MINIO | MICROSOFT AZURE KUBERNETES SERVICE

Customers run MinIO on Microsoft Azure Kubernetes Service (AKS) for three reasons.

01.

MinIO serves as the consistency layer in a hybrid cloud or multi-cloud deployment, bringing S3 API compatibility to Azure and enabling AI/ML workload portability.

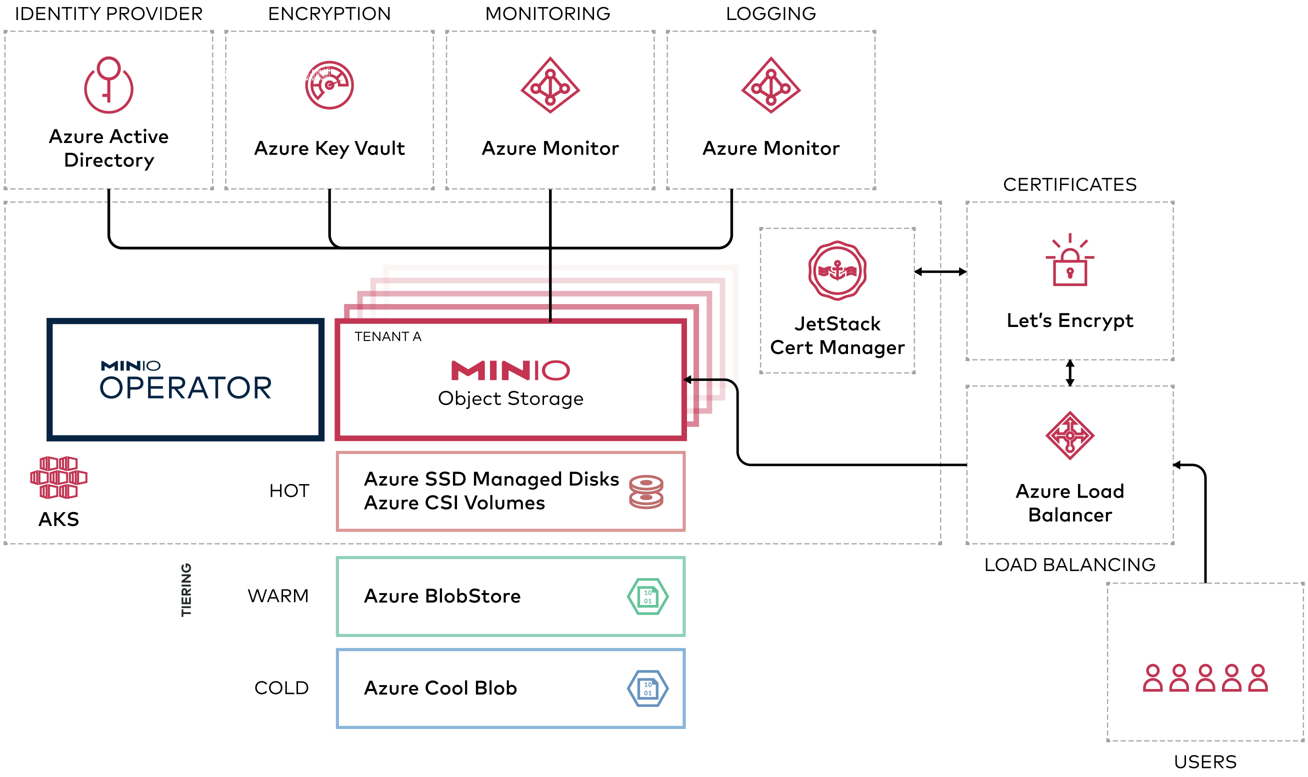
02.

MinIO is Kubernetes native and high performance it can deliver predictable performance across public, private and edge cloud environments.

03.

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

AKS is a highly available, secure and fully managed Kubernetes service from Microsoft Azure. Azure Kubernetes Service (AKS) offers serverless Kubernetes, an integrated continuous integration and continuous delivery (CI/CD) experience, and enterprise-grade security and governance.



