I WILL STAND HERE AND STARE AT YOU SILENTLY
@nathanwpylestrangeplanet

OpenShift Commons

What’s Next in OpenShift

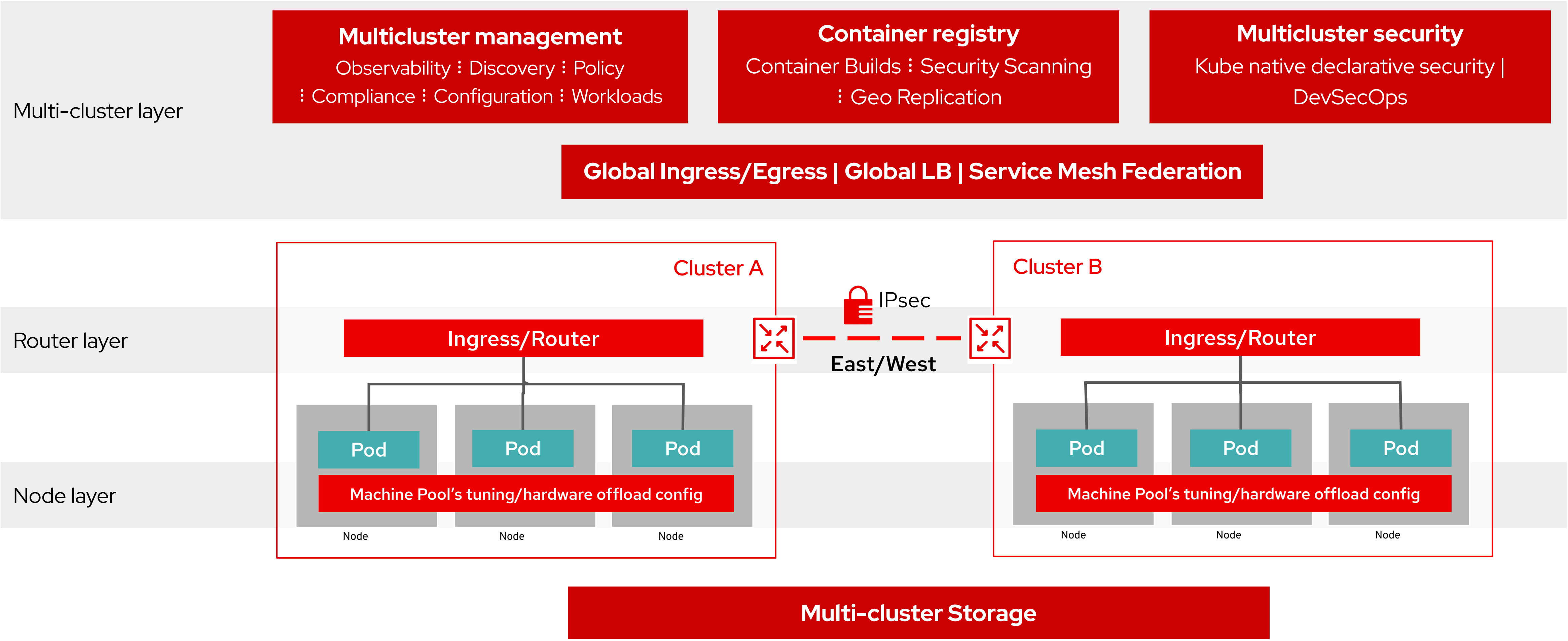
OpenShift Product Management

Rob Szumski

Karena Angell

Red Hat OpenShift

Standardized tools for your 1st and 100th cluster



Multi-cluster layer

Multicluster management
Observability ⁝ Discovery ⁝ Policy ⁝ Compliance ⁝ Configuration ⁝ Workloads

Container registry
Container Builds ⁝ Security Scanning ⁝ Geo Replication

Multicluster security
Kube native declarative security | DevSecOps

Global Ingress/Egress | Global LB | Service Mesh Federation

Router layer

Node layer

Multi-cluster Storage

Multi-cluster Security Automation Demo

Multi-cluster: What's going on upstream

open-cluster-management.io

Community focused on simplification of fleet management:

- Leverages OpenShift Hive for cluster provisioning
- Provides a Governance & Compliance framework for delivering and auditing fleet readiness
- Provides dynamic placement and visibility to applications running across the fleet
- Integrates other projects like ArgoCD, Open Policy Agent, Thanos along with additional capabilities

