Amazon CloudWatch: User Guide
Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.
# Table of Contents

What is Amazon CloudWatch? ................................................................. 1  
Accessing CloudWatch ........................................................................ 1  
Related AWS services ........................................................................ 1  
How CloudWatch works ..................................................................... 2  
Concepts ......................................................................................... 2  
Namespaces ...................................................................................... 3  
Metrics ............................................................................................ 3  
Dimensions ...................................................................................... 4  
Resolution ....................................................................................... 5  
Statistics ......................................................................................... 5  
Units ................................................................................................ 6  
Periods ............................................................................................ 6  
Aggregation ...................................................................................... 7  
Percentiles ...................................................................................... 7  
Alarms .............................................................................................. 7  
Resources ........................................................................................ 8  
Getting set up .................................................................................. 10  
Sign up for Amazon Web Services (AWS) ....................................... 10  
Sign in to the Amazon CloudWatch console .................................. 10  
Set up the AWS CLI ......................................................................... 10  
Getting started ............................................................................... 11  
See key metrics from all AWS services ........................................... 13  
Focus on a single service .................................................................. 14  
Focus on a resource group ............................................................... 15  
Focus on a single service .................................................................. 16  
Using dashboards ............................................................................ 17  
Create a dashboard ........................................................................... 18  
Cross-account cross-Region dashboards ....................................... 18  
Creating and using a cross-account cross-Region dashboard with the AWS Management Console .................................................... 19  
Create a cross-account cross-Region dashboard programmatically .......... 20  
Creating and working with widgets on CloudWatch dashboards ...... 21  
Add or remove a graph .................................................................. 22  
Graph metrics manually on a CloudWatch dashboard ....................... 24  
Edit a graph .................................................................................... 24  
Add a metrics explorer widget to a CloudWatch dashboard ............. 27  
Add an alarm widget to a CloudWatch dashboard ............................ 28  
Add a custom widget to a CloudWatch dashboard ......................... 29  
Add or remove a text widget ........................................................... 37  
Link and unlink graphs .................................................................. 37  
Sharing dashboards ......................................................................... 38  
Permissions required to share a dashboard ...................................... 38  
Permissions that are granted to people who you share the dashboard with ................................................................. 39  
Share a single dashboard with specific users .................................... 40  
Share a single dashboard publicly ................................................... 40  
Share all CloudWatch dashboards in the account by using SSO .......... 41  
Set up SSO for CloudWatch dashboard sharing ............................. 41  
See how many of your dashboards are shared ............................... 42  
Stop sharing one or more dashboards ............................................ 42  
Review shared dashboard permissions and change permission scope ................................................................. 43  
Allowing people that you share with to see composite alarms .......... 44  
Allowing people that you share with to see logs table widgets ........ 45  
Allowing people that you share with to see custom widgets .......... 46  

---

Amazon CloudWatch User Guide

iii
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use live data</td>
<td>47</td>
</tr>
<tr>
<td>Viewing an animated dashboard</td>
<td>47</td>
</tr>
<tr>
<td>Add a dashboard to your Favorites list</td>
<td>48</td>
</tr>
<tr>
<td>Change the period override setting or refresh interval</td>
<td>48</td>
</tr>
<tr>
<td>Change the time range or time zone format</td>
<td>49</td>
</tr>
<tr>
<td>Metrics explorer to monitor resources by their tags and properties</td>
<td>100</td>
</tr>
<tr>
<td>Using metrics</td>
<td>51</td>
</tr>
<tr>
<td>Viewing available metrics</td>
<td>51</td>
</tr>
<tr>
<td>Searching for available metrics</td>
<td>54</td>
</tr>
<tr>
<td>Getting statistics for a metric</td>
<td>55</td>
</tr>
<tr>
<td>CloudWatch statistics definitions</td>
<td>55</td>
</tr>
<tr>
<td>Getting statistics for a specific resource</td>
<td>58</td>
</tr>
<tr>
<td>Aggregating statistics across resources</td>
<td>61</td>
</tr>
<tr>
<td>Aggregating statistics by Auto Scaling group</td>
<td>63</td>
</tr>
<tr>
<td>Aggregating statistics by AMI</td>
<td>64</td>
</tr>
<tr>
<td>Graphing metrics</td>
<td>66</td>
</tr>
<tr>
<td>Graphing a metric</td>
<td>66</td>
</tr>
<tr>
<td>Using dynamic labels</td>
<td>69</td>
</tr>
<tr>
<td>Modifying the time range or time zone format for a graph</td>
<td>71</td>
</tr>
<tr>
<td>Modifying the y-axis for a graph</td>
<td>72</td>
</tr>
<tr>
<td>Creating an alarm from a metric on a graph</td>
<td>73</td>
</tr>
<tr>
<td>Publishing custom metrics</td>
<td>74</td>
</tr>
<tr>
<td>High-resolution metrics</td>
<td>74</td>
</tr>
<tr>
<td>Using dimensions</td>
<td>75</td>
</tr>
<tr>
<td>Publishing single data points</td>
<td>75</td>
</tr>
<tr>
<td>Publishing statistic sets</td>
<td>76</td>
</tr>
<tr>
<td>Publishing the value zero</td>
<td>77</td>
</tr>
<tr>
<td>Metric math</td>
<td>77</td>
</tr>
<tr>
<td>Adding a math expression to a CloudWatch graph</td>
<td>77</td>
</tr>
<tr>
<td>Metric math syntax and functions</td>
<td>78</td>
</tr>
<tr>
<td>Using IF expressions</td>
<td>88</td>
</tr>
<tr>
<td>Using search expressions in graphs</td>
<td>91</td>
</tr>
<tr>
<td>Search expression syntax</td>
<td>91</td>
</tr>
<tr>
<td>Search expression examples</td>
<td>95</td>
</tr>
<tr>
<td>Creating a graph with a search expression</td>
<td>97</td>
</tr>
<tr>
<td>Use metrics explorer to monitor resources by their tags and properties</td>
<td>100</td>
</tr>
<tr>
<td>CloudWatch agent configuration for metrics explorer</td>
<td>101</td>
</tr>
<tr>
<td>Using alarms</td>
<td>102</td>
</tr>
<tr>
<td>Metric alarm states</td>
<td>102</td>
</tr>
<tr>
<td>Evaluating an alarm</td>
<td>103</td>
</tr>
<tr>
<td>Alarm actions</td>
<td>104</td>
</tr>
<tr>
<td>Configuring how alarms treat missing data</td>
<td>104</td>
</tr>
<tr>
<td>How alarm state is evaluated when data is missing</td>
<td>105</td>
</tr>
<tr>
<td>High-resolution alarms</td>
<td>107</td>
</tr>
<tr>
<td>Alarms on math expressions</td>
<td>107</td>
</tr>
<tr>
<td>Percentile-based alarms and low data samples</td>
<td>108</td>
</tr>
<tr>
<td>Common features of CloudWatch alarms</td>
<td>108</td>
</tr>
<tr>
<td>Setting up an SNS topic</td>
<td>109</td>
</tr>
<tr>
<td>Setting up an Amazon SNS topic using the AWS Management Console</td>
<td>109</td>
</tr>
<tr>
<td>Setting up an SNS topic using the AWS CLI</td>
<td>110</td>
</tr>
<tr>
<td>Create an alarm based on a static threshold</td>
<td>111</td>
</tr>
<tr>
<td>Creating an alarm based on anomaly detection</td>
<td>112</td>
</tr>
<tr>
<td>Modifying an anomaly detection model</td>
<td>114</td>
</tr>
<tr>
<td>Deleting an anomaly detection model</td>
<td>115</td>
</tr>
<tr>
<td>Creating an alarm based on a metric math expression</td>
<td>115</td>
</tr>
<tr>
<td>Creating a composite alarm</td>
<td>117</td>
</tr>
<tr>
<td>Editing or deleting a CloudWatch alarm</td>
<td>119</td>
</tr>
<tr>
<td>Creating a CPU usage alarm</td>
<td>120</td>
</tr>
</tbody>
</table>
Using Container Insights

Cross-account cross-Region CloudWatch console

Using ServiceLens to monitor the health of your applications

Deploying ServiceLens

Using the service map

Using the traces view

Using the resource health view

Prerequisites

ServiceLens troubleshooting

I don't see all my logs

I don't see all my alarms on the service map

I don't see some AWS resources on the service map

There are too many nodes on my service map

Using anomaly detection

How anomaly detection works

Using Contributor Insights to analyze high-cardinality data

Creating a Contributor Insights rule

Contributor Insights rule syntax

Example rules

Viewing Contributor Insights reports

Graphing metrics generated by rules

Setting an alarm on Contributor Insights metric data

Using Contributor Insights built-in rules

Using Container Insights

Supported platforms

CloudWatch agent container image

Supported Regions

Setting up Container Insights

Setting up Container Insights on Amazon ECS

Setting up Container Insights on Amazon EKS and Kubernetes

Viewing Container Insights metrics

Viewing the top contributors

Using CloudWatch Logs Insights to view Container Insights data

Use case: Seeing task-level metrics in Amazon ECS containers

Other sample queries for Container Insights

Metrics collected by Container Insights

Amazon ECS Container Insights metrics

Amazon EKS and Kubernetes Container Insights metrics

Performance log reference

Performance log events for Amazon ECS

Performance log events for Amazon EKS and Kubernetes

Relevant fields in performance log events for Amazon EKS and Kubernetes

Container Insights Prometheus metrics monitoring

Set up and configure on Amazon ECS clusters

Set up and configure on Amazon EKS and Kubernetes clusters

Troubleshooting Container Insights
Detect common application problems with CloudWatch Application Insights .................................................. 546
Supported logs and metrics .............................................................................................................................. 615
View and troubleshoot Application Insights .................................................................................................. 613
Work with component configurations ........................................................................................................... 573
How Application Insights works ..................................................................................................................... 551
What is Amazon CloudWatch Application Insights? ....................................................................................... 546
Features ......................................................................................................................................................... 547
Concepts ....................................................................................................................................................... 547
Pricing ......................................................................................................................................................... 548
Related services .......................................................................................................................................... 548
Supported application components ............................................................................................................... 550
Supported technology stacks .......................................................................................................................... 550
Get started .................................................................................................................................................... 555
How Application Insights monitors applications .......................................................................................... 551
Data retention .................................................................................................................................................. 552
Quotas .......................................................................................................................................................... 552
SSM packages used by Application Insights .................................................................................................... 552
Set up, configure, and manage your application ............................................................................................. 557
Work with component configurations ........................................................................................................... 573
Template fragment ........................................................................................................................................ 573
Sections .......................................................................................................................................................... 574
Example configurations for relevant services ................................................................................................ 578
Use CloudFormation templates ........................................................................................................................ 599
Create an Application Insights application for the entire AWS CloudFormation stack ................................ 600
Create an Application Insights application with detailed settings ................................................................. 601
Create an Application Insights application with CUSTOM mode component configuration .................... 603
Create an Application Insights application with DEFAULT mode component configuration .................. 606
Create an Application Insights application with DEFAULT_WITH_OVERWRITE mode component configuration ........................................................................................................... 607
Tutorial: Set up monitors for .NET and SQL .................................................................................................... 608
Use case scenario .......................................................................................................................................... 608
Prerequisites .................................................................................................................................................. 609
Deploy resources .......................................................................................................................................... 609
Set up monitoring with Amazon CloudWatch Application Insights ............................................................... 610
Simulate problem scenarios and view insights ................................................................................................. 611
View and troubleshoot Application Insights .................................................................................................. 613
Configuration errors ....................................................................................................................................... 613
Supported logs and metrics ............................................................................................................................. 615
Amazon Elastic Compute Cloud (EC2) ............................................................................................................ 616
Elastic Block Store (EBS) ................................................................................................................................. 622
Amazon CloudWatch User Guide

Elastic Load Balancer (ELB) ................................................................. 622
Application ELB ........................................................................... 623
Amazon EC2 Auto Scaling groups ............................................... 623
Amazon Simple Queue Server (SQS) ........................................ 624
Amazon Relational Database Service (RDS) ............................... 624
AWS Lambda function ............................................................... 626
Amazon DynamoDB table .......................................................... 626
Amazon S3 bucket ...................................................................... 627
AWS Step Functions .................................................................. 627
API Gateway REST API stages .................................................. 629
Java ......................................................................................... 629
Amazon Elastic Container Service (Amazon ECS) ........................ 630
Kubernetes on AWS .................................................................... 631
Metrics with datapoints requirements ....................................... 633
Recommended metrics .............................................................. 640
Performance Counter metrics ..................................................... 653
Services that publish CloudWatch metrics ................................. 658
Alarm events and EventBridge ..................................................... 664
Sample events from CloudWatch ................................................. 664
Ingesting high-cardinality logs and generating metrics with CloudWatch embedded metric format .... 668
Generating logs using the embedded metric format ....................... 668
Using the client libraries ............................................................ 669
Using the embedded metric format with AWS Distro for OpenTelemetry ............... 669
Manually generating embedded metric format logs ....................... 669
Viewing your metrics and logs in the console ......................... 681
AWS usage metrics ..................................................................... 683
Visualizing your service quotas and setting alarms ...................... 683
AWS API usage metrics ............................................................. 684
CloudWatch usage metrics ......................................................... 688
CloudWatch tutorials ................................................................. 689
Scenario: Monitor estimated charges ......................................... 689
Step 1: Enable billing alerts ......................................................... 689
Step 2: Create a billing alarm ....................................................... 690
Step 3: Check the alarm status ...................................................... 691
Step 4: Edit a billing alarm .......................................................... 691
Step 5: Delete a billing alarm ....................................................... 691
Scenario: Publish metrics ............................................................ 691
Step 1: Define the data configuration ........................................... 692
Step 2: Add metrics to CloudWatch ........................................... 692
Step 3: Get statistics from CloudWatch ...................................... 693
Step 4: View graphs with the console ......................................... 693
Tagging your CloudWatch resources ........................................... 694
Supported resources in CloudWatch .......................................... 694
Managing tags ............................................................................. 694
Tag naming and usage conventions ............................................ 695
Security ........................................................................................ 696
Data protection ............................................................................. 696
Encryption in transit ................................................................. 697
Identity and access management ................................................ 697
Authentication ............................................................................ 697
Access control ............................................................................. 698
CloudWatch dashboard permissions update ............................... 699
Overview of managing access .................................................... 699
Using identity-based policies (IAM policies) ............................... 702
Using condition keys to limit access to CloudWatch namespaces .... 714
Using condition keys to limit Contributor Insights users' access to log groups ........ 715
Using condition keys to limit alarm actions ................................. 716
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance validation</td>
<td>736</td>
</tr>
<tr>
<td>Resilience</td>
<td>736</td>
</tr>
<tr>
<td>Infrastructure security</td>
<td>737</td>
</tr>
<tr>
<td>Network isolation</td>
<td>737</td>
</tr>
<tr>
<td>Interface VPC endpoints</td>
<td>737</td>
</tr>
<tr>
<td>CloudWatch</td>
<td>738</td>
</tr>
<tr>
<td>CloudWatch Synthetics</td>
<td>739</td>
</tr>
<tr>
<td>Security considerations for Synthetics canaries</td>
<td>741</td>
</tr>
<tr>
<td>Use secure connections</td>
<td>741</td>
</tr>
<tr>
<td>Canary naming considerations</td>
<td>741</td>
</tr>
<tr>
<td>Secrets in canary code</td>
<td>741</td>
</tr>
<tr>
<td>Permissions considerations</td>
<td>741</td>
</tr>
<tr>
<td>Stack traces and exception messages</td>
<td>741</td>
</tr>
<tr>
<td>Scope your IAM roles narrowly</td>
<td>742</td>
</tr>
<tr>
<td>Sensitive data redaction</td>
<td>742</td>
</tr>
<tr>
<td>Logging API calls with AWS CloudTrail</td>
<td>744</td>
</tr>
<tr>
<td>CloudWatch information in CloudTrail</td>
<td>744</td>
</tr>
<tr>
<td>Example: CloudWatch log file entries</td>
<td>745</td>
</tr>
<tr>
<td>CloudWatch Synthetics information in CloudTrail</td>
<td>747</td>
</tr>
<tr>
<td>Example: CloudWatch Synthetics log file entries</td>
<td>747</td>
</tr>
<tr>
<td>Grafana integration</td>
<td>750</td>
</tr>
<tr>
<td>Service quotas</td>
<td>751</td>
</tr>
<tr>
<td>Document history</td>
<td>754</td>
</tr>
</tbody>
</table>
What is Amazon CloudWatch?

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 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 that 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.

Accessing CloudWatch

You can access CloudWatch using any of the following methods:

- **Amazon CloudWatch console** – https://console.aws.amazon.com/cloudwatch/
- **AWS CLI** – For more information, see Getting Set Up with the AWS Command Line Interface in the AWS Command Line Interface User Guide.
- **CloudWatch API** – For more information, see the Amazon CloudWatch API Reference.
- **AWS SDKs** – For more information, see Tools for Amazon Web Services.

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 Setting up Amazon SNS notifications (p. 109).
- **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 (p. 744).
- **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 Identity and access management for Amazon CloudWatch (p. 697).
Amazon CloudWatch User Guide
How Amazon CloudWatch works

How Amazon CloudWatch works

Amazon CloudWatch is basically a metrics repository. An AWS service—such as Amazon EC2—puts metrics into the repository, and you retrieve statistics based on those metrics. If you put your own custom metrics into the repository, you can retrieve statistics on these metrics as well.

You can use metrics to calculate statistics and then present the data graphically in the CloudWatch console. For more information about the other AWS resources that generate and send metrics to CloudWatch, see AWS services that publish CloudWatch metrics (p. 658).

You can configure alarm actions to stop, start, or terminate an Amazon EC2 instance when certain criteria are met. In addition, you can create alarms that initiate Amazon EC2 Auto Scaling and Amazon Simple Notification Service (Amazon SNS) actions on your behalf. For more information about creating CloudWatch alarms, see Alarms (p. 8).

AWS Cloud computing resources are housed in highly available data center facilities. To provide additional scalability and reliability, each data center facility is located in a specific geographical area, known as a Region. Each Region is designed to be completely isolated from the other Regions, to achieve the greatest possible failure isolation and stability. Metrics are stored separately in Regions, but you can use CloudWatch cross-Region functionality to aggregate statistics from different Regions. For more information, see Cross-account cross-Region CloudWatch console (p. 242) and Regions and Endpoints in the Amazon Web Services General Reference.

Amazon CloudWatch concepts

The following terminology and concepts are central to your understanding and use of Amazon CloudWatch:

- Namespaces (p. 3)
Namespaces

A namespace is a container for CloudWatch metrics. Metrics in different namespaces are isolated from each other, so that metrics from different applications are not mistakenly aggregated into the same statistics.

There is no default namespace. You must specify a namespace for each data point you publish to CloudWatch. You can specify a namespace when you create a metric. These names must contain valid XML characters, and be fewer than 256 characters in length. Possible characters are: alphanumeric characters (0-9A-Za-z), period (.), hyphen (-), underscore (_), forward slash (/), hash (#), and colon (:).

The AWS namespaces typically use the following naming convention: `aws/service`. For example, Amazon EC2 uses the `aws/EC2` namespace. For the list of AWS namespaces, see AWS services that publish CloudWatch metrics (p. 658).

Metrics

Metrics are the fundamental concept in CloudWatch. A metric represents a time-ordered set of data points that are published to CloudWatch. Think of a metric as a variable to monitor, and the data points as representing the values of that variable over time. For example, the CPU usage of a particular EC2 instance is one metric provided by Amazon EC2. The data points themselves can come from any application or business activity from which you collect data.

By default, many AWS services provide free metrics for resources (such as Amazon EC2 instances, Amazon EBS volumes, and Amazon RDS DB instances). For a charge, you can also enable detailed monitoring for some resources, such as your Amazon EC2 instances, or publish your own application metrics. For custom metrics, you can add the data points in any order, and at any rate you choose. You can retrieve statistics about those data points as an ordered set of time-series data.

Metrics exist only in the Region in which they are created. Metrics cannot be deleted, but they automatically expire after 15 months if no new data is published to them. Data points older than 15 months expire on a rolling basis; as new data points come in, data older than 15 months is dropped.

Metrics are uniquely defined by a name, a namespace, and zero or more dimensions. Each data point in a metric has a time stamp, and (optionally) a unit of measure. You can retrieve statistics from CloudWatch for any metric.

For more information, see Viewing available metrics (p. 51) and Publishing custom metrics (p. 74).

Time stamps

Each metric data point must be associated with a time stamp. The time stamp can be up to two weeks in the past and up to two hours into the future. If you do not provide a time stamp, CloudWatch creates a time stamp for you based on the time the data point was received.

Time stamps are `dateTime` objects, with the complete date plus hours, minutes, and seconds (for example, 2016-10-31T23:59:59Z). For more information, see `dateTime`. Although it is not required,
we recommend that you use Coordinated Universal Time (UTC). When you retrieve statistics from CloudWatch, all times are in UTC.

CloudWatch alarms check metrics based on the current time in UTC. Custom metrics sent to CloudWatch with time stamps other than the current UTC time can cause alarms to display the Insufficient Data state or result in delayed alarms.

**Metrics retention**

CloudWatch retains metric data as follows:

- Data points with a period of less than 60 seconds are available for 3 hours. These data points are high-resolution custom metrics.
- Data points with a period of 60 seconds (1 minute) are available for 15 days
- Data points with a period of 300 seconds (5 minute) are available for 63 days
- Data points with a period of 3600 seconds (1 hour) are available for 455 days (15 months)

Data points that are initially published with a shorter period are aggregated together for long-term storage. For example, if you collect data using a period of 1 minute, the data remains available for 15 days with 1-minute resolution. After 15 days this data is still available, but is aggregated and is retrievable only with a resolution of 5 minutes. After 63 days, the data is further aggregated and is available with a resolution of 1 hour.

**Note**

Metrics that have not had any new data points in the past two weeks do not appear in the console. They also do not appear when you type their metric name or dimension names in the search box in the All metrics tab in the console, and they are not returned in the results of a list-metrics command. The best way to retrieve these metrics is with the get-metric-data or get-metric-statistics commands in the AWS CLI.

**Dimensions**

A dimension is a name/value pair that is part of the identity of a metric. You can assign up to 10 dimensions to a metric.

Every metric has specific characteristics that describe it, and you can think of dimensions as categories for those characteristics. Dimensions help you design a structure for your statistics plan. Because dimensions are part of the unique identifier for a metric, whenever you add a unique name/value pair to one of your metrics, you are creating a new variation of that metric.

AWS services that send data to CloudWatch attach dimensions to each metric. You can use dimensions to filter the results that CloudWatch returns. For example, you can get statistics for a specific EC2 instance by specifying the InstanceId dimension when you search for metrics.

For metrics produced by certain AWS services, such as Amazon EC2, CloudWatch can aggregate data across dimensions. For example, if you search for metrics in the AWS/EC2 namespace but do not specify any dimensions, CloudWatch aggregates all data for the specified metric to create the statistic that you requested. CloudWatch does not aggregate across dimensions for your custom metrics.

**Dimension combinations**

CloudWatch treats each unique combination of dimensions as a separate metric, even if the metrics have the same metric name. You can only retrieve statistics using combinations of dimensions that you specifically published. When you retrieve statistics, specify the same values for the namespace, metric name, and dimension parameters that were used when the metrics were created. You can also specify the start and end times for CloudWatch to use for aggregation.
For example, suppose that you publish four distinct metrics named ServerStats in the DataCenterMetric namespace with the following properties:

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Value</th>
<th>Timestamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server=Prod, Domain=Frankfurt, Unit: Count</td>
<td>105</td>
<td>2016-10-31T12:30:00Z</td>
</tr>
<tr>
<td>Server=Beta, Domain=Frankfurt, Unit: Count</td>
<td>115</td>
<td>2016-10-31T12:31:00Z</td>
</tr>
<tr>
<td>Server=Prod, Domain=Rio, Unit: Count</td>
<td>95</td>
<td>2016-10-31T12:32:00Z</td>
</tr>
<tr>
<td>Server=Beta, Domain=Rio, Unit: Count</td>
<td>97</td>
<td>2016-10-31T12:33:00Z</td>
</tr>
</tbody>
</table>

If you publish only those four metrics, you can retrieve statistics for these combinations of dimensions:

- Server=Prod, Domain=Frankfurt
- Server=Prod, Domain=Rio
- Server=Beta, Domain=Frankfurt
- Server=Beta, Domain=Rio

You can't retrieve statistics for the following dimensions or if you specify no dimensions. (The exception is by using the metric math SEARCH function, which can retrieve statistics for multiple metrics. For more information, see Using search expressions in graphs (p. 91).)

