Discipline

Machine Monitoring

CS5002

Activity-11

Sheikh Muhammed Tadeeb (AU19B1014)

❖ Problem Statement:

1. Show different aspect of Machine and make inference.

2. Which parameter we need to custom design for Ec2.

❖ Solution1)

Monitoring is an important part of maintaining the reliability, availability, and performance of your Amazon Elastic Compute Cloud (Amazon EC2) instances and your AWS solutions. You should collect monitoring data from all of the parts in your AWS solutions so that you can more easily debug a multi-point failure if one occurs.

The AWS/EC2 namespace includes the following instance metrics.

1. **CPU-Utilization:** The percentage of allocated EC2 compute units that are currently in use on the instance. This metric identifies the processing power required to run an application on a selected instance.

    Depending on the instance type, tools in our operating system can show a lower percentage than CloudWatch when the instance is not allocated a full processor core.
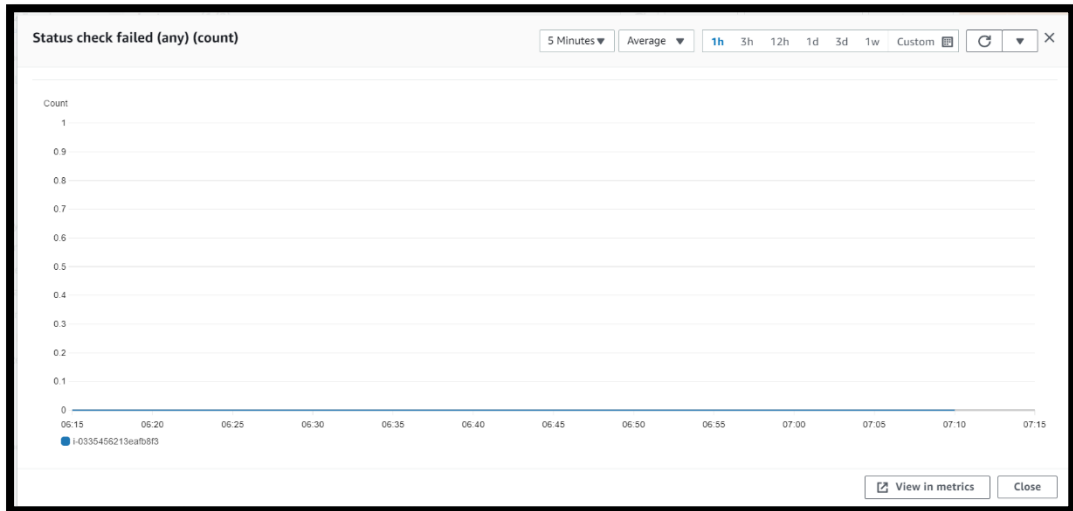
    Units: Percent
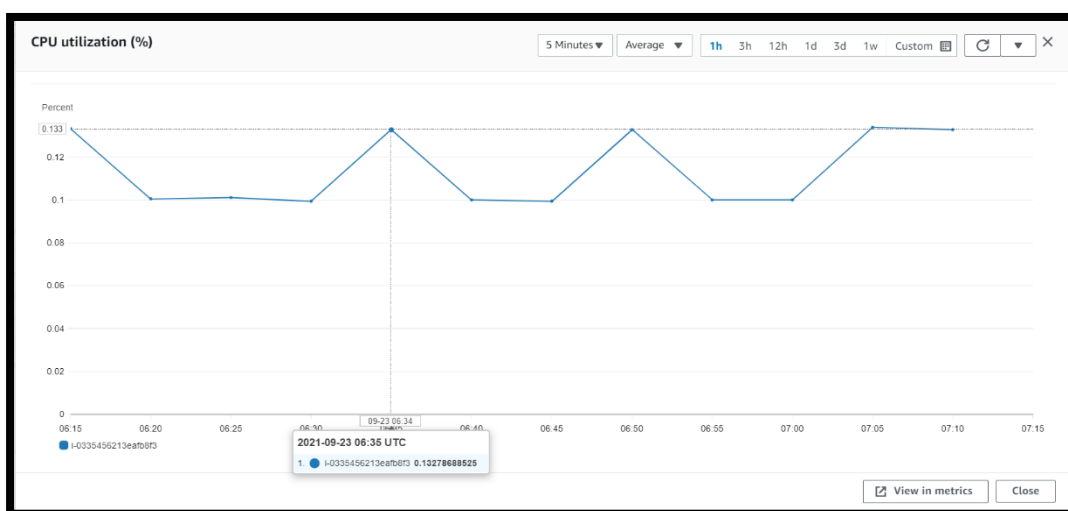
2. **Status Check Failed (any) (count):** Reports whether the instance has passed both the instance status check and the system status check in the last minute.

