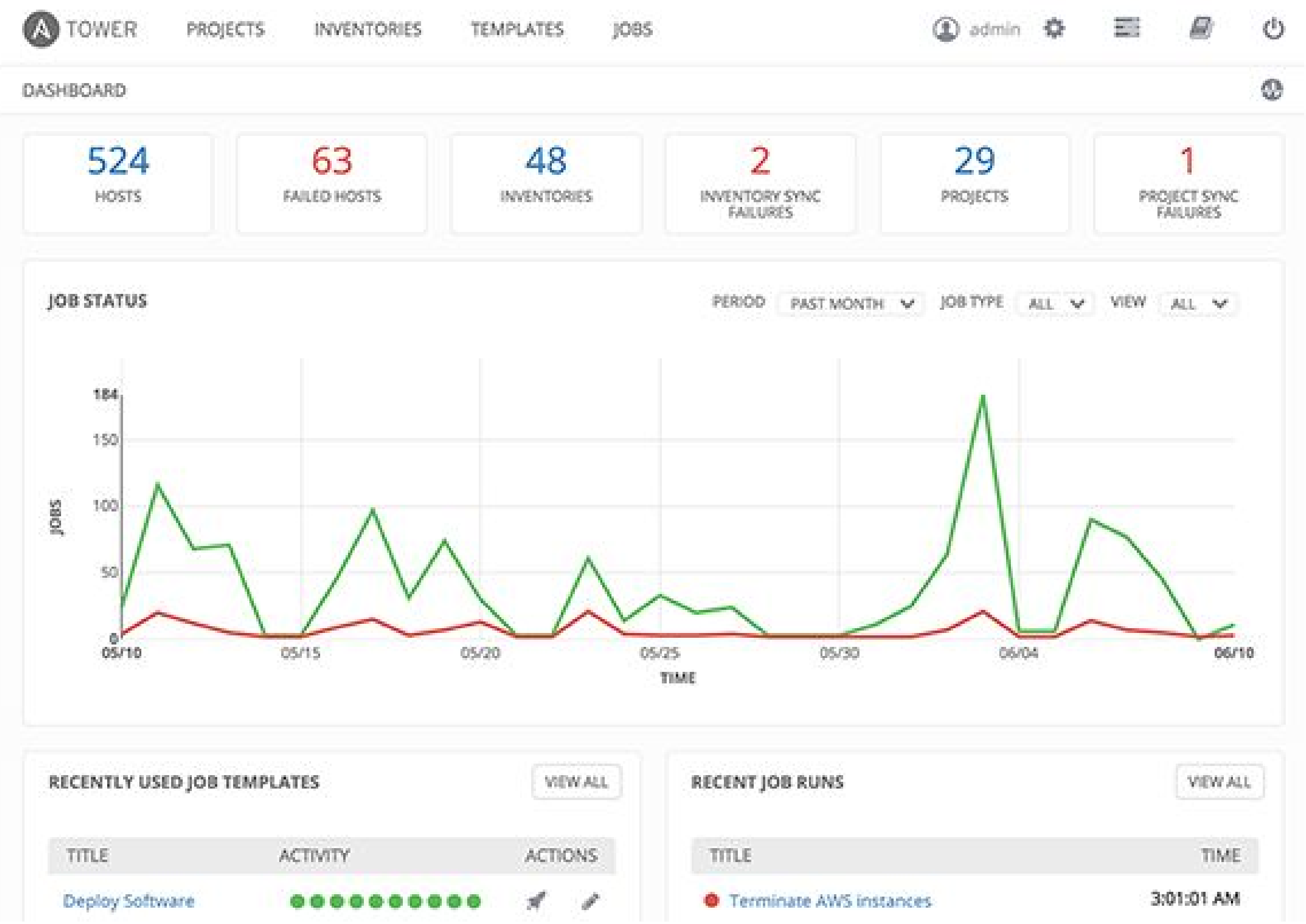
```yaml
- name: ensure PXE server is set up
  hosts: pxe_server
  roles:
    - role: pxe

- name: PXE boot servers
  hosts: pxe_server
  roles:
    - role: pxe_boot_hosts
  with_items:
    "{{ PXE_these_hosts }}"
```

Deploying Kubernetes
Without Scaring Away Your Security Team

Ansible Tower

- Adds reporting/accountability
- Dashboards
- Scheduled Jobs
- Multi-Playbook Workflows



524 HOSTS

63 FAILED HOSTS

48 INVENTORIES

2 INVENTORY SYNC FAILURES

29 PROJECTS

1 PROJECT SYNC FAILURES

JOB STATUS

PERIOD: PAST MONTH
JOB TYPE: ALL
VIEW: ALL

RECENTLY USED JOB TEMPLATES

TITLE	ACTIVITY	ACTIONS
Deploy Software	●●●●●●●●●●	

RECENT JOB RUNS

TITLE	TIME
● Terminate AWS instances	3:01:01 AM

ansible hardening

https://github.com/openstack/ansible-hardening

- Applies and audits over 180 controls from the STIG* in a few minutes.
- Supports CentOS/RHEL 7, Debian, Fedora, OpenSUSE, and Ubuntu 16.04.
- Fully open source and looking for new contributors/testers