- Server=Prod
- Server=Beta
- Domain=Frankfurt
- Domain=Rio

**Resolution**

Each metric is one of the following:

- Standard resolution, with data having a one-minute granularity
- High resolution, with data at a granularity of one second

Metrics produced by AWS services are standard resolution by default. When you publish a custom metric, you can define it as either standard resolution or high resolution. When you publish a high-resolution metric, CloudWatch stores it with a resolution of 1 second, and you can read and retrieve it with a period of 1 second, 5 seconds, 10 seconds, 30 seconds, or any multiple of 60 seconds.

High-resolution metrics can give you more immediate insight into your application's sub-minute activity. Keep in mind that every PutMetricData call for a custom metric is charged, so calling PutMetricData more often on a high-resolution metric can lead to higher charges. For more information about CloudWatch pricing, see Amazon CloudWatch Pricing.

If you set an alarm on a high-resolution metric, you can specify a high-resolution alarm with a period of 10 seconds or 30 seconds, or you can set a regular alarm with a period of any multiple of 60 seconds. There is a higher charge for high-resolution alarms with a period of 10 or 30 seconds.

**Statistics**

Statistics are metric data aggregations over specified periods of time. CloudWatch provides statistics based on the metric data points provided by your custom data or provided by other AWS services to
CloudWatch. Aggregations are made using the namespace, metric name, dimensions, and the data point unit of measure, within the time period you specify.

For detailed definitions of the statistics supported by CloudWatch, see CloudWatch statistics definitions (p. 55).

Units

Each statistic has a unit of measure. Example units include Bytes, Seconds, Count, and Percent. For the complete list of the units that CloudWatch supports, see the MetricDatum data type in the Amazon CloudWatch API Reference.

You can specify a unit when you create a custom metric. If you do not specify a unit, CloudWatch uses None as the unit. Units help provide conceptual meaning to your data. Though CloudWatch attaches no significance to a unit internally, other applications can derive semantic information based on the unit.

Metric data points that specify a unit of measure are aggregated separately. When you get statistics without specifying a unit, CloudWatch aggregates all data points of the same unit together. If you have two otherwise identical metrics with different units, two separate data streams are returned, one for each unit.

Periods

A period is the length of time associated with a specific Amazon CloudWatch statistic. Each statistic represents an aggregation of the metrics data collected for a specified period of time. Periods are defined in numbers of seconds, and valid values for period are 1, 5, 10, 30, or any multiple of 60. For example, to specify a period of six minutes, use 360 as the period value. You can adjust how the data is aggregated by varying the length of the period. A period can be as short as one second or as long as one day (86,400 seconds). The default value is 60 seconds.

Only custom metrics that you define with a storage resolution of 1 second support sub-minute periods. Even though the option to set a period below 60 is always available in the console, you should select a period that aligns to how the metric is stored. For more information about metrics that support sub-minute periods, see High-resolution metrics (p. 74).

When you retrieve statistics, you can specify a period, start time, and end time. These parameters determine the overall length of time associated with the statistics. The default values for the start time and end time get you the last hour's worth of statistics. The values that you specify for the start time and end time determine how many periods CloudWatch returns. For example, retrieving statistics using the default values for the period, start time, and end time returns an aggregated set of statistics for each minute of the previous hour. If you prefer statistics aggregated in ten-minute blocks, specify a period of 600. For statistics aggregated over the entire hour, specify a period of 3600.

When statistics are aggregated over a period of time, they are stamped with the time corresponding to the beginning of the period. For example, data aggregated from 7:00pm to 8:00pm is stamped as 7:00pm. Additionally, data aggregated between 7:00pm and 8:00pm begins to be visible at 7:00pm, then the values of that aggregated data may change as CloudWatch collects more samples during the period.

Periods are also important for CloudWatch alarms. When you create an alarm to monitor a specific metric, you are asking CloudWatch to compare that metric to the threshold value that you specified. You have extensive control over how CloudWatch makes that comparison. Not only can you specify the period over which the comparison is made, but you can also specify how many evaluation periods are used to arrive at a conclusion. For example, if you specify three evaluation periods, CloudWatch compares a window of three data points. CloudWatch only notifies you if the oldest data point is breaching and the others are breaching or missing. For metrics that are continuously emitted, CloudWatch doesn't notify you until three failures are found.
Aggregation

Amazon CloudWatch aggregates statistics according to the period length that you specify when retrieving statistics. You can publish as many data points as you want with the same or similar time stamps. CloudWatch aggregates them according to the specified period length. CloudWatch does not automatically aggregate data across Regions, but you can use metric math to aggregate metrics from different Regions.

You can publish data points for a metric that share not only the same time stamp, but also the same namespace and dimensions. CloudWatch returns aggregated statistics for those data points. You can also publish multiple data points for the same or different metrics, with any time stamp.

For large datasets, you can insert a pre-aggregated dataset called a statistic set. With statistic sets, you give CloudWatch the Min, Max, Sum, and SampleCount for a number of data points. This is commonly used when you need to collect data many times in a minute. For example, suppose you have a metric for the request latency of a webpage. It doesn't make sense to publish data with every webpage hit. We suggest that you collect the latency of all hits to that webpage, aggregate them once a minute, and send that statistic set to CloudWatch.

Amazon CloudWatch doesn't differentiate the source of a metric. If you publish a metric with the same namespace and dimensions from different sources, CloudWatch treats this as a single metric. This can be useful for service metrics in a distributed, scaled system. For example, all the hosts in a web server application could publish identical metrics representing the latency of requests they are processing. CloudWatch treats these as a single metric, allowing you to get the statistics for minimum, maximum, average, and sum of all requests across your application.

Percentiles

A percentile indicates the relative standing of a value in a dataset. For example, the 95th percentile means that 95 percent of the data is lower than this value and 5 percent of the data is higher than this value. Percentiles help you get a better understanding of the distribution of your metric data.

Percentiles are often used to isolate anomalies. In a typical distribution, 95 percent of the data is within two standard deviations from the mean and 99.7 percent of the data is within three standard deviations from the mean. Any data that falls outside three standard deviations is often considered to be an anomaly because it differs so greatly from the average value. For example, suppose that you are monitoring the CPU utilization of your EC2 instances to ensure that your customers have a good experience. If you monitor the average, this can hide anomalies. If you monitor the maximum, a single anomaly can skew the results. Using percentiles, you can monitor the 95th percentile of CPU utilization to check for instances with an unusually heavy load.

Some CloudWatch metrics support percentiles as a statistic. For these metrics, you can monitor your system and applications using percentiles as you would when using the other CloudWatch statistics (Average, Minimum, Maximum, and Sum). For example, when you create an alarm, you can use percentiles as the statistical function. You can specify the percentile with up to ten decimal places (for example, p95.0123456789).

Percentile statistics are available for custom metrics as long as you publish the raw, unsummarized data points for your custom metric. Percentile statistics are not available for metrics when any of the metric values are negative numbers.

CloudWatch needs raw data points to calculate percentiles. If you publish data using a statistic set instead, you can only retrieve percentile statistics for this data if one of the following conditions is true:

- The SampleCount value of the statistic set is 1 and Min, Max, and Sum are all equal.
- The Min and Max are equal, and Sum is equal to Min multiplied by SampleCount.
The following AWS services include metrics that support percentile statistics.

- API Gateway
- Application Load Balancer
- Amazon EC2
- Elastic Load Balancing
- Kinesis
- Amazon RDS

CloudWatch also supports trimmed mean and other performance statistics, which can have a similar use as percentiles. For more information, see CloudWatch statistics definitions (p. 55).

**Alarms**

You can use an *alarm* to automatically initiate actions on your behalf. An alarm watches a single metric over a specified time period, and performs one or more specified actions, based on the value of the metric relative to a threshold over time. The action is a notification sent to an Amazon SNS topic or an Auto Scaling policy. You can also add alarms to dashboards.

Alarms invoke actions for sustained state changes only. CloudWatch alarms do not invoke actions simply because they are in a particular state. The state must have changed and been maintained for a specified number of periods.

When creating an alarm, select an alarm monitoring period that is greater than or equal to the metric's resolution. For example, basic monitoring for Amazon EC2 provides metrics for your instances every 5 minutes. When setting an alarm on a basic monitoring metric, select a period of at least 300 seconds (5 minutes). Detailed monitoring for Amazon EC2 provides metrics for your instances with a resolution of 1 minute. When setting an alarm on a detailed monitoring metric, select a period of at least 60 seconds (1 minute).

If you set an alarm on a high-resolution metric, you can specify a high-resolution alarm with a period of 10 seconds or 30 seconds, or you can set a regular alarm with a period of any multiple of 60 seconds. There is a higher charge for high-resolution alarms. For more information about high-resolution metrics, see Publishing custom metrics (p. 74).

For more information, see Using Amazon CloudWatch alarms (p. 102) and Creating an alarm from a metric on a graph (p. 73).

**Amazon CloudWatch resources**

The following related resources can help you as you work with this service.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon CloudWatch FAQs</td>
<td>The FAQ covers the top questions developers have asked about this product.</td>
</tr>
<tr>
<td>AWS Developer Center</td>
<td>A central starting point to find documentation, code examples, release notes, and other information to help you build innovative applications with AWS.</td>
</tr>
<tr>
<td>AWS Management Console</td>
<td>The console allows you to perform most of the functions of Amazon CloudWatch and various other AWS offerings without programming.</td>
</tr>
<tr>
<td>Resource</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Amazon CloudWatch Discussion Forums</td>
<td>Community-based forum for developers to discuss technical questions related to Amazon CloudWatch.</td>
</tr>
<tr>
<td>AWS Support</td>
<td>The hub for creating and managing your AWS Support cases. Also includes links to other helpful resources, such as forums, technical FAQs, service health status, and AWS Trusted Advisor.</td>
</tr>
<tr>
<td>Amazon CloudWatch product information</td>
<td>The primary webpage for information about Amazon CloudWatch.</td>
</tr>
<tr>
<td>Contact Us</td>
<td>A central contact point for inquiries concerning AWS billing, account, events, abuse, etc.</td>
</tr>
</tbody>
</table>
Getting set up

To use Amazon CloudWatch you need an AWS account. Your AWS account allows you to use services (for example, Amazon EC2) to generate metrics that you can view in the CloudWatch console, a point-and-click web-based interface. In addition, you can install and configure the AWS command line interface (CLI).

Sign up for Amazon Web Services (AWS)

When you create an AWS account, we automatically sign up your account for all AWS services. You pay only for the services that you use.

If you have an account already, skip to the next step. If you don't have an account, use the following procedure to create one.

To sign up for an AWS account
2. Follow the online instructions.
   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

Sign in to the Amazon CloudWatch console

To sign in to the Amazon CloudWatch console
2. If necessary, use the navigation bar to change the Region to the Region where you have your AWS resources.
3. Even if this is the first time you are using the CloudWatch console, Your Metrics could already report metrics, because you have used an AWS product that automatically pushes metrics to Amazon CloudWatch for free. Other services require that you enable metrics.
   If you do not have any alarms, the Your Alarms section will have a Create Alarm button.

Set up the AWS CLI

You can use the AWS CLI or the Amazon CloudWatch CLI to perform CloudWatch commands. Note that the AWS CLI replaces the CloudWatch CLI; we include new CloudWatch features only in the AWS CLI.

For information about how to install and configure the AWS CLI, see Getting Set up with the AWS Command Line Interface in the AWS Command Line Interface User Guide.

For information about how to install and configure the Amazon CloudWatch CLI, see Set Up the Command Line Interface in the Amazon CloudWatch CLI Reference.
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 default dashboard, if one exists. The default dashboard is a custom dashboard that you have created and named CloudWatch-Default. 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. For more information, see What Is AWS Resource Groups?.

Topics

- See key metrics from all AWS services (p. 13)
- Focus on metrics and alarms in a single AWS service (p. 15)
- Focus on metrics and alarms in a resource group (p. 16)

See key metrics from all AWS services

If you use six or more AWS services, the cross-service dashboard is not displayed on the overview page. You can switch to this dashboard to see key metrics from all the AWS services that you are using.

To open the cross-service dashboard


   The overview appears.

2. Near the bottom of the page, choose View cross service dashboard.

   The cross-service dashboard appears, showing each AWS service you are using, displayed in alphabetical order. For each service, one or two key metrics are displayed.

3. You can focus on a particular service in two ways:

   a. To see more key metrics for a service, choose its name from the list at the top of the screen, where Cross service dashboard is currently shown. Or, you can choose View Service dashboard next to the service name.
An automatic dashboard for that service is displayed, showing more metrics for that service. Additionally, for some services, the bottom of the service dashboard displays resources related to that service. You can choose one of those resources to that service console and focus further on that resource.

b. To see all the alarms related to a service, choose the button on the right of the screen next to that service name. The text on this button indicates how many alarms you have created in this service, and whether any are in the ALARM state.

When the alarms are displayed, multiple alarms that have similar settings (such as dimensions, threshold, or period) may be shown in a single graph.

You can then view details about an alarm and see the alarm history. To do so, hover on the alarm graph, and choose the actions icon, View in alarms.

The alarms view appears in a new browser tab, displaying a list of your alarms, along with details about the chosen alarm. To see the history for this alarm, choose the History tab.

4. You can focus on resources in a particular resource group. To do so, choose the resource group from the list at the top of the page where All resources is displayed.

For more information, see Focus on metrics and alarms in a resource group (p. 16).

5. To change the time range shown in all graphs and alarms currently displayed, select the range you want next to Time range at the top of the screen. Choose custom to select from more time range options than those displayed by default.

6. Alarms are always refreshed once a minute. To refresh the view, choose the refresh icon (two curved arrows) at the top right of the screen. To change the automatic refresh rate for items on the screen other than alarms, choose the down arrow next to the refresh icon and choose the refresh rate you want. You can also choose to turn off automatic refresh.

Remove a service from appearing in the cross-service dashboard

You can prevent a service's metrics from appearing in the cross-service dashboard. This helps you focus your cross-service dashboard on the services you most want to monitor.

If you remove a service from the cross-service dashboard, the alarms for that service still appear in the views of your alarms.

To remove a service's metrics from the cross-service dashboard


   The home page appears.

2. At the top of the page, under Overview, choose the service you want to remove.

   The view changes to show metrics from only that service.

3. Choose Actions, then clear the check box next to Show on cross service dashboard.
Focus on metrics and alarms in a single AWS service

On the CloudWatch home page, you can focus the view to a single AWS service. You can drill down further by focusing on both a single AWS service and a resource group at the same time. The following procedure shows only how to focus on an AWS service.

To focus on a single service


   The home page appears.

2. Choose the service name from the list at the top of the screen, where Overview is currently shown.

   The view changes to display graphs of key metrics from the selected service.

3. To switch to viewing the alarms for this service, choose Alarms dashboard at the top of the screen where Service dashboard is currently displayed.

4. When viewing metrics, you can focus on a particular metric in several ways:

   a. To see more details about the metrics in any graph, hover on the graph, and choose the actions icon, View in metrics.

      The graph appears in a new tab, with the relevant metrics listed below the graph. You can customize your view of this graph, changing the metrics and resources shown, the statistic, the period, and other factors to get a better understanding of the current situation.

   b. You can view log events from the time range shown in the graph. This may help you discover events that happened in your infrastructure that are causing an unexpected change in your metrics.

      To see the log events, hover on the graph, and choose the actions icon, View in logs.

      The CloudWatch Logs view appears in a new tab, displaying a list of your log groups. To see the log events in one of these log groups that occurred during the time range shown in the original graph, choose that log group.

5. When viewing alarms, you can focus on a particular alarm in several ways:

   • To see more details about an alarm, hover on the alarm, and choose the actions icon, View in alarms.

      The alarms view appears in a new tab, displaying a list of your alarms, along with details about the chosen alarm. To see the history for this alarm, choose the History tab.

6. Alarms are always refreshed one time per minute. To refresh the view, choose the refresh icon (two curved arrows) at the top right of the screen. To change the automatic refresh rate for items on the screen other than alarms, choose the down arrow next to the refresh icon and choose a refresh rate. You can also choose to turn off automatic refresh.

7. To change the time range shown in all graphs and alarms currently displayed, next to Time range at the top of the screen, choose the range. To select from more time range options than those displayed by default, choose custom.

8. To return to the cross-service dashboard, choose Overview in the list at the top of the screen that currently shows the service you are focusing on.

   Alternatively, from any view, you can choose CloudWatch at the top of the screen to clear all filters and return to the overview page.
Focus on metrics and alarms in a resource group

You can focus your view to display metrics and alarms from a single resource group. Using resource groups enables you to use tags to organize projects, focus on a subset of your architecture, or distinguish between your production and development environments. They also enable you to focus on each of these resource groups on the CloudWatch overview. For more information, see What Is AWS Resource Groups?

When you focus on a resource group, the display changes to show only the services where you have tagged resources as part of this resource group. The recent alarms area shows only the alarms that are associated with resources that are part of the resource group. Additionally, if you have created a dashboard with the name CloudWatch-Default-ResourceGroupName, it is displayed in the Default dashboard area.

You can drill down further by focusing on both a single AWS service and a resource group at the same time. The following procedure shows just how to focus on a resource group.

To focus on a single resource group

2. At the top of the page, where All resources is displayed, choose a resource group.
3. To see more metrics related to this resource group, near the bottom of the screen, choose View cross service dashboard.

   The cross-service dashboard appears, showing only the services related to this resource group. For each service, one or two key metrics are displayed.
4. To change the time range shown in all graphs and alarms currently displayed, for Time range at the top of the screen, select a range. To select from more time range options than those displayed by default, choose custom.
5. Alarms are always refreshed one time per minute. To refresh the view, choose the refresh icon (two curved arrows) at the top right of the screen. To change the automatic refresh rate for items on the screen other than alarms, choose the down arrow next to the refresh icon and choose a refresh rate. You can also choose to turn off automatic refresh.
6. To return to showing information about all the resources in your account, near the top of the screen where the name of the resource group is currently displayed, choose All resources.
Using Amazon CloudWatch dashboards

Amazon CloudWatch dashboards are customizable home pages in the CloudWatch console that you can use to monitor your resources in a single view, even those resources that are spread across different Regions. You can use CloudWatch dashboards to create customized views of the metrics and alarms for your AWS resources.

With dashboards, you can create the following:

- A single view for selected metrics and alarms to help you assess the health of your resources and applications across one or more Regions. You can select the color used for each metric on each graph, so that you can easily track the same metric across multiple graphs.

You can create dashboards that display graphs and other widgets from multiple AWS accounts and multiple Regions. For more information, see Cross-account cross-Region CloudWatch console (p. 242).

- An operational playbook that provides guidance for team members during operational events about how to respond to specific incidents.

- A common view of critical resource and application measurements that can be shared by team members for faster communication flow during operational events.

You can create dashboards by using the console, the AWS CLI, or the PutDashboard API.

To access CloudWatch dashboards, you need one of the following:

- The AdministratorAccess policy
- The CloudWatchFullAccess policy
- A custom policy that includes one or more of these specific permissions:
  - cloudwatch:GetDashboard and cloudwatch:ListDashboards to be able to view dashboards
  - cloudwatch:PutDashboard to be able to create or modify dashboards
  - cloudwatch:DeleteDashboards to be able to delete dashboards

Contents

- Creating a CloudWatch dashboard (p. 18)
- Cross-account cross-Region dashboards (p. 18)
- Creating and working with widgets on CloudWatch dashboards (p. 21)
- Sharing CloudWatch dashboards (p. 38)
- Use live data (p. 47)
- Viewing an animated dashboard (p. 47)
- Add a dashboard to your Favorites list (p. 48)
- Change the period override setting or refresh interval for the CloudWatch dashboard (p. 48)
- Change the time range or time zone format of a CloudWatch dashboard (p. 49)
Creating a CloudWatch dashboard

To get started with CloudWatch dashboards, you must first create a dashboard. You can create multiple dashboards. There is no limit on the number of CloudWatch dashboards in your AWS account. All dashboards are global, not Region-specific.

The steps in this section are for creating a dashboard using the console. You can also create a dashboard with the PutDashboard API, which uses a JSON string to define the dashboard contents. To create a dashboard using PutDashboard and base this dashboard on an existing dashboard, choose Actions and then View/edit source to display and copy the JSON string of a current dashboard to use for your new dashboard.

For more information about creating a dashboard using the API, see PutDashboard in the Amazon CloudWatch API Reference.

To create a dashboard using the console

2. In the navigation pane, choose Dashboards and then Create dashboard.
3. In the Create new dashboard dialog box, enter a name for the dashboard and choose Create dashboard.

   If you use the name CloudWatch-Default, the dashboard appears on the overview on the CloudWatch home page. For more information, see Getting started with Amazon CloudWatch (p. 11).

   If you use resource groups and name the dashboard CloudWatch-Default-ResourceGroupName, it appears on the CloudWatch home page when you focus on that resource group.
4. Do one of the following in the Add to this dashboard dialog box:
   • To add a graph to your dashboard, choose Line or Stacked area and choose Configure. In the Add metric graph dialog box, select the metrics to graph and choose Create widget. If a specific metric doesn't appear in the dialog box because it hasn't published data in more than 14 days, you can add it manually. For more information, see Graph metrics manually on a CloudWatch dashboard (p. 24).
   • To add a number displaying a metric to the dashboard, choose Number and then Configure. In the Add metric graph dialog box, select the metrics to graph and choose Create widget.
   • To add a text block to your dashboard, choose Text and then Configure. In the New text widget dialog box, for Markdown, add and format your text using Markdown. Choose Create widget.
5. Optionally, choose Add widget and repeat step 4 to add another widget to the dashboard. You can repeat this step multiple times.
6. Choose Save dashboard.

Cross-account cross-Region dashboards

You can create cross-account cross-Region dashboards, which summarize your CloudWatch data from multiple AWS accounts and multiple Regions into one dashboard. From this high-level dashboard you can get a view of your entire application, and also drill down into more specific dashboards without having to sign in and out of accounts or switch Regions.

You can create cross-account cross-Region dashboards in the AWS Management Console and programmatically.

Prerequisite
Before you can create a cross-account cross-Region dashboard, you must enable at least one sharing account and at least one monitoring account. Additionally, to be able to use the CloudWatch console to create a cross-account dashboard, you must enable the console for cross-account functionality. For more information, see Cross-account cross-Region CloudWatch console (p. 242).

Creating and using a cross-account cross-Region dashboard with the AWS Management Console

You can use the AWS Management Console to create a cross-account cross-Region dashboard.

To create a cross-account cross-Region dashboard

1. Sign in to the monitoring account.
2. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
3. In the navigation pane, choose Dashboards.
4. Choose a dashboard, or create a new one.
5. At the top of the screen, you can switch between accounts and Regions. As you create your dashboard, you can include widgets from multiple accounts and Regions. Widgets include graphs, alarms, and CloudWatch Logs Insights widgets.

Creating a graph with metrics from different accounts and Regions

1. Sign in to the monitoring account.
2. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
3. In the navigation pane, choose Metrics.
4. Under All metrics, choose the account and Region that you want to add metrics from.
5. Add the metrics you want to the graph. For more information, see Graphing metrics (p. 66).
6. Repeat steps 4-5 to add metrics from other accounts and Regions.
7. (Optional) Choose the Graphed metrics tab and add a metric math function that uses the metrics that you have chosen. For more information, see Using metric math (p. 77).

You can also set up a single graph to include multiple SEARCH functions. Each search can refer to a different account or Region.
8. When you are finished with the graph, choose Actions, Add to dashboard.
   Select your cross-account dashboard, and choose Add to dashboard.

Adding an alarm from a different account to your cross-account dashboard

1. Sign in to the monitoring account.
2. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
3. At the top of the page, choose the account where the alarm is located.
4. In the navigation pane, choose Alarms.
5. Select the check box next to the alarm that you want to add, and choose Add to dashboard.
6. Select the cross-account dashboard that you want to add it to, and choose Add to dashboard.
Create a cross-account cross-Region dashboard programmatically

You can use the AWS APIs and SDKs to create dashboards programmatically. For more information, see PutDashboard.

To enable cross-account cross-Region dashboards, we have added new parameters to the dashboard body structure, as shown in the following table and examples. For more information about overall dashboard body structure, see Dashboard Body Structure and Syntax.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Use</th>
<th>Scope</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>accountId</td>
<td>Specifies the ID of the account where the widget or the metric is located.</td>
<td>Widget or metric</td>
<td>Account that is currently logged in</td>
</tr>
<tr>
<td>region</td>
<td>Specifies the Region of the metric.</td>
<td>Widget or metric</td>
<td>Current Region selected in the console</td>
</tr>
</tbody>
</table>

The following examples illustrate the JSON source for widgets in a cross-account cross-Region dashboard.

