

Operations for the Modern Data Centre

Ansible, Satellite and Red Hat Insights

Chris Milsted
Principal Solutions Architect, FSI, Red Hat
UK
cmilsted@redhat.com

Disclaimer

The content set forth herein is Red Hat confidential information and does not constitute in any way a binding or legal agreement or impose any legal obligation or duty on Red Hat.

This information is provided for discussion purposes only and is subject to change for any or no reason

Agenda

- Red Hat Management
- Problem statement
- Walk through past operation patterns
- Proposed operational pattern
- Summary and key takeaways

Red Hat Overview



Security and Management

Focus for today

RED HAT®
SATELLITE

RED HAT®
CLOUDFORMS



RED HAT®
INSIGHTS

Operations needs to evolve

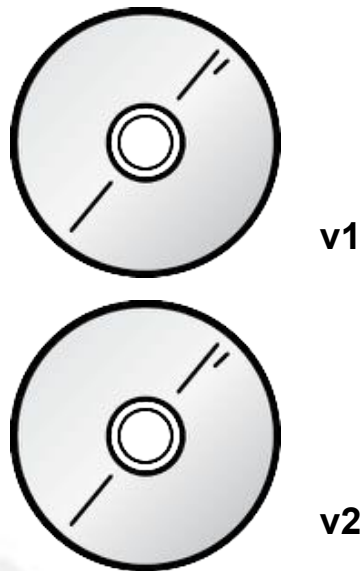
Operations for Next Generation I.T.

- **Information Technology** has evolved; it is no longer considered a cost-centre and is now a key aspect in **competitive differentiation**.
- Digital Disruption is impacting almost every industry, new digital **technologies** are being used to **disrupt existing business models**.
- To succeed we need to deliver:
 - Applications **faster** to market
 - End to End **automation** to deliver iterative developments quickly and error free
 - Integrations to emerging technology to take advantage of changes such as **Hybrid Cloud**.
 - **All of the above without increasing our costs.....**

A look back at the past - building snowflakes

Gold Builds, monthly patch-sets.

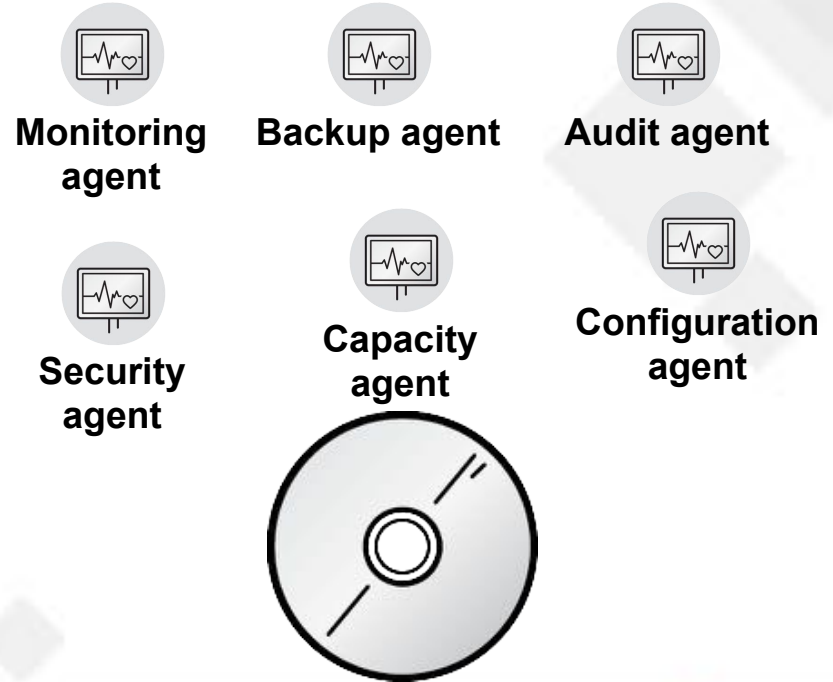
- Gold build created
- V1 becomes basis for all servers
- Used for circa 6 months
- V2 created
- New servers build from V2
- New snowflake every day
- Is V1 ever patched?



How did we Operate the servers?

The rise of the “agent”

- Agents have proliferated
- Different teams demand their own
- Agents all have lifecycles
- Agents consume resources



Compare this to containers

Immutable infrastructure

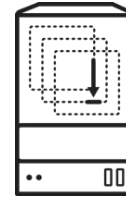


RED HAT ATOMIC

Application Delivery also driving changes.

Microservices, containers and immutability

Business demands ever greater pace of change - micro-services and containers assist

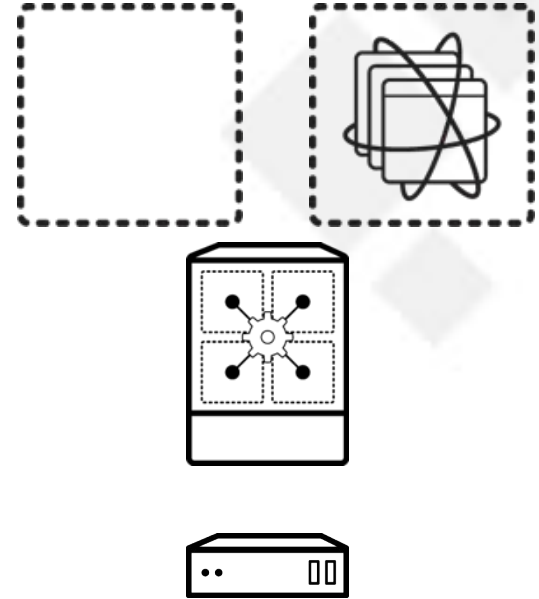


1 physical server	10 Virtual Machines	100 Containers
1 Monolithic application	1 application - 10 environments	1 app in 100 pieces
Health = binary	Health = binary	Health = complex

Containers - what does the end state look like

Container hosts, System containers and Application containers

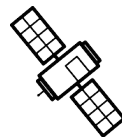
- **Containers:**
 - System containers - container services (e.g. log collection)
 - Application containers - applications or microservices
- **Container orchestration** - delivered via system containers.
- **Container host**



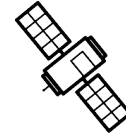
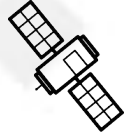
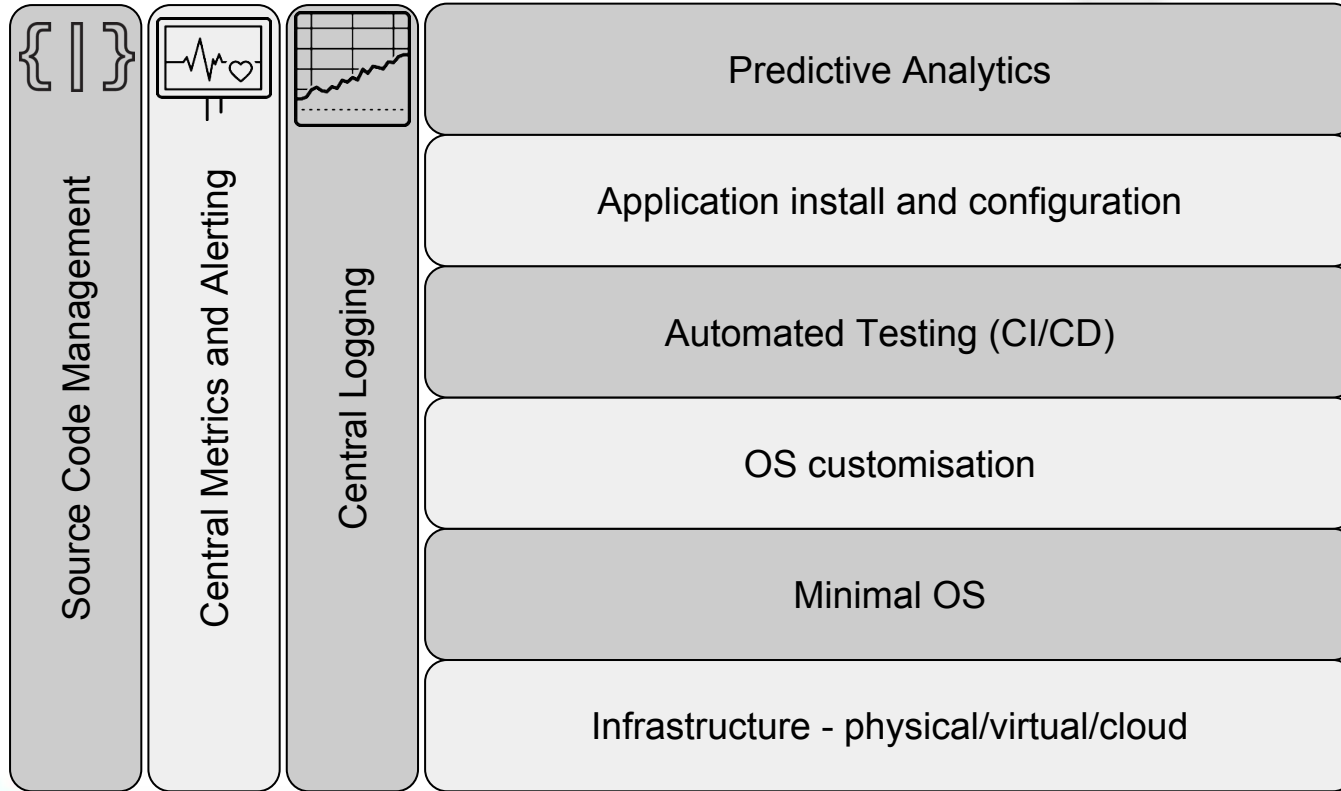
Mapping container thinking to legacy

How do we need to change our thinking?

