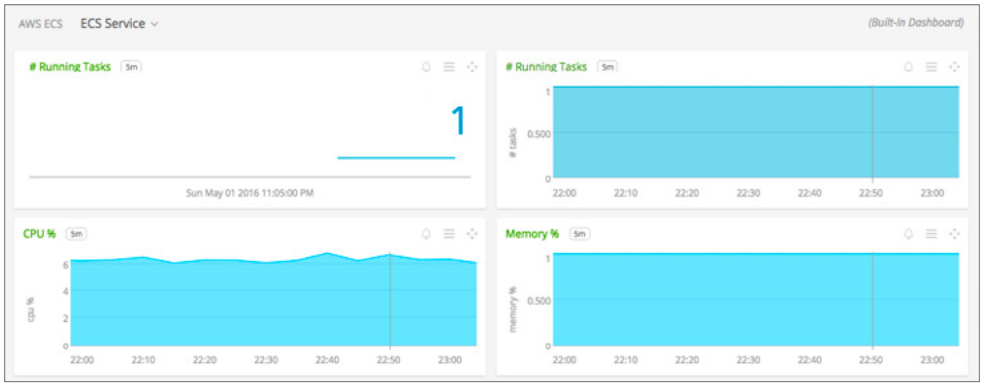
Monitoring AWS Container Services With Splunk Observability

Monitoring and observability are key considerations when choosing any AWS container service. The highly dynamic and ephemeral nature of containerized environments makes them difficult to monitor using traditional infrastructure monitoring or APM solutions. With hundreds — if not thousands — of components being spun up and down every day or even hour, batch-based monitoring solutions cannot keep up with the churn. In many cases, they cannot even see the new components, let alone enable multi-dimensional real-time analysis.

The Splunk streaming analytics engine — SignalFlow — is the only monitoring solution that can keep up with the dynamic nature of containerized environments without compromising performance and being overwhelmed by alert storms. Some of our customers are running the most demanding container-based production environments in the industry, with millions of components being churned on a daily basis.

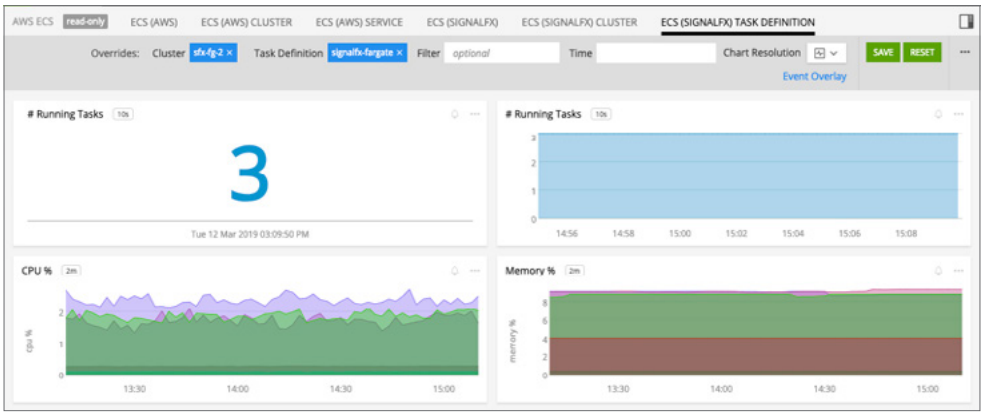


Metrics monitoring: Focus on single ECS Service using CloudWatch.

Create your monitoring plan geared for your specific container environment

Besides the container considerations listed earlier, we recommend you create a monitoring plan that addresses the specifics related to your container environments such as:

- Monitoring goals
- List of resource types and services that need to be monitored
- Monitoring frequency
- Tools and integration requirements
- Monitoring roles and responsibilities
- Process to notify and handle alerts and level of automation



Metrics monitoring: Focus on single ECS task definition using Smart Agent.