* *The Security Technical Implementation Guide (STIG) is a set of hardening configurations for various systems published by the US Department of Defense.*

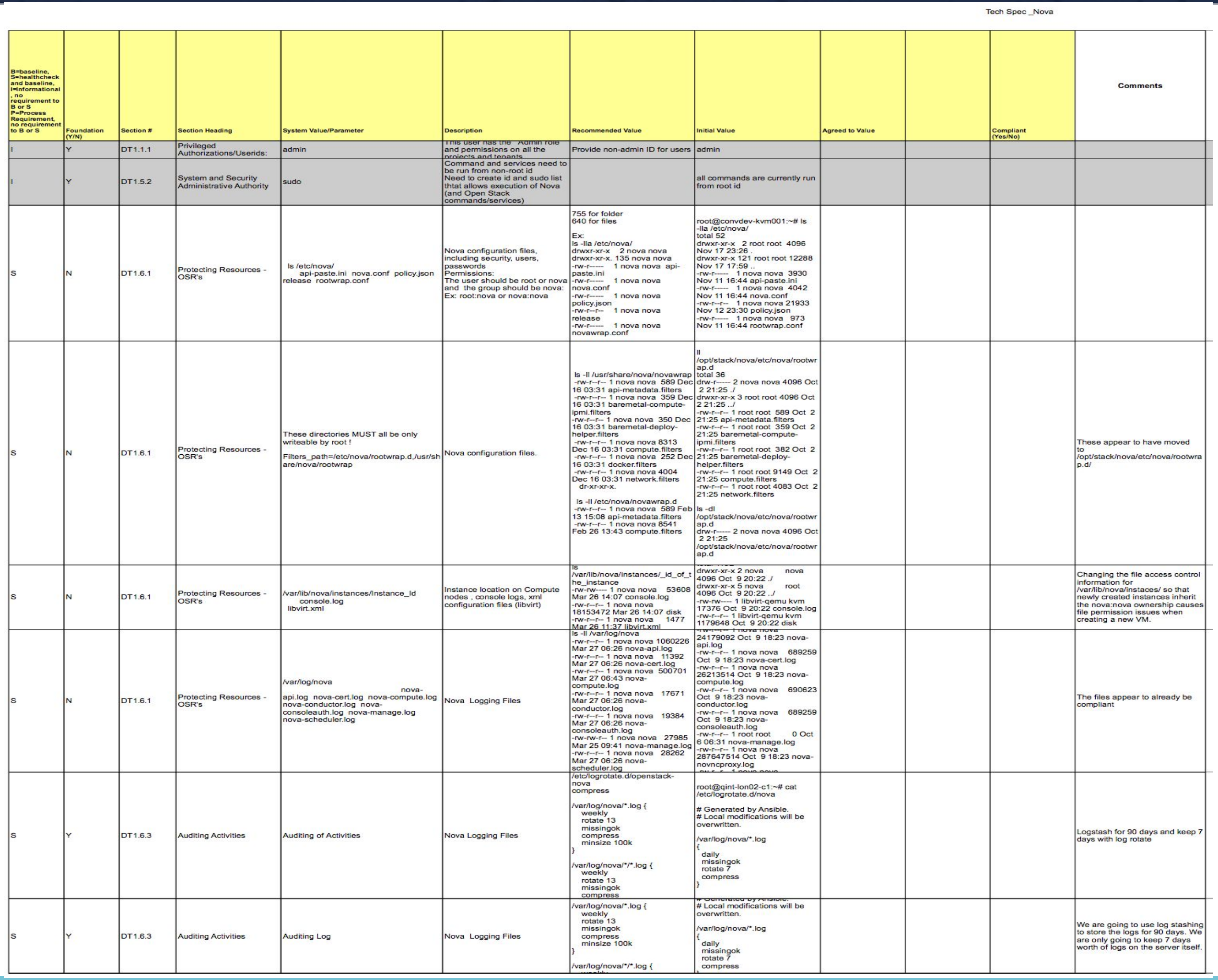
Deploying Kubernetes
Without Scaring Away Your Security Team

INSPEC

https://www.inspec.io

- Compliance as Code
- Ruby DSL for testing desired state
- Ansible to install Inspec
- Ansible to deploy Inspec Rules
- Sensu Check / Pagerduty Alert
- Inspec logs to ELK for Audit

