White Paper

AEROSPIKE CLOUD MANAGED SERVICE

Security by design for the Aerospike Cloud Managed Service

AEROSPIKE

Contents

Introduction

As companies migrate workloads to the cloud and develop new cloud-native applications, CIOs and CSOs face the grim reality of maintaining a secure cloud environment that aligns with their operations and provides value to the business. Aerospike offers a fully managed service engineered to meet these security and compliance requirements while accelerating time-to-value.

The Aerospike Cloud Managed Service (ACMS) deploys and manages Aerospike database clusters in a dedicated virtual private cloud (VPC) account with a framework that hides the complexity of securing, monitoring, and auditing database activities while enabling firms to build a secure and reliable foundation for their digital efforts in the cloud.

In The State of Cloud-native Security published in 2022, Palo Alto Networks (not affiliated with Aerospike) reported that organizations expanded their use of cloud infrastructure by more than 25% over previous years but struggled with security, compliance, and technical complexity. Companies with a clear and robust security protocol are more likely to have low friction levels and improved workforce productivity.

Highlights

- **Architected for Security and Compliance**
  Built on years of experience architecting and managing the Aerospike real-time data platform both on-premises and in the cloud, is like having your own specialized data platform security team.
- **Agility and flexibility**
  Delivering new digital value to your customers rather than managing databases and infrastructure.
- **Staff optimization**
  Aerospike takes the responsibility for delivering and maintaining an optimized deployment of the industry's most resilient, low latency, high-scale real-time data platform, your team can focus on delivering world-class applications.

This white paper explores and explains the policies, technologies, and controls of the Aerospike Cloud Managed Service. It also describes the roles and responsibilities for operational controls, highlighting how the ACMS security framework reduces friction and enhances productivity. For further details, please visit the ACMS web page or read the Solution Brief.

Benefits

- **Operational simplicity and efficiency**
  With Aerospike managing your environment, your staff can focus on your business rather than on designing and maintaining the Aerospike deployment.
- **Security and access management**
  Enterprise-class features provide security and operational controls for authentication, authorization, auditing, and more.

- **Enterprise-ready**
  Aerospike's flexible storage engine delivers predictable performance up to petabyte-scale using In-Memory or Hybrid Memory Architecture (HMA) namespaces.
- **Predictable controls**
  Workload profiling identifies the correct capacity plan and optimized configuration templates to help customers budget appropriately and avoid unforeseen costs.

Key factors in cloud security

Responsibility for cloud security is shared between users, providers, and administrators. Successful implementation of any cloud solution relies on best practices, tools, and technology. With the experience of deploying countless clusters in many different environments from development to production, Aerospike has developed a security framework that involves human capital and technology resources that adhere to international standards as demonstrated by the ISO 17001 and SOC 2 certifications.

Aerospike divides responsibilities for access management along the traditional lines of infrastructure and data management: ACMS has exclusive access and control of the infrastructure and the customer has exclusive access and control of the data. These lines are enforced through policies and tools to satisfy your data security policies.

Role-based access controls use a least-privileged model, limiting team members to the minimum access levels necessary for their required tasks.

ACMS organizes access levels in a tiered system with an on-call triage team providing 24x7 responses for change requests and an escalation team with additional expertise in infrastructure, database, and cloud management.

Network security

ACMS follows zero-trust principles. Clusters are located in the customer cloud account and isolated in a secure VPC. External access to the clusters is controlled through a VPC peering connection to ensure only approved applications can access the cluster. Intra-cluster communication uses TLS encryption for all network connections. Fig. 1 illustrates the overall architecture of ACMS, which is designed for high availability and data security.