This metric can be either 0 (passed) or 1 (failed).

By default, this metric is available at a 1-minute frequency at no charge.
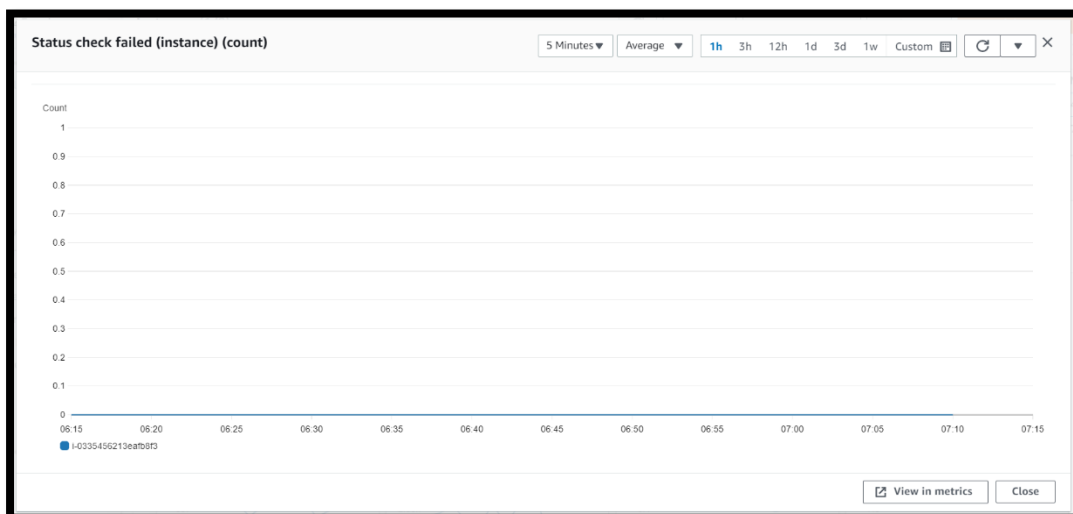
Units: Count

3. **Status Check Failed (instance) (count):** Reports whether the instance has passed the instance status check in the last minute.

This metric can be either 0 (passed) or 1 (failed).

By default, this metric is available at a 1-minute frequency at no charge.
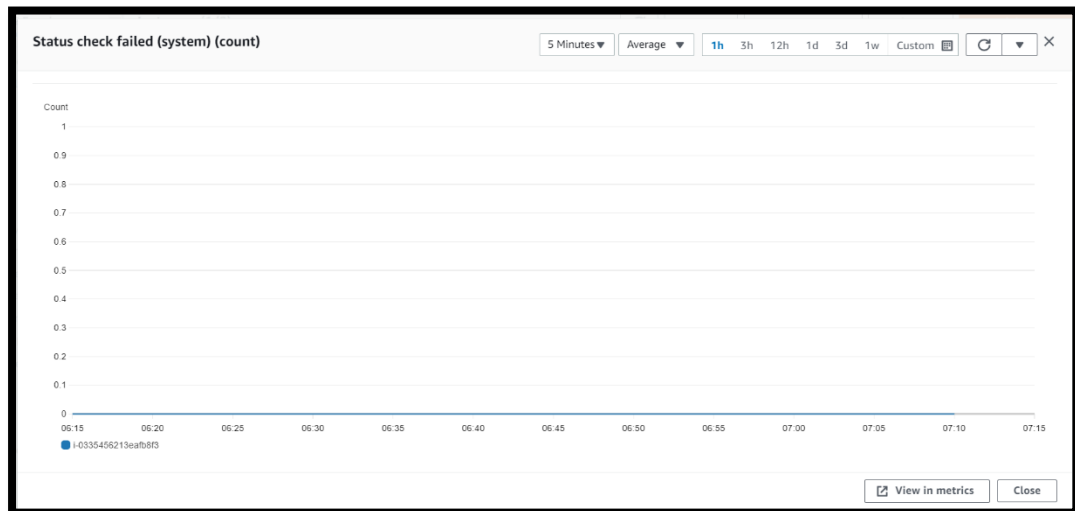
Units: Count