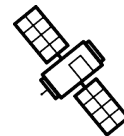
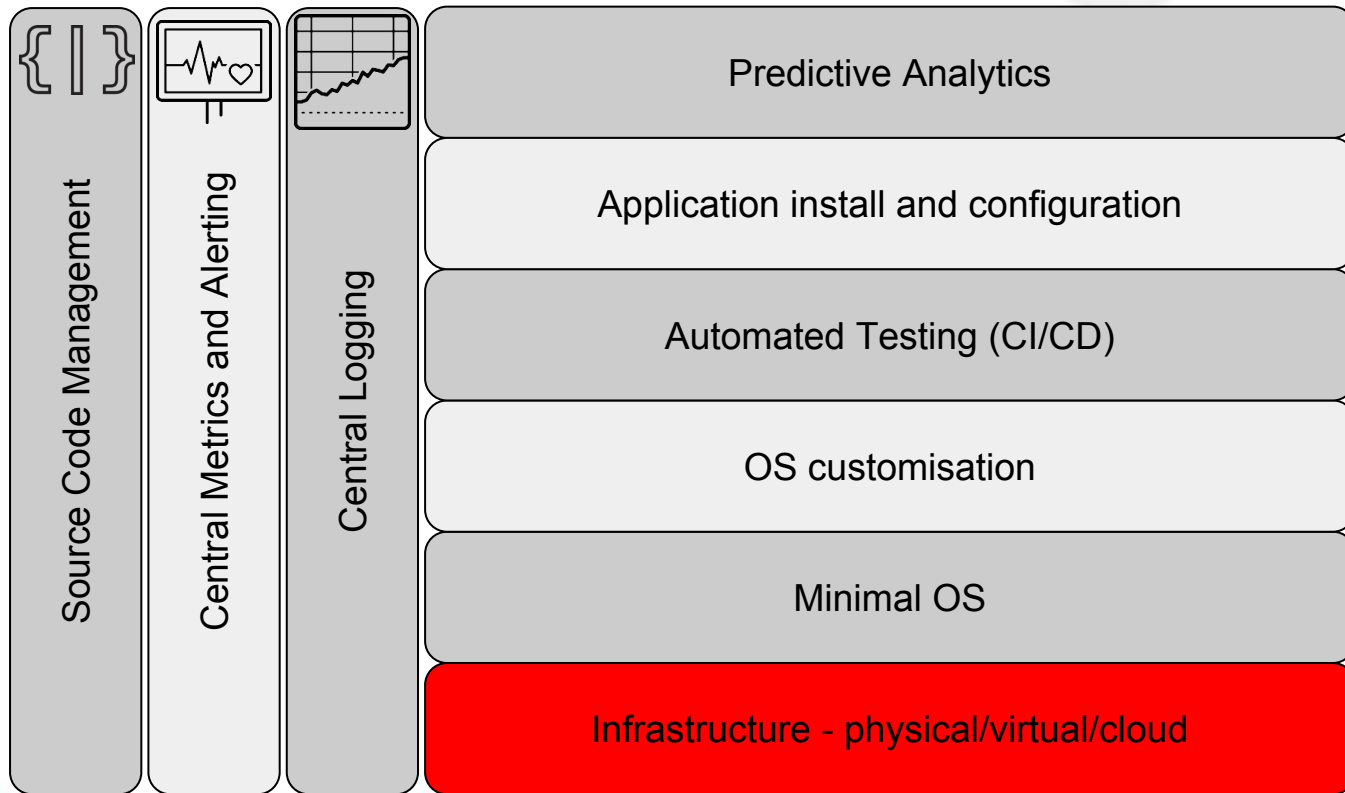
- **Configuration as code** - stored in Source Code Management tool.
 - Build Config - stored as code. Static information.
 - Specific config - depends on variables discovered (ip address)
 - Application configuration (dev/test/prod specifics)
- **Automated deployment** and (depending on life span of system) patching
 - OS + Build Config.
- Simple, Agentless, Powerful **automation** for configuration
 - Applies **latest** configuration to builds or built systems
- Automated **testing tools**
 - Repeatability



Layers with the Red Hat tooling mapped



Layers and tooling



Walkthrough lifecycle of a system

1. Deploy Build - use Tower and playbooks from Ansible

The screenshot shows the 'Edit Survey Prompt' interface in Ansible Tower. The title bar reads 'AWS WINDOWS PROVISIONING - SURVEY'. The interface is divided into two main sections: 'EDIT SURVEY PROMPT' on the left and 'PREVIEW' on the right.

EDIT SURVEY PROMPT:

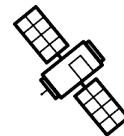
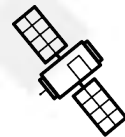
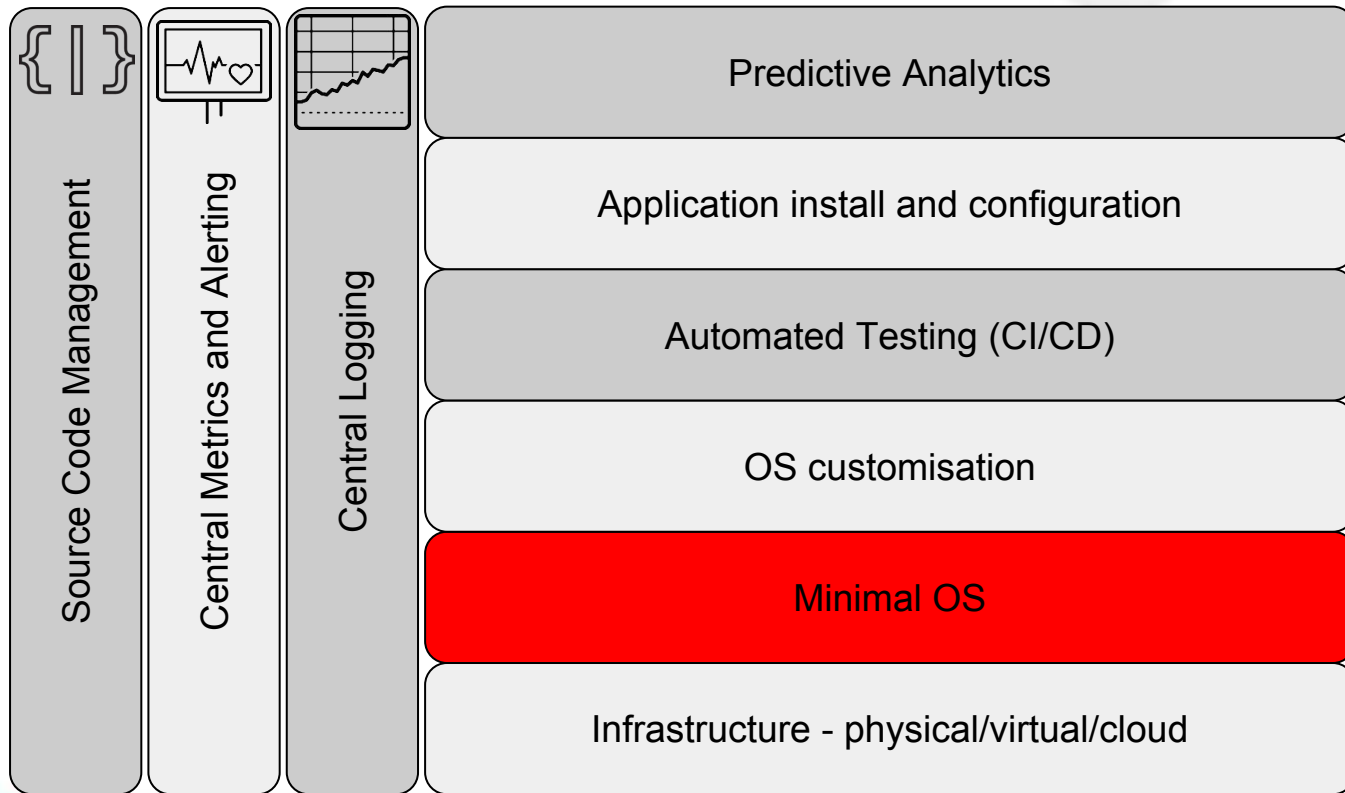
- PROMPT:** A text input field containing 'How many instances?'. Below it is a 'DESCRIPTION' label and an empty text area.
- ANSIBLE VARIABLE NAME:** A text input field containing 'ec2_instance_count'.
- ANSIBLE TYPE:** A dropdown menu with 'Integer' selected.
- MINIMUM:** A text input field containing '1'.
- MAXIMUM:** A text input field containing '10'.
- DEFAULT ANSWER:** A text input field containing '1'.
- REQUIRED:** A checkbox that is currently unchecked.