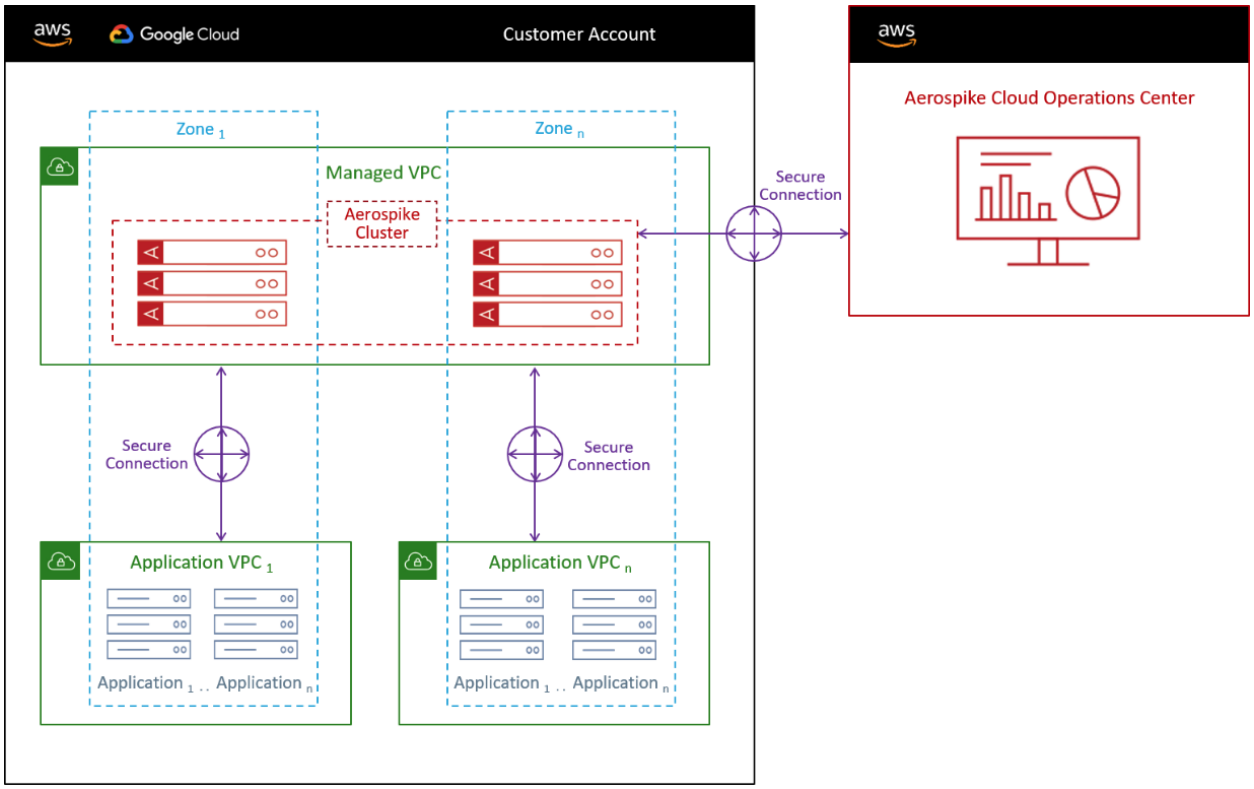

Figure 1: High-level architecture of the Aerospike Cloud Managed Service

The ACMS network configuration has two primary channels:

- Application access to Aerospike database clusters
- ACMS access to infrastructure deployed in the customer environment

Each channel has its own set of rules and configurations to isolate, optimize, and protect the communications between the different elements of the system.

Cloud Console

The Aerospike Cloud Console provides customers with a dashboard to request configuration changes to clusters. ACMS personnel implement those changes. The Cloud Console also presents aggregated Aerospike Metrics and SLA information, allowing customers to view high-level health, configuration, and performance of Aerospike clusters under management. For security, the Cloud Console HTTPS endpoints are protected by industry-standard TLS encryption, OpenID Connect and OAuth 2.0 based authentication and authorization, and a web application firewall with real-time monitoring.

Application access to Aerospike database clusters

Fig. 2 shows the connections from the application environment to the Aerospike-managed environments. Note that all these instances are running in the customer cloud account.

