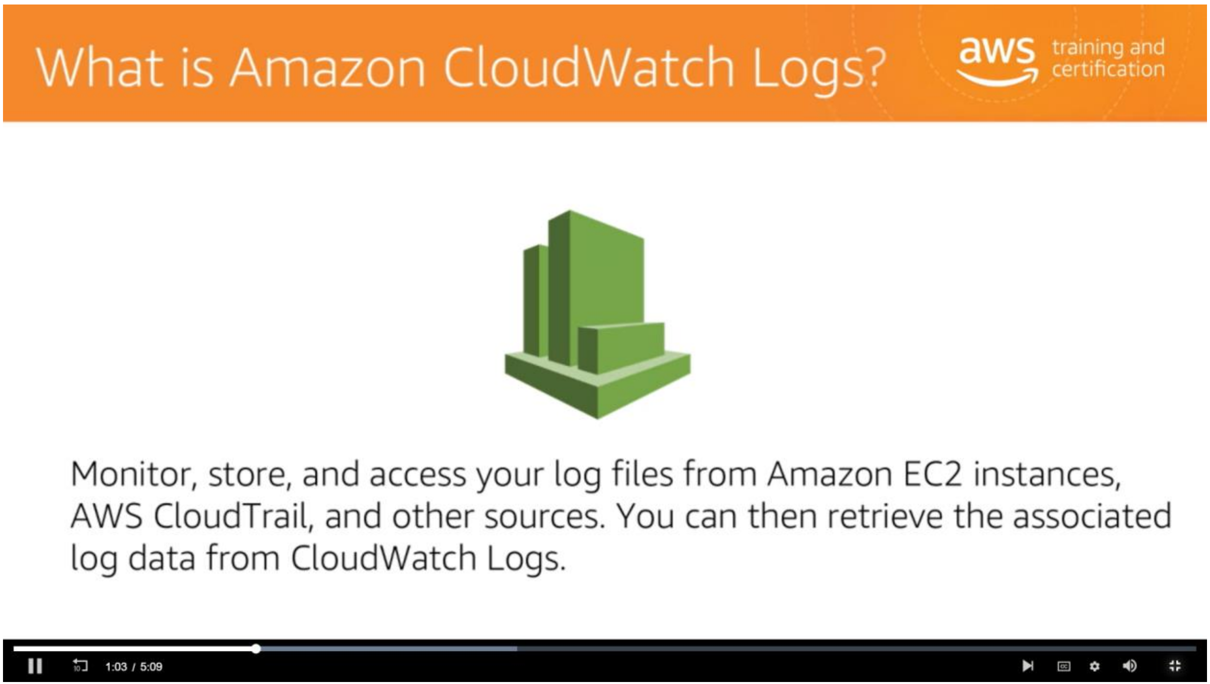
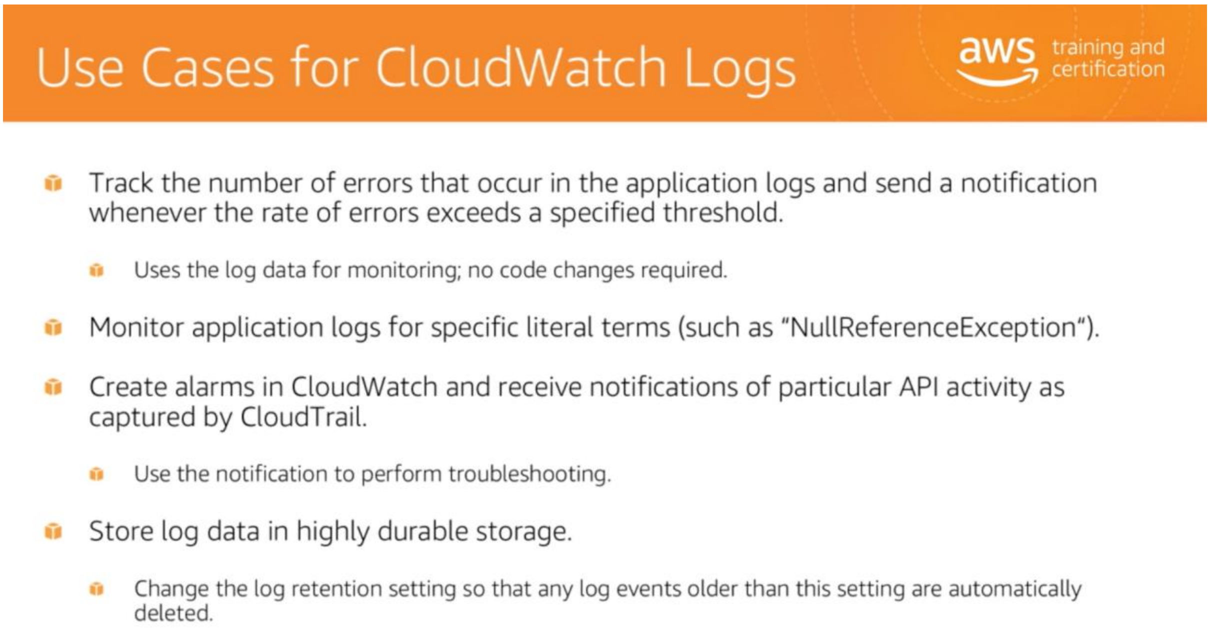


What is Amazon CloudWatch Logs?

Monitor, store, and access your log files from Amazon EC2 instances, AWS CloudTrail, and other sources. You can then retrieve the associated log data from CloudWatch Logs.

