DevOps for Defense

November 2019

Red Hat

Infrastructure-as-Code
& Cloud Native

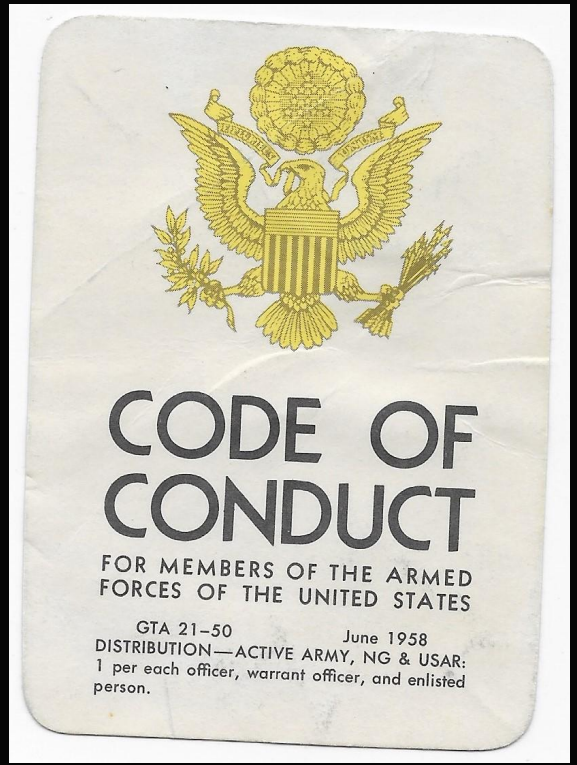
Joe Gavin & Chris Reynolds

https://devopsfordefense.org
https://www.meetup.com/DevOps-for-Defense/
https://github.com/jondavid-black/DevOpsForDefense
devopsfordefense@gmail.com
https://twitter.com/devops4defense

Sponsored by: TEKsystems Own change

DevOps for Defense Meetup: Code of Conduct

- UNCLASSIFIED ONLY!!!!
- Treat each other with respect and professionalism.
- Do not talk about private, sensitive, or proprietary work.
- Do talk about your experiences, needs, desires to improve work in our domain.
- Do share your thoughts.
- Do learn from others.
- Do respect & tip your bartenders!



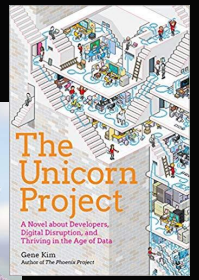
DOES 2019 was an Amazing 3 Days
Highlights & Links @ devopsfordefense.org blog

Outbrief from the conference:

- Key Themes
- Best Presentations
- New Tech
- My Takeaways for the Defense Industry

DEVOPS ENTERPRISE SUMMIT

Oct 28-30 | Las Vegas, NV



The Unicorn Project
By Gene Kim
Release Nov 26th
Available now for pre-order
Do4D Book Club in December

Community Challenge - Donate Time 1 Day a Month

https://girlswhocode.com/

Emeka Barclay Marshall
Language Arts | Liberty Middle Scho
Apple Teacher
Google Certified Educator
Microsoft Innovative Educator
Flipgrid Certified Educator

"Knowledge is power. Information is liberating. Education is the premise of progress, in every society, in every family." -Kofi Annan

Website: caffeinatedteacher.weebly.com
Twitter: @teacheremeka

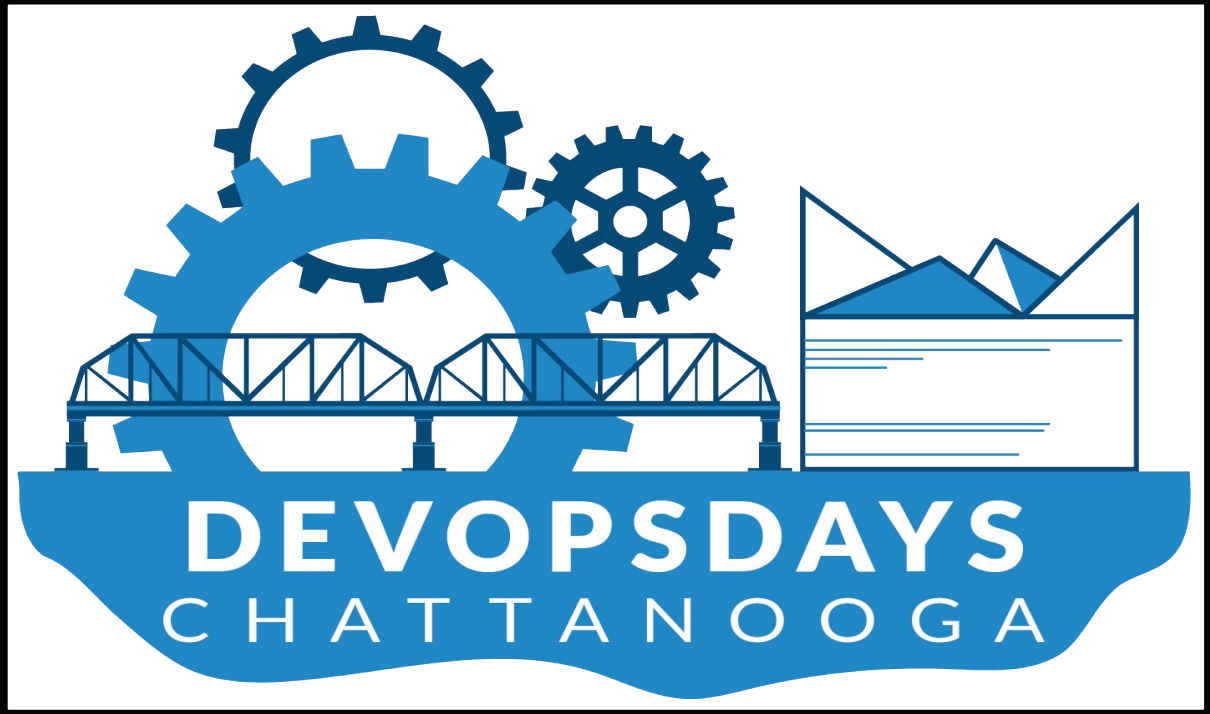
Help Drive Positive Change

Support Girls Who Code through smiles.amazon.com

Local(-ish) DevOps Conference - Nov 12, 2019

Carpool?

Details coming on our blog, twitter, and facebook.



~~$65~~ **$50**

Included coffee, water, snacks, and lunch last year.

Don't forget about the time zone change between here and Chattanooga!

Neighbor City Discount: https://ti.to/chattanooga-devopsdays/chattanooga-devopsdays-2019/discount/chadod-friends

Speakers Include:

https://devopsfordefense.org

DevOps for Defense Meetup Presents

Featuring John Willis

2 Year Anniversary!

The world's largest source code repository with 40 million developers and 100 million repositories!.

GitHub

Lead Engineer for DoD and IC will provide an update on GitHub capability and security advancements.

Thursday, December 5th, 2019 at 6:00pm

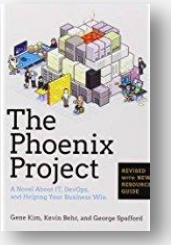
Rocket Republic Brewing Co
289 Production Ave, Madison, AL

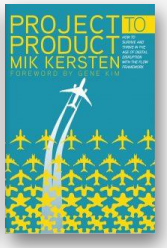
GitHub - Subsidiary of: Microsoft

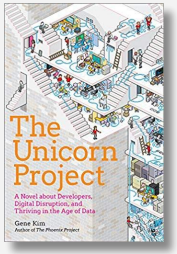
Meetup Sponsored by: TEKsystems — Own change

2020 - What's Next for DevOps for Defense?

January







Back to Basics

- DevOps 3 Ways
- The 4 Types of Work
- The 5 Ideals

February

Gradle

(Still Need to Confirm, but...)

Hans Dockter
CEO Gradle Inc.

Powerful build automation, telemetry, and insight.

Beyond

(Still coordinating & planning, but here's what we're thinking.)

Nicolas M. Chaillan
USAF Chief Software Officer - Bringing DevSecOps DoD-wide

Dr. Mik Kersten
CEO Tasktop - Author of Project to Product

Hack-a-thon?
Opportunity to put our DevOps learning into practice.

Provide us feedback so we can tailor to your needs.

And Now...Please Welcome

The world's leading provider of enterprise open source solutions, using a community-powered approach to deliver high-performing Linux, cloud, container, and Kubernetes technologies.

Red Hat

OPENSHIFT® by Red Hat®

ANSIBLE

Cloud Native

Infrastructure-as-Code

Joe Gavin & Chris Reynolds

Red Hat
Ansible Automation Platform

Automation for all

Ansible technical introduction and overview

Chris Reynolds, RHCA
Senior Cloud Guy
cloudguy@redhat.com

Red Hat

Teams are automating...

Lines Of Business

Network

Security

Operations

Developers

Infrastructure

Why Ansible?

Simple

Human readable automation

No special coding skills needed

Tasks executed in order

Usable by every team

Get productive quickly

Powerful

App deployment

Configuration management

Workflow orchestration

Network automation

Orchestrate the app lifecycle

Agentless

Agentless architecture

Uses OpenSSH & WinRM

No agents to exploit or update

Get started immediately

More efficient & more secure

Red Hat

What can I do using Ansible?

Automate the deployment and management of your entire IT footprint.

Do this...

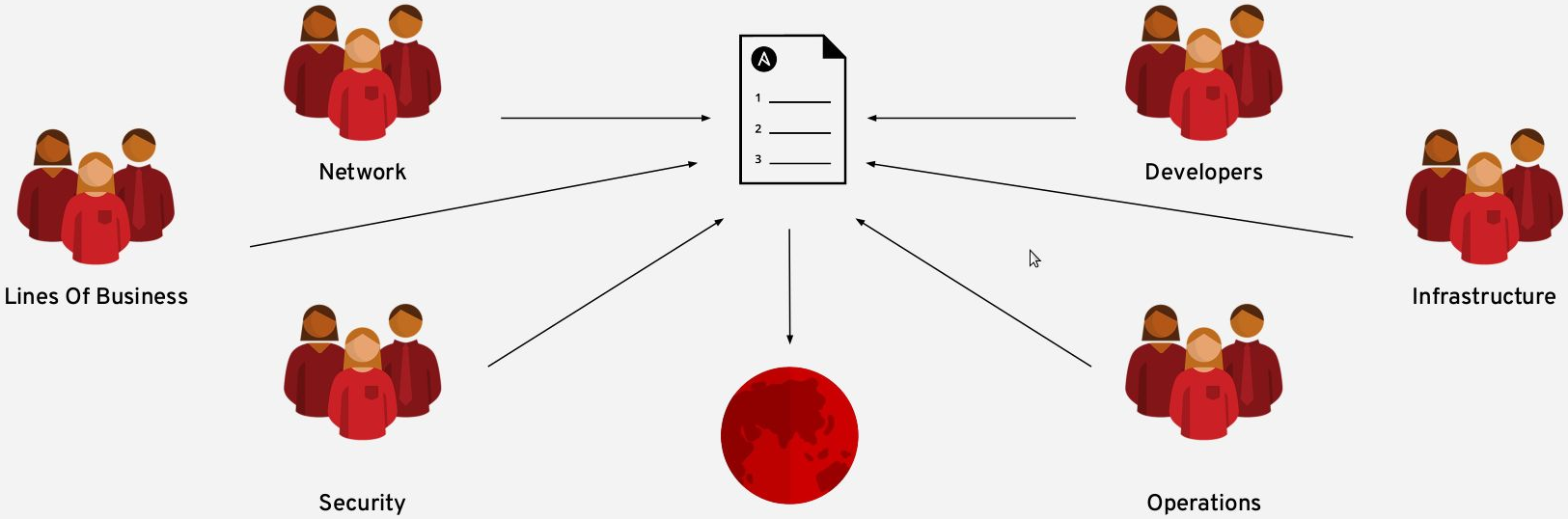
Orchestration	Configuration Management	Application Deployment	Provisioning	Continuous Delivery	Security and Compliance

On these...

Firewalls	Load Balancers	Applications	Containers	Clouds
Servers	Infrastructure	Storage	Network Devices	**And more...**

Red Hat

When automation crosses teams, you need an automation platform



Red Hat Ansible Automation Platform

Network | Lines of business | Security |  | Operations | Infrastructure | Developers

Engage	**Ansible SaaS:** Engage users with an automation focused experience
Scale	**Ansible Tower:** Operate & control at scale
Create	**Ansible Engine:** Universal language of automation

Fueled by an open source community

Red Hat

Ansible automates technologies you use

Time to automate is measured in minutes

Cloud

AWS
Azure
Digital Ocean
Google
OpenStack
Rackspace
+more

Operating Systems

RHEL
Linux
Windows
+more

Virt & Container

Docker
VMware
RHV
OpenStack
OpenShift
+more

Storage

Netapp
Red Hat Storage
Infinidat
+more

Windows

ACLs
Files
Packages
IIS
Regedits
Shares
Services
Configs
Users
Domains
+more

Network

A10
Arista
Aruba
Cumulus
Bigswitch
Cisco
Dell
Extreme
F5
Lenovo
MikroTik
Juniper
OpenSwitch
+more

Security

Checkpoint
Cisco
CyberArk
F5
Fortinet
Juniper
IBM
Palo Alto
Snort
+more

Monitoring

Dynatrace
Datadog
LogicMonitor
New Relic
Sensu
+more

Devops

Jira
GitHub
Vagrant
Jenkins
Slack
+more

Red Hat
Ansible Automation
Platform

Red Hat Ansible Engine:

Universal language of automation

Red Hat

Red Hat Ansible Automation Platform

Network | Lines of business | Security | Operations | Infrastructure | Developers

Engage — **Ansible SaaS:** Engage users with an automation focused experience

Scale — **Ansible Tower:** Operate & control at scale

Create

Simple	**Powerful**	**Agentless**
Human readable automation	Thousands of integrations	No agents to exploit or update

Fueled by an open source community

Red Hat

Red Hat Ansible Engine

Cross platform

Agentless support for all major OS variants, physical, virtual, cloud and network devices.

Human readable

Perfectly describe and document every aspect of your application environment.

Perfect description of application

Every change can be made by Playbooks, ensuring everyone is on the same page.

Version controlled

Playbooks are plain-text. Treat them like code in your existing version control.

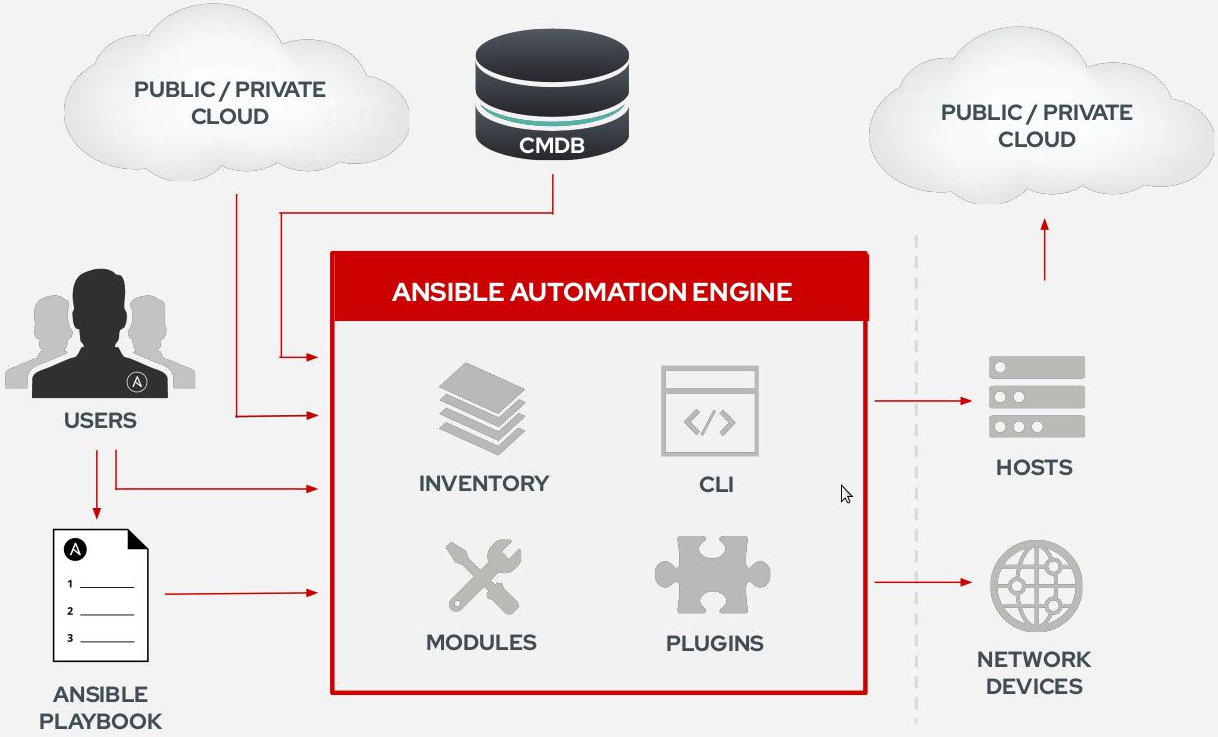
Dynamic inventories

Capture all the servers 100% of the time, regardless of infrastructure, location, etc.