PREVIEW:

- PROMPT MANY INSTANCES:** A preview of the survey prompt, showing the text 'How many instances?' and a numeric input field with the value '1'.

At the bottom of the interface, there are four buttons: 'CANCEL' (light blue), 'APPLY' (green), 'SAVE & RUN' (red), and 'OK' (light grey).

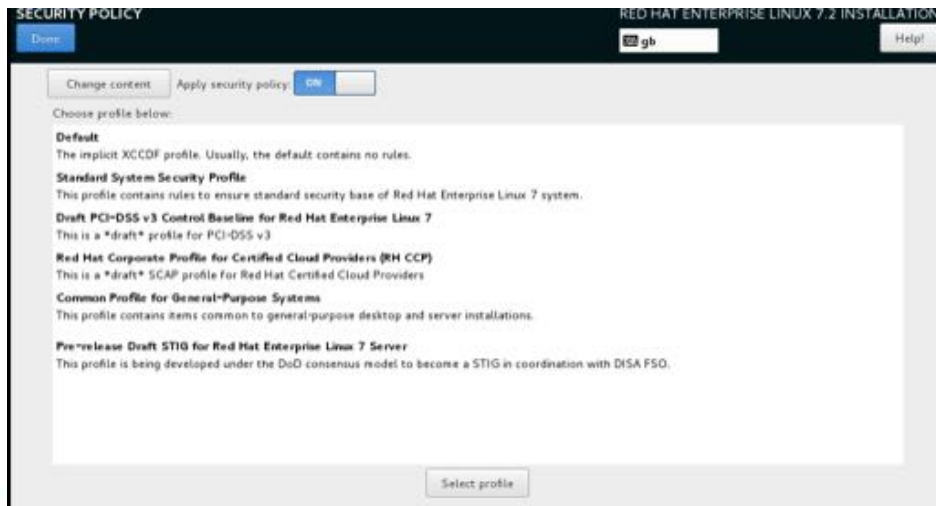
Layers and tooling



Walkthrough lifecycle of a system

2. Build gold build - use Satellite and configuration tool of choice (inbuilt puppet or Tower)

- Kickstart
- Generate “all base formats”



Walkthrough lifecycle of a system

Bonus points - using callbacks to configure OS. Credit Maxim Burgerhout.

1. Add to Kickstart (below)
2. Define snippet (right)
3. Set variable “ansible_enabled=true”

```
# Using systemd will make this not work on RHEL5 and RHEL6

<% if @host.params['ansible_enabled'] == 'true' %>
cat > /etc/systemd/system/ansible-callback.service << EOF
<%= snippet 'ansible_callback_service' %>
EOF
```

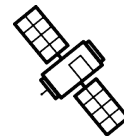
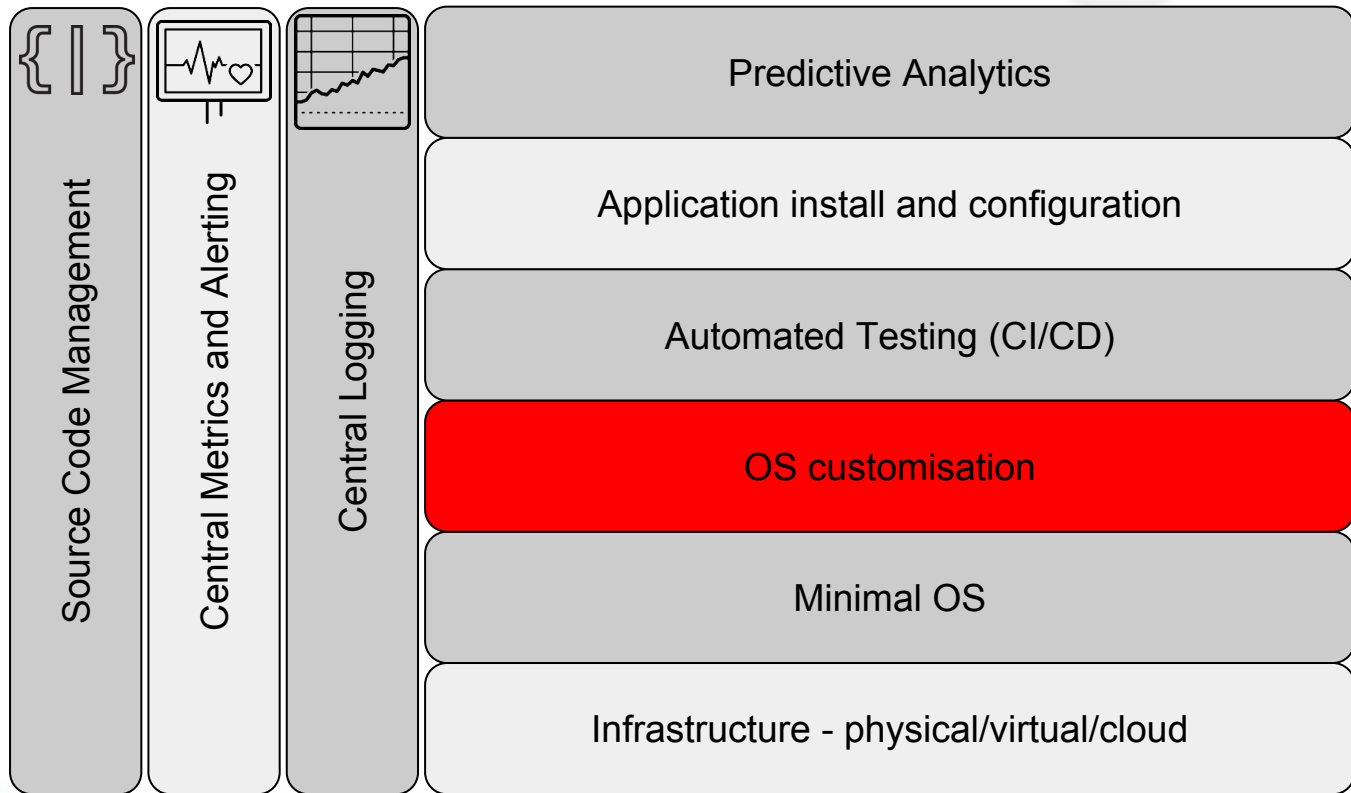
```
# Runs during first boot, removes itself
/usr/bin/systemctl enable ansible-callback
<% end -%>
```

```
[Unit]
Description=Provisioning callback to Ansible
Wants=network-online.target
After=network-online.target

[Service]
Type=oneshot
ExecStart=/usr/bin/curl -k -s --data
"host_config_key=$HOST_CONFIG_KEY"
https://$YOUR_TOWER_HOSTNAME/api/v1/job_templates/$JOB_TEMPL
ATE_ID/callback/
ExecStartPost=/usr/bin/systemctl disable ansible-callback

[Install]
WantedBy=multi-user.target
```