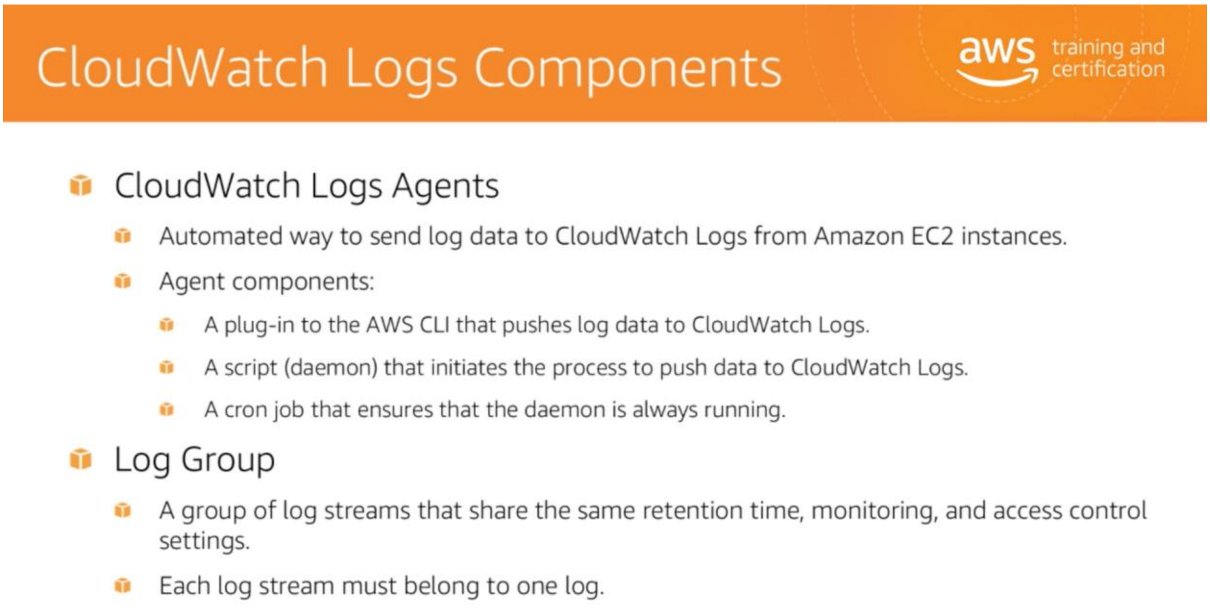
Amazon CloudWatch Logs Overview

- Monitor and troubleshoot systems and applications using existing system, application, and custom log files.
  - Monitor logs for specific phrases, values, or patterns.
  - Amazon EC2 instances, AWS CloudTrail, and other sources.
- Retrieves the associated log data from CloudWatch Logs.
- Includes an installable agent for Ubuntu, Amazon Linux, and Windows at no additional charge.



Use Cases for CloudWatch Logs

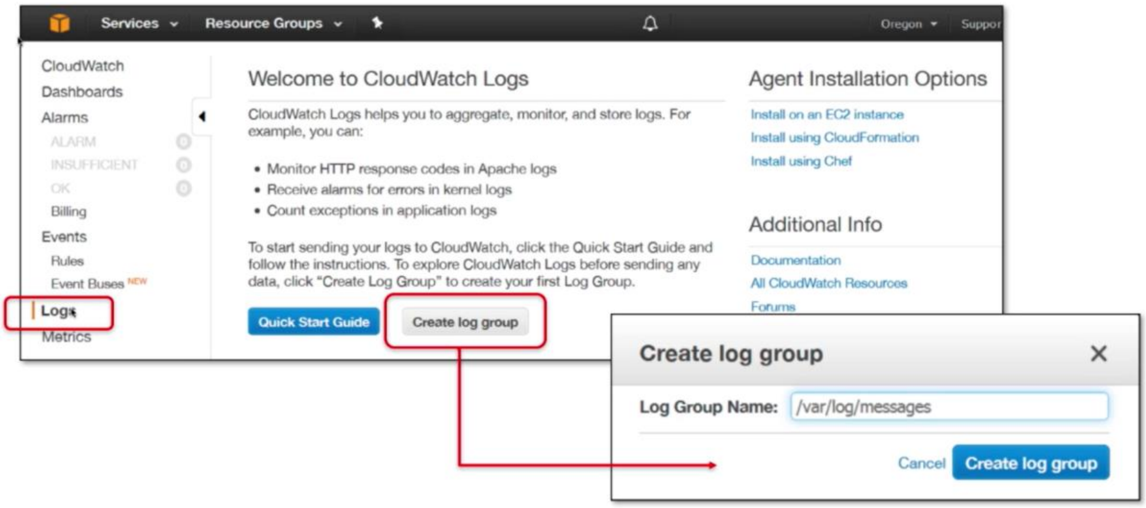
- Track the number of errors that occur in the application logs and send a notification whenever the rate of errors exceeds a specified threshold.
  - Uses the log data for monitoring; no code changes required.
- Monitor application logs for specific literal terms (such as "NullReferenceException").
- Create alarms in CloudWatch and receive notifications of particular API activity as captured by CloudTrail.
  - Use the notification to perform troubleshooting.
- Store log data in highly durable storage.
  - Change the log retention setting so that any log events older than this setting are automatically deleted.



CloudWatch Logs Components

- CloudWatch Logs Agents
  - Automated way to send log data to CloudWatch Logs from Amazon EC2 instances.
  - Agent components:
    - A plug-in to the AWS CLI that pushes log data to CloudWatch Logs.
    - A script (daemon) that initiates the process to push data to CloudWatch Logs.
    - A cron job that ensures that the daemon is always running.
- Log Group
  - A group of log streams that share the same retention time, monitoring, and access control settings.
  - Each log stream must belong to one log.

Create Log Group (1 of 2)



Welcome to CloudWatch Logs

CloudWatch Logs helps you to aggregate, monitor, and store logs. For example, you can:

- Monitor HTTP response codes in Apache logs
- Receive alarms for errors in kernel logs
- Count exceptions in application logs

To start sending your logs to CloudWatch, click the Quick Start Guide and follow the instructions. To explore CloudWatch Logs before sending any data, click "Create Log Group" to create your first Log Group.

