



# HI-TECH INSTITUTION

CORPORATE CAREER ENHANCEMENT TRAININGS

OUR ROOT LEVEL  
TRAINING WILL  
GIVE YOU BETTER  
GROWTH





## ABOUT US

### Our Vision:

To provide better training by full filling the requirements of our trainee.

### Our Mission:

We always ensure to give practical based training. And we make the candidates to get good hands-on experience on any platform.

### Philosophy:

Our Root Level Training Will give you Better Growth.

We successfully survived around 5 years in the IT field. Started this is as small Training room. But now we are having 5 branches across India.

Certified Trainers taking the session on various domain with any level of doubts clarification.

For More Details: [www.hitechins.in](http://www.hitechins.in)

Write feedback to [operations@hitechins.in](mailto:operations@hitechins.in)

## Cloud Watch

Amazon Cloud Watch provides a reliable, scalable, and flexible monitoring solution that you can start using within minutes. You no longer need to set up, manage, and scale your own monitoring systems and infrastructure.

- Use Cloud Watch to monitor your AWS resources and the applications you run on AWS in real time.
- Use Cloud Watch Events to send system events from AWS resources to AWS Lambda functions, Amazon SNS topics, streams in Amazon Kinesis, and other target types.
- Use Cloud Watch Logs to monitor, store, and access your log files from Amazon EC2 instances, AWS Cloud Trail, or other sources.

### Features & Benefits

#### Monitor Amazon EC2

View metrics for CPU utilization, data transfer, and disk usage activity from Amazon EC2 instances (Basic Monitoring) for no additional charge. For an additional charge, Cloud Watch provides Detailed Monitoring for EC2 instances with higher resolution and metric aggregation. No additional software needs to be installed.



#### Monitor Other AWS Resources

Monitor metrics on Amazon DynamoDB tables, Amazon EBS volumes, Amazon RDS DB instances, Amazon Elastic MapReduce job flows, Elastic Load Balancers, Amazon SQS queues, Amazon SNS topics, and more for no additional charge. No additional software needs to be installed.



## Monitor Custom Metrics

Submit Custom Metrics generated by your own applications via a simple API request and have them monitored by Amazon Cloud Watch. You can send and store metrics that are important to your application's operational performance to help you troubleshoot and spot trends.



## Monitor and Store Logs

You can use Cloud Watch Logs to monitor and troubleshoot your systems and applications using your existing system, application, and custom log files. You can send your existing system, application, and custom log files to Cloud Watch Logs and monitor these logs in near real-time. This can help you better understand and operate your systems and applications, and you can store your logs using highly durable, low-cost storage for later access.

## Set Alarms

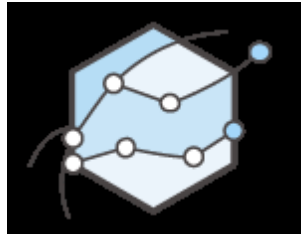
Set alarms on any of your metrics to send you notifications or take other automated actions. For example, when a specific Amazon EC2 metric crosses your alarm threshold, you can use Auto Scaling to dynamically add or remove EC2 instances or send you a notification.



## View Graphs and Statistics

Amazon Cloud watch Dashboards enable you to create re-usable graphs of AWS resources and custom metrics so you can quickly monitor operational status and identify issues at a glance. Metric data is kept for a period of fifteen months enabling you to view up to the minute data and also

historical data. Amazon Cloud Watch can load all the metrics in your account for search and graphing with the AWS Management Console. This includes logs, AWS resource metrics, and application metrics that you provide.

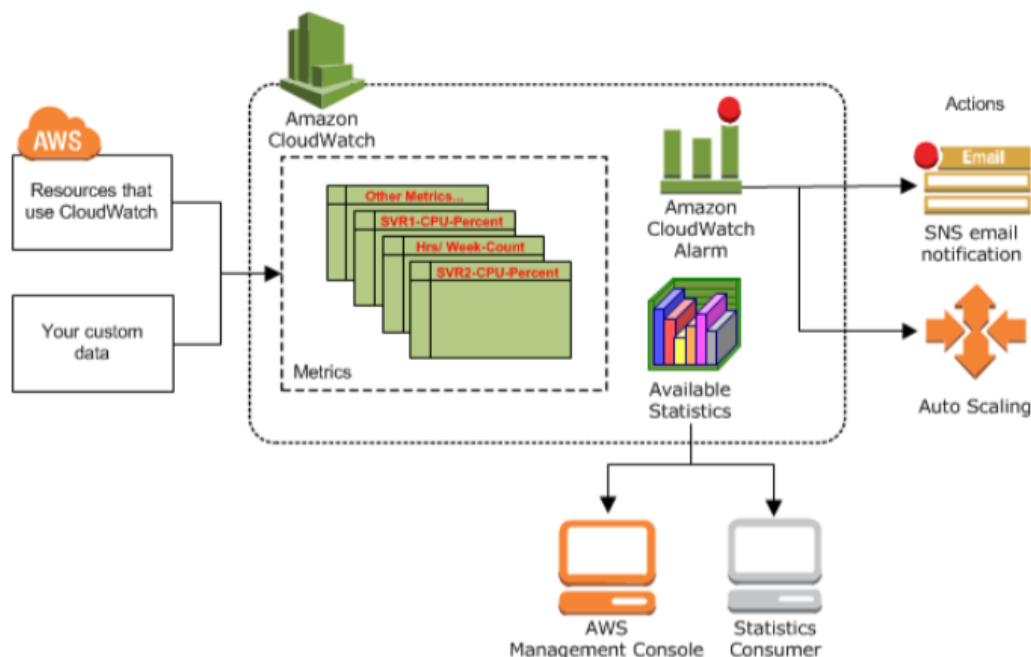


### Monitor and React to Resource Changes

Cloud Watch Events provides a stream of events describing changes to your AWS resources. You can easily build workflows that automatically take actions you define, such as invoking an AWS Lambda function, when an event of interest occurs.