4. **Status Check Failed (system) (count):** Reports whether the instance has passed the system status check in the last minute.

This metric can be either 0 (passed) or 1 (failed).

By default, this metric is available at a 1-minute frequency at no charge.
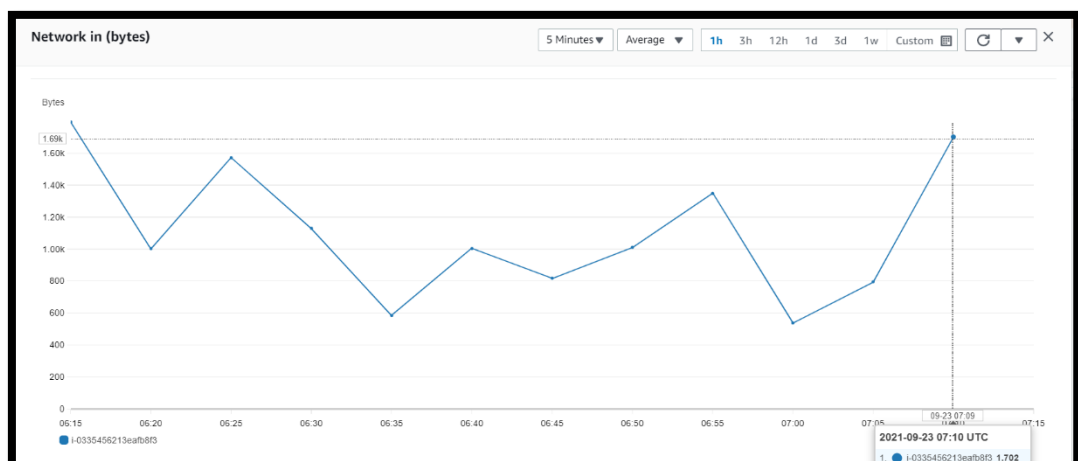
Units: Count

5. **Network in (bytes):** The number of bytes received by the instance on all network interfaces. This metric identifies the volume of incoming network traffic to a single instance.

The number reported is the number of bytes received during the period. If you are using basic (5-minute) monitoring and the statistic is Sum, you can divide this number by 300 to find Bytes/second. If you have detailed (1-minute) monitoring and the statistic is Sum, divide it by 60.
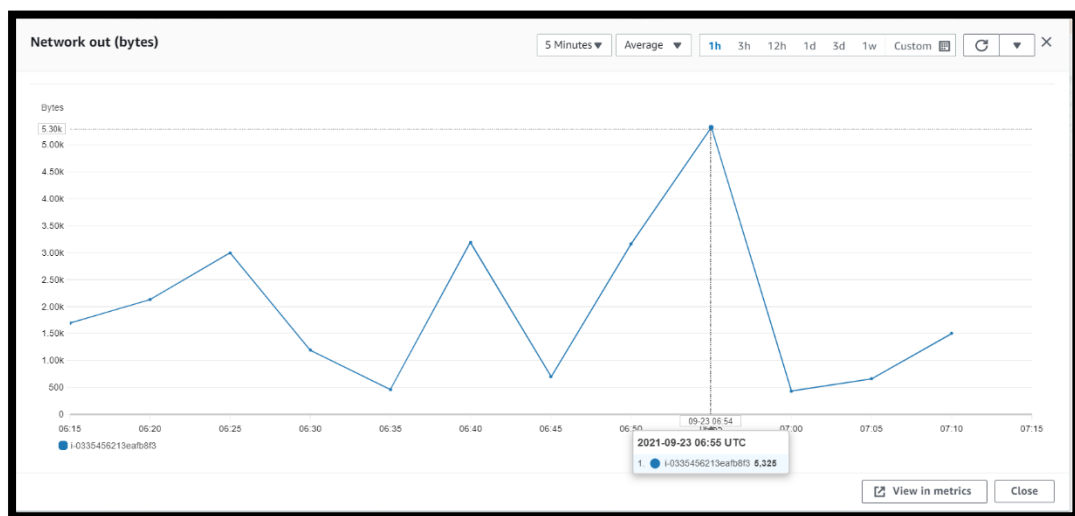
Units: Bytes