MinIO provides a portable high-performance object storage system across all of the major Kubernetes platforms (AWS, Tanzu, GCP, OpenShift). Developers can easily get an Amazon S3 compatible persistent storage service for all of their cloud native applications running on AKS. Unlike AWS S3, MinIO enables the applications to scale across any multi-cloud and hybrid cloud infrastructure, without requiring expensive software rewrites or proprietary integrations.

MinIO Operator integrates natively with AKS and Azure features to provide:

Storage Classes and Tiering

Tier across Azure SSD Managed Disks (Azure CSI Volumes), Azure BlobStore and Azure Cool Blob.

The key requirement to deploy MinIO at scale on Azure and AKS is the ability tier across storage classes (Azure SSD Managed Disks, Azure BlobStore, Azure Cool Blob). This allows enterprises to manage both cost and performance.

MinIO can be configured to automatically transition aged objects between AKS storage classes, moving objects from the hot Azure SSD Managed Disks tier to cost-efficient warm Azure BlobStore and cold Azure Cool Blob storage tiers.

When tiering, MinIO maintains a single object storage namespace by transparently retrieving transitioned objects without additional client-side logic. Objects can be moved back to the performance-optimized hot tier using the S3 Restore API.

This same capability also extends to hybrid cloud environments where the JBOD/JBOF act as the hot tier on the private cloud side and Azure BlobStore acts as the warm and Azure Cool Blob as the cold tier. The data on the public cloud remains encrypted - ensuring that data is safe at rest and in flight.

Encryption Key Management

Manage encryption keys with Azure Key Vault.

For cloud-native applications, the best practices dictate storing keys outside of the object system in an external vault. Azure Key Vault (AKV) is a secure and resilient service for managing keys by API across Azure services.

For those with more stringent security requirements or for consistency purposes, MinIO integrates with a number of external Key Management Services that operate outside of Azure.

When using MinIO as the object storage in a public instance of AKS, encryption on-disk is strongly recommended. MinIO uses AES-256-GCM or ChaCha20-Poly1305 encryption to protect data integrity and confidentiality without impacting performance. The MinIO Operator allows for tenants to be configured for the Azure Key Vault or a supported third-party KMS for automatic server-side encryption of objects.

MinIO supports setting a bucket-level default encryption key in the KMS with support for AWS-S3 semantics (SSE-S3). Clients can also specify a separate key on the KMS using SSE-KMS request headers.

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 Azure Load Balancer.

AKS offers built-in Azure Load Balancer to provide automatic load balancing and routing services across multiple MinIO tenants for applications accessing the storage service from outside of AKS. Exposing a MinIO tenant to external traffic can be done by simply adding annotations to a MinIO tenant.

Identity Management

Manage identity and policy with Azure ActiveDirectory.

When running MinIO on AKS, customers can manage single sign-on (SSO) through Azure ActiveDirectory or third party OpenID Connect/LDAP compatible identity providers like Okta/Auth0, Google, Facebook, Keycloak and OpenLDAP.

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 JetStack 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.

AKS uses Jetstack cert-manager to automatically generate and configure Let's Encrypt certificates. MinIO integrates with the Jetstack cert-manager so you can use the MinIO Operator to 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 Azure Monitor 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 sending logs to the Azure Monitor and using the Log Analytics features.

Monitoring and Alerting

Track metrics and issue alerts using Azure Monitor.

MinIO recommends using Azure Monitor as a Prometheus-compatible system for monitoring and alerting when deploying MinIO on AKS. MinIO publishes every object storage related Prometheus metric imaginable, from bucket capacity to access metrics. Those metrics can be collected and visualized in Azure Monitor, Grafana, the MinIO Console or any Prometheus-compatible tool already being used for Azure Kubernetes Service monitoring.

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. Microsoft Azure Kubernetes Service 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**.