### How Amazon Cloud Watch Works:





## Add or Remove a Graph from a Cloud Watch Dashboard

### To add a graph to a dashboard

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. In the navigation pane, choose **Dashboards** and select a dashboard.
3. Choose **Add widget**.
4. Choose either **Line** or **Stacked area**, and then choose **Configure**.
5. In the **All metrics** tab, select the metrics to graph.
6. (Optional) As you choose metrics to graph, you can change their color on the graph. To do so, choose **Graphed metrics** and select the color square next to the metric to display a color picker box. Choose another color square in the color picker, and then click outside the color picker to see your new color on the graph. Alternatively, in the color picker, you can type the six-digit standard HTML hex color code for the color you want and press ENTER.
7. Horizontal annotations can help dashboard users quickly see when a metric has spiked to a certain level, or whether the metric is within a predefined range. To add a horizontal annotation, choose **Graph options, Add horizontal annotation**:
  - a. For **Label**, type a label for the annotation.
  - b. For **Value**, type the metric value where the horizontal annotation appears.
  - c. For **Fill**, specify whether to use fill shading with this annotation. For example, choose **Above** or **Below** for the corresponding area to be filled. If you specify **Between**, another **Value** field appears, and the area of the graph between the two values is filled.
  - d. For **Axis**, specify whether the numbers in **Value** refer to the metric associated with the left Y-axis or the right Y-axis, if the graph includes multiple metrics.

You can change the fill color of an annotation by choosing the color square in the left column of the annotation.

Repeat these steps to add multiple horizontal annotations to the same graph.

To hide an annotation, clear the checkbox in the left column for that annotation.

To delete an annotation, choose **x** in the **Actions** column.

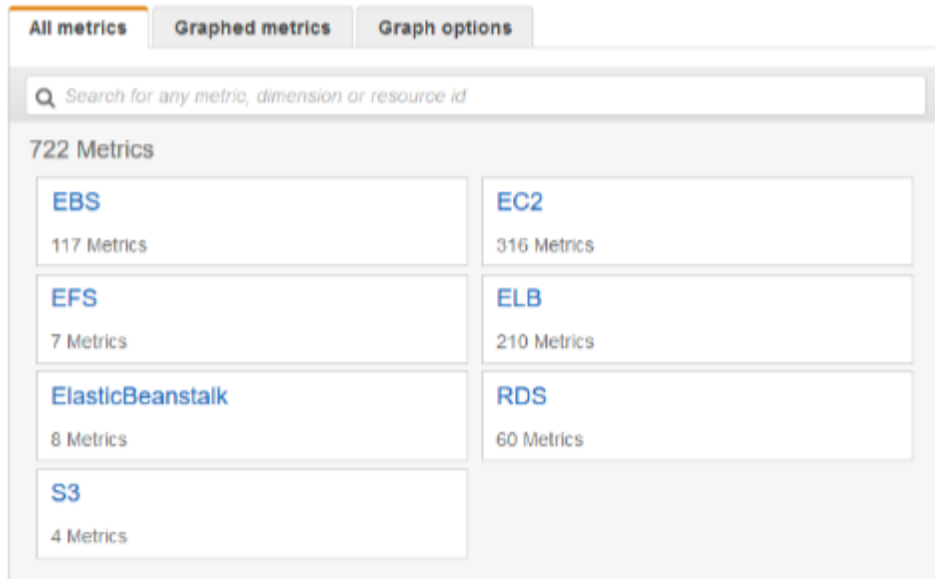
8. (Optional) To view more information about the metric being graphed, hover over the legend.
9. (Optional) To change the widget type, hover over the title area of the graph and choose **Widget actions, Widget type**.
10. Choose **Create widget**.
11. Choose **Save dashboard**.

### To remove a graph from a dashboard

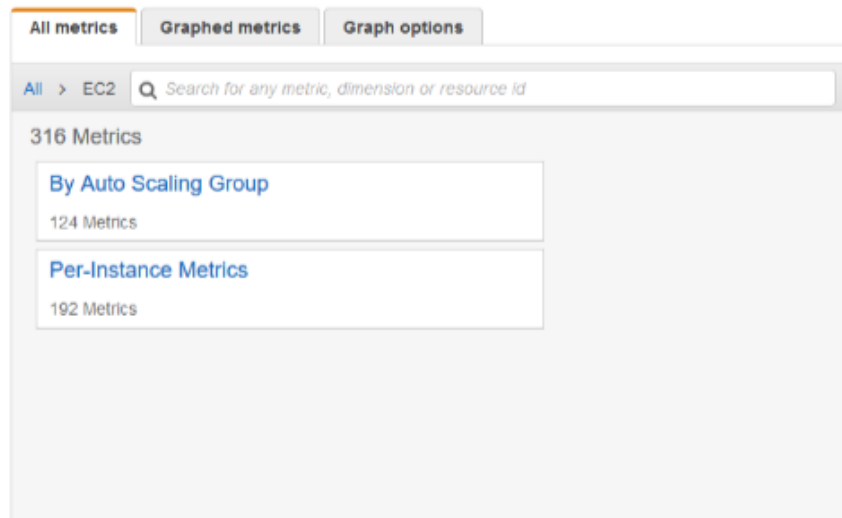
1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. In the navigation pane, choose **Dashboards** and select a dashboard.
3. Hover over the title of the graph and choose **Widget actions, Delete**.
4. Choose **Save dashboard**. If you attempt to navigate away from the dashboard before you save your changes, you are prompted to either save or discard your changes.

