GETTING STARTED WITH SPLUNK FOR MONITORING AND DIAGNOSTICS AND IIoT

A guide to gaining real-time insights into industrial operations

Introduction

Managing industrial processes and systems means you're likely working with industrial control systems (ICS) like SCADA, process historians, and alarm and event sensors. These diverse operational technologies (OT) make it challenging to gain a unified view into the availability and performance of your industrial environment.

By collecting, analyzing and visualizing time-series sensor data, alarms and events, and other machine data generated by your OT and IT systems, you can gain this unified view—and a competitive edge. This guide outlines how you can use this data and Splunk software to better monitor your industrial assets, applications and infrastructure, and quickly diagnose issues in your industrial operations and processes.

Benefits of Better Monitoring and Diagnostics

Gaining a real-time and unified view into the health, availability and performance of highly distributed industrial assets and complex control systems is an uphill battle. These systems often use proprietary protocols that frequently operate in silos in your environment.

Unifying and analyzing the machine data generated in industrial environments can help you to:

- Monitor multiple disparate systems from a single tool
- Ensure equipment is operating as intended
- Monitor, track and avoid unplanned asset downtime
- Rapidly perform root-cause analysis and pinpoint costly operational issues
- Understand the cause of failures and improve efficiency and availability

Getting Started

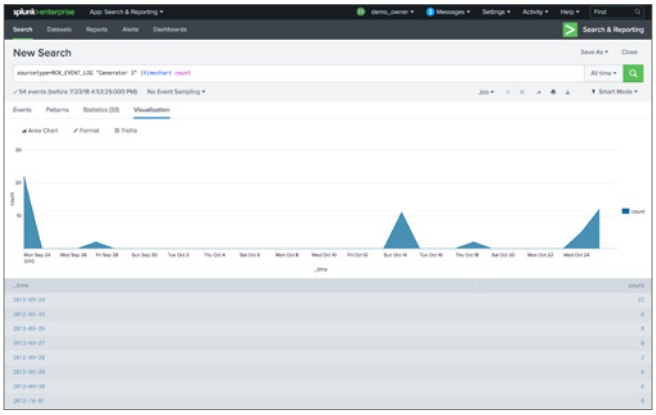
Many organizations already use Splunk software to gain a consolidated view across their IT systems to improve performance and availability. You can use the same platform to gain a unified view into OT systems as well. Additionally, Splunk software is already integrated with leading IoT platforms—including OPC, OSISoft PI, and Kepware—that enable fast time-to-value for developers and end users.

Data Sources Table

Data Type	Where to Find It	What It Can Tell You
Sensor data and other metrics	Historian databases, OPC, Kepware Industrial Data Forwarder for Splunk, HTTP event collector, MQTT, AMQP, COAP, JMS	Asset performance, anomaly detection, predictive maintenance, set point monitoring
Alarms and events	OPC, alarm and event servers, databases, log files	Root-cause analysis, failure forensics, nuisance alarm reduction, capacity planning
Application logs	SCADA application logs, device poller logs, internal application logs, scripted output	Operator activity, application performance, system state, communication information, errors and problems
Infrastructure data	Switches, routers, servers, desktops, HMIs	Networking and communications troubleshooting, cybersecurity

Using Splunk for Monitoring and Diagnostics

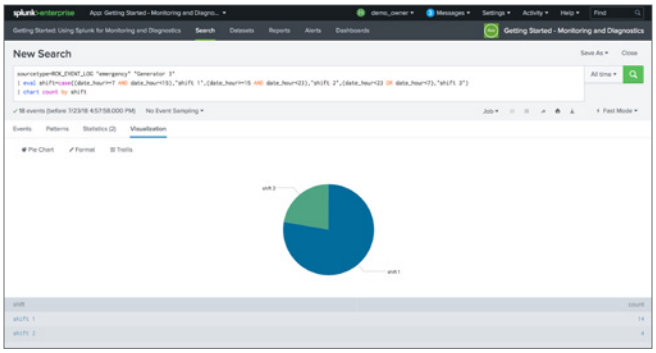
1) Get Baselines of Asset Performance



- **What to look for:** Equipment listed in SCADA system logs as well as alarm and event data.
- **Why?** You can perform real-time analysis that provides immediate insight into where your issues are occurring. Additionally, correlating this information with sensor data can provide insight into abnormal operating conditions and determine why issues are occurring.
- **Example search:** ... "Generator 3"|timechart count

---

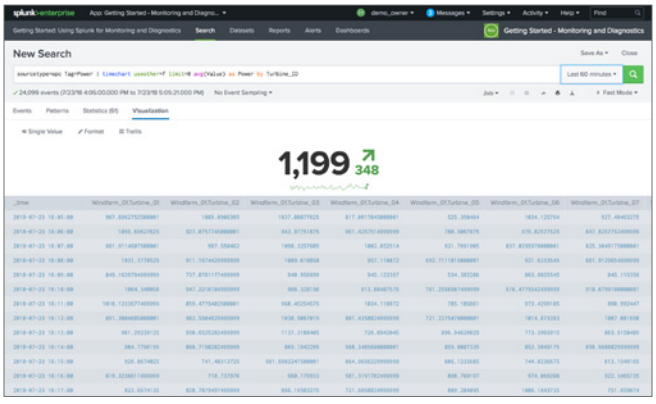
2) Find Seasonality in Operations



- **What to look for:** Trends in issues by date, time or shift.
- **Why?** Seasonality can help you pinpoint subtle operational issues that can be resolved with operator training or improved procedures, pinpoint problems that may be happening with equipment, and can help monitor after-hours activity by vendors and support staff.
- **Example search:** ... eval shift=case((date_hour>=7 AND date_hour<15),1,(date_hour>=15 AND date_hour<23),2,(date_hour>=23 OR date_hour<7),3) | stats count by shift