6. **Network out (bytes):** The number of bytes sent out by the instance on all network interfaces. This metric identifies the volume of outgoing network traffic from a single instance.

   The number reported is the number of bytes sent during the period. If you are using basic (5-minute) monitoring and the statistic is Sum, you can divide this number by 300 to find Bytes/second. If you have detailed (1-minute) monitoring and the statistic is Sum, divide it by 60.
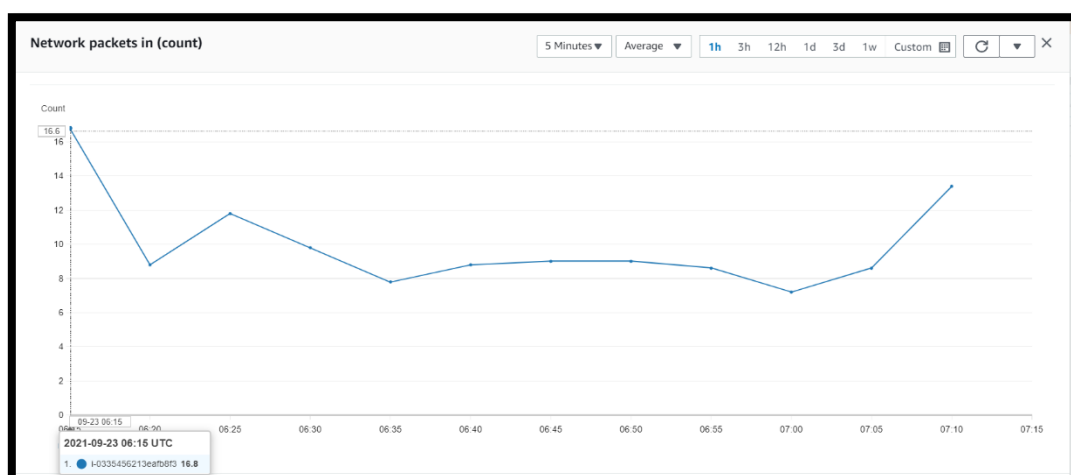
   Units: Bytes

7. **Network Packet in (count):** The number of packets received by the instance on all network interfaces. This metric identifies the volume of incoming traffic in terms of the number of packets on a single instance.

   This metric is available for basic monitoring only (5-minute periods). To calculate the number of packets per second (PPS) your instance received for the 5 minutes, divide the Sum statistic value by 300.

   Units: Count

8. **Network Packet Out (count):** The number of packets sent out by the instance on all network interfaces. This metric identifies the volume of outgoing traffic in terms of the number of packets on a single instance.