Agent Installation Options

- Install on an EC2 instance
- Install using CloudFormation
- Install using Chef

Additional Info

- Documentation
- All CloudWatch Resources
- Forums

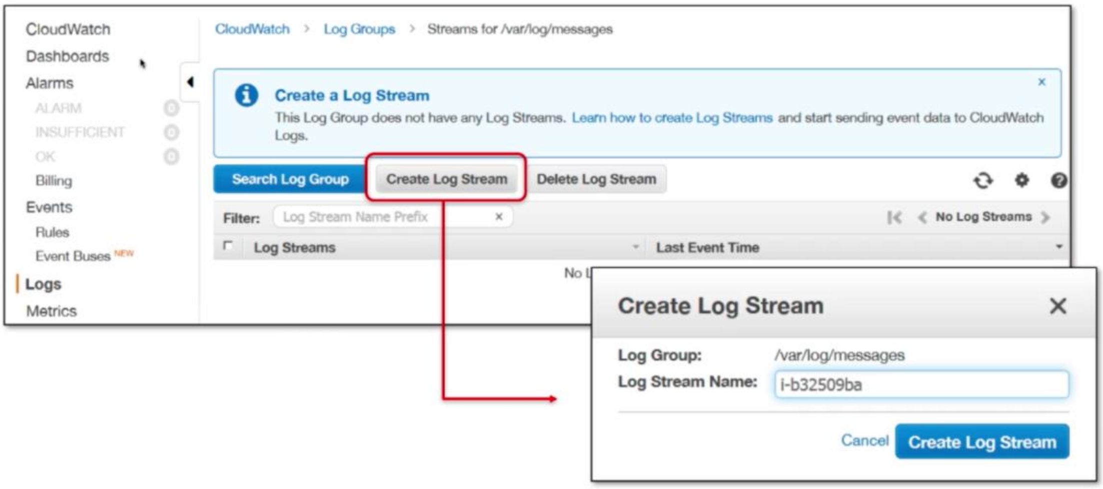
Create log group

Log Group Name: /var/log/messages

Cancel | Create log group

Create Log Stream (1 of 2)

Sequence of Log Events from the same source (a particular application instance or resource).



CloudWatch > Log Groups > Streams for /var/log/messages

Create a Log Stream

This Log Group does not have any Log Streams. Learn how to create Log Streams and start sending event data to CloudWatch Logs.

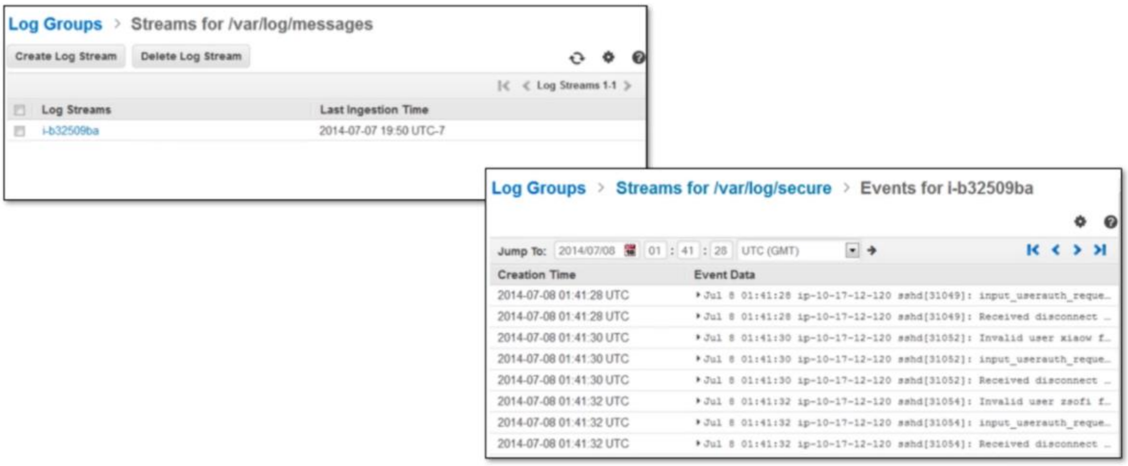
Create Log Stream

Log Group: /var/log/messages

Log Stream Name: i-b32509ba

Cancel | Create Log Stream

Create Log Stream (2 of 2)



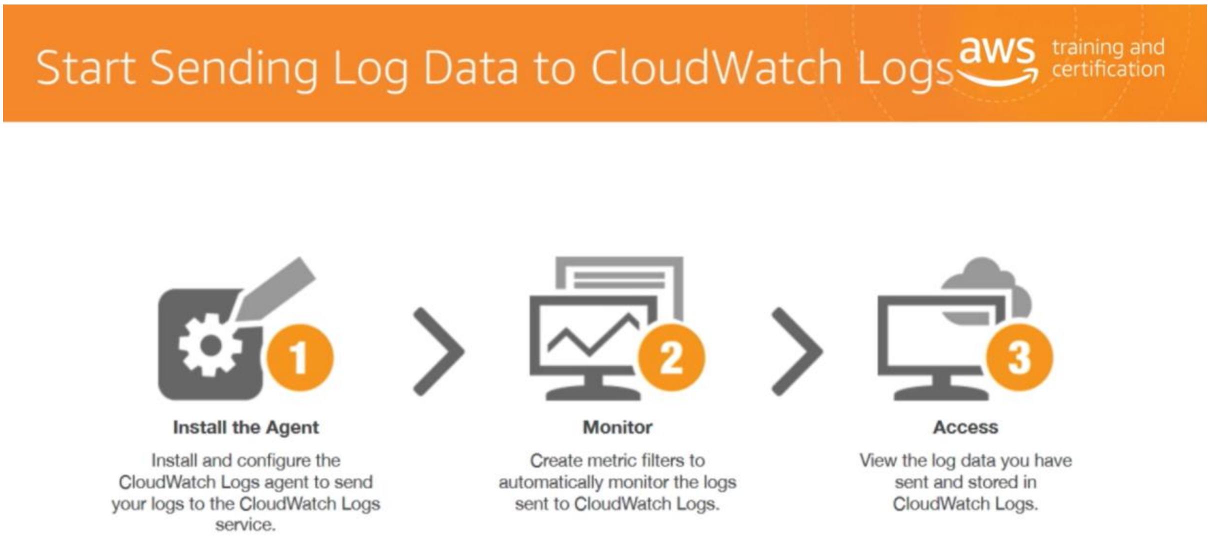
Log Groups > Streams for /var/log/messages
Create Log Stream
Delete Log Stream
Log Streams 1-1