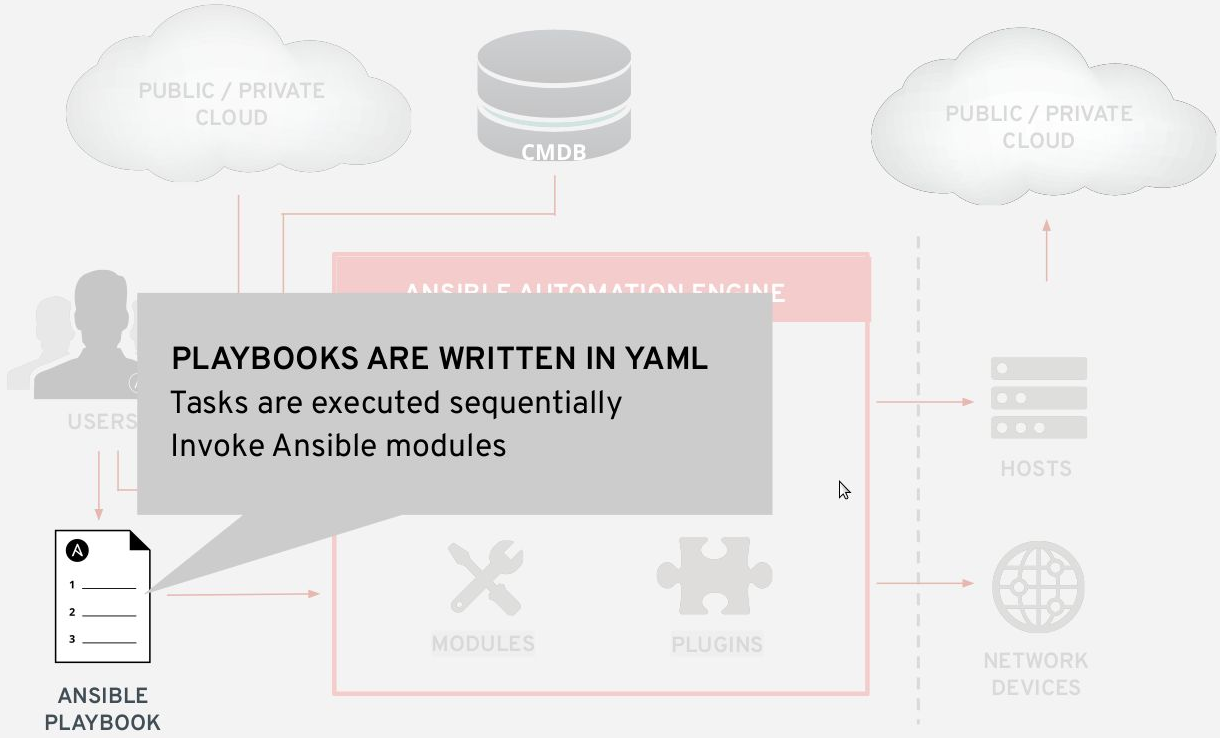
Orchestration plays well with others

Orchestration plays well with others: ServiceNow, Infoblox, AWS, Terraform, Cisco ACI and more

Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
ANSIBLE AUTOMATION ENGINE
USERS
INVENTORY
CLI
HOSTS
MODULES
PLUGINS
NETWORK DEVICES
ANSIBLE PLAYBOOK

Red Hat



PLAYBOOKS ARE WRITTEN IN YAML

Tasks are executed sequentially

Invoke Ansible modules

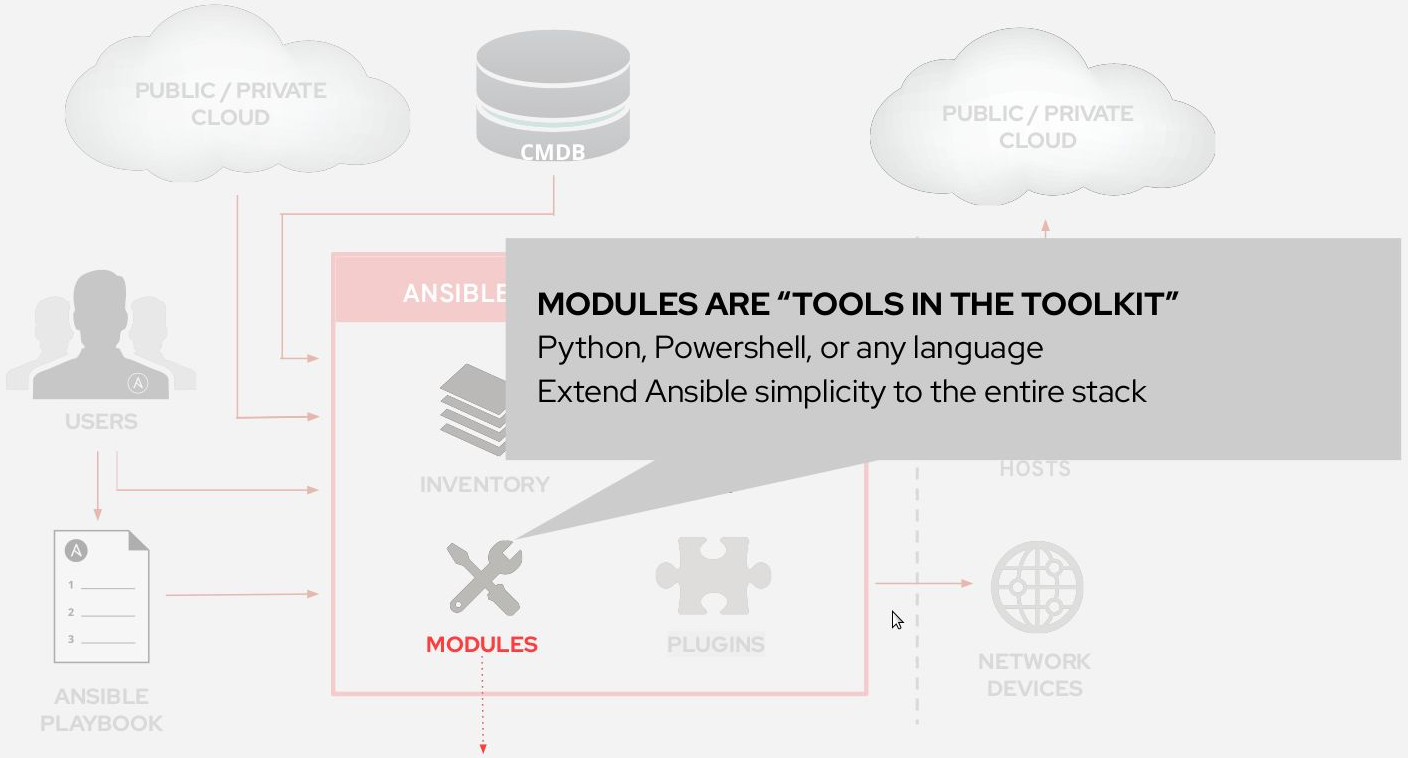
Red Hat

```
---
- name: install and start apache
  hosts: web
  become: yes
  vars:
    http_port: 80

  tasks:
    - name: httpd package is present
      yum:
        name: httpd
        state: latest

    - name: latest index.html file is present
      template:
        src: files/index.html
        dest: /var/www/html/

    - name: httpd is started
      service:
        name: httpd
        state: started
```



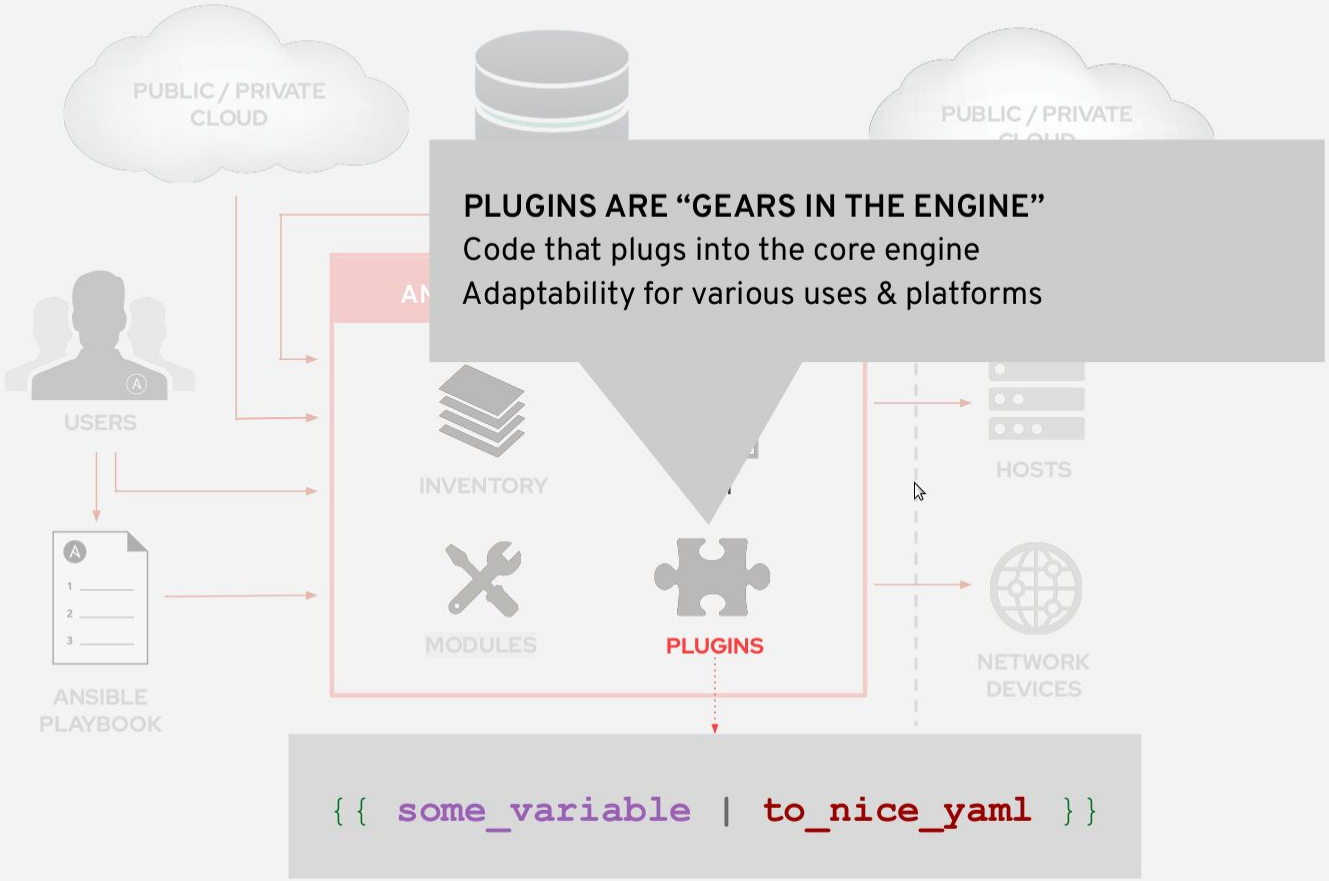
MODULES ARE "TOOLS IN THE TOOLKIT"

Python, Powershell, or any language

Extend Ansible simplicity to the entire stack

```
- name: latest index.html file is present
  template:
    src: files/index.html
    dest: /var/www/html/
```

Red Hat

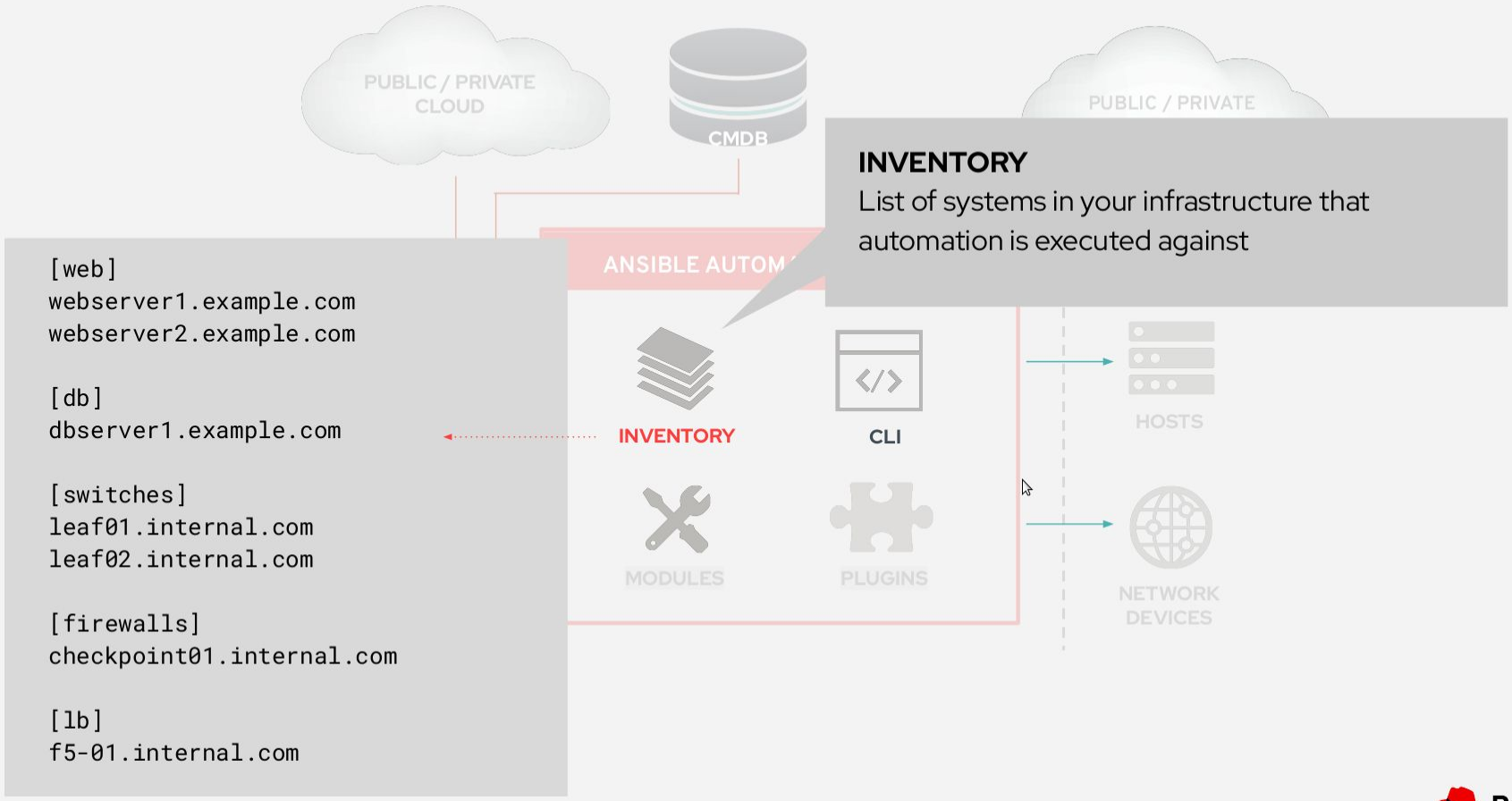


PLUGINS ARE "GEARS IN THE ENGINE"

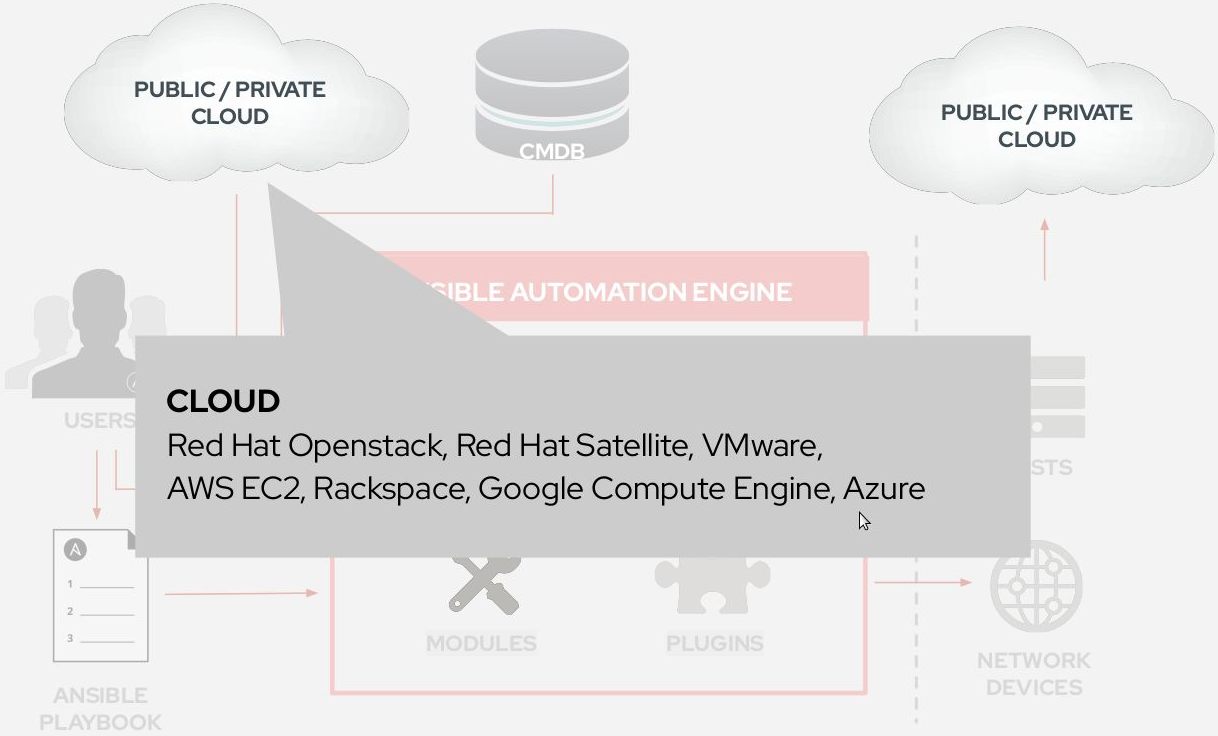
Code that plugs into the core engine

Adaptability for various uses & platforms

Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE
INVENTORY
List of systems in your infrastructure that automation is executed against
ANSIBLE AUTOM
[web]
webserver1.example.com
webserver2.example.com
[db]
dbserver1.example.com
[switches]
leaf01.internal.com
leaf02.internal.com
[firewalls]
checkpoint01.internal.com
[lb]
f5-01.internal.com
INVENTORY
CLI
HOSTS
MODULES
PLUGINS
NETWORK DEVICES

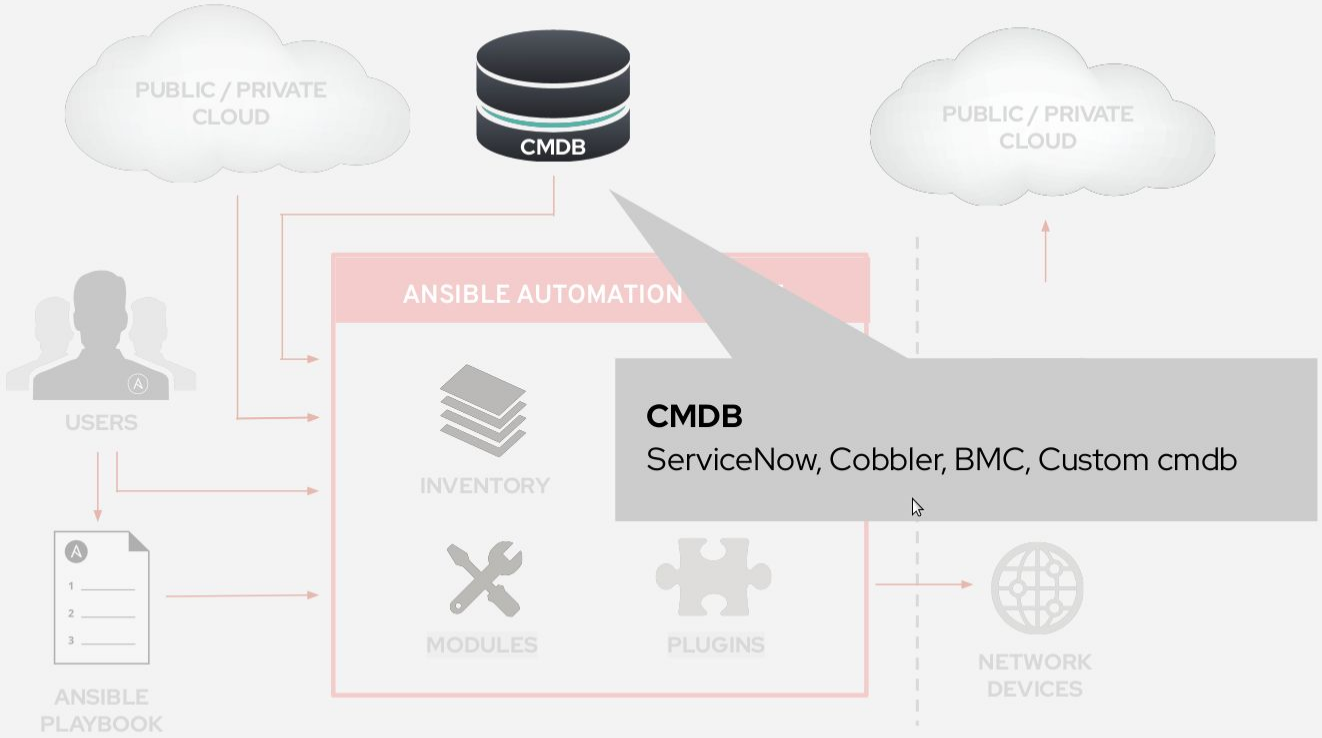
Red Hat



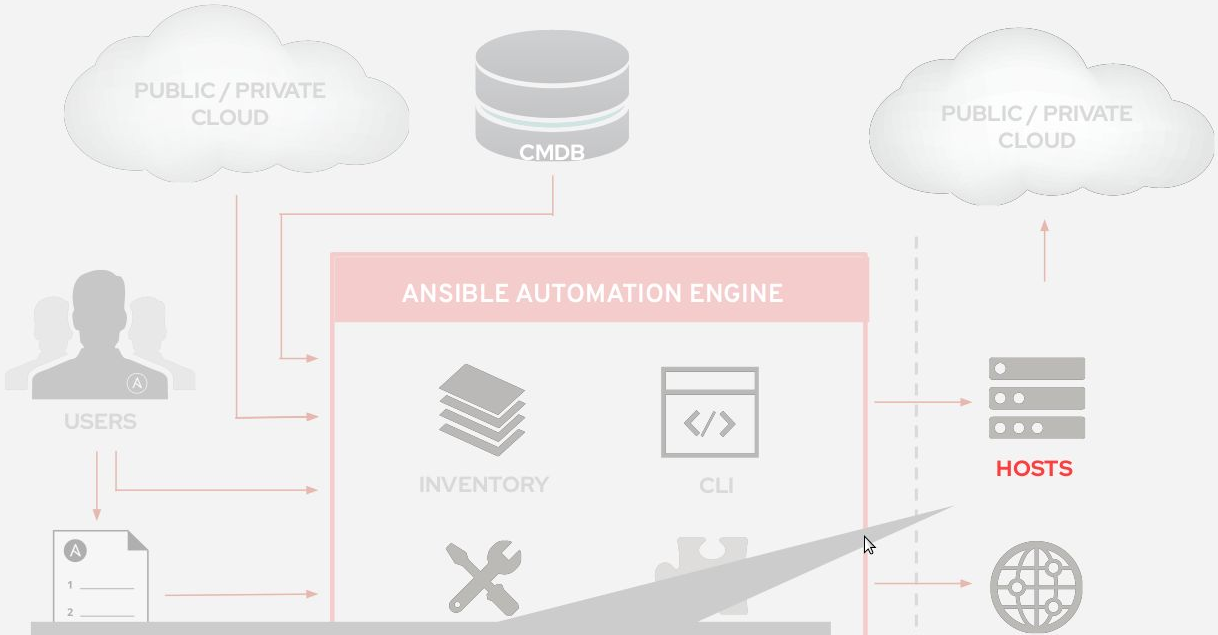
CLOUD

Red Hat Openstack, Red Hat Satellite, VMware,
AWS EC2, Rackspace, Google Compute Engine, Azure