## To view available metrics by namespace and dimension using the console

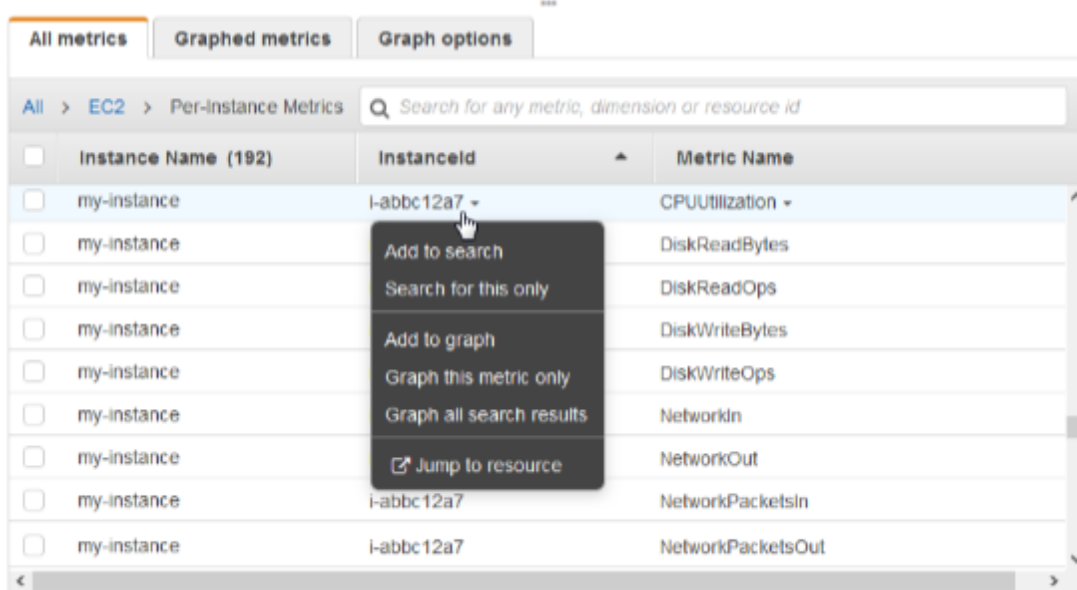
1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. In the navigation pane, choose **Metrics**.
3. Select a metric namespace (for example, EC2).



4. Select a metric dimension (for example, Per-Instance Metrics).

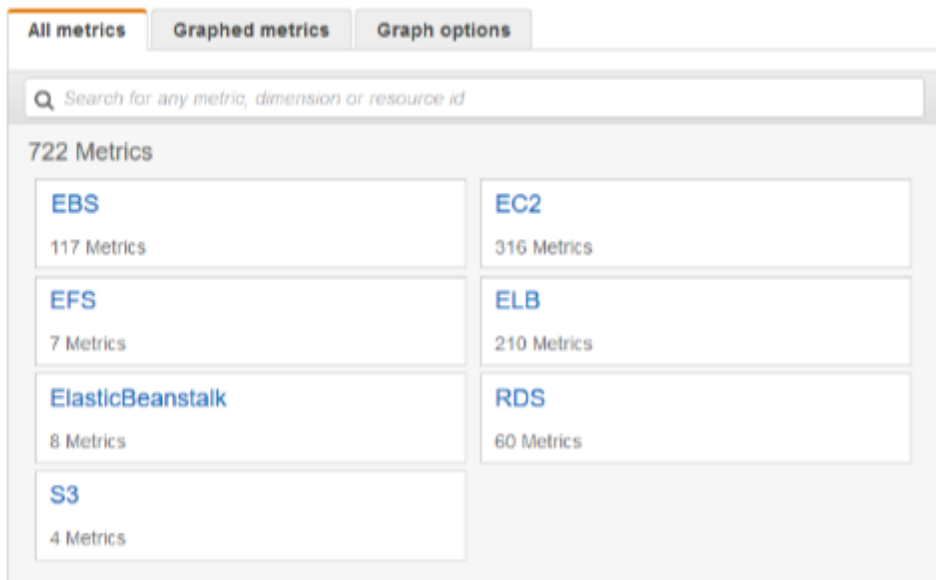


5. The **All metrics** tab displays all metrics for that dimension in the namespace. You can do the following:
  - a. To sort the table, use the column heading.
  - b. To graph a metric, select the check box next to the metric. To select all metrics, select the check box in the heading row of the table.
  - c. To filter by resource, choose the resource ID and then choose **Add to search**.
  - d. To filter by metric, choose the metric name and then choose **Add to search**.