Deploying Kubernetes Without Scaring Away Your Security Team



Tech Spec _Nova

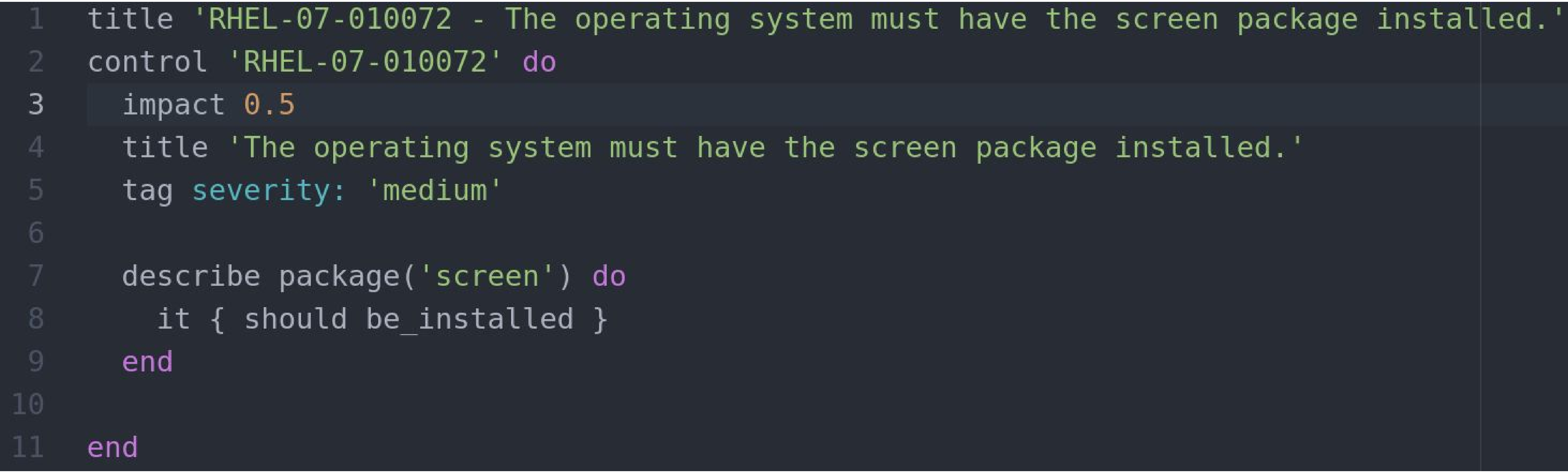
B=baseline, S=healthcheck and baseline, I=Informational, no requirement to B or S P=Process Requirement, no requirement to B or S	Foundation (Y/N)	Section #	Section Heading	System Value/Parameter	Description	Recommended Value	Initial Value	Agreed to Value		Compliant (Yes/No)	Comments
I	Y	DT1.1.1	Privileged Authorizations/Userids:	admin	This user has the "Admin role and permissions on all the projects and tenants	Provide non-admin ID for users	admin				
I	Y	DT1.5.2	System and Security Administrative Authority	sudo	Command and services need to be run from non-root id Need to create id and sudo list thtat allows execution of Nova (and Open Stack commands/services)		all commands are currently run from root id				
S	N	DT1.6.1	Protecting Resources - OSR's	ls /etc/nova/ api-paste.ini nova.conf policy.json release rootwrap.conf	Nova configuration files, including security, users, passwords Permissions: The user should be root or nova and the group should be nova: Ex: root:nova or nova:nova	755 for folder 640 for files Ex: ls -lla /etc/nova/ drwxr-xr-x 2 nova nova drwxr-xr-x. 135 nova nova -rw-r----- 1 nova nova api-paste.ini -rw-r----- 1 nova nova nova.conf -rw-r----- 1 nova nova policy.json -rw-r--r-- 1 nova nova release -rw-r----- 1 nova nova novawrap.conf	root@convdev-kvm001:~# ls -lla /etc/nova/ total 52 drwxr-xr-x 2 root root 4096 Nov 17 23:26 . drwxr-xr-x 121 root root 12288 Nov 17 17:59 .. -rw-r----- 1 nova nova 3930 Nov 11 16:44 api-paste.ini -rw-r----- 1 nova nova 4042 Nov 11 16:44 nova.conf -rw-r--r-- 1 nova nova 21933 Nov 12 23:30 policy.json -rw-r----- 1 nova nova 973 Nov 11 16:44 rootwrap.conf				
S	N	DT1.6.1	Protecting Resources - OSR's	These directories MUST all be only writeable by root ! Filters_path=/etc/nova/rootwrap.d,/usr/share/nova/rootwrap	Nova configuration files.	ls -ll /usr/share/nova/novawrap -rw-r--r-- 1 nova nova 589 Dec 16 03:31 api-metadata.filters -rw-r--r-- 1 nova nova 359 Dec 16 03:31 baremetal-compute-ipmi.filters -rw-r--r-- 1 nova nova 350 Dec 16 03:31 baremetal-deploy-helper.filters -rw-r--r-- 1 nova nova 8313 Dec 16 03:31 compute.filters -rw-r--r-- 1 nova nova 252 Dec 16 03:31 docker.filters -rw-r--r-- 1 nova nova 4004 Dec 16 03:31 network.filters dr-xr-xr-x. ls -ll /etc/nova/novawrap.d -rw-r--r-- 1 nova nova 589 Feb 13 15:08 api-metadata.filters -rw-r--r-- 1 nova nova 8541 Feb 26 13:43 compute.filters	ll /opt/stack/nova/etc/nova/rootwrap.d total 36 drw-r----- 2 nova nova 4096 Oct 2 21:25 ./ drwxr-xr-x 3 root root 4096 Oct 2 21:25 ../ -rw-r--r-- 1 root root 589 Oct 2 21:25 api-metadata.filters -rw-r--r-- 1 root root 359 Oct 2 21:25 baremetal-compute-ipmi.filters -rw-r--r-- 1 root root 382 Oct 2 21:25 baremetal-deploy-helper.filters -rw-r--r-- 1 root root 9149 Oct 2 21:25 compute.filters -rw-r--r-- 1 root root 4083 Oct 2 21:25 network.filters ls -dl /opt/stack/nova/etc/nova/rootwrap.d drw-r----- 2 nova nova 4096 Oct 2 21:25 /opt/stack/nova/etc/nova/rootwrap.d				These appear to have moved to /opt/stack/nova/etc/nova/rootwrap.d/
S	N	DT1.6.1	Protecting Resources - OSR's	/var/lib/nova/instances/Instance_Id console.log libvirt.xml	Instance location on Compute nodes , console logs, xml configuration files (libvirt)	ls /var/lib/nova/instances/_id_of_the_instance -rw-rw---- 1 nova nova 53608 Mar 26 14:07 console.log -rw-r--r-- 1 nova nova 18153472 Mar 26 14:07 disk -rw-r--r-- 1 nova nova 1477 Mar 26 11:37 libvirt.xml	drwxr-xr-x 2 nova nova 4096 Oct 9 20:22 ./ drwxr-xr-x 5 nova root 4096 Oct 9 20:22 ../ -rw-rw---- 1 libvirt-qemu kvm 17376 Oct 9 20:22 console.log -rw-r--r-- 1 libvirt-qemu kvm 1179648 Oct 9 20:22 disk				Changing the file access control information for /var/lib/nova/instaces/ so that newly created instances inherit the nova:nova ownership causes file permission issues when creating a new VM.
S	N	DT1.6.1	Protecting Resources - OSR's	/var/log/nova nova-api.log nova-cert.log nova-compute.log nova-conductor.log nova-consoleauth.log nova-manage.log nova-scheduler.log	Nova Logging Files	ls -ll /var/log/nova -rw-r--r-- 1 nova nova 1060226 Mar 27 06:26 nova-api.log -rw-r--r-- 1 nova nova 11392 Mar 27 06:26 nova-cert.log -rw-r--r-- 1 nova nova 500701 Mar 27 06:43 nova-compute.log -rw-r--r-- 1 nova nova 17671 Mar 27 06:26 nova-conductor.log -rw-r--r-- 1 nova nova 19384 Mar 27 06:26 nova-consoleauth.log -rw-rw-r-- 1 nova nova 27985 Mar 25 09:41 nova-manage.log -rw-r--r-- 1 nova nova 28262 Mar 27 06:26 nova-scheduler.log	-rw-r--r-- 1 nova nova 24179092 Oct 9 18:23 nova-api.log -rw-r--r-- 1 nova nova 689259 Oct 9 18:23 nova-cert.log -rw-r--r-- 1 nova nova 26213514 Oct 9 18:23 nova-compute.log -rw-r--r-- 1 nova nova 690623 Oct 9 18:23 nova-conductor.log -rw-r--r-- 1 nova nova 689259 Oct 9 18:23 nova-consoleauth.log -rw-r--r-- 1 root root 0 Oct 6 06:31 nova-manage.log -rw-r--r-- 1 nova nova 287647514 Oct 9 18:23 nova-novncproxy.log				The files appear to already be compliant