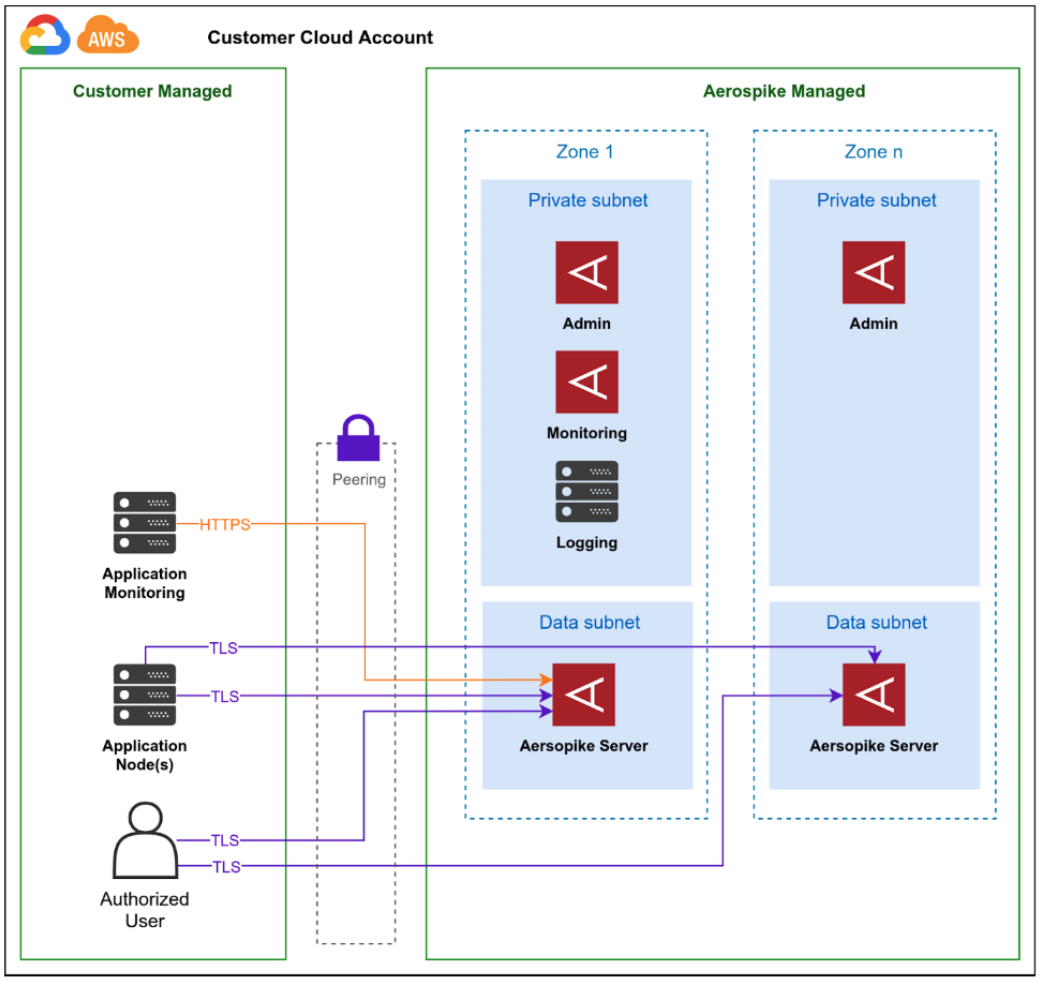

Figure 2: Application access to Aerospike database clusters

Database connections

Database connections (aka service connections) from users and applications are only allowed from application nodes or authorized users (e.g., database administrators) to Aerospike server nodes. Traffic is encrypted with TLS and restricted using cloud firewall rules and Aerospike Access Control.

Aerospike Monitoring

ACMS uses the Aerospike Monitoring Stack to collect cluster metrics and evaluate current operating conditions to initiate warnings and alerts. A Prometheus service running in the private subnet collects data from every host for use by the ACMS operations team. It is important to note that only Aerospike Metrics are collected and stored on the monitoring server which does not include any data stored within the database.

ACMS access to infrastructure deployed in customer account

As shown in Fig. 3, ACMS creates a secure inbound connection to access and manage the infrastructure deployed in the customer cloud account. These secure connections employ several controls to enable Aerospike employees to administer the environment, as explained shortly.