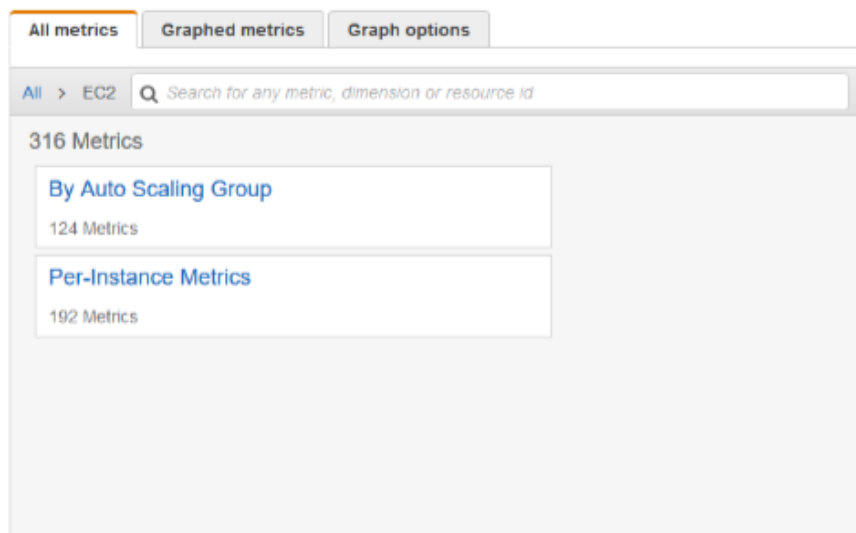
To display the average CPU utilization for a specific instance using the console

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. In the navigation pane, choose **Metrics**.
3. Select the EC2 metric namespace.

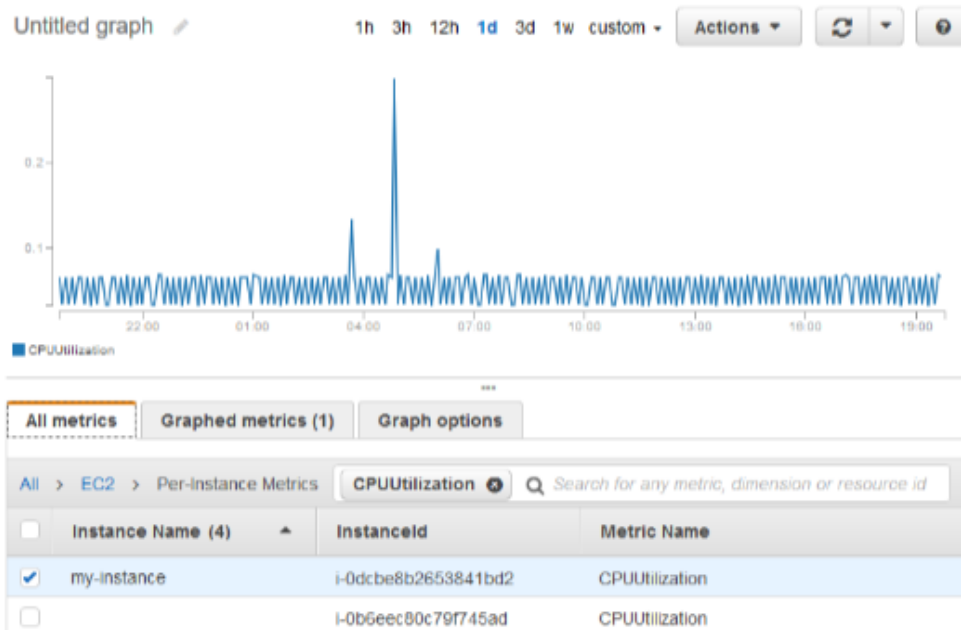


4. Select the Per-Instance Metrics dimension.

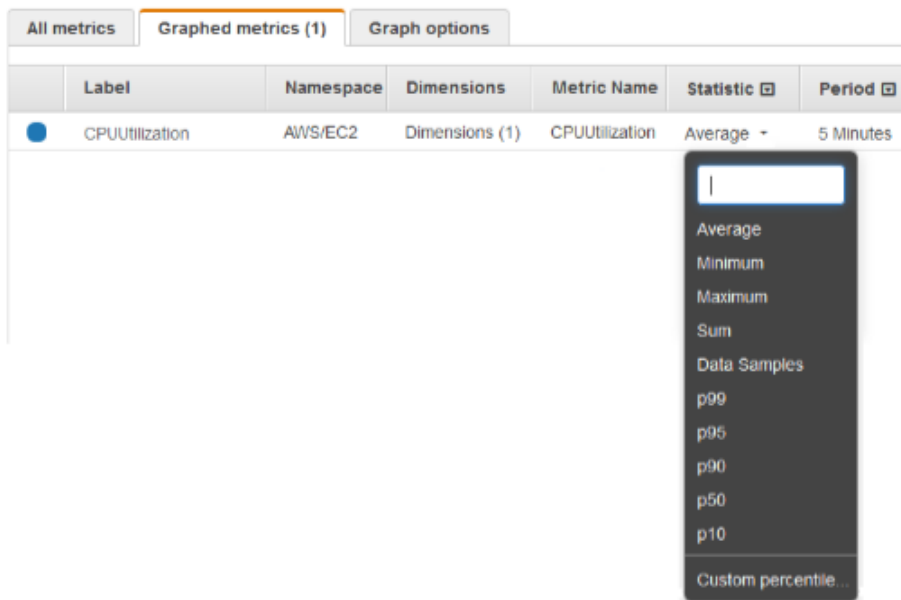




5. In the search field, type **CPUUtilization** and press Enter. Select the row for the specific instance, which displays a graph for the **CPUUtilization** metric for the instance. To change the name of the graph, choose the pencil icon. To change the time range, select one of the predefined values or choose **custom**.