S	Y	DT1.6.3	Auditing Activities	Auditing of Activities	Nova Logging Files	/etc/logrotate.d/openstack-nova
						compress
						
						/var/log/nova/*.log {
						weekly
						rotate 13
						missingok
						compress
						minsize 100k
						}
						
						/var/log/nova/*/*.log {
						weekly
						rotate 13
						missingok
						compress
							root@qint-lon02-c1:~# cat /etc/logrotate.d/nova
							
							# Generated by Ansible.
							# Local modifications will be overwritten.
							
							/var/log/nova/*.log
							{
							daily
							missingok
							rotate 7
							compress
							}
											Logstash for 90 days and keep 7 days with log rotate

S	Y	DT1.6.3	Auditing Activities	Auditing Log	Nova Logging Files	/var/log/nova/*.log {
						weekly
						rotate 13
						missingok
						compress
						minsize 100k
						}
						
						/var/log/nova/*/*.log {
							# Local modifications will be overwritten.
							
							/var/log/nova/*.log
							{
							daily
							missingok
							rotate 7
							compress
											We are going to use log stashing to store the logs for 90 days. We are only going to keep 7 days worth of logs on the server itself.

Example INSPEC rule

https://github.com/inspec-stigs/inspec-stig-rhel7



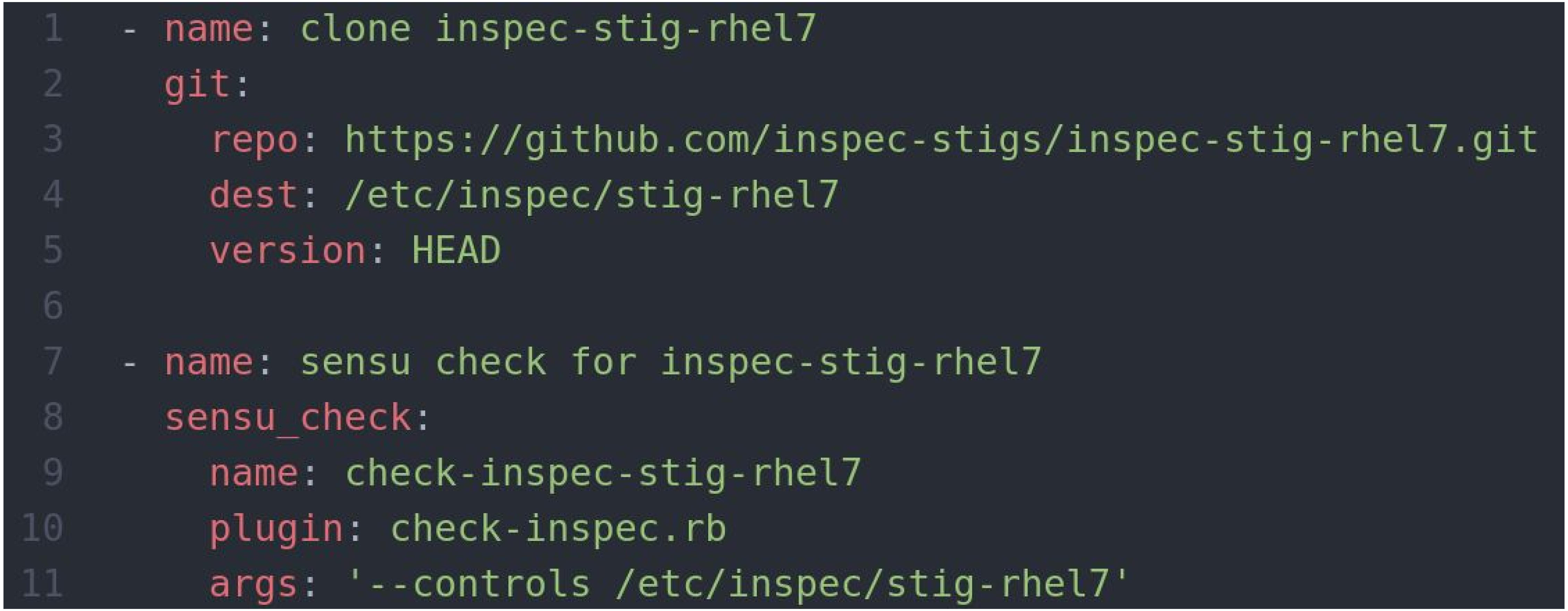
```ruby
title 'RHEL-07-010072 - The operating system must have the screen package installed.'
control 'RHEL-07-010072' do
  impact 0.5
  title 'The operating system must have the screen package installed.'
  tag severity: 'medium'

  describe package('screen') do
    it { should be_installed }
  end

end
```

Deploying Kubernetes Without Scaring Away Your Security Team

Compliance as Code



```yaml
- name: clone inspec-stig-rhel7
  git:
    repo: https://github.com/inspec-stigs/inspec-stig-rhel7.git
    dest: /etc/inspec/stig-rhel7
    version: HEAD

- name: sensu check for inspec-stig-rhel7
  sensu_check:
    name: check-inspec-stig-rhel7
    plugin: check-inspec.rb
    args: '--controls /etc/inspec/stig-rhel7'
```

Deploying Kubernetes Without Scaring Away Your Security Team

Cuttle

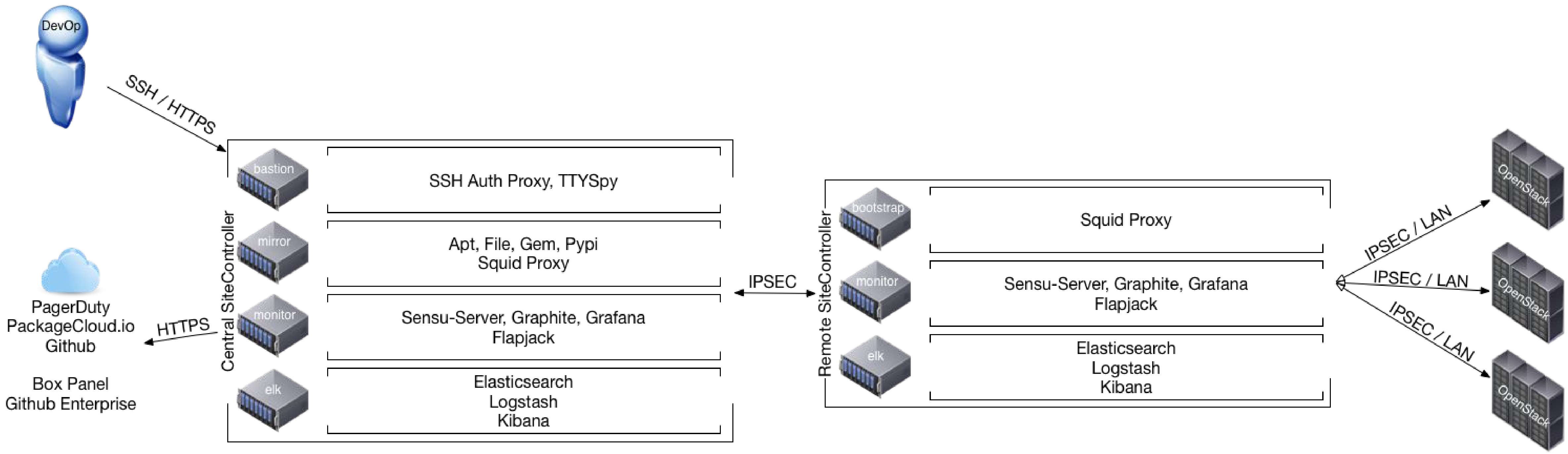
(pronounced Cuddle)