   This metric is available for basic monitoring only (5-minute periods). To calculate the number of packets per second (PPS) your instance received for the 5 minutes, divide the Sum statistic value by 300.
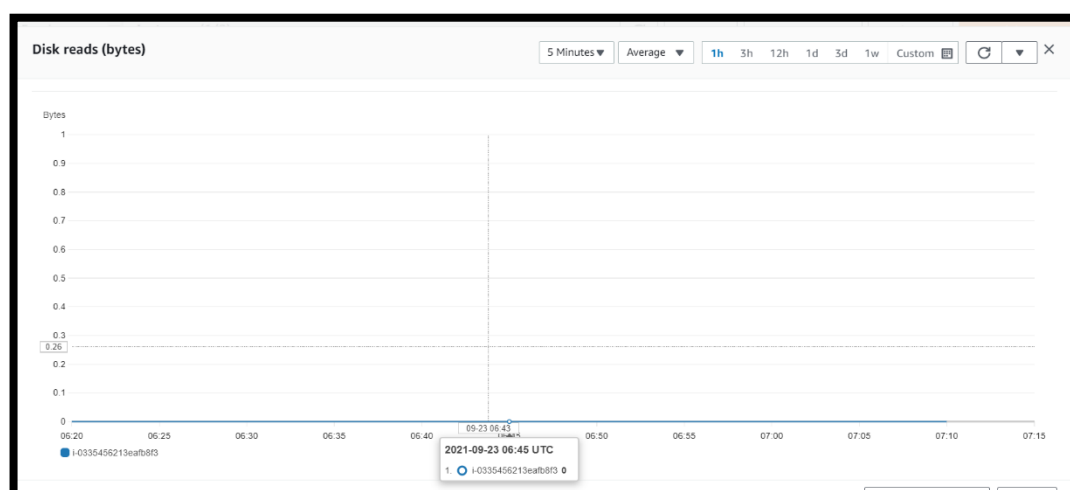
   Units: Count
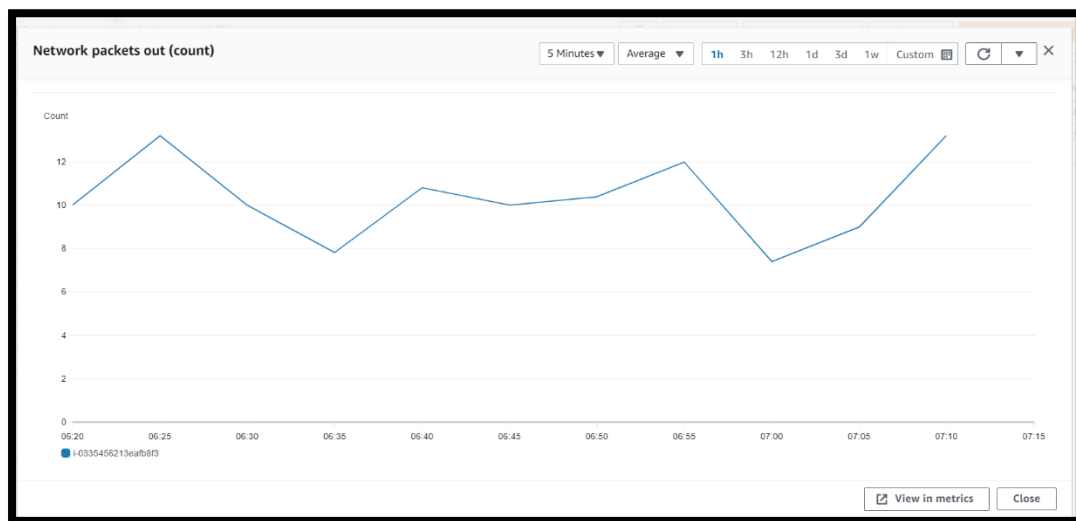
9. **Disk Read (bytes):** Bytes read from all instance store volumes available to the instance.

   This metric is used to determine the volume of the data the application reads from the hard disk of the instance. This can be used to determine the speed of the application.

   The number reported is the number of bytes received during the period. If you are using basic (5-minute) monitoring, you can divide this number by 300 to find Bytes/second. If you have detailed (1-minute) monitoring, divide it by 60. If there are no instance store volumes, either the value is 0 or the metric is not reported. Units: Bytes

10. **Disk Read Ops:** Completed read operations from all instance store volumes available to the instance in a specified period of time.

