# What is Amazon CloudWatch (is monitoring tool)?

Amazon CloudWatch **monitors** your Amazon Web Services (AWS) resources and the applications you run on AWS in real time. You can use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications.

**The CloudWatch home page (dashboard)** automatically displays metrics about every AWS service you use. You can additionally create custom dashboards to display metrics about your custom applications, and display custom collections of metrics that you choose.

You can create alarms which **watch metrics** and send notifications or automatically make **changes to the resources you are monitoring when a threshold is breached**. For example, you can monitor the **CPU usage and disk reads and writes of your Amazon EC2 instances and then use this data to determine whether you should launch additional instances to handle increased load**. You can also use this data to stop under-used instances to save money.

With CloudWatch, you gain system-wide visibility into resource utilization, application performance, and **operational health.**

## Related AWS Services

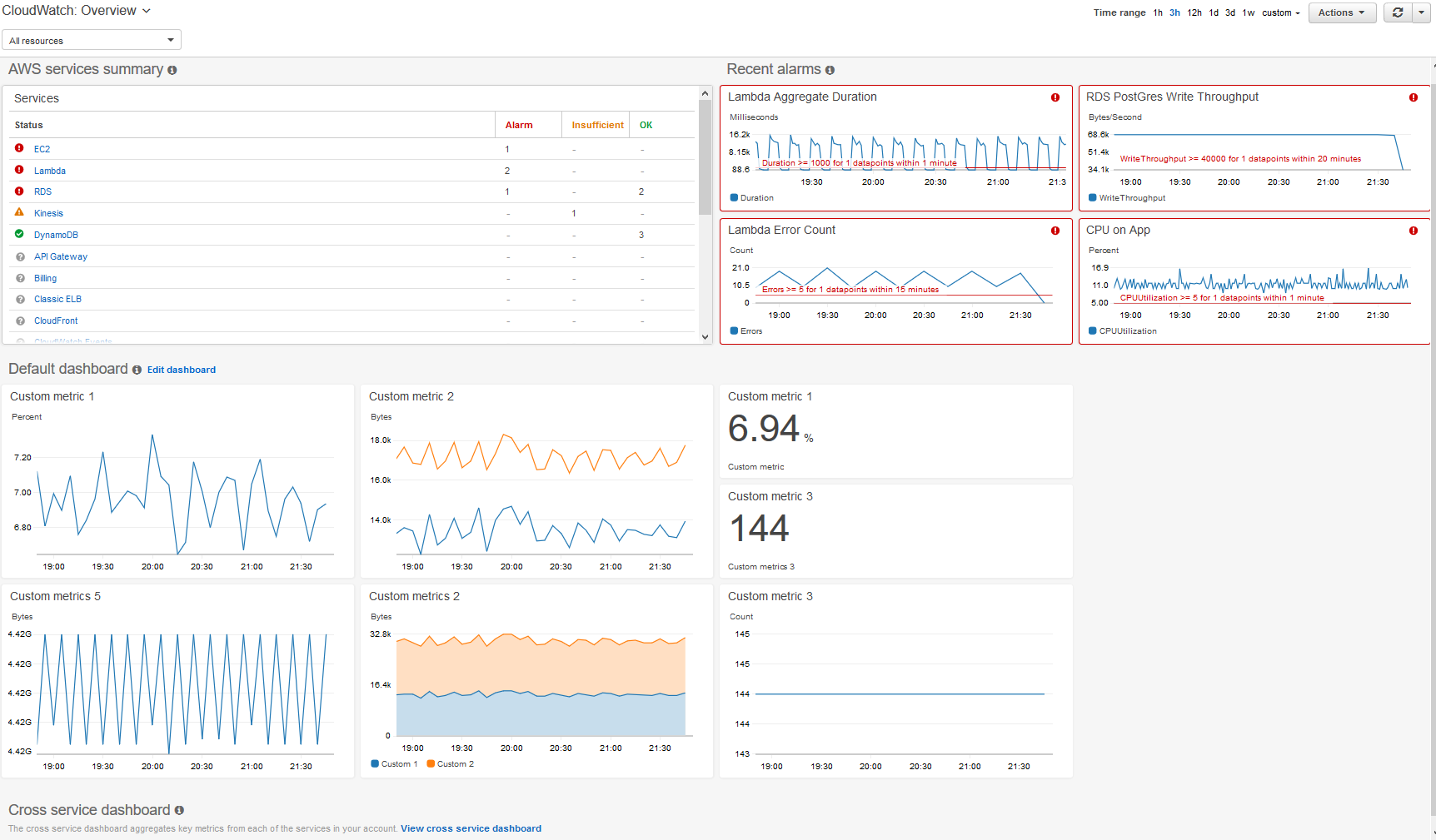
The following services are used along with Amazon CloudWatch:

* **Amazon Simple Notification Service (Amazon SNS)** coordinates and manages the delivery or sending of messages to subscribing endpoints or clients. You use Amazon SNS with CloudWatch to send messages when an alarm threshold has been reached. For more information, see Set Up Amazon SNS Notifications.
* **Amazon EC2 Auto Scaling** enables you to automatically launch or terminate Amazon EC2 instances based on user-defined policies, health status checks, and schedules. You can use a CloudWatch alarm with Amazon EC2 Auto Scaling to scale your EC2 instances based on demand. For more information, see Dynamic Scaling in the Amazon EC2 Auto Scaling User Guide.
* **AWS CloudTrail** enables you to monitor the calls made to the Amazon CloudWatch API for your account, including calls made by the AWS Management Console, AWS CLI, and other services. When CloudTrail logging is turned on, CloudWatch writes log files to the Amazon S3 bucket that you specified when you configured CloudTrail. For more information, see Logging Amazon CloudWatch API Calls with AWS CloudTrail.
* **AWS Identity and Access Management (IAM)** is a web service that helps you securely control access to AWS resources for your users. Use IAM to control who can use your AWS resources (authentication) and what resources they can use in which ways (authorization). For more information, see Authentication and Access Control for Amazon CloudWatch.

