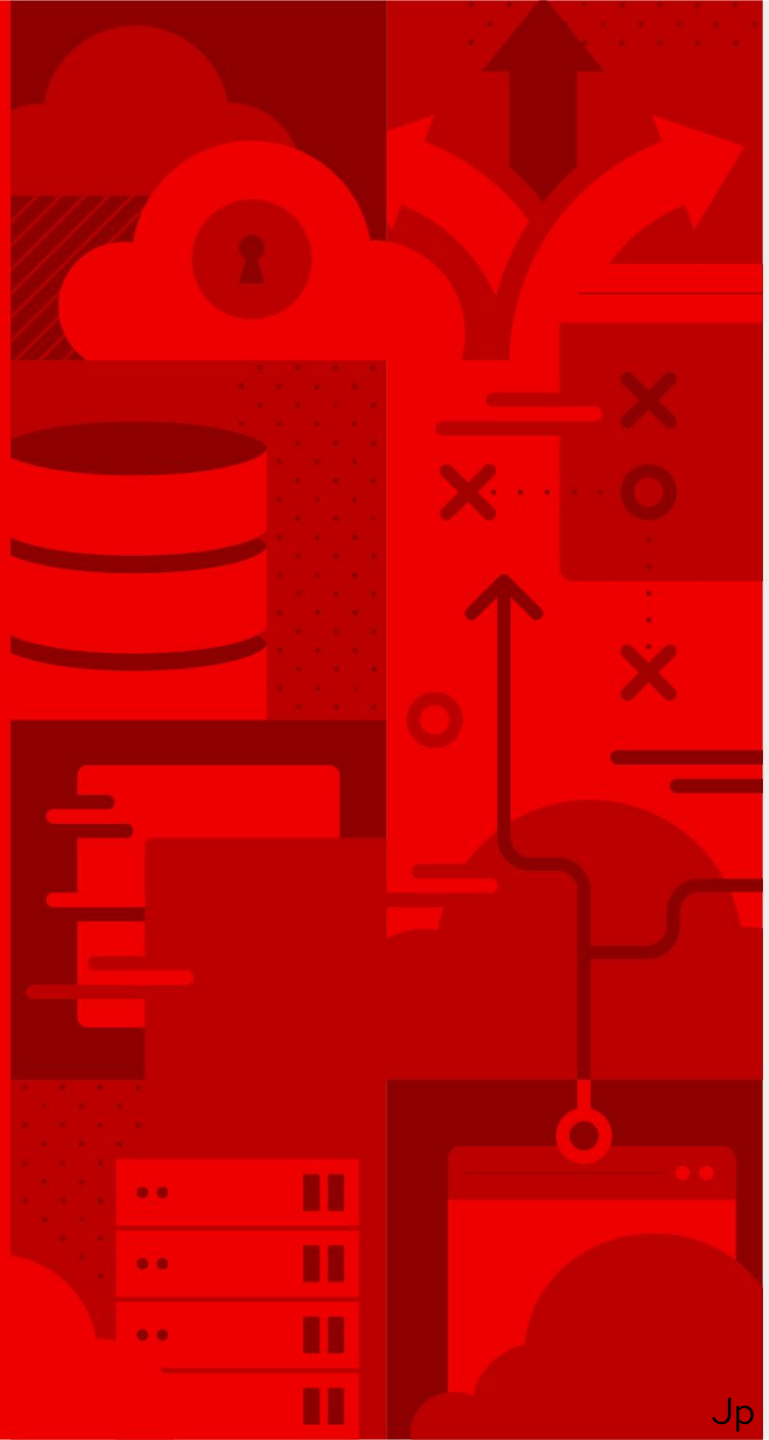


RED HAT
Advanced
Cluster Management

Security and Governance Strategy & Architecture

Jaya Ramanathan, Ph.D.
DIstinguished Engineer
ACM Chief Security and Governance Architect

Yu Cao
ACM Security and Governance Squad Lead

Red Hat

Jp

Security and Compliance Challenges when adopting Cloud

- Enterprise clients need to meet internal enterprise security standards as well as external regulatory compliance requirements
- Enterprise clients need to go through periodic audits by external auditors of their IT infrastructure
- Securing clouds typically requires new security tools in addition to existing security tools used for traditional non-cloud IT infrastructures
- Cloud environments are dynamic
- Enterprises typically use more than one cloud provider
- Enterprises require interaction with existing systems of record and data
- Customers want ‘open’ not proprietary solutions