□	Log Streams	Last Ingestion Time
□	i-b32509ba	2014-07-07 19:50 UTC-7

Log Groups > Streams for /var/log/secure > Events for i-b32509ba

Jump To: 2014/07/08 01 : 41 : 28 UTC (GMT)

Creation Time	Event Data
2014-07-08 01:41:28 UTC	▸Jul 8 01:41:28 ip-10-17-12-120 sshd[31049]: input_userauth_reque...
2014-07-08 01:41:28 UTC	▸Jul 8 01:41:28 ip-10-17-12-120 sshd[31049]: Received disconnect ...
2014-07-08 01:41:30 UTC	▸Jul 8 01:41:30 ip-10-17-12-120 sshd[31052]: Invalid user xiaow f...
2014-07-08 01:41:30 UTC	▸Jul 8 01:41:30 ip-10-17-12-120 sshd[31052]: input_userauth_reque...
2014-07-08 01:41:30 UTC	▸Jul 8 01:41:30 ip-10-17-12-120 sshd[31052]: Received disconnect ...
2014-07-08 01:41:32 UTC	▸Jul 8 01:41:32 ip-10-17-12-120 sshd[31054]: Invalid user zsofi f...
2014-07-08 01:41:32 UTC	▸Jul 8 01:41:32 ip-10-17-12-120 sshd[31054]: input_userauth_reque...
2014-07-08 01:41:32 UTC	▸Jul 8 01:41:32 ip-10-17-12-120 sshd[31054]: Received disconnect ...



Start Sending Log Data to CloudWatch Logs

Install the Agent

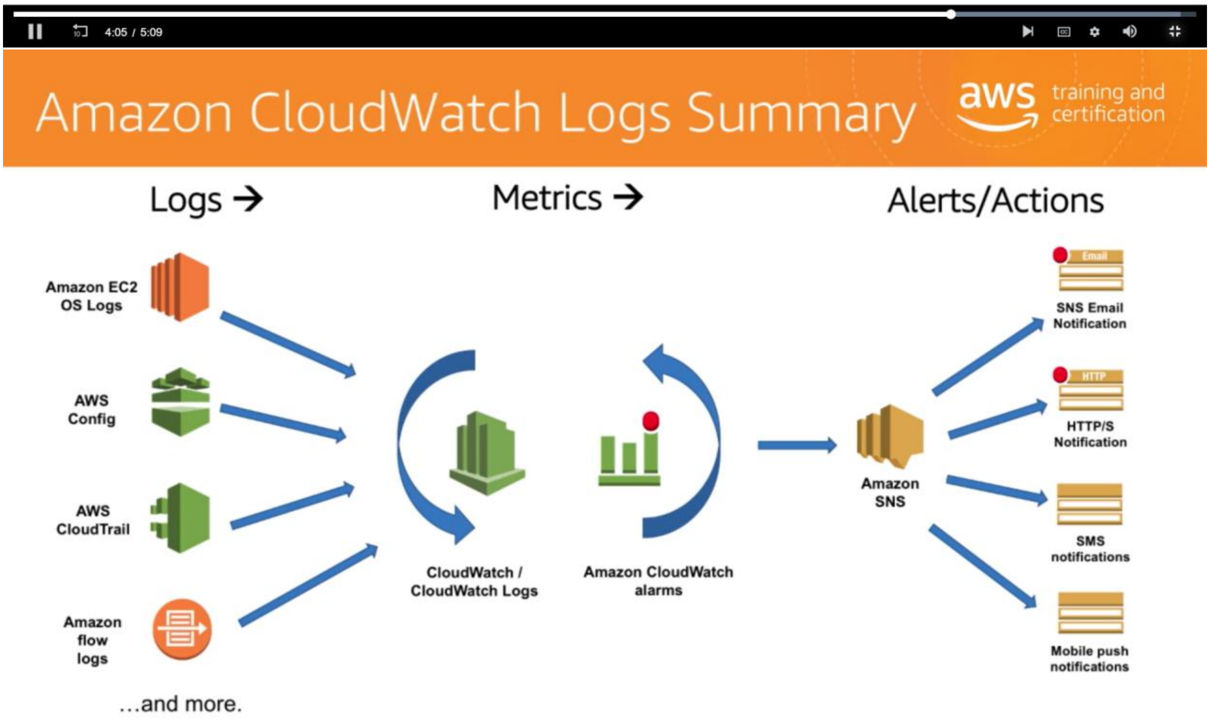
Install and configure the CloudWatch Logs agent to send your logs to the CloudWatch Logs service.

Monitor

Create metric filters to automatically monitor the logs sent to CloudWatch Logs.

