Ceph Day Chicago

Kubernetes-native IAM for Ceph object storage

Declarative access control for Kubernetes workloads using Ceph IAM and STS.

Billy Ridgway | IBM Senior Software Engineer



THE PROBLEM

Object storage access doesn't fit the Kubernetes model



Static Credentials

Long-lived S3 access keys stored in Kubernetes Secrets.



Manual IAM Management

Roles, policies, and permissions managed outside Kubernetes.



Disconnected Workload Identity

No declarative connection between Kubernetes ServiceAccounts and Ceph S3 permissions.

THE ANALOGY

Kubernetes RBAC, Applied to Object Storage

KUBERNETES		OBJECT STORAGE
ServiceAccount who the pod is	= THE SAME ONE	**ServiceAccount** no new identity to manage

THE ANALOGY

Kubernetes RBAC, Applied to Object Storage

KUBERNETES		OBJECT STORAGE
ServiceAccount who the pod is	= THE SAME ONE	**ServiceAccount** no new identity to manage
Role / Permissions verbs on resources	→	**PolicySpec** what the object storage permits

THE ANALOGY

Kubernetes RBAC, Applied to Object Storage

KUBERNETES		OBJECT STORAGE
ServiceAccount who the pod is	THE SAME ONE =	**ServiceAccount** no new identity to manage
Role / Permissions verbs on resources	→	**PolicySpec** what the object storage permits
RoleBinding subject ↔ role	→	**ObjectRoleBinding** ServiceAccount ↔ Ceph IAM role

DECLARE S3 ACCESS WITH ONE KUBERNETES RESOURCE

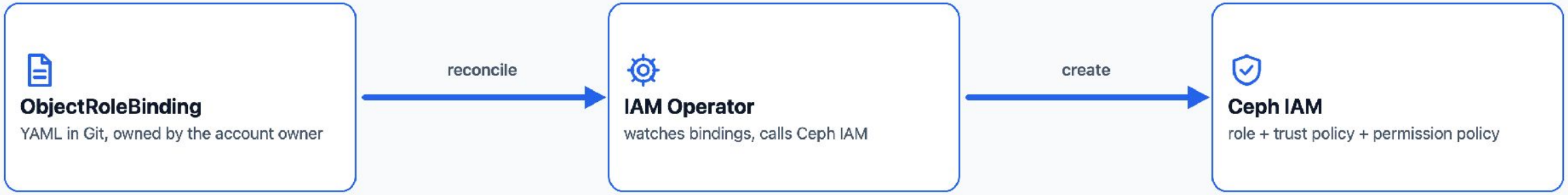
```yaml
apiVersion: storage.ceph.io/v1alpha1
kind: ObjectRoleBinding
metadata:
  name: spark-reports-read
  namespace: analytics
spec:
  objectAccountRef:
    name: analytics
  subjects:
  - kind: ServiceAccount
    name: spark-driver
    namespace: analytics
  policySpec:
    bucketAccess:
    - bucket: lake-data
      prefix: reports/
      permissions: ReadOnly
```

HOW IT WORKS

Declare, then vend

DECLARE — Control Plane

The operator continuously reconciles desired IAM state.

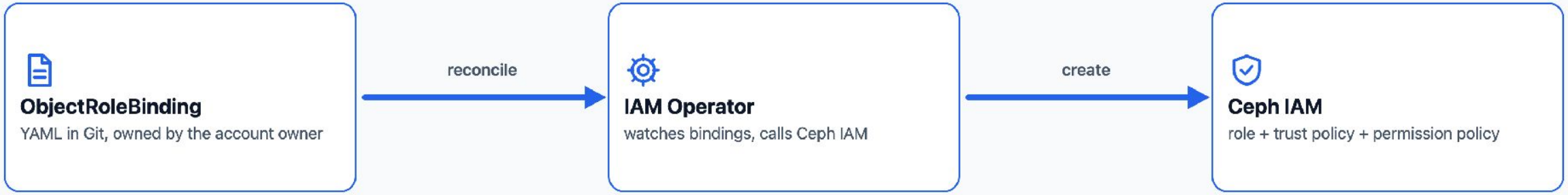


HOW IT WORKS

Declare, then vend

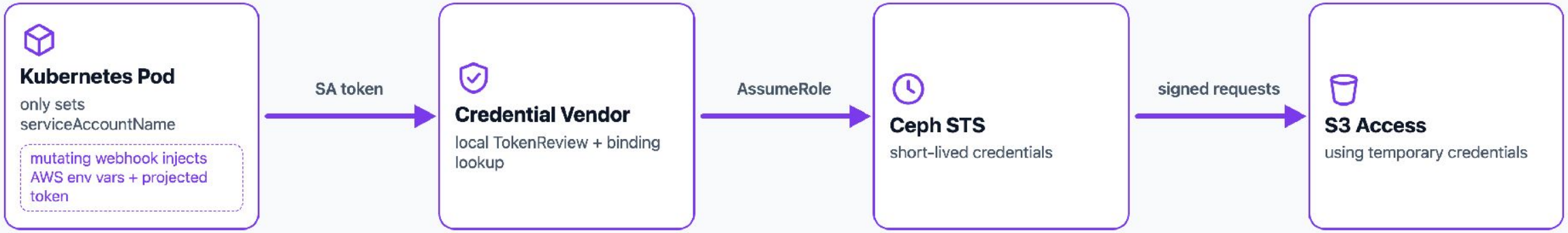
DECLARE — Control Plane

The operator continuously reconciles desired IAM state.