Red Hat


PUBLIC / PRIVATE CLOUD
CMDB
PUBLIC / PRIVATE CLOUD
ANSIBLE AUTOMATION
USERS
INVENTORY
CMDB
ServiceNow, Cobbler, BMC, Custom cmdb
MODULES
PLUGINS
NETWORK DEVICES
ANSIBLE PLAYBOOK

Red Hat



AUTOMATE EVERYTHING

Red Hat Enterprise Linux, Cisco routers, Arista switches, Juniper routers, Windows hosts, Checkpoint firewalls, NetApp storage, F5 load balancers and more

Red Hat

Ansible Playbook examples:

GITHUB EXAMPLES
github.com/ansible/ansible-examples
github.com/ansible/workshops

LAMP + HAPROXY + NAGIOS
bit.ly/lamp_haproxy

WINDOWS
bit.ly/ansible_windows

COMPLIANCE
bit.ly/ansible_compliance

NETWORK
github.com/network-automation

SECURITY
github.com/ansible-security/

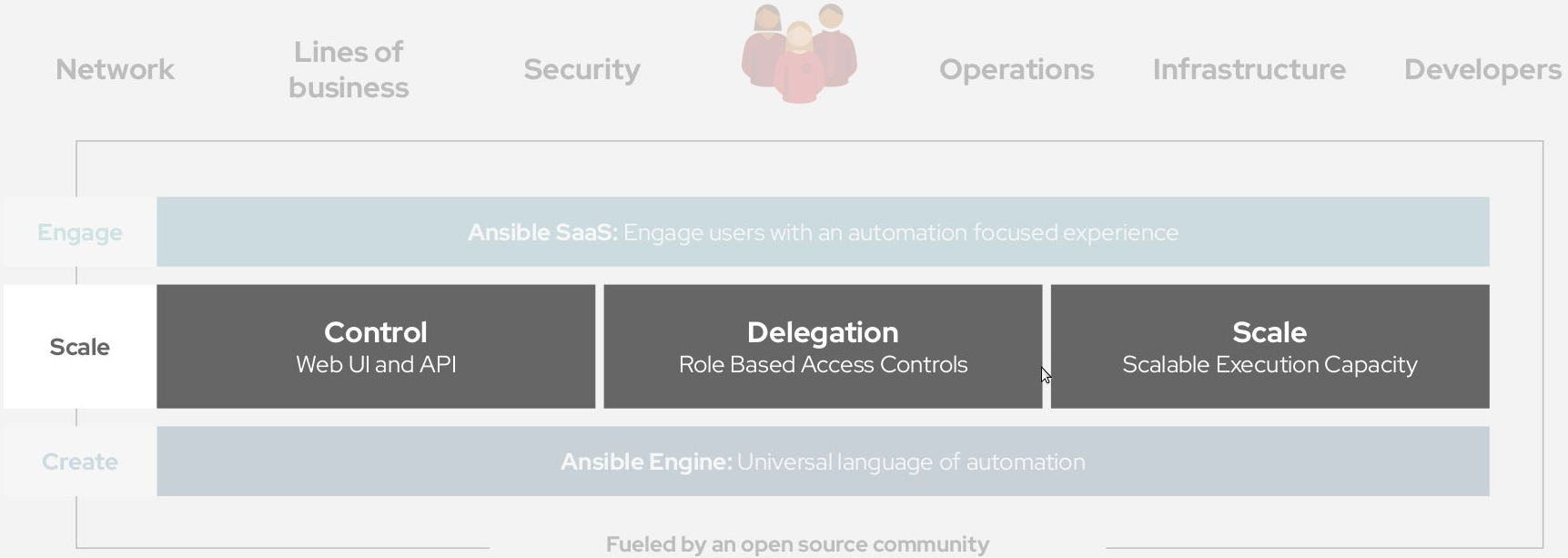
Red Hat
Ansible Automation
Platform

Red Hat Ansible Tower:

Operate and control at scale

Red Hat

Red Hat Ansible Automation Platform



Red Hat

What is Ansible Tower?

Ansible Tower is a UI and RESTful API allowing you to scale IT automation, manage complex deployments and speed productivity.

- Role-based access control
- Deploy entire applications with push-button deployment access
- All automations are centrally logged
- Powerful workflows match your IT processes

Red Hat

Red Hat Ansible Tower

Push button

An intuitive user interface experience makes it easy for novice users to execute playbooks you allow them access to.

RESTful API

With an API first mentality every feature and function of Tower can be API driven. Allow seamless integration with other tools like ServiceNow and Infoblox.

RBAC

Allow restricting playbook access to authorized users. One team can use playbooks in check mode (read-only) while others have full administrative abilities.

Enterprise integrations

Integrate with enterprise authentication like TACACS+, RADIUS, Azure AD. Setup token authentication with OAuth 2. Setup notifications with PagerDuty, Slack and Twilio.

Centralized logging

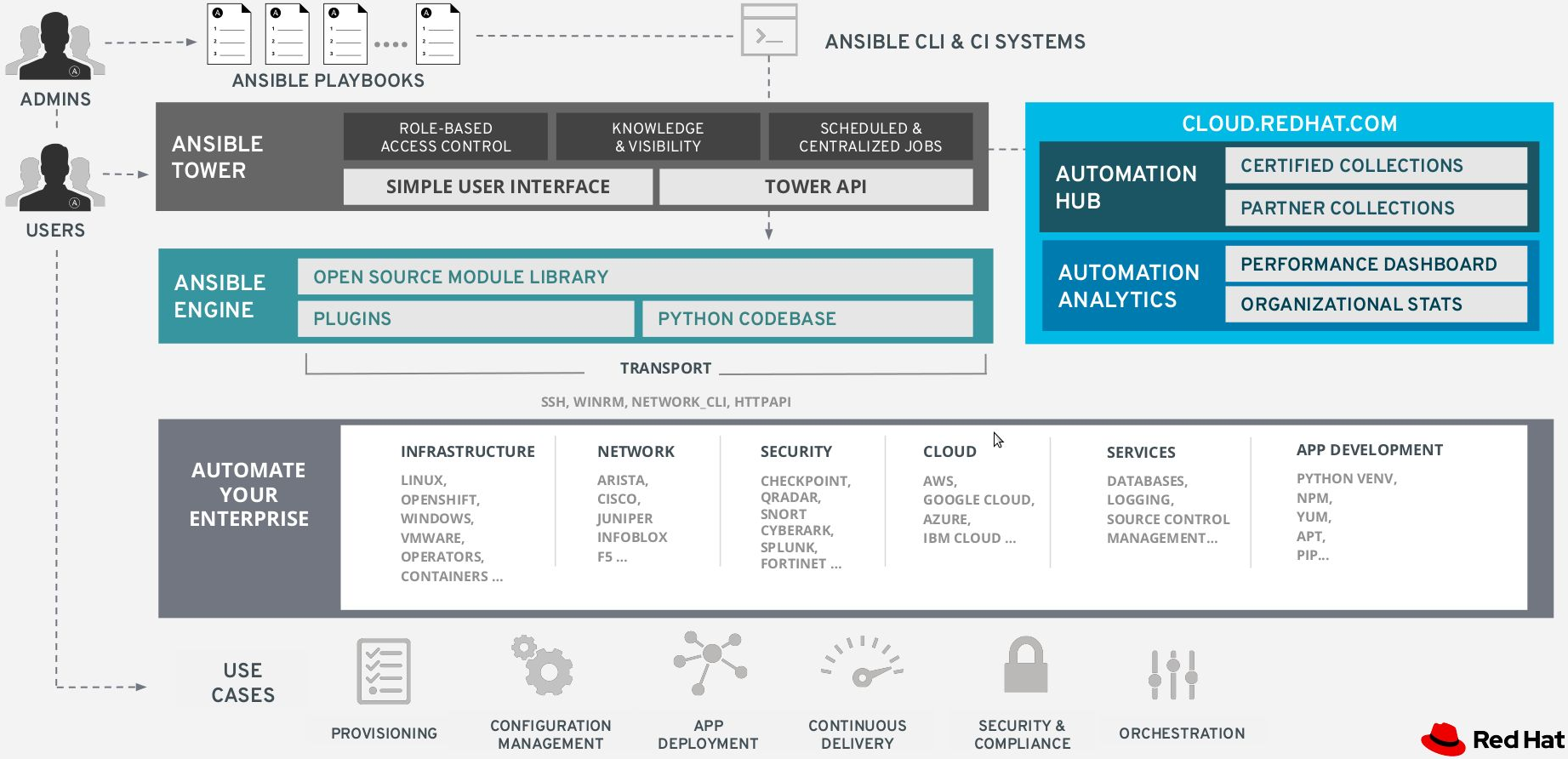
All automation activity is securely logged. Who ran it, how they customized it, what it did, where it happened - all securely stored and viewable later, or exported through Ansible Tower's API.

Workflows

Ansible Tower's multi-playbook workflows chain any number of playbooks, regardless of whether they use different inventories, run as different users, run at once or utilize different credentials.

Red Hat

Ansible Automation Platform



Red Hat

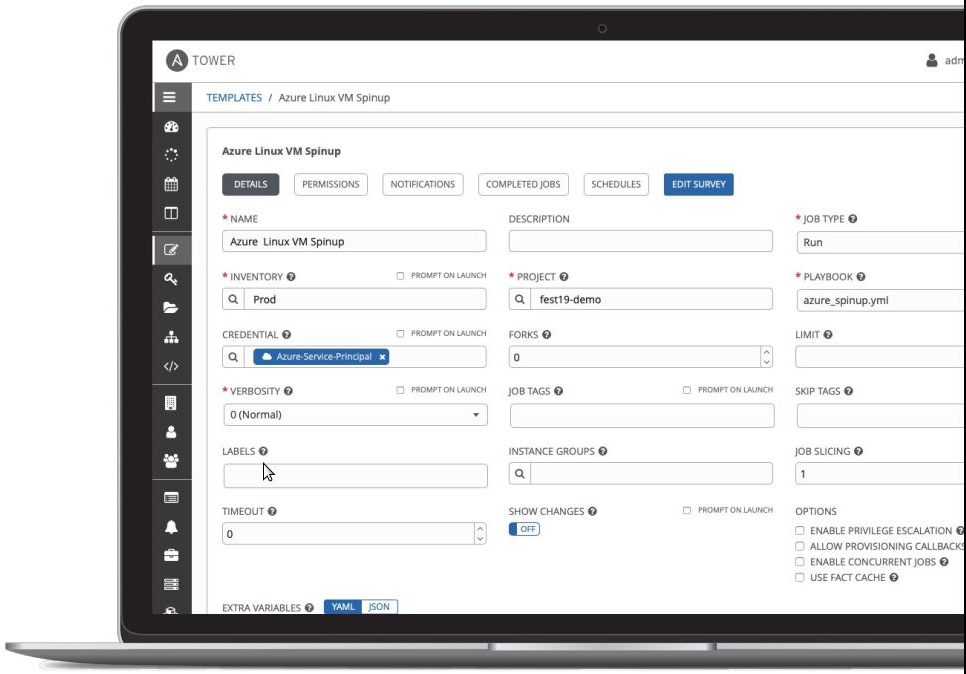
Job Templates

Everything in Ansible Tower revolves around the concept of a **Job Template**. Job Templates allow Ansible Playbooks to be controlled, delegated and scaled for an organization.

Job templates also encourage the reuse of Ansible Playbook content and collaboration between teams.

A **Job Template** requires:

- An **Inventory** to run the job against
- A **Credential** to login to devices.
- A **Project** which contains Ansible Playbooks

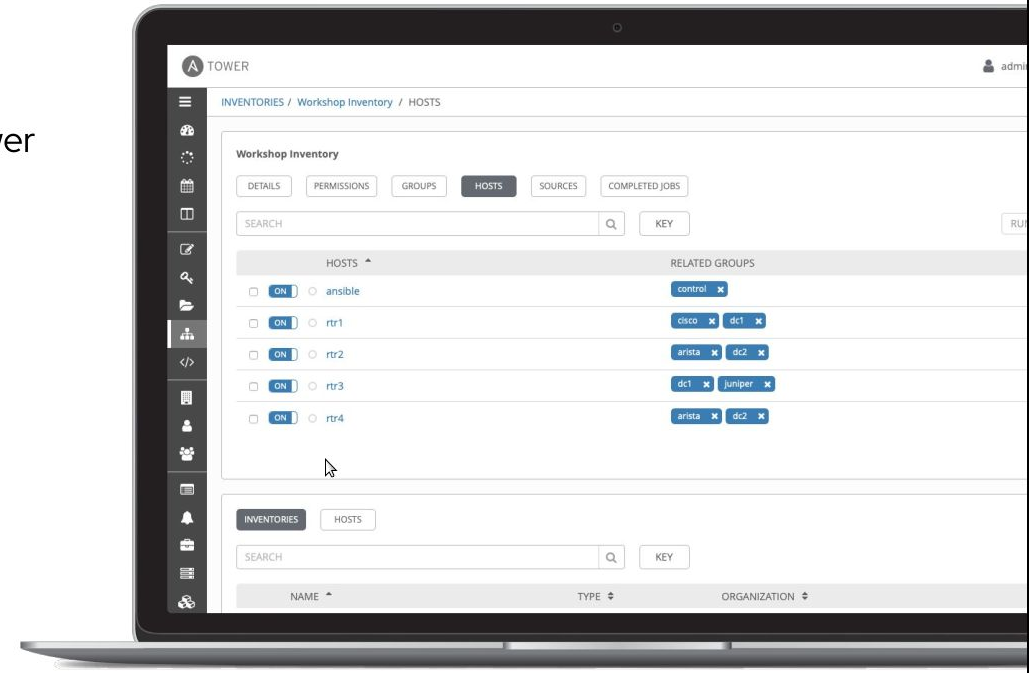


Red Hat

Inventory

Inventory is a collection of hosts (nodes) with associated data and groupings that Ansible Tower can connect to and manage.

- Hosts (nodes)
- Groups
- Inventory-specific data (variables)
- Static or dynamic sources



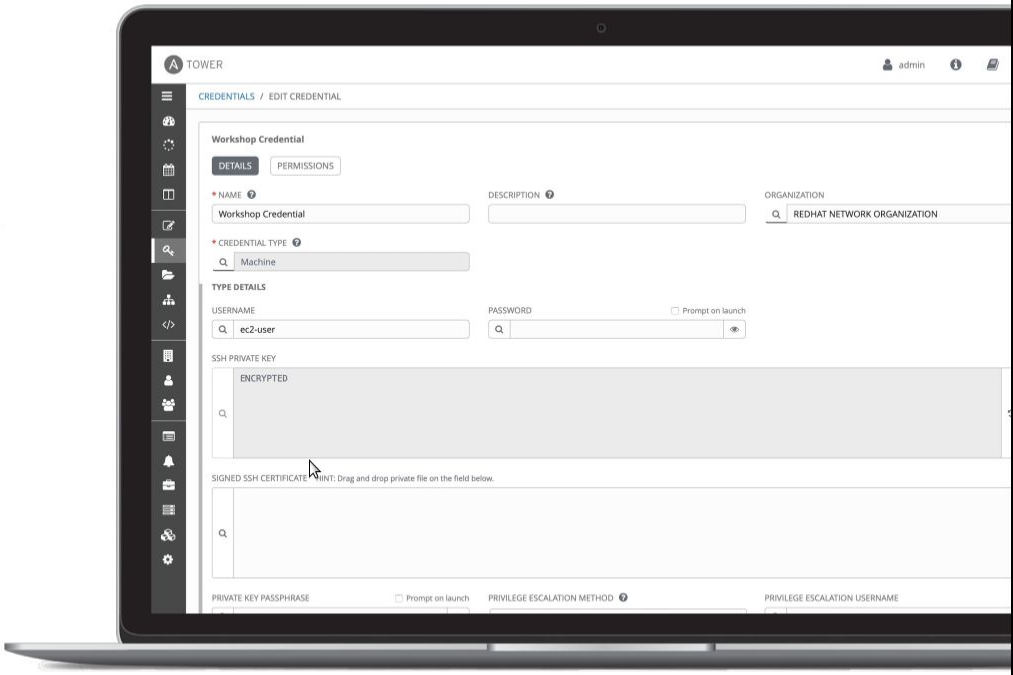
Red Hat

Credentials

Credentials are utilized by Ansible Tower for authentication with various external resources:

- Connecting to remote machines to run jobs
- Syncing with inventory sources
- Importing project content from version control systems
- Connecting to and managing network devices

Centralized management of various credentials allows end users to leverage a secret without ever exposing that secret to them.

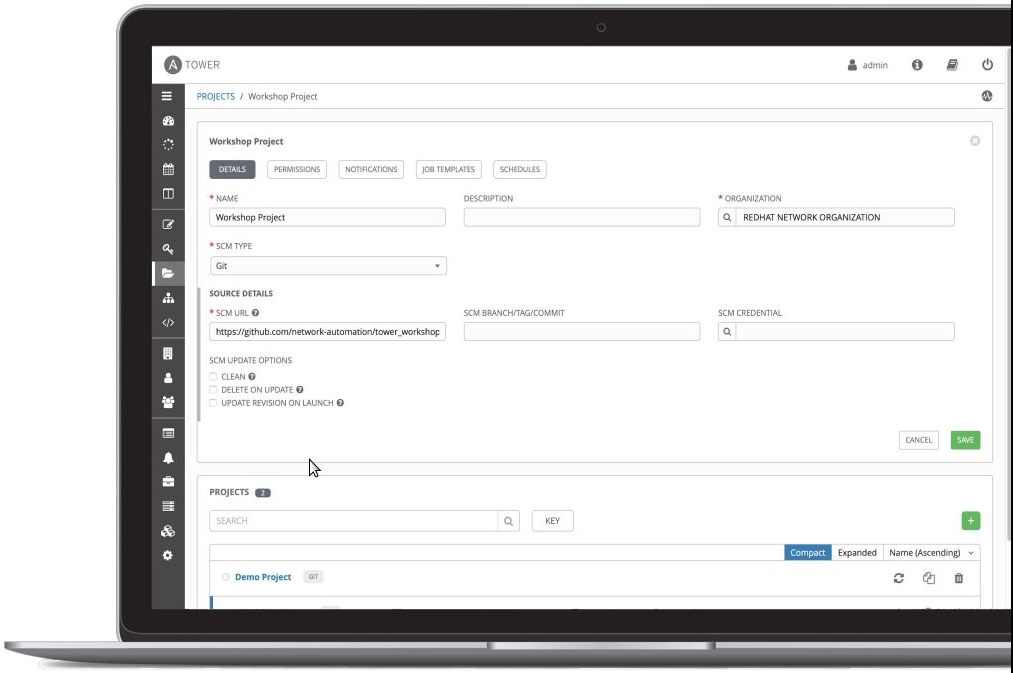


Red Hat

Project

A project is a logical collection of Ansible Playbooks, represented in Ansible Tower.