This example sets the accountId field to the ID of the sharing account at the widget level. This specifies that all metrics in this widget will come from that sharing account and Region.

```json
{
    "widgets": [
        {
            "properties": {
                "metrics": [
                    ...
                ],
                "accountId": "111122223333",
                "region": "us-east-1"
            }
        }
    ]
}
```

This example sets the accountId field differently at the level of each metric. In this example, the different metrics in this metric math expression come from different sharing accounts and different Regions.

```json
{
    "widgets": [
        {
            "properties": {
                "metrics": [
                    { "expression": "SUM(METRICS())", "label": "[avg: ${AVG}] Expression1", "id": "e1", "stat": "Sum" } ],
                    [ "AWS/EC2", "CPUUtilization", { "id": "m2", "accountId": "5555666677778888", "region": "us-east-1", "label": "[avg: ${AVG}] ApplicationALabel" } ],
                    [ ".", ".", { "id": "m1", "accountId": "9999000011112222", "region": "eu-west-1", "label": "[avg: ${AVG}] ApplicationBLabel" } ]
                ]
            }
        }
    ]
}
```
Creating and working with widgets on CloudWatch dashboards

This example shows an alarm widget.

```json
{
  "type": "metric",
  "x": 6,
  "y": 0,
  "width": 6,
  "height": 6,
  "properties": {
    "accountID": "111122223333",
    "title": "over50",
    "annotations": {
      "alarms": [
        "arn:aws:cloudwatch:us-east-1:379642911888:alarm:over50"
      ]
    },
    "view": "timeSeries",
    "stacked": false
  }
}
```

This example is for a CloudWatch Logs Insights widget.

```json
{
  "type": "log",
  "x": 0,
  "y": 6,
  "width": 24,
  "height": 6,
  "properties": {
    "query": "SOURCE 'route53test' | fields @timestamp, @message\n| sort @timestamp desc\n| limit 20",
    "accountid": "111122223333",
    "region": "us-east-1",
    "stacked": false,
    "view": "table"
  }
}
```

Another way to create dashboards programmatically is to first create one in the AWS Management Console, and then copy the JSON source of this dashboard. To do so, load the dashboard and choose Actions, View/edit source. You can then copy this dashboard JSON to use as a template to create similar dashboards.

Creating and working with widgets on CloudWatch dashboards

Use the topics in this section to create and work with graphs, alarms, and text widgets in your dashboards.
Add or remove a graph from a CloudWatch dashboard

You can add graphs containing one or more metrics to your dashboard for the resources you monitor. You can remove the graphs when they're no longer needed.

To add a graph to a dashboard

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Choose Add widget.
4. Choose the type of graph you want: Line, Stacked area, Bar, or Pie. Then choose Next.
5. Choose Metrics and then choose Configure.
6. In the All metrics tab, select the metrics to graph. If a specific metric doesn't appear in the dialog box because it hasn't published data in more than 14 days, you can add it manually. For more information, see Graph metrics manually on a CloudWatch dashboard (p. 24).
7. (Optional) To change the type of graph, choose Graph options. You can then choose between a line graph, stacked area chart, bar chart, pie chart, or number.
8. (Optional) As you choose metrics to graph, you can specify a dynamic label to appear on the graph legend for each metric. Dynamic labels display a statistic about the metric and automatically update when the dashboard or graph is refreshed. To add a dynamic label, choose Graphed metrics and then Dynamic labels.

By default, the dynamic values you add to the label appear at the beginning of the label. You can then choose the Label value for the metric to edit the label. For more information, see Using dynamic labels (p. 69).

9. (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. Click outside the color picker to see your new color on the graph. Alternatively, in the color picker, you can enter the six-digit standard HTML hex color code for the color you want and press Enter.
10. (Optional) To view more information about the metric being graphed, hover over the legend.
11. (Optional) To change the widget type, hover over the title area of the graph and choose Widget actions, Widget type.
12. (Optional) To change the statistic used for a metric, choose Graphed metrics, Statistic, and select the statistic you want to use. For more information, see Statistics (p. 5).
13. (Optional) To change the time range shown on the graph, choose either custom at the top of the graph or one of the time periods to the left of custom.
14. (Optional) Horizontal annotations 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**, enter a label for the annotation.
   b. For **Value**, enter 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 check box in the left column for that annotation.

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

15. (Optional) Vertical annotations help you mark milestones in a graph, such as operational events or the beginning and end of a deployment. To add a vertical annotation, choose **Graph options, Add vertical annotation**:

   a. For **Label**, enter a label for the annotation. To show only the date and time on the annotation, keep the **Label** field blank.
   b. For **Date**, specify the date and time where the vertical annotation appears.
   c. For **Fill**, specify whether to use fill shading before or after a vertical annotation or between two vertical annotations. For example, choose **Before** or **After** for the corresponding area to be filled. If you specify **Between**, another **Date** field appears, and the area of the graph between the two values is filled.

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

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

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

16. Choose **Create widget**.
17. Choose **Save dashboard**.

**To remove a graph from a dashboard**

2. In the navigation pane, choose **Dashboards** and select a dashboard.
3. Hover over the title of the graph and choose **Widget actions** and then **Delete**.
4. Choose **Save dashboard**. If you attempt to navigate away from the dashboard before you save your changes, you're prompted to either save or discard your changes.
Graph metrics manually on a CloudWatch dashboard

If a metric hasn’t published data in the past 14 days, you can’t find it when searching for metrics to add to a graph on a CloudWatch dashboard. Use the following steps to add any metric manually to an existing graph.

To add a metric that you can’t find in search to a graph

2. In the navigation pane, choose Dashboards and select a dashboard.
3. The dashboard must already contain a graph where you want to add the metric. If it doesn’t, create the graph and add any metric to it. For more information, see Add or remove a graph from a CloudWatch dashboard (p. 22).

A JSON block appears. The block specifies the widgets on the dashboard and their contents. The following is an example of one part of this block, which defines one graph.

```json
{
    "type": "metric",
    "x": 0,
    "y": 0,
    "width": 6,
    "height": 3,
    "properties": {
        "view": "singleValue",
        "metrics": [
            [ "AWS/EBS", "VolumeReadOps", "VolumeId", "vol-1234567890abcdef0" ],
            [ "AWS/EBS", "VolumeReadOps", "VolumeId", "vol-1234567890abcdef0" ],
            "region": "us-west-1"
        ]
    }
}
```

In this example, the following section defines the metric shown on this graph.

```json
[ "AWS/EBS", "VolumeReadOps", "VolumeId", "vol-1234567890abcdef0" ]
```

5. Add a comma after the end bracket if there isn’t already one and then add a similar bracketed section after the comma. In this new section, specify the namespace, metric name, and any necessary dimensions of the metric that you’re adding to the graph. The following is an example.

```json
[ "AWS/EBS", "VolumeReadOps", "VolumeId", "vol-1234567890abcdef0" ],
[ "MyNamespace", "MyMetricName", "DimensionName", "DimensionValue" ]
```

For more information about the formatting of metrics in JSON, see Properties of a Metric Widget Object.

6. Choose Update.

Working with existing graphs

Follow the procedures in these sections to edit and modify your existing dashboard graph widgets.

Topics

• Edit a graph on a CloudWatch dashboard (p. 25)
• Move or resize a graph on a CloudWatch dashboard (p. 26)
• Rename a graph on a CloudWatch dashboard (p. 27)

Edit a graph on a CloudWatch dashboard

You can edit a graph to change the title, statistic, or period, or to add or remove metrics. If you have multiple metrics displayed on a graph, you can reduce the clutter by temporarily hiding the metrics that don’t interest you.

To edit a graph on a dashboard

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Hover over the title of the graph and choose Widget actions, Edit.
4. To change the graph’s title, select the title, enter a new title, and press Enter.
5. To change the type of graph, choose Graph options. You can then choose between a line graph, stacked area chart, bar chart, pie chart, or number.
6. To change the time range shown on the graph, choose either custom at the top of the graph, or one of the time periods to the left of custom.
7. To change the type of widget between separate lines on a graph, stacked lines on a graph, and a number, choose the box next to the right of custom and select either Line, Stacked area, or Number.
8. In the lower half of the screen, in the Graphed metrics tab, you can change the dynamic label, colors, statistic, or period corresponding to a metric:
   a. (Optional) To specify a dynamic label for a metric, choose Dynamic labels. Dynamic labels display a statistic about the metric, and automatically update when the dashboard or graph is refreshed.

      By default, the dynamic values you add to the label appear at the beginning of the label. You can then choose the Label value for the metric to edit the label. For more information, see Using dynamic labels (p. 69).

      b. To change the color of one of the lines, select the color square next to the metric to display a color picker box. Choose another color in the color picker, and click outside the color picker to see your new color on the graph. Alternatively, in the color picker, you can enter the six-digit HTML hex color code for the color you want and press Enter.

      c. To change the statistic, choose Statistic in the lower half of the window, and choose the new statistic you want. For more information, see Statistics (p. 5).

      d. To change the time period, which is next to Statistic in the lower half of the window, choose Period and select another value. This new setting is used on the dashboard only if the period setting of the dashboard itself is set to Auto. Otherwise, the period setting of the dashboard overrides the period setting for individual widgets.
9. To add or edit horizontal annotations, choose Graph options:
   a. To add a horizontal annotation, choose Add horizontal annotation.
   b. For Label, enter a label for the annotation.
   c. For Value, enter the metric value where the horizontal annotation appears.
   d. For Fill, specify how 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.

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

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

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

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

10. To add or edit vertical annotations, choose **Graph options**: **Add vertical annotation**:

a. To add a vertical annotation, choose **Add vertical annotation**.

b. For **Label**, enter a label for the annotation. To show only the date and time on the annotation, keep the **Label** field blank.

c. For **Date**, specify the date and time where the vertical annotation appears.

d. For **Fill**, specify whether to use fill shading before or after a vertical annotation, or between two vertical annotations. For example, choose **Before** or **After** for the corresponding area to be filled. If you specify **Between**, another **Date** field appears, and the area of the graph between the two values is filled.

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

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

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

11. To hide or change the position of the graph legend, hover over the title of the graph and choose **Widget actions**, **Edit**. Hover over **Legend** and choose **Hidden**, **Bottom**, or **Right**.

12. To customize the y-axis, choose **Graph options**. You can enter a custom label in **Label** under **Left Y Axis**. If the graph also displays values on the right y-axis, you can customize that label, too. You can also set minimums and maximums on the y-axis values, and the graph displays only the value range that you specify.

13. When you’re finished with your changes, choose **Update widget**.

**To temporarily hide metrics for a graph on a dashboard**

2. In the navigation pane, choose **Dashboards** and select a dashboard.
3. In the graph’s footer, hover over the colored square in the legend. When it changes to an X, choose it.
4. To restore the metric, choose the grayed-out square and metric name.

**Move or resize a graph on a CloudWatch dashboard**

You can arrange and resize graphs on your CloudWatch dashboard.

**To move a graph on a dashboard**

2. In the navigation pane, choose **Dashboards** and select a dashboard.
3. Hover over the title of the graph until the selection icon appears. Select and drag the graph to a new location on the dashboard.
4. Choose **Save dashboard**.
To resize a graph

2. In the navigation pane, choose Dashboards and choose a dashboard.
3. To increase or decrease the size, hover over the graph and drag the lower right corner of the graph. Stop dragging the corner when you have the size that you want.
4. Choose Save dashboard.

To enlarge a graph temporarily

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Select the graph. Alternatively, hover over the title of the graph and choose Widget actions, Enlarge.

Rename a graph on a CloudWatch dashboard

You can change the default name that CloudWatch assigns to a graph on your dashboard.

To rename a graph on a dashboard

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Hover over the title of the graph and choose Widget actions and Edit.
4. On the Edit graph screen, near the top, choose the title of the graph.
5. For Title, enter a new name and choose Ok (check mark). In the lower-right corner of the Edit graph screen, choose Update widget.

Add a metrics explorer widget to a CloudWatch dashboard

Metrics explorer widgets include graphs of multiple resources that have the same tag, or share the same resource property such as an instance type. These widgets stay up to date, as resources that match are created or deleted. Adding metrics explorer widgets to your dashboard helps you to troubleshoot your environment more efficiently.

For example, you can monitor your fleet of EC2 instances by assigning tags that represent their environments, such as production or test. You can then use these tags to filter and aggregate the operational metrics, such as CPUUtilization, to understand the health and performance of the EC2 instances that are associated with each tag.

The following steps explain how to add a metrics explorer widget to a dashboard using the console. You can also add it programmatically or by using AWS CloudFormation. For more information, see Metrics Explorer Widget Object Definition and AWS::CloudWatch::Dashboard.

To add a metrics explorer widget to a dashboard

2. In the navigation pane, choose Dashboards.
3. Choose the name of the dashboard where you want to add the metrics explorer widget.
4. Choose Add widget.
5. Choose Explorer and then choose Next.

Note
You must be opted in to the new dashboard view to be able to add a Metrics Explorer widget. To opt in, choose Dashboards in the navigation pane, then choose try out the new interface in the banner at the top of the page.

6. Do one of the following:
   • To use a template, choose Pre-filled Explorer widget and then select a template to use.
   • To create a custom visualization, choose Empty Explorer widget.
7. Choose Create.

If you used a template, the widget appears on your dashboard with the selected metrics. If you're satisfied with the explorer widget and the dashboard, choose Save dashboard.

If you did not use a template, continue to the following steps.
8. In the new widget under Explorer, in the Metrics box, choose a single metric or all the available metrics from a service.

After you choose a metric, you can optionally repeat this step to add more metrics.
9. For each metric selected, CloudWatch displays the statistic that it will use immediately after the metric name. To change this, choose the statistic name and then choose the statistic that you want.
10. Under From, choose a tag or a resource property to filter your results.

After you do this, you can optionally repeat this step to choose more tags or resource properties.

If you choose multiple values of the same property, such as two EC2 instance types, the explorer displays all the resources that match either chosen property. It's treated as an OR operation.

If you choose different properties or tags, such as the Production tag and the M5 instance type, only the resources that match all of these selections are displayed. This is treated as an AND operation.
11. (Optional) For Aggregate by, choose a statistic to use to aggregate the metrics. Then, next to for, choose how to aggregate the metric from the list. You can aggregate together all the resources that are currently displayed, or aggregate by a single tag or resource property.

Depending on how you choose to aggregate, the result may be a single time series or multiple time series.
12. Under Split by, you can choose to split a single graph with multiple time series into multiple graphs. The split can be made by a variety of criteria, which you choose under Split by.
13. Under Graph options, you can refine the graph by changing the period, the type of graph, the legend placement, and the layout.
14. If you're satisfied with the explorer widget and the dashboard, choose Save dashboard.

Add an alarm widget to a CloudWatch dashboard

To add an alarm widget to a dashboard, you have two options.

• You can add a single alarm in a widget, which displays both the graph of the alarm's metric and the alarm status.
• You can add an alarm status widget, which displays the status of multiple alarms in a grid. Only the alarm names and current status are displayed; the graphs are not displayed. Up to 100 alarms can be included in one alarm status widget.
To add a single alarm, including its graph, to a dashboard

2. In the navigation pane, choose Alarms, select the alarm to add, and then choose Add to Dashboard.
3. Select a dashboard, choose a widget type (Line, Stacked area, or Number), and then choose Add to dashboard.
4. To see your alarm on the dashboard, choose Dashboards in the navigation pane and select the dashboard.
5. (Optional) To temporarily make an alarm graph larger, select the graph.
6. (Optional) To change the widget type, pause on the title of the graph, choose Widget actions, and then choose Widget type.

To add an alarm status widget to a dashboard

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Choose Add widget.
5. Select the check boxes next to the alarms that you want to add to the widget, and then choose Create widget.
6. Choose Add to dashboard.

To remove an alarm widget from a dashboard

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Pause on the widget, choose Widget actions, and then choose Delete.
4. Choose Save dashboard. If you attempt to navigate away from the dashboard before you save your changes, you're prompted to either save or discard your changes.

Add a custom widget to a CloudWatch dashboard

A custom widget is a CloudWatch dashboard widget that can call any AWS Lambda function with custom parameters. It then displays the returned HTML or JSON. Custom widgets are a simple way to build a custom data view on a dashboard. If you can write Lambda code and create HTML, you can create a useful custom widget. Additionally, Amazon provides several pre-built custom widgets that you can create without any code.

When you create a Lambda function to use as a custom widget, we strongly recommend that you include the prefix customWidget in the function name. This helps you know which of your Lambda functions are safe to use when you add custom widgets to your dashboard.

Custom widgets behave like other widgets on your dashboard. They can be refreshed and auto-refreshed, resized, and moved around. They react to the time range of the dashboard.

If you have set up CloudWatch console cross-account functionality, you can add a custom widget created in one account to dashboards in other accounts. For more information, see Cross-account cross-Region CloudWatch console (p. 242).

You can also use custom widgets on your own website by using the CloudWatch dashboard sharing feature. For more information, see Sharing CloudWatch dashboards (p. 38).

Topics
Details about custom widgets

Custom widgets work as follows:

1. The CloudWatch dashboard calls the Lambda function containing the widget code. It passes in any custom parameters that are defined in the widget.
2. The Lambda function returns a string of HTML, JSON, or Markdown. Markdown is returned as JSON in the following format:

   ```json
   {"markdown":"markdown content"}
   ```
3. The dashboard displays the returned HTML or JSON.

   If the function returns HTML, most HTML tags are supported. You can use Cascading Style Sheets (CSS) styles and Scalable Vector Graphics (SVG) to build sophisticated views.

   The default style of HTML elements such as links and tables follow the styling of CloudWatch dashboards. You can customize this style by using inline styles, using the `<style>` tag. You can also deactivate the default styles by including a single HTML element with the class of `cwdb-no-default-styles`. The following example deactivates default styles:

   `<div class="cwdb-no-default-styles"></div>`

   Every call by a custom widget to Lambda includes a `widgetContext` element with the following contents, to provide the Lambda function developer with useful context information.

   ```json
   {
     "widgetContext": {
       "dashboardName": "Name-of-current-dashboard",
       "widgetId": "widget-16",
       "accountId": "012345678901",
       "locale": "en",
       "timezone": {
         "label": "UTC",
         "offsetISO": "+00:00",
         "offsetInMinutes": 0
       },
       "period": 300,
       "isAutoPeriod": true,
       "timeRange": {
         "mode": "relative",
         "start": 1627236199729,
         "end": 1627322599729,
         "relativeStart": 86400012,
         "zoom": {
           "start": 1627276030434,
           "end": 1627282956521
         }
       },
       "theme": "light",
       "linkCharts": true,
       "title": "Tweets for Amazon website problem",
       "forms": {
       ```
Default CSS styling

Custom widgets provide the following default CSS styling elements:

- You can use the CSS class `btn` to add a button. It turns an anchor `<a>` into a button as in the following example:

  ```html
  <a class="btn" href=https://amazon.com">Open Amazon</a>
  ```

- You can use the CSS class `btn btn-primary` to add a primary button.

- The following elements are styled by default: `table`, `select`, headers (h1, h2, and h3), preformatted text (pre), `input`, and `textarea`.

Using the describe parameter

We strongly recommend that you support the `describe` parameter in your functions, even if it just returns an empty string. If you don't support it, and it is called in the custom widget, it displays widget content as if it was documentation.

If you include the `describe` parameter, the Lambda function returns the documentation in Markdown format and does nothing else.

When you create a custom widget in the console, after you select the Lambda function a `Get documentation` button appears. If you choose this button, the function is invoked with the `describe` parameter and the function's documentation is returned. If the documentation is well-formatted in markdown, CloudWatch parses the first entry in the documentation that is surrounded by three single backtick characters (```) in YAML. Then, it automatically populates the documentation in the parameters. The following is an example of such well-formatted documentation.

```yaml
---

```
yaml

```yaml

Security and JavaScript

For security reasons, JavaScript is not allowed in the returned HTML. Removing the JavaScript prevents permission escalation issues, where the writer of the Lambda function injects code that could run with higher permissions than the user viewing the widget on the dashboard.

If the returned HTML contains any JavaScript code or other known security vulnerabilities, it is cleaned from the HTML before it is rendered on the dashboard. Specifically, the `<iframe>` and `<use>` tags are not allowed and are removed.

Interactivity in the custom widget

Even though JavaScript is not allowed, there are other ways to allow interactivity with the returned HTML.
• Any element in the returned HTML can be tagged with special configuration in a `<cwdb-action>` tag, which can display information in pop-ups, ask for confirmation on clicks, and call any Lambda function when that element is chosen. For example, you can define buttons that call any AWS API using a Lambda function. The returned HTML can be set to either replace the existing Lambda widget's content, or display inside a modal.

• The returned HTML can include links that open new consoles, open other customer pages, or load other dashboards.

• The HTML can include the `title` attribute for an element, which gives additional information if the user pauses on that element.

• The element can include CSS selectors, such as `:hover`, which can invoke animations or other CSS effects. You can also show or hide elements in the page.

### `<cwdb-action>` definition and usage

The `<cwdb-action>` element defines a behavior on the immediately previous element. The content of the `<cwdb-action>` is either HTML to display or a JSON block of parameters to pass to a Lambda function.

The following is an example of a `<cwdb-action>` element.

```xml
<wb-admin-tooltip>
    <cwdb-action
        action="call|html"
        confirmation="message"
        display="popup|widget"
        endpoint="<lambda ARN>"
        event="click|dblclick|mouseenter">
        html | params in JSON
    </cwdb-action>
</wb-admin-tooltip>
```

• **action**— Valid values are `call`, which calls a Lambda function, and `html`, which displays any HTML contained within `<cwdb-action>`. The default is `html`.

• **confirmation**— Displays a confirmation message that must be acknowledged before the action is taken, allowing the customer to cancel.

• **display**— Valid values are `popup` and `widget`, which replaces the content of the widget itself. The default is `widget`.

• **endpoint**— The Amazon Resource Name (ARN) of the Lambda function to call. This is required if action is `call`.

• **event**— Defines the event on the previous element that invokes the action. Valid values are `click`, `dblclick`, and `mouseenter`. The default is `click`.

### Examples

The following is an example of how to use the `<cwdb-action>` tag to create a button that reboots an Amazon EC2 instance using a Lambda function call. It displays the success or failure of the call in a pop-up.

```html
<a class="btn">Reboot Instance</a>
<wb-admin-tooltip>
    <cwdb-action action="call" endpoint="arn:aws:lambda:us-east-1:123456:function:rebootInstance" display="popup">
        { "instanceId": "i-342389adbef" }
    </cwdb-action>
</wb-admin-tooltip>
```

The next example displays more information in a pop-up.
This example is a Next button that replaces the content of a widget with a call to a Lambda function.

Create a custom widget

To create a custom widget, you can use one of the samples provided by Amazon, or you can create your own. The Amazon samples include samples in both JavaScript and Python, and are created by a AWS CloudFormation stack. For a list of samples, see Sample custom widgets (p. 34).

To create a custom widget in a CloudWatch dashboard

2. In the navigation pane, choose Dashboards, and then select a dashboard.
3. Choose Add widget.
4. Choose Custom widget.
5. Use one of the following methods:
   - To use a sample custom widget provided by Amazon, do the following:
     a. Select the sample in the dropdown box.
        The AWS CloudFormation console launches in a new browser. In the AWS CloudFormation console, do the following:
     b. (Optional) Customize the AWS CloudFormation stack name.
     c. Make selections for any parameters used by the sample.
     d. Select I acknowledge that AWS CloudFormation might create IAM resources, and choose Create stack.
   - To create your own custom widget provided by Amazon, do the following:
     a. Choose Next.
     b. Choose to either select your Lambda function from a list, or enter its Amazon Resource Name (ARN). If you select it from a list, also specify the Region where the function is and the version to use.
     c. For Parameters, make selections for any parameters used by the function.
     d. Enter a title for the widget.
     e. For Update on, configure when the widget should be updated (when the Lambda function should be called again). This can be one or more of the following: Refresh to update it when the dashboard auto-refreshes, Resize to update it whenever the widget is resized, or Time Range to update it whenever the dashboard's time range is adjusted, including when graphs are zoomed into.
     f. If you are satisfied with the preview, choose Create widget.
Sample custom widgets

AWS provides sample custom widgets in both JavaScript and Python. You can create these sample widgets by using the link for each widget in this list. Alternatively, you can create and customize a widget by using the CloudWatch console. The links in this list open an AWS CloudFormation console and use an AWS CloudFormation quick-create link to create the custom widget.

You can also access the custom widget samples on GitHub.

Following this list, complete examples of the Echo widget are shown for each language.

