

# OCM Multicluster App & Config Management

Kubecon 2022

Matt Prah  
Maggie Chen



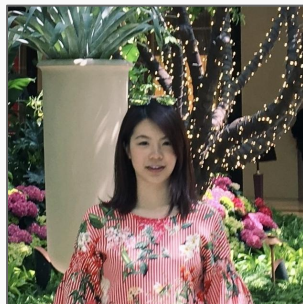
# About Us



[github.com/mprah](https://github.com/mprah)

**Matt Prah**

Open Cluster Management Policy SIG Lead,  
Principal Software Engineer at Red Hat on  
Advanced Cluster Management for Kubernetes



[github.com/chenz4027](https://github.com/chenz4027)

**Maggie Chen**

Open Cluster Management Application LC,  
Software Engineer at Red Hat on  
Advanced Cluster Management for Kubernetes

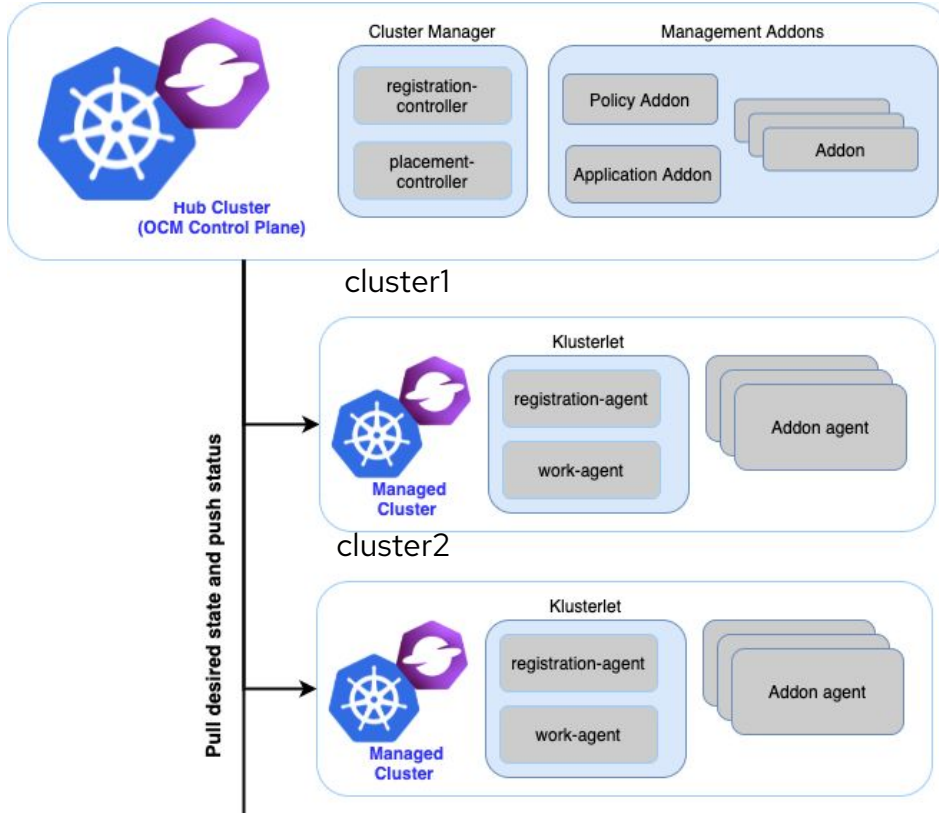
# A Summary of Open Cluster Management



Simplify fleet management across the open hybrid cloud at scale.  
[open-cluster-management.io](https://open-cluster-management.io)

- An open-source CNCF Sandbox project
- Simplifies the management of Kubernetes clusters
- Hub and spoke architecture
- Allows targeted distribution of Kubernetes manifests from the Hub
- Integration point for making Kubernetes capabilities multicluster aware

# OCM Architecture



# Management: What's going on upstream

Community focused on simplification of fleet management

- Provides a Governance & Compliance framework for delivering and auditing fleet readiness
- Provides dynamic placement and visibility to applications running across the fleet
- Introduces [Cluster Manager](#) & Klusterlet operators on operatorhub.io to provide a connected management agent within the cluster
- Integrates other projects like ArgoCD, Open Policy Agent, [Thanos](#) along with additional capabilities

