Internal License and Usage Document: Elasticsearch with Azure Blob Retention & Rehydration for Jaeger in AKS

\*\*Document Owner:\*\* [Your Team/Department Name]

\*\*Document Date:\*\* [Current Date]

\*\*Application:\*\* Jaeger (Distributed Tracing)

\*\*Backend Storage:\*\* Elasticsearch (Hot) + Azure Blob Storage (Cold)

\*\*Deployment Environment:\*\* Azure Kubernetes Service (AKS)

\*\*Elasticsearch License Tiers:\*\*

- Production: Platinum Subscription

- Development: Basic (Self-Managed)

# 1. Introduction

This document defines the licensing, compliance, and architecture for deploying Jaeger with Elasticsearch in AKS, with Azure Blob Storage for long-term retention and rehydration workflows for audit and compliance.  
  
- Hot Storage: Elasticsearch keeps recent traces (7–30 days).  
- Cold Storage: Archived traces stored in Azure Blob.  
- Rehydration: On-demand restoration for audits, incident response, or compliance.  
- Audit Logging: Automated logs capture every rehydration event.

# 2. Licensing & Compliance

Production: Elastic Platinum with advanced features (security, ML, CCR, support).  
Development: Elastic Basic (free, self-managed).

# 3. Deployment Architecture & Retention Flow

- Elasticsearch (Hot): 30 days prod, 7 days dev.  
- Azure Blob (Cold): Retains up to 1 year (prod) / 30 days (dev).  
- CronJobs: Export/delete from Elasticsearch into Blob daily.  
- Rehydration Jobs: Restore archived data into temporary Elasticsearch indices.  
- Audit Logs: Captured in centralized logging (Azure Monitor, Loki, or ELK).

# 4. Technical Implementation

## 4.1 Retention Job (Elasticsearch → Blob)

Daily CronJob exports indices older than retention and archives them in Azure Blob Storage.

## 4.2 Rehydration Job (Blob → Elasticsearch)

On-demand job to pull archived traces from Blob back into Elasticsearch.  
Temporary indices are used (jaeger-restore-\*) to avoid polluting active storage.

## 4.3 Automated Audit Logging

Each rehydration job writes metadata to a dedicated audit log index in Elasticsearch or to Azure Monitor/Loki. This includes timestamp, blob file, restored index, user, and job status.

# 5. Governance & Retention

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Environment | Hot (Elasticsearch) | Cold (Blob) | Rehydration | Audit Logging |
| Prod | 30 days | 1 year (Cool→Archive) | On-demand by compliance request | Required |
| Dev | 7 days | 30 days (Cool only) | Optional | Required (internal only) |

# 6. Benefits

- Cost Optimization: Data offloaded to Blob archive tiers.  
- Regulatory Compliance: Audit-ready trace lifecycle with immutable logs.  
- Security Enforcement: Only authorized teams can run rehydration jobs.  
- Forensic Capability: Historical traces retrievable for investigations.

# 7. Conclusion

This architecture ensures:  
- Short-term performance (Elasticsearch hot storage).  
- Long-term compliance (Azure Blob).  
- Traceability & accountability (audit logging on rehydration).  
  
The result is a resilient, auditable, and cost-effective solution for Jaeger trace data in AKS.