**Getting Started with Amazon CloudWatch**

Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.

The CloudWatch overview home page appears.



The overview displays the following items, refreshed automatically.

* The upper left shows a list of AWS services you use in your account, along with the state of alarms in those services. The upper right shows two or four alarms in your account, depending on how many AWS services you use. The alarms shown are those in the ALARM state or those that most recently changed state.

These upper areas enable you to assess the health of your AWS services, by seeing the alarm states in every service and the alarms that most recently changed state. This helps you monitor and quickly diagnose issues.

* Below these areas is the custom dashboard that you have created and named **CloudWatch-Default**, if any. This is a convenient way for you to add metrics about your own custom services or applications to the overview page, or to bring forward additional key metrics from AWS services that you most want to monitor.
* If you use six or more AWS services, below the default dashboard is a link to the automatic cross-service dashboard. The cross-service dashboard automatically displays key metrics from every AWS service you use, without requiring you to choose what metrics to monitor or create custom dashboards. You can also use it to drill down to any AWS service and see even more key metrics for that service.

If you use fewer than six AWS services, the cross-service dashboard is shown automatically on this page.

From this overview, you can focus your view to a specific resource group or a specific AWS service. This enables you to narrow your view to a subset of resources in which you are interested. Using resource groups enables you to use tags to organize projects, focus on a subset of your architecture, or just distinguish between your production and development environments.

# Set Up Amazon SNS Notifications

Amazon CloudWatch uses Amazon SNS to send email. First, create and subscribe to an SNS topic. When you create a CloudWatch alarm, you can add this SNS topic to send an email notification when the alarm changes state. For more information, see the Amazon Simple Notification Service Getting Started Guide.

**Note**

Alternatively, if you plan to create your CloudWatch alarm using the AWS Management Console, you can skip this procedure because you can create the topic through the **Create Alarm Wizard**.

## Set Up an Amazon SNS Topic Using the AWS Management Console

First, create a topic, then subscribe to it. You can optionally publish a test message to the topic.

**To create an SNS topic**

1. Open the Amazon SNS console at https://console.aws.amazon.com/sns/v2/home.
2. On the Amazon SNS dashboard, under **Common actions**, choose **Create Topic**.
3. In the **Create new topic** dialog box, for **Topic name**, type a name for the topic (for example, my-topic).
4. Choose **Create topic**.
5. Copy the **Topic ARN** for the next task (for example, arn:aws:sns:us-east-1:111122223333:my-topic).

**To subscribe to an SNS topic**

1. Open the Amazon SNS console at https://console.aws.amazon.com/sns/v2/home.
2. In the navigation pane, choose **Subscriptions**, **Create subscription**.
3. In the **Create subscription** dialog box, for **Topic ARN**, paste the topic ARN that you created in the previous task.
4. For **Protocol**, choose **Email**.
5. For **Endpoint**, type an email address that you can use to receive the notification, and then choose **Create subscription**.
6. From your email application, open the message from AWS Notifications and confirm your subscription.

Your web browser displays a confirmation response from Amazon SNS.

**To publish a test message to an SNS topic**

1. Open the Amazon SNS console at https://console.aws.amazon.com/sns/v2/home.
2. In the navigation pane, choose **Topics**.
3. On the **Topics** page, select a topic and choose **Publish to topic**.
4. In the **Publish a message** page, for **Subject**, type a subject line for your message, and for **Message**, type a brief message.
5. Choose **Publish Message**.
6. Check your email to confirm that you received the message.

## Set Up an SNS Topic Using the AWS CLI

First you create an SNS topic, and then publish a message directly to the topic to test that you have properly configured it.

**To set up an SNS topic**

1. Create the topic using the create-topic command as follows.

**aws sns create-topic --name *my-topic***

Amazon SNS returns a topic ARN with the following format:

{

"TopicArn": "arn:aws:sns:us-east-1:111122223333:my-topic"

}

1. Subscribe your email address to the topic using the subscribe command. If the subscription request succeeds, you receive a confirmation email message.

**aws sns subscribe --topic-arn arn:aws:sns:*us-east-1*:*111122223333*:*my-topic* --protocol email --notification-endpoint** *my-email-address*

Amazon SNS returns the following:

{

"SubscriptionArn": "pending confirmation"

}

1. From your email application, open the message from AWS Notifications and confirm your subscription.

Your web browser displays a confirmation response from Amazon Simple Notification Service.

1. Check the subscription using the list-subscriptions-by-topic command.

**aws sns list-subscriptions-by-topic --topic-arn arn:aws:sns:*us-east-1*:*111122223333*:*my-topic***

Amazon SNS returns the following:

{

"Subscriptions": [

{

"Owner": "111122223333",

"Endpoint": "me@mycompany.com",

"Protocol": "email",

"TopicArn": "arn:aws:sns:us-east-1:111122223333:my-topic",

"SubscriptionArn": "arn:aws:sns:us-east-1:111122223333:my-topic:64886986-bf10-48fb-a2f1-dab033aa67a3"

}

]

}

1. (Optional) Publish a test message to the topic using the publish command.

**aws sns publish --message "Verification" --topic arn:aws:sns:*us-east-1*:*111122223333*:*my-topic***

Amazon SNS returns the following:

{

"MessageId": "42f189a0-3094-5cf6-8fd7-c2dde61a4d7d"

}

1. Check your email to confirm that you received the message.