VEND — Runtime

Workloads acquire temporary credentials using their existing Kubernetes identities.

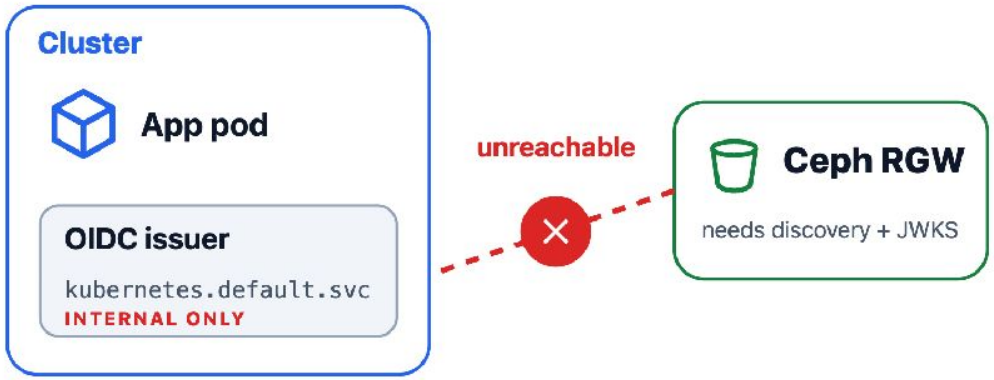


IAM state is continuously reconciled. Temporary credentials are issued on demand.

DESIGN DECISION

Supporting Kubernetes Clusters with Internal OIDC Issuers

Direct OIDC Federation

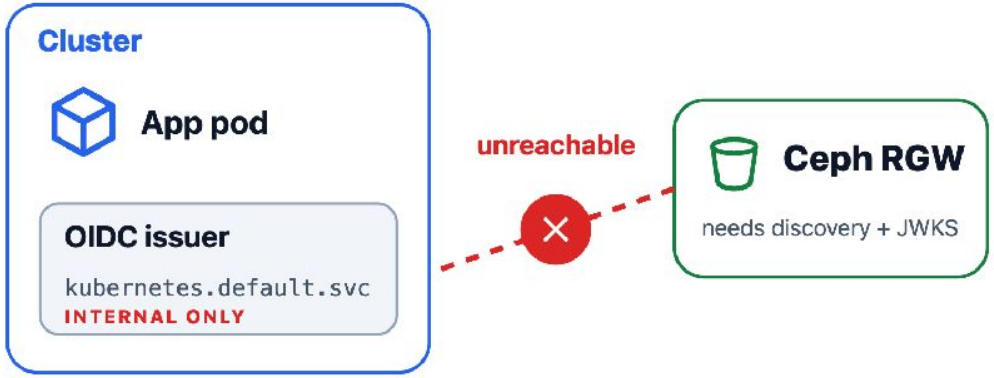


Requires an issuer with discovery and signing-key endpoints reachable by Ceph RGW.

DESIGN DECISION

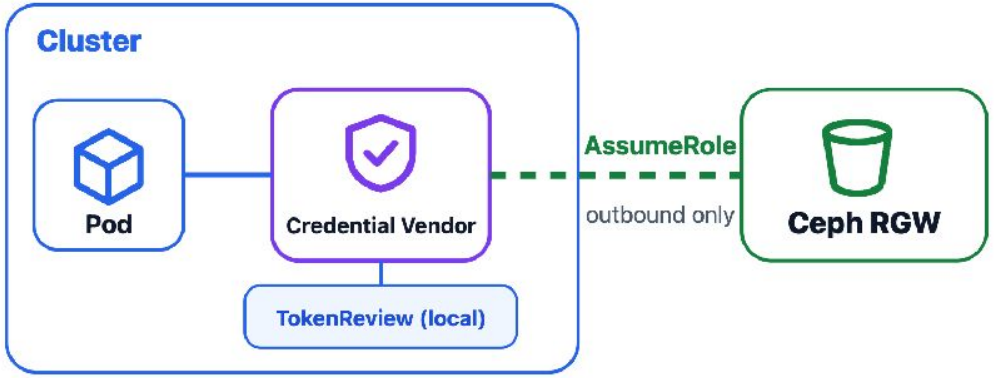
Supporting Kubernetes Clusters with Internal OIDC Issuers

Direct OIDC Federation



Requires an issuer with discovery and signing-key endpoints reachable by Ceph RGW.