Cluster API

APIs to simplify provisioning of Kubernetes clusters:

- Goal is to fill gaps in tools like kubeadm that are not as declarative as required for infra-as-code
- Defines concepts like Machine Pools and Machine Health Checks to drive automation
- Adding support for advanced types of cluster like those with Windows nodes

Multi-cluster in OpenShift

Cluster creation in ACM

Deploy new clusters that inherit RBAC, governance and security policies automatically:

- Manage the full life cycle of OpenShift clusters
- Claim a booted cluster with cluster pools

Monitoring across your fleet

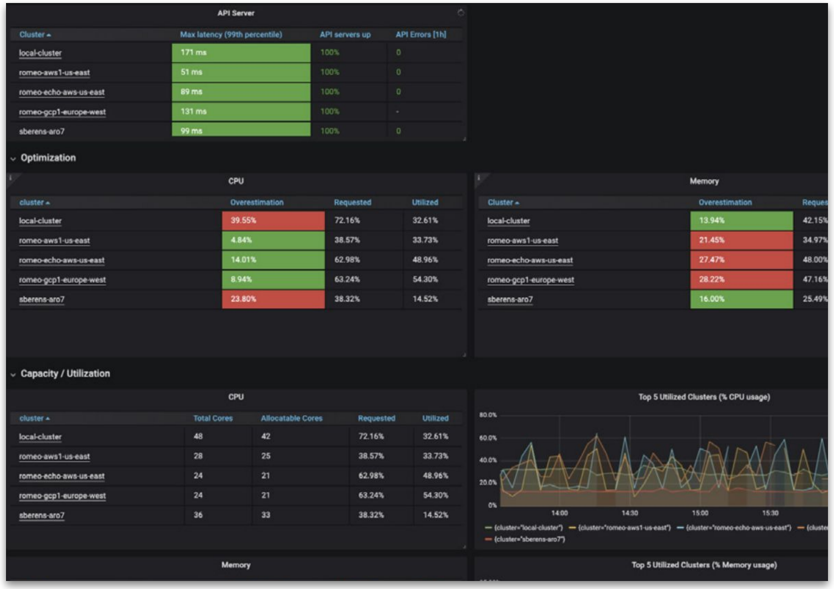
ACM aggregates metrics from all clusters to give you a global picture of your OpenShift clusters:

- Built in dashboards
- Prometheus & Thanos are the backing technologies

Cross-cluster Networking

Connect dependencies on different clusters together:

- Extends the Pod network across an encrypted link
- CNCF's Submariner is the backing technology



API Server

Cluster ▲	Max latency (99th percentile)	API servers up	API Errors [1h]
local-cluster	171 ms	100%	0
romeo-aws1-us-east	51 ms	100%	0
romeo-echo-aws-us-east	89 ms	100%	0
romeo-gcp1-europe-west	131 ms	100%	-
sberens-aro7	99 ms	100%	0

Optimization

CPU

cluster ▲	Overestimation	Requested	Utilized
local-cluster	39.55%	72.16%	32.61%
romeo-aws1-us-east	4.84%	38.57%	33.73%
romeo-echo-aws-us-east	14.01%	62.98%	48.96%
romeo-gcp1-europe-west	8.94%	63.24%	54.30%
sberens-aro7	23.80%	38.32%	14.52%

Memory

Cluster ▲	Overestimation	Reques
local-cluster	13.94%	42.15%
romeo-aws1-us-east	21.45%	34.97%
romeo-echo-aws-us-east	27.47%	48.00%
romeo-gcp1-europe-west	28.22%	47.16%
sberens-aro7	16.00%	25.49%

Capacity / Utilization

CPU

cluster ▲	Total Cores	Allocatable Cores	Requested	Utilized
local-cluster	48	42	72.16%	32.61%
romeo-aws1-us-east	28	25	38.57%	33.73%
romeo-echo-aws-us-east	24	21	62.98%	48.96%
romeo-gcp1-europe-west	24	21	63.24%	54.30%
sberens-aro7	36	33	38.32%	14.52%

Top 5 Utilized Clusters (% CPU usage)
80.0%
60.0%
40.0%
20.0%
0%
14:00
14:30
15:00
15:30
{cluster="local-cluster"}
{cluster="romeo-aws1-us-east"}
{cluster="romeo-echo-aws-us-east"}
{cluste
{cluster="sberens-aro7"}
Memory
Top 5 Utilized Clusters (% Memory usage)