To calculate the average, I/O operations per second (IOPS) for the period, divide the total operations in the period by the number of seconds in that period.
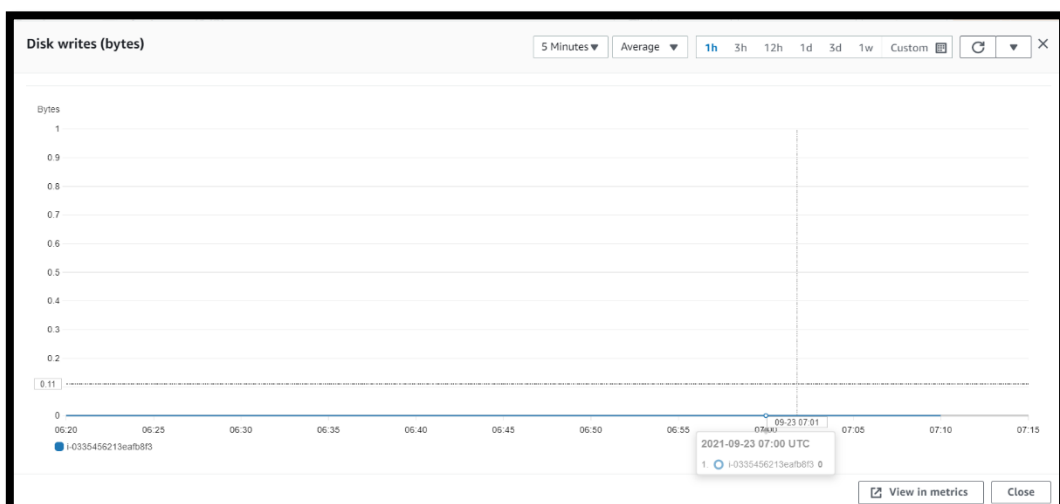
If there are no instance store volumes, either the value is 0 or the metric is not reported.

Units: Count
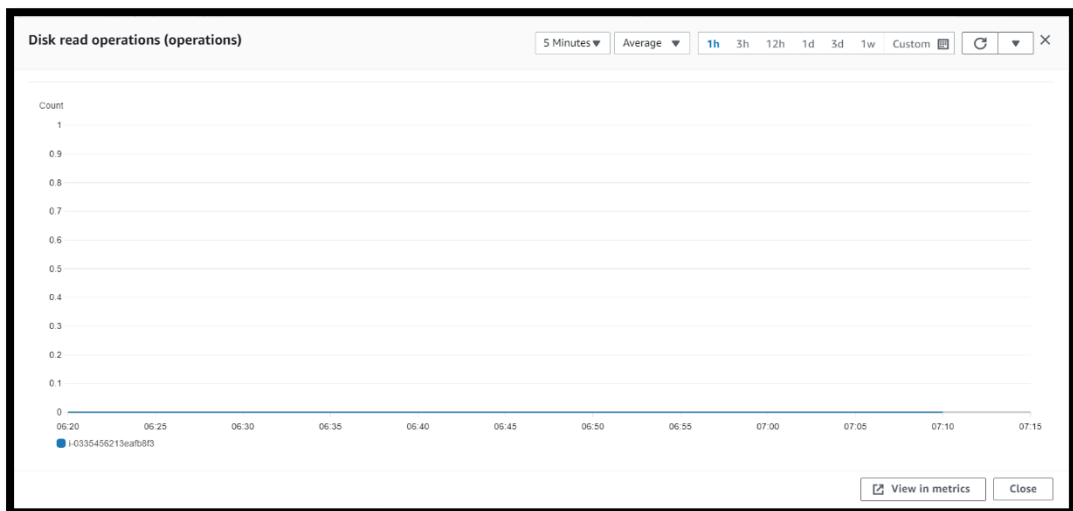
11. **Disk Write (bytes):** Bytes written to all instance store volumes available to the instance.

This metric is used to determine the volume of the data the application writes onto the hard disk of the instance. This can be used to determine the speed of the application. The number reported is the number of bytes received during the period. If you are using basic (5-minute) monitoring, you can divide this number by 300 to find Bytes/second. If you have detailed (1-minute) monitoring, divide it by 60. If there are no instance store volumes, either the value is 0 or the metric is not reported. Units: Bytes.

12. **Disk Write Ops (operations):** Completed write operations to all instance store volumes available to the instance in a specified period of time.