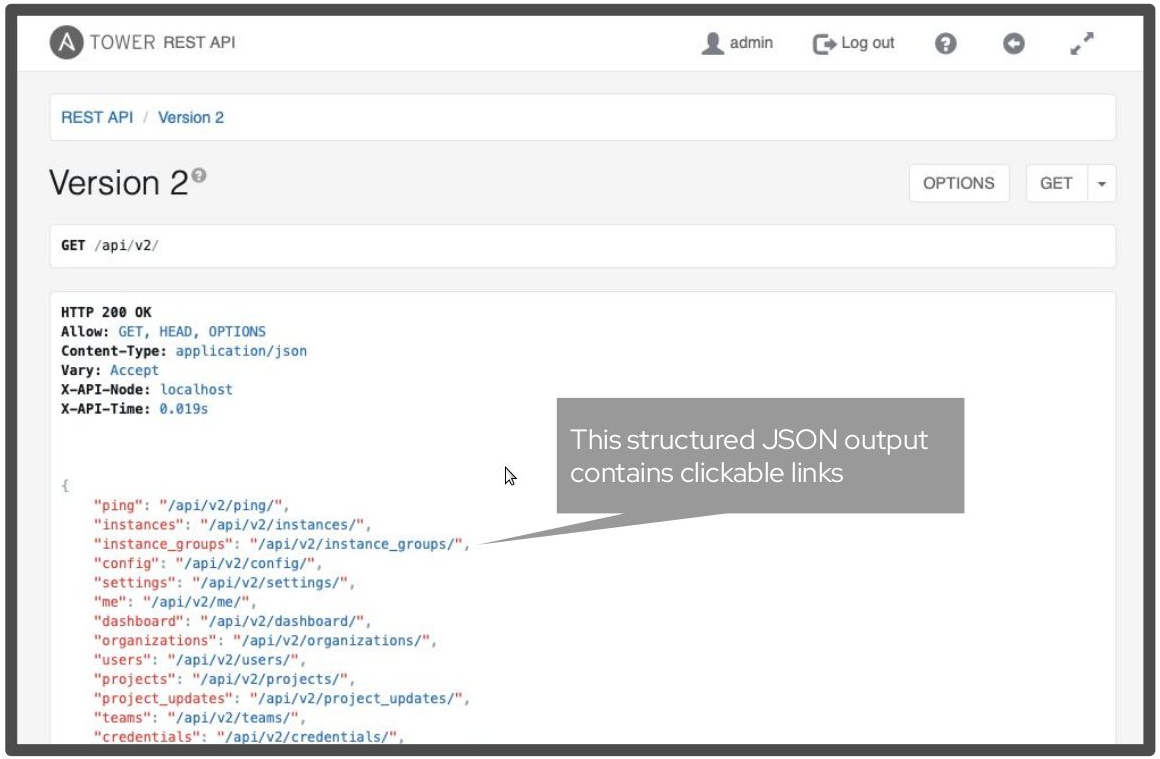
You can manage Ansible Playbooks and playbook directories by placing them in a source code management system supported by Ansible Tower, including Git, Subversion, and Mercurial.



Red Hat

RESTful API

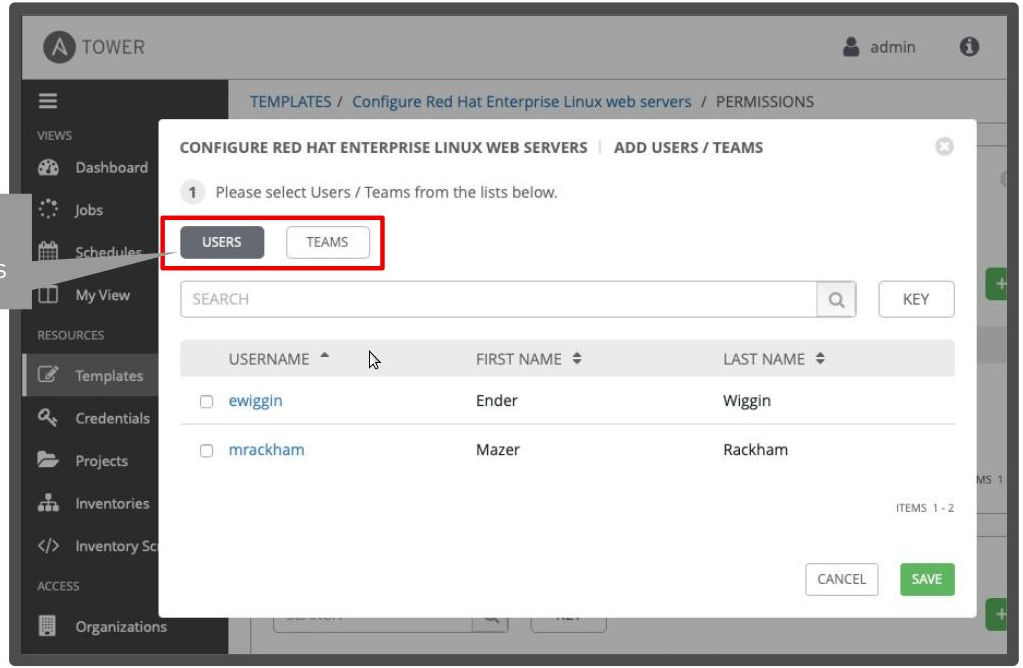
Fully browsable API, everything within the Web UI can be accessed via the API for programmatic access



Red Hat

Role Based Access Control (RBAC)

Job Templates, Inventory, Credentials and Projects can be assigned to specific Users and Teams.

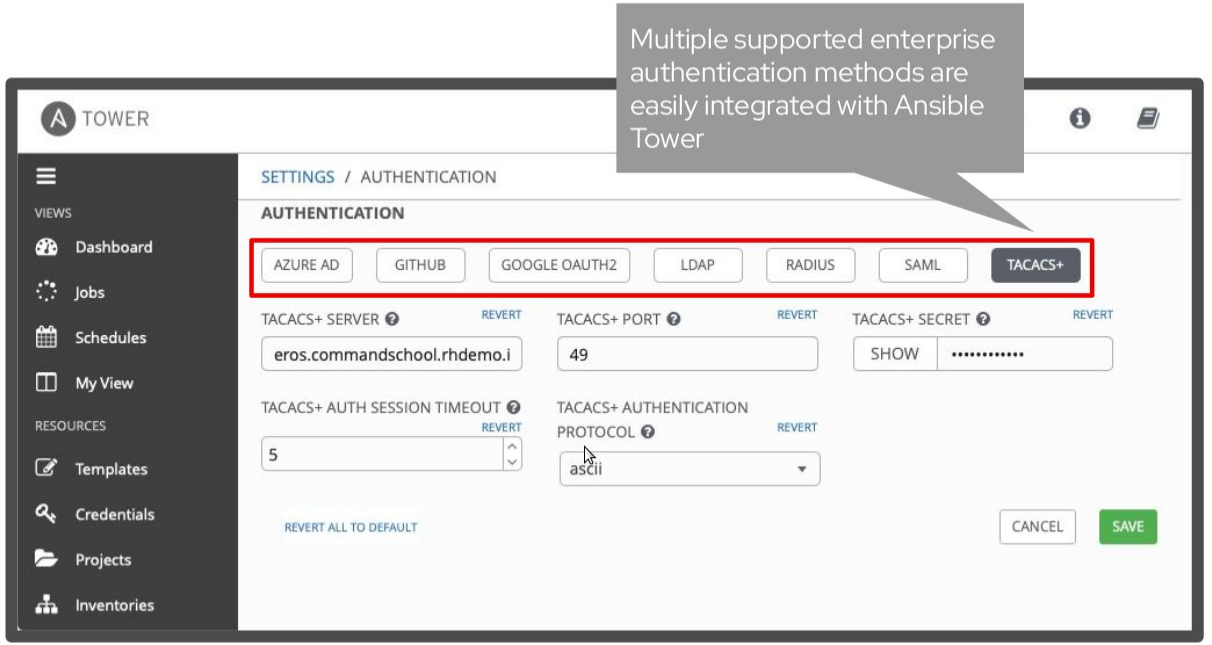


Red Hat

Enterprise Authentication

Use your existing enterprise authentication including:

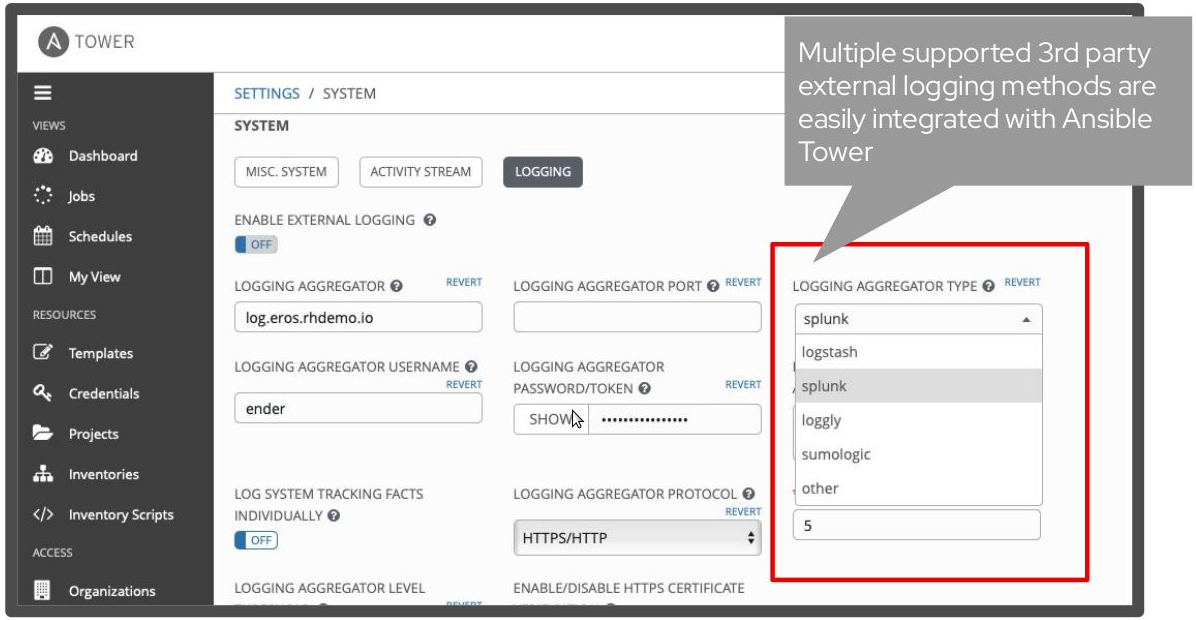
- Azure AD
- Github
- Google OAuth2
- LDAP
- Radius
- SAML
- TACACS+



Red Hat

Centralized Logging

Ansible Tower creates a centralized control point for Ansible Automation. If desired Ansible Tower can integrated with existing log aggregation services.



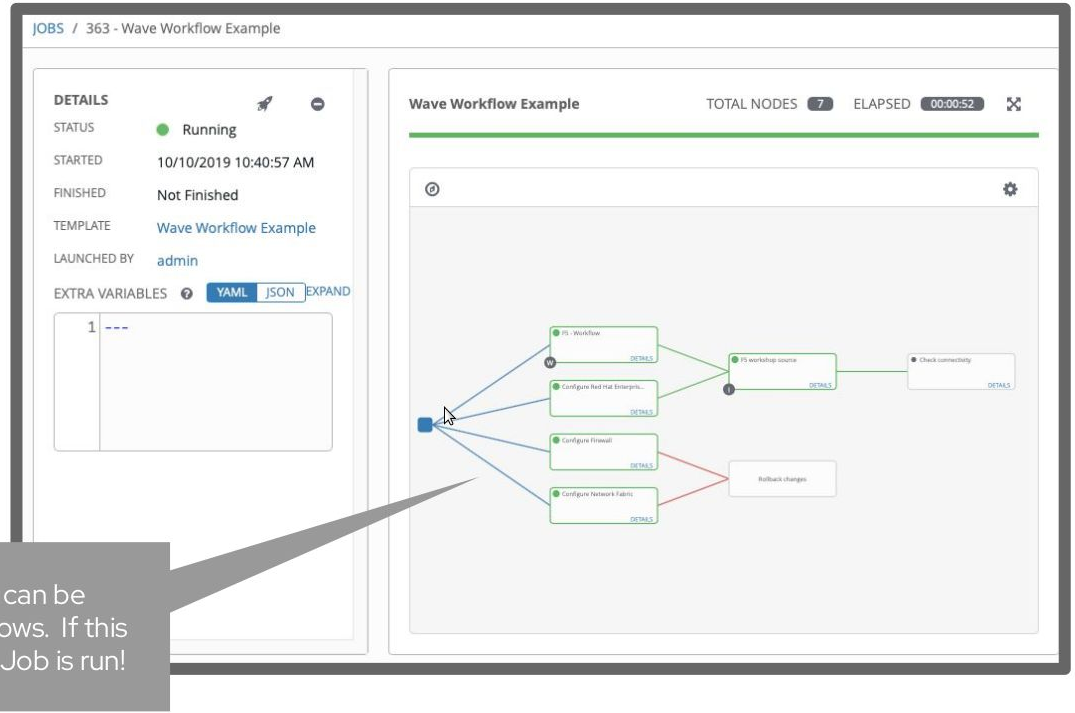
Red Hat

Workflows

Create powerful holistic automation using Ansible Workflows.

Orchestration can easily be configured by linking Job Templates.

Workflow approvals allow Workflows to pause and wait for human interaction



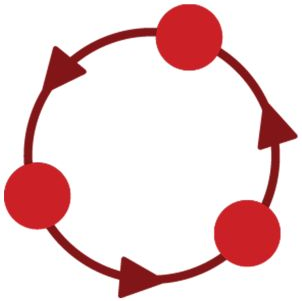
Conditional logic can be applied to workflows. If this job fails this next Job is run!

Red Hat

Webhooks - Enabling GitOps

Trigger Job Templates or Workflows straight via configurable webhooks

Automatically provision, update, configure, and apply based on pushes to your source control.

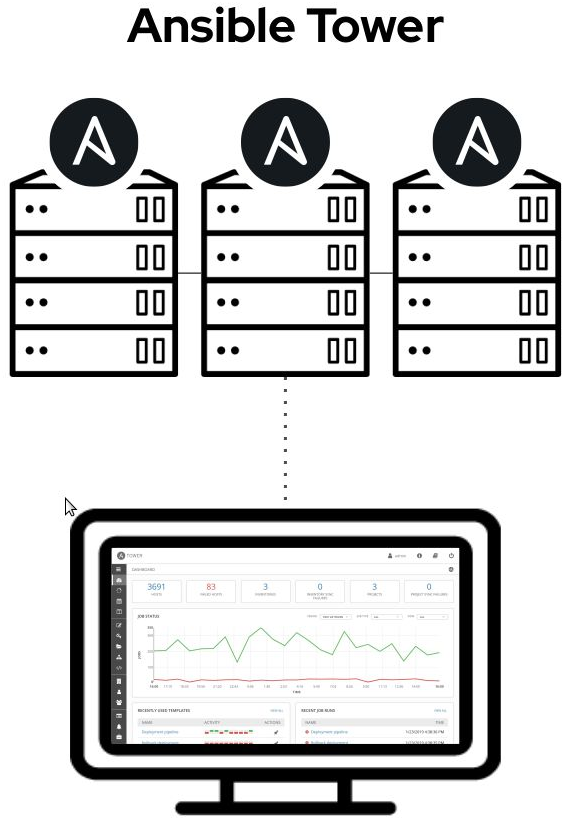


Red Hat

Scale

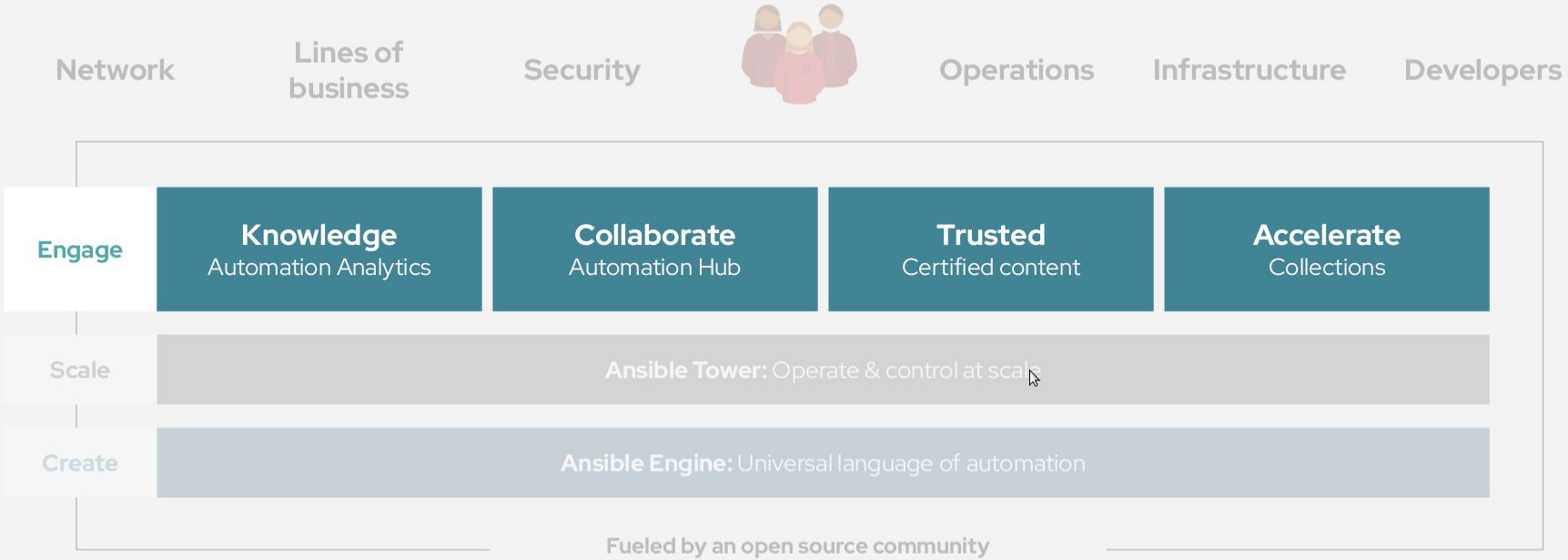
Ansible Tower clusters add redundancy and capacity, allowing you to scale Ansible automation across your enterprise.