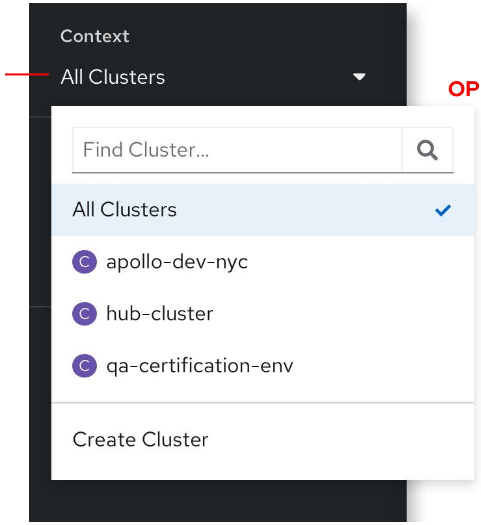
Multi-cluster Roadmap

New cluster switcher

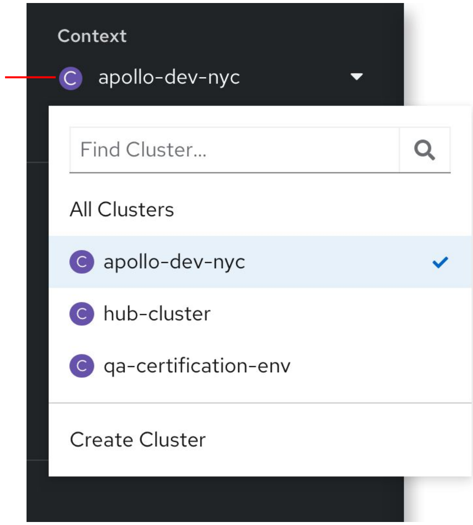
The OpenShift experience moves up to fleet level:

- Easily switch cluster contexts
- Access a fleet-wide view of apps, policy, and config

THIS IS ACM



THIS IS OPENSHIFT



Enhanced ACM features

Use ACM to aid management of your fleet:

- Shared SSO configured on your entire fleet
- Additional built-in governance, risk and compliance policies
- Configure Submariner multi-cluster networking between clusters in the fleet
- Discover and Import clusters from cloud.redhat.com

Multi-cluster Security Automation Demo

OpenShift Commons

Red Hat OpenShift

Security: What’s going on upstream

Pod Security Policies – > Pod Security

Policy format and framework for enforcement for legal, security and operational requirements:

- PodSecurityPolicy is deprecated
- SecurityContextConstraints is still supported in OpenShift
- The future in-tree replacement for PodSecurityPolicy will be simpler
- External policy tools such as OPA/Gatekeeper and Kyverno may be a better fit for complex policies