# OCM Application Addon

# The OCM App add-on

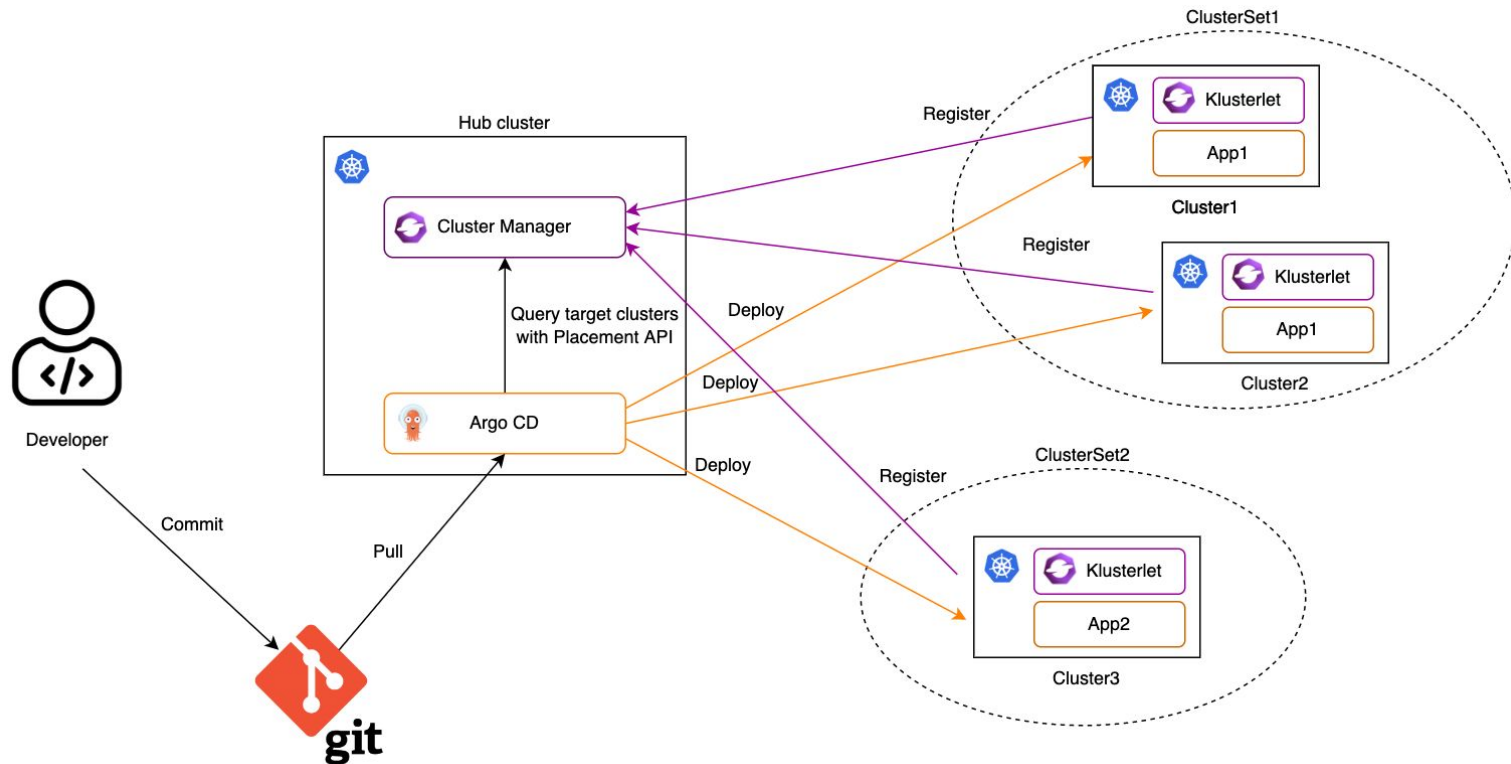
- Stand-alone and multi-cluster deployment
- GitOps(Git, Helm) subscription
- Object storage subscription
- Integration with ArgoCD

