Basic Log Aggregation Strategy

Siddhartha Devkota

Purpose & Scope

When we deal with multiple systems, logs can quickly become scattered and disorganized. A log aggregation strategy can help to keep everything organized in one place, so teams can find issues faster, monitor activity more effectively, and have a clearer view of what is happening across the environment. The scope covers collecting, formatting, and storing logs from critical sources like applications, servers, databases, and security tools.

Why We Need It

When systems run separately, their logs are scattered. That makes it hard to see patterns or detect issues early. By bringing all logs together:

- We can spot problems before they grow.
- Troubleshooting is faster because we don’t jump between servers.
- Security and compliance are easier with a single source of truth.

What Logs to Collect

- **System Logs:** Operating system events like startup, shutdown, and errors.
- **Application Logs:** Messages from the apps we build or run.
- **Security Logs:** Authentication attempts, access logs, firewall alerts.
- **Database Logs:** Queries, errors, and slow performance warnings.

How to Collect

- Use lightweight agents or built-in tools to ship logs from servers.
- Standardize format (JSON or key-value pairs) so logs are easy to parse.
- Tag logs with source information (server, app, environment).

Where to Store

- A **central log server** (like ELK stack or a managed cloud logging service).
- Ensure storage is scalable (logs can grow quickly).
- Apply retention rules: keep critical logs longer, drop low-value logs sooner.

Considerations

- **Sources:** Decide which systems must always send logs (critical apps, security devices).
- **Format:** Use a consistent structure to simplify searching and dashboards.
- **Storage:** Balance cost and retention. Not all logs need to be kept forever.
- **Security:** Protect logs from tampering; sensitive data should be masked.

Next Steps

1. Pick a log aggregation tool (e.g., ELK, Loki, or a cloud-native service).
2. Deploy agents on key systems.
3. Define retention policies.
4. Set up dashboards and alerts for quick insights.

References

- NIST SP 800-92: Guide to Computer Security Log Management
- Elastic Stack Documentation: https://www.elastic.co/docs/get-started/the-stack
- Grafana Loki Documentation: https://grafana.com/oss/loki/