Customers run MinIO on Red Hat OpenShift for three reasons.

01.

Create and control AWS-like infrastructure where Kubernetes provides compute infrastructure and MinIO provides object storage.

02.

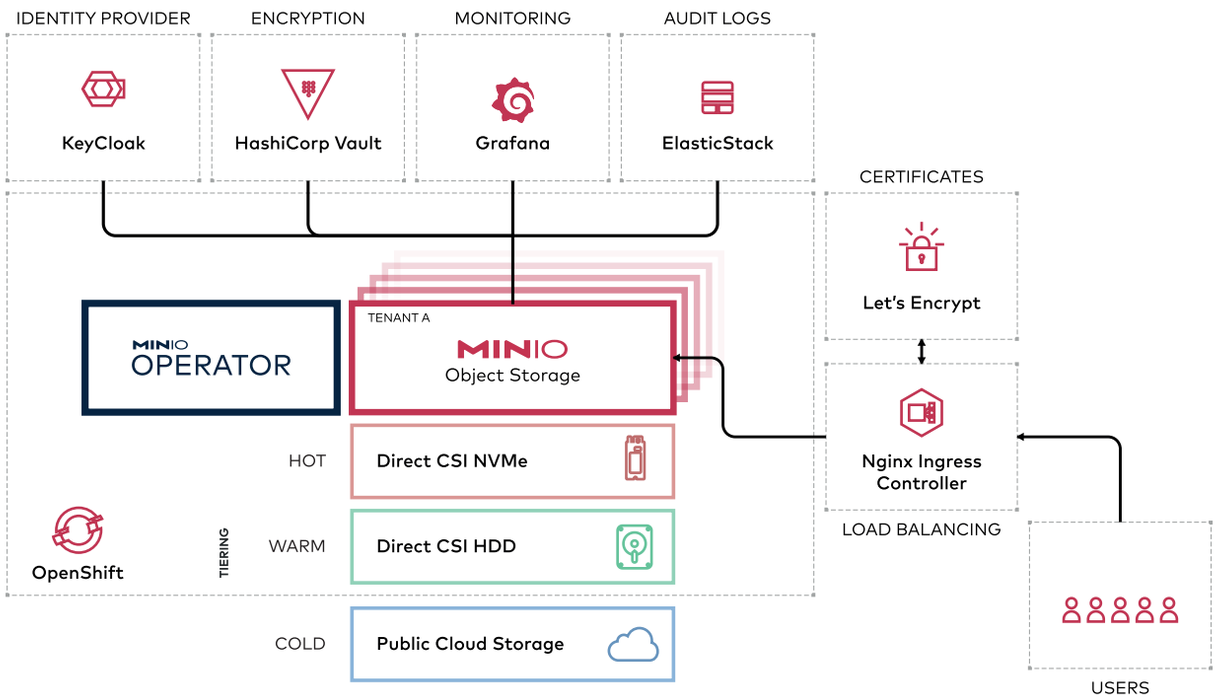
Unify disparate silos (enterprise IT, data/HDFS and modern workloads/apps) for greater efficiency, security and resiliency.

03.

Running MinIO on OpenShift provides control over the software stack with flexibility to avoid cloud lock-in.

Red Hat® OpenShift® is an enterprise-ready Kubernetes container platform with full-stack automated operations to manage hybrid cloud, multi-cloud, and edge deployments. OpenShift includes an enterprise-grade Linux operating system, container runtime, networking, monitoring, registry, and authentication and authorization solutions.

MinIO natively integrates with OpenShift making it easier to operate your own large scale multi-tenant object storage as a service. MinIO Operator works with the OpenShift toolchain, such as the oc OpenShift Cluster Manager CLI and the Quay container registry, ensuring you get the best out of your investment in the OpenShift ecosystem.



MinIO provides a consistent, performant and scalable object store because it is Kubernetes-native by design and S3 compatible from inception. Developers can easily get an Amazon S3 compatible persistent storage service for all of their cloud native applications running on OpenShift. Unlike AWS S3, MinIO enables the applications to scale across any multi-cloud and hybrid cloud infrastructure and still be managed within the OpenShift ecosystem, without public cloud lock-in.

MinIO Operator integrates natively with OpenShift features to provide:

Storage Classes and Tiering

Tier across NVMe, HDD and Public Cloud Storage.

The key requirement to deploy MinIO at scale on OpenShift is the ability tier across storage classes (NVMe, HDD, Public Cloud). This allows enterprises to manage both cost and performance.