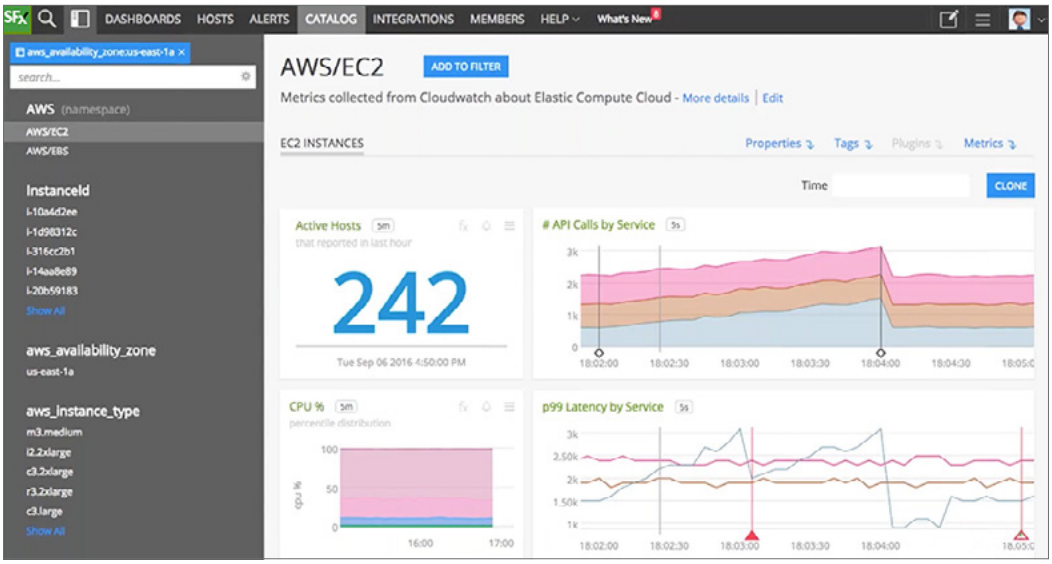
Splunk helps you closely monitor AWS container services and resources in real time. Use Splunk to monitor Amazon ECS via our out-of-the-box integration with AWS. For greater insight into your ECS environment, Splunk's Smart Agent can autodiscover services and provide more in-depth metrics about your containers that are running in ECS.

Splunk can help you better monitor and manage your container environments. It bridges the gap between your monitoring requirements and what CloudWatch offers. Also, it provides a simpler way to visualize your monitored data as opposed to the programming interface of CloudWatch. When Amazon ECS collects metrics, it collects multiple data points every minute. It then aggregates them to one data point before sending the data to CloudWatch. So with CloudWatch, one sample count is actually the aggregate of multiple data points during one minute. Splunk allows you to monitor your container metrics at a finer grained frequency of one second. AWS allows you to access historical metrics and logs for a period of two weeks. This data can be used for baselining and identifying patterns for troubleshooting.

With Splunk, you can have more rich, fine-grained metrics roll ups, resolution and data retention of up to a year based on your subscription plan. Splunk AWS Optimizer gives you actionable insight into cost-saving opportunities and underutilized EC2 investments. You can see usage patterns and cost attribution by InstanceType, AWS Region, AWS Availability Zone, as well as categories specific to your setup, such as Service, Team, or any other dimensions that are sourced from EC2 instance tags.

Splunk provides a robust integration with CloudWatch, has a CloudWatch-powered mode for the Infrastructure Navigator, and includes many built-in dashboards to help you get started monitoring Amazon Web Services. You can also monitor Amazon Web Services instances and the services running on them by using the Splunk Smart Agent. The Splunk Smart Agent offers a much higher degree of customization than is possible with AWS CloudWatch, and may be preferable for instances where you want to see metrics at a finer resolution, or where detailed control over the metrics sent matters.