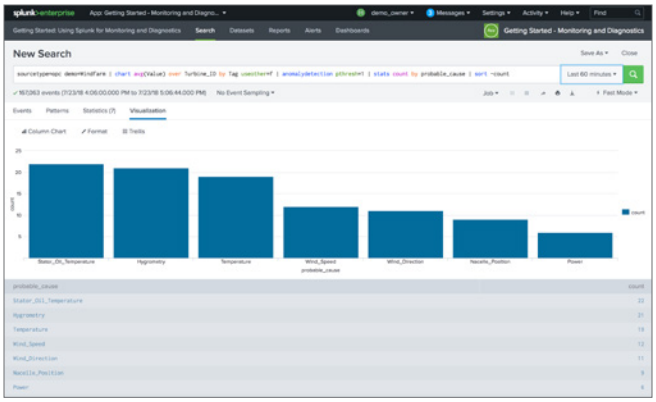
---

3) Monitor Trends in Sensor Data



- **What to look for:** Trends in metrics collected from your assets and industrial control systems.
- **Why?** Using granular or aggregated time series analytics can give you a real-time view into the performance of your assets and processes. Aggregate data on-the-fly into KPIs and easily drill down into the root cause of spikes or drops.
- **Example search:** ... Tag=Power | timechart partial=false avg(Value) as Power

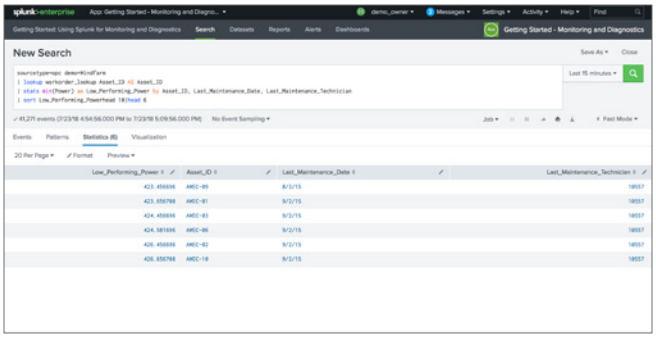
4) Identify Anomalies in Sensor Data



- **What to look for:** Anomalies in individual sensor readings or anomalies against a body of historical data from a group of assets.
- **Why?** Using advanced analytics such as anomaly detection or machine learning can quickly identify outliers and patterns.
- **Example search:** ... sourcetype=opc demo=Windfarm | chart avg(Value) over Turbine_ID by Tag useother=f | anomalydetection pthresh=1 | stats count by probable_cause

---

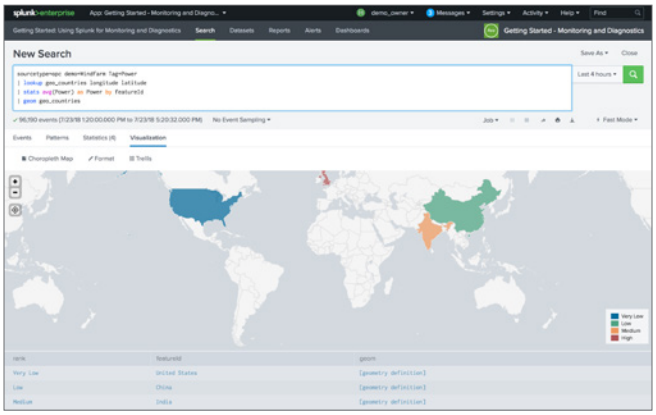
5) Enrich Operational Data With Data From Work Order, Asset and Other External Systems



- **What to look for:** Patterns in metrics related to activities not stored with your sensor data.
- **Why?** Activities affecting your sensor data might not be stored in your tag historian or operational database. Find subtle root causes of operational problems by mashing up data from all of your operational data sources.
- **Example search:** ... | lookup workorder_lookup Asset_ID AS Asset_ID OUTPUTNEW Last_Maintenance_Date AS Last_Maintenance_Date | stats min(Power) by Last_Maintenance_Technician, Last_Maintenance_Date, Asset_ID | sort min(Power) | head 5

---

6) Enrich Operational Data With Geolocation Data to Gain a Global View of Operations



- **What to look for:** Patterns in data related to geographic or other location-based groupings.
- **Why?** The physical nature of industrial environments means that cause and effect may be related to proximity. Automatically group data on-the-fly using any location-based borders—as big as a country or as small as a production line—to monitor metrics and KPIs.
- **Example search:** ... demo=windfarm Tag="Power"| lookup geo_countries longitude latitude | stats avg(Value) as Power by featureId | geom geo_countries

Connecting Splunk to Industrial Data and the IoT

Kepware Industrial Data Forwarder for Splunk
Get real-time data collection from over 150 open and proprietary industrial data protocols common in energy, manufacturing, and oil and gas environments.

Modular Inputs
There are many free apps and add-ons that simplify the connection and collection of data from industrial systems. Use MQTT, COAP, AMQP, JMS and other modular inputs for Splunk to quickly and easily configure connectivity to these message brokers and protocols. For a complete list, go to our website.

HTTP Event Collector
Use a standard API and token-based authentication to enable applications and devices to send millions of events per second directly to Splunk Enterprise or Splunk Cloud for analysis.

Summary

Managing complex industrial operations isn't easy, but getting full visibility of your operations can help. With this guide and data sources you may already be analyzing, you can move from being reactive to proactive, while maximizing your operations performance, security and availability.

Try Splunk Cloud or Splunk Enterprise for free or learn more about IoT and industrial data.
Already have Splunk? Download Splunk Apps on Splunkbase.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

GSG-Splunk-Monitoring-and-Diagnostics-IIoT-104