Access

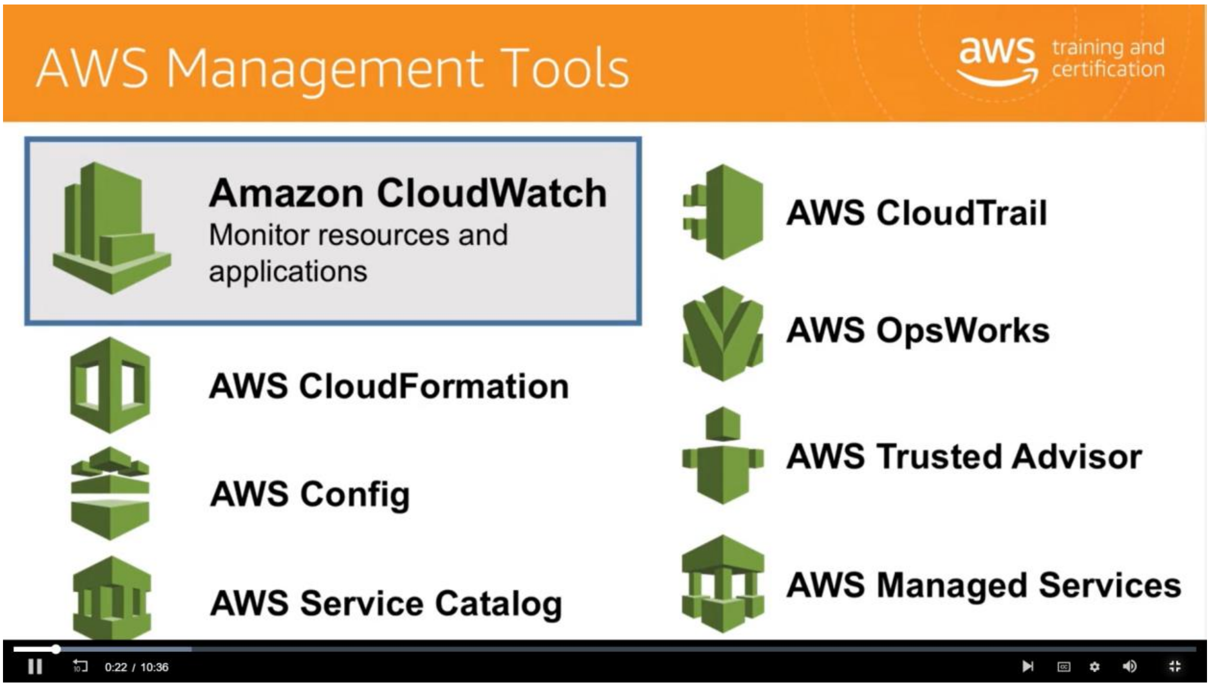
View the log data you have sent and stored in CloudWatch Logs.



Amazon CloudWatch Logs Summary

Logs → Metrics → Alerts/Actions

…and more.



