kemp

SOLUTION BRIEF

Zero Trust Object Storage Access Control

Kemp load balancers deliver the most flexible, scalable, and easy-to-deploy zero-trust model on the market, providing businesses with a highly granular policy-based access control.

Kemp load balancers optimize object storage environments by enforcing QoS policies, enabling distributed single-namespace deployment, and providing frontend proxy optimization.

The Challenge

Object storage is a data storage model that treats data as objects as opposed to a hierarchical file system. It is seeing increased usage in modern applications thanks to the unquestionable benefits of the ease of bringing in new data sources, cost control, efficiency, scalability, and detailed data analytics.

However, as a critical infrastructure component, ensuring its security is vital.

Why Kemp?

Access to storage objects or buckets typically passes through a load balancer, which makes Kemp load balancers optimally positioned for applying zero-trust security models and ensure compliant and policy-based access control.

The Kemp model provides granularity that is hard to achieve otherwise. It tailors itself to your data access policy, ensuring maximum protection of your business-critical assets. For maximum ease of use, the solution is packaged and includes a policy-builder, making it the most accessible and rapidly-deployable zero trust access control solution out there.

Main Features

- Default least privileged security model
- Fine-grained access control
- Security zone-based policy logic
- Bucket and object-level policy application
- Storage operation awareness

Key Benefits

- **Security zone identification** - Network segmentation awareness to determine the trust level of security zones at initial connection attempt.
- **Transparent Visibility** – Traffic flow decryption and network telemetry can combine with a network monitoring solution to enable detailed analysis of transactions and forensics.
- **Identify Context** - Analysis of authentication headers, IdP validation (if leveraged) along with other traffic flow characteristics enables application identity validation and enforcement of appropriate policies.
- **Intent Analysis** - Determine entitlement and enforce controls around allowable storage transaction types.
- **Granular Policy Application** - Flexibility to determine which abstraction layer the policies are applied to (i.e. network, storage bucket, etc.).

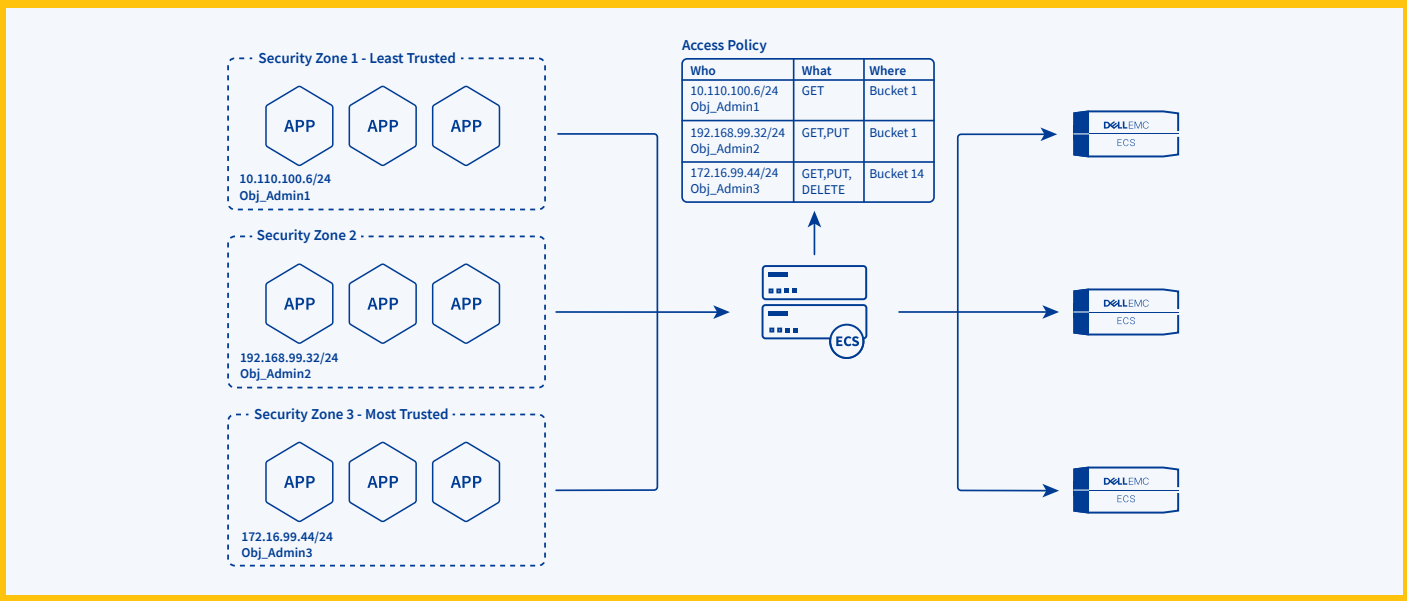
How it Works

In a standard deployment, network segments where client applications reside are assigned to different security zones along with dedicated authentication artefacts.

With a Kemp load balancer acting as a zero-trust access gateway, these attributes are leveraged to control S3 storage operations on a published virtual service. An API-based policy builder framework enables the automated definition, application, and maintenance of complex object storage access policies.

All that is required of the user is to define the client network IP addresses and security zones. With the zero-trust policy thus defined, the system will apply it automatically.

Kemp's zero-trust model of object storage access provides a peerless level of control, granularity, and ease of use in the most innovative approach to data storage out there.



About Kemp

Kemp powers the secure, always-on application experience [AX] that enterprises and service providers demand. Kemp's load balancing, network performance monitoring, and network detection and response solutions deliver maximum value through simplified deployments, flexible licensing, and top-rated technical support. Kemp is the world's most-popular application experience solution with more than 100,000 deployments in 138 countries. Take control of your AX at kemp.ax.