- Unifying task execution across execution nodes
- Leverage Kubernetes and OpenShift to spin up execution capacity at runtime
- Expand execution to be able to pull jobs from a central Ansible Tower infrastructure



Red Hat

Red Hat Ansible Automation Platform



Red Hat

Ansible Content Collections

Simplified and consistent content delivery

Provides quick benefit by lowering barriers to automation

Streamlines tech partners providing direct-to-user automation

Simplifies internal collaboration, distribution, versioning

Ability to distribute, share and consume content at your own pace

Red Hat

Ansible Content Collection example

Directory Layout

```
.
├── galaxy.yml
├── plugins
│   ├── action
│   │   └── ping.py
│   ├── module_utils
│   │   └── pingutils.py
│   └── modules
│       └── ping.py
└── roles
    ├── ping_bootstrap
    │   ├── defaults
    │   ├── filters
    │   ├── meta
    │   ├── tasks
    │   └── vars
    └── ping_deploy
        ├── defaults
        ├── meta
        └── tasks
```

In a playbook

```yaml
hosts: somehosts
collections:
  - custom.pinger
  - redhat.open_ping

tasks:
  - custom.pinger.ping:

  - ansible.builtin.ping: # use only the ping packaged in core

  - ansible.legacy.ping: # use core or library(etc)/ping.py
    when: thing | custom.pinger.filter == 42

  - ping: # searches collections “path” otherwise…
          # still works, == ansible.legacy.ping:
```

Red Hat

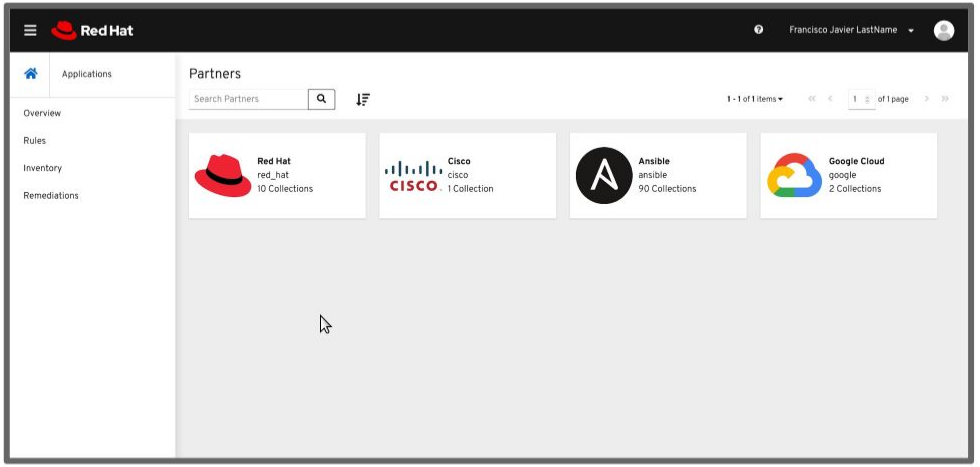
Automation Hub

Discover, publish, and manage Collections

Quickly discover available Red Hat and certified content through Collections.

Manage and test your organization's view of available content.*

Manage your locally available automation via on-premise.*



Red Hat

Next steps:

Get started

ansible.com/get-started

ansible.com/tower-trial

Join the community

ansible.com/community

Workshops and training

ansible.com/workshops

Red Hat Training

Share your story

Follow us @Ansible

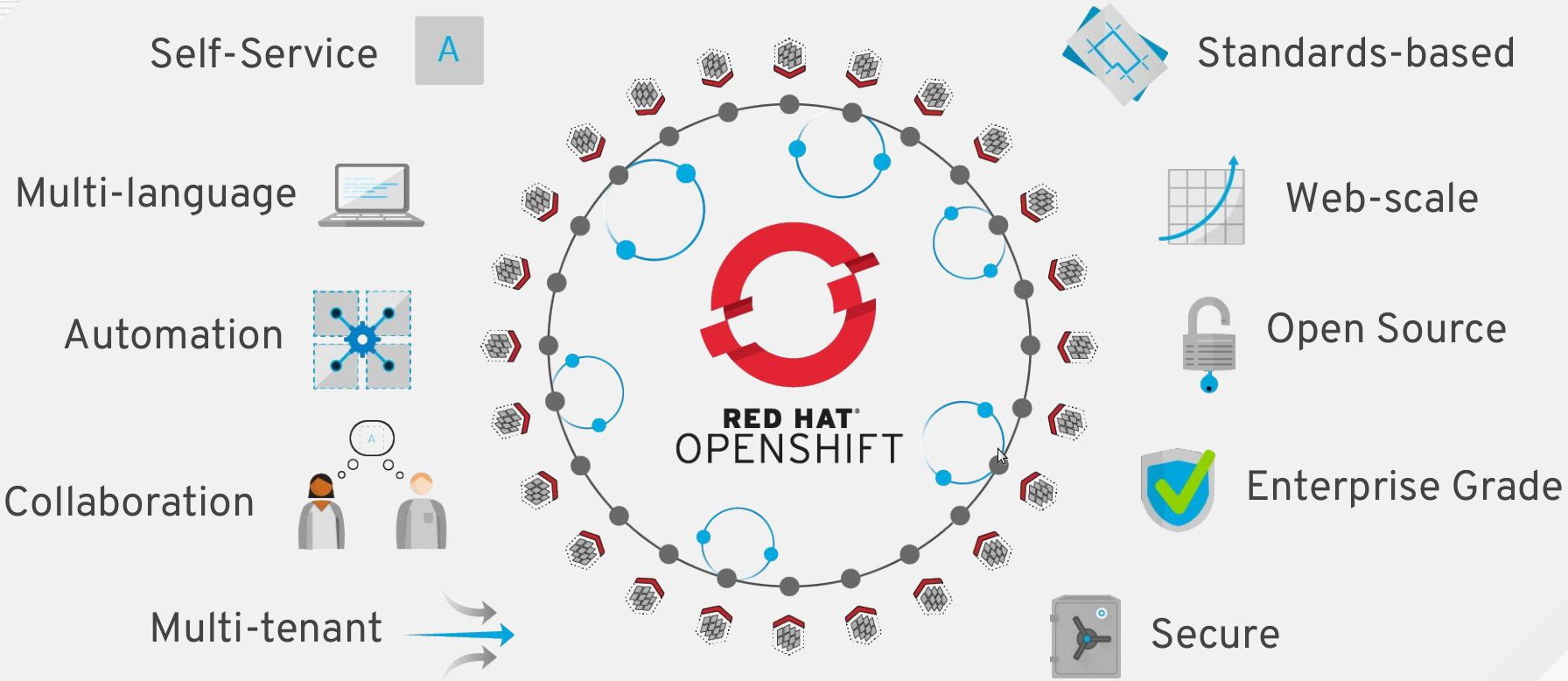
Friend us on Facebook

Red Hat

redhat.

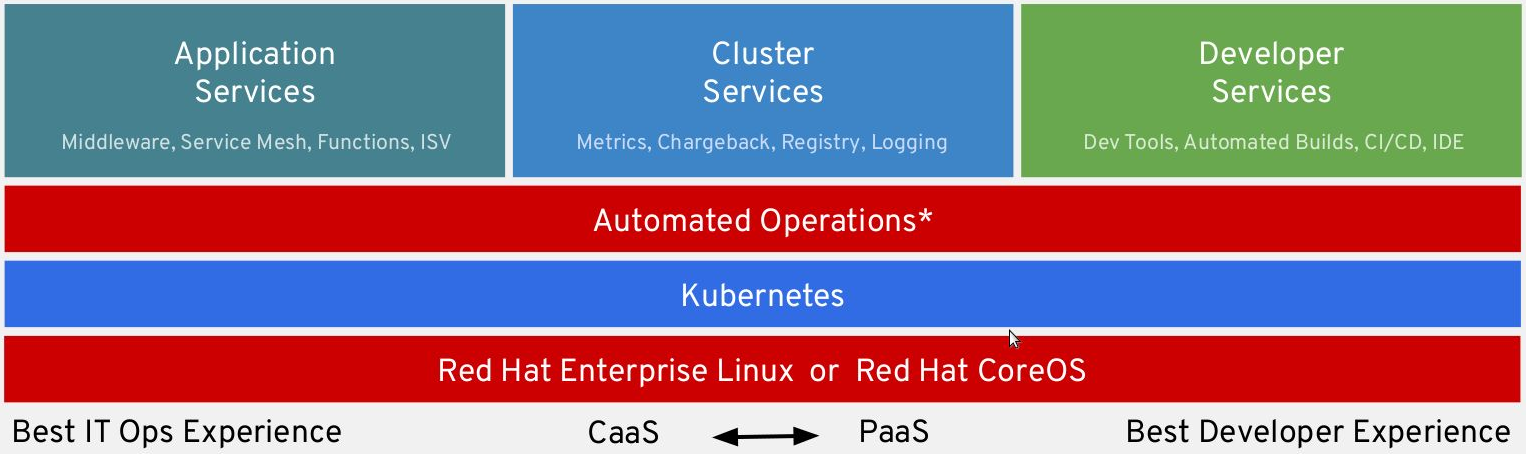
OPENSHIFT CONTAINER PLATFORM TECHNICAL OVERVIEW

Chris Reynolds, RHCA
Senior Cloud Guy
cloudguy@redhat.com


Self-Service
Multi-language
Automation
Collaboration
Multi-tenant
RED HAT
OPENSHIFT
Standards-based
Web-scale
Open Source
Enterprise Grade
Secure

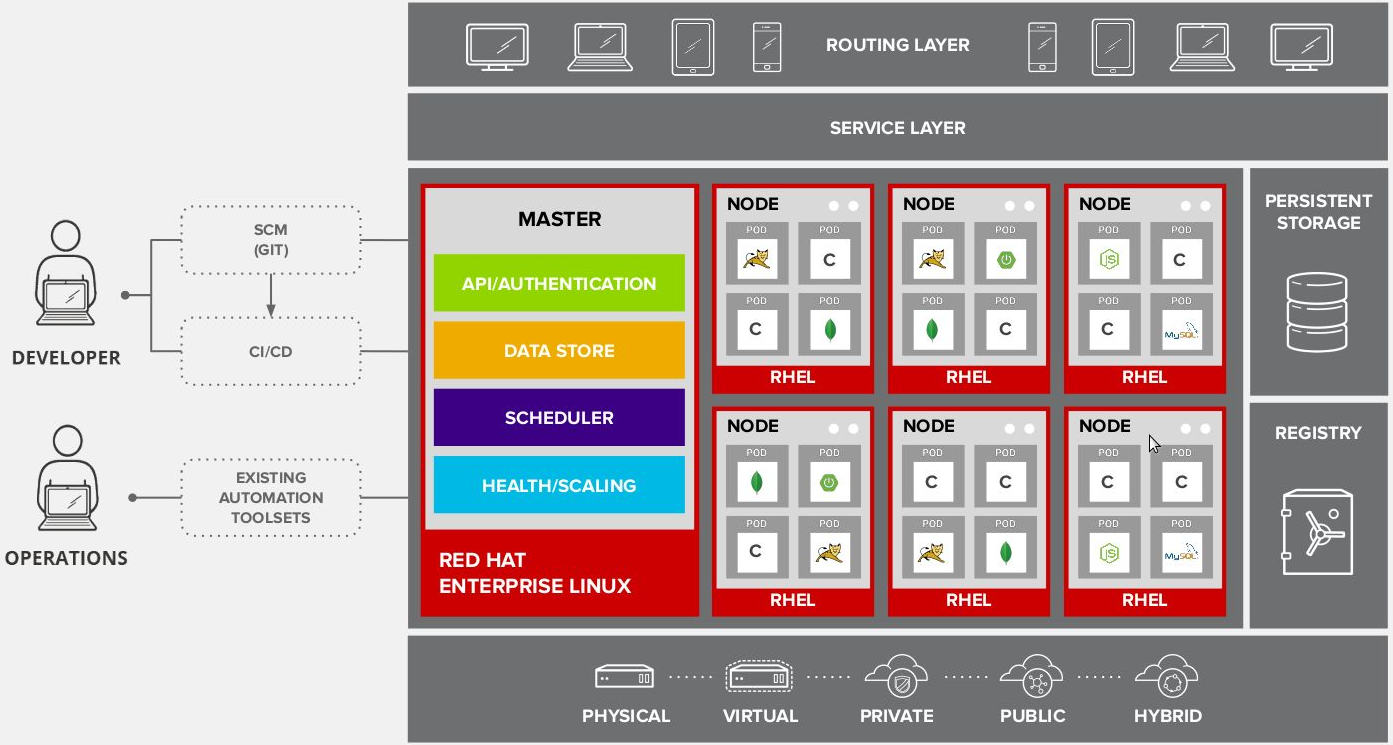
redhat.

OPENSHIFT CONTAINER PLATFORM



*coming soon

OPENSHIFT ARCHITECTURE

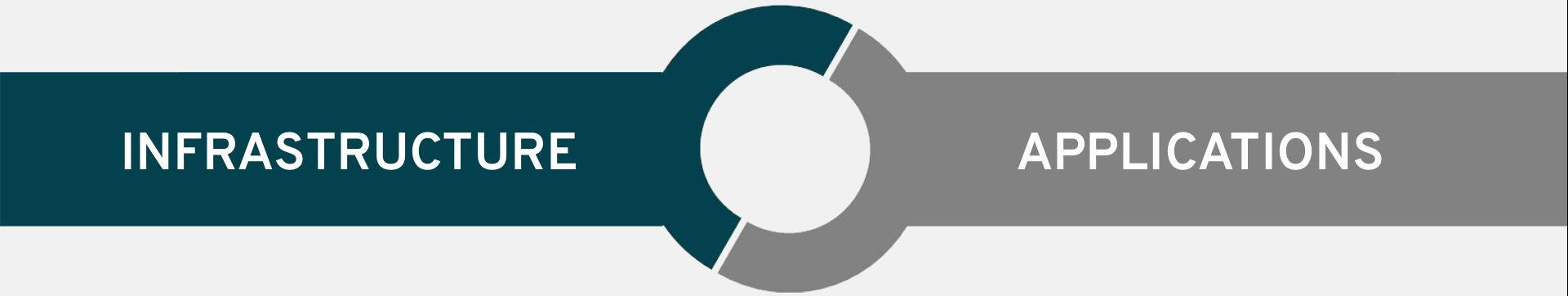


redhat.


LINUX CONTAINERS
redhat.

WHAT ARE CONTAINERS?

It Depends Who You Ask

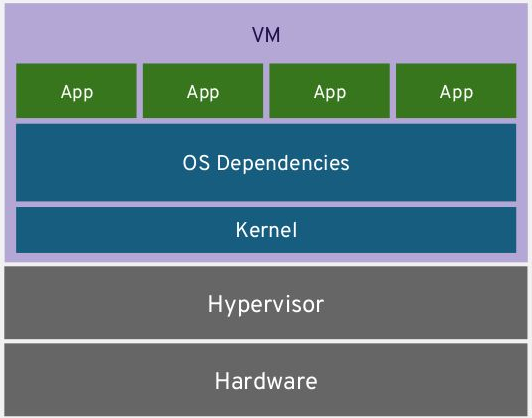


- Application processes on a shared kernel
- Simpler, lighter, and denser than VMs
- Portable across different environments

- Package apps with all dependencies
- Deploy to any environment in seconds
- Easily accessed and shared

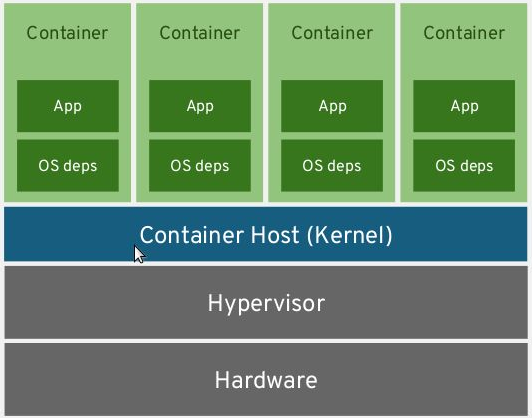
VIRTUAL MACHINES AND CONTAINERS

VIRTUAL MACHINES



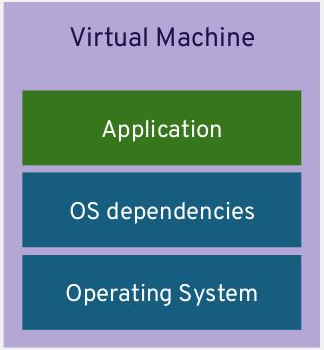
VM isolates the hardware

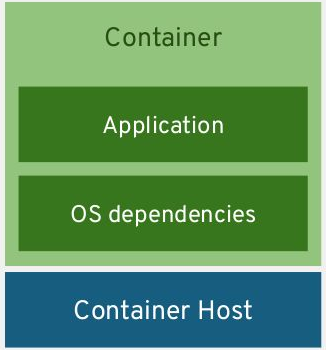
CONTAINERS



Container isolates the process

VIRTUAL MACHINES AND CONTAINERS

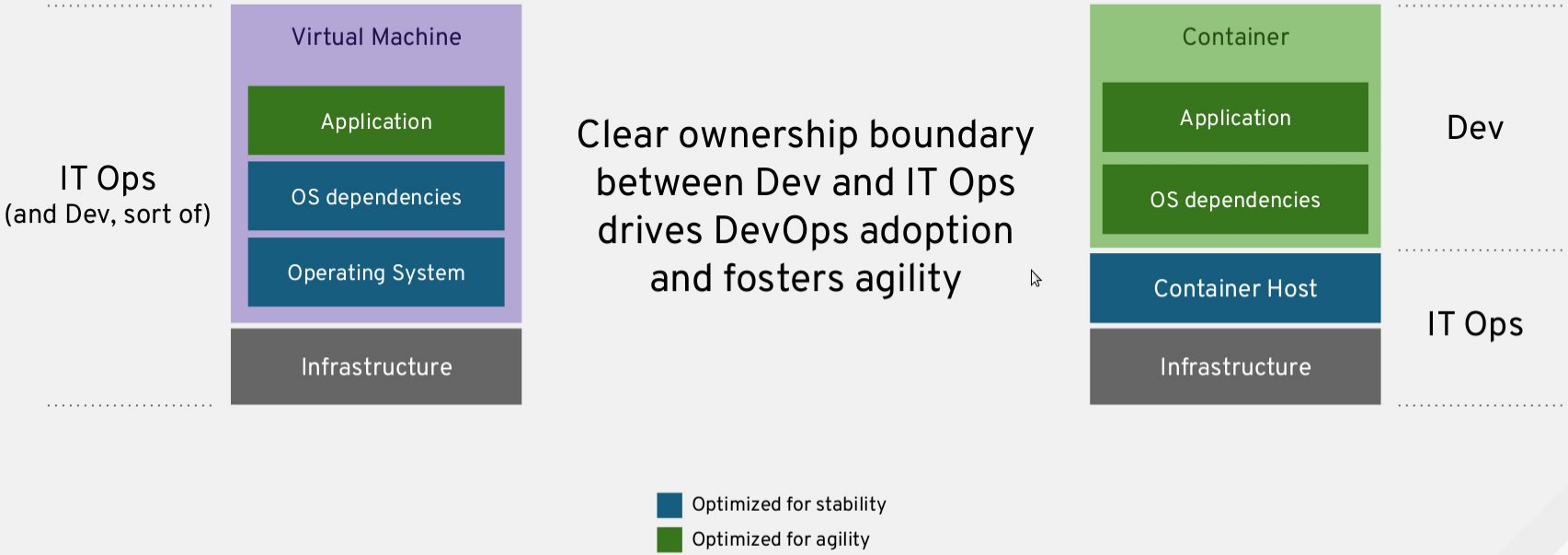




- ✚ VM Isolation
- ▬ Complete OS
- ▬ Static Compute
- ▬ Static Memory
- ▬ High Resource Usage

- ✚ Container Isolation
- ✚ Shared Kernel
- ✚ Burstable Compute
- ✚ Burstable Memory
- ✚ Low Resource Usage

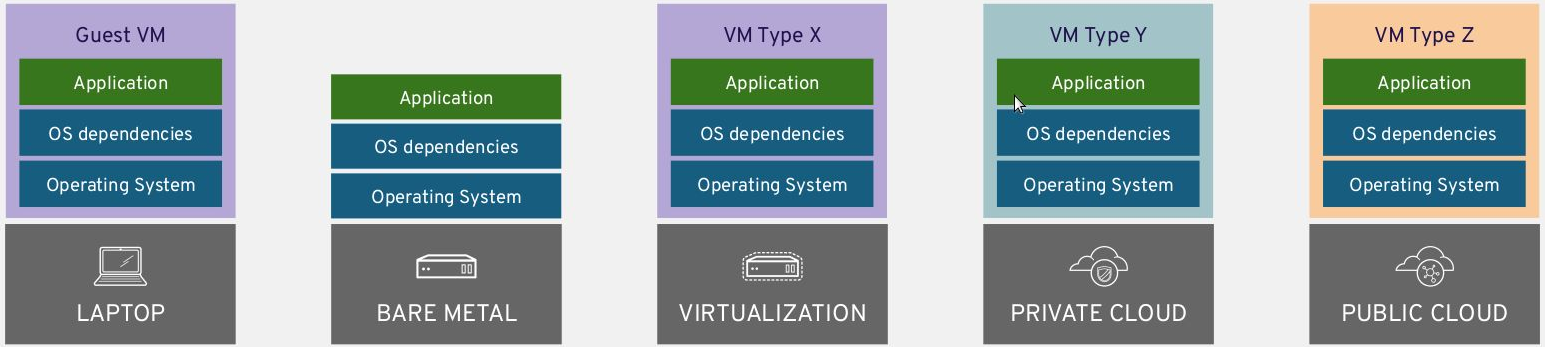
VIRTUAL MACHINES AND CONTAINERS



redhat.