Requirement: ‘Continuous security and audit readiness for open hybrid cloud’

Policy based Governance

Enable governance end to end to meet standards across hardware/software stack to facilitate continuous security and audit readiness

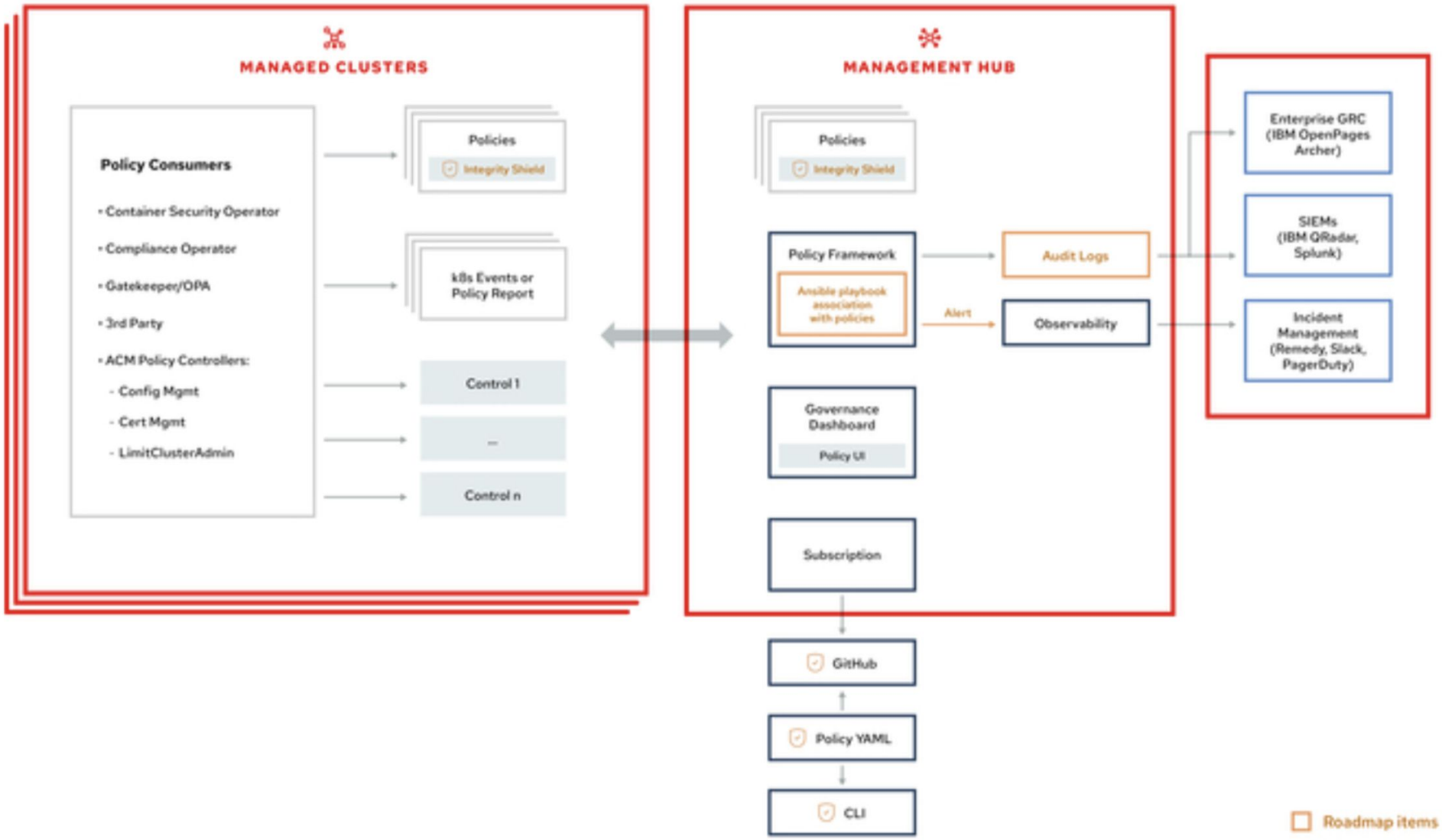
- **GRC Terminology**
  - **Governance** - A structured way of operating an IT infrastructure based on defined policies, processes, and procedures
  - **Risk** – Identify risk areas to help IT Operations prioritize their actions to minimize risks
  - **Compliance –** Assess if specified policies are complied to by various controls