JavaScript

Sample custom widgets in JavaScript

- **Echo** – A basic echoer that you can use to test how HTML appears in a custom widget, without having to write a new widget.
- **Hello world** – A very basic starter widget.
- **Custom widget debugger** – A debugger widget that displays useful information about the Lambda runtime environment.
- **Query CloudWatch Logs Insights** – Run and edit CloudWatch Logs Insights queries.
- **Run Amazon Athena queries** – Run and edit Athena queries.
- **Call AWS API** – Call any read-only AWS API and display the results in JSON format.
- **Fast CloudWatch bitmap graph** – Render CloudWatch graphs using on the server side, for fast display.
- **Text widget from CloudWatch dashboard** – Displays the first text widget from the specified CloudWatch dashboard.
- **CloudWatch metric data as a table** – Displays raw CloudWatch metric data in a table.
- **Amazon EC2 table** – Displays the top EC2 instances by CPU utilization. This widget also includes a Reboot button, which is disabled by default.
- **AWS CodeDeploy deployments** – Displays CodeDeploy deployments.
- **AWS Cost Explorer report** – Displays a report on the cost of each AWS service for a selected time range.
- **Display content of external URL** – Displays the content of an externally accessible URL.
- **Display an Amazon S3 object** – Displays an object in an Amazon S3 bucket in your account.
- **Simple SVG pie chart** – Example of a graphical SVG-based widget.

Python

Sample custom widgets in Python

- **Echo** – A basic echoer which you can use to test how HTML appears in a custom widget, without having to write a new widget.
- **Hello world** – A very basic starter widget.
- **Custom widget debugger** – A debugger widget that displays useful information about the Lambda runtime environment.
- **Call AWS API** – Call any read-only AWS API and display the results in JSON format.
- **Fast CloudWatch bitmap graph** – Render CloudWatch graphs using on the server side, for fast display.
- **Send dashboard snapshot by email** – Take a snapshot of the current dashboard and send it to email recipients.
• **Send dashboard snapshot to Amazon S3** – Take a snapshot of the current dashboard and store it in Amazon S3.
• **Text widget from CloudWatch dashboard** – Displays the first text widget from the specified CloudWatch dashboard.
• **Display content of external URL** – Displays the content of an externally accessible URL.
• **RSS reader** – Displays RSS feeds.
• **Display an Amazon S3 object** – Displays an object in an Amazon S3 bucket in your account.
• **Simple SVG pie chart** – Example of a graphical SVG-based widget.

**Echo widget in JavaScript**

The following is the Echo sample widget in JavaScript.

```javascript
const DOCS = `## Echo
A basic echo script. Anything passed in the `\`\`\``echo\`\`\` parameter is returned as the content of the custom widget.

### Widget parameters

<table>
<thead>
<tr>
<th>Param</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>echo</strong></td>
<td>The content to echo back</td>
</tr>
</tbody>
</table>

### Example parameters
```
yaml
```
\``yaml
```
echo: &h1>Hello world</h1>
```

exports.handler = async (event) => {
  if (event.describe) {
    return DOCS;
  }

  let widgetContext = JSON.stringify(event.widgetContext, null, 4);
  widgetContext = widgetContext.replace(/</g, '&lt;');
  widgetContext = widgetContext.replace(/>/g, '>');

  return `#(event.echo || '')<pre>${widgetContext}</pre>`;
};
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
```
def lambda_handler(event, context):
    if 'describe' in event:
        return DOCS

    echo = event.get('echo', '')
    widgetContext = event.get('widgetContext')
    widgetContext = json.dumps(widgetContext, indent=4)
    widgetContext = widgetContext.replace('<', '&lt;')
    widgetContext = widgetContext.replace('>', '&gt;')

    return f'{echo}<pre>{widgetContext}</pre>'

Echo widget in Java

The following is the Echo sample widget in Java.

```java
package example;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.RequestHandler;
import com.google.gson.Gson;
import com.google.gson.GsonBuilder;

public class Handler implements RequestHandler<Event, String> {
    static String DOCS = "
    """Echo"
    """A basic echo script. Anything passed in the ```echo``` parameter is returned as the content of the custom widget.
    """Widget parameters"
    """Param | Description
    """|---|--|
    ""``echo`` | The content to echo back
    ""``yaml``
    ""``Hello world``
    """"
    Gson gson = new GsonBuilder().setPrettyPrinting().create();

    @Override
    public String handleRequest(Event event, Context context) {
        if (event.describe) {
            return DOCS;
        }

        return (event.echo != null ? event.echo : "") + "<pre>
        gson.toJson(event.widgetContext) + "</pre>";
    }
}

class Event {
    public boolean describe;
    public String echo;
    public Object widgetContext;

    public Event() {}

    public Event(String echo, boolean describe, Object widgetContext) {
        this.describe = describe;
        this.echo = echo;
        this.widgetContext = widgetContext;
    }
```
Add or remove a text widget from a CloudWatch dashboard

A text widget contains a block of text in Markdown format. You can add, edit, or remove text widgets from your CloudWatch dashboard.

To add a text widget to a dashboard

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Choose Add widget.
4. Choose Text and then Configure.
5. For Markdown, add and format your text using Markdown and choose Create widget.
6. Choose Save dashboard.

To edit a text widget on a dashboard

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Hover over the upper-right corner of the text block and choose Widget actions and then Edit.
4. Update the text as needed and choose Update widget.
5. Choose Save dashboard.

To remove a text widget from a dashboard

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Hover over the upper-right corner of the text block and choose Widget actions and then Delete.
4. Choose Save dashboard.

Link and unlink graphs on a CloudWatch dashboard

You can link the graphs on your dashboard together, so that when you zoom in or zoom out on one graph, the other graphs zoom in or zoom out at the same time. You can unlink graphs to limit zoom to one graph.

To link the graphs on a dashboard

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Choose Actions and then Link graphs.

To unlink the graphs on a dashboard

2. In the navigation pane, choose **Dashboards** and select a dashboard.
3. Clear **Actions** and then **Link graphs**.

### Sharing CloudWatch dashboards

You can share your CloudWatch dashboards with people who do not have direct access to your AWS account. This enables you to share dashboards across teams, with stakeholders, and with people external to your organization. You can even display dashboards on big screens in team areas, or embed them in Wikis and other webpages.

**Warning**

All people who you share the dashboard with are granted the permissions listed in Permissions that are granted to people who you share the dashboard with (p. 39) for the account. If you share the dashboard publicly, then everyone who has the link to the dashboard has these permissions.

The `cloudwatch:GetMetricData` and `ec2:DescribeTags` permissions cannot be scoped down to specific metrics or EC2 instances, so the people with access to the dashboard can query all CloudWatch metrics and the names and tags of all EC2 instances in the account.

When you share dashboards, you can designate who can view the dashboard in three ways:

- Share a single dashboard and designate specific email addresses of the people who can view the dashboard. Each of these users creates their own password that they must enter to view the dashboard.
- Share a single dashboard publicly, so that anyone who has the link can view the dashboard.
- Share all the CloudWatch dashboards in your account and specify a third-party single sign-on (SSO) provider for dashboard access. All users who are members of this SSO provider's list can access all the dashboards in the account. To enable this, you integrate the SSO provider with Amazon Cognito. The SSO provider must support Security Assertion Markup Language (SAML). For more information about Amazon Cognito, see [What is Amazon Cognito?](#)

### Permissions required to share a dashboard

To be able to share dashboards using any of the following methods and to see which dashboards have already been shared, you must be logged on to an IAM user or IAM role that has certain permissions.

To be able to share dashboards, your IAM user or IAM role must include the permissions included in the following policy statement:

```
{
  "Effect": "Allow",
  "Action": [
    "iam:CreateRole",
    "iam:CreatePolicy",
    "iam:AttachRolePolicy",
    "iam:PassRole"
  ],
  "Resource": [
    "arn:aws:iam::*:role/service-role/CWDBSharing*",
    "arn:aws:iam::*:policy/*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "cognito-idp:*",
    "cognito:*",
    "iam:CreateRole",
    "iam:CreatePolicy",
    "iam:AttachRolePolicy",
    "iam:PassRole"
  ],
  "Resource": [
    "arn:aws:iam::*:role/service-role/CWDBSharing*",
    "arn:aws:iam::*:policy/*"
  ]
}
```

---

38
Permissions that are granted to people who you share the dashboard with

When you share a dashboard, CloudWatch creates an IAM role in the account which gives the following permissions to the people who you share the dashboard with:

- `cloudwatch:GetInsightRuleReport`
- `cloudwatch:GetMetricData`
- `cloudwatch:DescribeAlarms`
- `ec2:DescribeTags`

**Warning**

All people who you share the dashboard with are granted these permissions for the account. If you share the dashboard publicly, then everyone who has the link to the dashboard has these permissions.

The `cloudwatch:GetMetricData` and `ec2:DescribeTags` permissions cannot be scoped down to specific metrics or EC2 instances, so the people with access to the dashboard can query all CloudWatch metrics and the names and tags of all EC2 instances in the account.
When you share a dashboard, by default the permissions that CloudWatch creates restrict access to only the alarms and Contributor Insights rules that are on the dashboard when it is shared. If you add new alarms or Contributor Insights rules to the dashboard and want them to also be seen by the people who you shared the dashboard with, you must update the policy to allow these resources.

**Share a single dashboard with specific users**

Use the steps in this section to share a dashboard with specific email addresses that you choose.

**Note**

By default, any CloudWatch Logs widgets on the dashboard are not visible to people who you share the dashboard with. For more information, see Allowing people that you share with to see logs table widgets (p. 45).

By default, any composite alarm widgets on the dashboard are not visible to people who you share the dashboard with. For more information, see Allowing people that you share with to see composite alarms (p. 44).

**To share a dashboard with specific users**

2. In the navigation pane, choose **Dashboards**.
3. Choose the name of your dashboard.
4. Choose **Actions**, **Share dashboard**.
5. Next to **Share your dashboard and require a username and password**, choose **Start sharing**.
6. Under **Add email addresses**, enter the email addresses that you want to share the dashboard with.
7. When you have all the email addresses entered, read the agreement and select the confirmation box. Then choose **Preview policy**.
8. Confirm that the resources that will be shared are what you want, and choose **Confirm and generate shareable link**.
9. On the next page, choose **Copy link to clipboard**. You can then paste this link into email and send it to the invited users. They automatically receive a separate email with their user name and a temporary password to use to connect to the dashboard.

**Share a single dashboard publicly**

Follow the steps in this section to share a dashboard publicly. This can be useful to display the dashboard on a big screen in a team room, or embed it in a Wiki page.

**Important**

Sharing a dashboard publicly makes it accessible to anyone who has the link, with no authentication. Do this only for dashboards that do not contain sensitive information.

**Note**

By default, any CloudWatch Logs widgets on the dashboard are not visible to people who you share the dashboard with. For more information, see Allowing people that you share with to see logs table widgets (p. 45).

By default, any composite alarm widgets on the dashboard are not visible to people who you share the dashboard with. For more information, see Allowing people that you share with to see composite alarms (p. 44).

**To share a dashboard publicly**

2. In the navigation pane, choose **Dashboards**.
3. Choose the name of your dashboard.
5. Next to Share your dashboard publicly, choose Start sharing.
6. Enter Confirm in the text box.
7. Read the agreement and select the confirmation box. Then choose Preview policy.
8. Confirm that the resources that will be shared are what you want, and choose Confirm and generate shareable link.
9. On the next page, choose Copy link to clipboard. You can then share this link. Anyone you share the link with can access the dashboard, without providing credentials.

Share all CloudWatch dashboards in the account by using SSO

Use the steps in this section to share all the dashboards in your account with users by using single sign-on (SSO).

**Note**
By default, any CloudWatch Logs widgets on the dashboard are not visible to people who you share the dashboard with. For more information, see Allowing people that you share with to see logs table widgets (p. 45).

By default, any composite alarm widgets on the dashboard are not visible to people who you share the dashboard with. For more information, see Allowing people that you share with to see composite alarms (p. 44).

To share your CloudWatch dashboards with users who are in an SSO provider's list

2. In the navigation pane, choose Dashboards.
3. Choose the name of your dashboard.
5. Choose Go to CloudWatch Settings.
6. If the SSO provider that you want isn't listed in Available SSO providers, choose Manage SSO providers and follow the instructions in Set up SSO for CloudWatch dashboard sharing (p. 41).

Then return to the CloudWatch console and refresh the browser. The SSO provider that you enabled should now appear in the list.

7. Choose the SSO provider that you want in the Available SSO providers list.
8. Choose Save changes.

Set up SSO for CloudWatch dashboard sharing

To set up dashboard sharing through a third-party single sign-on provider that supports SAML, follow these steps.

**Important**
We strongly recommend that you do not share dashboards using a non-SAML SSO provider. Doing so causes a risk of inadvertently allowing third parties to access your account’s dashboards.

To set up an SSO provider to enable dashboard sharing

1. Integrate the SSO provider with Amazon Cognito. For more information, see Integrating Third-Party SAML Identity Providers with Amazon Cognito User Pools.
2. Download the metadata XML file from your SSO provider.
4. In the navigation pane, choose Settings.
5. In the Dashboard sharing section, choose Configure.
6. Choose Manage SSO providers.

This opens the Amazon Cognito console in the US East (N. Virginia) Region (us-east-1). If you don't see any User Pools, the Amazon Cognito console might have opened in a different Region. If so, change the Region to US East (N. Virginia) us-east-1 and proceed with the next steps.
7. Choose the CloudWatchDashboardSharing pool.
8. In the navigation pane, choose Identity providers.
9. Choose SAML.
10. Enter a name for your SSO provider in Provider name.
11. Choose Select file, and select the metadata XML file that you downloaded in step 1.
12. Choose Create provider.

See how many of your dashboards are shared

You can use the CloudWatch console to see how many of your CloudWatch dashboards are currently being shared with others.

To see how many of your dashboards are being shared
2. In the navigation pane, choose Settings.
3. The Dashboard sharing section displays how many dashboards are shared.
4. To see which dashboards are shared, choose number dashboards shared under Username and password and under Public dashboards.

See which of your dashboards are shared

You can use the CloudWatch console to see which of your dashboards are currently being shared with others.

To see which of your dashboards are being shared
2. In the navigation pane, choose Dashboards.
3. In the list of dashboards, see the Share column. Dashboards that have the icon in this column filled in are currently being shared.
4. To see which users a dashboard is being shared with, choose the dashboard name, and then choose Actions, Share dashboard.

The Share dashboard dashboard name page displays how the dashboard is being shared. If you want, you can stop sharing the dashboard by choosing Stop sharing.

Stop sharing one or more dashboards

You can stop sharing a single shared dashboard, or stop sharing all shared dashboards at once.
To stop sharing a single dashboard
2. In the navigation pane, choose Dashboards.
3. Choose the name of the shared dashboard.
5. Choose Stop sharing.
6. In the confirmation box, choose Stop sharing.

To stop sharing all shared dashboards
2. In the navigation pane, choose Settings.
3. In the Dashboard sharing section, choose Stop sharing all dashboards.
4. In the confirmation box, choose Stop sharing all dashboards.

Review shared dashboard permissions and change permission scope
Use the steps in this section if you want to review the permissions of the users of your shared dashboards, or change the scope of shared dashboard permissions.

To review shared dashboard permissions
2. In the navigation pane, choose Dashboards.
3. Choose the name of the shared dashboard.
5. Under Resources, choose IAM Role.
6. In the IAM console, choose the displayed policy.
7. (Optional) To limit which alarms that shared dashboard users can see, choose Edit policy and move the cloudwatch:DescribeAlarms permission from its current position to a new Allow statement that lists the ARNs of only the alarms that you want to be seen by shared dashboard users. See the following example.

```json
{
   "Effect": "Allow",
   "Action": "cloudwatch:DescribeAlarms",
   "Resource": [
      "AlarmARN1",
      "AlarmARN2"
   ]
}
```

If you do this, be sure to remove the cloudwatch:DescribeAlarms permission from a section of the current policy that looks like this:

```json
{
   "Effect": "Allow",
   "Action": [
      "cloudwatch:GetInsightRuleReport",
      ...
   ]
}
```
8. (Optional) To limit the scope of what Contributor Insights rules that shared dashboard users can see, choose Edit policy and move the `cloudwatch:GetInsightRuleReport` from its current position to a new Allow statement that lists the ARNs of only the Contributor Insights rules that you want to be seen by shared dashboard users. See the following example.

```
{
  "Effect": "Allow",
  "Action": [ "cloudwatch:GetInsightRuleReport",
              "PublicContributorInsightsRuleARN1",
              "PublicContributorInsightsRuleARN2"
            ],
  "Resource": "*"
}
```

If you do this, be sure to remove `cloudwatch:GetInsightRuleReport` from a section of the current policy that looks like this:

```
{
  "Effect": "Allow",
  "Action": [ "cloudwatch:GetInsightRuleReport",
              "cloudwatch:GetMetricData",
              "cloudwatch:DescribeAlarms",
              "ec2:DescribeTags"
            ],
  "Resource": "*"
}
```

Allowing people that you share with to see composite alarms

When you share a dashboard, by default the composite alarm widgets on the dashboard are not visible to the people who you share the dashboard with. For composite alarm widgets to be visible, you need to add a `DescribeAlarms: *` permission to the dashboard sharing policy. That permission would look like this:

```
{
  "Effect": "Allow",
  "Action": "cloudwatch:DescribeAlarms",
  "Resource": "*"
}
```

Warning

The preceding policy statement give access to all alarms in the account. To reduce the scope of `cloudwatch:DescribeAlarms`, you must use a Deny statement. You can add a Deny statement to the policy and specify the ARNs of the alarms that you want to lock down. That deny statement should look similar to the following:

```
{
  "Effect": "Deny",
  "Action": "cloudwatch:DescribeAlarms",
  "Resource": "PublicContributorInsightsRuleARN1",
  "PublicContributorInsightsRuleARN2"
}
```
Allowing people that you share with to see logs table widgets

When you share a dashboard, by default the CloudWatch Logs Insights widgets that are on the dashboard are not visible to the people who you share the dashboard with. This affects both CloudWatch Logs Insights widgets that exist now and any that are added to the dashboard after you share it.

If you want these people to be able to see CloudWatch Logs widgets, you must add permissions to the IAM role for dashboard sharing.

To allow the people that you share a dashboard with to see the CloudWatch Logs widgets

2. In the navigation pane, choose Dashboards.
3. Choose the name of the shared dashboard.
5. Under Resources, choose IAM Role.
6. In the IAM console, choose the displayed policy.
7. Choose Edit policy and add the following statement. In the new statement, we recommend that you specify the ARNs of only the log groups that you want shared. See the following example.

```json
{
    "Effect": "Allow",
    "Action": [ "logs:FilterLogEvents",
    "logs:StartQuery",
    "logs:StopQuery",
    "logs:GetLogRecord"
    ],
    "Resource": [ "SharedLogGroup1ARN",
    "SharedLogGroup2ARN"
    ]
}
```

8. Choose Save Changes.

If your IAM policy for dashboard sharing already includes those four permissions with * as the resource, we strongly recommend that you change the policy and specify only the ARNs of the log groups that you want shared. For example, if your Resource section for these permissions was the following:

```
"Resource": "*
```
Change the policy to specify only the ARNs of the log groups that you want shared, as in the following example:

```
"Resource": [
    "SharedLogGroup1ARN",
    "SharedLogGroup2ARN"
]
```

### Allowing people that you share with to see custom widgets

When you share a dashboard, by default the custom widgets that are on the dashboard are not visible to the people who you share the dashboard with. This affects both custom widgets that exist now and any that are added to the dashboard after you share it.

If you want these people to be able to see custom widgets, you must add permissions to the IAM role for dashboard sharing.

**To allow the people that you share a dashboard with to see the custom widgets**

2. In the navigation pane, choose **Dashboards**.
3. Choose the name of the shared dashboard.
4. Choose **Actions**, **Share dashboard**.
5. Under **Resources**, choose **IAM Role**.
6. In the IAM console, choose the displayed policy.
7. Choose **Edit policy** and add the following statement. In the new statement, we recommend that you specify the ARNs of only the Lambda functions that you want shared. See the following example.

```
{
    "Sid": "Invoke",
    "Effect": "Allow",
    "Action": [ 
        "lambda:InvokeFunction"
    ],
    "Resource": [ 
        "LambdaFunction1ARN",
        "LambdaFunction2ARN"
    ]
}
```

8. Choose **Save Changes**.

If your IAM policy for dashboard sharing already includes that permission with * as the resource, we strongly recommend that you change the policy and specify only the ARNs of the Lambda functions that you want shared. For example, if your **Resource** section for these permissions was the following:

```
"Resource": "*
```

Change the policy to specify only the ARNs of the custom widgets that you want shared, as in the following example:

```
"Resource": [ 
    "LambdaFunction1ARN",
    "LambdaFunction2ARN"
]
Use live data

You can choose whether your metric widgets display live data. Live data is data published within the last minute that has not been fully aggregated.

- If live data is turned off, only data points with an aggregation period of at least one minute in the past are shown. For example, when using 5-minute periods, the data point for 12:35 would be aggregated from 12:35 to 12:40, and displayed at 12:41.
- If live data is turned on, the most recent data point is shown as soon as any data is published in the corresponding aggregation interval. Each time you refresh the display, the most recent data point may change as new data within that aggregation period is published. If you use a cumulative statistic such as Sum or Sample Count, using live data may result in a dip at the end of your graph.

You can choose to enable live data for a whole dashboard, or for individual widgets on the dashboard.

To choose whether to use live data on your entire dashboard

2. In the navigation pane, choose Dashboards and select a dashboard.
3. To permanently turn live data on or off for all widgets on the dashboard, do the following:
   a. Choose Actions, Settings, Bulk update live data.
   b. Choose Live Data on or Live Data off, and choose Set.
4. To temporarily override the live data settings of each widget, choose Actions. Then, under Overrides, next to Live data, do one of the following:
   - Choose On to temporarily turn on live data for all widgets.
   - Choose Off to temporarily turn off live data for all widgets.
   - Choose Do not override to preserve each widget's live data setting.

To choose whether to use live data on a single widget

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Select a widget, and choose Actions, Edit.
4. Choose the Graph options tab.
5. Select or clear the check box under Live Data.

Viewing an animated dashboard

You can view an animated dashboard that replays CloudWatch metric data that was captured over time. This can help you see trends, make presentations, or analyze issues after they occur.

Animated widgets in the dashboard include line widgets, stacked area widgets, number widgets, and metrics explorer widgets. Pie graphs, bar charts, text widgets, and logs widgets are displayed in the dashboard but are not animated.
To view an animated dashboard
2. In the navigation pane, choose Dashboards.
3. Choose the name of the dashboard.
4. Choose Actions, Replay dashboard.
5. (Optional) By default, when you start the animation, it appears as a sliding window. If you want the animation to appear as a point-by-point animation instead, choose the magnifying glass icon while the animation is paused and reset the zoom.
6. To start the animation, choose the Play button. You can also choose the back and forward buttons to move to other points in time.
7. (Optional) To change the time window for the animation, choose the calendar and select the time period.
8. To change the speed of the animation, choose Auto speed and select the new speed.
9. When you are finished, choose Exit animate.

Add a dashboard to your Favorites list

You can add a CloudWatch dashboard to a list of favorite dashboards to help you find it quickly. The Favorites list appears at the bottom of the navigation pane.

To add a dashboard to the Favorites list
2. In the navigation pane, choose Dashboards.
3. Select the star symbol next to the dashboard to add it.

Change the period override setting or refresh interval for the CloudWatch dashboard

You can specify how the period setting of graphs added to this dashboard are retained or modified.

To change the period override options
2. Choose Actions.
3. Under Period override, choose one of the following:
   - Choose Auto to have the period of the metrics on each graph automatically adapt to the dashboard’s time range.
   - Choose Do not override to ensure that the period setting of each graph is always obeyed.
   - Choose one of the other options to cause graphs added to the dashboard to always adapt that chosen time as their period setting.

The Period override always reverts to Auto when the dashboard is closed or the browser is refreshed. Different settings for Period override can’t be saved.
You can change how often the data on your CloudWatch dashboard is refreshed or set it to automatically refresh.

**To change the dashboard refresh interval**

2. In the navigation pane, choose **Dashboards** and select a dashboard.
3. On the **Refresh options** menu (upper-right corner), choose 10 Seconds, 1 Minute, 2 Minutes, 5 Minutes, or 15 Minutes.

**To automatically refresh the dashboard**

2. In the navigation pane, choose **Dashboards** and select a dashboard.
3. Choose **Refresh options** and then **Auto refresh**.

### Change the time range or time zone format of a CloudWatch dashboard

You can change the time range to display dashboard data over minutes, hours, days, or weeks. You can also change the time format to display dashboard data in UTC or local time. Local time is the time zone specified as your local time zone in the operating system of the computer you are using to view the CloudWatch console.

**Note**

If you create a dashboard with graphs that contain close to 100 or more high-resolution metrics, we recommend that you set the time range to no longer than one hour to ensure good dashboard performance. For more information about high-resolution metrics, see High-resolution metrics (p. 74).

**To change the dashboard time range**

2. In the navigation pane, choose **Dashboards** and select a dashboard.
3. Do one of the following:
   - Select one of the predefined ranges shown, which span from 1 hour to 1 week: 1h, 3h, 12h, 1d, 3d, or 1w.
   - Choose **custom** and then **Relative**. Select one of the predefined ranges, which span from 1 minute to 15 months.
   - Choose **custom** and then **Absolute**. Use the calendar picker or the text fields to specify the time range.

**Note**

When you change the time range of a graph while the aggregation period is set to **Auto**, CloudWatch might change the period. To manually set the period, choose **Actions** and select a new value for **Period**.

**To change the dashboard time format**

2. In the navigation pane, choose **Dashboards** and select a dashboard.
3. Choose custom.
4. From the upper corner, choose UTC or Local timezone.
Using Amazon CloudWatch metrics

Metrics are data about the performance of your systems. By default, many services provide free metrics for resources (such as Amazon EC2 instances, Amazon EBS volumes, and Amazon RDS DB instances). You can also enable detailed monitoring for some resources, such as your Amazon EC2 instances, or publish your own application metrics. Amazon CloudWatch can load all the metrics in your account (both AWS resource metrics and application metrics that you provide) for search, graphing, and alarms.

Metric data is kept for 15 months, enabling you to view both up-to-the-minute data and historical data.

Contents

• Viewing available metrics (p. 51)
• Searching for available metrics (p. 54)
• Getting statistics for a metric (p. 55)
• Graphing metrics (p. 66)
• Publishing custom metrics (p. 74)
• Using metric math (p. 77)
• Using search expressions in graphs (p. 91)

Viewing available metrics

Metrics are grouped first by namespace, and then by the various dimension combinations within each namespace. For example, you can view all EC2 metrics, EC2 metrics grouped by instance, or EC2 metrics grouped by Auto Scaling group.

Only the AWS services that you’re using send metrics to Amazon CloudWatch.

For a list of AWS services that send metrics to CloudWatch, see AWS services that publish CloudWatch metrics (p. 658). From this page, you can also see the metrics and dimensions that are published by each of those services.

Note
Metrics that have not had any new data points in the past two weeks do not appear in the console. They also do not appear when you type their metric name or dimension names in the search box in the All metrics tab in the console, and they are not returned in the results of a list-metrics command. The best way to retrieve these metrics is with the get-metric-data or get-metric-statistics commands in the AWS CLI.

If the old metric you want to view has a current metric with similar dimensions, you can view that current similar metric and then choose the Source tab, and change the metric name and dimension fields to the ones that you want, and also change the time range to a time when the metric was being reported.

To view available metrics by namespace and dimension using the console

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**.
6. (Optional) To add this graph to a CloudWatch dashboard, choose **Actions, Add to dashboard**.

**To view available metrics by namespace, dimension, or metric using the AWS CLI**

Use the `list-metrics` command to list CloudWatch metrics. For a list of the namespaces, metrics, and dimensions for all services that publish metrics, see [AWS services that publish CloudWatch metrics](p. 658).

The following example specifies the **AWS/EC2** namespace to view all the metrics for Amazon EC2.