6. To change the statistic, choose the **Graphed metrics** tab. Choose the column heading or an individual value, and then choose one of the statistics or predefined percentiles, or specify a custom percentile (for example, p95.45).

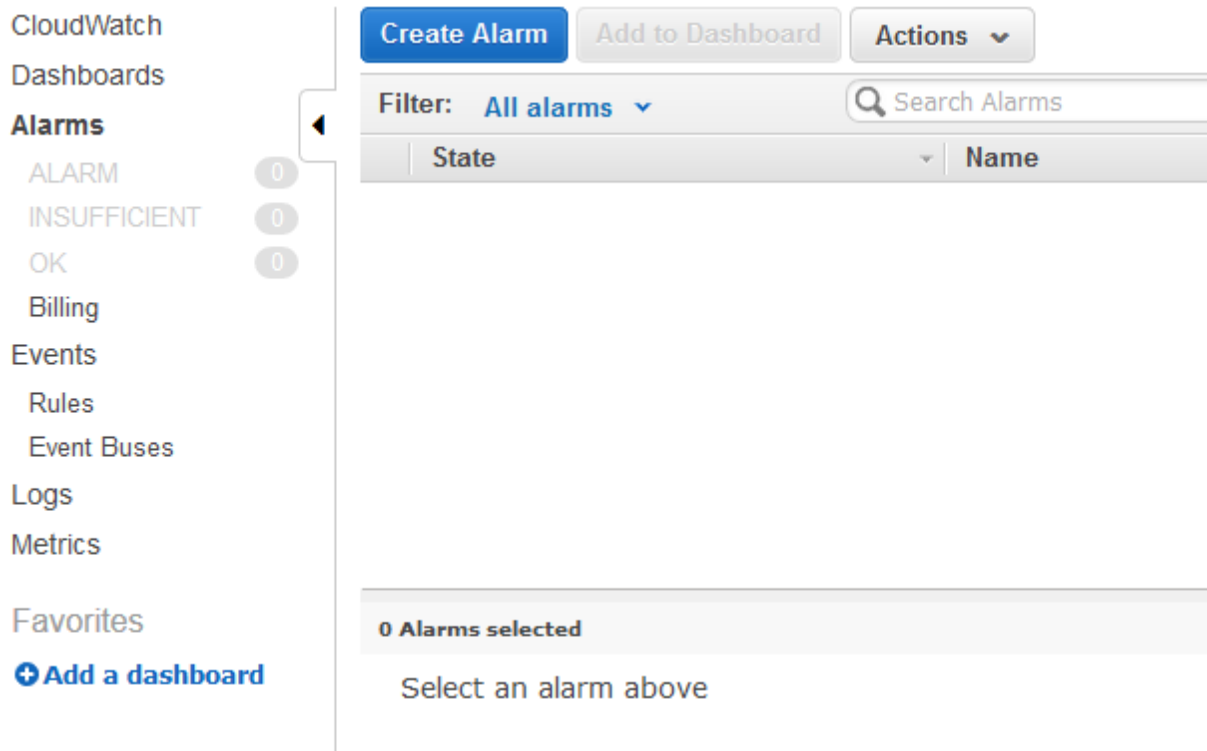


The screenshot shows the 'Graphed metrics (1)' tab in the AWS CloudWatch console. A table lists the metric 'CPUUtilization' in the 'AWS/EC2' namespace with 'Dimensions (1)'. The 'Statistic' column is set to 'Average' and the 'Period' is '5 Minutes'. A dropdown menu is open for the 'Statistic' column, showing options: Average, Minimum, Maximum, Sum, Data Samples, p99, p95, p90, p50, p10, and Custom percentile...

	Label	Namespace	Dimensions	Metric Name	Statistic	Period
	CPUUtilization	AWS/EC2	Dimensions (1)	CPUUtilization	Average	5 Minutes

7. To change the period, choose the **Graphed metrics** tab. Choose the column heading or an individual value, and then choose a different value.

To create a Alarm:



The screenshot shows the AWS CloudWatch 'Alarms' page. On the left, a navigation menu includes 'CloudWatch', 'Dashboards', 'Alarms' (selected), 'Billing', 'Events', 'Rules', 'Event Buses', 'Logs', 'Metrics', and 'Favorites'. The 'Alarms' section shows '0' alarms. The main content area has a 'Create Alarm' button, an 'Add to Dashboard' button, and an 'Actions' dropdown. Below these is a 'Filter: All alarms' dropdown and a 'Search Alarms' search bar. A table header shows 'State' and 'Name' columns. At the bottom, it says '0 Alarms selected' and 'Select an alarm above'.