AWS Management Tools

Amazon CloudWatch
Monitor resources and applications

AWS CloudFormation

AWS Config

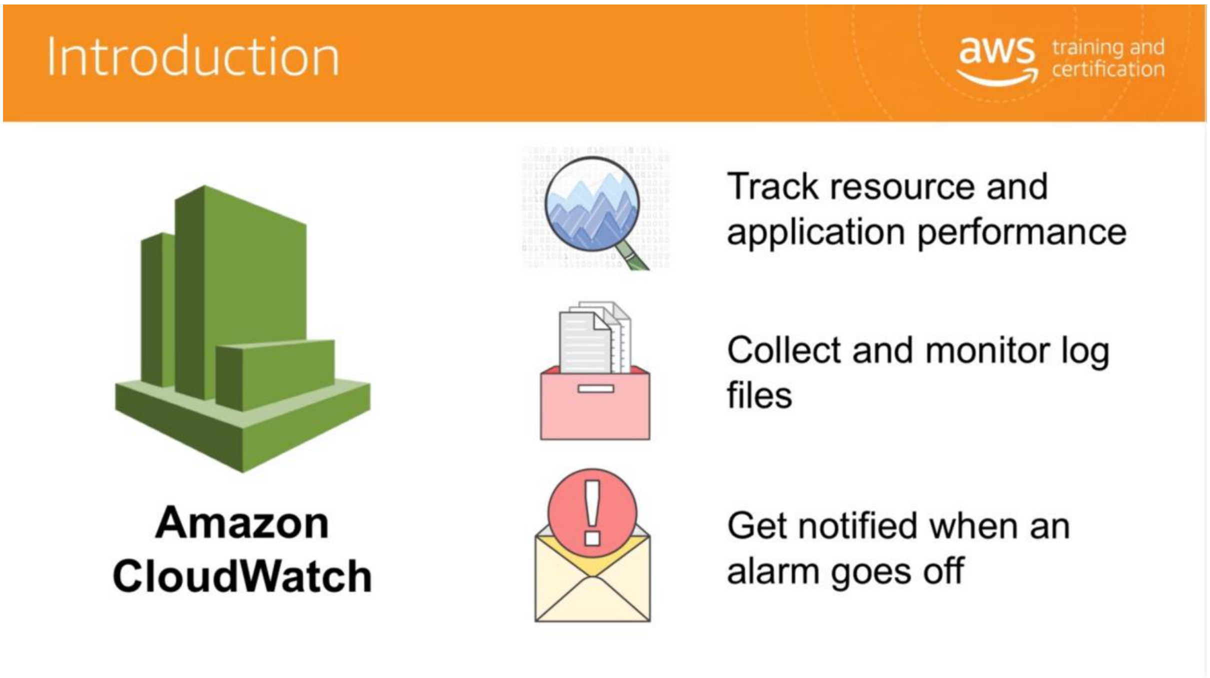
AWS Service Catalog

AWS CloudTrail

AWS OpsWorks

AWS Trusted Advisor

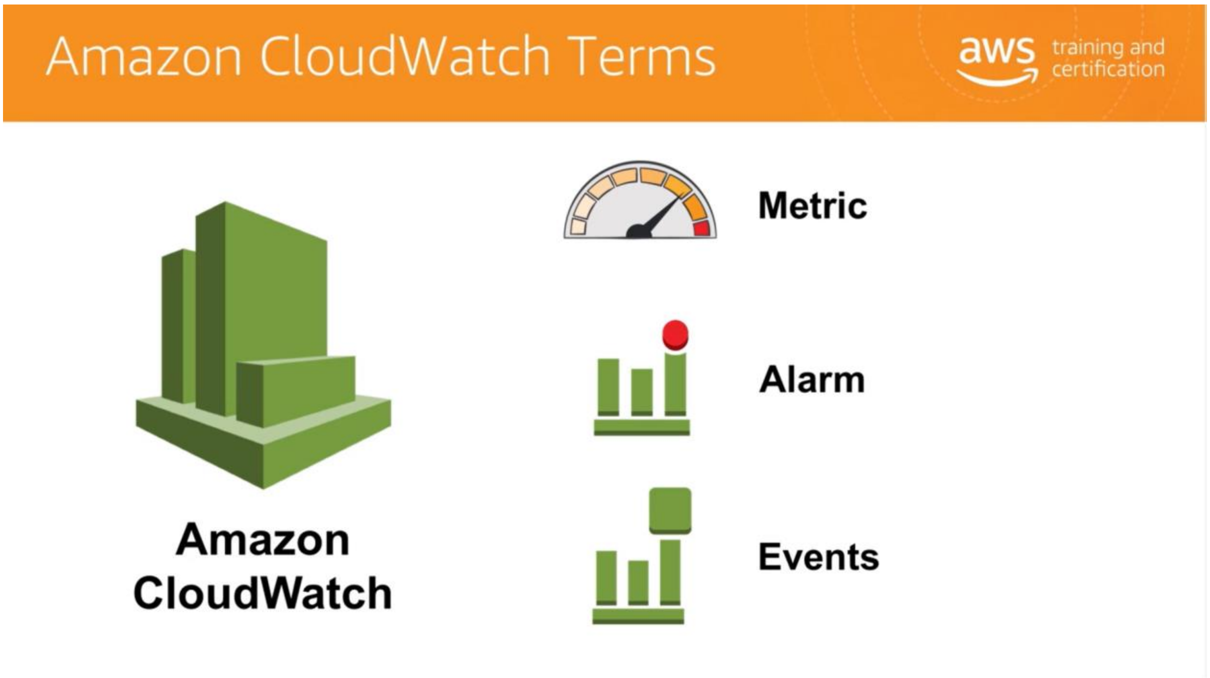
AWS Managed Services



Introduction

Amazon CloudWatch

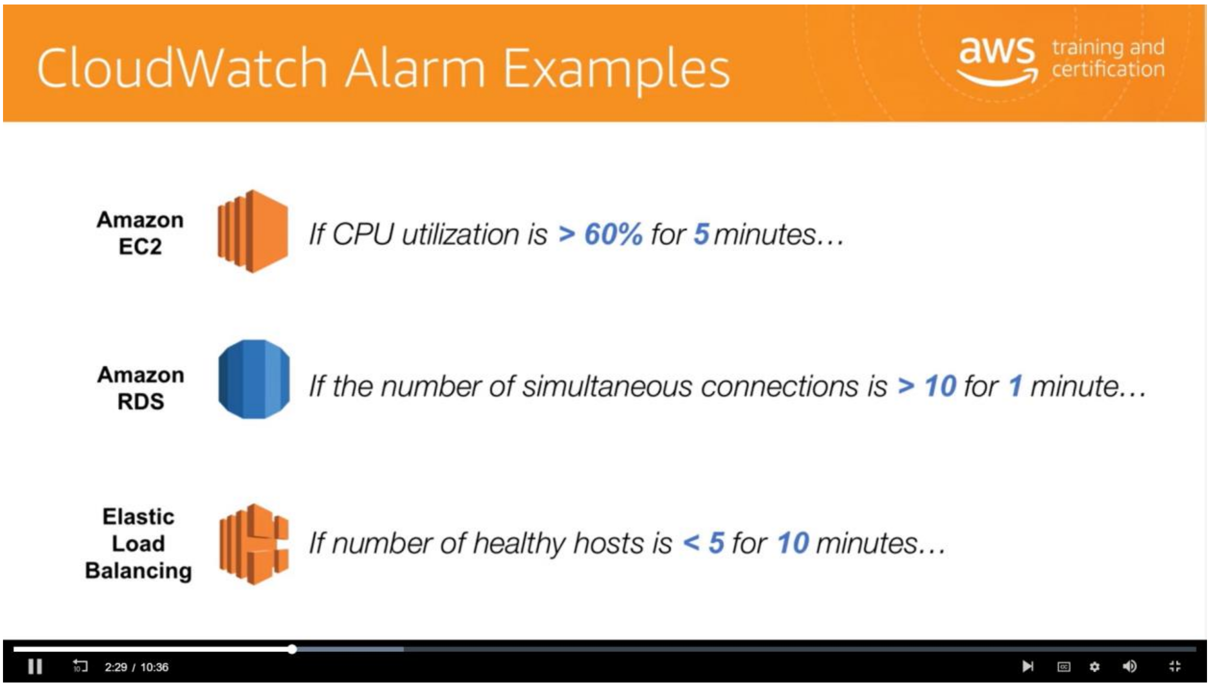
- Track resource and application performance
- Collect and monitor log files
- Get notified when an alarm goes off



Amazon CloudWatch Terms

Amazon CloudWatch

- **Metric**
- **Alarm**
- **Events**



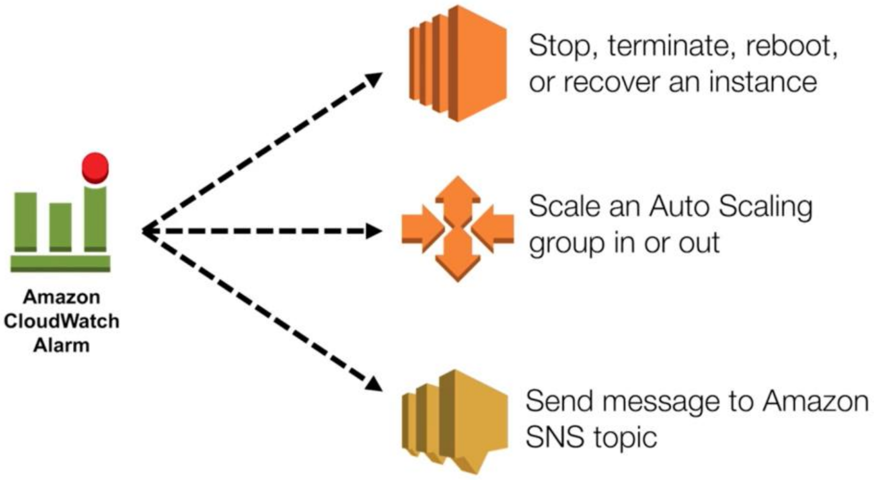
CloudWatch Alarm Examples

Amazon EC2 — *If CPU utilization is **> 60%** for **5** minutes…*

Amazon RDS — *If the number of simultaneous connections is **> 10** for **1** minute…*