Layers and tooling



Walkthrough lifecycle of a system

3. OS Customisations - check firewall, ntp etc. all setup

HOST EVENT

DETAILS

JSON

EVENT

HOST10.39.167.226

STATUS● changed

ID97

CREATED2016-09-20T08:48:42.035Z

PLAYall

TASKfirewalld

MODULEfirewalld

RESULTS

CHANGEDtrue

_ANSIBLE_NO_LOGfalse

_ANSIBLE_ITEM_RESULTtrue

ITEM443/tcp

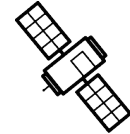
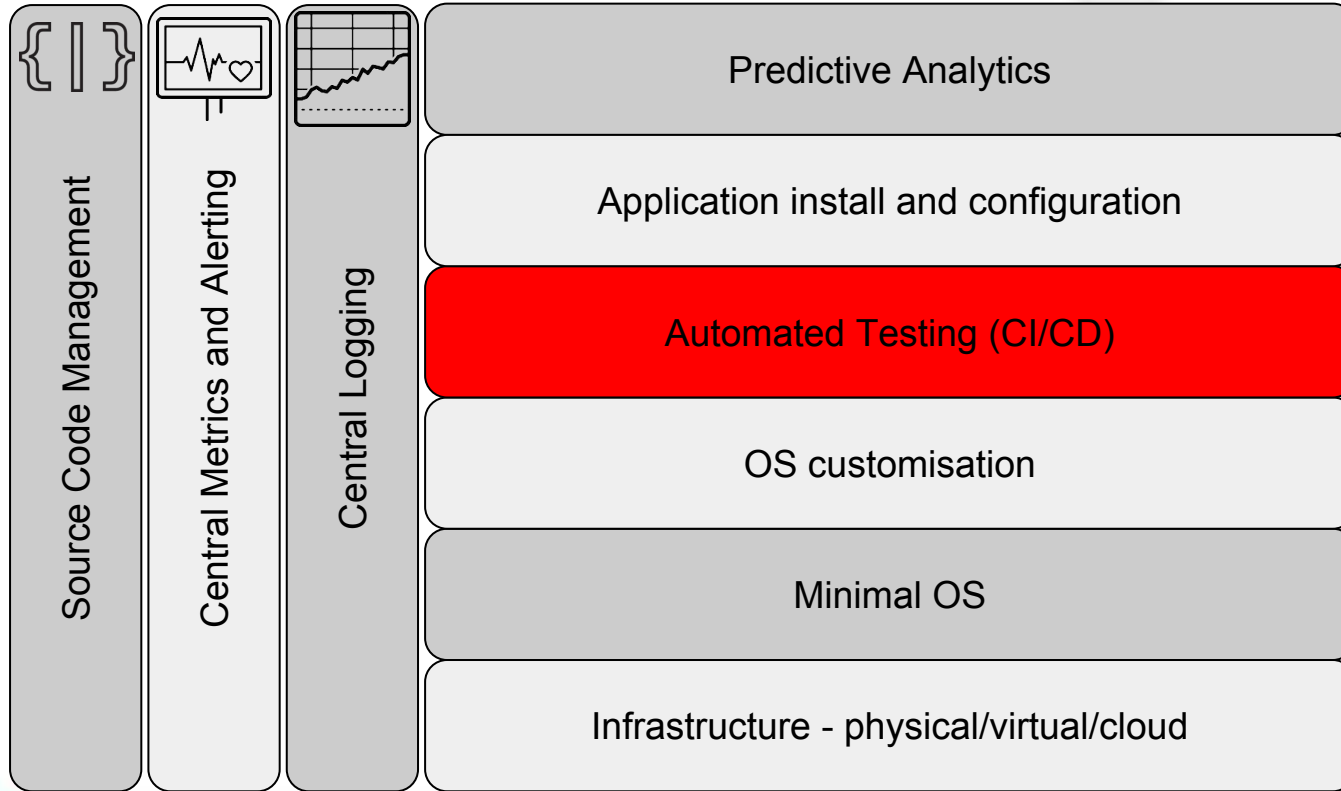
MSGPermanent operation, Changed port 443/tcp to enabled

PREV HOST

NEXT HOST

CLOSE

Layers and tooling



Walkthrough lifecycle of a system

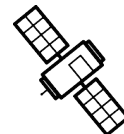
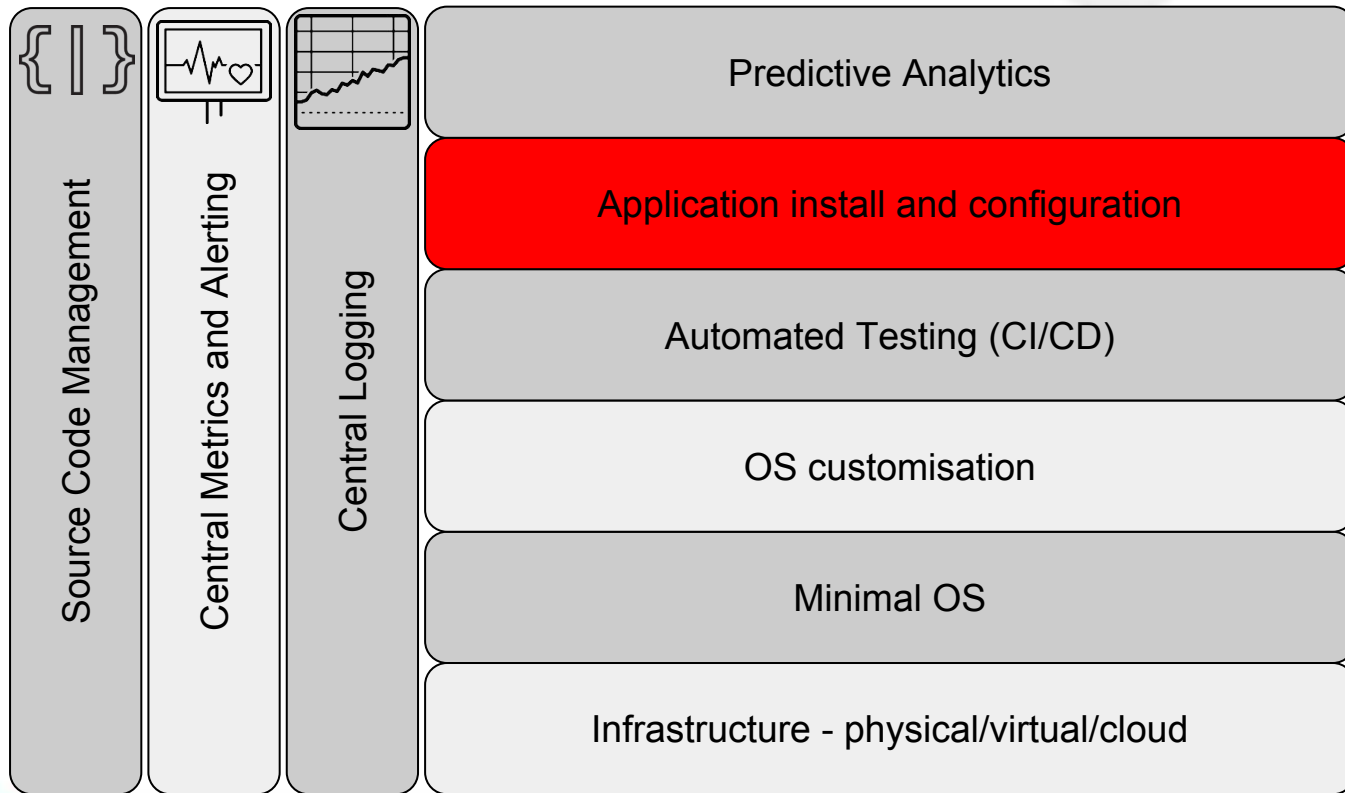
4. Automated testing - for example scan for PCI-DSS Security compliance

2 Please select a task below to view its associated hosts

TASK NAME

TASKS	STARTED	ELAPSED	HOST STATUS
● setup	22:16:06	00:00:02	1
● file	22:16:09	00:00:00	1
● Install openSCAP ...	22:16:09	00:00:11	1
● Run oscap securi...	22:16:21	00:00:07	1
● Wait for report to...	22:16:28	00:00:00	1

Layers and tooling



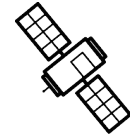
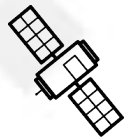
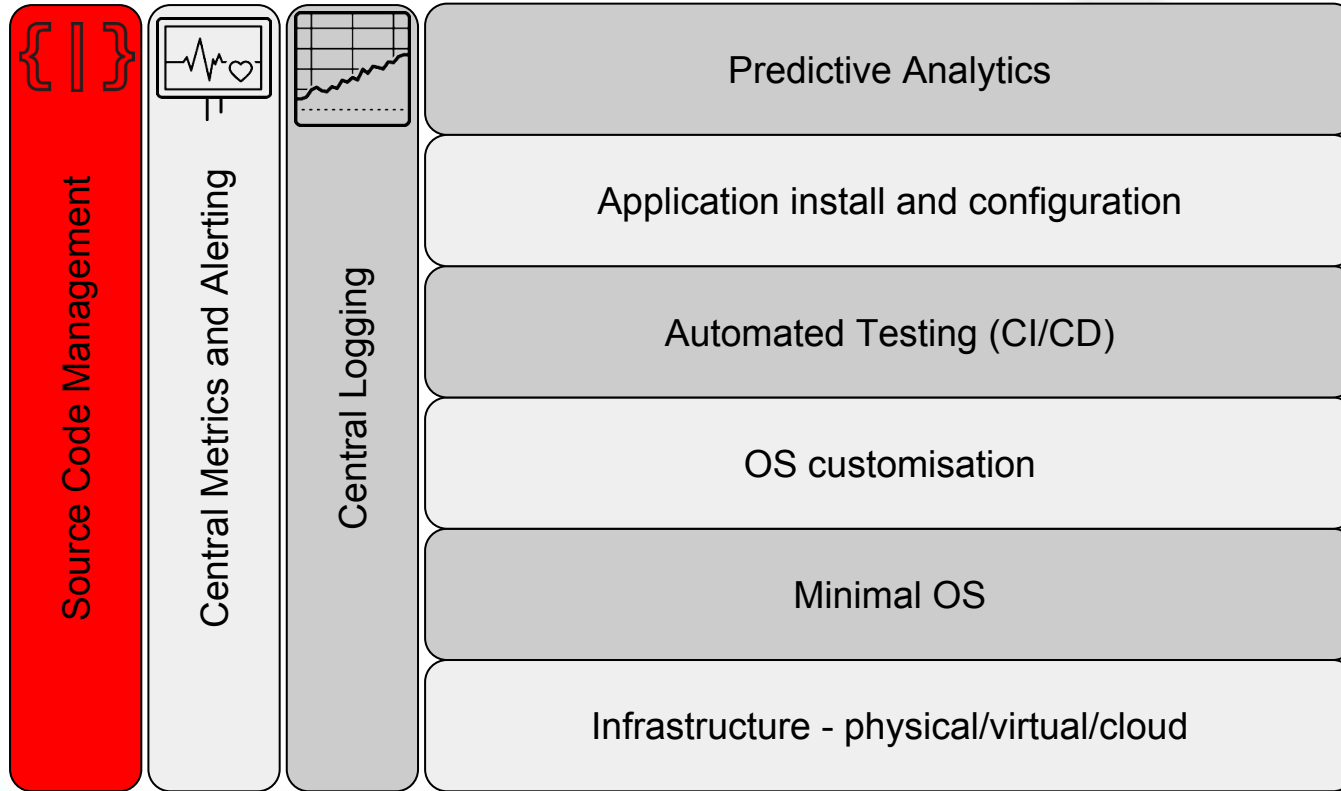
Application install and configuration