### Create Alarm

1. Select Metric2. Define Alarm

Browse MetricsSearch Metrics

#### CloudWatch Metrics by Category

Your CloudWatch metric summary has loaded. Total metrics: 1,249

<b>EBS Metrics: 354</b> Per-Volume Metrics: 354	<b>EC2 Metrics: 591</b> Per-Instance Metrics: 526 By Auto Scaling Group: 65	<b>ELB Metrics: 144</b> Per-LB Metrics: 52 Per LB, per AZ Metrics: 47 By Availability Zone: 21 Across All LBs: 8 By Namespace: 8 By Service: 8
<b>ElasticBeanstalk Metrics: 6</b> Environment Metrics: 6	<b>Events Metrics: 9</b> Across All Rules: 4 By Rule Name: 5	<b>Lambda Metrics: 30</b> Across All Functions: 6 By Function Name: 12 By Resource: 12
<b>Logs Metrics: 8</b> Account Metrics: 2 Log Group Metrics: 6	<b>NATGateway Metrics: 14</b> NAT Gateway Metrics: 14	<b>RDS Metrics: 76</b> Per-Database Metrics: 28 By Database Class: 16

Update Graph

CancelPreviousNextCreate Alarm

## 1. Select a metric for what we need

### Create Alarm

1. Select Metric2. Define Alarm

EC2Search Metrics

1 to 50 of 200 metrics

<input type="checkbox"/>	i-00419b2a7c4745c58	CPU Surplus Credits Charged
<input checked="" type="checkbox"/>	i-00419b2a7c4745c58	CPU Utilization
<input type="checkbox"/>	i-00419b2a7c4745c58	Disk Read Bytes
<input type="checkbox"/>	i-00419b2a7c4745c58	Disk Read Ops
<input type="checkbox"/>	i-00419b2a7c4745c58	Disk Write Bytes

**Title: CPUUtilization**

Average5 Minutes

1.00

0.5

0

00:30 01:30 02:30 03:30 04:30 05:30 06:30 07:30 08:30 09:30 10:30 11:30

CPUUtilization

Update Graph

Time Range

RelativeAbsoluteUTC (GMT)

From: 12.02 hours ago

To: 0 hours ago

Zoom: 1h | 3h | 6h | 12h | 1d | 3d | 1w | 2w

Left Y-axis

Limits Min 0 Max

AutoAuto

CancelPreviousNextCreate Alarm

## 2. Define a ALARM

### Create Alarm

1. Select Metric

2. Define Alarm

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name:

Description:


Whenever: CPUUtilization

is:

for: 1  datapoints

This alarm will trigger when the blue line goes up to or above the red line for 1 datapoints within 5 minutes

CPUUtilization >= 75 for 1 datapoints within 5 mi...



Namespace: AWS/EC2

Instanceld:

Metric Name:

Period:

Statistic: ☒ Standard ☐ Custom

Additional settings

Provide additional configuration for your alarm.

Treat missing data as:

Actions

Define what actions are taken when your alarm changes state.

Cancel Previous Next Create Alarm

### Notification

Define what actions are taken when your alarm changes state.

Whenever this alarm:

Send notification to:

Email list:

+ Notification + AutoScaling Action + EC2 Action

Cancel Previous Next Create Alarm

## Types of Status Checks

There are two types of status checks: system status checks and instance status checks.

### System Status Checks

Monitor the AWS systems on which your instance runs. These checks detect underlying problems with your instance that require AWS involvement to repair. When a system status check fails, you can choose to wait for AWS to fix the issue, or you can resolve it yourself. For instances backed by Amazon EBS, you can stop and start the instance yourself, which in most cases migrates it to a new host computer. For instances backed by instance store, you can terminate and replace the instance.

The following are examples of problems that can cause system status checks to fail:

- Loss of network connectivity
- Loss of system power
- Software issues on the physical host
- Hardware issues on the physical host that impact network reachability

### Instance Status Checks

Monitor the software and network configuration of your individual instance. These checks detect problems that require your involvement to repair. When an instance status check fails, typically you will need to address the problem yourself (for example, by rebooting the instance or by making instance configuration changes).

The following are examples of problems that can cause instance status checks to fail:

- Failed system status checks
- Incorrect networking or startup configuration
- Exhausted memory
- Corrupted file system
- Incompatible kernel

### Viewing Status Checks

Amazon EC2 provides you with several ways to view and work with status checks.