Local Credential Vendor



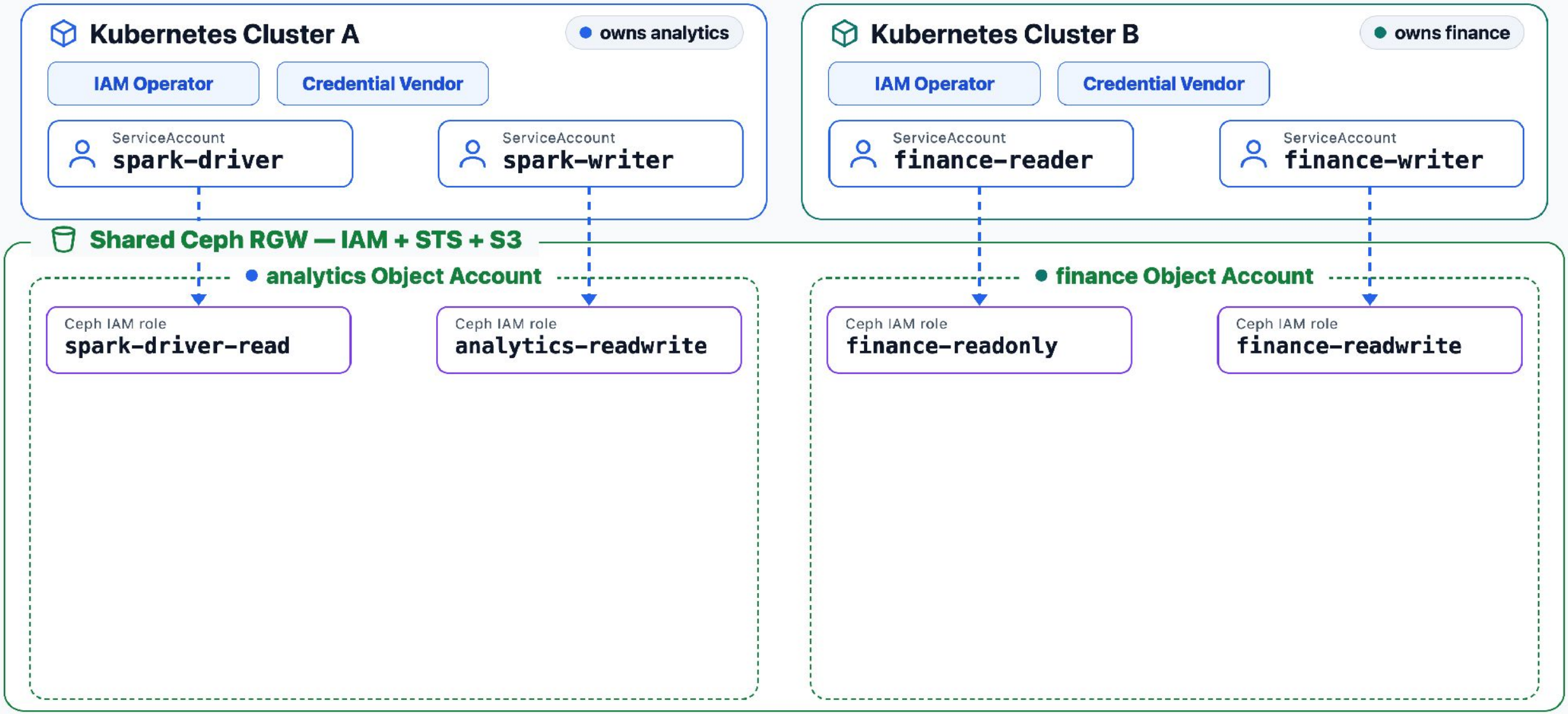
Validates Kubernetes ServiceAccount tokens locally, then obtains temporary credentials through Ceph STS.

Workload identity works even when Ceph cannot reach the Kubernetes OIDC issuer.