Elastic Load Balancing — *If number of healthy hosts is **< 5** for **10** minutes…*

CloudWatch Alarms and Actions



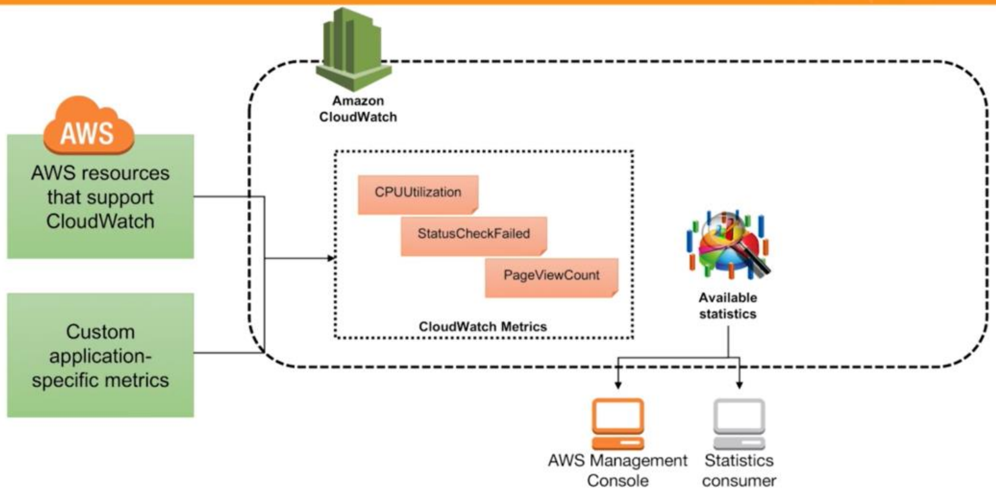
Amazon CloudWatch Alarm

Stop, terminate, reboot, or recover an instance

Scale an Auto Scaling group in or out

Send message to Amazon SNS topic

CloudWatch Architecture



AWS resources that support CloudWatch

Custom application-specific metrics

Amazon CloudWatch

CloudWatch Metrics

CPUUtilization

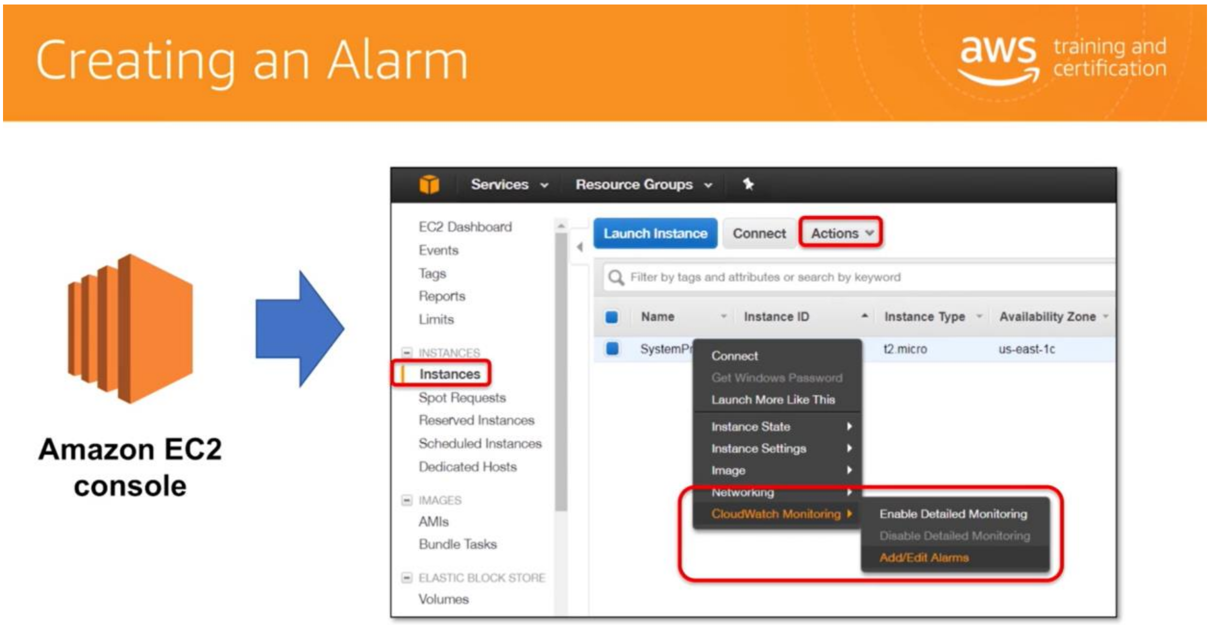
StatusCheckFailed

PageViewCount

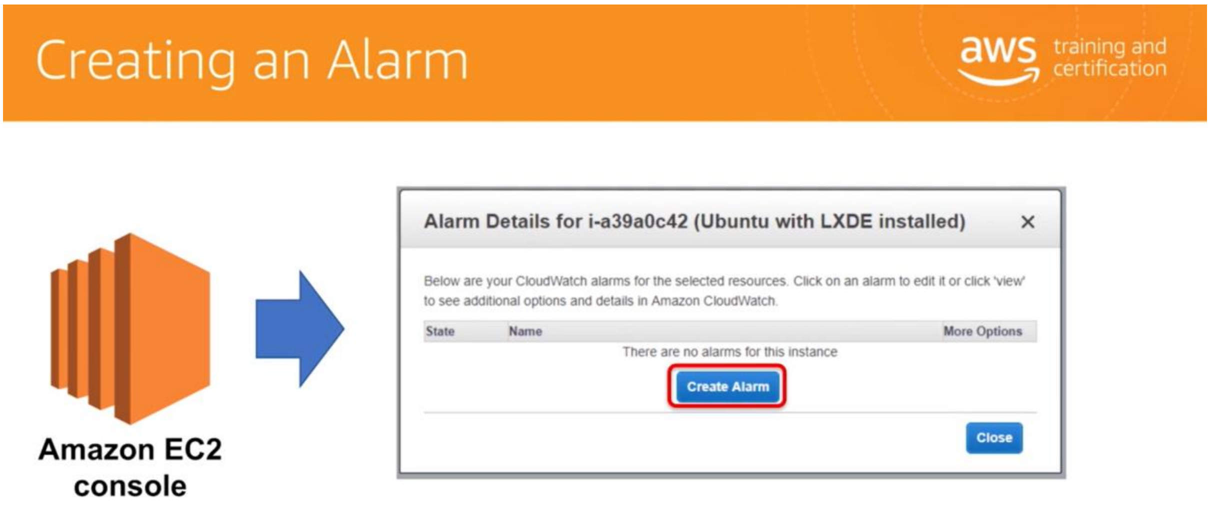
Available statistics

AWS Management Console

Statistics consumer



Creating an Alarm



Creating an Alarm

Alarm Details for i-a39a0c42 (Ubuntu with LXDE installed)

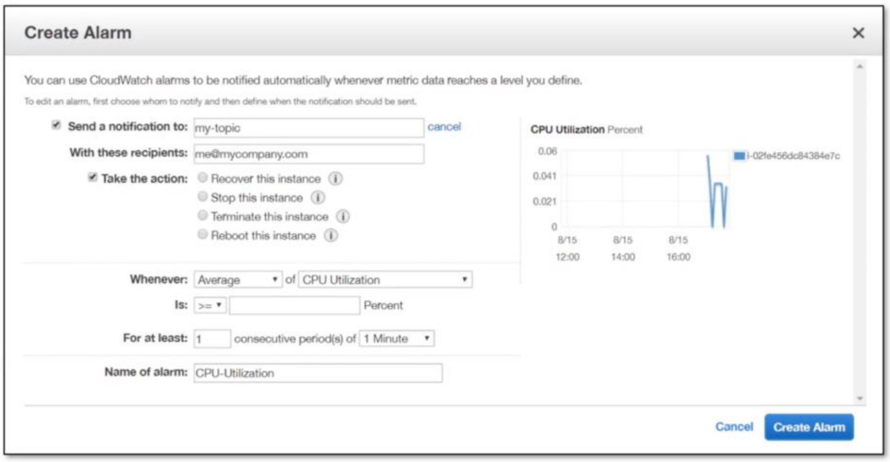
Below are your CloudWatch alarms for the selected resources. Click on an alarm to edit it or click 'view' to see additional options and details in Amazon CloudWatch.

State	Name	More Options