# OCM Application API Concepts

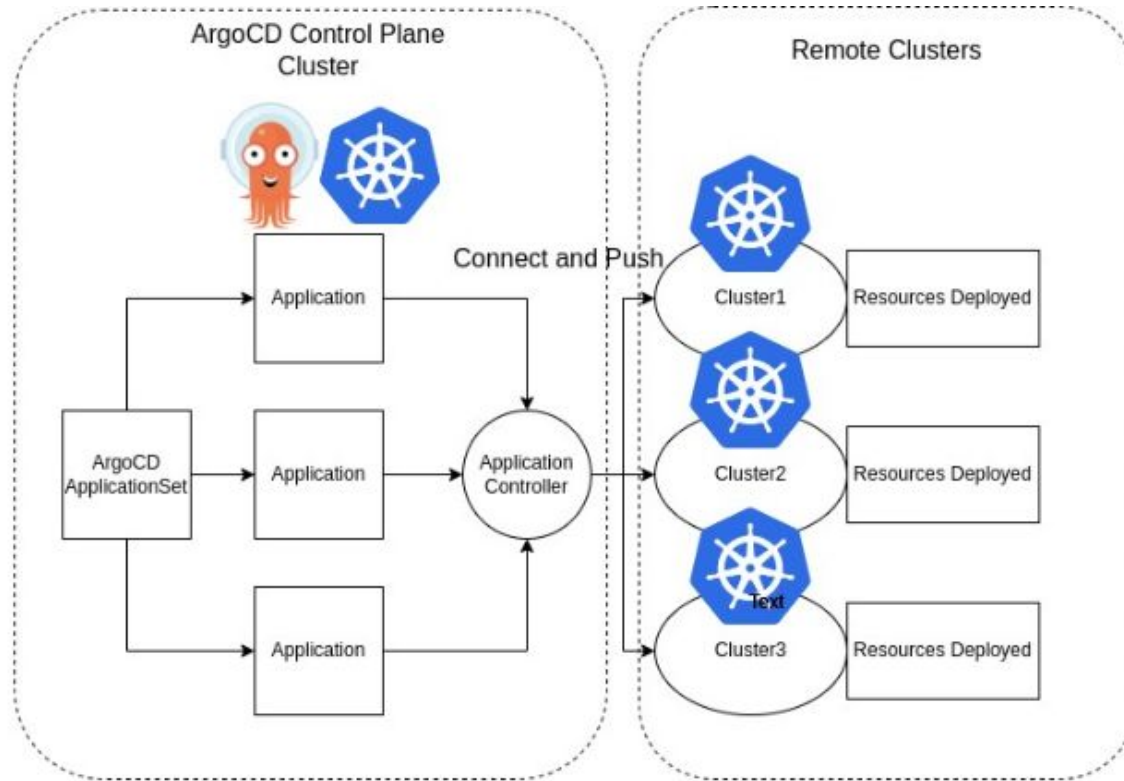
- **Placement**: dynamically select a set of managed clusters i.e. multi-cluster scheduling.
- **ApplicationSet**: supports deployments to large numbers of clusters, deployments of large monorepos, and enabling secure Application self-service.
- More details can be found on the [open-cluster-management.io](https://open-cluster-management.io) website.



# Integration with Argo CD



# Pushing resources



# Demo



- Deploy application “guestbook-ui” to kind clusters (cluster1 and cluster2) with Argo CD and OCM

# Future: pull model



argo

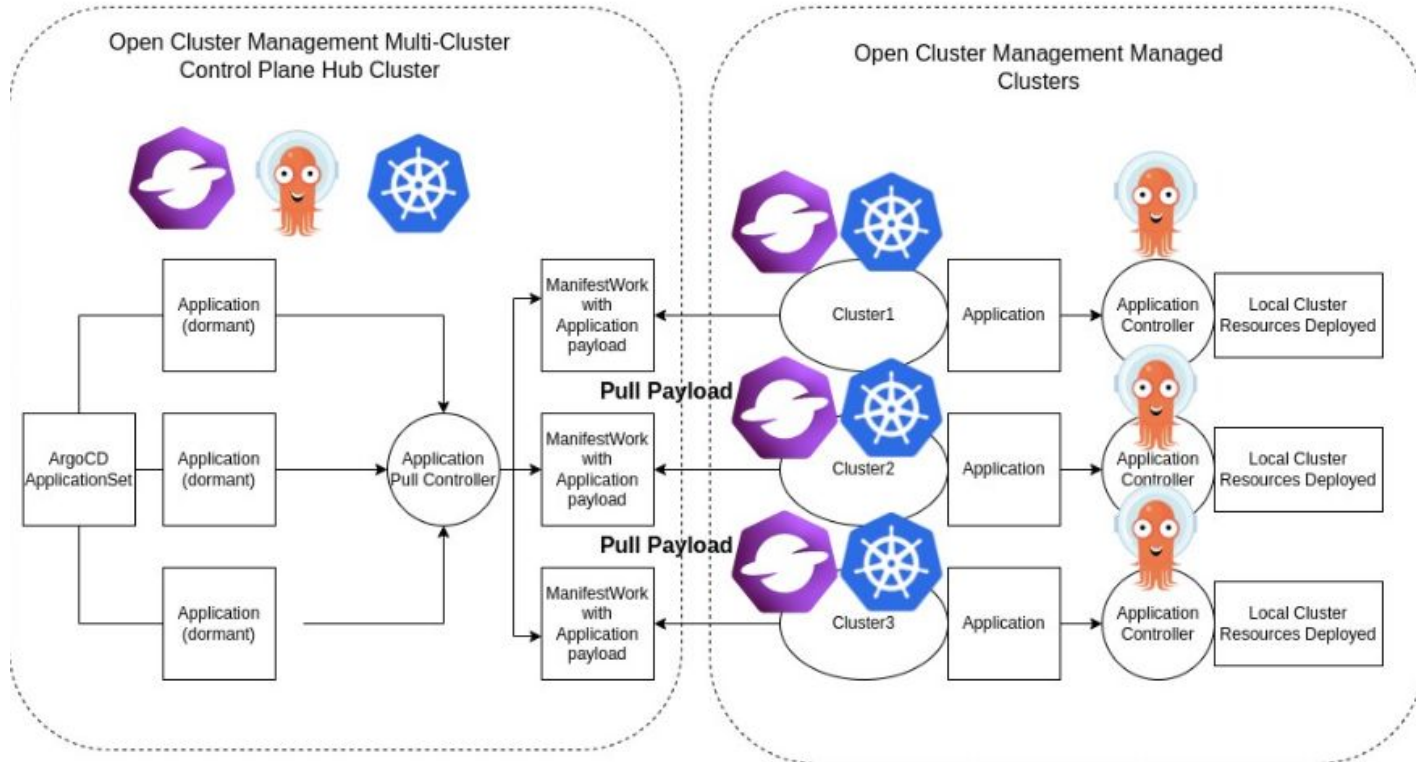
The pull model offers some advantages over the existing push model:

