MINIO | VMWARE TANZU

Customers run MinIO on VMware Tanzu for three reasons.

01.

MinIO is pre-bundled in VSphere 7.0 U1 and onwards and provides a native integration with the vSAN Data Persistence platform - for which MinIO was a design partner.

02.

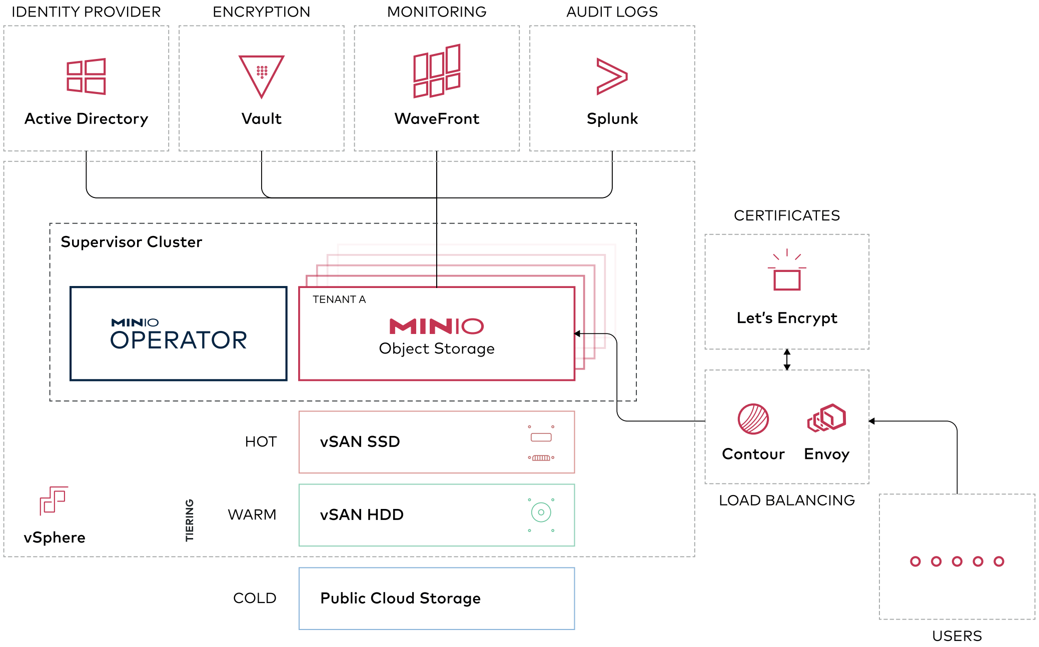
VMware customers can rapidly and easily deploy multi-tenant object-storage-as-a-service with just a few clicks in the vCenter console.

03.

Using a specific integration with the DPp called vSAN Direct, customers can achieve direct control over the underlying hardware to deliver greater performance, scalability and security.

VMware Cloud Foundation™ with Tanzu™ accelerates Kubernetes infrastructure provisioning with full-stack consisting of compute, storage, networking, and management. Through automatic and reliable deployment of multiple workload domains, it increases admin productivity while reducing overall TCO to deliver a faster path to a hybrid cloud.

MinIO provides a portable high-performance object storage system across all of the major Kubernetes platforms (AWS, Azure, GCP, OpenShift). Developers can easily get an Amazon S3 compatible persistent storage service for all of their cloud native applications running on Tanzu Application Service (TAS) or Tanzu Kubernetes Grid (TKGI).



Through this integration, IT administrators can create and manage tenants, without requiring DevOps skills. Those administrators can then enable their application teams to self-serve object storage within the policy and security framework designed by the IT function. This approach allows the organization to employ containers or virtual machines on the same infrastructure - facilitating their application modernization journey.

MinIO Operator leverages VMware Tanzu features to provide:

Storage Classes and Tiering

Tier across vSAN Direct, vSAN (SSD, HDD) and public cloud storage.

MinIO supports all three storage vSAN configurations: vSAN, vSAN SNA, vSAN Direct. MinIO recommends vSAN Direct in almost all cases as it provides direct local access to the drives. This is the equivalent of gaining JBOD-like access, enabling MinIO to handle distributed erasure code, high availability, fault tolerance and encryption.

Tiering within MinIO enables you to cost-effectively scale storage capacity to petabytes.

MinIO can automatically transition aged objects from the "hot" VMware DPp tier to a cost-efficient HDD VMware DPp tier. To optimize for cost, tiering can be configured to use the public clouds. For example, MinIO can be configured to automatically transition objects from DPp tiers to AWS S3 IA, Google Cloud Storage, or Azure Blob Storage. MinIO protects data stored in DPp and the public cloud using encryption.

Encryption Key Management

Manage encryption keys with HashiCorp Vault.

MinIO supports using Hashicorp Vault, Amazon KMS, Google Cloud KMS and Thales CipherTrust (formerly Gemalto KeySecure) for Key Management Services (KMS). These choices are available in the vCenter interface for MinIO. MinIO recommends Hashicorp Vault.

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 tenants require access to the configured KMS, whether the KMS is internal or external to the Tanzu infrastructure. The only requirement on the KMS is to provide access to one or more Customer Master Keys (CMK) for use with MinIO server-side encryption. MinIO manages cryptographic operations using the CMK at scale for per-object server-side encryption at high speed. Server-side encryption can be automatically enabled using a supported KMS during tenant creation.

MinIO supports enabling both automatic tenant-wide object encryption and bucket-level encryption using SSE-S3 semantics. Clients can also specify SSE-KMS headers to specify a per-object CMK.

External Load Balancing

Load balance incoming requests with Contour and Envoy.

MinIO manages TLS automatically for applications running within Tanzu. Certificate management and ingress are required to provide access to applications running outside of the Kubernetes environment.

VMware recommends using the Contour Ingress Controller and Envoy Load Balancer extensions to automatically distribute incoming application traffic across multiple targets, including MinIO tenant pods and services.

The MinIO Operator integrates completely with the Contour and Envoy extensions to provide automatic load balancing and routing services across multiple MinIO Tenants. Exposing a MinIO tenant to external traffic is done automatically as part of tenant deployment via the vCenter interface.

Identity Management

Manage identity and policy with OpenID Connect over LDAP.

When running MinIO on Tanzu, customers can manage single sign-on (SSO) through a third party OpenID/LDAP compatible identity provider like Keycloak, Okta/Auth0, Google, Facebook, ActiveDirectory and OpenLDAP. MinIO anticipates that most customers will use Microsoft Active Directory identity platform. MinIO recommends OpenID Connect (OIDC) over the LDAP protocol.

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 any ACME compatible solution.

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.

MinIO integrates with any ACME protocol compatible Certificate Manager 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 Elasticsearch or Splunk 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 Splunk, Elasticsearch and others for analysis and alerting.

Monitoring and Alerting

Track metrics and issue alerts using Wavefront or Grafana.

MinIO recommends using Prometheus-compatible systems for VMware Tanzu monitoring and alerting. 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 Wavefront or Grafana depending on architectural goals and Tanzu observability requirements. 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. VMware Tanzu 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**.