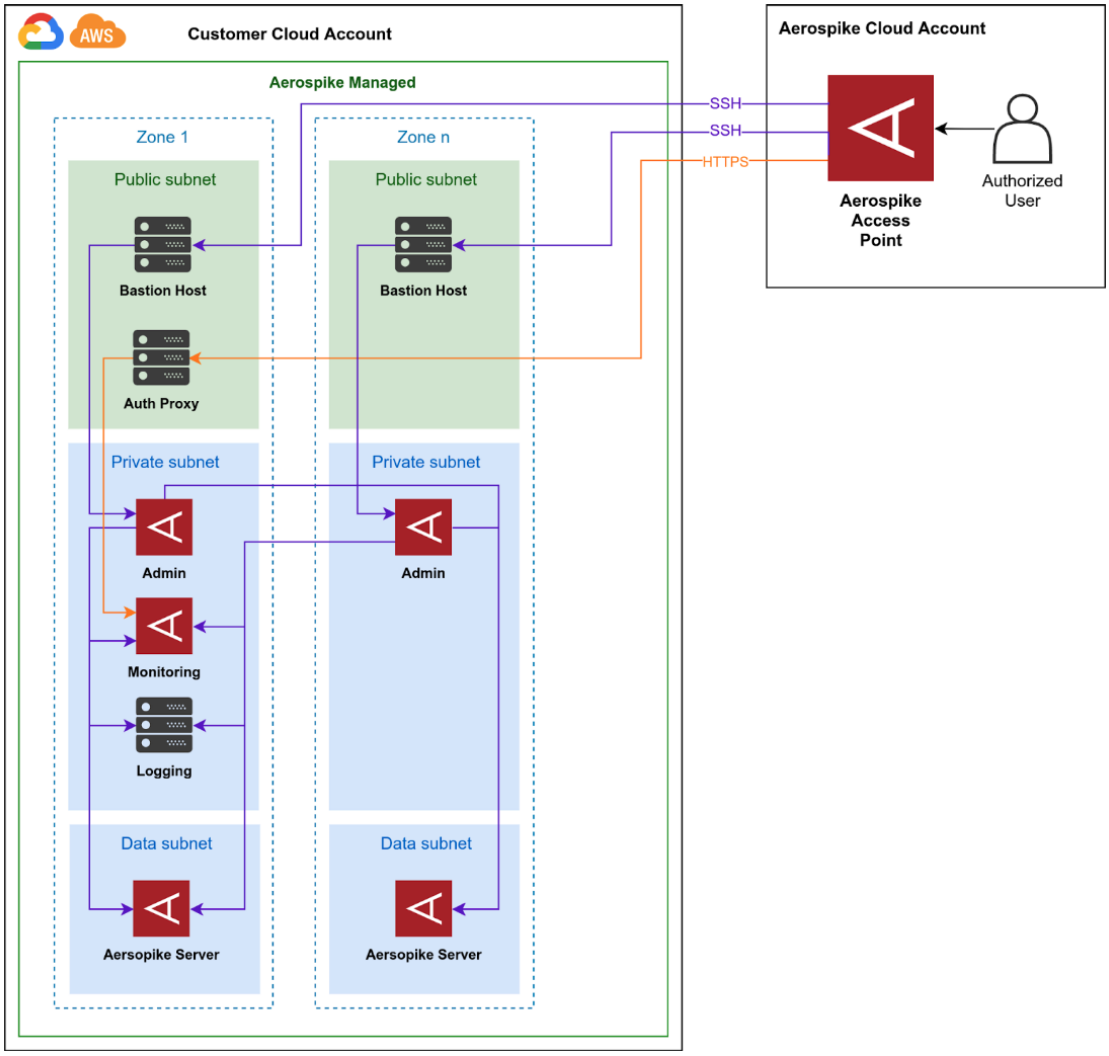

Figure 3: Inbound from Aerospike cloud

The procedure to connect into the customer environment follows a strict process. First, users must be authenticated, authorized, and connected to a remote VPN. Next, a connection is established to a bastion host or jump host in the public subnet of the environment using public key authentication. SSH connections are allowed into the admin nodes in the private subnet from the bastion host.

ACMS executes automated playbooks from the admin nodes that indirectly allow the individual to establish a connection with the other nodes through the private subnets to conduct configuration management for the cluster.

As part of the security and audit protocol, Aerospike retains audit logs of all SSH logins and the commands executed on all instances under Aerospike management for 90 days. These logs are kept in object storage within the customer cloud account and are available upon request.

Monitoring dashboard access

To monitor proper operation of the cluster, the Aerospike Monitoring Stack requires a connection from the instrumentation in the cluster to the dashboard. ACMS allows HTTPS connections over the public internet to an auth proxy in a public subnet; this connection protects the Aerospike Monitoring Stack used by the Aerospike staff operating the clusters. Only authorized Aerospike employees can access the monitoring dashboard, and access is limited to:

- TLS connections originating from the Aerospike corporate VPN
- Authentication with the Aerospike corporate directory via OpenID Connect

Cloud Identity and Access Management (IAM)

ACMS requires access to resources in the customer cloud, as it uses role-chaining to grant required access to the infrastructure contained in the customer account. As you'll see, this access is restricted to the lowest levels necessary to fulfill the requirements of each implementation phase.

Granting access to Aerospike

ACMS employs a two-phase approach to onboard and deploy customer accounts and projects.

During the onboarding phase, the customer temporarily grants ACMS access to the cloud resources to define the IAM access policies and associated resources. Once the initial setup is completed, this temporary administrative access is removed and the policies are reviewed jointly by the customer and ACMS.

After the onboarding phase, authorized ACMS operations staff retain a more restrictive form of access so they can execute runbooks to provision and modify ACMS resources. ACMS uses infrastructure-as-code (IaC) principles to reduce the risks of changing a live production database cluster. In particular, all changes undergo a peer code review process before being applied to the environments and clusters.

Auditing Aerospike activity

Cloud auditing is one of the best practices that security teams must define to monitor any cloud infrastructure's administration, access, and activity levels. ACMS recommends that customers establish mechanisms to ingest and review the Aerospike-managed environment audit logs.