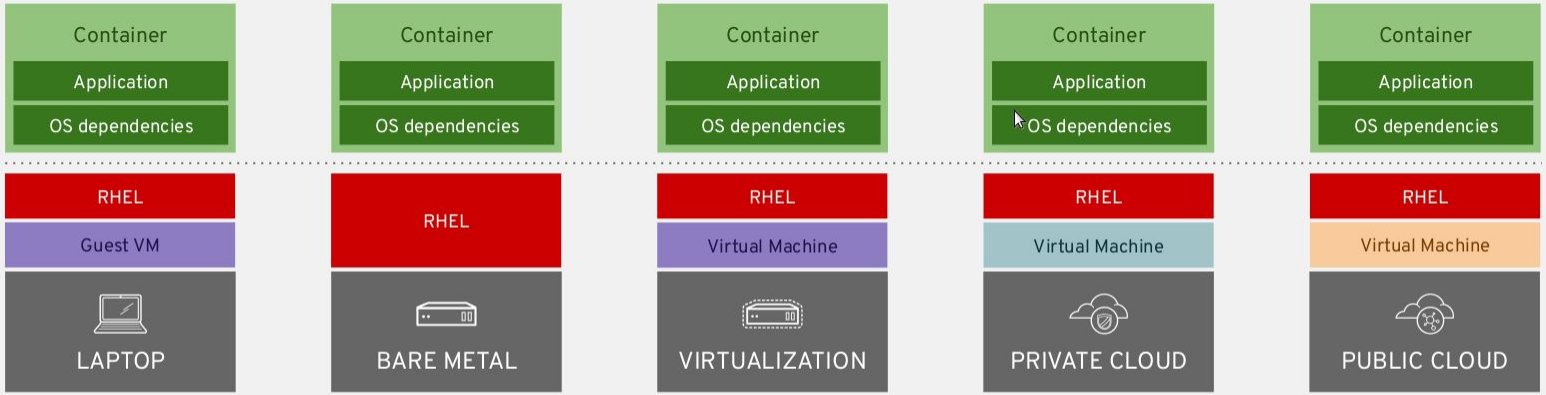
APPLICATION PORTABILITY WITH VM

Virtual machines are NOT portable across hypervisor and do NOT provide portable packaging for applications



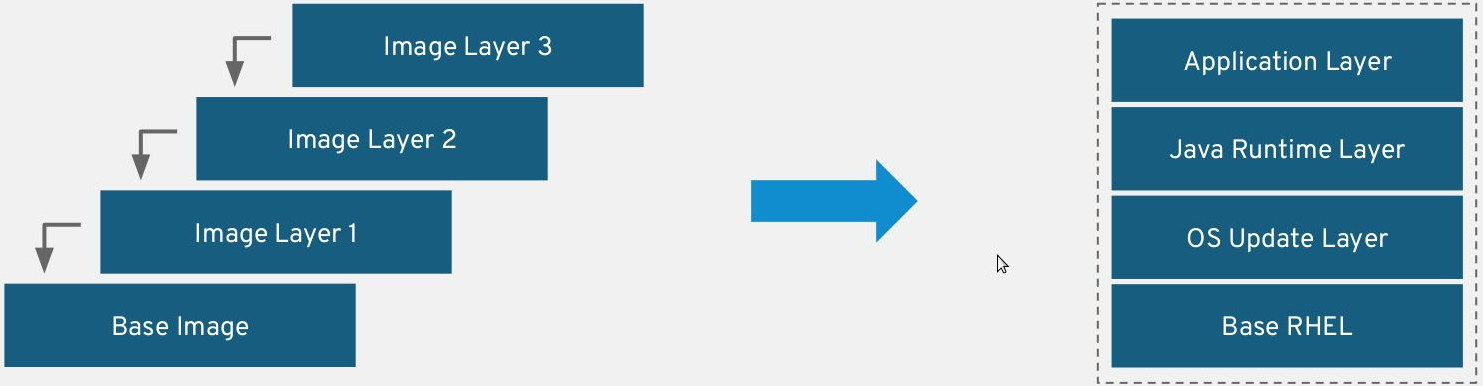
APPLICATION PORTABILITY WITH CONTAINERS

RHEL Containers + RHEL Host = Guaranteed Portability
Across Any Infrastructure



redhat.

RAPID SECURITY PATCHING USING CONTAINER IMAGE LAYERING



Container Image Layers

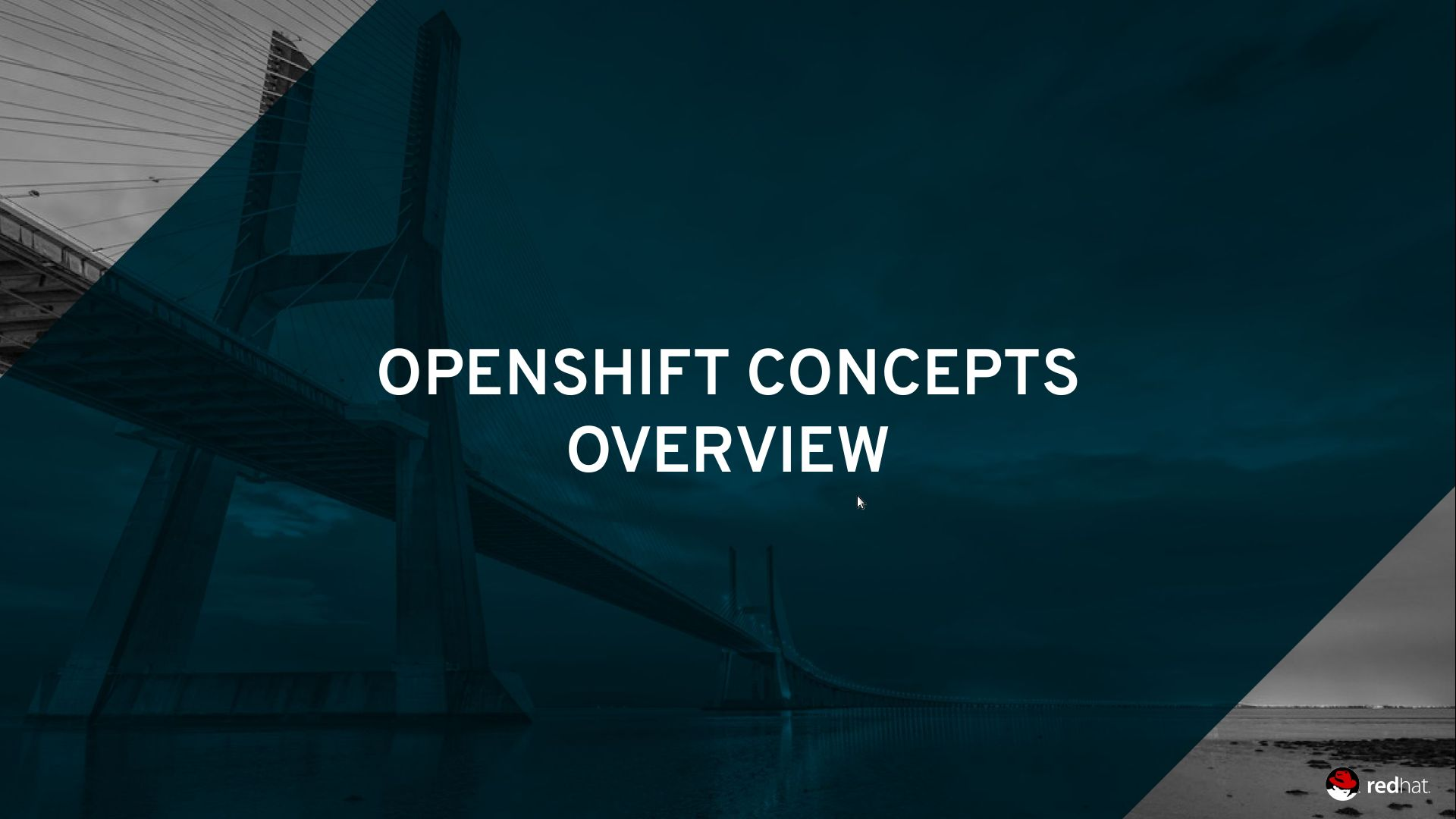
Example Container Image

cri-o

A lightweight, OCI-compliant container runtime

Minimal and Secure Architecture	Optimized for Kubernetes	Runs any OCI-compliant image (including docker)

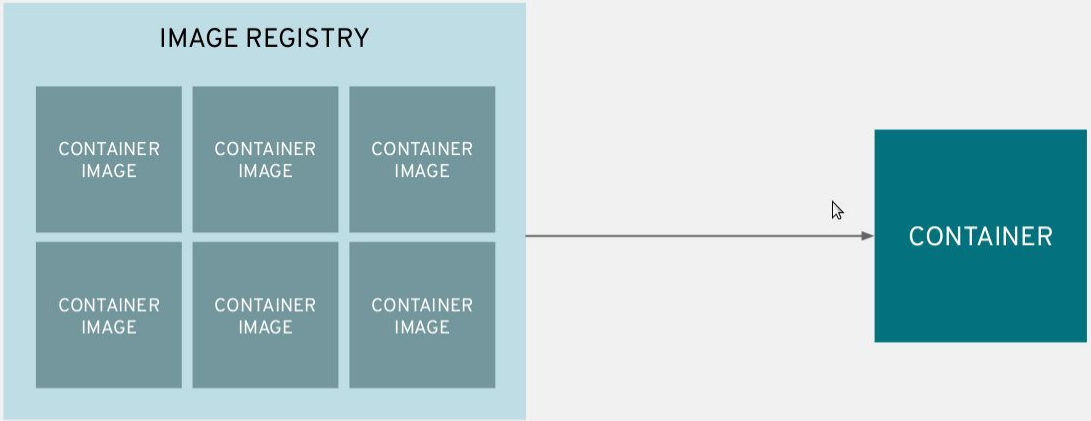
Optional runtime in OCP 3.10, default OCP 3.11+


OPENSHIFT CONCEPTS
OVERVIEW
redhat.

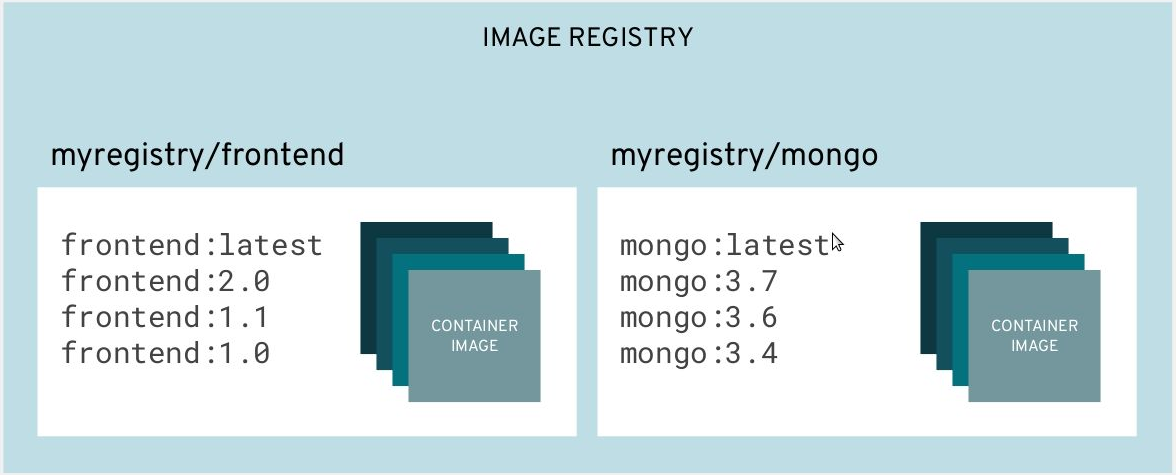
A container is the smallest compute unit

containers are created from container images

container images are stored in an image registry



an image repository contains all versions of an image in the image registry

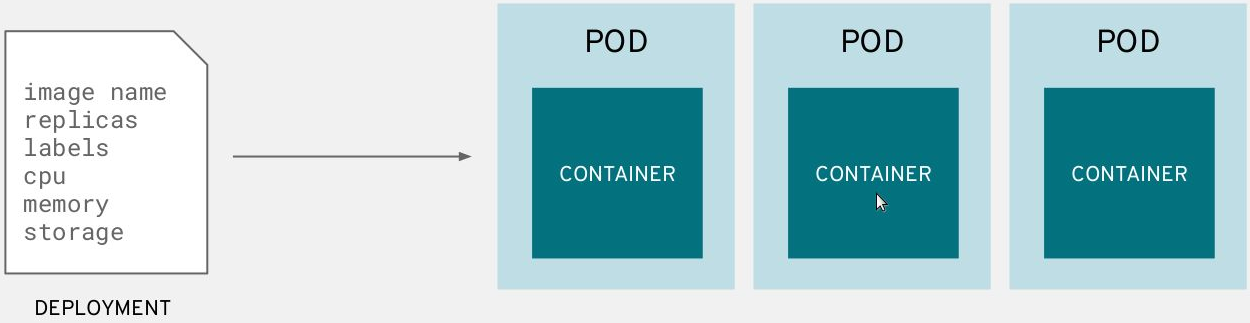


containers are wrapped in pods which are units of deployment and management

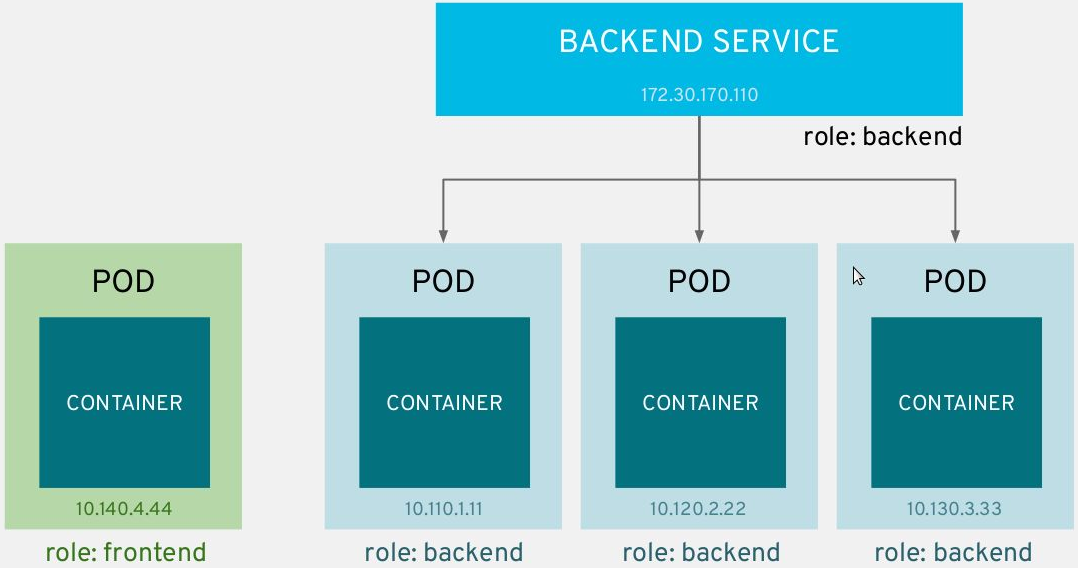
IP: 10.1.0.11

IP: 10.1.0.55

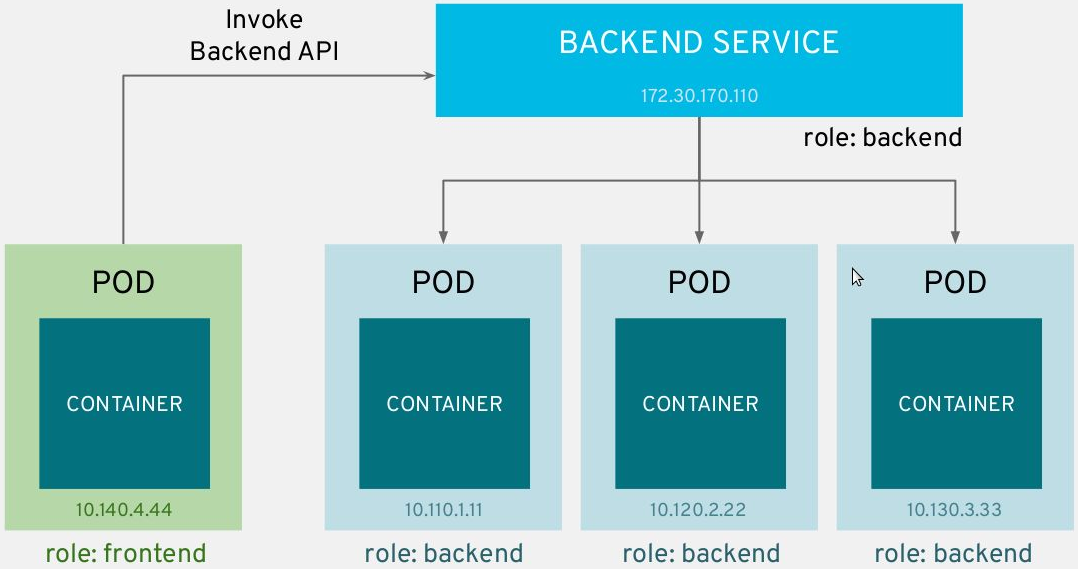
pods configuration is defined in a `deployment`



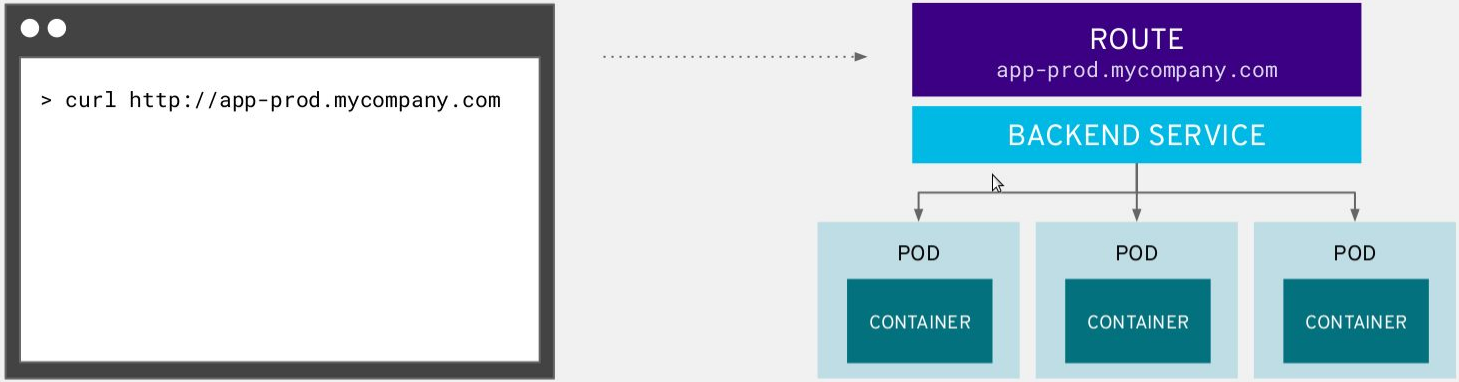
services provide internal load-balancing and service discovery across pods