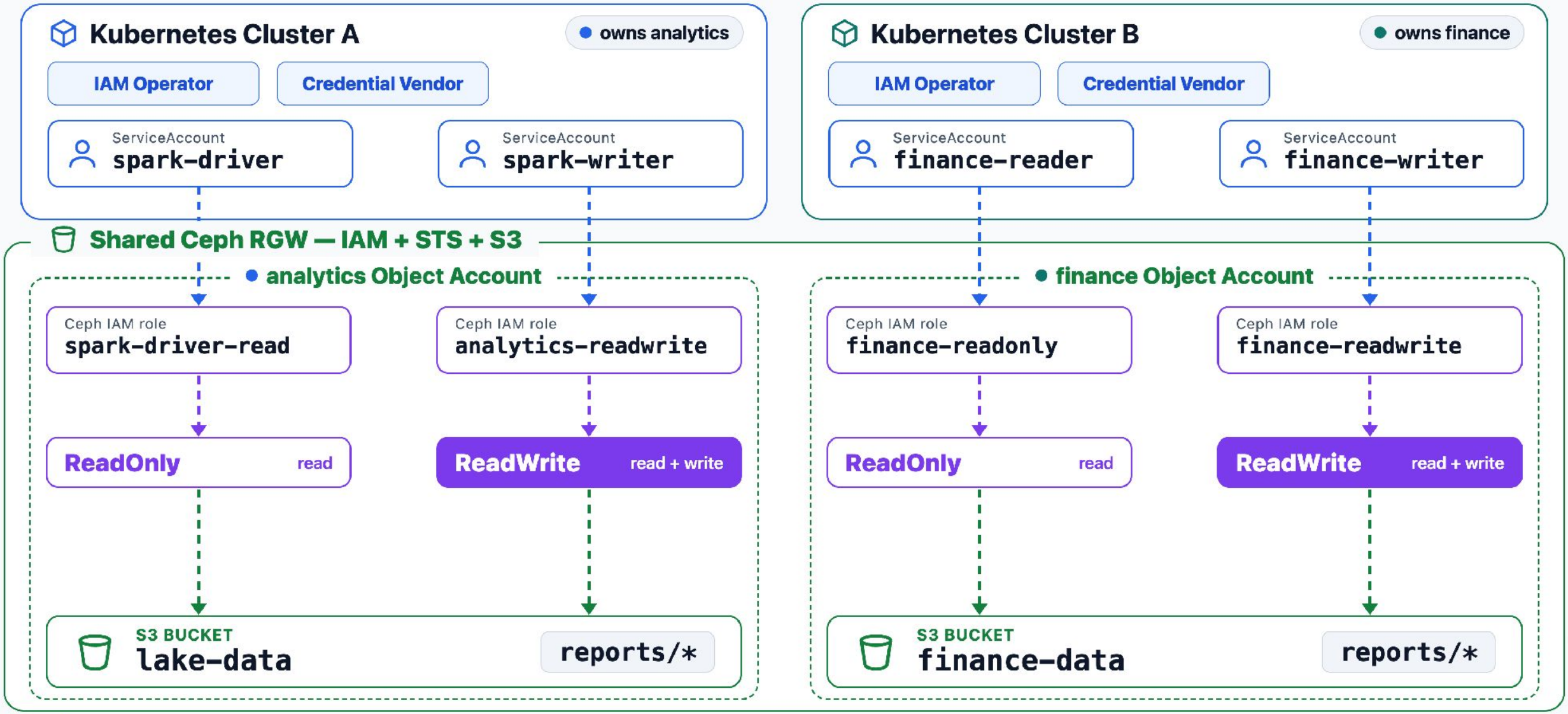
Scaling Declarative IAM Across Clusters



Scaling Declarative IAM Across Clusters

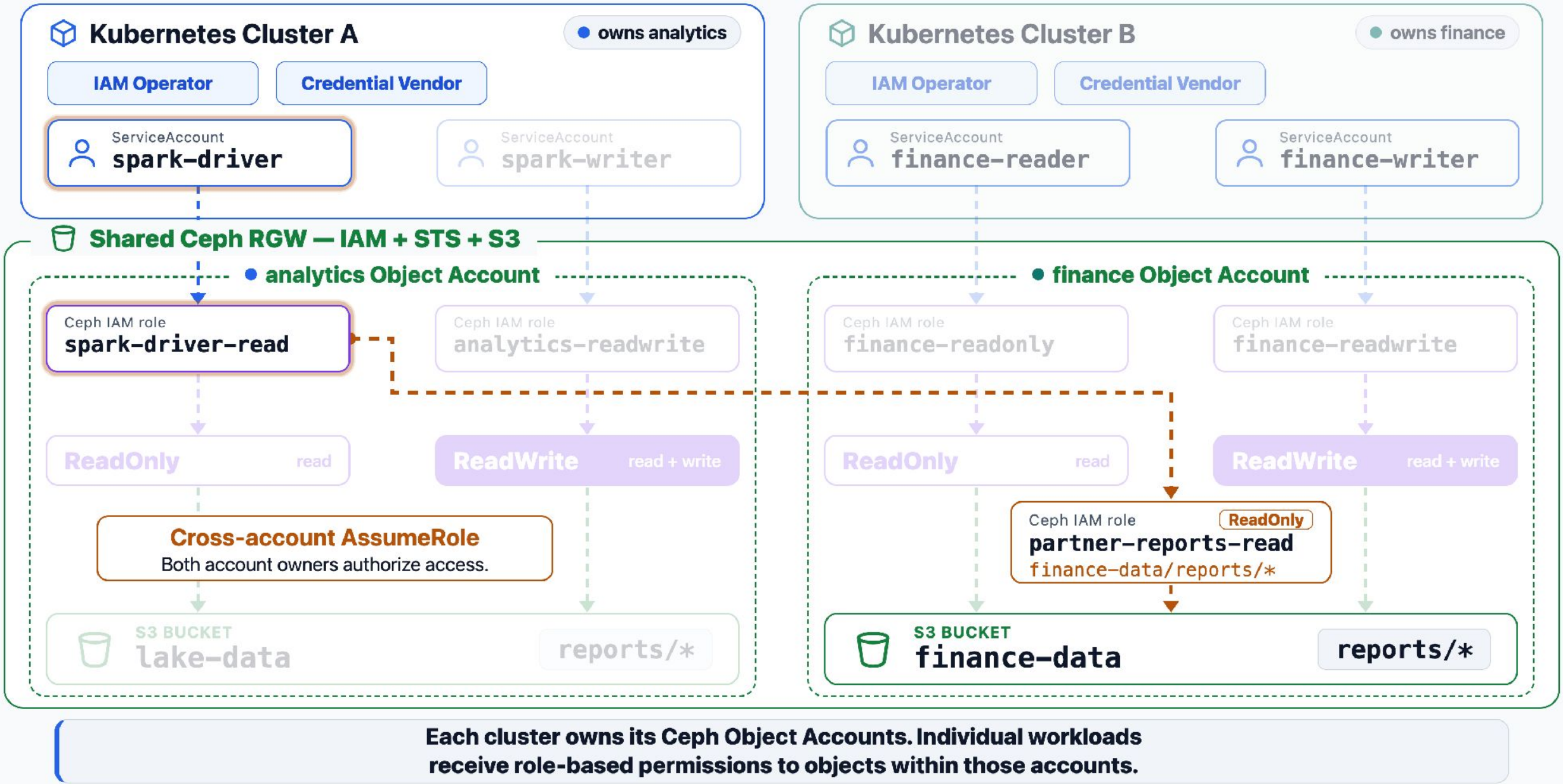


Scaling Declarative IAM Across Clusters



Each cluster owns its Ceph Object Accounts. Individual workloads receive role-based permissions to objects within those accounts.