Open Policy Agent

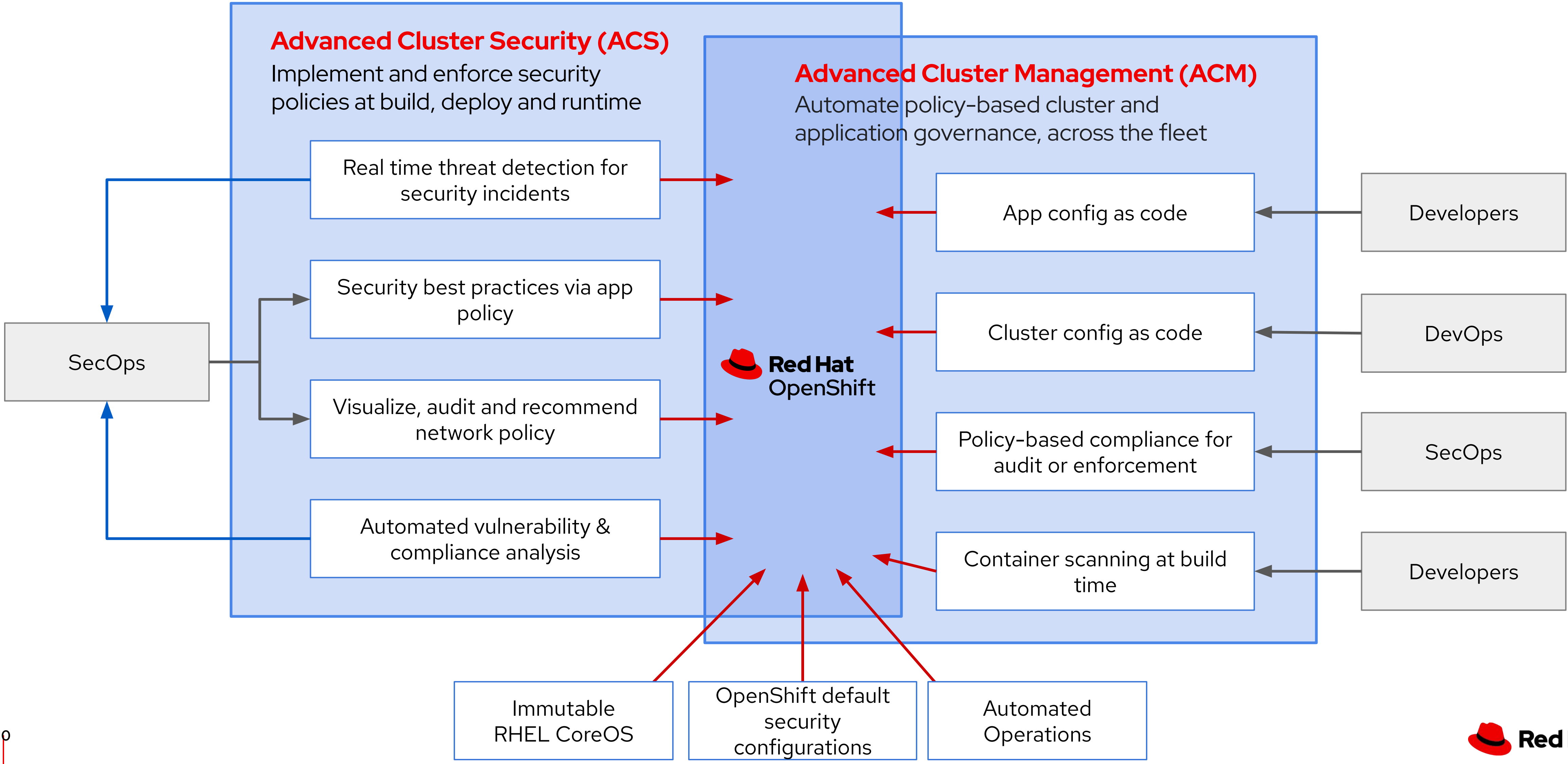
Kyverno

User Namespaces

Together with SELinux protect namespaces from each other on the cluster:

- This is a CRI level feature, which is now default for talking to runtimes including in OpenShift
- OpenShift’s runtime, CRI-O, can do UID mapping, we are waiting on Kubernetes to use it
- Still in the KEP process

Security in OpenShift



Advanced Cluster Security (ACS)

Implement and enforce security policies at build, deploy and runtime

Real time threat detection for security incidents

Security best practices via app policy

Visualize, audit and recommend network policy

Automated vulnerability & compliance analysis

SecOps

Advanced Cluster Management (ACM)

Automate policy-based cluster and application governance, across the fleet

App config as code

Cluster config as code

Policy-based compliance for audit or enforcement

Container scanning at build time

Developers

DevOps

SecOps

Developers

Red Hat OpenShift

Immutable RHEL CoreOS

OpenShift default security configurations

Automated Operations

Security Roadmap

Surface compliance reports in UI

Easier auditing with the Compliance Operator for CIS and other benchmarks through UI enhancements:

- Reports in ACS UI (available now)
- Expanded compliance workflow ACS

New Cert-Manager Operator

Automated certificate management for cluster users:

- Issue certs *from* the internal cluster CA, Hashicorp Vault, or LetsEncrypt
- Issue certs *to* developer's apps, installed Operators, cluster components (after install), Red Hat middleware, and more.

