AWS Elastic Compute Cloud (EC2) monitoring using Splunk Infrastructure Monitoring

You’ve got your AWS Cloud data into Splunk Observability Cloud, and now you’re looking to answer some questions about EC2 instances hosting critical workloads. Using Splunk Infrastructure Monitoring, you might want to identify EC2 instances that:

- Have consistently low CPU utilization (over-provisioned) that might be contributing to excessive or wasted cloud spend
- Appear to be overutilized (under-provisioned) and might be impacting the performance of the workloads being hosted
- Have CPU utilization running high to determine if that is normal behavior based upon historical performance
- Experience disk read or write operations that are not normal for the host, or in other words, that deviate from the historical baseline average

Data required

AWS EC2 data

How to use Splunk software for this use case

CPU utilization running low (over-provisioned)

The CPU utilization % metric is the total number of CPU units used, expressed as a percentage of the total available. EC2 instances with consistently low CPU utilization may indicate over-provisioning, and may contribute to excessive or wasted cloud spend.

You can customize dashboards to identify these instances so they can be addressed. The example below shows a list chart which can be incorporated into a dashboard that lists the EC2 instances running low CPU utilization %.
You can also add dashboard filters to narrow the list to focus on. The example below shows filtering to a specific AWS region and a specific AWS EC2 instance type which may represent high dollar price points.

**CPU utilization running high**

In some instances, it can be challenging to create good alerts in high CPU utilization situations - for example, when an EC2 instance is designed to run at high CPU utilization. In an example like this, an EC2 instance used for batch processing workloads between 1-3AM daily results in the workloads maxing out the CPUs. Classic static alerting thresholds fall short in this scenario, resulting in low alert quality and too much "alert noise".

You can start to create more useful alerts, using data analytics to determine what is historically normal or not normal, by using Detectors in Splunk Infrastructure Monitoring.

**EC2 disk read/write operations**

There are two different disk operations scenarios you might encounter while your EC2 instances are performing read/write operations on connected storage:

- DiskReadOps. The total completed read operations by the EC2 instance in a given period of time. When this metric deviates from the historical baseline average, it could signify that something is wrong with the application running inside the instance.
• DiskWriteOps. The total completed write operations by the EC2 instance in a given period of time. Like spikes in DiskReadOps, DiskWriteOps data that deviates from the norm could signal an application problem.

Creating a detector in Splunk Infrastructure Monitoring to address disk operations scenarios

Best practices for creating and managing detectors

• Before developing detectors, spend some time writing down your requirements and expected outcomes.
• Apply good naming conventions to detector names. Configure detectors and alert messages in a standard way. Establish operational practices, policies, and governance around standards.
• Make sure each detector alert has a clear SOP (Standard Operating Procedures) documented. This drives operational excellence.
• Use critical severity sparingly and only under special conditions requiring the highest level of intervention. Consistent standards are also important so that severity levels are interpreted in a consistent way by all consumers.
• Detectors require validation and ongoing tuning to remain relevant. Establish best practices around managing the lifecycle of a detector, from initial creation and onboarding to archiving or decommissioning.

Next steps

Still having trouble? Splunk has many resources available to help get you back on track:

• Splunk OnDemand Services: Credit-based services that allow direct access to Splunk technical consultants for a variety of technical services from a pre-defined catalog. Many Splunk customers already have OnDemand credits included as part of their software license. To request OnDemand Services, file a ticket through the Support Portal.
• Splunk Answers: Ask your question to the Splunk Community, which has provided over 50,000 user solutions to date.
• Splunk Customer Support: Contact Splunk to discuss your environment and receive customer support.

To fully unlock the power of Splunk, we strongly recommend our comprehensive Splunk training. If you haven't already, we recommend you explore the Splunk Observability Training Courses.

You can get even more value through implementing use cases or finding out how to get data in from additional data sources.

You might also want to look at similar searches in our article Managing an Amazon Web Services environment.