https://github.com/sitectl/cuttle

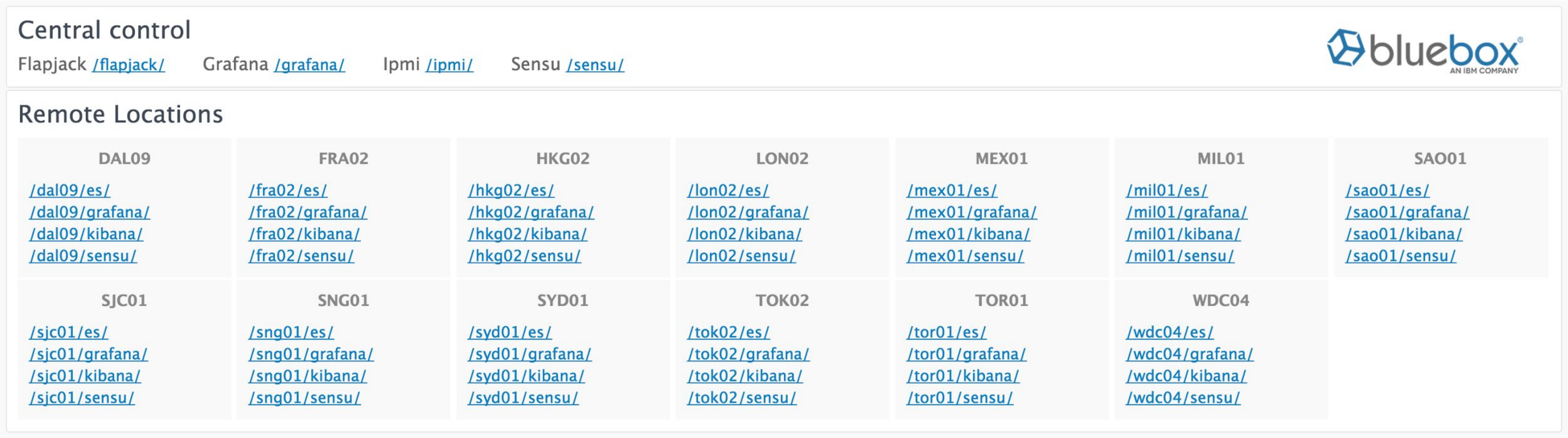
Ops Platform [as code]

- **2FA SSH Bastion**
- **OAuth Web Portal**
- Centralized Logging (ELK)
- Centralized Monitoring (Sensu)
- Builds / Tests / Jobs (Jenkins)
- Mirrors (ubuntu, pypi, rubygems)
- and a LOT MORE!