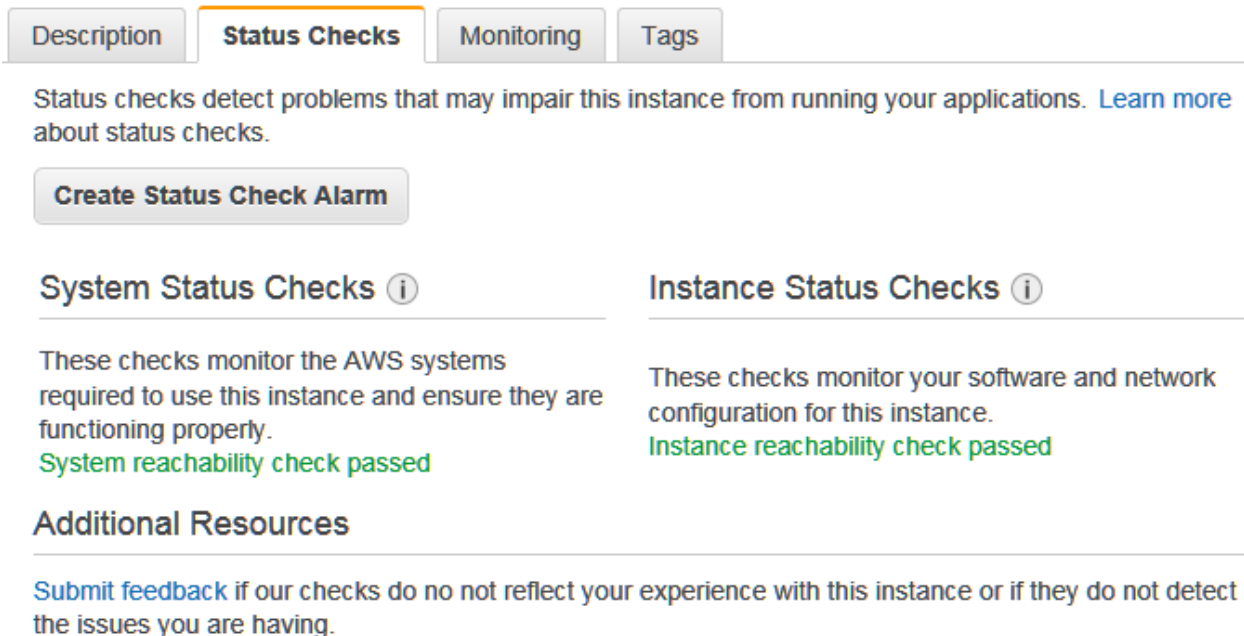
#### Viewing Status Using the Console

You can view status checks using the AWS Management Console.



## To view status checks using the console

- Open the Amazon EC2 console at <https://console.aws.amazon.com/ec2/>.
- In the navigation pane, choose **Instances**.
- On the **Instances** page, the **Status Checks** column lists the operational status of each instance.
- To view the status of a specific instance, select the instance, and then choose the **Status Checks** tab.



Buttons: Description, **Status Checks**, Monitoring, Tags

Status checks detect problems that may impair this instance from running your applications. [Learn more](#) about status checks.

[Create Status Check Alarm](#)

### System Status Checks ⓘ

These checks monitor the AWS systems required to use this instance and ensure they are functioning properly.

System reachability check passed

### Instance Status Checks ⓘ

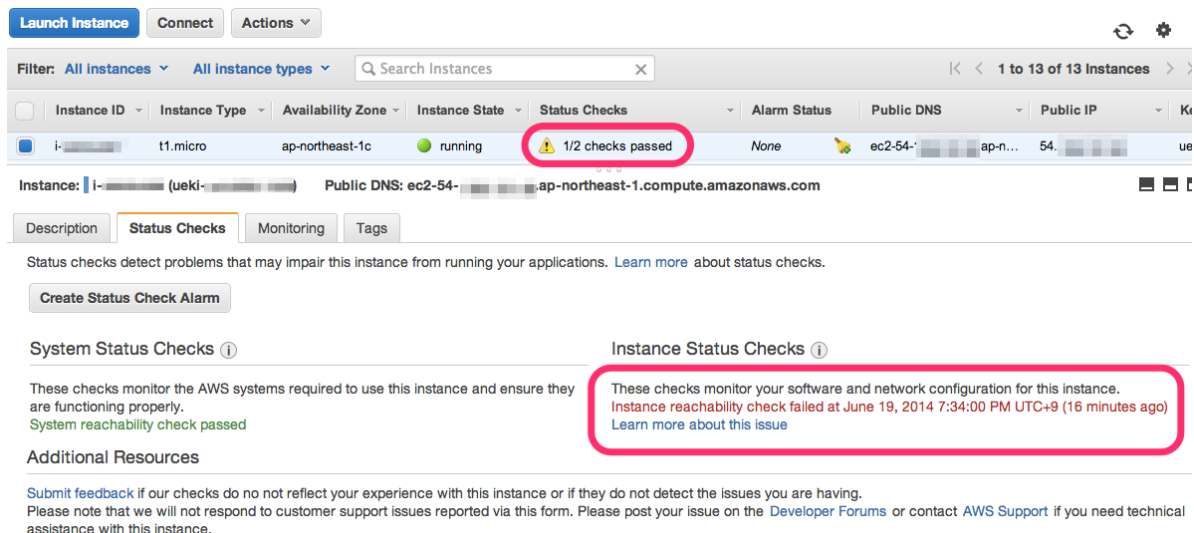
These checks monitor your software and network configuration for this instance.

Instance reachability check passed

### Additional Resources

[Submit feedback](#) if our checks do not reflect your experience with this instance or if they do not detect the issues you are having.

If you have an instance with a failed status check and the instance has been unreachable for over 20 minutes, choose **AWS Support** to submit a request for assistance. To troubleshoot system or instance status check failures yourself



Buttons: Launch Instance, Connect, Actions

Filter: All instances, All instance types, Search Instances

Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP
i-...	t1.micro	ap-northeast-1c	running	1/2 checks passed	None	ec2-54-...	54-...

Instance: i-... (ueki-...) Public DNS: ec2-54-... ap-northeast-1.compute.amazonaws.com

Buttons: Description, **Status Checks**, Monitoring, Tags

Status checks detect problems that may impair this instance from running your applications. [Learn more](#) about status checks.

[Create Status Check Alarm](#)

### System Status Checks ⓘ

These checks monitor the AWS systems required to use this instance and ensure they are functioning properly.