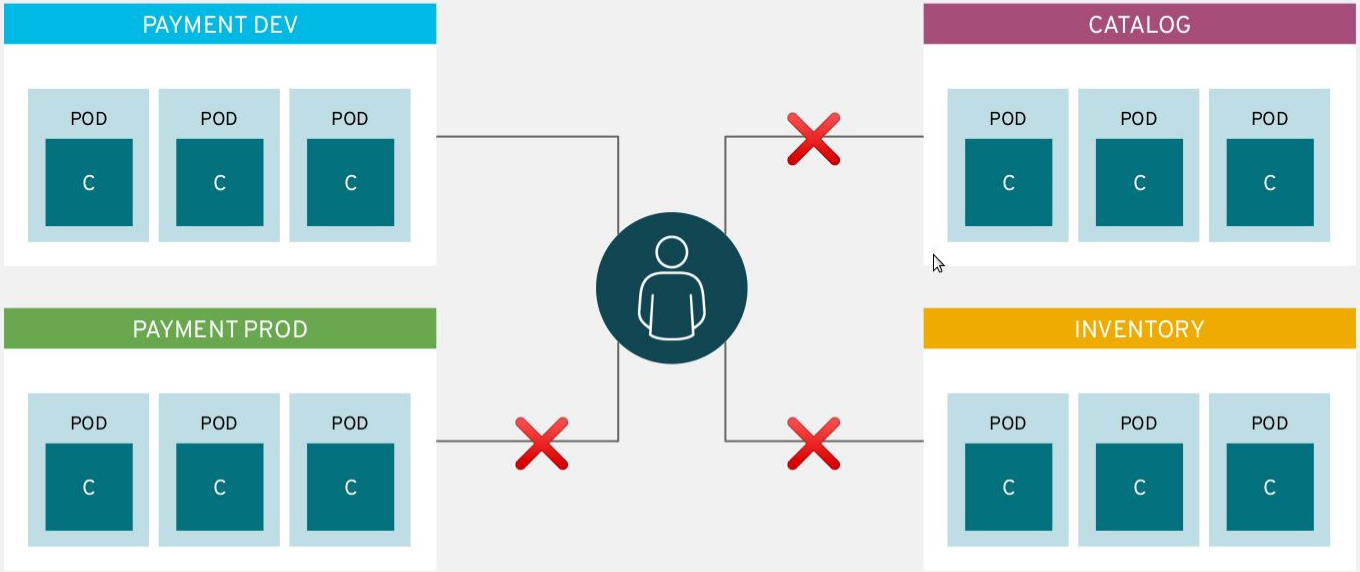
apps can talk to each other via services

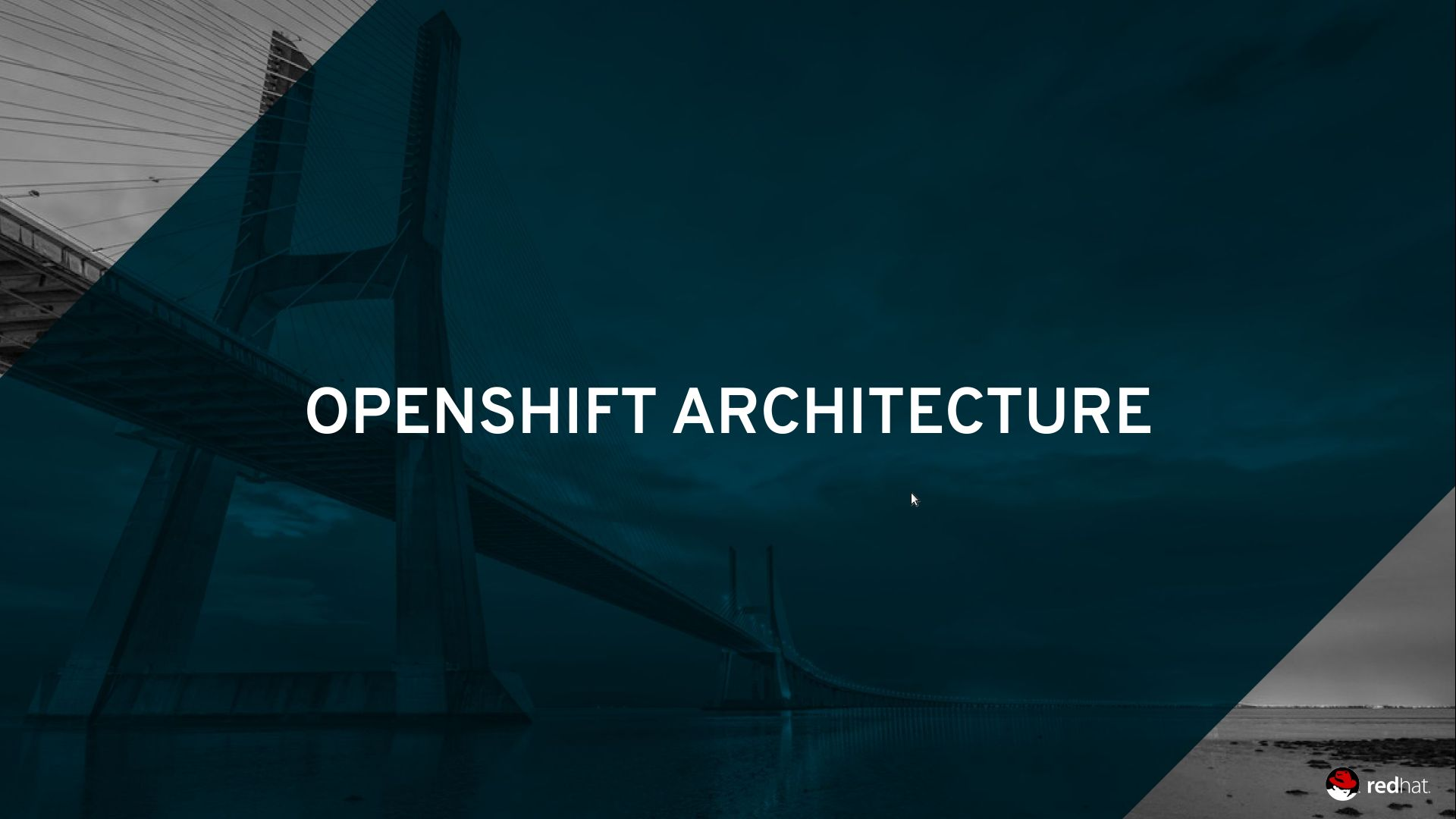


routes add services to the external load-balancer and provide readable urls for the app



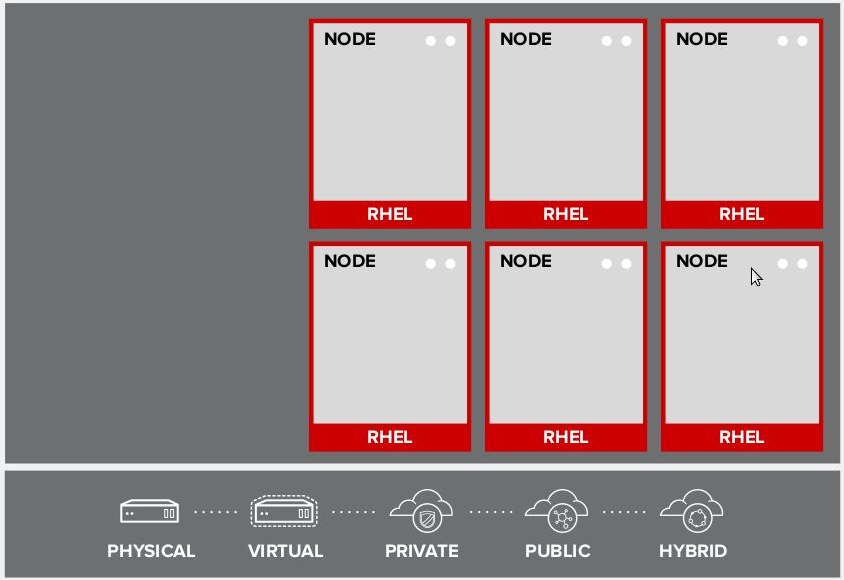
projects isolate apps across environments, teams, groups and departments



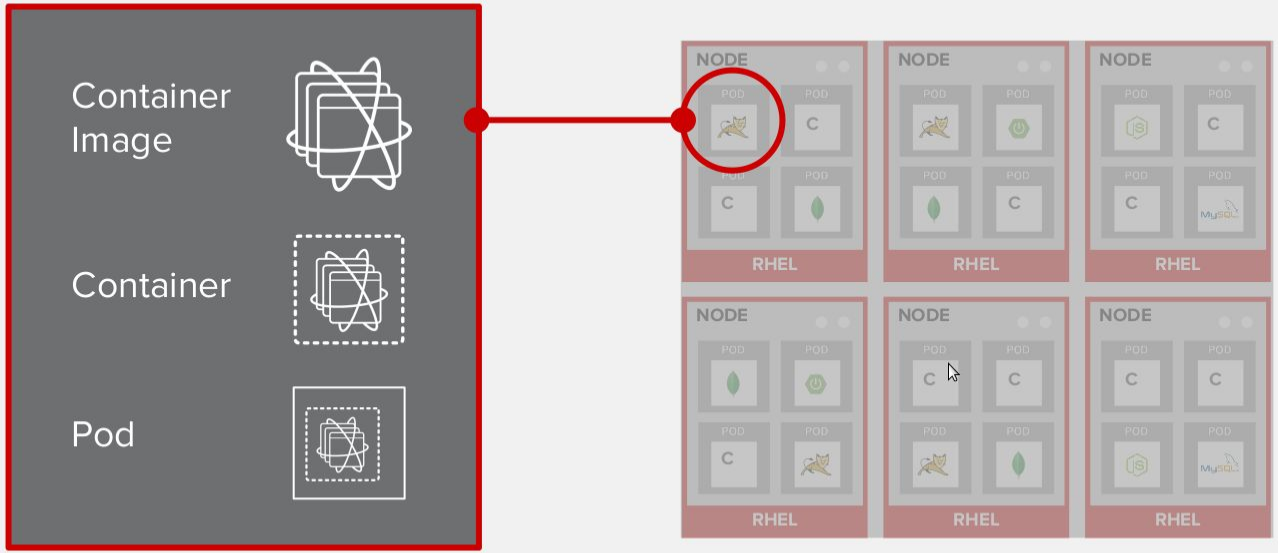

OPENSHIFT ARCHITECTURE

YOUR CHOICE OF INFRASTRUCTURE

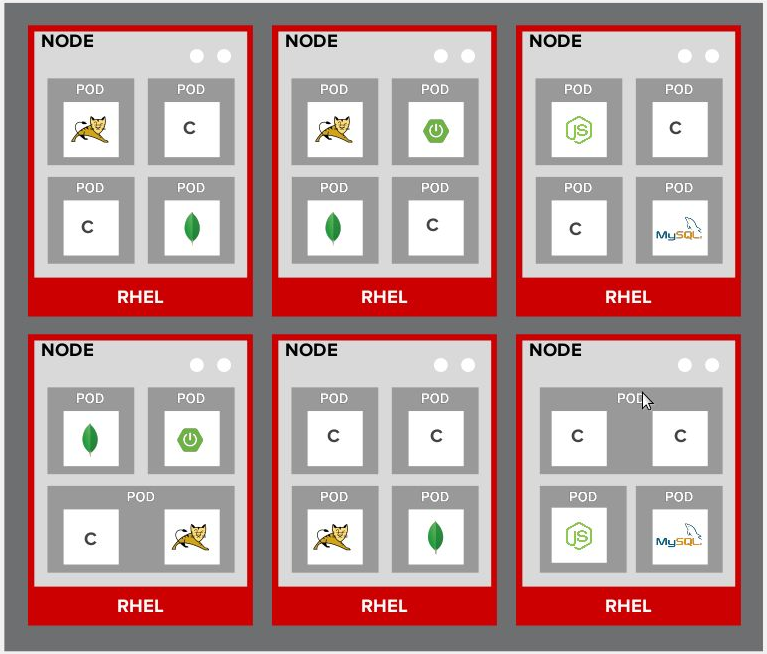
NODES RHEL INSTANCES WHERE APPS RUN



APPS RUN IN CONTAINERS

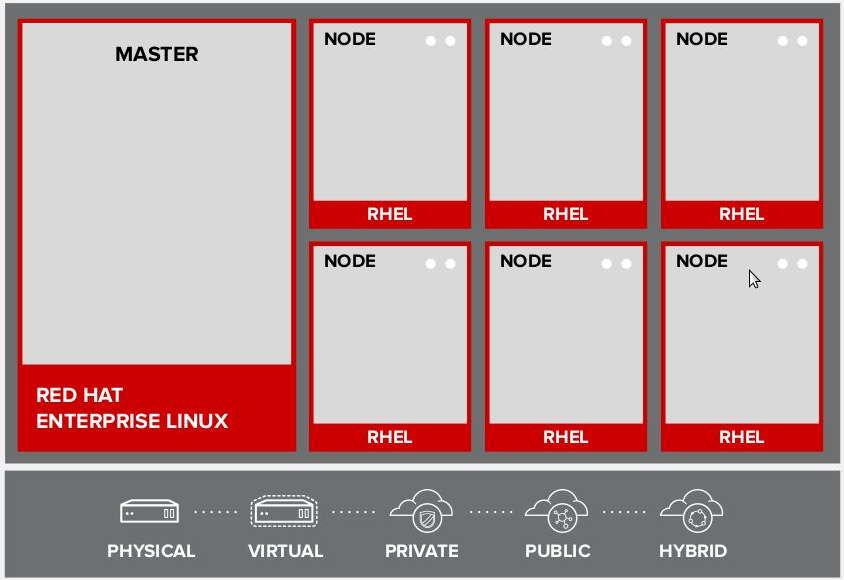


PODS ARE THE UNIT OF ORCHESTRATION

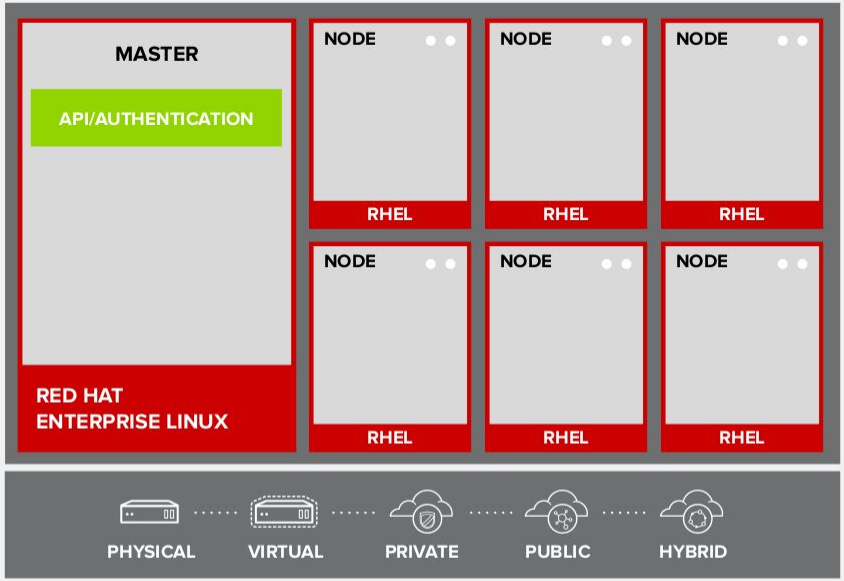


redhat.

MASTERS ARE THE CONTROL PLANE

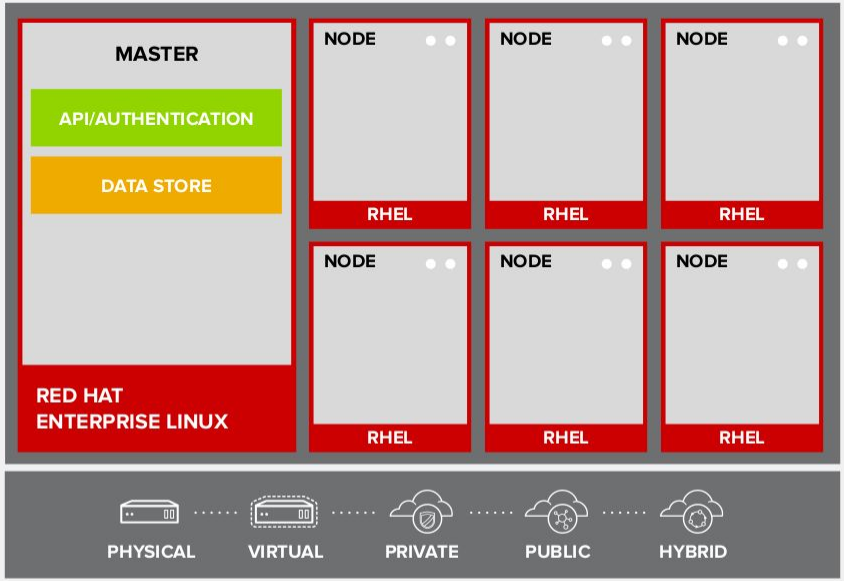


API AND AUTHENTICATION

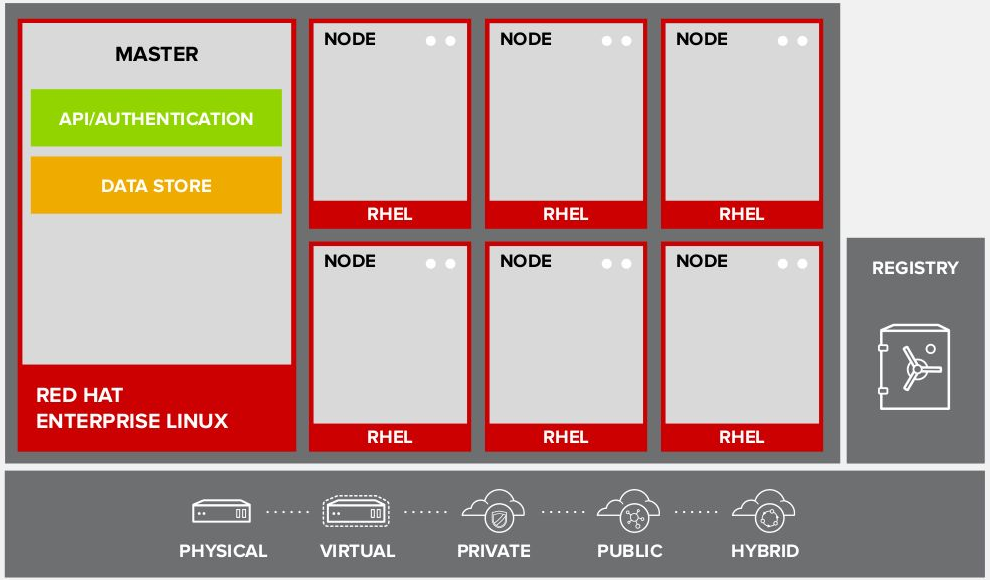


redhat.