Sandboxed Containers

Designed for apps that are cloud native but need extra kernel isolation:

- Running 3rd party or untrusted code
- FIPS certification coming 2H2022

Enable user namespaces

Configure in OpenShift once it lands in upstream Kubernetes:

- Huge gain in out-of-box security
- Helpful for OpenShift Builds & Quay builds

Multi-cluster Security Automation Demo

Automation: What’s going on upstream

ArgoCD

Gaining features to scale as enterprises onboard more teams and workflows into ArgoCD:

- First class support for Helm, Kustomize and other tools
- Move to project scoped repositories and clusters
- Improvements to app and cluster detail pages

Tekton

Build pipelines from composable tasks that can be shared between teams and apps:

- Pipeline as Code and Tekton Workflows
- Rootless image builds and experimental hermetic execution mode

KEDA

Event-aware autoscaling of containers and applications:

- Multi-tenant behavior by allowing multiple instances in a cluster
- Exposing CloudEvents for certain events
- HTTP based autoscaling

Knative

Streamline developer productivity through Knative functions, eventing and serving:

- Deploy and manage event-driven functions
- Deeper integration with Apache Kafka in Eventing
- End-to-end encryption and cold start improvements in Serving

Workload Automation in OpenShift

Automated build & deployment

OpenShift contains all of the tools to built fully featured CI and CD workflows:

- OpenShift GitOps generally available (ArgoCD)
- OpenShift Pipelines generally available (Tekton)
- ACM understands GitOps/ArgoCD app definitions
- Off-cluster automation through ACM & Ansible

Dynamic scaling via automation

Once running, there are several models of scaling and resource automation:

- Vertical and horizontal pod autoscaling
- Serverless apps connect to event sources like Kafka streams, cloud services, & workflow tools like Zendesk for scaling
- Operators that understand app-specific scaling guidelines to auto-tune themselves

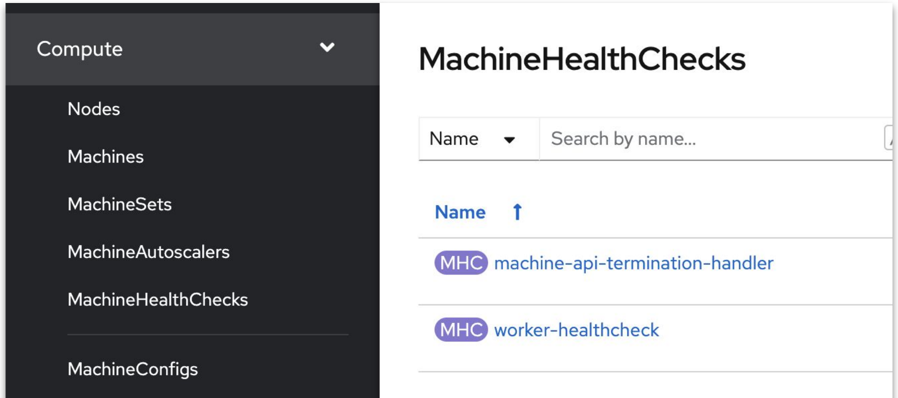
Operators embed operational logic like this in a single unit

Cluster Automation in OpenShift

Self-managed cluster infrastructure

OpenShift 4 is designed for “automated operations”, including:

- Machine health checks can assess node status and allowed failure percentage
- Machine autoscaling adds capacity due to failures or resource capacity
- Automated “one click” cluster upgrades



MHC machine-api-termination-handler

MHC worker-healthcheck

Manage entire fleet via ACM

From your Hub, orchestrate the lifecycle of your OpenShift clusters:

- Change cluster channels and trigger upgrades
- Work with self-managed and cloud-managed OpenShift from your Hub
- Manage 1000 clusters in a single Hub

Automation Roadmap

OpenShift GitOps and Pipelines

Strengthening the killer combo of infrastructure and deployment as code:

- Continuing to bring the latest ArgoCD and Tekton
- Smoother experience for consuming from TektonHub
- Improved “pipelines-as-code” use cases
- DevSecOps as pipeline tasks
- GA of OpenShift Builds v2/Buildpacks for use in Pipelines
- OpenShift Sandboxed Containers in Pipelines

Advanced Cluster Management

Meet the scale, workflow and communication needs for OpenShift customers:

- Introduce key & secret management
- Manage 2000 clusters in a single Hub
- Bring existing configuration policies in Kubernetes or Rego format

Serverless

Build, run and deploy event-driven applications:

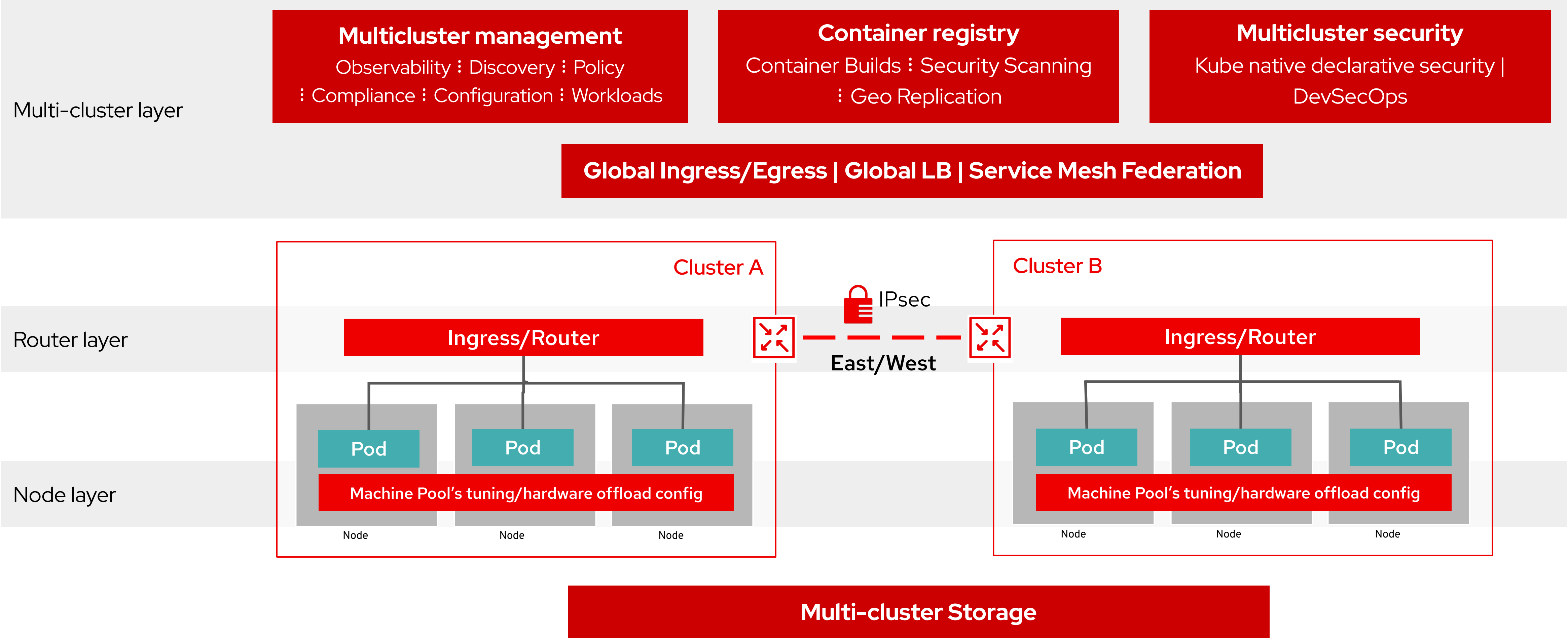
- Security enhancements including end-to-end encryption and eventing improvements
- Integrations with Kogito, Data Grid, 3Scale API Gateway, KEDA

Multi-cluster Security Automation Demo

Demo

- Talk through the set up, which is OPP:
    - Infra cluster with ACM, ACS, Quay
    - All installed in a central location for X and Y and Z reasons
    - GitOps is also installed, that is our software supply chain
- The demo is:
    - Input to the pipeline is X
    - Pipeline protects/stops supply chain attacks in X and Y ways
    - ...skip apps but state that everyone's apps are different and all can run on OCP
    - But what matters is your cluster security too, here's how Compliance Operator + ACS + whatever keep that app env secure no matter where it runs

Standardized tools for your 1st and 100th cluster



Multi-cluster layer

Multicluster management
Observability ⁝ Discovery ⁝ Policy ⁝ Compliance ⁝ Configuration ⁝ Workloads

Container registry
Container Builds ⁝ Security Scanning ⁝ Geo Replication

Multicluster security
Kube native declarative security | DevSecOps

Global Ingress/Egress | Global LB | Service Mesh Federation

Router layer

Node layer

Cluster A

Ingress/Router

Pod

Pod

Pod

Machine Pool's tuning/hardware offload config

Node

Node

Node

IPsec

East/West

Cluster B

Ingress/Router

Pod

Pod

Pod

Machine Pool's tuning/hardware offload config

Node

Node

Node

Multi-cluster Storage

Red Hat

Thank you

Red Hat is the world's leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.

linkedin.com/company/red-hat

youtube.com/openshift

facebook.com/OpenShift

twitter.com/openshift