Scaling Declarative IAM Across Clusters

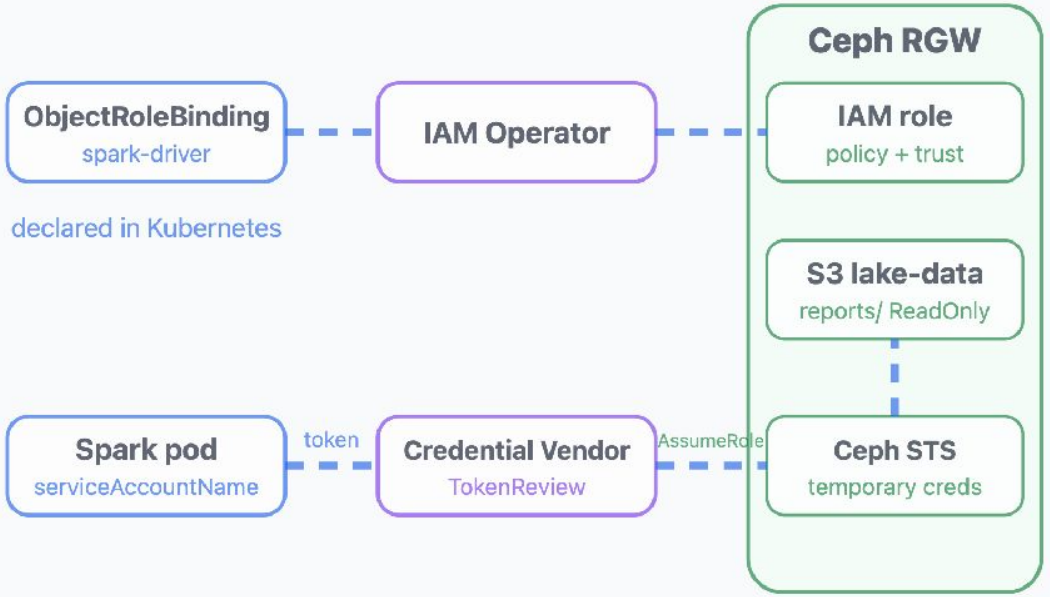


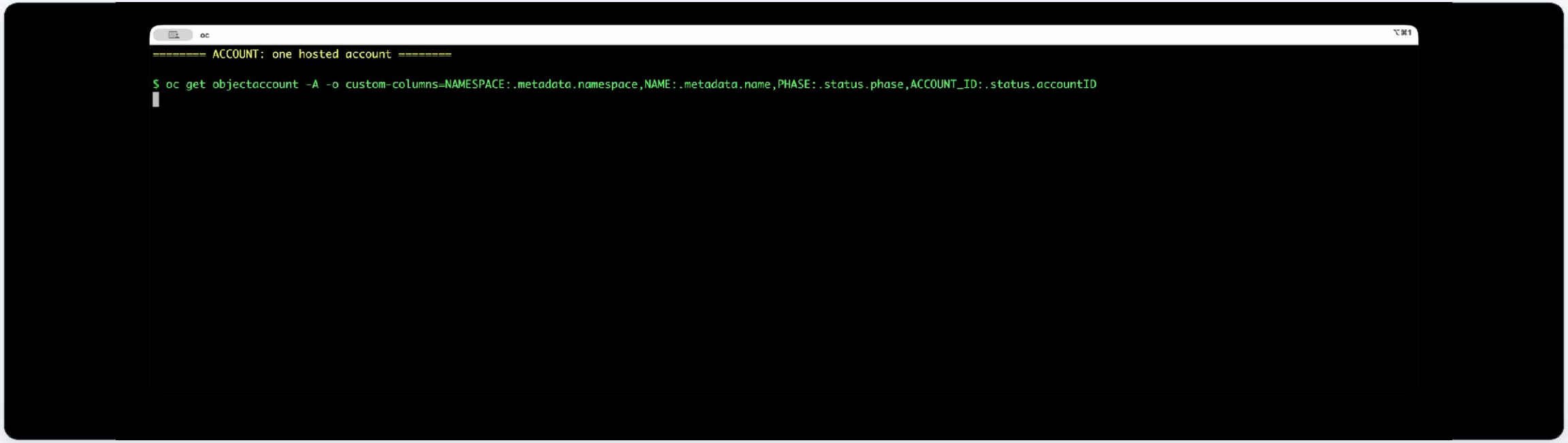
Each cluster owns its Ceph Object Accounts. Individual workloads receive role-based permissions to objects within those accounts.

