OpenSearch Guide

This document describes the OpenSearch index templates, ISM retention policies, and pre-built Dashboards saved objects that are automatically provisioned when the stack deploys. All objects are created by custom resources during CloudFormation stack creation and updated on stack updates.

Note: Some pattern specific dashboards, and visualizations may only display data at tier levels advanced or above.

1. Index Templates

An index template is applied to every new index matching the pattern. Templates are created per index type configured in the deployment profile (typically `app` and `audit`).

Template name: `logs-<indexType>` (e.g. `logs-app`, `logs-audit`)

Index pattern: `logs-<indexType>-*`

Field mappings:

- `@timestamp` – `date`
- `accountId` – `keyword`
- `logGroup` – `keyword`
- `logStream` – `keyword`
- `message` – `text`
- `pattern_detected` – `boolean`
- `pattern_types` – `keyword`

Settings:

- `index.number_of_shards` – configured per index type in the profile
- `index.number_of_replicas` – configured per index type in the profile
- `index.codec` – `best_compression`

Shard and replica counts vary by tier. For example, essential tier uses 2 shards / 1 replica for app, 1 shard / 1 replica for audit.

2. ISM Retention Policies

An Index State Management (ISM) policy is created per index type to automatically delete old indexes after a configurable retention period.

Policy ID: `log-retention-<indexType>` (e.g. `log-retention-app`, `log-retention-audit`)

States:

- **active** – index is in use. Transitions to *delete* when `min_index_age` exceeds the retention period.
- **delete** – index is permanently deleted.

Tier defaults (overridable via AppRetentionDays / AuditRetentionDays parameters):

- **Basic:** app = 30 days, audit = 365 days
- **Essential:** app = 30 days, audit = 365 days
- **Advanced:** app = 90 days, audit = 1095 days (3 years)
- **Enterprise:** app = 365 days, audit = 2555 days (7 years)

To override, set the `AppRetentionDays` or `AuditRetentionDays` CloudFormation parameter to a value other than `-1`. The ISM policy is updated on each stack update.

3. Index Patterns

Three index patterns are provisioned for use in Discover and visualizations:

- `logs-*` – all log indexes (app + audit + custom). Default time field: `@timestamp`
- `logs-app-*` – application log indexes only
- `logs-audit-*` – audit log indexes only

To view: **Management → Index Patterns**. To refresh field lists after new data arrives: select the pattern and click the refresh icon.

4. Saved Searches

Saved searches are pre-configured Discover queries accessible from the Discover tab or embeddable in dashboards.

- **Recent Errors** – `message: ERROR` across all indexes. Columns: @timestamp, logGroup, logStream, message.
- **By Log Group** – all events sorted by timestamp. Columns: @timestamp, logGroup, logStream, message, accountId.
- **Audit Recent Logs** – recent audit events (last 24h). Index: `logs-audit-*`.
- **App Recent Logs** – recent application events (last 24h). Index: `logs-app-*`.
- **Pattern Detections** – `pattern_detected: true`. Columns: @timestamp, logGroup, logStream, message, pattern_types.
- **SQL Injection Attempts** – `pattern_types: sql_injection`.
- **SSN Detections** – `pattern_types: ssn` OR `pattern_types: ssn_nondash`.
- **Credential Detections** – `pattern_types: aws_access_key OR pattern_types: aws_secret_key`.

5. Visualizations

Log Overview visualizations:

- **Events Over Time** – line chart of event count over time (all indexes).
- **Top Log Groups** – pie chart of top 10 log groups by event count.
- **Error Rate** – line chart of events matching `message: ERROR` over time.
- **Events by Account** – donut chart of event volume by accountId (useful for cross-account).
- **Log Volume by Group Over Time** – stacked area chart of top 8 log groups over time.

Audit visualizations:

- **Audit Events Over Time** – line chart. Index: `logs-audit-*`.
- **Audit Top Log Groups** – pie chart. Index: `logs-audit-*`.
- **Audit Error Rate** – line chart. Index: `logs-audit-*`.

App visualizations:

- **App Events Over Time** – line chart. Index: `logs-app-*`.
- **App Top Log Groups** – pie chart. Index: `logs-app-*`.
- **App Error Rate** – line chart. Index: `logs-app-*`.

Pattern Detection visualizations:

- **Pattern Detections Over Time** – line chart of events where `pattern_detected: true`.
- **Pattern Detections by Type** – pie chart of top 15 pattern types.
- **Pattern Detections by Log Group** – horizontal bar chart of top 10 log groups with detections.
- **Pattern Types Over Time** – stacked area chart of pattern types over time.
- **Pattern Detections by Hour** – hourly histogram of pattern detections.

All visualizations use bottom-positioned legends for readability.

6. Dashboards

Four dashboards are provisioned, each combining related visualizations and saved searches:

Log Processor - Log Overview

Overview of all log ingestion across indexes.

- Events Over Time (line)
- Top Log Groups (pie)
- Error Rate (line)
- Events by Account (donut)
- Log Volume by Group Over Time (stacked area)

Log Processor - Logs Audit

Audit index events with 24-hour default time range.

- Audit Events Over Time (line)
- Audit Top Log Groups (pie)
- Audit Error Rate (line)
- Audit Recent Logs (saved search table)

Log Processor - Logs App

Application index events with 24-hour default time range.

- App Events Over Time (line)
- App Top Log Groups (pie)
- App Error Rate (line)
- App Recent Logs (saved search table)

Log Processor - Pattern Detections

Pattern detection overview with 24-hour default time range.

- Pattern Detections Over Time (line)
- Pattern Detections by Type (pie)
- Pattern Detections by Log Group (horizontal bar)
- Pattern Types Over Time (stacked area)
- Pattern Detections by Hour (histogram)
- Pattern Detections (saved search table)

7. Accessing Dashboards

1. Open `https://<dashboards-domain>/_dashboards`
2. Log in with your Cognito credentials
3. Click **Dashboards** in the left navigation menu
4. Select a dashboard (Log Overview, Logs Audit, Logs App, or Pattern Detections)

To view all saved objects: **Management** → **Saved Objects**.

To create custom visualizations: **Visualize** → **Create visualization**. Select an index pattern and build your chart. Save it and add it to any dashboard.

8. Refreshing Index Patterns

After new data arrives (especially if new fields like `pattern_detected` or `pattern_types` appear for the first time), refresh the index pattern field list:

1. Go to **Management** → **Index Patterns**
2. Select the index pattern (e.g. `logs-*`)
3. Click the refresh icon (circular arrow) in the top right

This ensures all fields are available for filtering, aggregation, and visualization.

9. Notes

- All saved objects are re-imported with `overwrite=true` on every stack update, so customizations to the provisioned objects will be overwritten. Create new objects with different IDs for your own custom dashboards.
- Index templates only apply to new indexes. Existing indexes retain their original mapping. To apply new mappings to existing data, delete the old indexes and let new data recreate them.
- ISM policies are updated in place on stack updates. Changes to retention periods take effect on the next ISM policy evaluation cycle (typically within 5 minutes).
- The `pattern_detected` and `pattern_types` fields are only present on events that matched a pattern rule. Use `pattern_detected: true` as a filter in Discover or visualizations.