```
aws cloudwatch list-metrics --namespace AWS/EC2
```

The following is example output.

```json
{
  "Metrics": [ 
    ...
    {
      "Namespace": "AWS/EC2",
      "Dimensions": [
        {
          "Name": "InstanceId",
          "Value": "i-1234567890abcdef0"
        }
      ],
      "MetricName": "NetworkOut"
    },
    {
      "Namespace": "AWS/EC2",
      "Dimensions": [
        {
          "Name": "InstanceId",
          "Value": "i-1234567890abcdef0"
        }
      ],
      "MetricName": "CPUUtilization"
    }
  ]
}
```
Searching for available metrics

You can search within all of the metrics in your account using targeted search terms. Metrics are returned that have matching results within their namespace, metric name, or dimensions.

**Note**
Metrics that have not had any new data points in the past two weeks do not appear in the console. They also do not appear when you type their metric name or dimension names in the search box in the All metrics tab in the console, and they are not returned in the results of a list-metrics command. The best way to retrieve these metrics is with the get-metric-data or get-metric-statistics commands in the AWS CLI.

**To search for available metrics in CloudWatch**

2. In the navigation pane, choose **Metrics**.
3. In the search field on the **All metrics** tab, enter a search term, such as a metric name, namespace, dimension name or value, or resource name. This shows you all of the namespaces with metrics with this search term.

   For example, if you search for **volume**, this shows the namespaces that contain metrics with this term in their name.

   For more information on search, see **Using search expressions in graphs** (p. 91)
4. To graph all the search results, choose **Graph search**
   
   or

   Select a namespace to view the metrics from that namespace. You can then do the following:
a. To graph one or more metrics, select the check box next to each metric. To select all metrics, select the check box in the heading row of the table.
b. To refine your search, hover over a metric name and choose **Add to search** or **Search for this only**.
c. To view one of the resources on its console, choose the resource ID and then choose **Jump to resource**.
d. To view help for a metric, select the metric name and choose **What is this?**.

The selected metrics appear on the graph.

5. (Optional) Select one of the buttons in the search bar to edit that part of the search term.

## Getting statistics for a metric

### CloudWatch statistics definitions

Statistics are metric data aggregations over specified periods of time. When you graph or retrieve the statistics for a metric, you specify the **Period** of time, such as five minutes, to use to calculate each statistical value. For example, if the **Period** is five minutes, the **Sum** is the sum of all sample values collected during the five-minute period, while the **Minimum** is the lowest value collected during the five-minute period.

CloudWatch supports the following statistics for metrics.

- **SampleCount** is the number of data points during the period.
- **Sum** is sum of the values of the all data points collected during the period.
- **Average** is the value of Sum/SampleCount during the specified period.
- **Minimum** is the lowest value observed during the specified period.
- **Maximum** is the highest value observed during the specified period.
- **Percentile (p)** indicates the relative standing of a value in a dataset. For example, p95 is the 95th percentile and means that 95 percent of the data within the period is lower than this value and 5
percent of the data is higher than this value. Percentiles help you get a better understanding of the
distribution of your metric data.

- **Trimmed mean (TM)** is the mean of all values that are between two specified boundaries. Values outside of the boundaries are ignored when the mean is calculated. You define the boundaries as one or two numbers between 0 and 100, up to 10 decimal places. The numbers can be absolute values or percentages. For example, **tm90** calculates the average after removing the 10% of data points with the highest values. **TM(2%;:98%)** calculates the average after removing the 2% lowest data points and the 2% highest data points. **TM(150:1000)** calculates the average after removing all data points that are lower than or equal to 150, or higher than 1000.

- **Interquartile mean (IQM)** is the trimmed mean of the interquartile range, or the middle 50% of values. It is equivalent to **TM(25%;75%)**.

- **Winsorized mean (WM)** is similar to trimmed mean. However, with winsorized mean, the values that are outside the boundary are not ignored, but instead are considered to be equal to the value at the edge of the appropriate boundary. After this normalization, the average is calculated. You define the boundaries as one or two numbers between 0 and 100, up to 10 decimal places. For example, **wm98** calculates the average while treating the 2% of the highest values to be equal to the value at the 98th percentile. **WM(10%;90%)** calculates the average while treating the highest 10% of data points to be the value of the 90% boundary, and treating the lowest 10% of data points to be the value of the 10% boundary.

- **Percentile rank (PR)** is the percentage of values that meet a fixed threshold. For example, **PR(=300)** returns the percentage of data points that have a value of 300 or less. **PR(100;2000)** returns the percentage of data points that have a value between 100 and 2000.

- **Trimmed count (TC)** is the number of data points in the chosen range for a trimmed mean statistic. For example, **tc90** returns the number of data points not including any data points that fall in the highest 10% of the values. **TC(0.005;0.030)** returns the number of data points with values between 0.005 (exclusive) and 0.030 (inclusive).

- **Trimmed sum (TS)** is the sum of the values of data points in a chosen range for a trimmed mean statistic. It is equivalent to (Trimmed Mean) * (Trimmed count). For example, **ts90** returns the sum of the data points not including any data points that fall in the highest 10% of the values. **TS(80%;:)** returns the sum of the data point values, not including any data points with values in the lowest 80% of the range of values.

**Note**
For Trimmed Mean, Trimmed Count, Trimmed Sum, and Winsorized Mean, if you define two boundaries as fixed values instead of percentages, the calculation includes values equal to the higher boundary, but does not include values equal to the lower boundary.

**Syntax**
For Trimmed Mean, Trimmed Count, Trimmed Sum, and Winsorized Mean, the following syntax rules apply:

- Using parentheses with one or two numbers with percent signs defines the boundaries to use as the values in the data set that fall in between the two percentiles that you specify. For example, **TM(10%;90%)** uses only the values between the 10th and 90th percentiles. **TM(:95%)** uses the values from the lowest end of the data set up to the 95th percentile, ignoring the 5% of data points with the highest values.

- Using parentheses with one or two numbers without percent signs defines the boundaries to use as the values in the data set that fall in between the explicit values that you specify. For example, **TC(80;500)** uses only the values that are between 80 (exclusive) and 500 (inclusive). **TC(0.5)** uses only the values that equal 0.5 or are lower.

- Using one number without parentheses calculates using percentages, ignoring data points that are higher than the specified percentile. For example, **tm99** calculates the mean while ignoring the 1% of the data points with the highest value. It is the same as **TM(99%)**.
• Trimmed mean, Trimmed Count, Trimmed Sum, and Winsorized Mean can all be abbreviated using uppercase letters when specifying a range, such as \text{TM}(5\%:95\%), \text{TM}(100:200), or \text{TM}(95\%). They can only be abbreviated using lowercase letters when you specifying only one number, such as \text{tm}99.

Statistics use cases

• **Trimmed mean** is most useful for metrics with a large sample size, such as webpage latency. For example, \text{tm}99 disregards extreme high outliers that could result from network problems or human errors, to give a more accurate number for the average latency of typical requests. Similarly, \text{TM}(10\%:) disregards the lowest 10\% of latency values, such as those resulting from cache hits. And \text{TM}(10\%:99\%) excludes both of these types of outliers.

• It is a good idea to keep watch on trimmed count whenever you are using trimmed mean, to make sure that the number of values being used in your trimmed mean calculations are enough to be statistically significant.

• Percentile rank enables you to put values into "bins" of ranges, and you can use this to manually create a histogram. To do this, break your values down into various bins, such as \text{PR}(:1), \text{PR}(1:5), \text{PR}(5:10), and \text{PR}(10:). Put each of these bins into a visualization as bar charts, and you have a histogram.

Percentiles versus trimmed mean

A percentile such as \text{p}99 and a trimmed mean such as \text{tm}99 measure similar, but not identical values. Both \text{p}99 and \text{tm}99 ignore the 1\% of the data points with the highest values, which are considered outliers. After that, \text{p}99 is the maximum value of the remaining 99\%, while \text{tm}99 is the average of the remaining 99\%. If you are looking at the latency of web requests, \text{p}99 tells you the worst customer experience, ignoring outliers, while \text{tm}99 tells you the average customer experience, ignoring outliers.

Trimmed mean is a good latency statistic to watch if you are looking to optimize your customer experience. For alarming on latency, we recomend to use a percentile statistic, to receive alerts early if there is an issue that leads to a partial loss of service.

Requirements to use percentiles, trimmed mean, and some other statistics

CloudWatch needs raw data points to calculate the following statistics:

• Percentiles
• Trimmed mean
• Interquartile mean
• Winsorized mean
• Trimmed sum
• Trimmed count
• Percentile rank

If you publish data for a custom statistics using a statistic set instead of raw data, you can retrieve these types of statistics for this data only if one of the following conditions is true:

• The SampleCount value of the statistic set is 1 and Min, Max, and Sum are all equal.
• The Min and Max are equal, and Sum is equal to Min multiplied by SampleCount.

The following AWS services include metrics that support these types of statistics.
• API Gateway
• Application Load Balancer
• Amazon EC2
• Elastic Load Balancing
• Kinesis
• Amazon RDS

Additionally, these type of statistics are not available for metrics when any of the metric values are negative numbers.

The following examples show you how to get statistics for the CloudWatch metrics for your resources, such as your EC2 instances.

Examples
• Getting statistics for a specific resource (p. 58)
• Aggregating statistics across resources (p. 61)
• Aggregating statistics by Auto Scaling group (p. 63)
• Aggregating statistics by Amazon Machine Image (AMI) (p. 64)

Getting statistics for a specific resource

The following example shows you how to determine the maximum CPU utilization of a specific EC2 instance.

Requirements
• You must have the ID of the instance. You can get the instance ID using the Amazon EC2 console or the describe-instances command.
• By default, basic monitoring is enabled, but you can enable detailed monitoring. For more information, see Enable or Disable Detailed Monitoring for Your Instances in the Amazon EC2 User Guide for Linux Instances.

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

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, enter **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, **p99.999**).

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 get the CPU utilization per EC2 instance using the AWS CLI**

Use the `get-metric-statistics` command as follows to get the `CPUUtilization` metric for the specified instance.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization --dimensions Name=InstanceId,Value=i-1234567890abcdef0 --statistics Maximum
```
The returned statistics are 6-minute values for the requested 24-hour time interval. Each value represents the maximum CPU utilization percentage for the specified instance for a particular 6-minute time period. The data points aren't returned in chronological order. The following shows the beginning of the example output (the full output includes data points for every 6 minutes of the 24-hour period).

```
{
  "Datapoints": [
    {
      "Timestamp": "2016-10-19T00:18:00Z",
      "Maximum": 0.33000000000000002,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2016-10-19T03:18:00Z",
      "Maximum": 99.670000000000002,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2016-10-19T07:18:00Z",
      "Maximum": 0.34000000000000002,
      "Unit": "Percent"
    },
    ...
  ],
  "Label": "CPUUtilization"
}
```

### Aggregating statistics across resources

You can aggregate the metrics for AWS resources across multiple resources. Metrics are completely separate between Regions, but you can use metric math to aggregate similar metrics across Regions. For more information, see Using metric math (p. 77).

For example, you can aggregate statistics for your EC2 instances that have detailed monitoring enabled. Instances that use basic monitoring aren't included. Therefore, you must enable detailed monitoring (at an additional charge), which provides data in 1-minute periods. For more information, see Enable or Disable Detailed Monitoring for Your Instances in the Amazon EC2 User Guide for Linux Instances.

This example shows you how to get the average CPU usage for your EC2 instances. Because no dimension is specified, CloudWatch returns statistics for all dimensions in the AWS/EC2 namespace. To get statistics for other metrics, see AWS services that publish CloudWatch metrics (p. 658).

**Important**

This technique for retrieving all dimensions across an AWS namespace doesn't work for custom namespaces that you publish to CloudWatch. With custom namespaces, you must specify the complete set of dimensions that are associated with any given data point to retrieve statistics that include the data point.

To display average CPU utilization for your EC2 instances

2. In the navigation pane, choose **Metrics**.
3. Choose the **EC2** namespace and choose **Across All Instances**.
4. Select the row that contains **CPUUtilization**, which displays a graph for the metric for all your EC2 instances. 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**.
5. 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`).

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

**To get average CPU utilization across your EC2 instances using the AWS CLI**

Use the `get-metric-statistics` command as follows:

```bash
calculations
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization --statistics "Average" "SampleCount" \ --start-time 2016-10-11T23:18:00 --end-time 2016-10-12T23:18:00 --period 3600
```

The following is example output:

```
{
    "Datapoints": [
        {
            "SampleCount": 238.0,
            "Timestamp": "2016-10-12T07:18:00Z",
            "Average": 0.038235294117647062,
            "Unit": "Percent"
        },
        {
            "SampleCount": 240.0,
            "Timestamp": "2016-10-12T09:18:00Z",
            "Average": 0.16670833333333332,
            "Unit": "Percent"
        },
        {
            "SampleCount": 238.0,
            "Timestamp": "2016-10-11T23:18:00Z",
            "Average": 0.041596638655462197,
            "Unit": "Percent"
        }
    ]
}
```
Aggregating statistics by Auto Scaling group

You can aggregate statistics for the EC2 instances in an Auto Scaling group. Metrics are completely separate between Regions, but you can use CloudWatch metric math to aggregate and transform metrics from multiple Regions. You can also use the cross-account dashboard to perform metric math on metrics from different accounts.

This example shows you how to get the total bytes written to disk for one Auto Scaling group. The total is computed for 1-minute periods for a 24-hour interval across all EC2 instances in the specified Auto Scaling group.

To display DiskWriteBytes for the instances in an Auto Scaling group using the console

2. In the navigation pane, choose Metrics.
3. Choose the EC2 namespace and then choose By Auto Scaling Group.
4. Select the row for the DiskWriteBytes metric and the specific Auto Scaling group, which displays a graph for the metric for the instances in the Auto Scaling group. 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.

5. 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).
6. To change the period, choose the Graphed metrics tab. Choose the column heading or an individual value and then choose a different value.

To get DiskWriteBytes for the instances in an Auto Scaling group using the AWS CLI

Use the `get-metric-statistics` command as follows.
Aggregating statistics by Amazon Machine Image (AMI)

You can aggregate statistics for the EC2 instances that have detailed monitoring enabled. Instances that use basic monitoring aren't included. For more information, see Enable or Disable Detailed Monitoring for Your Instances in the Amazon EC2 User Guide for Linux Instances.

This example shows you how to determine average CPU utilization for all instances that use the specified AMI. The average is over 60-second time intervals for a one-day period.

To display the average CPU utilization by AMI using the console

2. In the navigation pane, choose Metrics.
3. Choose the EC2 namespace and then choose By Image (AMI) Id.
4. Select the row for the CPUUtilization metric and the specific AMI, which displays a graph for the metric for the specified AMI. 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.
5. 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, \textit{p95.45}).

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

**To get the average CPU utilization by AMI using the AWS CLI**

Use the \texttt{get-metric-statistics} command as follows.

```
aws cloudwatch get-metric-statistics --namespace AWS/EC2 --metric-name CPUUtilization \ 
--dimensions Name=ImageId,Value=ami-3c47a355 --statistics Average \ 
--start-time 2016-10-10T00:00:00 --end-time 2016-10-11T00:00:00 --period 3600
```

The operation returns statistics that are one-hour values for the one-day interval. Each value represents an average CPU utilization percentage for EC2 instances running the specified AMI. The following is example output.

```
{
  "Datapoints": [
    {
      "Timestamp": "2016-10-10T07:00:00Z",
      "Average": 0.041000000000000009,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2016-10-10T14:00:00Z",
      "Average": 0.079579831932773085,
      "Unit": "Percent"
    },
    {
      "Timestamp": "2016-10-10T06:00:00Z",
      "Average": 0.036000000000000011,
      "Unit": "Percent"
    },
    ...]
  "Label": "CPUUtilization"
}
```
Graphing metrics

Use the CloudWatch console to graph metric data generated by other AWS services. This makes it more efficient to see the metric activity on your services. The following procedures describe how to graph metrics in CloudWatch.

Contents
- Graphing a metric (p. 66)
- Using dynamic labels (p. 69)
- Modifying the time range or time zone format for a graph (p. 71)
- Modifying the y-axis for a graph (p. 72)
- Creating an alarm from a metric on a graph (p. 73)

Graphing a metric

You can select metrics and create graphs of the metric data using the CloudWatch console.

CloudWatch supports the following statistics on metrics: Average, Minimum, Maximum, Sum, and SampleCount. For more information, see Statistics (p. 5).

You can view your data at different levels of detail. For example, you can choose a one-minute view, which can be useful when troubleshooting. Or, choose a less detailed, one-hour view. That can be useful when viewing a broader time range (for example, 3 days) so that you can see trends over time. For more information, see Periods (p. 6).

Creating a graph

To graph a metric

2. In the navigation pane, choose Metrics.
3. On the All metrics tab, enter a search term in the search field, such as a metric name or resource name, and press Enter.

   For example, if you search for the CPUUtilization metric, you see the namespaces and dimensions with this metric.
4. Select one of the results for your search to view the metrics.
5. To graph one or more metrics, select the check box next to each metric. To select all metrics, select the check box in the heading row of the table.
6. Choose View graphed metrics.
7. (Optional) To change the statistic used in the graph, choose the new statistic in the Statistic column next to the metric name.

   For more information about CloudWatch statistics, see CloudWatch statistics definitions (p. 55).
   For more information about the pxx percentile statistics, see Percentiles (p. 7).
8. (Optional) To change the type of graph, choose Graph options. You can then choose between a line graph, stacked area chart, bar chart, pie chart, or number.
9. (Optional) To add an anomaly detection band that shows expected values for the metric, choose the anomaly detection icon under Actions next to the metric.
Graphing a metric

CloudWatch uses up to two weeks of the metric's recent historical data to calculate a model for expected values. It then displays this range of expected values as a band on the graph. CloudWatch adds a new row under the metric to display the anomaly detection band math expression, labeled ANOMALY_DETECTION_BAND. If recent historical data exists, you immediately see a preview anomaly detection band, which is an approximation of the anomaly detection band generated by the model. It takes up to 15 minutes for the actual anomaly detection band to appear.

By default, CloudWatch creates the upper and lower bounds of the band of expected values with a default value of 2 for the band threshold. To change this number, change the value at the end of the formula under Details for the band.

- (Optional) Choose Edit model to change how the anomaly detection model is calculated. You can exclude past and future time periods from being used in the training for calculating the model. It is critical to exclude unusual events system as system outage, deployments, and holidays from the training data. You can also specify the time zone to use for the model for daylight saving time changes.

For more information, see Using CloudWatch anomaly detection (p. 247).

To hide the model from the graph, remove the checkmark from the line with the ANOMALY_DETECTION_BAND function or choose the X icon. To delete the model entirely, choose Edit model, Delete model.

10. (Optional) As you choose metrics to graph, specify a dynamic label to appear on the graph legend for each metric. Dynamic labels display a statistic about the metric, and automatically update when
the dashboard or graph is refreshed. To add a dynamic label, choose Graphed metrics, Dynamic labels.

By default, the dynamic values that you add to the label appear at the beginning of the label. You can then choose the Label value for the metric to edit the label. For more information, see Using dynamic labels (p. 69).

11. To view more information about the metric being graphed, pause the mouse over the legend.

12. Horizontal annotations can help graph users more efficiently 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 and then Add horizontal annotation:

   a. For Label, enter a label for the annotation.
   b. For Value, enter 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 check box in the left column for that annotation.

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

13. To get a URL for your graph, choose Actions, Share. Copy the URL to save or share.

14. To add your graph to a dashboard, choose Actions, Add to dashboard.

**Updating a graph**

To update your graph

1. To change the name of the graph, choose the pencil icon.
2. To change the time range, select one of the predefined values or choose custom. For more information, see Modifying the time range or time zone format for a graph (p. 71).
3. 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).
4. To change the period, choose the Graphed metrics tab. Choose the column heading or an individual value and then choose a different value.
5. To add a horizontal annotation, choose Graph options and then Add horizontal annotation:
   a. For Label, enter a label for the annotation.
   b. For Value, enter 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 check box in the left column for that annotation.

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

6. To change the refresh interval, choose Refresh options and then select Auto refresh or choose 1 Minute, 2 Minutes, 5 Minutes, or 15 Minutes.

**Duplicating a metric**

*To duplicate a metric*

1. Choose the Graphed metrics tab.
2. For Actions, choose the Duplicate icon.

3. Update the duplicate metric as needed.

**Using dynamic labels**

You can use dynamic labels with your graphs. Dynamic labels add a dynamically updated value to the label for the selected metric. You can add a wide range of values to the labels, as shown in the following tables.

The dynamic value shown in the label is derived from the time range currently shown on the graph. The dynamic part of the label automatically updates when either the dashboard or the graph is refreshed.

If you use a dynamic label with a search expression, the dynamic label applies to every metric returned by the search.

You can use the CloudWatch console to add a dynamic value to a label, edit the label, change the position of the dynamic value within the label column, and make other customizations.