- **Scalability:** well documented that hub-spoke pattern offers better scalability.
- **Security:** cluster credentials doesn't have to be stored in a centralized environment.
- Reduce the impact of a single point of centralized failure.

This ArgoCD pull model controller on the Hub cluster will create ManifestWork objects wrapping Application objects as payload. The OCM agent on the Managed cluster will see the ManifestWork on the Hub cluster and pull the Application down.

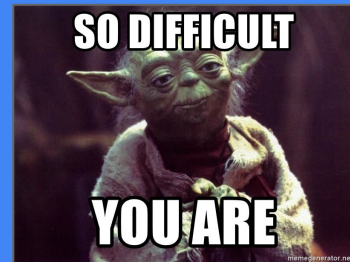
Argo CD pull integration: <https://github.com/mikeshng/argocd-pull-integration>

# Integration with Argo CD



# OCM Policy Addon

# Multicloud Governance Challenges



- Consistent configuration management in a multicloud or multicloud environment
- Meeting organization security standards
- Complying with external regulatory compliance requirements for security, resiliency, and software engineering practices
- Accounting for the fluidity of Cloud environments
- Find an open and extensible solution
- Integrating with existing tooling or procedures

# The OCM Policy Addon



- Declarative policies
- Configuration management in a multicluster or multcloud environment
- Informs or enforces Kubernetes manifests on desired Kubernetes clusters
- Supports dynamic policies with templating
- Secure secrets distribution from the Hub to managed clusters
- Can wrap other policy engines
- An extensive collection of policies
  - [github.com/stolostron/policy-collection](https://github.com/stolostron/policy-collection)
- Extensible framework for custom policy controllers



# OCM Policy API Concepts

- **Policy Templates** are the policies that perform a desired check or action
    - For example, **ConfigurationPolicy** objects
  - A **Policy** is a grouping mechanism for Policy Templates
  - Embedded Policy Templates are distributed to applicable managed clusters
  - A **PlacementBinding** binds a Placement to a Policy or PolicySet
  - A **PolicySet** is a grouping mechanism of Policy objects
- 
- More details can be found on the [open-cluster-management.io](https://open-cluster-management.io) website.

# Policy Templating

- Allows dynamic ConfigurationPolicy definitions
- Uses Go [text template](#) syntax (similar to Helm)
- The template functions can be executed on:
  - The Hub with “`{{hub ... hub}}`”
  - The managed cluster with “`{{ ... }}`”
- Example template functions
  - `{{ fromConfigMap "namespace" "name" "field" }}`
  - `{{hub fromSecret "" "name" "field" hub}}`
  - `http://{{ (lookup "v1" "Service" "default" "metrics").spec.clusterIP }}:8080`

# Demo

- Creating the “apps” Namespace with a pod security admission on clusters in the “detroit” data center

# Simplify Writing Policies

- The Policy Generator is a Kustomize generator plugin
- It simplifies writing policies, especially in a GitOps environment
- A Red Hat blog on the Policy Generator:  
<https://cloud.redhat.com/blog/generating-governance-policies-using-kustomize-and-gitops>

# OCM Policy Roadmap

- Improve Hub policy templates
- Policy order of execution
- Selective Policy Enforcement
- Improvements in the Ansible integration
- Making it easier to integrate with Kyverno
- Document how to install on a single cluster without the rest of OCM

# Get Involved

- GitHub: <https://github.com/open-cluster-management-io/OCM>
- Website: <https://open-cluster-management.io/>
- Docs: <https://open-cluster-management.io/concepts/>
- Slack: <https://kubernetes.slack.com/channels/open-cluster-mgmt>
- YouTube: <https://www.youtube.com/c/OpenClusterManagement>
- Mailing Group: <https://groups.google.com/g/open-cluster-management>
- Community Meetings:  
<https://calendar.google.com/calendar/u/0/embed?src=openclustermanagement@gmail.com>



**Open Cluster Management**  
<https://open-cluster-management.io/>