PRE-RECORDED DEMO

From ObjectRoleBinding to S3 Access

1. Declare Access
2. Reconcile IAM
3. Spark — No Static Credentials
4. Revoke Access

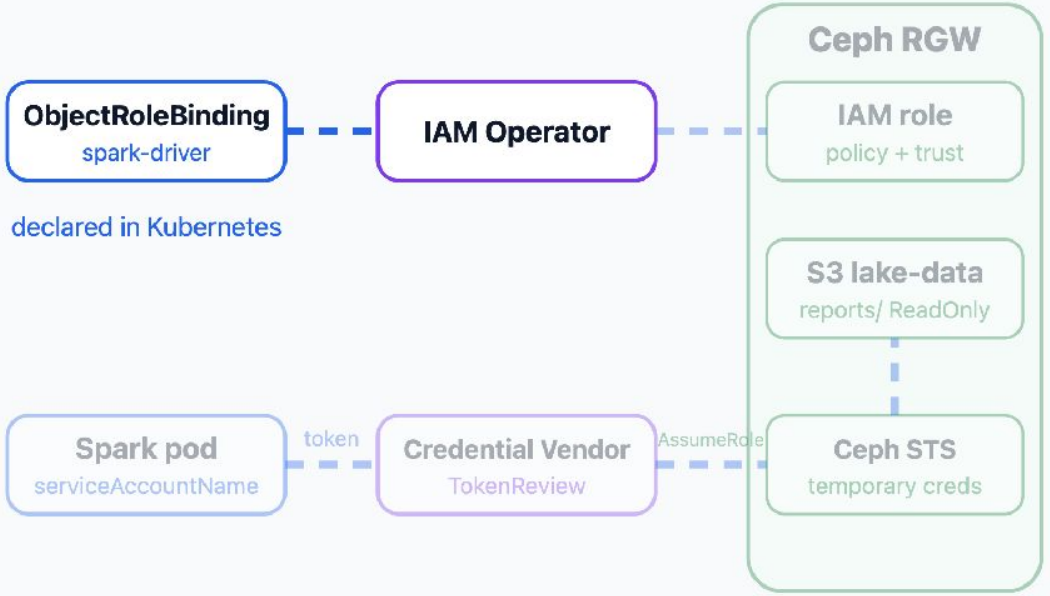




PRE-RECORDED DEMO

From ObjectRoleBinding to S3 Access

1. Declare Access
2. Reconcile IAM
3. Spark — No Static Credentials
4. Revoke Access



clear

```
======== DECLARE: the account owner states intent ========

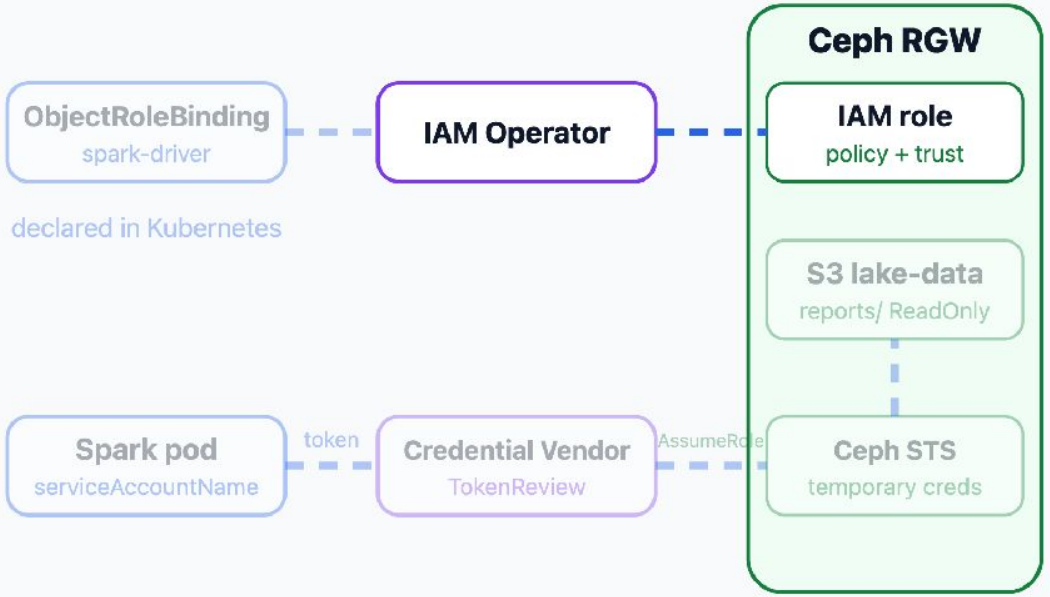
$ sed -n '/^apiVersion/,$p' manifests/10-objectrolebinding.yaml
apiVersion: storage.ceph.io/v1alpha1
kind: ObjectRoleBinding
metadata:
  name: spark-reports-read
  namespace: analytics
spec:
  objectAccountRef:
    name: analytics
    namespace: analytics
  subjects:
    - kind: ServiceAccount
      name: spark-driver
      namespace: analytics
  policySpec:
    bucketAccess:
      - bucket: lake-data
        prefix: reports/
        permissions: ReadOnly

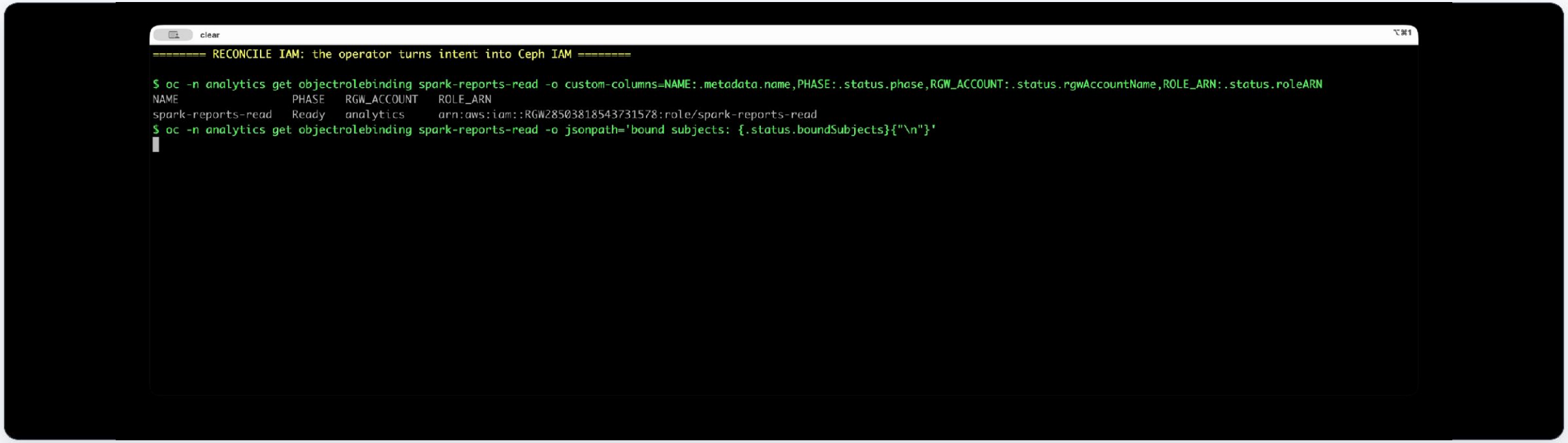
<Press Enter>
```