DESIRED AND CURRENT STATE

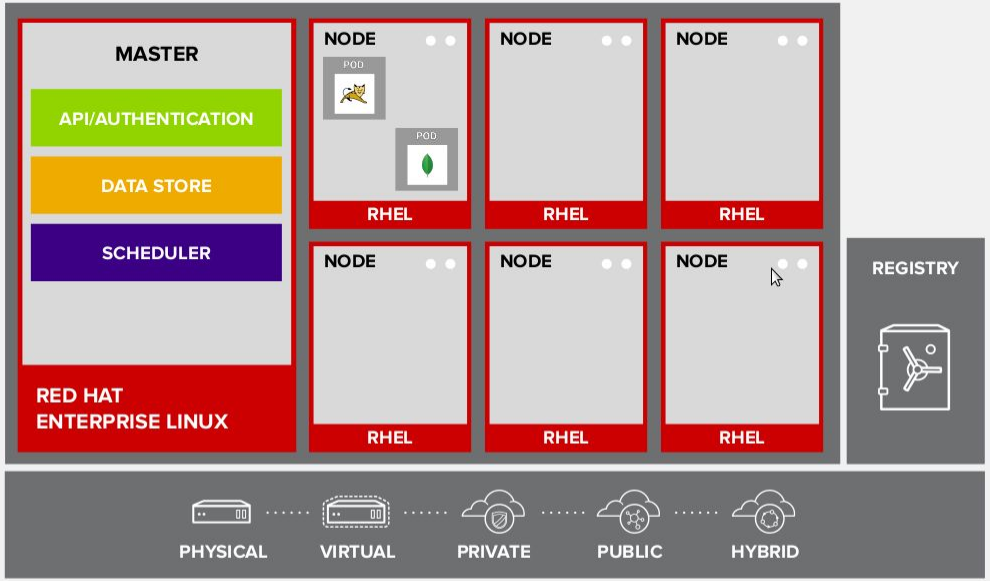


INTEGRATED CONTAINER REGISTRY



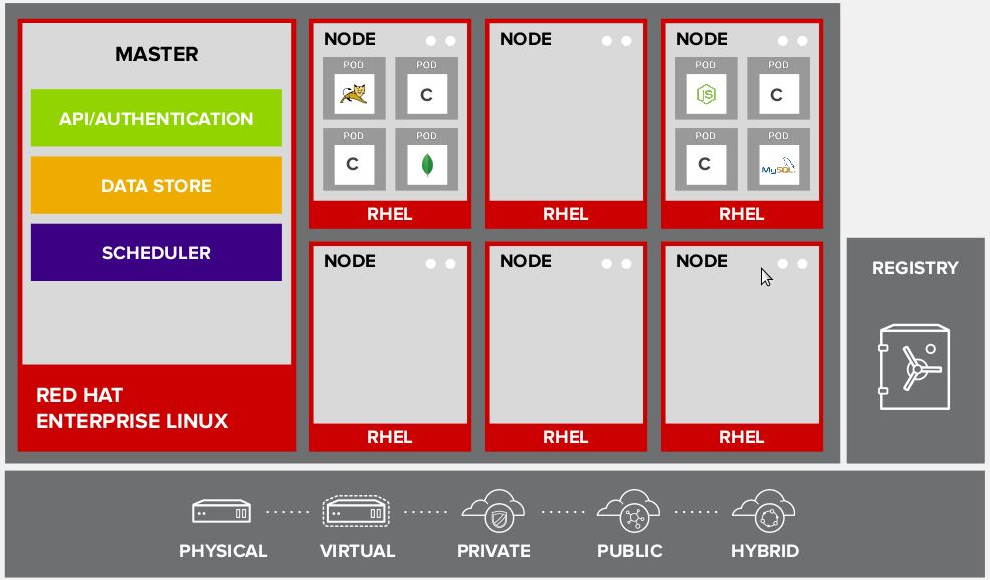
redhat.

ORCHESTRATION AND SCHEDULING



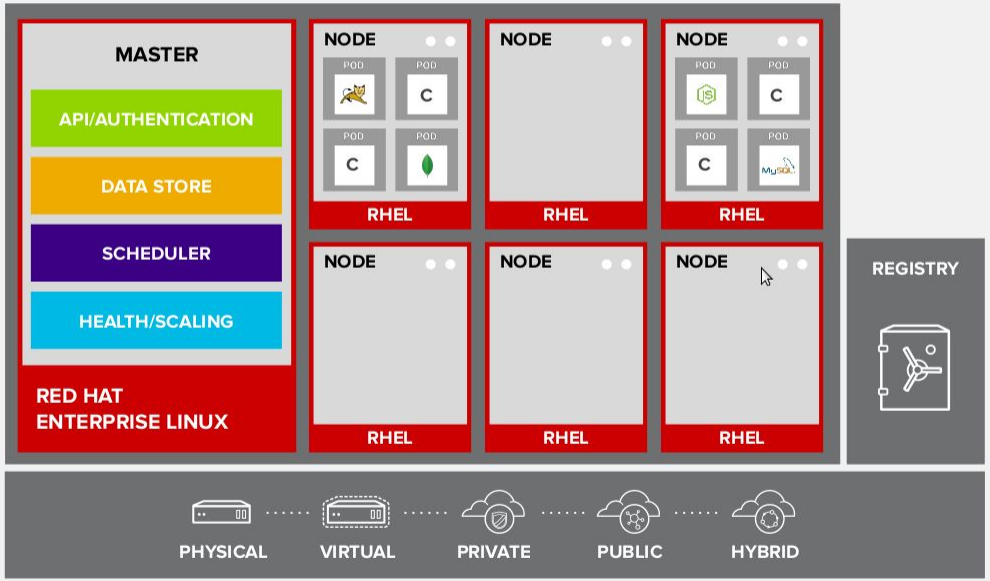
redhat.

PLACEMENT BY POLICY

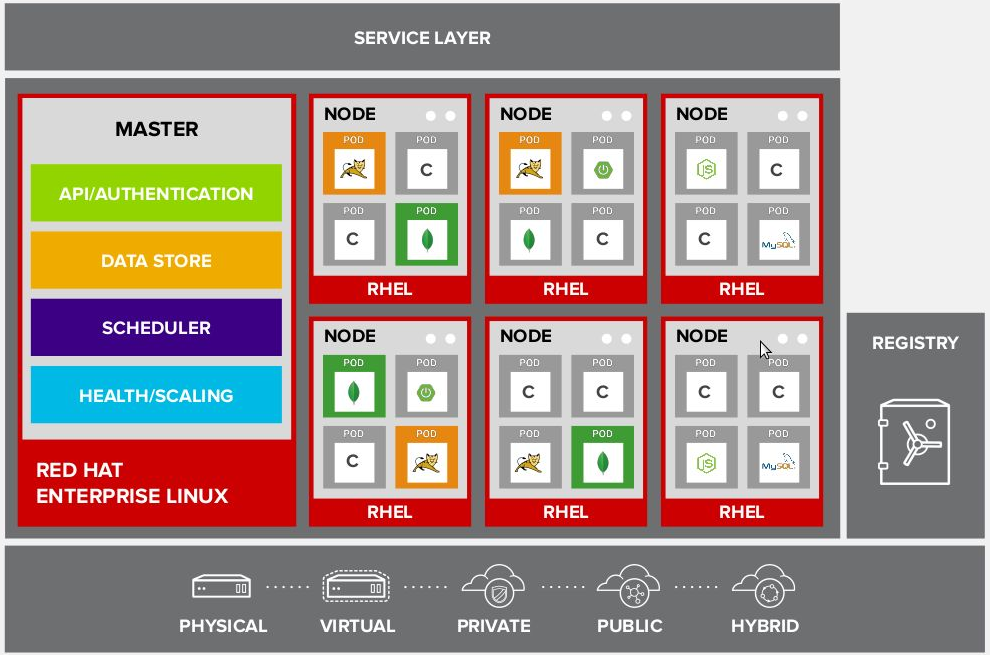


redhat.

AUTOSCALING PODS

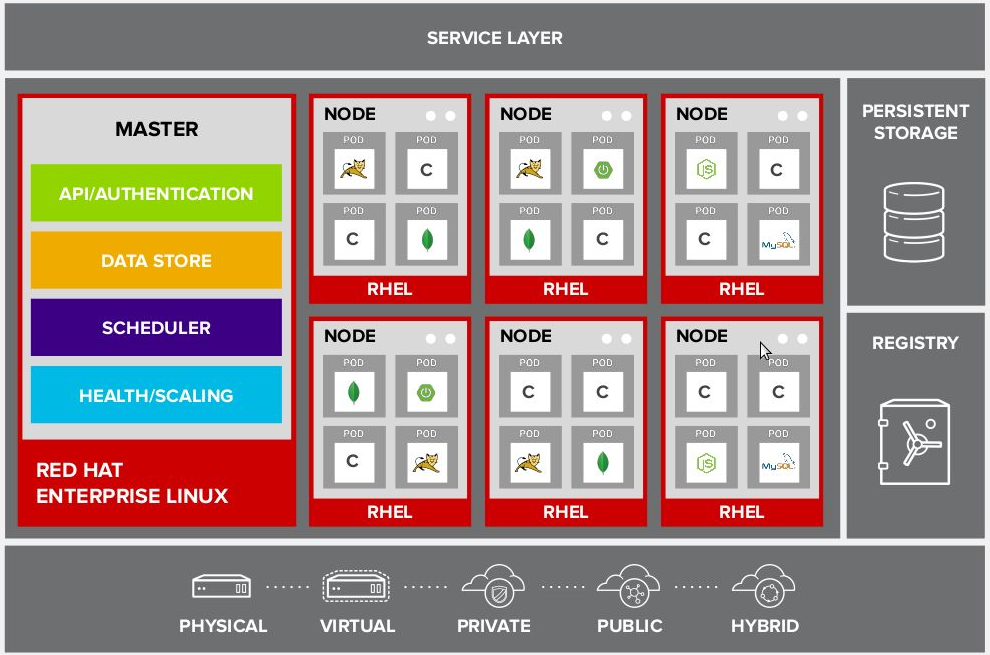


SERVICE DISCOVERY



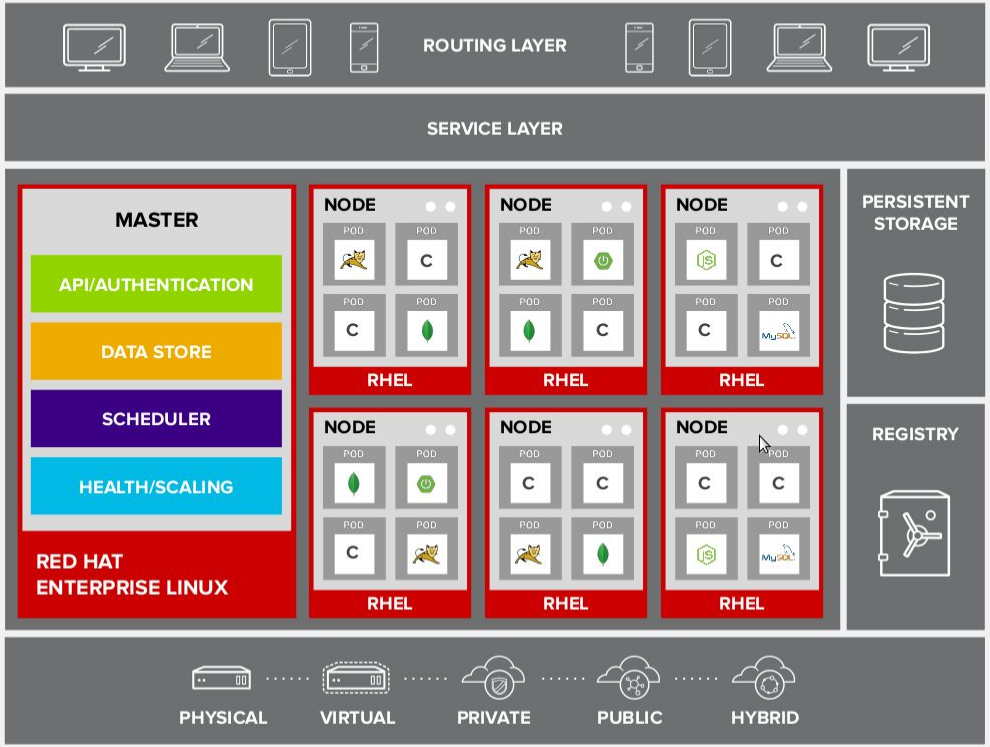
redhat.

PERSISTENT DATA IN CONTAINERS



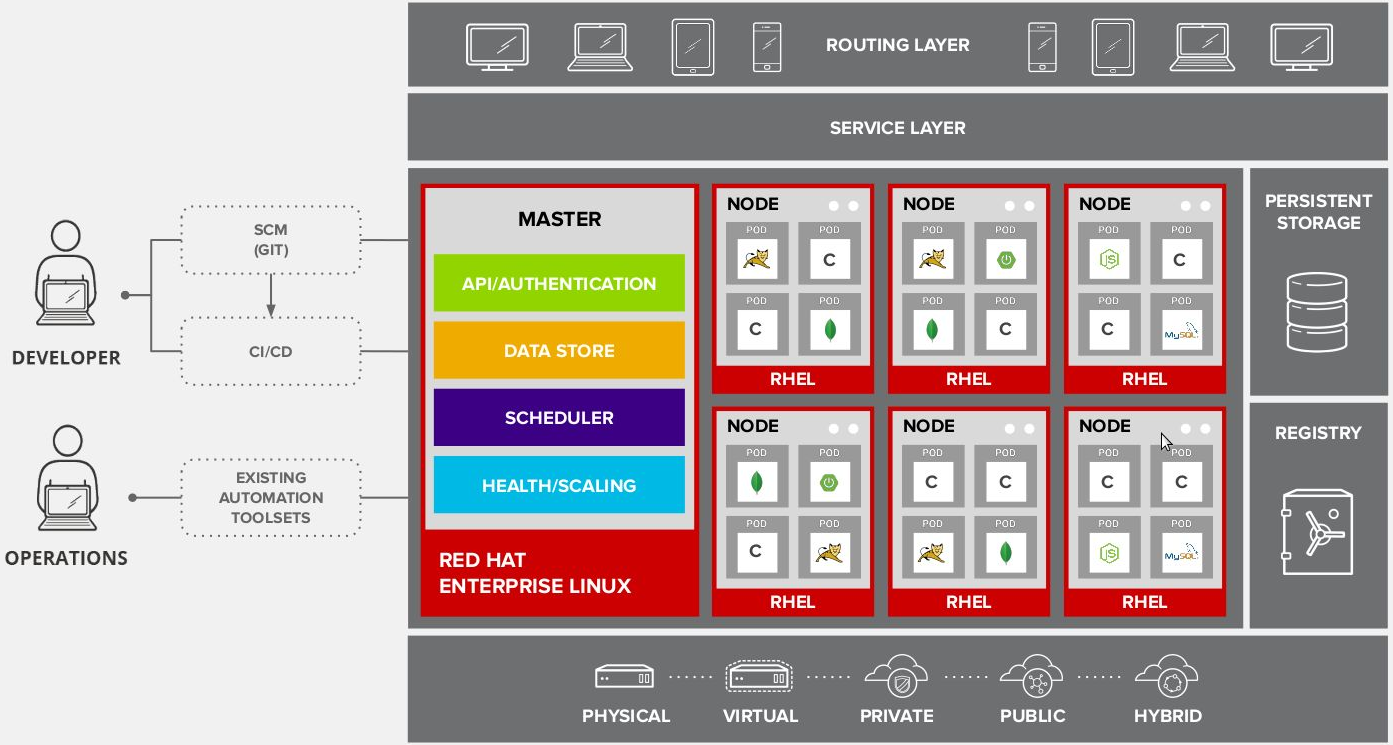
redhat.

ROUTING AND LOAD-BALANCING



redhat.

ACCESS VIA WEB, CLI, IDE AND API



redhat.

redhat.

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

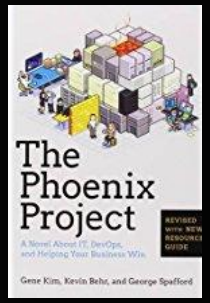
youtube.com/user/RedHatVideos

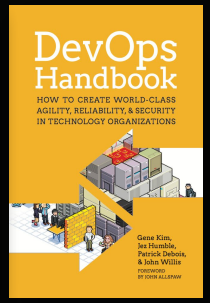
DevOps Resources

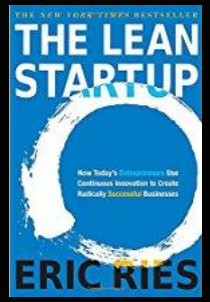
https://devopsfordefense.org/resources/

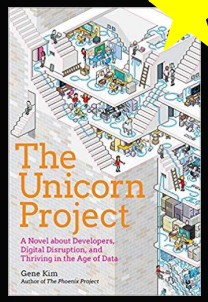
https://www.meetup.com/DevOps-for-Defense/
https://github.com/jondavid-black/DevOpsForDefense
devopsfordefense@gmail.com

Books / Publications:



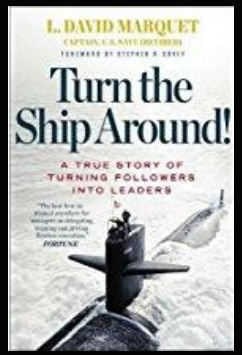


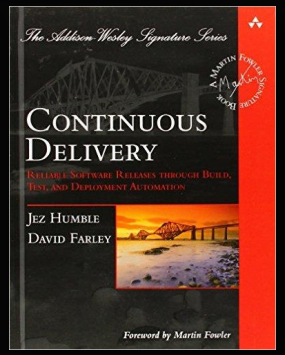


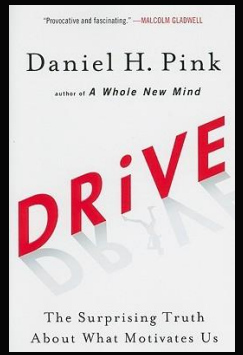


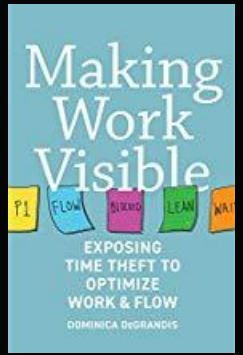
- DevOps Enterprise Summit (DOES)
- IT Revolution
- Velocity
- GoTo

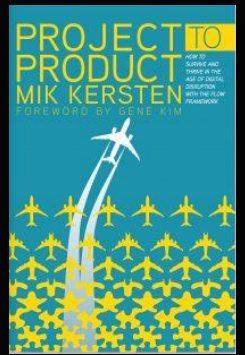
YouTube

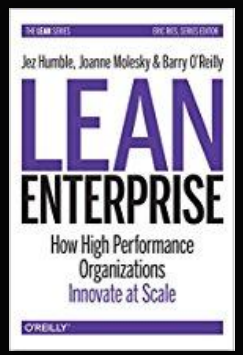


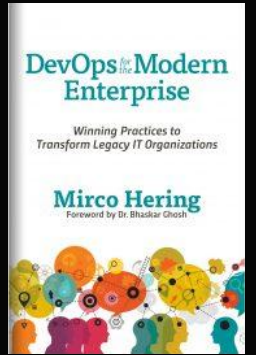












Group Exercise: Lean Coffee

1. Each table has a facilitator.
2. The facilitator has a short introduction.
3. Everyone write down questions or topics for discussion on the subject. Place them in the middle of the table.
4. The group votes on each question or topic by placing a dot on the card. 3 votes per person.
5. Cards with most dots goes first. Set a timer for 5 minutes and discuss.
6. After 5 minutes, either vote (thumbs up/down) to keep going or move on to the next card.

Topics: “Cloud Isn’t for Us”, “Security-as-Code”, “Automate my job away?”