To calculate the average, I/O operations per second (IOPS) for the period, divide the total operations in the period by the number of seconds in that period.

If there are no instance store volumes, either the value is 0 or the metric is not reported.

Units: Count
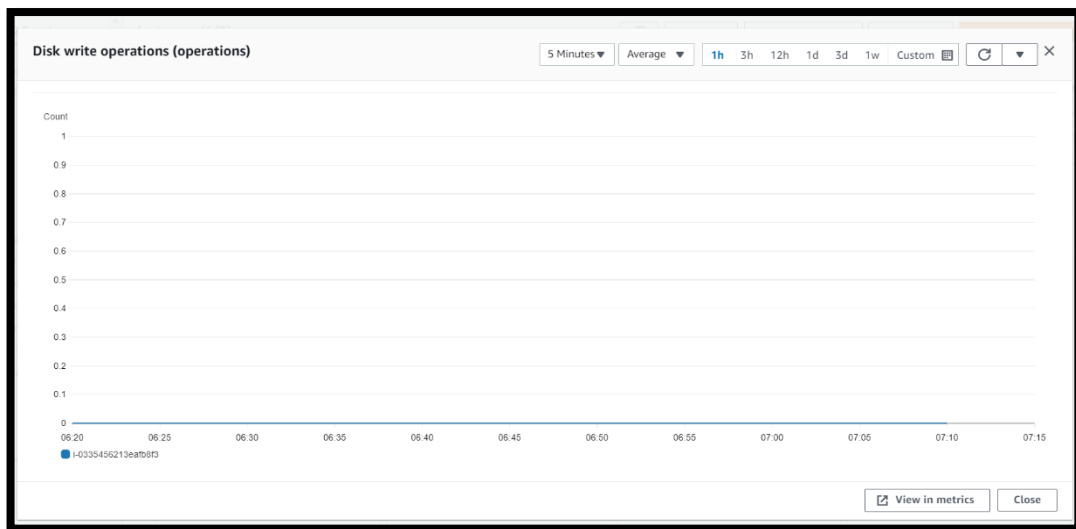
13. **CPU Credit Usage:** The number of CPU credits spent by the instance for CPU utilization. One CPU credit equals one vCPU running at 100% utilization for one minute or an equivalent combination of vCPUs, utilization, and time (for example, one vCPU running at 50% utilization for two minutes or two vCPUs running at 25% utilization for two minutes).

CPU credit metrics are available at a 5-minute frequency only. If you specify a period greater than five minutes, use the Sum statistic instead of the Average statistic.

Units: Credits (vCPU-minutes)
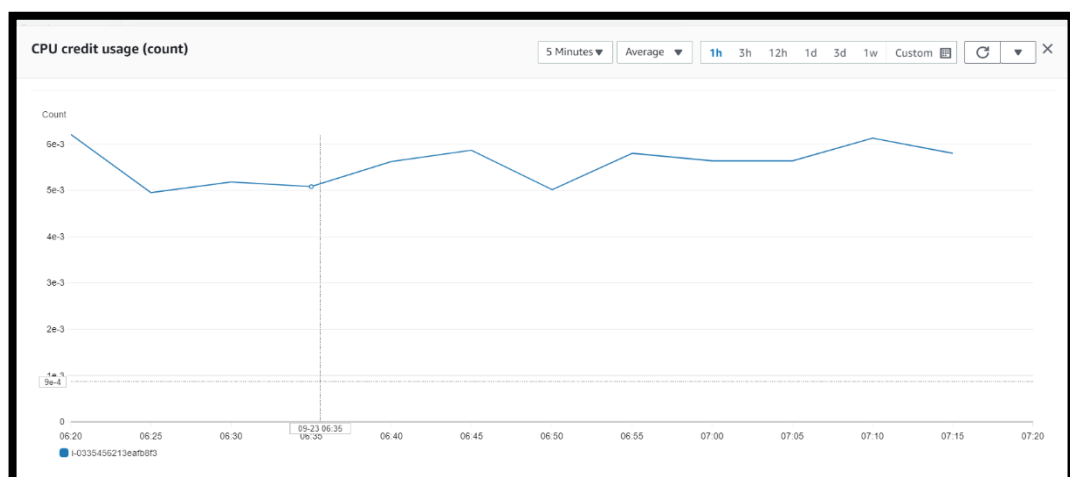
14. **CPU Credit Balance:** The number of earned CPU credits that an instance has accrued since it was launched or started. For T2 Standard, the CPUCreditBalance also includes the number of launch credits that have been accrued.