5. Application deployment



```
---  
- name: install and start apache  
  hosts: all  
  vars:  
    http_port: 80  
    max_clients: 200  
    remote_user: root  
  
  tasks:  
    - name: install httpd  
      yum: pkg=httpd state=latest  
    - name: write the apache config file  
      template: src=/srv/httpd.j2 dest=/etc/httpd.conf  
    - name: start httpd  
      service: name=httpd state=running
```


Layers and tooling



Optional step - errata and patching

If long lived; need to keep re-applying the most recent configuration

HOST EVENT

DETAILS

JSON

EVENT

HOST 10.39.167.226

STATUS ● changed

ID 97

CREATED 2016-09-20T08:48:42.035Z

PLAY all

TASK firewallld

MODULE firewallld

RESULTS

CHANGED true

_ANSIBLE_NO_LOG false

_ANSIBLE_ITEM_RESULT true

ITEM 443/tcp

MSG Permanent operation, Changed port 443/tcp to enabled

PREV HOST

NEXT HOST

CLOSE

Content Hosts

Filter...

Search

Showing 8 of 8 (8 Total)

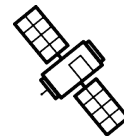
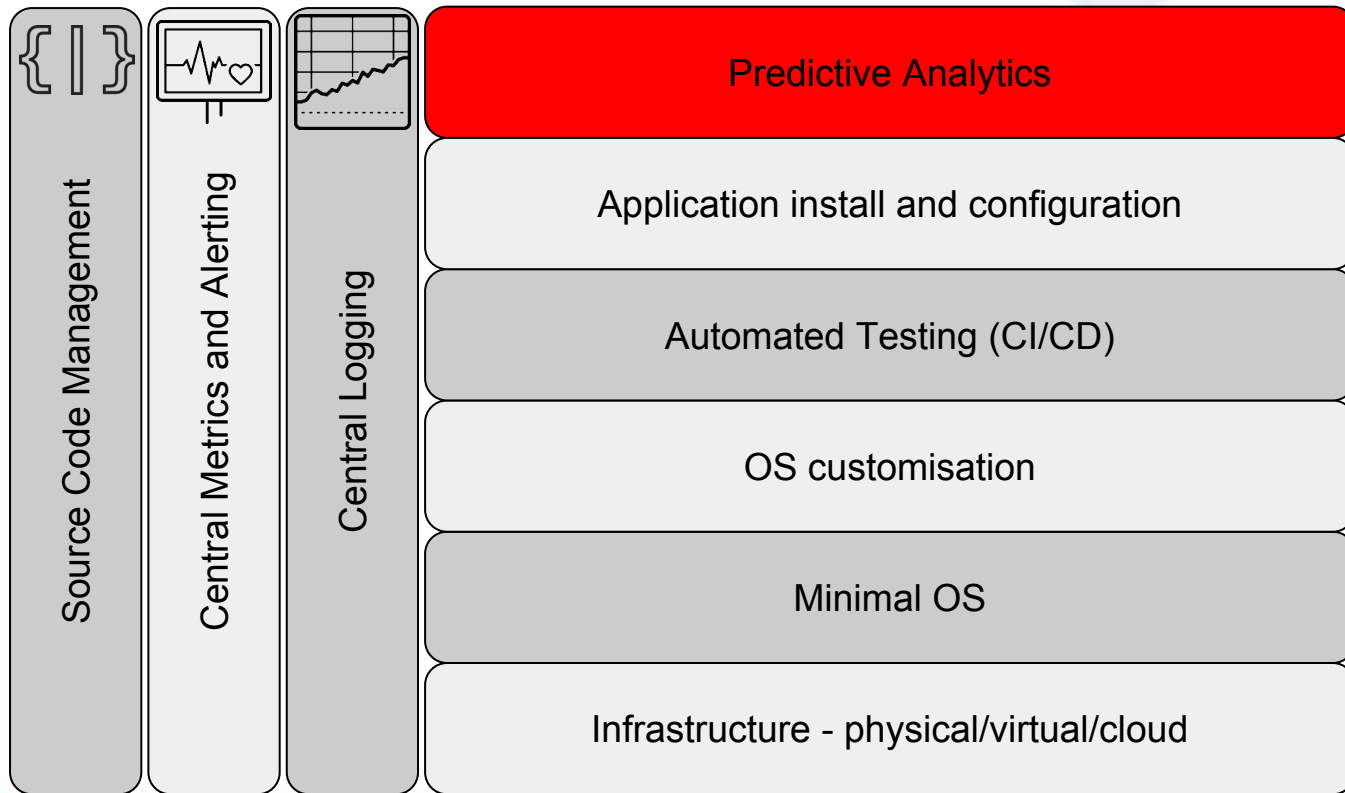
0 Selected

Bulk Actions

Register Content Host

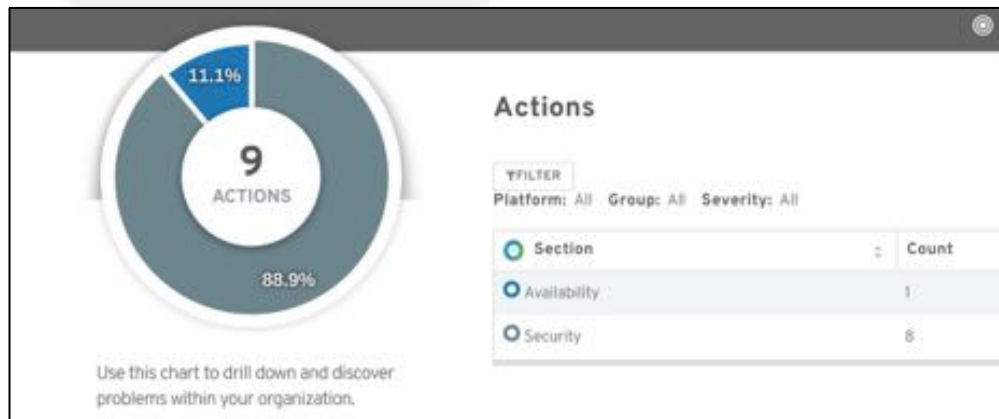
Name	Type	Id	Title	Issued
amazon1.myork	Bug Fix Advisory - None	RHBA-2016:1843	NetworkManager bug fix update	9/14/16
gitlab.myork	Bug Fix Advisory - None	RHBA-2016:1834	python bugfix update	9/14/16
git.myork	Bug Fix Advisory - None	RHBA-2016:1835	systemd bug fix update	9/14/16
isotest.myork	Bug Fix Advisory - None	RHBA-2016:1873	libteam bug fix update	9/14/16
jenkins.myork	Bug Fix Advisory - None	RHBA-2016:1863	selinux-policy bug fix update	9/14/16
satellite-test-host.myork	Bug Fix Advisory - None	RHBA-2016:1846	dnsmasq bug fix update	9/14/16
sssdtest.myork				
tower.myork				

Layers and tooling



Predictive Analytics

6. Find issues before they happen



Availability > skb_over_panic after add_qrhead

DETECTED ISSUE

This host is running the kernel version of **3.10.0-123.el7.x86_64**, which is prior to **3.10.0-327.el7**. Network interfaces `[object Object]`, whose MTU is more than 1500, are joined in an IPv6 multicast group. In this situation, a kernel panic might happen.

