OpenSearch Guide

Overview
AI Monitor automatically imports a set of pre-built OpenSearch Dashboards visualizations during deployment. These dashboards provide real-time visibility into your metric data, anomaly detection results, cost trends, and cross-account health.

Dashboards are hosted on the same OpenSearch domain used by LogProcessor and are accessible via the Dashboards link on the AI Monitor landing page.

Prerequisites
- A deployed AI Monitor stack with OpenSearch connectivity
- The os_config Lambda must have successfully run (check CloudFormation events)
- Access to OpenSearch Dashboards via the LogProcessor ALB

Accessing Dashboards
Navigate to your OpenSearch Dashboards URL (shown on the AI Monitor landing page). Select the **Dashboards** icon in the left navigation, then choose from the available AI Monitor dashboards.

Included Dashboards

The following dashboards are automatically imported:

1. AI Monitor – Metrics Overview

- Metric Values Over Time – line chart of raw metric values across all subscriptions
- Datapoints by Namespace – pie chart showing data volume per AWS namespace
- Metric Activity Heatmap – horizontal bar showing which metrics are most active

2. AI Monitor – Anomaly Detection

- Anomaly Scores Over Time – line chart of anomaly scores (higher = more anomalous)
- Anomalies Detected – count of anomaly events over time
- Recent Anomalies – table of the latest anomaly records with score, value, and subscription
- Top Anomalous Metrics – bar chart of metrics with the most anomaly events

3. AI Monitor – Anomaly Overview

- Anomalies by Hour – bar chart showing which hours of day have the most anomalies
- Anomaly Severity Distribution – breakdown by score ranges (low/medium/high)
- Anomaly Count Over Time – time series of anomaly volume
- Anomalies per Account – bar chart for cross-account anomaly distribution

4. AI Monitor – Cross-Account Health

- Datapoints per Account – volume of metric data flowing from each account
- Account Health Summary – overview of active accounts and their anomaly counts
- Metrics by Account – which metrics are being collected per account

5. AI Monitor – Cost Trends

- Daily Spend Over Time – line chart of daily AWS costs
- Spend by Service – pie/bar chart showing cost breakdown by AWS service

6. AI Monitor – Namespace Summary

- Datapoints by Namespace Over Time – stacked area chart of data volume per namespace
- Total Datapoints per Namespace – summary bar chart

7. AI Monitor – Metric Explorer

- Metric Explorer – Time Series – interactive time series for ad-hoc metric investigation
- Metric Explorer – Anomaly Markers – overlay showing detected anomalies on the time series

Index Pattern

All dashboards use the **metrics-*** index pattern with **@timestamp** as the time field. This pattern matches the daily indices created by the metric collector (e.g. metrics-2026-06-15).

Data Fields

Key fields available in the metrics index:

- @timestamp – when the metric was recorded
- namespace – AWS CloudWatch namespace (e.g. AWS/Lambda)
- metric_name – the CloudWatch metric name
- value – the metric value
- dimensions.* – dimension key-value pairs (e.g. dimensions.FunctionName)
- account_id – the AWS account the metric originated from
- region – the AWS region
- is_anomaly – true if this record is an anomaly event
- anomaly_score – the z-score (0–10) for anomaly records
- subscription_id – which subscription detected the anomaly
- hour_of_day – hour (0–23) for time-of-day analysis
- day_of_week – weekday (0=Mon, 6=Sun) for day-of-week patterns

Customizing Dashboards

You can customize the imported dashboards directly in OpenSearch Dashboards. However, note that customizations will be overwritten on the next deployment. To preserve custom dashboards:

- Clone the dashboard (Dashboards > select > Clone)
- Give the clone a different name (do not use the "AI Monitor" prefix)
- Custom dashboards with non-matching names are not affected by re-imports

Troubleshooting

No data in dashboards

- Verify the metric collector is running (check Lambda invocations)
- Ensure the metrics-* index pattern exists (Management > Index Patterns)
- Check that the time range picker is set correctly (default: last 15 minutes may be too narrow)

Dashboards not appearing

- Check the CloudWatch dashboard

Dimension fields show as "keyword" errors

- Dimension fields require the .keyword suffix for Terms aggregations
- This is already handled in the bundled visualizations
- If creating custom visualizations, use dimensions.ServiceName.keyword (not dimensions.ServiceName)

Create a support bundle using the *support-bundle* script included in the scripts.zip download and send to support.