Deploying Kubernetes
Without Scaring Away Your Security Team



Deploying Kubernetes Without Scaring Away Your Security Team

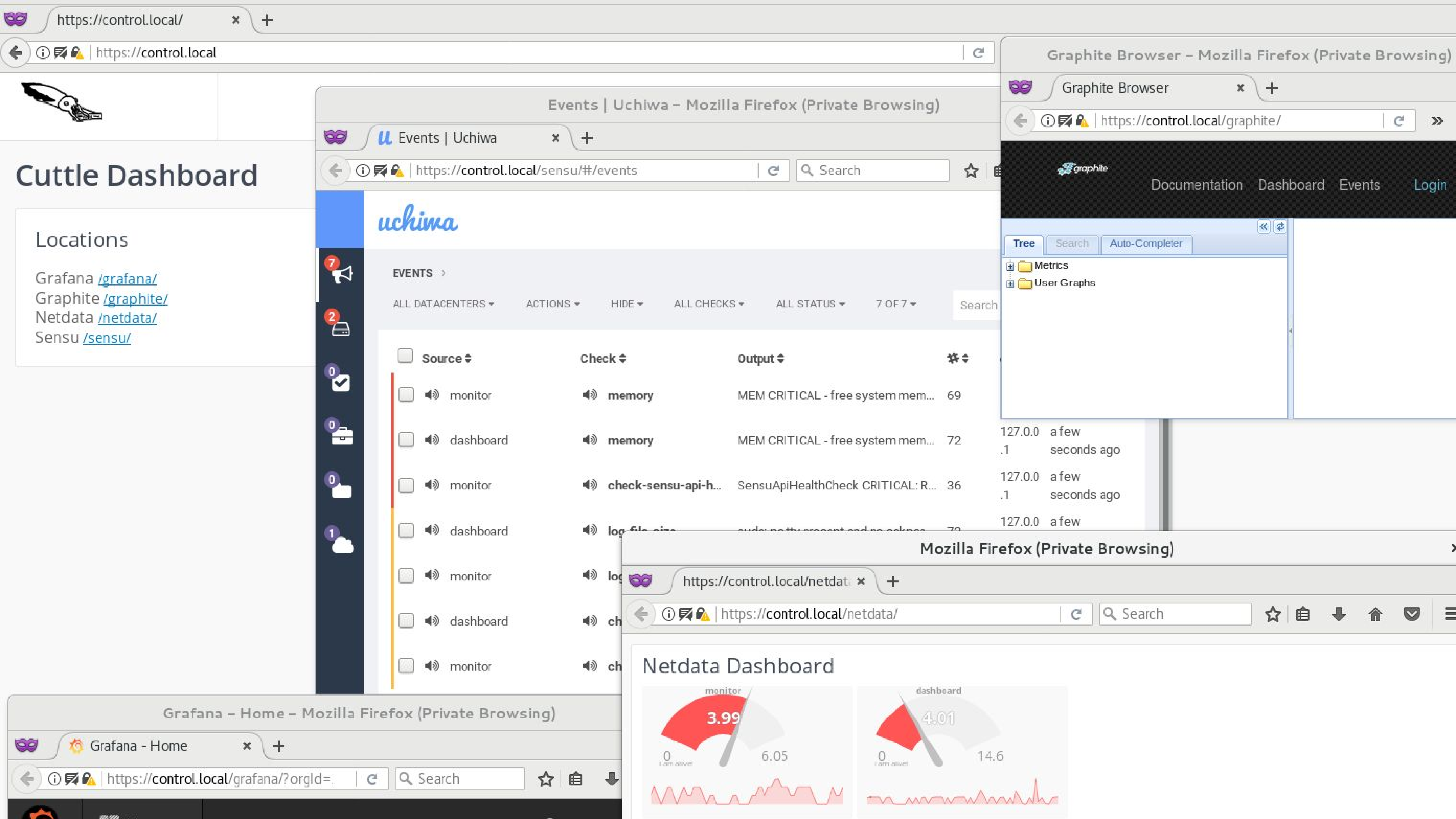


Central control

Flapjack /flapjack/ Grafana /grafana/ Ipmi /ipmi/ Sensu /sensu/

Remote Locations

DAL09	FRA02	HKG02	LON02	MEX01	MIL01	SAO01
/dal09/es/ /dal09/grafana/ /dal09/kibana/ /dal09/sensu/	/fra02/es/ /fra02/grafana/ /fra02/kibana/ /fra02/sensu/	/hkg02/es/ /hkg02/grafana/ /hkg02/kibana/ /hkg02/sensu/	/lon02/es/ /lon02/grafana/ /lon02/kibana/ /lon02/sensu/	/mex01/es/ /mex01/grafana/ /mex01/kibana/ /mex01/sensu/	/mil01/es/ /mil01/grafana/ /mil01/kibana/ /mil01/sensu/	/sao01/es/ /sao01/grafana/ /sao01/kibana/ /sao01/sensu/
SJC01	**SNG01**	**SYD01**	**TOK02**	**TOR01**	**WDC04**	
/sjc01/es/ /sjc01/grafana/ /sjc01/kibana/ /sjc01/sensu/	/sng01/es/ /sng01/grafana/ /sng01/kibana/ /sng01/sensu/	/syd01/es/ /syd01/grafana/ /syd01/kibana/ /syd01/sensu/	/tok02/es/ /tok02/grafana/ /tok02/kibana/ /tok02/sensu/	/tor01/es/ /tor01/grafana/ /tor01/kibana/ /tor01/sensu/	/wdc04/es/ /wdc04/grafana/ /wdc04/kibana/ /wdc04/sensu/	


https://control.local/
https://control.local
Events | Uchiwa – Mozilla Firefox (Private Browsing)
Events | Uchiwa
https://control.local/sensu/#/events
Search
Graphite Browser – Mozilla Firefox (Private Browsing)
Graphite Browser
https://control.local/graphite/
graphite
Documentation
Dashboard
Events
Login
Tree
Search
Auto-Completer
Metrics
User Graphs
uchiwa
7
2
0
0
0
1
EVENTS ›
ALL DATACENTERS ▾
ACTIONS ▾
HIDE ▾
ALL CHECKS ▾
ALL STATUS ▾
7 OF 7 ▾
Search
Mozilla Firefox (Private Browsing)
https://control.local/netdat
https://control.local/netdata/
Search
Grafana – Home – Mozilla Firefox (Private Browsing)
Grafana - Home
https://control.local/grafana/?orgId=
Search
monitor
3.99
0
6.05
I am alive!
dashboard
4.01
0
14.6
I am alive!

Cuttle Dashboard

Locations

Grafana /grafana/
Graphite /graphite/
Netdata /netdata/
Sensu /sensu/

Source	Check	Output			
monitor	memory	MEM CRITICAL - free system mem...	69		
dashboard	memory	MEM CRITICAL - free system mem...	72	127.0.0.1	a few seconds ago
monitor	check-sensu-api-h...	SensuApiHealthCheck CRITICAL: R...	36	127.0.0.1	a few seconds ago
dashboard	log-file-size	sudo: no tty present and no askpa...	72	127.0.0	a few
monitor	log				
dashboard	ch				
monitor	ch				