**Dynamic labels**

Within a dynamic label, you can use the following values relating to properties of the metric:

<table>
<thead>
<tr>
<th>Dynamic label live value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>${AVG}</td>
<td>The average of the values in the time range currently shown in the graph.</td>
</tr>
<tr>
<td>${DATAPoint_COUNT}</td>
<td>The number of data points in the time range that is currently shown in the graph.</td>
</tr>
<tr>
<td>Dynamic label live value</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>${FIRST}</td>
<td>The oldest of the metric values in the time range that is currently shown in the graph.</td>
</tr>
<tr>
<td>${FIRST_LAST_RANGE}</td>
<td>The difference between the metric values of the oldest and newest data points that are currently shown in the graph.</td>
</tr>
<tr>
<td>${FIRST_LAST_TIME_RANGE}</td>
<td>The absolute time range between the oldest and newest data points that are currently shown in the graph.</td>
</tr>
<tr>
<td>${FIRST_TIME}</td>
<td>The timestamp of the oldest data point in the time range that is currently shown in the graph.</td>
</tr>
<tr>
<td>${FIRST_TIME_RELATIVE}</td>
<td>The absolute time difference between now and the timestamp of the oldest data point in the time range that is currently shown in the graph.</td>
</tr>
<tr>
<td>${LABEL}</td>
<td>The representation of the default label for a metric.</td>
</tr>
<tr>
<td>${LAST}</td>
<td>The most recent of the metric values in the time range that is currently shown in the graph.</td>
</tr>
<tr>
<td>${LAST_TIME}</td>
<td>The timestamp of the newest data point in the time range that is currently shown in the graph.</td>
</tr>
<tr>
<td>${LAST_TIME_RELATIVE}</td>
<td>The absolute time difference between now and the timestamp of the newest data point in the time range that is currently shown in the graph.</td>
</tr>
<tr>
<td>${MAX}</td>
<td>The maximum of the values in the time range currently shown in the graph.</td>
</tr>
<tr>
<td>${MAX_TIME}</td>
<td>The timestamp of the data point that has the highest metric value, of the data points that are currently shown in the graph.</td>
</tr>
<tr>
<td>${MAX_TIME_RELATIVE}</td>
<td>The absolute time difference between now and the timestamp of the data point with the highest value, of those data points that are currently shown in the graph.</td>
</tr>
<tr>
<td>${MIN}</td>
<td>The minimum of the values in the time range currently shown in the graph.</td>
</tr>
<tr>
<td>${MIN_MAX_RANGE}</td>
<td>The difference in metric values between the data points with the highest and lowest metric values, of those data points that are currently shown in the graph.</td>
</tr>
<tr>
<td>${MIN_MAX_TIME_RANGE}</td>
<td>The absolute time range between the data points with the highest and lowest metric values, of those data points that are currently shown in the graph.</td>
</tr>
<tr>
<td>${MIN_TIME}</td>
<td>The timestamp of the data point that has the lowest metric value, of the data points that are currently shown in the graph.</td>
</tr>
<tr>
<td>${MIN_TIME_RELATIVE}</td>
<td>The absolute time difference between now and the timestamp of the data point with the lowest value, of those data points that are currently shown in the graph.</td>
</tr>
<tr>
<td>${PROP('AccountId')}</td>
<td>The AWS account ID of the metric.</td>
</tr>
</tbody>
</table>
Dynamic label live value | Description
--- | ---
${PROP('Dim.' + dimension_name)} | The value of the specified dimension.
${PROP('MetricName')} | The name of the metric.
${PROP('Namespace')} | The namespace of the metric.
${PROP('Period')} | The period of the metric, in seconds.
${PROP('Region')} | The AWS Region where the metric is published.
${PROP('Stat')} | The metric statistic that is being graphed.
${SUM} | The sum of the values in the time range currently shown in the graph.

For example, suppose you have a search expression `SEARCH(' {AWS/Lambda, FunctionName} Errors ', 'Sum', 300)`, which finds the Errors for each of your Lambda functions. If you set the label to be `[max: ${MAX} Errors for Function Name ${LABEL}]`, the label for each metric is `[max: number Errors for Function Name Name]`.

You can add up to five dynamic values to a label. You can use the ${LABEL} placeholder only once within each label.

**Modifying the time range or time zone format for a graph**

You can change the time range or the time zone format of a graph.

**Setting a relative time range**

You can set a relative time range for your graph.

To specify a relative time range for a graph

2. In the navigation pane, choose Metrics.
3. Select one of the predefined ranges shown at the top of the page, which span from 1 hour to 1 week ago.
4. For more predefined ranges, choose the custom menu and then choose Relative. Select one of the predefined ranges, which span from 5 minutes to 15 months ago.

**Setting an absolute time range**

You can set an absolute time range for your graph.

To specify an absolute time range for a graph

2. In the navigation pane, choose Metrics.
3. Choose the custom menu and then choose Absolute. Use the calendar picker or the text fields to specify the time range.
Setting the time zone format

You can specify whether the graph uses UTC time or your local time.

**To specify the time zone for a graph**

2. In the navigation pane, choose Metrics.
3. Choose the custom menu and then choose UTC or Local timezone.

Zooming in on a graph

You can change the granularity of a graph and zoom in to see data over a shorter time period.

**To zoom in on a graph**

2. In the navigation pane, choose Metrics.
3. Choose and drag on the graph area and then release the drag.
4. To reset a zoomed-in graph, choose the Reset zoom icon.

Modifying the y-axis for a graph

You can set custom bounds for the y-axis on a graph to help you see the data better. For example, you can change the bounds on a CPUUtilization graph to 100 percent so that it’s easy to see whether the CPU is low (the plotted line is near the bottom of the graph) or high (the plotted line is near the top of the graph).

You can switch between two different y-axes for your graph. This is useful if the graph contains metrics that have different units or that differ greatly in their range of values.

**To modify the y-axis on a graph**

2. In the navigation pane, choose Metrics.
3. Select a metric namespace (for example, EC2) and then a metric dimension (for example, Per-Instance Metrics).
4. The All metrics tab displays all metrics for that dimension in that namespace. To graph a metric, select the check box next to the metric.
5. On the Graph options tab, specify the Min and Max values for Left Y Axis. The value of Min can't be greater than the value of Max.
Creating an alarm from a metric on a graph

You can graph a metric and then create an alarm from the metric on the graph, which has the benefit of populating many of the alarm fields for you.

To create an alarm from a metric on a graph

2. In the navigation pane, choose Metrics.
3. Select a metric namespace (for example, EC2) and then a metric dimension (for example, Per-Instance Metrics).
4. The All metrics tab displays all metrics for that dimension in that namespace. To graph a metric, select the check box next to the metric.
5. To create an alarm for the metric, choose the Graphed metrics tab. For Actions, choose the alarm icon.

6. Under Conditions, choose Static or Anomaly detection to specify whether to use a static threshold or anomaly detection model for the alarm.

Depending on your choice, enter the rest of the data for the alarm conditions.

7. Choose Additional configuration. For Datapoints to alarm, specify how many evaluation periods (data points) must be in the ALARM state to trigger the alarm. If the two values here match, you create an alarm that goes to ALARM state if that many consecutive periods are breaching.
To create an M out of N alarm, specify a lower number for the first value than you specify for the second value. For more information, see Evaluating an alarm (p. 103).

8. For Missing data treatment, choose how to have the alarm behave when some data points are missing. For more information, see Configuring how CloudWatch alarms treat missing data (p. 104).

9. Choose Next.

10. Under Notification, select an SNS topic to notify when the alarm is in ALARM state, OK state, or INSUFFICIENT_DATA state.

   To have the alarm send multiple notifications for the same alarm state or for different alarm states, choose Add notification.

   To have the alarm not send notifications, choose Remove.

11. To have the alarm perform Auto Scaling or EC2 actions, choose the appropriate button and choose the alarm state and action to perform.

12. When finished, choose Next.

13. Enter a name and description for the alarm. The name must contain only ASCII characters. Then choose Next.

14. Under Preview and create, confirm that the information and conditions are what you want, then choose Create alarm.

### Publishing custom metrics

You can publish your own metrics to CloudWatch using the AWS CLI or an API. You can view statistical graphs of your published metrics with the AWS Management Console.

CloudWatch stores data about a metric as a series of data points. Each data point has an associated time stamp. You can even publish an aggregated set of data points called a statistic set.

**Topics**

- High-resolution metrics (p. 74)
- Using dimensions (p. 75)
- Publishing single data points (p. 75)
- Publishing statistic sets (p. 76)
- Publishing the value zero (p. 77)

### High-resolution metrics

Each metric is one of the following:

- Standard resolution, with data having a one-minute granularity
- High resolution, with data at a granularity of one second

Metrics produced by AWS services are standard resolution by default. When you publish a custom metric, you can define it as either standard resolution or high resolution. When you publish a high-resolution metric, CloudWatch stores it with a resolution of 1 second, and you can read and retrieve it with a period of 1 second, 5 seconds, 10 seconds, 30 seconds, or any multiple of 60 seconds.
High-resolution metrics can give you more immediate insight into your application's sub-minute activity. Keep in mind that every `PutMetricData` call for a custom metric is charged, so calling `PutMetricData` more often on a high-resolution metric can lead to higher charges. For more information about CloudWatch pricing, see Amazon CloudWatch Pricing.

If you set an alarm on a high-resolution metric, you can specify a high-resolution alarm with a period of 10 seconds or 30 seconds, or you can set a regular alarm with a period of any multiple of 60 seconds. There is a higher charge for high-resolution alarms with a period of 10 or 30 seconds.

### Using dimensions

In custom metrics, the `--dimensions` parameter is common. A dimension further clarifies what the metric is and what data it stores. You can have up to 10 dimensions in one metric, and each dimension is defined by a name and value pair.

How you specify a dimension is different when you use different commands. With `put-metric-data`, you specify each dimension as `MyName=MyValue`, and with `get-metric-statistics` or `put-metric-alarm` you use the format `Name=Value`. For example, the following command publishes a `Buffers` metric with two dimensions named `InstanceId` and `InstanceType`.

```bash
aws cloudwatch put-metric-data --metric-name Buffers --namespace MyNameSpace --unit Bytes --value 231434333 --dimensions InstanceId=1-23456789,InstanceType=m1.small
```

This command retrieves statistics for that same metric. Separate the Name and Value parts of a single dimension with commas, but if you have multiple dimensions, use a space between one dimension and the next.

```bash
aws cloudwatch get-metric-statistics --metric-name Buffers --namespace MyNameSpace --dimensions Name=InstanceId,Value=1-23456789 Name=InstanceType,Value=m1.small --start-time 2016-10-15T04:00:00Z --end-time 2016-10-19T07:00:00Z --statistics Average --period 60
```

If a single metric includes multiple dimensions, you must specify a value for every defined dimension when you use `get-metric-statistics`. For example, the Amazon S3 metric `BucketSizeBytes` includes the dimensions `BucketName` and `StorageType`, so you must specify both dimensions with `get-metric-statistics`.

```bash
aws cloudwatch get-metric-statistics --metric-name BucketSizeBytes --start-time 2017-01-23T14:23:00Z --end-time 2017-01-26T19:30:00Z --period 3600 --namespace AWS/S3 --statistics Maximum --dimensions Name=BucketName,Value=MyBucketName Name=StorageType,Value=StandardStorage --output table
```

To see what dimensions are defined for a metric, use the `list-metrics` command.

### Publishing single data points

To publish a single data point for a new or existing metric, use the `put-metric-data` command with one value and time stamp. For example, the following actions each publish one data point.

```bash
aws cloudwatch put-metric-data --metric-name PageViewCount --namespace MyService --value 2 --timestamp 2016-10-20T12:00:00.000Z
aws cloudwatch put-metric-data --metric-name PageViewCount --namespace MyService --value 4 --timestamp 2016-10-20T12:00:01.000Z
aws cloudwatch put-metric-data --metric-name PageViewCount --namespace MyService --value 5 --timestamp 2016-10-20T12:00:02.000Z
```
If you call this command with a new metric name, CloudWatch creates a metric for you. Otherwise, CloudWatch associates your data with the existing metric that you specified.

**Note**
When you create a metric, it can take up to 2 minutes before you can retrieve statistics for the new metric using the `get-metric-statistics` command. However, it can take up to 15 minutes before the new metric appears in the list of metrics retrieved using the `list-metrics` command.

Although you can publish data points with time stamps as granular as one-thousandth of a second, CloudWatch aggregates the data to a minimum granularity of 1 second. CloudWatch records the average (sum of all items divided by number of items) of the values received for each period, as well as the number of samples, maximum value, and minimum value for the same time period. For example, the `PageViewCount` metric from the previous examples contains three data points with time stamps just seconds apart. If you have your period set to 1 minute, CloudWatch aggregates the three data points because they all have time stamps within a 1-minute period.

You can use the `get-metric-statistics` command to retrieve statistics based on the data points that you published.

```
aws cloudwatch get-metric-statistics --namespace MyService --metric-name PageViewCount \
--statistics "Sum" "Maximum" "Minimum" "Average" "SampleCount" \ 
--start-time 2016-10-20T12:00:00.000Z --end-time 2016-10-20T12:05:00.000Z --period 60
```

The following is example output.

```
{
  "Datapoints": [
    {
      "SampleCount": 3.0,
      "Timestamp": "2016-10-20T12:00:00Z",
      "Average": 3.6666666666666665,
      "Maximum": 5.0,
      "Minimum": 2.0,
      "Sum": 11.0,
      "Unit": "None"
    }
  ],
  "Label": "PageViewCount"
}
```

### Publishing statistic sets

You can aggregate your data before you publish to CloudWatch. When you have multiple data points per minute, aggregating data minimizes the number of calls to `put-metric-data`. For example, instead of calling `put-metric-data` multiple times for three data points that are within 3 seconds of each other, you can aggregate the data into a statistic set that you publish with one call, using the `--statistic-values` parameter.

```
aws cloudwatch put-metric-data --metric-name PageViewCount --namespace MyService \
--statistic-values Sum=11,Minimum=2,Maximum=5,SampleCount=3 -- 
timestamp 2016-10-14T12:00:00.000Z
```

CloudWatch needs raw data points to calculate percentiles. If you publish data using a statistic set instead, you can't retrieve percentile statistics for this data unless one of the following conditions is true:

- The `SampleCount` of the statistic set is 1
- The `Minimum` and the `Maximum` of the statistic set are equal
Publishing the value zero

When your data is more sporadic and you have periods that have no associated data, you can choose to publish the value zero (0) for that period or no value at all. If you use periodic calls to `PutMetricData` to monitor the health of your application, you might want to publish zero instead of no value. For example, you can set a CloudWatch alarm to notify you if your application fails to publish metrics every five minutes. You want such an application to publish zeros for periods with no associated data.

You might also publish zeros if you want to track the total number of data points or if you want statistics such as minimum and average to include data points with the value 0.

Using metric math

Metric math enables you to query multiple CloudWatch metrics and use math expressions to create new time series based on these metrics. You can visualize the resulting time series on the CloudWatch console and add them to dashboards. Using AWS Lambda metrics as an example, you could divide the `Errors` metric by the `Invocations` metric to get an error rate. Then add the resulting time series to a graph on your CloudWatch dashboard.

You can also perform metric math programmatically, using the `GetMetricData` API operation. For more information, see `GetMetricData`.

Adding a math expression to a CloudWatch graph

You can add a math expression to a graph on your CloudWatch dashboard. Each graph is limited to using a maximum of 500 metrics and expressions, so you can add a math expression only if the graph has 499 or fewer metrics. This applies even if not all the metrics are displayed on the graph.

To add a math expression to a graph

2. Create or edit a graph. There needs to be at least one metric in the graph.
3. Choose Graphed metrics.
5. In the new line, under the Details column, enter the math expression. The tables in the Metric Math Syntax and Functions section list the functions that you can use in the expression.

   To use a metric or the result of another expression as part of the formula for this expression, use the value shown in the Id column: for example, m1+m2 or e1-MIN(e1).

   You can change the value of Id. It can include numbers, letters, an underscore, and must start with a lowercase letter. Changing the value of Id to a more meaningful name can also make a graph easier to understand; for example, changing m1 and m2 to `errors` and `requests`.

   **Tip**
   Choose the down arrow next to Math Expression to see a list of supported functions, which you can use when creating your expression.

6. For the Label column of the expression, enter a name that describes what the expression is calculating.

   If the result of an expression is an array of time series, each of those time series is displayed on the graph with a separate line, with different colors. Immediately under the graph is a legend for each line in the graph. For a single expression that produces multiple time series, the legend captions for those time series are in the format `Expression-Label Metric-Label`. For example, if the graph includes a metric with a label of `Errors` and an expression `FILL(METRICS(), 0)` that has a label of
Filled With 0: one line in the legend would be Filled With 0: Errors. To have the legend show only the original metric labels, set Expression-Label to be empty.

When one expression produces an array of time series on the graph, you can't change the colors used for each of those time series.

7. After you have added the desired expressions, you can simplify the graph by hiding some of the original metrics. To hide a metric or expression, clear the check box to the left of the Id field.

## Metric math syntax and functions

The following sections explain the functions available for metric math. All functions must be written in uppercase letters (such as `AVG`), and the Id field for all metrics and math expressions must start with a lowercase letter.

The final result of any math expression must be a single time series or an array of time series. Some functions produce a scalar number. You can use these functions within a larger function that ultimately produces a time series. For example, taking the AVG of a single time series produces a scalar number, so it can't be the final expression result. But you could use it in the function `m1-AVG(m1)` to display a time series of the difference between each individual data point and the average value in the time series.

### Data type abbreviations

Some functions are valid for only certain types of data. The abbreviations in the following list are used in the tables of functions to represent the types of data supported for each function:

- `s` represents a scalar number, such as 2, -5, or 50.25
- `TS` is a time series (a series of values for a single CloudWatch metric over time): for example, the `CPUUtilization` metric for instance `i-1234567890abcdef0` over the last 3 days
- `TS[]` is an array of time series, such as the time series for multiple metrics

### The METRICS() function

The `METRICS()` function returns all the metrics in the request. Math expressions aren't included.

You can use `METRICS()` within a larger expression that produces a single time series or an array of time series. For example, the expression `SUM(METRICS())` returns a time series (TS) that is the sum of the values of all the graphed metrics. `METRICS()/100` returns an array of time series, each of which is a time series showing each data point of one of the metrics divided by 100.

You can use the `METRICS()` function with a string to return only the graphed metrics that contain that string in their Id field. For example, the expression `SUM(METRICS("errors"))` returns a time series that is the sum of the values of all the graphed metrics that have 'errors' in their Id field. You can also use `SUM(METRICS("4xx"), METRICS("5xx"))` to match multiple strings.

### Basic arithmetic functions

The following table lists the basic arithmetic functions that are supported. Missing values in a time series are treated as 0. If the value of a data point causes a function to attempt to divide by zero, the data point is dropped.

<table>
<thead>
<tr>
<th>Operation</th>
<th>Arguments</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arithmetic operators: + - * / ^</td>
<td><code>s, s</code></td>
<td><code>PERIOD(m1)/60</code></td>
</tr>
<tr>
<td></td>
<td><code>s, TS</code></td>
<td><code>5 * m1</code></td>
</tr>
</tbody>
</table>
Metric math syntax and functions

<table>
<thead>
<tr>
<th>Operation</th>
<th>Arguments</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>TS, TS</td>
<td></td>
<td>m1 - m2</td>
</tr>
<tr>
<td>S, TS[]</td>
<td></td>
<td>SUM(100/[m1, m2])</td>
</tr>
<tr>
<td>TS, TS[]</td>
<td></td>
<td>AVG([m1,m2]/m3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>METRICS()*100</td>
</tr>
<tr>
<td>Unary subtraction -</td>
<td>S</td>
<td>-5*m1</td>
</tr>
<tr>
<td>TS</td>
<td></td>
<td>-m1</td>
</tr>
<tr>
<td>TS[]</td>
<td></td>
<td>SUM(-[m1, m2])</td>
</tr>
</tbody>
</table>

### Comparison and logical operators

You can use comparison and logical operators with either a pair of time series or a pair of single scalar values. When you use a comparison operator with a pair of time series, the operators return a time series where each data point is either 0 (false) or 1 (true). If you use a comparison operator on a pair of scalar values, a single scalar value is returned, either 0 or 1.

When comparison operators are used between two time series, and only one of the time series has a value for a particular time stamp, the function treats the missing value in the other time series as **0**.

You can use logical operators in conjunction with comparison operators, to create more complex functions.

The following table lists the operators that are supported.

<table>
<thead>
<tr>
<th>Type of operator</th>
<th>Supported operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparison operators</td>
<td>==</td>
</tr>
<tr>
<td></td>
<td>!=</td>
</tr>
<tr>
<td></td>
<td>&lt;=</td>
</tr>
<tr>
<td></td>
<td>&gt;=</td>
</tr>
<tr>
<td></td>
<td>&lt;</td>
</tr>
<tr>
<td></td>
<td>&gt;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Logical operators</th>
<th>AND or &amp;&amp;</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OR or</td>
</tr>
</tbody>
</table>

To see how these operators are used, suppose we have two time series: `metric1` has values of [30, 20, 0, 0] and `metric2` has values of [20, -, 20, -] where - indicates that there is no value for that timestamp.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Output</th>
</tr>
</thead>
<tbody>
<tr>
<td>(metric1 &lt; metric2)</td>
<td>0, 0, 1, 0</td>
</tr>
</tbody>
</table>
Expression | Output
---|---
(metric1 >= 30) | 1, 0, 0, 0
(metric1 > 15 AND metric2 > 15) | 1, 0, 0, 0

**Functions supported for metric math**

The following table describes the functions that you can use in math expressions. Enter all functions in uppercase letters.

The final result of any math expression must be a single time series or an array of time series. Some functions in tables in the following sections produce a scalar number. You can use these functions within a larger function that ultimately produces a time series. For example, taking the AVG of a single time series produces a scalar number, so it can't be the final expression result. But you could use it in the function m1-AVG(m1) to display a time series of the difference between each individual data point and the average value of that data point.

In the following table, every example in the Examples column is an expression that results in a single time series or an array of time series. These examples show how functions that return scalar numbers can be used as part of a valid expression that produces a single time series.