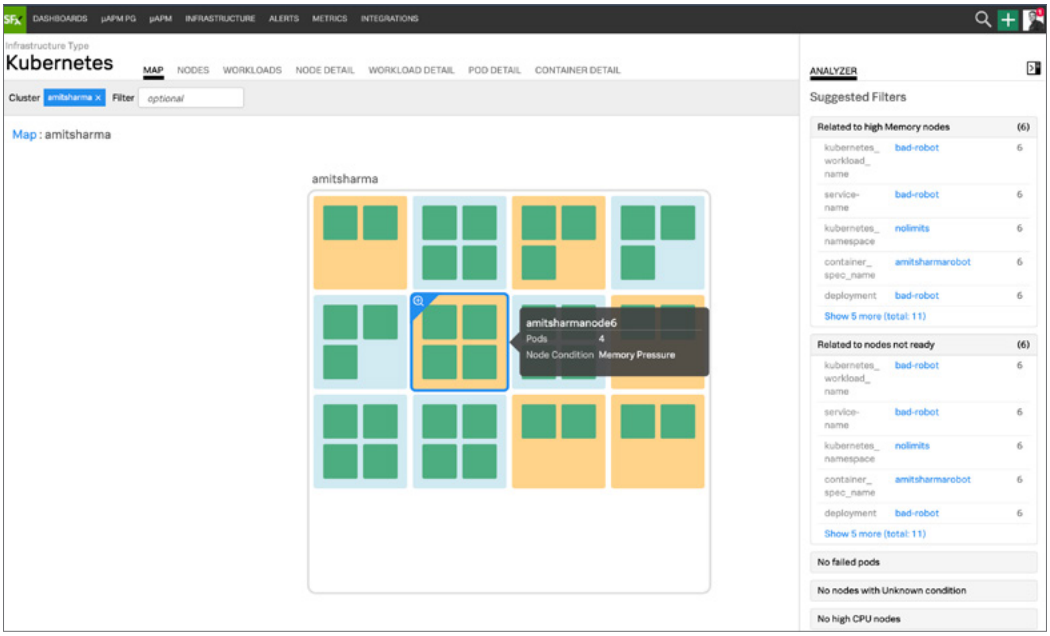
If you wish to know how to deploy the Smart Agent in ECS, see the Smart Agent ECS Deployment Guide for instructions. Also, Smart Agent can be deployed in ECS task to monitor AWS Fargate containers. See the Smart Agent Fargate Deployment Guide for more detailed deployment instructions.



Splunk AWS EC2 monitoring dashboard

Kubernetes Navigator

Included with Splunk Infrastructure Monitoring, Kubernetes Navigator is an enterprise-grade and turn-key Kubernetes monitoring solution that provides an easy and intuitive way to understand and manage the performance of EKS environments. Working alongside hundreds of customers, we designed a solution that works for every team — irrespective of their maturity and experience with Kubernetes. Kubernetes Navigator brings immediate value to teams that are starting on their cloud-native journey while also addressing monitoring challenges for the world's most complex Kubernetes deployments at scale.



With Kubernetes Navigator, your teams can detect, triage and resolve performance issues faster than ever before. DevOps and SRE teams can successfully navigate the complexity associated with operating Kubernetes at scale by taking advantage of these features:

- **Dynamic cluster map:** An intuitive way to instantly understand the health of Kubernetes clusters
- **Drill downs:** Faster and effective troubleshooting with quick drill downs
- **Logs in context:** Deep linking to contextual logs to gain granular insights, eliminate context switching and accelerate root cause analysis
- **Kubernetes analyzer:** AI-driven analytics to expedite troubleshooting

Dynamic Cluster Map

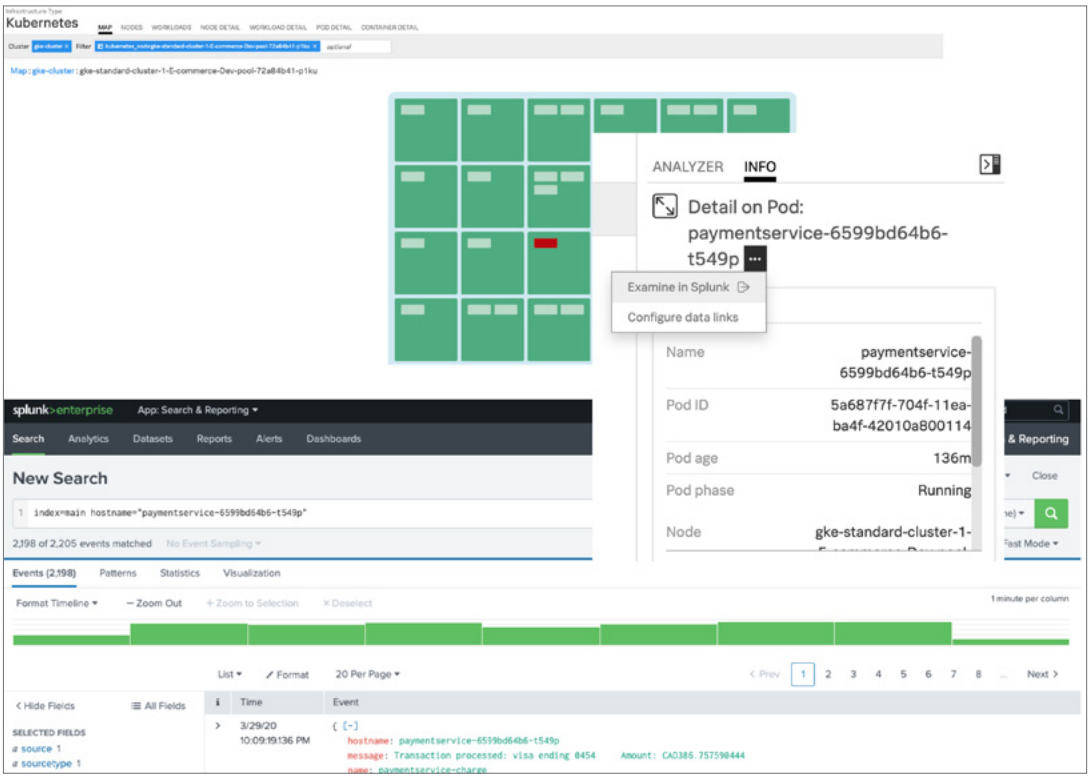
Starting with the bird's eye view, Kubernetes Navigator enables teams to quickly understand the performance of the entire Kubernetes environment with intuitive and hierarchical navigation. Select, filter, or search for any Kubernetes entity, e.g., node, pod and container level within seconds. Splunk automatically discovers Kubernetes components and containerized services to instantly monitor your entire stack. Understand relationships between dynamic Kubernetes components and quickly fix interdependent performance issues.