MinIO supports automatic transition of aged objects from the fast NVMe tier to a more cost-efficient HDD tier and even cost-optimized cold Public Cloud storage tiers.

When tiering, MinIO presents a unified namespace across the tiers. Movement across the tiers is transparent to the application and is triggered by policies determined by the customer.

MinIO provides secure storage across an OpenShift hybrid cloud by encrypting objects right at the source - ensuring customers are always in complete control over the data. When OpenShift is deployed inside the public cloud the tiering functionality helps OpenShift efficiently manage data across persistent block storage and cheaper object storage tiers.

Encryption Key Management

Manage encryption keys with HashiCorp Vault.

There is no native OpenShift key management functionality. As a result, MinIO recommends using HashiCorp Vault to store keys outside of the object storage system. This is a best practice for cloud native applications.

For all production environments we recommend encryption to be enabled on all buckets by default. MinIO uses AES-256-GCM or ChaCha20-Poly1305 encryption to protect data integrity and confidentiality with negligible performance impact.

MinIO supports all of the three server-side encryption (SSE-KMS, SSE-S3 and SSE-C) modes. SSE-S3 and SSE-KMS integrates with the KMS on the server side, whereas SSE-C uses the client supplied keys.

MinIO will use this KMS to bootstrap its internal key encryption server (KES service) to enable high-performance, per object encryption. Each tenant runs its own KES server in an isolated namespace.

External Load Balancing

Load balance incoming requests with NGINX Ingress Controller.

All of MinIO's communication is based on HTTPs, RESTful APIs and will support any standard, Kubernetes compatible ingress controller. This includes hardware based and software defined solutions. The most popular choice is NGINX. Use the OperatorHub or the OpenShift Marketplace to install, then expose a MinIO tenant(s) using annotations.

Identity Management

Manage identity and policy with OpenID Connect compatible Keycloak IDP.

When running MinIO on OpenShift, customers can manage single sign-on (SSO) through a third party OpenID Connect/LDAP compatible identity provider like Keycloak, Okta/Auth0, Google, Facebook, ActiveDirectory and OpenLDAP. MinIO recommends OpenID Connect compatible Keycloak IDP.

An external IDP allows administrators to centrally manage user/application identity. MinIO builds on top of the IDP, providing AWS IAM-style users, groups, roles, policies and token service API. The ability to have a unified identity and access management (IAM) layer independent of the infrastructure provides significant architectural flexibility.

Certificate Management

Configure and manage certificates with OpenShift Certificate Manager and Let's Encrypt.

All traffic from the application to MinIO, including internode traffic, is encrypted with TLS. TLS certificates are used to secure network communications and establish the identity of network-connected resources, such as a MinIO server domain.

MinIO integrates with the OpenShift certificate manager so you can use the MinIO Operator to automatically configure, provision, manage and update certificates for the MinIO tenants. The tenants are completely isolated from each other in their own Kubernetes namespace with their own certificates for improved security.

Logging and Auditing

Output logs to an Elastic Stack for analysis.

Enabling MinIO auditing generates a log for every operation on the object storage cluster. In addition to the audit log, MinIO also logs console errors for operational troubleshooting purposes.

MinIO supports outputting logs to the Elastic Stack (or third parties) for analysis and alerting.

Monitoring and Alerting

Track metrics and issue alerts using OpenShift workload monitoring or Grafana.

MinIO recommends either Grafana, the platform monitoring components installed in the OpenShift-user-workload-monitoring project, or any other OpenShift container monitoring tool to connect to MinIO. MinIO publishes every object storage related Prometheus metric imaginable, from bucket capacity to access metrics. Those metrics can be collected and visualized in any Prometheus-compatible tool or the MinIO Console.

External monitoring solutions scrape the MinIO Prometheus endpoint at regular intervals. MinIO recommends either Grafana or the platform monitoring components installed in the `openshift-user-workload-monitoring` project to connect to MinIO. These same tools can also be used to establish baselines and set alert thresholds for notifications, which can then be routed to a notification platform such as PagerDuty, Freshservice or even SNMP.

MinIO offers the most deployment options of any object storage across hybrid, multicloud and edge environments using Kubernetes. Red Hat OpenShift users can quickly and easily deploy multi-tenant MinIO object storage within their existing environment.

The MinIO Kubernetes Operator supports end-to-end configuration and deployment of MinIO tenants, seamlessly integrating with supporting infrastructure for storage tiering, monitoring, audit logging, identity management, certificate management, key management for automatic server-side object encryption and load balancing and ingress.

Learn more at **min.io** or try it for yourself at **min.io/download**. Join the conversation at **minio.slack.com**.