<table>
<thead>
<tr>
<th>Function</th>
<th>Argument(s)</th>
<th>Return type*</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABS</td>
<td>TS</td>
<td>TS</td>
<td>Returns the absolute value of each data point.</td>
<td>ABS(m1-m2) MIN(ABS([m1, m2])) ABS(METRICS())</td>
</tr>
<tr>
<td>ANOMALY_DETECTION_BAND</td>
<td>TS, S</td>
<td>TS[]</td>
<td>Returns an anomaly detection band for the specified metric. The band consists of two time series, one representing the upper limit of the &quot;normal&quot; expected value of the metric, and the other representing the lower limit. The function can take two arguments. The first is the ID of the metric to create the band for. The second argument is the number of standard deviations to use for the band. If you don't specify this argument, the default of 2 is used. For more information, see Using CloudWatch anomaly detection (p. 247).</td>
<td>ANOMALY_DETECTION_BAND(m1) ANOMALY_DETECTION_BAND(m1,4)</td>
</tr>
<tr>
<td>AVG</td>
<td>TS</td>
<td>S</td>
<td>The AVG of a single time series returns a scalar representing the average of all the data points in the metric. The AVG of an array</td>
<td>SUM([m1,m2])/AVG(m2) AVG(METRICS())</td>
</tr>
<tr>
<td>Function</td>
<td>Argument Type</td>
<td>Return Type</td>
<td>Description</td>
<td>Examples</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------</td>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>of time series returns a single time series. Missing values are treated as 0.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note</strong> We recommend that you do not use this function in CloudWatch alarms.</td>
<td></td>
</tr>
<tr>
<td>CEIL</td>
<td>TS</td>
<td>TS</td>
<td>Returns the ceiling of each metric. The ceiling is the smallest integer greater than or equal to each value.</td>
<td>CEIL(m1)</td>
</tr>
<tr>
<td></td>
<td>TS[]</td>
<td>TS[]</td>
<td></td>
<td>CEIL(METRICS())</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SUM(CEIL(METRICS()))</td>
</tr>
<tr>
<td>DATAPoint_COUNT</td>
<td>S</td>
<td>TS</td>
<td>Returns a count of the datapoints that reported values. This is useful for calculating averages of sparse metrics.</td>
<td>SUM(m1) / DATAPoint_COUNT(m1)</td>
</tr>
<tr>
<td></td>
<td>TS[]</td>
<td>TS</td>
<td></td>
<td>DATAPoint_COUNT(METRICS())</td>
</tr>
<tr>
<td>DIFF</td>
<td>TS</td>
<td>TS</td>
<td>Returns the difference between each value in the time series and the preceding value from that time series.</td>
<td>DIFF(m1)</td>
</tr>
<tr>
<td></td>
<td>TS[]</td>
<td>TS[]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DIFF_TIME</td>
<td>TS</td>
<td>TS</td>
<td>Returns the difference in seconds between the timestamp of each value in the time series and the timestamp of the preceding value from that time series.</td>
<td>DIFF_TIME(METRICS())</td>
</tr>
<tr>
<td></td>
<td>TS[]</td>
<td>TS[]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Argument Type</td>
<td>Return Type</td>
<td>Description</td>
<td>Examples</td>
</tr>
<tr>
<td>----------</td>
<td>---------------</td>
<td>-------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
</tbody>
</table>
| FILL | TS, [S | REPEAT | LINEAR] TS[], [TS | S | REPEAT | LINEAR] TS[] | Fills the missing values of a time series. There are several options for the values to use as the filler for missing values:  
• You can specify a value to use as the filler value.  
• You can specify a metric to use as the filler value.  
• You can use the REPEAT keyword to fill missing values with the most recent actual value of the metric before the missing value.  
• You can use the LINEAR keyword to fill the missing values with values that create a linear interpolation between the values at the beginning and the end of the gap.  
**Note**  
We recommend that you do not use this function in CloudWatch alarms. | FILL(m1,10)  
FILL(METRICS(), 0)  
FILL(METRICS(), m1)  
FILL(m1, MIN(m1))  
FILL(m1, REPEAT)  
FILL(METRICS(), LINEAR) |
| FIRST | TS[] | TS | Returns the first or last time series from an array of time series. This is useful when used with the SORT function. It can also be used to get the high and low thresholds from the ANOMALY_DETECTION_BAND function. | IF(FIRST(SORT(METRICS(), AVG, DESC))>100, 1, 0)  
LAST(ANOMALY_DETECTION_BAND(m1)) returns the lower bound of the anomaly prediction band. |
| LAST | | TS |  |
| FLOOR | TS TS[] | TS TS[] | Returns the floor of each metric. The floor is the largest integer less than or equal to each value. | FLOOR(m1)  
FLOOR(METRICS()) |
<table>
<thead>
<tr>
<th>Function</th>
<th>Arguments</th>
<th>Return type</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>IF</td>
<td>IF expression</td>
<td>TS</td>
<td>Use IF along with a comparison operator to filter out data points from a time series, or create a mixed time-series composed of multiple collated time series. For more information, see Using IF expressions (p. 88).</td>
<td>For examples, see Using IF expressions (p. 88).</td>
</tr>
<tr>
<td>INSIGHT_RULE_METRIC</td>
<td>ruleName, metricName</td>
<td>TS</td>
<td>Use INSIGHT_RULE_METRIC to extract statistics from a rule in Contributor Insights. For more information, see Graphing metrics generated by rules (p. 259).</td>
<td></td>
</tr>
<tr>
<td>LOG</td>
<td>TS</td>
<td>TS</td>
<td>The LOG of a time series returns the natural logarithm value of each value in the time series.</td>
<td>LOG(METRICS())</td>
</tr>
<tr>
<td>LOG10</td>
<td>TS</td>
<td>TS</td>
<td>The LOG10 of a time series returns the base-10 logarithm value of each value in the time series.</td>
<td>LOG10(m1)</td>
</tr>
<tr>
<td>MAX</td>
<td>TS</td>
<td>S</td>
<td>The MAX of a single time series returns a scalar representing the maximum value of all data points in the metric. The MAX value of an array of time series returns a single time series.</td>
<td>MAX(m1)/m1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TS</td>
<td></td>
<td>MAX(METRICS())</td>
</tr>
<tr>
<td></td>
<td></td>
<td>S</td>
<td>Note: We recommend that you do not use this function in CloudWatch alarms.</td>
<td></td>
</tr>
<tr>
<td>METRIC_COUNT</td>
<td>TS</td>
<td>S</td>
<td>Returns the number of metrics in the time series array.</td>
<td>m1/METRIC_COUNT(METRICS())</td>
</tr>
<tr>
<td>Function</td>
<td>Arguments</td>
<td>Return type*</td>
<td>Description</td>
<td>Examples</td>
</tr>
<tr>
<td>------------</td>
<td>-----------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
</tbody>
</table>
| METRICS    | null      | TS[]         | The `METRICS()` function returns all CloudWatch metrics in the request. Math expressions aren't included. You can use `METRICS()` within a larger expression that produces a single time series or an array of time series. You can use the `METRICS()` function with a string to return only the graphed metrics that contain that string in their Id field. For example, the expression `SUM(METRICS("errors"))` returns a time series that is the sum of the values of all the graphed metrics that have 'errors' in their Id field. You can also use `SUM([METRICS("4xx"), METRICS("5xx")])` to match multiple strings. | AVG(METRICS())
|            | string    |              |                                                                                                                                             | SUM(METRICS("errors"))            |
| MIN        | TS        | S            | The `MIN` of a single time series returns a scalar representing the minimum value of all data points in the metric. The `MIN` of an array of time series returns a single time series. **Note** We recommend that you do not use this function in CloudWatch alarms. | m1-MIN(m1)
<p>|            | TS[]      | TS           |                                                                                                                                             | MIN(METRICS())                     |</p>
<table>
<thead>
<tr>
<th>Function</th>
<th>Argument Type</th>
<th>Return Type</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>MINUTE</td>
<td>TS</td>
<td>TS</td>
<td>These functions take the period and range of the time series and return a new non-sparse time series where each value is based on its timestamp.</td>
<td>MINUTE(m1)</td>
</tr>
<tr>
<td>HOUR</td>
<td>TS</td>
<td>TS</td>
<td>• MINUTE returns a non-sparse time series of integers between 0 and 59 that represent the UTC minute of each timestamp in the original time series.</td>
<td>IF(DAY(m1) &lt; 6, m1) returns metrics only from weekdays, Monday to Friday.</td>
</tr>
<tr>
<td>DAY</td>
<td>TS</td>
<td>TS</td>
<td>• HOUR returns a non-sparse time series of integers between 0 and 23 that represent the UTC hour of each timestamp in the original time series.</td>
<td>IF(MONTH(m1) == 4, m1) returns only metrics published in April.</td>
</tr>
<tr>
<td>DATE</td>
<td>TS</td>
<td>TS</td>
<td>• DAY returns a non-sparse time series of integers between 1 and 7 that represent the UTC day of the week of each timestamp in the original time series. 1 represents Monday and 7 represents Sunday.</td>
<td></td>
</tr>
<tr>
<td>MONTH</td>
<td>TS</td>
<td>TS</td>
<td>• DATE returns a non-sparse time series of integers between 1 and 31 that represent the UTC day of the month of each timestamp in the original time series.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TS</td>
<td>S</td>
<td>• MONTH returns a non-sparse time series of integers between 1 and 12 that represent the UTC month of each timestamp in the original time series. 1 represents January and 12 represents December.</td>
<td>m1/PERIOD(m1)</td>
</tr>
<tr>
<td>PERIOD</td>
<td>TS</td>
<td>S</td>
<td>Returns the period of the metric in seconds. Valid input is metrics, not the results of other expressions.</td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Argument Type</td>
<td>Return Type*</td>
<td>Description</td>
<td>Examples</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td><strong>RATE</strong></td>
<td>TS</td>
<td>TS</td>
<td>Returns the rate of change of the metric per second. This is calculated as the difference between the latest data point value and the previous data point value, divided by the time difference in seconds between the two values.</td>
<td>RATE(m1)</td>
</tr>
<tr>
<td></td>
<td>TS[]</td>
<td>TS[]</td>
<td></td>
<td>RATE(METRICS())</td>
</tr>
<tr>
<td><strong>REMOVEEMPTY</strong></td>
<td>TS[]</td>
<td>TS[]</td>
<td>Removes any time series that have no datapoints from an array of time series. The result is an array of time series where each time series contains at least one datapoint.</td>
<td>REMOVE_EMPTY(METRICS())</td>
</tr>
<tr>
<td><strong>RUNNING_SUM</strong></td>
<td>TS</td>
<td>TS</td>
<td>Returns a time series with the running sum of the values in the original time series.</td>
<td>RUNNING_SUM([m1,m2])</td>
</tr>
<tr>
<td></td>
<td>TS[]</td>
<td>TS[]</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SEARCH</strong></td>
<td>Search expression</td>
<td>One or more TS</td>
<td>Returns one or more time series that match a search criteria that you specify. The SEARCH function enables you to add multiple related time series to a graph with one expression. The graph is dynamically updated to include new metrics that are added later and match the search criteria. For more information, see Using search expressions in graphs (p. 91).</td>
<td></td>
</tr>
<tr>
<td>Function</td>
<td>Arguments</td>
<td>Return type</td>
<td>Description</td>
<td>Examples</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------</td>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SERVICE QUOTA</td>
<td>TS that is a usage metric</td>
<td>TS</td>
<td>Returns the service quota for the given usage metric. You can use this to visualize how your current usage compares to the quota, and to set alarms that warn you when you approach the quota. For more information, see AWS usage metrics (p. 683).</td>
<td></td>
</tr>
<tr>
<td>SLICE</td>
<td>(TS[], S, S) or (TS[], S)</td>
<td>TS[]</td>
<td>Retrieves part of an array of time series. This is especially useful when combined with SORT. For example, you can exclude the top result from an array of time series. You can use two scalar arguments to define the set of time series that you want returned. The two scalars define the start (inclusive) and end (exclusive) of the array to return. The array is zero-indexed, so the first time series in the array is time series 0. Alternatively, you can specify just one value, and CloudWatch returns all time series starting with that value.</td>
<td>SLICE(SORT(METRICS()), SUM, DESC), 0, 10 returns the 10 metrics from the array of metrics in the request that have the highest SUM value. SLICE(SORT(METRICS()), AVG, ASC), 5 sorts the array of metrics by the AVG statistic, then returns all the time series except for the 5 with the lowest AVG.</td>
</tr>
<tr>
<td>SORT</td>
<td>(TS[], FUNCTION, SORT_ORDER)</td>
<td>TS[]</td>
<td>Sorts an array of time series according to the function you specify. The function you use can be AVG, MIN, MAX, or SUM. The sort order can be either ASC for ascending (lowest values first) or DESC to sort the higher values first. You can optionally specify a number after the sort order which acts as a limit. For example, specifying a limit of 5 returns only the top 5 time series from the sort. When this math function is displayed on a graph, the labels for each metric in the graph are also sorted and numbered.</td>
<td>SORT(METRICS(), AVG, DESC, 10) calculates the average value of each time series, sorts the time series with the highest values at the beginning of the sort, and returns only the 10 time series with the highest averages. SORT(METRICS(), MAX, ASC) sorts the array of metrics by the MAX statistic, then returns all of them in ascending order.</td>
</tr>
<tr>
<td>Function</td>
<td>Argument Type</td>
<td>Return Type</td>
<td>Description</td>
<td>Examples</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>STDDEV</td>
<td>TS</td>
<td>S</td>
<td>The STDDEV of a single time series returns a scalar representing the standard deviation of all data points in the metric. The STDDEV of an array of time series returns a single time series.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TS[]</td>
<td>TS</td>
<td>Note: We recommend that you do not use this function in CloudWatch alarms.</td>
<td>m1/STDDEV(m1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>STDDEV(METRICS())</td>
<td></td>
</tr>
<tr>
<td>SUM</td>
<td>TS</td>
<td>S</td>
<td>The SUM of a single time series returns a scalar representing the sum of the values of all data points in the metric. The SUM of an array of time series returns a single time series.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TS[]</td>
<td>TS</td>
<td>Note: We recommend that you do not use this function in CloudWatch alarms.</td>
<td>SUM(METRICS())/SUM(m1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SUM([m1,m2])</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SUM(METRICS(&quot;errors&quot;))/SUM(METRICS(&quot;requests&quot;))*100</td>
<td></td>
</tr>
<tr>
<td>TIME_SERIES</td>
<td>S</td>
<td>TS</td>
<td>Returns a non-sparse time series where every value is set to a scalar argument.</td>
<td>TIME_SERIES(MAX(m1))</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TIME_SERIES(5*AVG(m1))</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TIME_SERIES(10)</td>
<td></td>
</tr>
</tbody>
</table>

*Using a function that returns only a scalar number is not valid, as all final results of expressions must be a single time series or an array of time series. Instead, use these functions as part of a larger expression that returns a time series.

**Using IF expressions**

Use **IF** along with a comparison operator to filter out data points from a time series, or create a mixed time-series composed of multiple collated time series.

**IF** uses the following arguments:

```
IF(condition, trueValue, falseValue)
```

The condition evaluates to FALSE if the value of the condition data point is 0, and to TRUE if the value of the condition is any other value, whether that value is positive or negative. If the condition is a time series, it is evaluated separately for every timestamp.

The following lists the valid syntaxes. For each of these syntaxes, the output is a single time series.

- **IF(TS Comparison Operator S, S | TS, S / TS)**
- IF(TS, TS, TS)
- IF(TS, S, TS)
- IF(TS, TS, S)
- IF(TS, S, S)
- IF(S, TS, TS)

The following sections provide more details and examples for these syntaxes.

**IF(TS Comparison Operator S, scalar2 | metric2, scalar3 | metric3)**

The corresponding output time series value:

- has the value of scalar2 or metric2, if TS Comparison Operator S is TRUE
- has the value of scalar3 or metric3, if TS Comparison Operator S is FALSE
- is an empty time series, if the corresponding data point of does not exist in metric3, or if scalar3/metric3 is omitted from the expression

**IF(metric1, metric2, metric3)**

For each data point of metric1, the corresponding output time series value:

- has the value of metric2, if the corresponding data point of metric1 is TRUE.
- has the value of metric3, if the corresponding data point of metric1 is FALSE.
- has the value of 0, if the corresponding data point of metric1 is TRUE and the corresponding data point does not exist in metric2.
- is dropped, if the corresponding data point of metric1 is FALSE and the corresponding data point does not exist on metric3 or if metric3 is omitted from the expression.

The following table shows an example for this syntax.

<table>
<thead>
<tr>
<th>Metric or function</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>(metric1)</td>
<td>[1, 1, 0, 0, -]</td>
</tr>
<tr>
<td>(metric2)</td>
<td>[30, -, 0, 0, 30]</td>
</tr>
<tr>
<td>(metric3)</td>
<td>[0, 0, 20, -, 20]</td>
</tr>
<tr>
<td>IF(metric1, metric2, metric3)</td>
<td>[30, 0, 20, -, -]</td>
</tr>
</tbody>
</table>

**IF(metric1, scalar2, metric3)**

For each data point of metric1, the corresponding output time series value:

- has the value of scalar2, if the corresponding data point of metric1 is TRUE.
- has the value of metric3, if the corresponding data point of metric1 is FALSE.
- is dropped, if the corresponding data point of metric1 is FALSE and the corresponding data point does not exist on metric3, or if metric3 is omitted from the expression.

<table>
<thead>
<tr>
<th>Metric or function</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>(metric1)</td>
<td>[1, 1, 0, 0, -]</td>
</tr>
<tr>
<td>Metric or function</td>
<td>Values</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>scalar2</td>
<td>5</td>
</tr>
<tr>
<td>(metric3)</td>
<td>[0, 0, 20, -, 20]</td>
</tr>
<tr>
<td>IF(metric1, scalar2, metric3)</td>
<td>[5, 5, 20, -, -]</td>
</tr>
</tbody>
</table>

**IF(metric1, metric2, scalar3)**

For each data point of **metric1**, the corresponding output time series value:

- has the value of **metric2**, if the corresponding data point of **metric1** is TRUE.
- has the value of **scalar3**, if the corresponding data point of **metric1** is FALSE.
- has the value of 0, if the corresponding data point of **metric1** is TRUE and the corresponding data point does not exist in **metric2**.
- is dropped if the corresponding data point in **metric1** does not exist.

<table>
<thead>
<tr>
<th>Metric or function</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>(metric1)</td>
<td>[1, 1, 0, 0, -]</td>
</tr>
<tr>
<td>(metric2)</td>
<td>[30, -, 0, 0, 30]</td>
</tr>
<tr>
<td>scalar3</td>
<td>5</td>
</tr>
<tr>
<td>IF(metric1, metric2, scalar3)</td>
<td>[30, 0, 5, 5, -]</td>
</tr>
</tbody>
</table>

**IF(scalar1, metric2, metric3)**

The corresponding output time series value:

- has the value of **metric2**, if **scalar1** is TRUE.
- has the value of **metric3**, if **scalar1** is FALSE.
- is an empty time series, if **metric3** is omitted from the expression.

**Use case examples for IF expressions**

The following examples illustrate the possible uses of the IF function.

- To display only the low values of a metric:
  
  IF(metric1<400, metric1)

- To change each data point in a metric to one of two values, to show relative highs and lows of the original metric:
  
  IF(metric1<400, 10, 2)

- To display a 1 for each timestamp where latency is over the threshold, and display a 0 for all other data points:
  
  IF(latency>threshold, 1, 0)
Using metric math with the GetMetricData API operation

You can use GetMetricData to perform calculations using math expressions, and also retrieve large batches of metric data in one API call. For more information, see GetMetricData.

Using search expressions in graphs

Search expressions are a type of math expression that you can add to CloudWatch graphs. Search expressions enable you to quickly add multiple related metrics to a graph. They also enable you to create dynamic graphs that automatically add appropriate metrics to their display, even if those metrics don't exist when you first create the graph.

For example, you can create a search expression that displays the AWS/EC2 CPUUtilization metric for all instances in the Region. If you later launch a new instance, the CPUUtilization of the new instance is automatically added to the graph.

When you use a search expression in a graph, the search finds the search expression in metric names, namespaces, dimension names, and dimension values. You can use Boolean operators for more complex and powerful searches.

Topics
- CloudWatch search expression syntax (p. 91)
- CloudWatch search expression examples (p. 95)
- Creating a CloudWatch graph with a search expression (p. 97)

CloudWatch search expression syntax

A valid search expression has the following format.

```
SEARCH(' {Namespace, DimensionName1, DimensionName2, ...} SearchTerm', 'Statistic', Period)
```

For example:

```
SEARCH(' {AWS/EC2,InstanceId} MetricName="CPUUtilization" ', 'Average', 300)
```

- The first part of the query after the word SEARCH, enclosed in curly braces, is the metric schema to be searched. The metric schema contains a metric namespace and one or more dimension names. Including a metric schema in a search query is optional. If specified, the metric schema must contain a namespace and can optionally contain one or more dimension names that are valid in that namespace.

  You don't need to use quote marks inside the metric schema unless a namespace or dimension name includes spaces or non-alphanumeric characters. In that case, you must enclose the name that contains those characters with double quotes.

- The SearchTerm is also optional, but a valid search must contain either the metric schema, the SearchTerm, or both. The SearchTerm usually contains one or more metric names or dimension values. The SearchTerm can include multiple terms to search for, by both partial match and exact match. It can also contain Boolean operators.

  The SearchTerm can include one or more designators, such as MetricName= as in this example, but using designators isn't required.

  The metric schema and SearchTerm must be enclosed together in a pair of single quote marks.
• The Statistic is the name of any valid CloudWatch statistic. It must be enclosed by single quotes. For more information, see Statistics (p. 5).
• The Period is the aggregation time period in seconds.

The preceding example searches the AWS/EC2 namespace for any metrics that have InstanceId as a dimension name. It returns all CPUUtilization metrics that it finds, with the graph showing the Average statistic with an aggregation period of 5 minutes.

Search expression limits

The maximum search expression query size is 1024 characters. You can have as many as 100 search expressions on one graph. A graph can display as many as 500 time series.

CloudWatch search expressions: Tokenization

When you specify a SearchTerm, the search function searches for tokens, which are substrings that CloudWatch automatically generates from full metric names, dimension names, dimension values, and namespaces. CloudWatch generates tokens distinguished by the camel-case capitalization in the original string. Numeric characters also serve as the start of new tokens, and non-alphanumeric characters serve as delimiters, creating tokens before and after the non-alphanumeric characters.

A continuous string of the same type of token delimiter character results in one token.

All generated tokens are in lowercase. The following table shows some examples of tokens generated.

<table>
<thead>
<tr>
<th>Original string</th>
<th>Tokens generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>CustomCount1</td>
<td>customcount1, custom, count, 1</td>
</tr>
<tr>
<td>SDBFailure</td>
<td>sdbfailure, sdb, failure</td>
</tr>
<tr>
<td>Project2-trial333</td>
<td>project2trial333, project, 2, trial, 333</td>
</tr>
</tbody>
</table>

CloudWatch search expressions: Partial matches

When you specify a SearchTerm, the search term is also tokenized. CloudWatch finds metrics based on partial matches, which are matches of a single token generated from the search term to a single token generated from a metric name, namespace, dimension name, or dimension value.

Partial match searches to match a single token are case insensitive. For example, using any of the following search terms can return the CustomCount1 metric:

• count
• Count
• COUNT

However, using count as a search term doesn't find CustomCount1 because the capitalization in the search term count is tokenized into cou and NT.

Searches can also match composite tokens, which are multiple tokens that appear consecutively in the original name. To match a composite token, the search is case sensitive. For example, if the original term is CustomCount1, searches for CustomCount or Count1 are successful, but searches for customcount or count1 aren't.
CloudWatch search expressions: Exact matches

You can define a search to find only exact matches of your search term by using double quotes around the part of the search term that requires an exact match. These double-quotes are enclosed in the single-quotes used around the entire search term. For example, `SEARCH('{MyNamespace}, "CustomCount1" ', 'Maximum', 120)` finds the exact string CustomCount1 if it exists as a metric name, dimension name, or dimension value in the namespace named MyNamespace. However, the searches `SEARCH('{MyNamespace}, "customcount1" ', 'Maximum', 120)` or `SEARCH('{MyNamespace}, "Custom" ', 'Maximum', 120)` do not find this string.

You can combine partial match terms and exact match terms in a single search expression. For example, `SEARCH(' {AWS/NetworkELB, LoadBalancer} "ConsumedLCUs" OR flow ', 'Maximum', 120)` returns the Elastic Load Balancing metric named ConsumedLCUs as well as all Elastic Load Balancing metrics or dimensions that contain the token flow.

Using exact match is also a good way to find names with special characters, such as non-alphanumeric characters or spaces, as in the following example.

```
SEARCH(' {"My Namespace", "Dimension@Name"}, "Custom:Name[Special_Characters" ', 'Maximum', 120)
```

CloudWatch search expressions: Excluding a metric schema

All examples shown so far include a metric schema, in curly braces. Searches that omit a metric schema are also valid.

For example, `SEARCH(' "CPUUtilization" ', 'Average', 300)` returns all metric names, dimension names, dimension values, and namespaces that are an exact match for the string CPUUtilization. In the AWS metric namespaces, this can include metrics from several services including Amazon EC2, Amazon ECS, SageMaker, and others.

To narrow this search to only one AWS service, the best practice is to specify the namespace and any necessary dimensions in the metric schema, as in the following example. Although this narrows the search to the AWS/EC2 namespace, it would still return results of other metrics if you have defined CPUUtilization as a dimension value for those metrics.

```
SEARCH(' {AWS/EC2, InstanceType} "CPUUtilization" ', 'Average', 300)
```

Alternatively you could add the namespace in the `SearchTerm` as in the following example. But in this example, the search would match any AWS/EC2 string, even if it was a custom dimension name or value.

```
SEARCH(' "AWS/EC2" MetricName="CPUUtilization" ', 'Average', 300)
```

CloudWatch search expressions: Specifying property names in the search

The following exact match search for "CustomCount1" returns all metrics with exactly that name.

```
SEARCH(' "CustomCount1" ', 'Maximum', 120)
```

But it also returns metrics with dimension names, dimension values, or namespaces of CustomCount1. To structure your search further, you can specify the property name of the type of object that you want to find in your searches. The following example searches all namespaces and returns metrics named CustomCount1.
You can also use namespaces and dimension name/value pairs as property names, as in the following examples. The first of these examples also illustrates that you can use property names with partial match searches as well.

```
SEARCH(' MetricName="CustomCount1" ', 'Maximum', 120)
```

```
SEARCH(' InstanceType=micro ', 'Average', 300)
```

```
SEARCH(' InstanceType="t2.micro" Namespace="AWS/EC2" ', 'Average', 300)
```

**CloudWatch search expressions: Non-alphanumeric characters**

Non-alphanumeric characters serve as delimiters, and mark where the names of metrics, dimensions, namespaces, and search terms are to be separated into tokens. When terms are tokenized, non-alphanumeric characters are stripped out and don’t appear in the tokens. For example, `Network-Errors_2` generates the tokens `network`, `errors`, and `2`.