- **Goals**
  - Represent industry/enterprise best practices as policies that result in desired config state
  - Extensible policy framework that can be applied to entire hardware/software stack
  - Ability to incorporate multiple policy languages including Gatekeeper/OPA
  - Customization of built-in policy templates
  - Ability to integrate 3rd party provided controls
  - Dashboard and API for overall posture and deviations from policies
  - Customization of policy templates for internal enterprise standards and external compliance standards (NIST CSF, NIST 800-53, PCI, FISMA, HIPAA, etc)
  - UI, CLI, and Subscription (GitOps) interfaces to deploy policies
  - Ease of integration with existing enterprise tools (Incident Management, Security Operations Center, Enterprise GRC)

Policy based governance - Terminology

- **Policy authoring point - where the policy is specified**
  - UI/Console
  - CLI
  - GiTOps
- **Policy management point - distributes policy, consolidates policy violations across a fleet of clusters, integrates with enterprise tools (security operations center, incident management, GRC etc)**
  - ACM Hub/Open Cluster Management upstream community
- **Policy Enforcement Point (PEP) - consumes policy and returns violations**
  - k8s Admission Web Hook
  - Runtime controllers (k8s, ACM configuration policy controller, ACM certificate management controller, OpenShift Compliance Operator, SysDig Operator, Falco Operator, etc)
- **Policy Decision Point - invoked (optionally) to check whether the specified policy matches how a control is configured**
  - Gatekeeper/OPA
  - Kyverno

Policy based governance - Architecture



Gatekeeper/OPA Overview

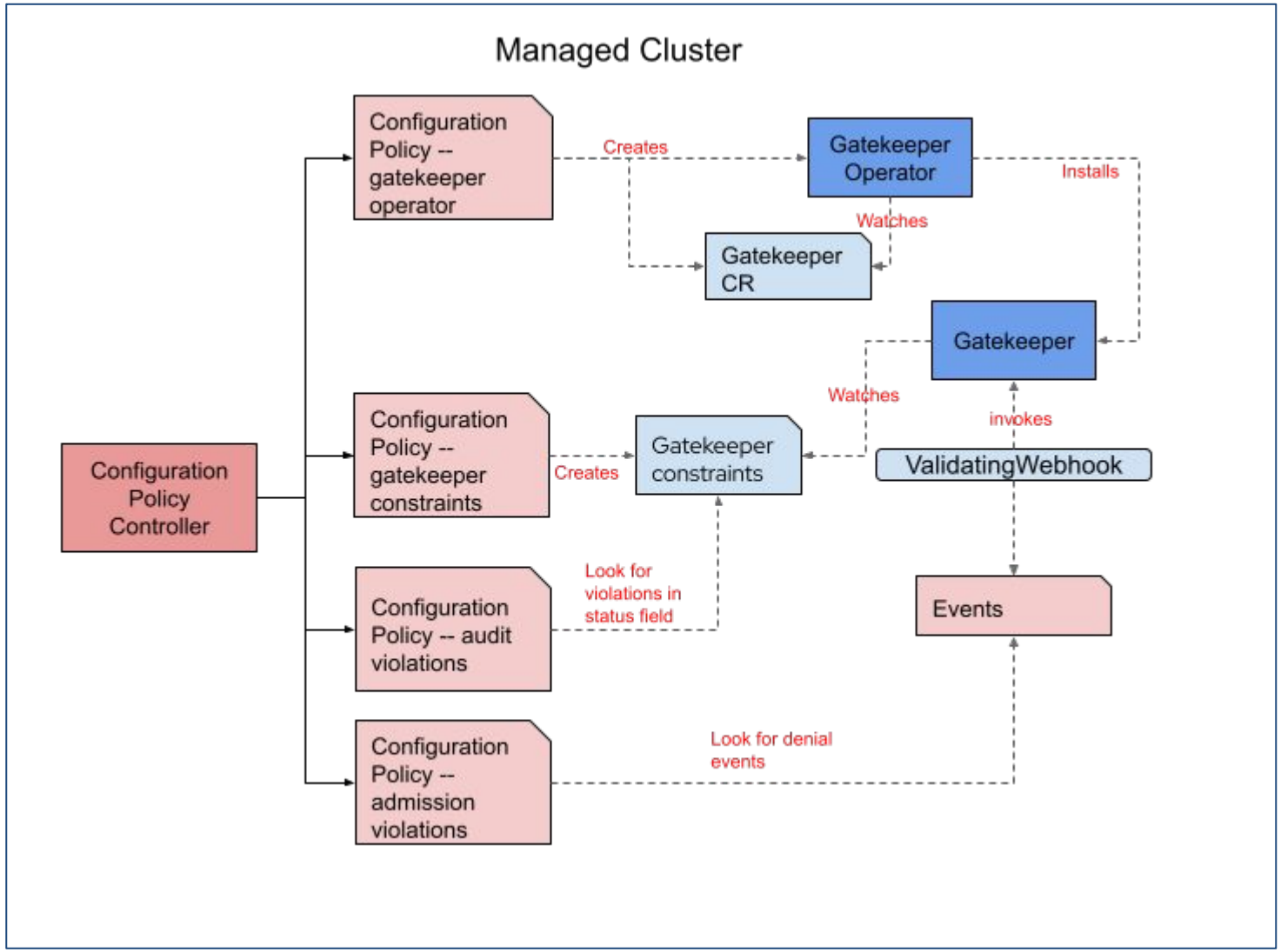
- Gatekeeper can evaluate compliance of k8s resources to policies.
- Leverages OPA as the policy engine which uses Rego as the policy language.
- Two scenarios:
  - Admission -- executed whenever a k8s resource is created or updated to block any non-compliance to policies
  - Audit -- periodically evaluate existing k8s resources against policies to detect pre-existing noncompliances (if any)