Credits are accrued in the credit balance after they are earned, and removed from the credit balance when they are spent. The credit balance has a maximum limit, determined by the instance size. After the limit is reached, any new credits that are earned are discarded. For T2 Standard, launch credits do not count towards the limit.

The credits in the CPUCreditBalance are available for the instance to spend to burst beyond its baseline CPU utilization.

When an instance is running, credits in the CPUCreditBalance do not expire. When a T3 or T3a instance stops, the CPUCreditBalance value persists for seven days. Thereafter, all accrued credits are lost. When a T2 instance stops, the CPUCreditBalance value does not persist, and all accrued credits are lost.

CPU credit metrics are available at a 5-minute frequency only.

Units: Credits (vCPU-minutes)
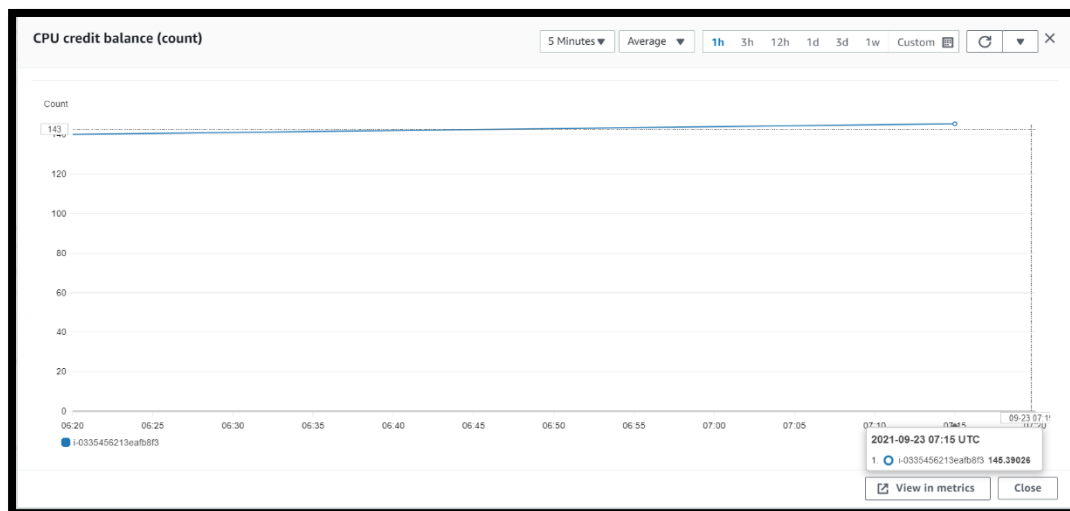
❖ Solution2)

Another important part of monitoring Amazon EC2 involves manually monitoring those items that the monitoring scripts, status checks, and CloudWatch alarms don't cover. The

Amazon EC2 and CloudWatch console dashboards provide an at-a-glance view of the state of your Amazon EC2 environment.

- Amazon EC2 Dashboard shows:

    o Service Health and Scheduled Events by Region
    o Instance state
    o Status checks
    o Alarm status
    o Instance metric details (In the navigation pane choose Instances, select an instance, and choose the Monitoring tab)
    o Volume metric details (In the navigation pane choose Volumes, select a volume, and choose the Monitoring tab)

- Amazon CloudWatch Dashboard shows:

    o Current alarms and status
    o Graphs of alarms and resources
    o Service health status

In addition, we can use CloudWatch to do the following:

    o Graph Amazon EC2 monitoring data to troubleshoot issues and discover trends
    o Search and browse all your AWS resource metrics
    o Create and edit alarms to be notified of problems
    o See at-a-glance overviews of your alarms and AWS resources