Public clouds provide documentation and tools to help customers with auditing. Amazon Web Services provides AWS CloudTrail and Google Cloud Platform provides Cloud Audit Logs. We'll briefly discuss each in turn.

AWS CloudTrail enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage. CloudTrail logs, monitors, and retains account activity information across your AWS infrastructure, giving you control over storage, analysis, and remediation actions.

Cloud Audit Logs help security teams maintain audit trails in Google Cloud Platform (GCP). With this tool, enterprises can attain transparency over administrative activities and data access on the GCP.

Database authentication and user management

Authentication is required to access the Aerospike database. Upon initial provisioning of an Aerospike cluster, ACMS will securely share credentials with the user-admin privilege to allow customers to create and manage credentials for client applications and administrators. Customers are responsible for managing the lifecycle of the provided user admin and derivative credentials.

ACMS separately manages the lifecycle of a subset of users who operate the database – i.e., users employed by Aerospike for managing its cloud service. ACMS database users only have access to the configuration and metrics in the cluster. They never have access to user data; only customers have access to the data they've stored in their databases.

As noted earlier, all operations performed by Aerospike employees and system processes are logged in the Aerospike Audit Trail and retained in cloud object storage for 90 days (default).

Encryption

Data is encrypted in transit and at rest. We'll discuss each form of encryption in turn.

Encryption in transit

All ACMS database traffic in transit is encrypted with the TLS 1.2 protocol. This includes service traffic between the application and Aerospike database instances, fabric traffic of replicated data

between Aerospike database nodes, and heartbeat traffic for clustering. Aerospike manages the TLS configuration and the certificate lifecycle.

Encryption at rest

Aerospike has two options for encrypting data stored on disk (i.e., data at rest): AES-128 encryption (the default) or AES-256 encryption. Customers determine which option is to be deployed, taking performance and security requirements into consideration. Each Aerospike namespace has a randomly generated key, distinct from other namespaces.

Encryption keys

Aerospike installs the encryption keys for both TLS and encryption at rest on server instances with automated configuration management (CM). ACMS stores the secrets in a separately encrypted vault with AES-256 encryption. CM decrypts the secrets at runtime while installing them to the filesystem, which restricts access to read-only by the Linux user of the Aerospike database process.

OS hardening

ACMS systems run a hardened version of an official CentOS distribution with added security measures and controls. ACMS performs the hardening process by an automation pipeline installing and configuring software building images for specific purposes.

Customer auditable artifacts

ACMS maintains auditable logs from the managed environment and access logs to the database. Both are available to the customer on demand. Available artifacts include:

- **Access logs for database users**
  Successful and failed authentication attempts and other system admin operations against the Aerospike database captured by Aerospike Audit Trail.
- **Access logs for the ACMS employees' access to Linux systems**
  Sessions initiated by ACMS.
- **Security audit scan report for deployed images**
  Scan results from OS hardening audit.
- **Malware scan report for deployed images**
  Scan results for the version of the image(s) deployed.

Conclusion

Digital security in the cloud is a complex process that requires training, adaptability, agility, and commitment. By working with ACMS, firms can leverage Aerospike's experience acquired from deploying hundreds of clusters in different environments to satisfy the demand of real-time applications. Aerospike applies rigor and discipline to its cloud managed service, helping firms quickly and effectively deploy a real-time data platform solution to meet their needs for development, staging, testing, or production. ACMS offers options for disaster recovery, multi-region, or multi-cloud deployments.

Corporations can direct their IT staff to focus on supporting core business initiatives by delegating deployment and operation of Aerospike in the cloud to skilled, experienced Aerospike and cloud specialists capable of delivering the highest level of security for Aerospike's real-time data platform.

About Aerospike

The Aerospike Real-time Data Platform enables organizations to act instantly across billions of transactions while reducing cloud instances by up to 80 percent. The Aerospike data platform powers real-time applications with predictable sub-millisecond performance from gigabytes to petabytes of data with five-nines uptime with globally distributed, strongly consistent data. Applications built on the Aerospike Real-time Data Platform fight fraud, provide recommendations that dramatically increase shopping cart size, enable global digital payments, and deliver hyper-personalized user experiences to tens of millions of users. Customers such as Airtel, Experian, Nielsen, PayPal, Snap, Wayfair, and Yahoo rely on Aerospike as their data foundation for the future. Headquartered in Mountain View, California, the company also has offices in London, Bangalore, and Tel Aviv.

For more information, please visit https://www.aerospike.com.