System reachability check passed

### Instance Status Checks ⓘ

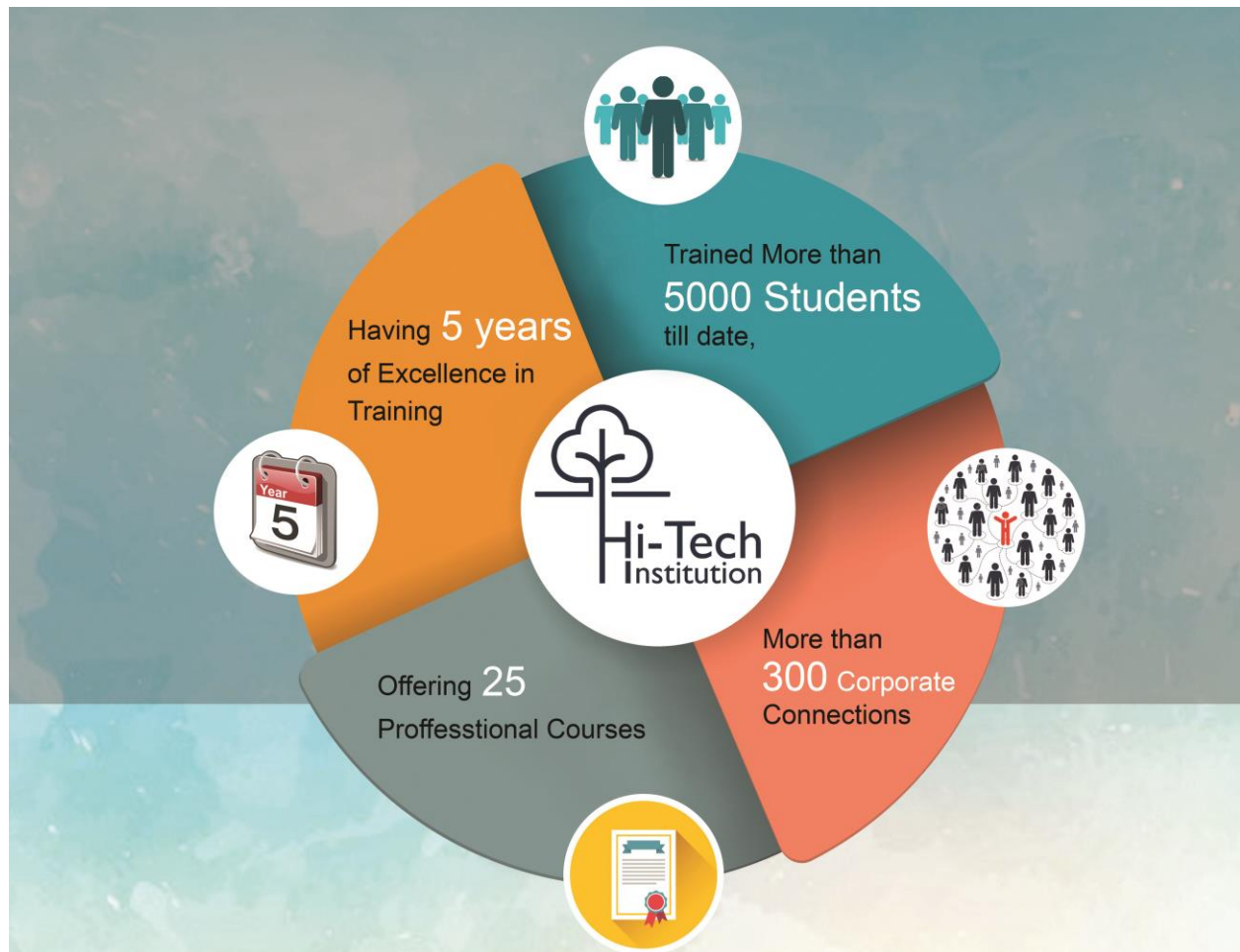
These checks monitor your software and network configuration for this instance.

Instance reachability check failed at June 19, 2014 7:34:00 PM UTC+9 (16 minutes ago)

[Learn more about this issue](#)

### Additional Resources

[Submit feedback](#) if our checks do not reflect your experience with this instance or if they do not detect the issues you are having. Please note that we will not respond to customer support issues reported via this form. Please post your issue on the [Developer Forums](#) or contact [AWS Support](#) if you need technical assistance with this instance.



## TOP RECRUITERS





**offer for School or College students**

**30% offer for IT Employees**

Above offer applicable only technical courses. Terms and conditions apply



[operations@hitechins.in](mailto:operations@hitechins.in)



[www.hitechins.in](http://www.hitechins.in)



**CONTACT US**

**7092 90 91 92 / 82 20 21 7640**

**PONDICHERRY**

No.32, 100 feet road,  
Ellaipillaichavady,  
Pondicherry – 605 005,  
Nearby Rajiv Gandhi Hospital

**TAMBARAM**

No.24, Chithi Vinayagar Kovil street,  
KamarajNagar, Tambaram Sanatorium,  
Chennai – 600 047,  
Nearby Sanatorium Railway Station

**VELACHERRY**

No: 21, Officer Colony,  
100 feet road, VijayaNagar,  
Velacherry – 600 042,  
Nearby Sathya Home Appliances

**Locations**

**Chennai & Pondicherry**