STEPS TO RESOLVE

Red Hat recommends that you update your kernel to the version of **3.10.0-327.el7** or later, even you have not experienced the issue.

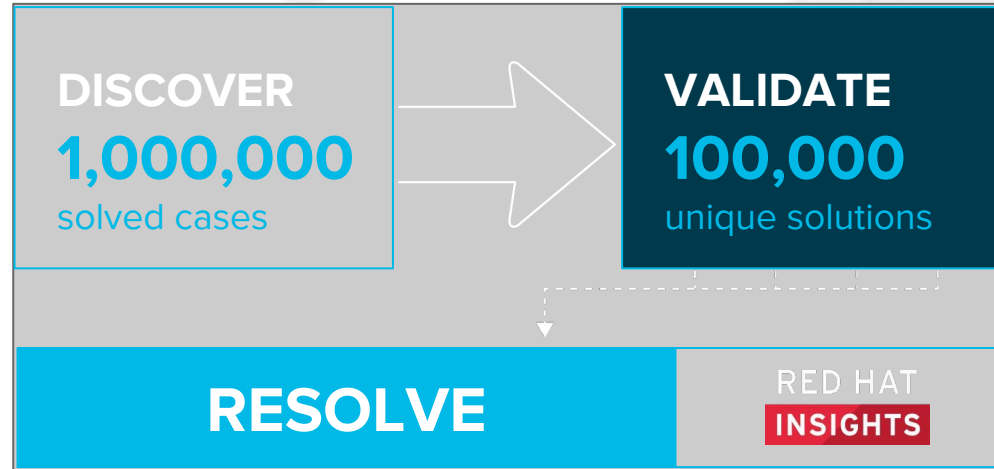
```
# yum update kernel
```

Related Knowledgebase articles: [skb_over_panic after add_qrhead](#)

Insights

Resolve critical issues before they occur

1. What happened?
 - a. Descriptive
2. Why did it happen?
 - a. Diagnostic
3. What will happen?
 - a. Predictive
4. How can we prevent/cause it to happen?
 - a. Prescriptive



Insights beta and future

Beta and beyond

More Red Hat technologies

Automated Ansible playbooks to remediate



Create Ansible playbook

Rule summary:

A flaw in `openssh` could allow an attacker to bypass the `MaxAuthTries` limit and perform a brute-force attack on the system. This issue was reported as [CVE-2015-5600](#).

UPGRADE
openssh-server
package

DISABLE
the insecure
access method

[View selected system](#)

[Reset selections](#)

RED HAT ENTERPRISE LINUX

22 Stability | 26
Performance | 244 Security
| 6 Availability

RED HAT CONTAINERS

1 Stability | 1 Performance
| 3 Security | 0 Availability

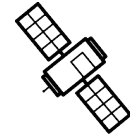
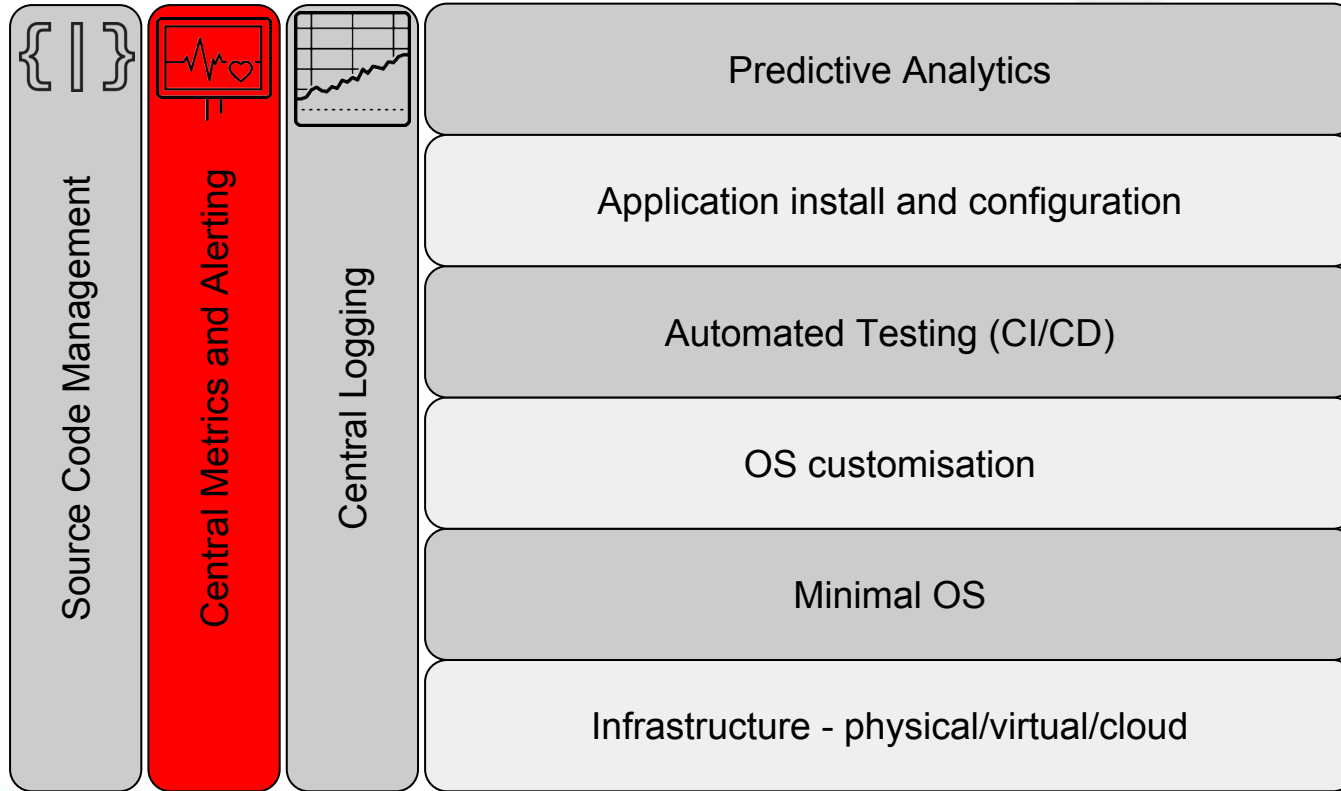
RED HAT ENTERPRISE VIRTUALIZATION