PRE-RECORDED DEMO

From ObjectRoleBinding to S3 Access

1. Declare Access
2. Reconcile IAM
3. Spark — No Static Credentials
4. Revoke Access

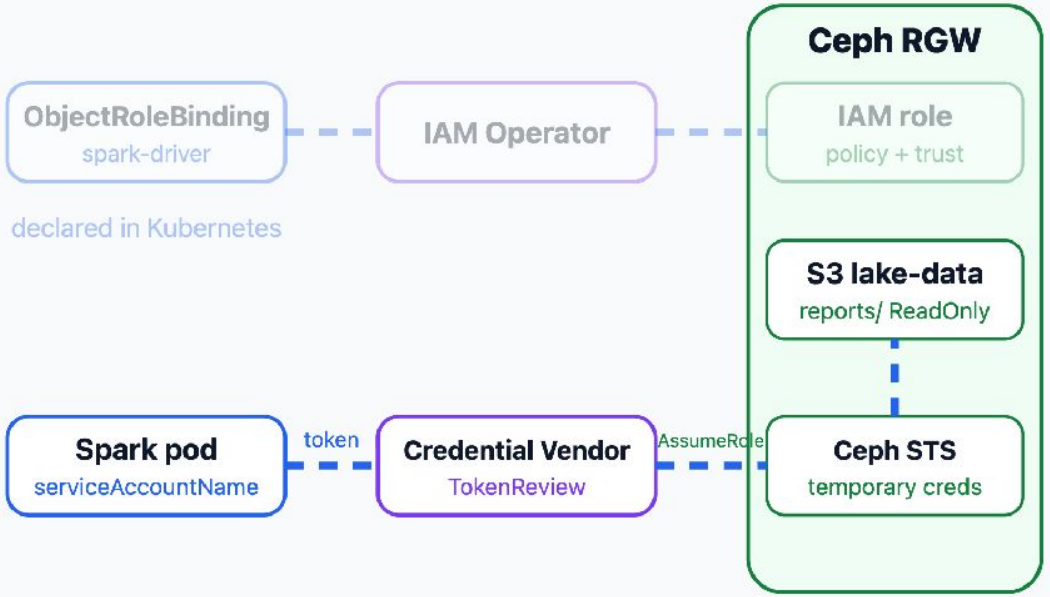




PRE-RECORDED DEMO

From ObjectRoleBinding to S3 Access

1. Declare Access
2. Reconcile IAM
3. Spark — No Static Credentials
4. Revoke Access




```
bash
======== VEND: the workload gets credentials without anyone handling a key ========

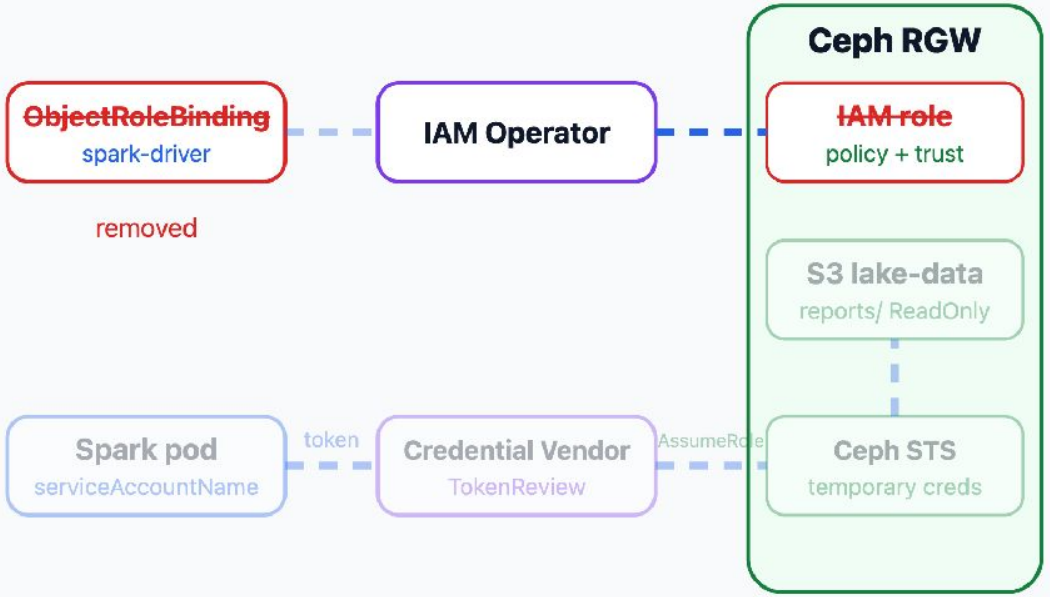
$ grep -n -B1 -A1 '^ *serviceAccountName:' manifests/30-spark-job.yaml
24-    spec:
25:      serviceAccountName: spark-driver
26-      restartPolicy: Never

<Press Enter>
```

PRE-RECORDED DEMO

From ObjectRoleBinding to S3 Access

1. Declare Access
2. Reconcile IAM
3. Spark — No Static Credentials
4. Revoke Access





Where do we go from here?

Thank you! Questions?