Kubernetes in the Enterprise
Andrew Block

- Distinguished Architect, Red Hat
- Specialities
  - Container and cloud technologies
  - Automation
  - Integration
- Enterprise experience with organizations large and small
- Designed and developed reference architecture on cloud native patterns
- Published author - Learn Helm

ablock@redhat.com
@sabre1041
Why Kubernetes?

**Containers/Microservices**
Model for packaging operating system and application in a single atomic unit and decomposing them into smaller units of work

**Container Management**
Declarative based configuration model along with handling the lifecycle of containers

**Scalability**
Leverage the elastic compute capabilities provided in the cluster to increase or decrease as necessary

**It’s Popular**
Kubernetes dominates the container orchestration market with contributions from over 130 organizations
But, have you thought about.....?

- Security
- Storage
- Monitoring and Metrics
- Logging
- User Experience
- Compliance
- ...

Red Hat
Developer

DevNation
So….

You want to deploy Kubernetes in the Enterprise
A Brave New World
Containers are a Disruptor

Containers transforms how applications are obtained, developed and used

- Immediate access to a wide range of applications and services
- Can be destroyed and recreated as necessary
- New design patterns have been introduced
- Applicable for use by developers and infrastructure administrators

“Containers are the Napster of the 21st century”

$ podman run -it --rm busybox
Applying Kubernetes patterns and technologies can be difficult for many organizations.
Security
Kubernetes Ecosystem

Organizations want a detailed list of components that are part of any software stack:

- Support
- Compliance
- Vulnerability Assessment
Cloud Native Landscape is Vast

- Understand the core components of any Kubernetes deployment
- Determine set of additional components to support cloud native development and operations
- Engage with key representatives to understand their concerns and goals
Kubernetes Platform and Security Concerns

What are some of the top concerns to be aware of?

- Containers
- Kubernetes Control Plane
- Access Control
- Certificates
- Networking
- Storage
Engage Security Team Early and Often

- Security team typically needs to sign off on any enterprise implementation

- Kubernetes introduces technologies that security teams have may not be familiar with

- Collaboration encourages DevSecOps

- Can result in the overall failure of the implementation if not approached correctly
Some Assembly is Required

Kubernetes provides the base platform for running containers at scale

The rest is up to administrators and consumers.....
Supporting Services

Additional components required for a full Kubernetes deployment

- Areas of concern
  - Logging
  - Platform and application monitoring
  - Alerting
  - Continuous Integration and Continuous Delivery
  - Secure values

- Many existing services have added support for Kubernetes deployment
Avoid building your own implementations

- Limited number of developers/features
- Difficult to manage over time
- Lack of community support
- The majority of attempts eventually fail
Container images are a foundational components of a Kubernetes deployment

**Image Composition**
Types of images that should be allowed to be run within an organization

**Image Sources**
Most organizations do not allow direct retrieval from public image registries such as Docker Hub

**Image Registry**
Images produced within the organization must be stored in an image registry
Managing Images in the Enterprise

Image Import Pipeline
- Develop and implement a process for sourcing images from external registries
- Scanning of images should be implemented to verify content does not contain active vulnerabilities

Develop Base Images
- Determine common programming languages and patterns that will be deployed to the platform
- Package required enterprise software
- Ensure images are readily available
- Keep images up to date
Certificates

- Kubernetes makes extensive use of PKI
- Most organizations have their own Certificate Authority that creates and manages certificates
- Develop a process for managing infrastructure and application certificates
Networking

Kubernetes Networking
- Identify IP address ranges needed for deployment
- SDN plugin can accelerate or limit what can be achieved by the cluster

It’s Always the Proxy...
- Most organizations have a firewall/proxy to govern access to external resources
- Network proxies can interfere with intra-cluster as well as external communication

Additional Concerns
- Determine ingress and egress methods along with source/destinations
- Dependencies on supporting services, such as storage
Storage: The fallacy of Microservices

No matter the hype, storage will be required to support the platform and end user applications

- Plan ahead
- Investigate newer cloud native compatible storage
- Integration with existing storage backends typically required
- Lift and shift application to cloud presents greatest challenge
Defend the Platform

Proactive actions mitigate threats and streamline responses to issues

- Employ principle of least privilege
- Enable various forms of auditing
- Tools, such as Open Policy Agent/Gatekeeper can enforce policies and reject malicious actions
- Understand monitoring and alerting capabilities and integrate into existing SEIM systems
Developer Experience
Life as a Developer

I just found this great sample application to deploy to the Kubernetes cluster.

This is going to be easy and fun!
We all can’t have nice things

Security and network restrictions make it difficult to get started

- Cannot create Kubernetes resources
- Cannot access images
- Cannot obtain dependencies
- External runtime resources restricted
Local Development

Most organization provided machines disallow installation and runtime of many components

- Software packages
- Command line tools
- Hypervisors (VirtualBox, Hyper-V)
- Container runtimes
  - Docker
  - Podman
- IDE's
- Development tooling
Local Development

Implement processes for enabling developer productivity
- Software available in enterprise repository
- Documentation and automation

Investigate new development methodologies
- Containerized development
- Cloud based IDE’s
Resource Management

Kubernetes requires developers to truly understand their applications and any requirements

- Replicas
- LimitRanges and Quotas
- Autoscaling
- Scheduling options
The Organization
Outside of the Comfort Zone

Kubernetes introduces new roles and responsibilities

DEVOPS is hard!

DEVELOPERS
- New languages and frameworks
- Infrastructure concerns
- Full stack ownership

OPERATIONS
- Shift from managing servers to managing containers
- Infrastructure as Code
- Interaction with development teams
Organizational practices are exposed

Assessment to introduce Kubernetes often uncovers unflattering organizational practices

- New or existing processes are reviewed in order to align with Kubernetes common procedures
- Can include insecure or forbidden actions
- Unnecessary blame placed on Kubernetes as it triggered assessment
Marketing the Platform

Awareness of the platform and its benefits drives adoption

- Typically introduced to an organization by an infrastructure team
  - Can get lost in a large, siloed organization

- Make the platform approachable
  - Avoid shadow IT (Other Kubernetes implementations)

- Overall failure of initiative can occur if not managed properly
Build the Community Within

It takes a village to deploy Kubernetes successfully at Enterprise scale

Documentation
Enablement
Open Communication
It Doesn’t End There...
Kubernetes is a Journey

- Plan ahead if you intend to implement Kubernetes

- Every organization is at a different point in their journey
  - Not everyone is Netflix!

- Assess level of success within your own organization
Thank You!