Splunk Ingestion Optimization

Safely reduce Splunk Cloud log ingestion with a control-first, data-driven approach.

Overview

Splunk Cloud costs often grow faster than engineering teams can react. Most log ingestion is hard to manage, noisy or redundant. However, reducing it feels risky.

Splunk Ingestion Optimization is a structured, low-risk consulting engagement designed to:

- Quickly identify **high-impact savings opportunities**
- Prove value early
- Then, if desired, implement **long-term ingestion control and cost governance**

Who This Is For

- Companies using **Splunk Cloud**
- Engineering or platform teams under pressure to reduce observability costs
- Organizations that want **measurable savings without blind log deletion**
- Teams that need clarity before committing to large changes

Engagement Structure (2 Stages)

Stage 1: Rapid Ingestion Analysis & Savings Validation

Objective:
Quickly identify whether >**10% ingestion savings** are achievable with low risk.

What We Do

- Analyze Splunk ingestion to extract the **top N log patterns** by log size
- Attribute ingestion to:
    - Log patterns
    - Fields related to apps
    - Sources
    - Sourcetypes
    - Indexes
- Identify:
    - Big-size wasteful log patterns
    - Debug-level logs
    - Candidates for shortening & truncation

What You Get

- Clear visibility into *what is driving your Splunk costs*
- Estimated **realistic savings potential**
- Initial, low-risk optimization recommendations

Outcome

- A clear **go / no-go decision** for deeper optimization
- No long-term commitment required

Stage 2: Ingestion Optimization & Cost Control Enablement

Objective:
Implement sustainable, high-impact ingestion reduction with full team alignment.

Scope (If Client Proceeds)

1. Cost Visibility & Control Dashboards

- Custom dashboards showing:
    - Top N log patterns by log size
    - Trends, spikes, and budget risk for ingestion
- Enable teams to **see cost impact in near-real time**

2. High-Impact Savings Strategy

- Detailed recommendations to achieve **significant ingestion reduction**, including:
    - Log dropping process creation
    - Log format improvements
    - Log patterns converted to metrics or traces
    - Potential areas to perform log truncation, deduplication and sampling
- Focus on **preserving signal while removing/reducing noise**

3. Logging Architecture Improvement & Guardrails

- Review and improve (if applicable) ingestion pipelines with **built-in control points**
- Define:
    - What must always be logged
    - What can be reduced safely
    - Rollback and alerting mechanisms
- Limit cost regression as the system scales

4. Knowledge Sharing & Enablement

- Knowledge-sharing session with core engineers and platform owners
- Topics include:

    - How Splunk pricing really works
    - How to design cost-aware logging
    - How to maintain savings over time
- Ensure **internal ownership**, not long-term dependency

Typical Engagement

- **Step 1 Duration:** ~1 week
- **Step 2 Duration:** 2–4 weeks (depending on complexity & scope)
- **Delivery:** Remote, minimal disruption to engineering teams
- **Approach:** Data-driven, vendor-neutral, engineering-driven, risk-aware

Why StarCluster Solutions

- Deep understanding of **Splunk Cloud ingestion mechanics**
- Strong emphasis on **control, safety, and sustainability**
- Designed for teams that need results without operational risk
- Focused on **practical savings** and **client's ROI**, not theoretical optimizations

Get Started

Start with **Stage 1: Rapid Ingestion Analysis**
Validate savings potential before committing further. **Reach out** to us to **learn** more about this **service** and our **pricing**.

📩 **Contact**: starclustersolutions@outlook.com

🌐 **Website**: yaohong.kok-family.com

📰 **Article**: How to Reduce Splunk Cloud Cost Without Losing Observability