Netdata Dashboard

Cuttle - Bastion

- SSH (obviously!)
- 2FA (Google Authenticator or Yubikey)
  - https://github.com/blueboxgroup/yubiauthd
  - Each user has own user + pubkey + second factor.
- SSH Agent Auth Proxy
  - https://github.com/blueboxgroup/sshagentmux
  - Adds keys to user’s Agent based on group membership
- ttyspy
  - https://github.com/ibm/ttyspy
  - emulates `script | curl -XPOST https://log-server`

https://github.com/kubernetes-incubator/kubespray

- Ansible Playbooks to deploy Kubernetes
- Official(ish)
- Install K8s on any Infrastructure
  - Bare Metal
  - private cloud
  - public cloud
  - VMWare

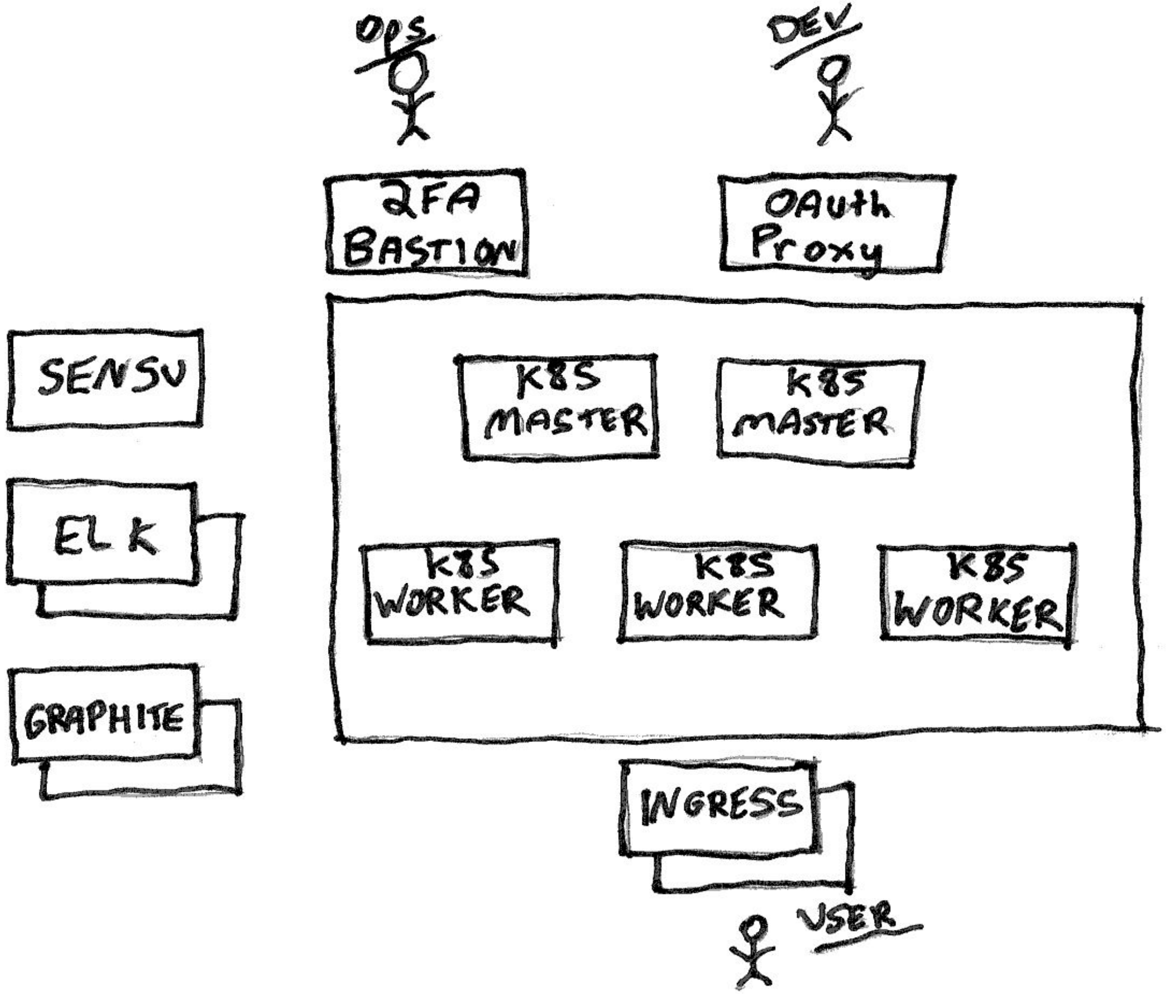
Deploying Kubernetes
Without Scaring Away Your Security Team

https://github.com/kubernetes-incubator/kubespray

Kubespray is production ready!

- Continuous integration
- High availability
- Upgrades!

Deploying Kubernetes Without Scaring Away Your Security Team



ANSIBLE

KUBESPRAY

INSPEC

ansible hardening

Deploying Kubernetes
Without Scaring Away Your Security Team

Other Considerations:

- Build Pipeline - ConcourseCI, Jenkins, etc
- Registry - Quay.io or vmware/harbor
- extra secure containers - Clear Linux and Kata Containers
- Secret Management - Vault
- k8s auth/acls - openpolicyagent

Deploying Kubernetes
Without Scaring Away Your Security Team

Thank you!

Paul Czarkowski
@pczarkowski

Major Hayden
@majorhayden