Gatekeeper/OPA Integration with ACM

- Deliver Gatekeeper/OPA as an operator as part of ACM (Downstream Gatekeeper/OPA Operator)
- Provide RHACM policy to deploy this operator
- Provide RHACM policy to propagate Gatekeeper policy from Hub to managed cluster
- Detect policy violations
  - For admission scenario violations
    - Use RHACM configuration policy to process events generated by Gatekeeper admission webhook
    - Deploy Gatekeeper with emit-admission-events=true
    - Example Violation message: NonCompliant; violation - events exist and should be deleted: [openshift-multus.16282a3f3cb422b5] in namespace gatekeeper-system
  - For audit scenario violations,
    - Use RHACM configuration policy to look for violations in status field of Gatekeeper constraint CR
    - Example violation message: NonCompliant; notification - K8sRequiredLabels `ns-must-have-gk` doesn't exist as it should be. Expected field `totalViolations: 0`, actual field `totalViolations: 67`; Expected field `violations: []`, actual field `violations: - enforcementAction: deny kind: Namespace message: 'you must provide labels: {"gatekeeper"}'  name: cert-manager`

RHACM Integration with Gatekeeper/OPA

RHACM Hub



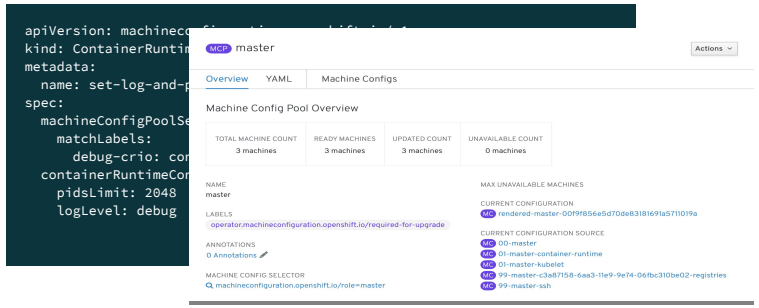
Integration of RH ACM with Compliance Operator

1 A user requests a new cluster/defines RHACM policy

Red Hat Advanced Cluster Management for Kubernetes

[RHACM Policy to deploy Compliance Operator]
[RHACM Policy for EB Security Profile Scan]

Describe intent with declarative config



2 *Red Hat curates MachineConfigs to meet security profiles, like CIS or NIST-800-53*

Red Hat OpenShift Container Platform

Red Hat Enterprise Linux CoreOS

3 *The Machine Config Operator applies the selected secure machine config*

Observe

Maintain

4 Metrics are sent to Red Hat Insights for analysis via secured HTTPS.

Monitor, scale, troubleshoot, backup

Install, upgrade, *reconcile*, config

Red Hat OpenShift Container Platform

Red Hat

THANK YOU!

For questions and more details:

- ACM Security and Governance blog links here: https://github.com/open-cluster-management/policy-collection
- Open Cluster Management Community: https://github.com/open-cluster-management/community/projects/1