1 Stability | 1 Performance
| 3 Security | 3 Availability

RED HAT OPENSTACK PLATFORM

1 Stability | 1 Performance
| 7 Security | 0 Availability

Layers and tooling

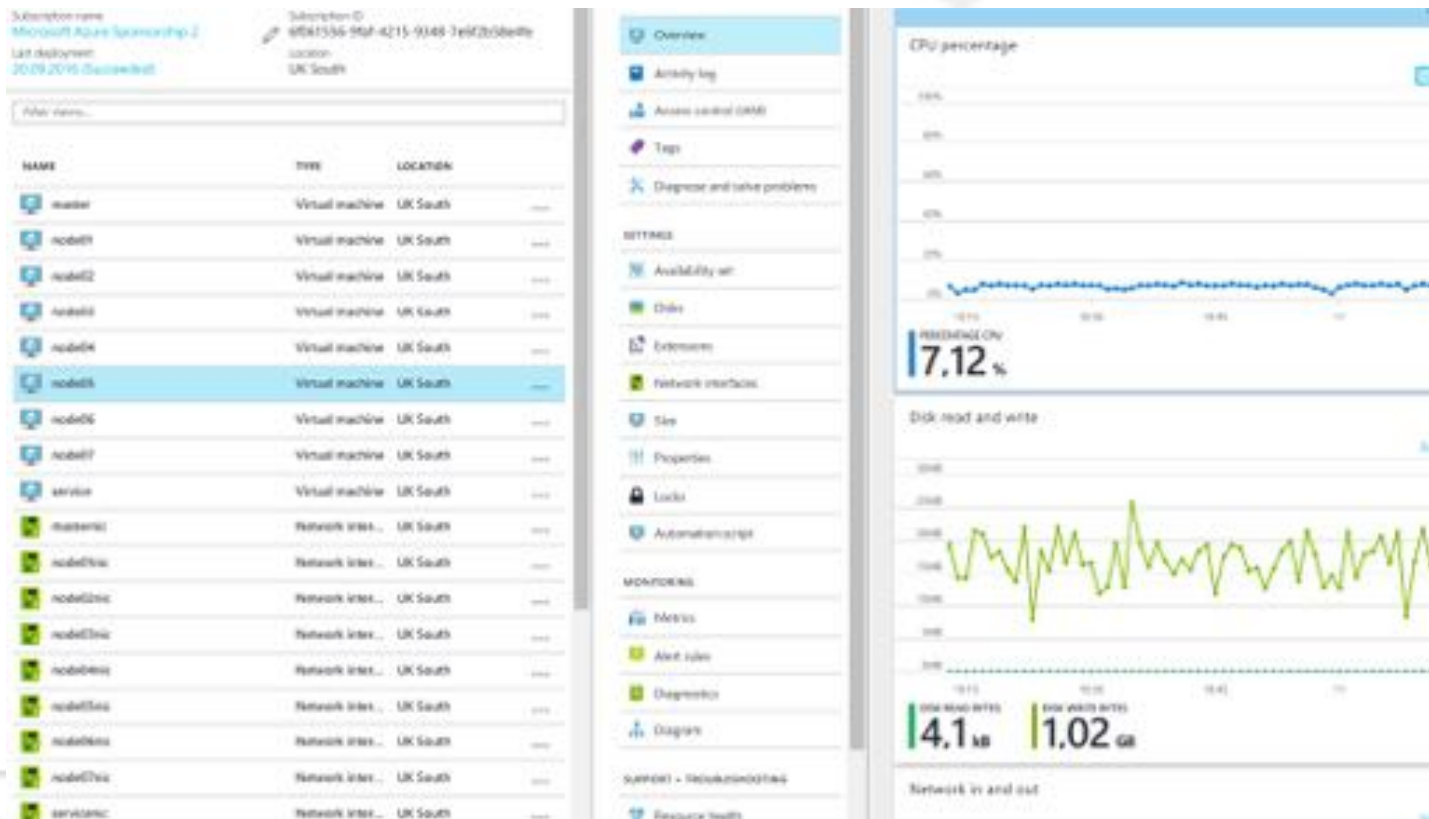


Metrics - Cloud approaches

Unified collection

- Platforms such as Azure and AWS - use hypervisor or single agent to provide common collection framework.
- So we should think about the data we wish to collect, and use a single source.
- Different requirements should process this data in different ways:
 - Real time security - stream data through real-time decision engine (Apache Spark like). For example - real time alerts for failed logins.
 - Batch oriented question - run through batch processing engine (Apache Hadoop like). For example - what are the new errors we see in logs to investigate.

Keynote demo - metrics from the “cloud”



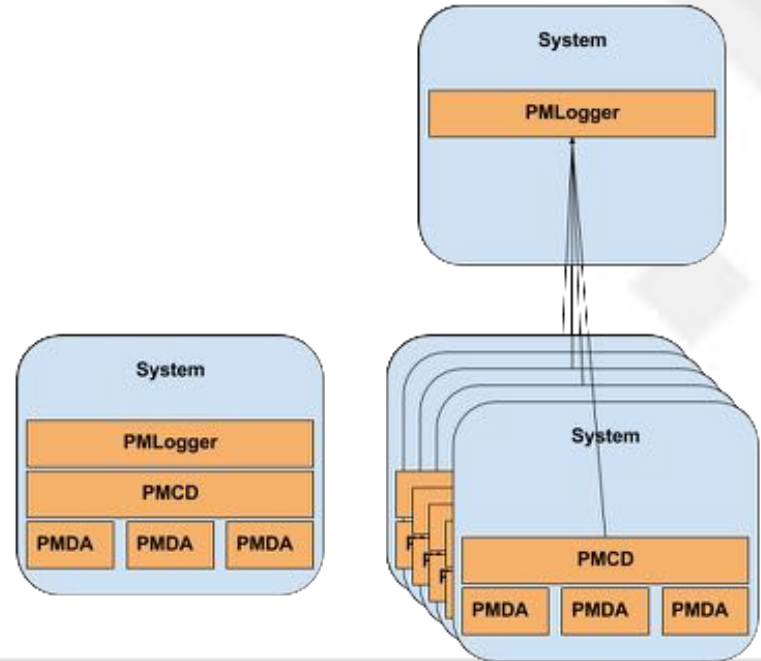
Performance Co-Pilot deployments

Sample Architectures - fully supported performance daemon in RHEL

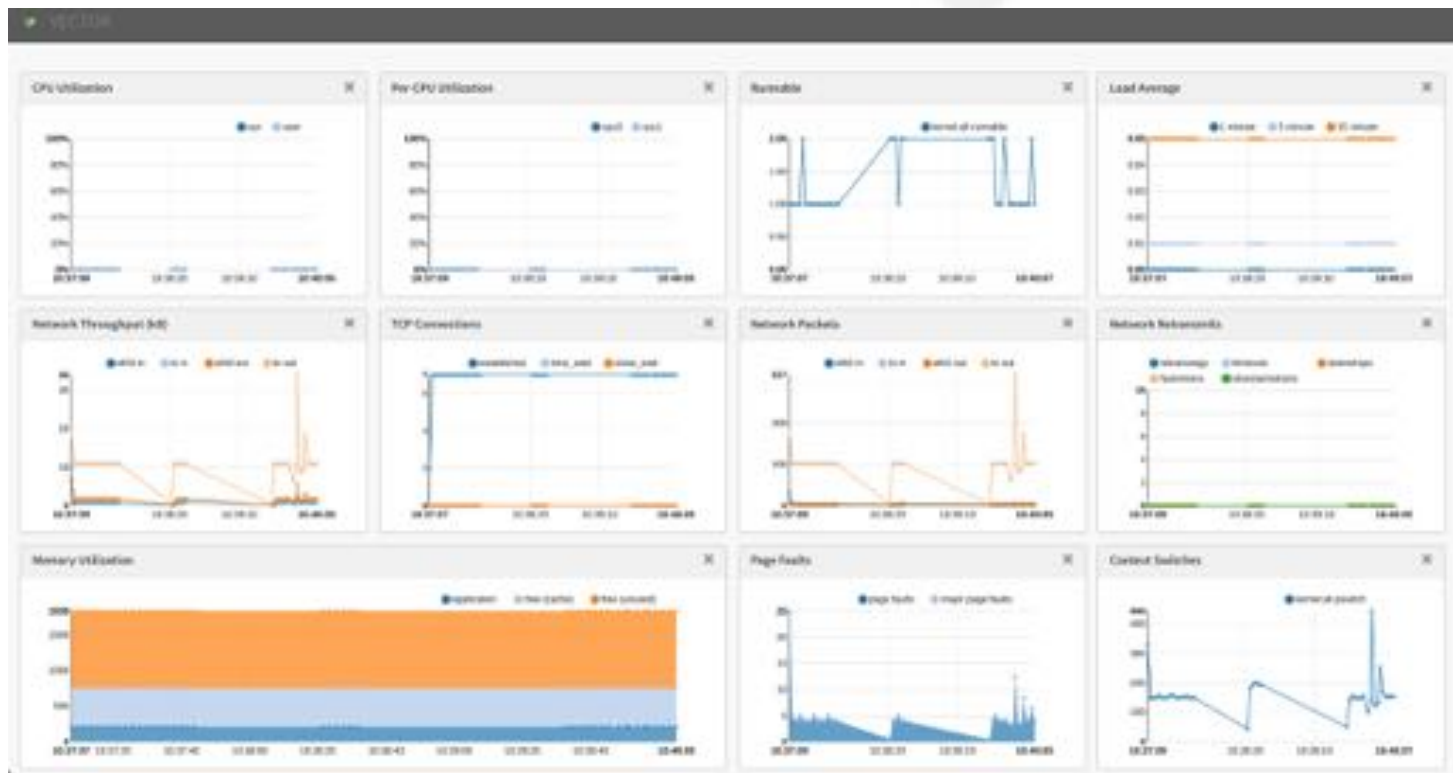
PMDA - Performance Monitor Domain Agent; responds with metrics when queried.

PMCD - Performance Metrics Collector Daemon; collects PMDA metrics.