Drill downs

A global, at-a-glance view into the entire Kubernetes environment helps teams understand how the overall system is performing. It is equally important to have a granular, detailed view into individual components as teams narrow down to the source of the problem — drilling down from nodes to pods to containers to workloads. Our streaming architecture enables in-depth analysis with search and filters within seconds at a massive scale.

Logs in context

Seamlessly pivot to logs and get granular visibility into application, Kubernetes and container logs to correlate performance across the entire stack without any context switching. Visibility into lifecycle events of Kubernetes and API Server Audit logs help you understand and maintain your security and compliance postures.



Kubernetes Analyzer

To understand the "why" behind performance anomalies, Kubernetes Navigator uses AI-driven analytics, which automatically surface insights and recommendations to precisely answer, in real time, what is causing anomalies across the entire Kubernetes cluster — nodes, pods, containers and workloads. In the example below, Kubernetes Analyzer automatically detects a pattern causing memory pressure on some of the Kubernetes nodes. In this case, a container with an unlimited memory limit ends up consuming all the available memory on these nodes, draining other pods scheduled by Kubernetes. This scenario is commonly known as a noisy neighbor issue. Following suggested filters, SRE teams can narrow down to the underlying issue within minutes. Sophisticated algorithms (e.g., Historical Performance Baselines and Sudden Change) detect system-level issues within seconds. This includes a sudden increase in Goroutines, container restarts or alerts.

Summary

While new cloud-native technologies like containers support faster innovation with more nimble and resilient application development, these new technologies also increase the level of complexity for monitoring and troubleshooting use cases. It's critical to implement the correct monitoring, troubleshooting and overall observability strategy as you adopt containers. By supporting AWS container infrastructure and services integration, Splunk helps companies easily manage their application performance in K8s environments and maximize the benefits of adopting containers at scale.

Customers are increasingly adopting containers, orchestration and microservices architecture-based applications to deliver innovation faster and to make applications more resilient. AWS container services and Splunk platform complement the efforts of Site Reliability Engineers and operations teams with streaming intelligence to assist with problem detection and troubleshooting in container environments. Together, AWS and Splunk can also accelerate code deployment and allow for automated performance data capture for applications. Splunk Infrastructure Monitoring offers pre-built dashboards featuring performance metrics and other visualizations to customers with system-wide monitoring, observability and directed troubleshooting — all critical requirements for confidently adopting containers at scale in production environments.

Future-proof your observability investment with a proven solution trusted by enterprises for most advanced use cases at a massive scale. Sign up for a free trial of Splunk Infrastructure Monitoring today.

To learn more about Splunk Infrastructure Monitoring and Splunk APM, go to https://www.splunk.com/en_us/devops.html or contact sales for more information.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

22-25586-Splunk-MonitoringAWSContainerServicesWithSplunkObservability-SG-102