JioCloud

Container Registry

Overview

JioCloud's Container Registry gives you a fully managed, enterprise-grade platform to store, secure, and distribute container images at scale. Using trusted open standards and powered by Harbor, it brings everything together in one place - from vulnerability scanning and image signing to lifecycle management and audit logging. It also connects smoothly with your CI/CD pipelines and Kubernetes clusters, so your workflows staysimple and fast. From development to deployment, you stay in control, gain visibility, and meet security goals - without the hassle of managing the backend infrastructure.

Key Features

- **Private image storage**
  Keep your container images safe in a secure, isolated environment - built for enterprise use.
- **Role-based access control (RBAC)**
  Assign precise permissions by user, team, or project to ensure only the right people access the right images.
- **Vulnerability scanning**
  Auto scan images for known vulnerabilities (CVEs) during the build phase - so issues don't reach production.
- **Content trust and signing**
  Sign and verify every image before deployment - so you know exactly what's being pulled into your clusters.
- **High availability and replication**
  Distribute registries across regions to improve performance and add redundancy.
- **Image lifecycle policies**
  Set automated cleanup rules to remove unused or outdated images and keep storage lean.
- **Audit logging**
  Track who accessed what, and when - useful for compliance and internal reviews.
- **CI/CD ready**
  Plug into your existing CI/CD pipelines and Kubernetes clusters without extra steps.

JioCloud

Benefits

- **Faster delivery pipelines**
  Speed up your software rollout with secure, reliable image workflowsthat fit right into your delivery cycle.
- **Stronger security and governance**
  Build security into every stage - from image creation to deployment - without slowing teams down.
- **Less infrastructure to manage**
  Offload the hassle of running and maintaining registry infrastructure so you can focus on shipping code.
- **Better compliance made simple**
  Stay audit-ready with clear traceability and built-in logging across your image activity.
- **Room to grow**
  Whether you're handling thousands of pulls or managing large multi-team workloads - scale without slowing down.

Technologies Supported

- **Artifacts:** OCI/Docker images, Helm charts, OCI artifacts
- **Registry Core:** Harbor (CNCF)
- **Replication:** Harbor-to-Harbor, Harbor-to-DockerHub/ECR/ACR/GCR
- **Protocols:** OCI distribution spec, HTTPS
- **Integrations:** Jio CI/CD, Jio Cloud Kubernetes clusters

Technical Specifications

Availability and Scale

- Multi-AZ HA deployment (core, database, job service, registry, portal)
- Scalable block/object storage backend (Cinder, NetApp, S3-compatible)
- Configurable replication policies per project

Performance

- Layered caching and deduplication
- Parallel pushes/pulls with configurable rate limits

Security

- TLS-encrypted connections
- RBAC integrated with Jio Cloud SSO/LDAP/AD
- Signed and verified images

Data Protection

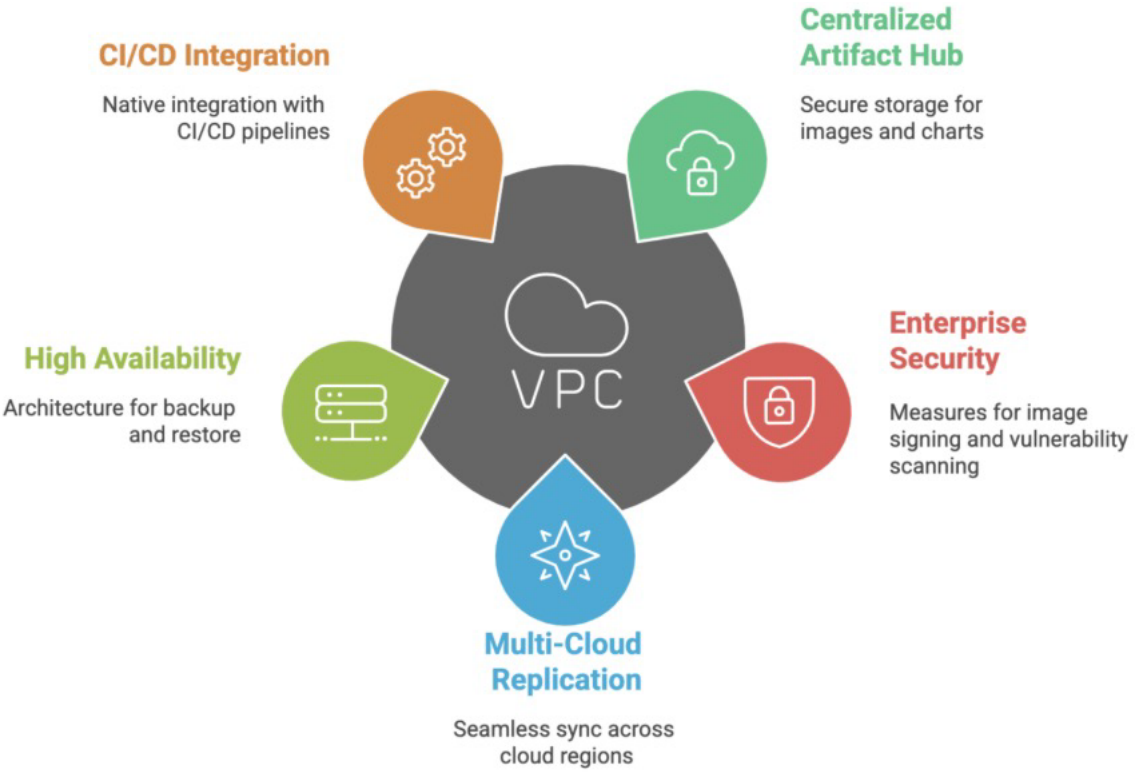
- Schedule backups of metadata and configurations
- Apply storage GC and retention policies
- Enable disaster recovery replication

JioCloud

Observability

- Monitor metrics on pushes, pulls, storage, and vulnerabilities
- Expose logs and audit trails via the Observability stack

Architecture Diagram



Use Cases

- **Ship faster, ship safer**
  Push signed images from your pipeline directly to a secure private registry.
  Teams can deploy with confidence across environments.

- **Secure every stage**
  Scan images early in the CI/CD flow to catch issues before they reach production.

- **Stay in control**
  Control access with RBAC, track changes through audit logs, and meet internal or external governance needs.

- **Optimize storage automatically**
  Clean up stale images with lifecycle policies - no manual tracking required.

- **OCI-compliant multi-tenant container registry**
  Multi-artefact/OCI compliance (Helm charts, OPAs, multi-arch images),
  Identity integration and SSO using Keycloak, Project quotas and multi-tenancy.