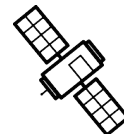
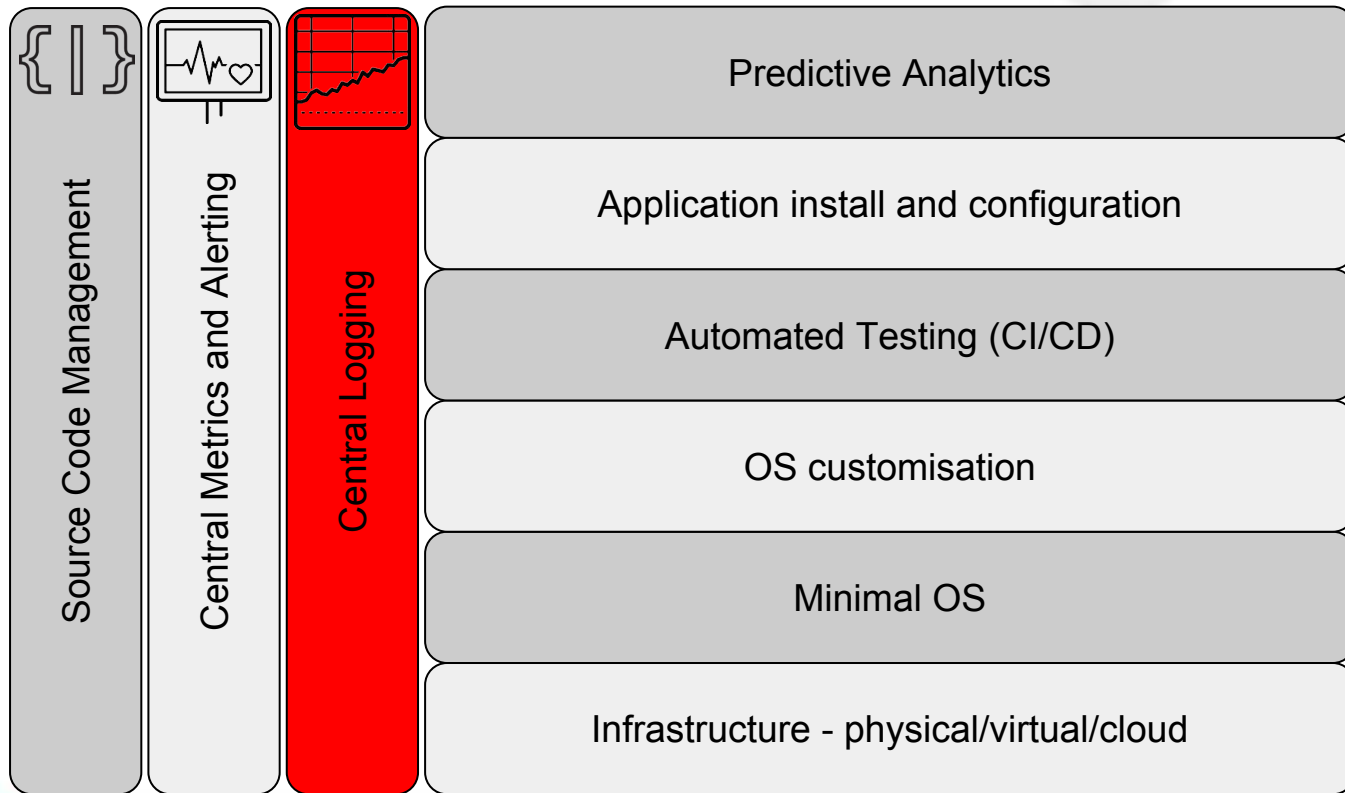
PMLogger - Performance Metric Logger; writes archivelog of performance metrics.



Vector - Browser based dashboard

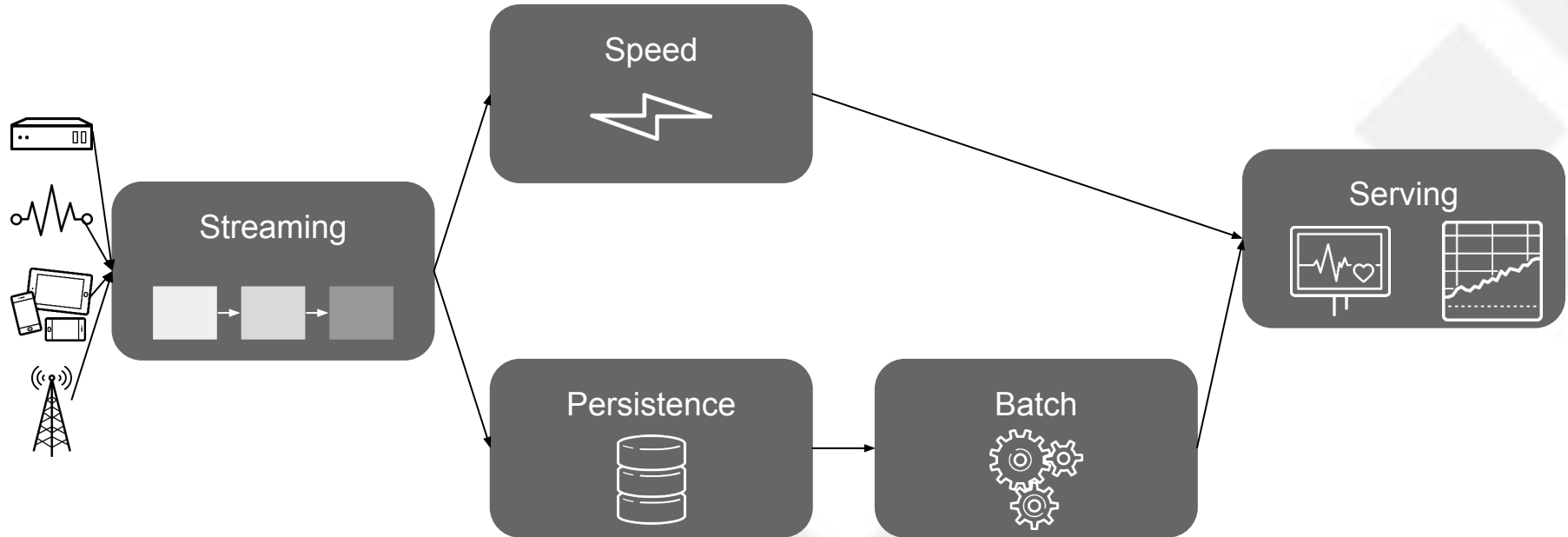


Layers and tooling



New Logging patterns

Streaming, Lambda, Kappa..... and more.



Common Logging in Redhat

Aiming to deliver as part of future releases of OpenShift and OpenStack.

- Aggregate, correlate and centrally searchable logs for the operator
 - RHEL, system specific, application
 - Across multiple product(s) and deployments
 - Node(s), Cluster(s), Data Center(s), Cloud(s)
- Do same for developer
 - Containers, pods, services
 - Across dev/CI/CD and production
 - For traditional and DevOps centric

Links to find out more

<http://rhelblog.redhat.com/2015/12/18/getting-started-using-performance-co-pilot-and-vector-for-browser-based-metric-visualizations/>

<http://www.pcp.io/docs/lab.containers.html>

[Index of Performance Co-Pilot \(PCP\) articles, solutions, tutorials and white papers](#)

<https://access.redhat.com/insights/info/>

<https://www.ansible.com/tower>

<https://access.redhat.com/products/red-hat-satellite#getstarted>

Maxime Thoosen @maxthoon · Mar 9
Simple @ansible playbooks with my best practices ! #devops #symfony #laravel
#nodejs buff.ly/1YttVgT @theodo



References.... And Twitter...



Peter Palaga @ppalaga · 6 Aug 2015
Patching IKEA's 3500 Red Hat Enterprise Linux (RHEL) servers prepared, tested and deployed in 2.5h using RH Satellite



Ikea Patched for Shellshock by Methodically Upgra...

It took about 2.5 hours to test, deploy and upgrade Ikea's entire IT infrastructure to defend against Shellshock. Here's how Ikea did it so quickly.

eweek.com



"With Ansible Tower, we just click a button and deploy to production in 5 minutes. It used to take us 5 hours with 6 people sitting in a room, making sure we didn't do anything wrong (and we usually still had errors). We now deploy to production every other day instead of every 2 weeks, and nobody has to be up at 4am making sure it was done right."

APG

Pension fund administration

Netherlands

- Red Hat Satellite
- Red Hat Enterprise Linux
- Red Hat Training

APG, one of the world's largest collective pension fund administrators, wanted to completely phase out its IBM UNIX-based operating system. It deployed a Red Hat Enterprise Linux environment managed by Red Hat Satellite to secure continuity for applications in use and gain fast deployment of security patches and other changes.

- Improved efficiency to reduce management time
- Reduced server running costs to three times less than previous solution
- Enhanced solution-related skills with Red Hat training courses for IT staff

"The level of support provided was a major reason for us to choose Red Hat. Services such as Red Hat Satellite made Red Hat the obvious choice."

— MAURICE PIJERS
SENIOR SPECIALIST, APG

LEARN MORE AT: [HTTP://RED.HT/2A0MNEJ](http://red.ht/2A0MNEJ)

Key Takeaways

What must we do

- Embrace automation; think about the layers and try to align this to container thinking to align to future patterns
- People and Process - break down the silos. Get the Security, Networking, Application, Linux Engineering, Cloud and Storage teams all in a room to plan deployments so that all requirements are considered - no more per-team agents or build tools.
- Think about how to leverage things like Predictive analytics to replace boring repetitive manual tasks.

Monthly Tech-Talks for more information

All held at Red Hat Monument office.

<https://www.redhat.com/en/about/events/tech-talks-uk>

October 26th An introduction to 3Scale and API Management.

November 23rd EAP 7 and A-MQ 7. JEE and core

December 13th RHEL, RHEV, Atomic and OpenStack.

January 25th Software Defined Storage, Gluster, Ceph.

February 22nd Hybrid Cloud Architectures and Cloudforms



redhat.®