There are no alarms for this instance

Creating an Alarm

Either console



Create Alarm ✕

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

☑ **Send a notification to:** my-topic cancel

With these recipients: me@mycompany.com

☑ **Take the action:**
○ Recover this instance
○ Stop this instance
○ Terminate this instance
○ Reboot this instance

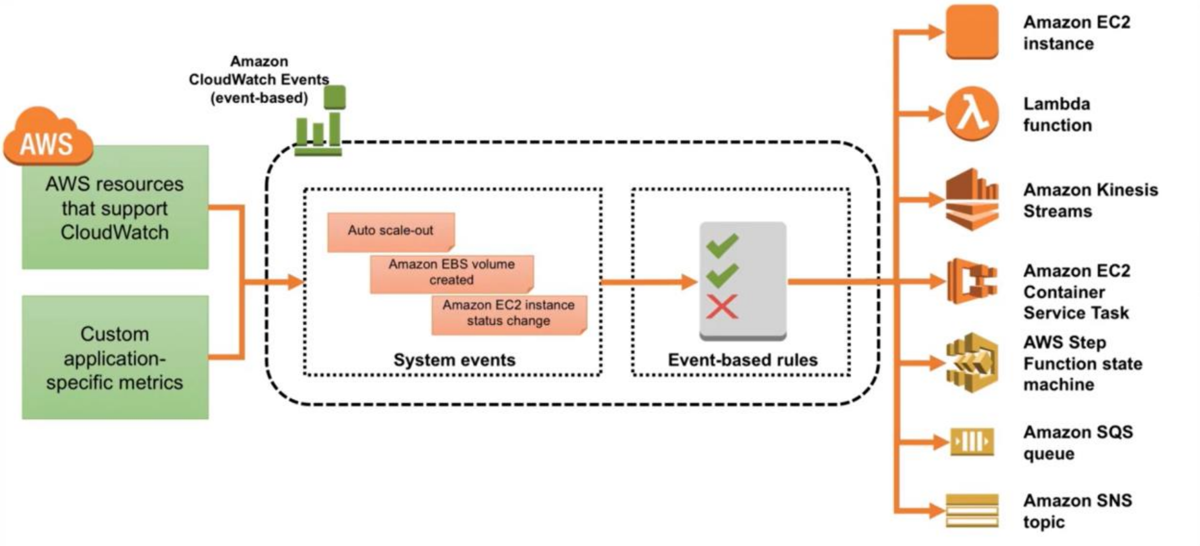
Whenever: Average of CPU Utilization

Is: >= Percent

For at least: 1 consecutive period(s) of 1 Minute

Name of alarm: CPU-Utilization

CloudWatch Event-Based Workflow



Amazon CloudWatch Events (event-based)

AWS

AWS resources that support CloudWatch

Custom application-specific metrics

Auto scale-out

Amazon EBS volume created

Amazon EC2 instance status change

System events

Event-based rules

Amazon EC2 instance

Lambda function

Amazon Kinesis Streams

Amazon EC2 Container Service Task

AWS Step Function state machine

Amazon SQS queue

Amazon SNS topic