Your search term can include any non-alphanumeric characters. If these characters appear in your search term, they can specify composite tokens in a partial match. For example, all of the following searches would find metrics named either `Network-Errors-2` or `NetworkErrors2`.

```
network/errors
network+errors
network-errors
Network_Errors
```

When you’re doing an exact value search, any non-alphanumeric characters used in the exact search must be the correct characters that appear in the string being searched for. For example, if you want to find `Network-Errors-2`, searching for "Network-Errors-2" is successful, but a search for "Network_Errors_2" isn’t.

When you perform an exact match search, the following characters must be escaped with a backslash.

```
" \\ ( )
```

For example, to find the metric name `Europe\France Traffic(Network)` by exact match, use the search term "Europe\France Traffic\(Network\)"

**CloudWatch search expressions: Boolean operators**

Search supports the use of the Boolean operators AND, OR, and NOT within the SearchTerm. Boolean operators are enclosed in the single quote marks that you use to enclose the entire search term. Boolean operators are case sensitive, so and, or, and not aren’t valid as Boolean operators.

You can use AND explicitly in your search, such as `SEARCH('{AWS/EC2,InstanceId} network AND packets', 'Average', 300)`. Not using any Boolean operator between search terms implicitly searches them as if there were an AND operator, so `SEARCH('{AWS/EC2,InstanceId} network packets', 'Average', 300)` yields the same search results.

Use NOT to exclude subsets of data from the results. For example, `SEARCH(' {AWS/EC2,InstanceId} MetricName="CPUUtilization" NOT i-1234567890123456 ', 'Average', 300)` returns the CPUUtilization for all your instances, except for the instance i-1234567890123456. You can also use a NOT clause as the only search term. For example, `SEARCH( 'NOT Namespace=AWS ', 'Maximum', 120)` yields all your custom metrics (metrics with namespaces that don’t include AWS).
You can use multiple NOT phrases in a query. For example, `SEARCH(' {AWS/EC2, InstanceId} MetricName="CPUUtilization" NOT "ProjectA" NOT "ProjectB" ', 'Average', 300)` returns the CPUUtilization of all instances in the Region, except for those with dimension values of ProjectA or ProjectB.

You can combine Boolean operators for more powerful and detailed searches, as in the following examples. Use parentheses to group the operators.

Both of the next two examples return all metric names containing `ReadOps` from both the EC2 and EBS namespaces.

```
SEARCH(' (EC2 OR EBS) AND MetricName=ReadOps ', 'Maximum', 120)
```

```
SEARCH(' (EC2 OR EBS) MetricName=ReadOps ', 'Maximum', 120)
```

The following example narrows the previous search to only results that include ProjectA, which could be the value of a dimension.

```
SEARCH(' (EC2 OR EBS) AND ReadOps AND ProjectA ', 'Maximum', 120)
```

The following example uses nested grouping. It returns Lambda metrics for Errors from all functions, and invocations of functions with names that include the strings ProjectA or ProjectB.

```
SEARCH(' {AWS/Lambda, FunctionName} MetricName="Errors" OR (MetricName="Invocations" AND (ProjectA OR ProjectB)) ', 'Average', 600)
```

### CloudWatch search expressions: Using math expressions

You can use a search expression within a math expressions in a graph.

For example, `SUM(SEARCH(' {AWS/Lambda, FunctionName} MetricName="Errors" ', 'Sum', 300))` returns the sum of the Errors metric of all your Lambda functions.

Using separate lines for your search expression and math expression might yield more useful results. For example, suppose that you use the following two expressions in a graph. The first line displays separate Errors lines for each of your Lambda functions. The ID of this expression is e1. The second line adds another line showing the sum of the errors from all of the functions.

```
SEARCH(' {AWS/Lambda, FunctionName}, MetricName="Errors" ', 'Sum', 300)
SUM(e1)
```

### CloudWatch search expression examples

The following examples illustrate more search expression uses and syntax. Let's start with a search for CPUUtilization across all instances in the Region and then look at variations.

This example displays one line for each instance in the Region, showing the CPUUtilization metric from the AWS/EC2 namespace.

```
SEARCH(' {AWS/EC2, InstanceId} MetricName="CPUUtilization" ', 'Average', 300)
```

Changing InstanceId to InstanceType changes the graph to show one line for each instance type used in the Region. Data from all instances of each type is aggregated into one line for that instance type.
Removing the dimension name but keeping the namespace in the schema, as in the following example, results in a single line showing the aggregation of CPUUtilization metrics for all instances in the Region.

```
SEARCH(' {AWS/EC2} MetricName="CPUUtilization" ', 'Average', 300)
```

The following example aggregates the CPUUtilization by instance type and displays one line for each instance type that includes the string micro.

```
SEARCH(' {AWS/EC2,InstanceType} InstanceType=micro MetricName="CPUUtilization" ', 'Average', 300)
```

This example narrows the previous example, changing the InstanceType to an exact search for t2.micro instances.

```
SEARCH(' {AWS/EC2,InstanceType} InstanceType="t2.micro" MetricName="CPUUtilization" ', 'Average', 300)
```

The following search removes the {metric schema} part of the query, so the CPUUtilization metric from all namespaces appears in the graph. This can return quite a few results because the graph includes multiple lines for the CPUUtilization metric from each AWS service, aggregated along different dimensions.

```
SEARCH(' MetricName="CPUUtilization" ', 'Average', 300)
```

To narrow these results a bit, you can specify two specific metric namespaces.

```
SEARCH(' MetricName="CPUUtilization" AND ("AWS/ECS" OR "AWS/ES") ', 'Average', 300)
```

The preceding example is the only way to do a search of specific multiple namespaces with one search query, as you can specify only one metric schema in each query. However, to add more structure, you could use two queries in the graph, as in the following example. This example also adds more structure by specifying a dimension to use to aggregate the data for Amazon ECS.

```
SEARCH(' {AWS/ECS, ClusterName}, MetricName="CPUUtilization" ', 'Average', 300)
SEARCH(' {AWS/EBS}, MetricName="CPUUtilization" ', 'Average', 300)
```

The following example returns the Elastic Load Balancing metric named ConsumedLCUs as well as all Elastic Load Balancing metrics or dimensions that contain the token flow.

```
SEARCH(' {AWS/NetworkELB, LoadBalancer} "ConsumedLCUs" OR flow ', 'Maximum', 120)
```

The following example uses nested grouping. It returns Lambda metrics for Errors from all functions and Invocations of functions with names that include the strings ProjectA or ProjectB.

```
SEARCH(' {AWS/Lambda,FunctionName} MetricName="Errors" OR (MetricName="Invocations" AND (ProjectA OR ProjectB)) ', 'Average', 600)
```

The following example displays all of your custom metrics, excluding metrics generated by AWS services.
The following example displays metrics with metric names, namespaces, dimension names, and dimension values that contain the string `Errors` as part of their name.

```
SEARCH(' NOT Namespace=AWS ', 'Average', 120)
```

The following example narrows that search to exact matches. For example, this search finds the metric name `Errors` but not metrics named `ConnectionErrors` or `errors`.

```
SEARCH(' "Errors" ', 'Average', 300)
```

The following example shows how to specify names that contain spaces or special characters in the metric schema part of the search term.

```
SEARCH(' ("Custom-Namespace", "Dimension Name With Spaces"), ErrorCount ', 'Maximum', 120)
```

### Creating a CloudWatch graph with a search expression

On the CloudWatch console, you can access search capability when you add a graph to a dashboard, or by using the Metrics view.

#### To add a graph with a search expression to an existing dashboard

2. In the navigation pane, choose Dashboards and select a dashboard.
3. Choose Add widget.
4. Choose either Line or Stacked area and choose Configure.
5. On the Graphed metrics tab, choose Add a math expression.
6. For Details, enter the search expression that you want. For example, `SEARCH(' (AWS/EC2,InstanceId) MetricName="CPUUtilization" ', 'Average', 300)`
7. (Optional) To add another search expression or math expression to the graph, choose Add a math expression.
8. (Optional) After you add a search expression, you can specify a dynamic label to appear on the graph legend for each metric. Dynamic labels display a statistic about the metric and automatically update when the dashboard or graph is refreshed. To add a dynamic label, choose Graphed metrics and then Dynamic labels.
   
   By default, the dynamic values you add to the label appear at the beginning of the label. You can then click the Label value for the metric to edit the label. For more information, see Using dynamic labels (p. 69).
9. (Optional) To add a single metric to the graph, choose the All metrics tab and drill down to the metric you want.
10. (Optional) To change the time range shown on the graph, choose either custom at the top of the graph or one of the time periods to the left of custom.
11. (Optional) Horizontal annotations 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 and then Add horizontal annotation:
   
   a. For Label, enter a label for the annotation.
b. For **Value**, enter 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 check box in the left column for that annotation.

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

12. (Optional) Vertical annotations help you mark milestones in a graph, such as operational events or the beginning and end of a deployment. To add a vertical annotation, choose **Graph options** and then **Add vertical annotation**:

   a. For **Label**, enter a label for the annotation. To show only the date and time on the annotation, keep the **Label** field blank.

   b. For **Date**, specify the date and time where the vertical annotation appears.

   c. For **Fill**, specify whether to use fill shading before or after a vertical annotation or between two vertical annotations. For example, choose **Before** or **After** for the corresponding area to be filled. If you specify **Between**, another **Date** field appears, and the area of the graph between the two values is filled.

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

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

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

13. Choose **Create widget**.

14. Choose **Save dashboard**.

**To use the Metrics view to graph searched metrics**


2. In the navigation pane, choose **Metrics**.

3. In the search field, enter the tokens to search for: for example, **cpuutilization t2.small**.

   Results that match your search appear.

4. To graph all of the metrics that match your search, choose **Graph search**.

   or

   To refine your search, choose one of the namespaces that appeared in your search results.

5. If you selected a namespace to narrow your results, you can do the following:

   a. To graph one or more metrics, select the check box next to each metric. To select all metrics, select the check box in the heading row of the table.

   b. To refine your search, hover over a metric name and choose **Add to search** or **Search for this only**.
c. To view help for a metric, select the metric name and choose **What is this?**.

The selected metrics appear on the graph.

6. (Optional) Select one of the buttons in the search bar to edit that part of the search term.
7. (Optional) To add the graph to a dashboard, choose **Actions** and then **Add to dashboard**.
Use metrics explorer to monitor resources by their tags and properties

Metrics explorer is a tag-based tool that enables you to filter, aggregate, and visualize your metrics by tags and resource properties, to enhance observability for your services. This gives you a flexible and dynamic troubleshooting experience, so that you to create multiple graphs at a time and use these graphs to build your application health dashboards.

Metrics explorer visualizations are dynamic, so if a matching resource is created after you create a metrics explorer widget and add it to a CloudWatch dashboard, the new resource automatically appears in the explorer widget.

For example, if all of your EC2 production instances have the production tag, you can use metrics explorer to filter and aggregate metrics from all of these instances to understand their health and performance. If a new instance with a matching tag is later created, it's automatically added to the metrics explorer widget.

With metrics explorer, you can choose how to aggregate metrics from the resources that match the criteria, and whether to show them all in a single graph or on different graphs within one metrics explorer widget.

Metrics explorer includes templates that you can use to see useful visualization graphs with one click, and you can also extend these templates to create completely customized metrics explorer widgets.

Metrics explorer supports metrics emitted by AWS and EC2 metrics that are published by the CloudWatch agent, including memory, disk, and CPU metrics. To use metrics explorer to see the metrics that are published by the CloudWatch agent, you might have to update your CloudWatch agent configuration file. For more information, see CloudWatch agent configuration for metrics explorer (p. 101)

To create a visualization with metrics explorer and optionally add it to a dashboard, follow these steps.

To create a visualization with metrics explorer

2. In the navigation pane, choose Explorer.
3. Do one of the following:
   • To use a template, select it in the box that currently shows Empty Explorer.
     Depending on the template, the explorer might immediately display graphs of metrics. If it doesn't, choose one or more tags or properties in the From box and then data should appear. If it doesn't, use the options at the top of the page to display a longer time range in the graphs.
   • To create a custom visualization, under Metrics, choose a single metric or all the available metrics from a service.
     After you choose a metric, you can optionally repeat this step to add more metrics.
4. For each metric selected, CloudWatch displays the statistic that it will use immediately after the metric name. To change this, choose the statistic name, and then choose the statistic that you want.
5. Under From, choose a tag or a resource property to filter your results.
After you do this, you can optionally repeat this step to choose more tags or resource properties.

If you choose multiple values of the same property, such as two EC2 instance types, the explorer displays all the resources that match either chosen property. It's treated as an OR operation.

If you choose different properties or tags, such as the `Production` tag and the M5 instance type, only the resources that match all of these selections are displayed. It's treated as an AND operation.

6. (Optional) For **Aggregate by**, choose a statistic to use to aggregate the metrics. Then, next to **for**, choose how to aggregate the metric from the list. You can aggregate together all the resources that are currently displayed, or aggregate by a single tag or resource property.

   Depending on how you choose to aggregate, the result may be a single time series or multiple time series.

7. Under **Split by**, you can choose to split a single graph with multiple time series into multiple graphs. The split can be made by a variety of criteria, which you choose under **Split by**.

8. Under **Graph options**, you can refine the graph by changing the period, the type of graph, the legend placement, and the layout.

9. To add this visualization as a widget to a CloudWatch dashboard, choose **Add to dashboard**.

### CloudWatch agent configuration for metrics explorer

To enable metrics explorer to discover EC2 metrics published by the CloudWatch agent, make sure that the CloudWatch agent configuration file contains the following values:

- In the `metrics` section, make sure that the `aggregation_dimensions` parameter includes `[InstanceId"]. It can also contain other dimensions.
- In the `metrics` section, make sure that the `append_dimensions` parameter includes a `{InstanceId":"${aws:InstanceId}"} line. It can also contain other lines.
- In the `metrics` section, inside the `metrics_collected` section, check the sections for each resource type that you want metrics explorer to discover, such as the `cpu`, `disk`, and `memory` sections. Make sure that each of these sections has a "resources": [ "*" ] line. `aggregation_dimensions` parameter includes `[InstanceId"]`. It can also contain other dimensions.
- In the `cpu` section of the `metrics_collected>` section, make sure there is a "totalcpu": true line.

The settings in the previous list cause the CloudWatch agent to publish aggregate metrics for disks, CPUs, and other resources that can be plotted in metrics explorer for all the instances that use it.

These settings will republish the metrics that you had previously set up to be published with multiple dimensions, adding to your metric costs.

For more information about editing the CloudWatch agent configuration file, see [Manually create or edit the CloudWatch agent configuration file](p. 471).
Using Amazon CloudWatch alarms

You can create both metric alarms and composite alarms in CloudWatch.

- A **metric alarm** watches a single CloudWatch metric or the result of a math expression based on CloudWatch metrics. The alarm performs one or more actions based on the value of the metric or expression relative to a threshold over a number of time periods. The action can be sending a notification to an Amazon SNS topic, performing an Amazon EC2 action or an Auto Scaling action, or creating an OpsItem or incident in Systems Manager.

- A **composite alarm** includes a rule expression that takes into account the alarm states of other alarms that you have created. The composite alarm goes into ALARM state only if all conditions of the rule are met. The alarms specified in a composite alarm's rule expression can include metric alarms and other composite alarms.

Using composite alarms can reduce alarm noise. You can create multiple metric alarms, and also create a composite alarm and set up alerts only for the composite alarm. For example, a composite might go into ALARM state only when all of the underlying metric alarms are in ALARM state.

Composite alarms can send Amazon SNS notifications when they change state, and can create Systems Manager OpsItems or incidents when they go into ALARM state, but can't perform EC2 actions or Auto Scaling actions.

You can add alarms to CloudWatch dashboards and monitor them visually. When an alarm is on a dashboard, it turns red when it is in the ALARM state, making it easier for you to monitor its status proactively.

An alarm invokes actions only when the alarm changes state. The exception is for alarms with Auto Scaling actions. For Auto Scaling actions, the alarm continues to invoke the action once per minute that the alarm remains in the new state.

An alarm can watch a metric in the same account. If you have enabled cross-account functionality in your CloudWatch console, you can also create alarms that watch metrics in other AWS accounts. Creating cross-account composite alarms is not supported. Creating cross-account alarms that use math expressions is supported, except that the `ANOMALY_DETECTION_BAND`, `INSIGHT_RULE`, and `SERVICE_QUOTA` functions are not supported for cross-account alarms.

**Note**
CloudWatch doesn't test or validate the actions that you specify, nor does it detect any Amazon EC2 Auto Scaling or Amazon SNS errors resulting from an attempt to invoke nonexistent actions. Make sure that your alarm actions exist.

Metric alarm states

A metric alarm has the following possible states:

- **OK** – The metric or expression is within the defined threshold.
- **ALARM** – The metric or expression is outside of the defined threshold.
- **INSUFFICIENT_DATA** – The alarm has just started, the metric is not available, or not enough data is available for the metric to determine the alarm state.
Evaluating an alarm

When you create an alarm, you specify three settings to enable CloudWatch to evaluate when to change the alarm state:

- **Period** is the length of time to evaluate the metric or expression to create each individual data point for an alarm. It is expressed in seconds. If you choose one minute as the period, the alarm evaluates the metric once per minute.
- **Evaluation Periods** is the number of the most recent periods, or data points, to evaluate when determining alarm state.
- **Datapoints to Alarm** is the number of data points within the Evaluation Periods that must be breaching to cause the alarm to go to the **ALARM** state. The breaching data points don't have to be consecutive, they just must all be within the last number of data points equal to **Evaluation Period**.

In the following figure, the alarm threshold for a metric alarm is set to three units. Both **Evaluation Period** and **Datapoints to Alarm** are 3. That is, when all existing data points in the most recent three consecutive periods are above the threshold, the alarm goes to **ALARM** state. In the figure, this happens in the third through fifth time periods. At period six, the value dips below the threshold, so one of the periods being evaluated is not breaching, and the alarm state changes back to **OK**. During the ninth time period, the threshold is breached again, but for only one period. Consequently, the alarm state remains **OK**.

When you configure **Evaluation Periods** and **Datapoints to Alarm** as different values, you're setting an "M out of N" alarm. **Datapoints to Alarm** is ("M") and **Evaluation Periods** is ("N"). The evaluation interval is the number of data points multiplied by the period. For example, if you configure 4 out of 5 data points with a period of 1 minute, the evaluation interval is 5 minutes. If you configure 3 out of 3 data points with a period of 10 minutes, the evaluation interval is 30 minutes.

**Note**

If data points are missing soon after you create an alarm, and the metric was being reported to CloudWatch before you created the alarm, CloudWatch retrieves the most recent data points from before the alarm was created when evaluating the alarm.
Alarm actions

You can specify what actions an alarm takes when it changes state between the OK, ALARM, and INSUFFICIENT_DATA states. The most common type of alarm action is to notify one or more people by sending a message to an Amazon Simple Notification Service topic. For more information about Amazon SNS, see What is Amazon SNS?

Alarms based on EC2 metrics can also perform EC2 actions, such as stopping, terminating, rebooting, or recovering an EC2 instance. For more information, see Create alarms to stop, terminate, reboot, or recover an EC2 instance (p. 125).

Alarms can also perform actions to scale an Auto Scaling group. For more information, see Step and simple scaling policies for Amazon EC2 Auto Scaling.

You can also configure alarms to create OpsItems in Systems Manager Ops Center or create incidents in AWS Systems Manager Incident Manager. These actions be performed only when the alarm goes into ALARM state. For more information, see Configuring CloudWatch to create OpsItems from alarms and Incident creation.

Configuring how CloudWatch alarms treat missing data

Sometimes, not every expected data point for a metric gets reported to CloudWatch. For example, this can happen when a connection is lost, a server goes down, or when a metric reports data only intermittently by design.

CloudWatch enables you to specify how to treat missing data points when evaluating an alarm. This helps you to configure your alarm so that it goes to ALARM state only when appropriate for the type of data being monitored. You can avoid false positives when missing data doesn't indicate a problem.

Similar to how each alarm is always in one of three states, each specific data point reported to CloudWatch falls under one of three categories:

- Not breaching (within the threshold)
- Breaching (violating the threshold)
- Missing

For each alarm, you can specify CloudWatch to treat missing data points as any of the following:

- notBreaching – Missing data points are treated as “good” and within the threshold,
- breaching – Missing data points are treated as “bad” and breaching the threshold
- ignore – The current alarm state is maintained
- missing – If all data points in the alarm evaluation range are missing, the alarm transitions to INSUFFICIENT_DATA.

The best choice depends on the type of metric. For a metric that continually reports data, such as CPUUtilization of an instance, you might want to treat missing data points as breaching, because they might indicate that something is wrong. But for a metric that generates data points only when an error occurs, such as ThrottledRequests in Amazon DynamoDB, you would want to treat missing data as notBreaching. The default behavior is missing.

Choosing the best option for your alarm prevents unnecessary and misleading alarm condition changes, and also more accurately indicates the health of your system.
How alarm state is evaluated when data is missing

Whenever an alarm evaluates whether to change state, CloudWatch attempts to retrieve a higher number of data points than the number specified as Evaluation Periods. The exact number of data points it attempts to retrieve depends on the length of the alarm period and whether it is based on a metric with standard resolution or high resolution. The time frame of the data points that it attempts to retrieve is the evaluation range.

Once CloudWatch retrieves these data points, the following happens:

- If no data points in the evaluation range are missing, CloudWatch evaluates the alarm based on the most recent data points collected. The number of data points evaluated is equal to the Evaluation Periods for the alarm. The extra data points from farther back in the evaluation range are not needed and are ignored.
- If some data points in the evaluation range are missing, but the total number of existing data points that were successfully retrieved from the evaluation range is equal to or more than the alarm’s Evaluation Periods, CloudWatch evaluates the alarm state based on the most recent real data points that were successfully retrieved, including the necessary extra data points from farther back in the evaluation range. In this case, the value you set for how to treat missing data is not needed and is ignored.
- If some data points in the evaluation range are missing, and the number of actual data points that were retrieved is lower than the alarm’s number of Evaluation Periods, CloudWatch fills in the missing data points with the result you specified for how to treat missing data, and then evaluates the alarm. However, all real data points in the evaluation range are included in the evaluation. CloudWatch uses missing data points only as few times as possible.

Note
A particular case of this behavior is that CloudWatch alarms might repeatedly re-evaluate the last set of data points for a period of time after the metric has stopped flowing. This re-evaluation might cause the alarm to change state and re-execute actions, if it had changed state immediately prior to the metric stream stopping. To mitigate this behavior, use shorter periods.

The following tables illustrate examples of the alarm evaluation behavior. In the first table, Datapoints to Alarm and Evaluation Periods are both 3. CloudWatch retrieves the 5 most recent data points when evaluating the alarm, in case some of the most recent 3 data points are missing. 5 is the evaluation range for the alarm.

Column 1 shows the 5 most recent data points, because the evaluation range is 5. These data points are shown with the most recent data point on the right. 0 is a non-breaching data point, X is a breaching data point, and - is a missing data point.

Column 2 shows how many of the 3 necessary data points are missing. Even though the most recent 5 data points are evaluated, only 3 (the setting for Evaluation Periods) are necessary to evaluate the alarm state. The number of data points in Column 2 is the number of data points that must be “filled in”, using the setting for how missing data is being treated.

In columns 3-6, the column headers are the possible values for how to treat missing data. The rows in these columns show the alarm state that is set for each of these possible ways to treat missing data.

<table>
<thead>
<tr>
<th>Data points</th>
<th># of data points that must be filled</th>
<th>MISSING</th>
<th>IGNORE</th>
<th>BREACHING</th>
<th>NOT BREACHING</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 - X - X</td>
<td>0</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
<tr>
<td>0 - - - -</td>
<td>2</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
<td>OK</td>
</tr>
</tbody>
</table>
Data points  | # of data points that must be filled | MISSING | IGNORE | BREACHING | NOT BREACHING
--- | --- | --- | --- | --- | ---
- - - - - | 3 | INSUFFICIENT | Retain current state | ALARM | OK
0 X X - X | 0 | ALARM | ALARM | ALARM | ALARM
--X-- | 2 | ALARM | Retain current state | ALARM | OK

In the second row of the preceding table, the alarm stays OK even if missing data is treated as breaching, because the one existing data point is not breaching, and this is evaluated along with two missing data points which are treated as breaching. The next time this alarm is evaluated, if the data is still missing it will go to ALARM, as that non-breaching data point will no longer be in the evaluation range.

The third row, where all five of the most recent data points are missing, illustrates how the various settings for how to treat missing data affect the alarm state. If missing data points are considered breaching, the alarm goes into ALARM state, while if they are considered not breaching, then the alarm goes into OK state. If missing data points are ignored, the alarm retains the current state it had before the missing data points. And if missing data points are just considered as missing, then the alarm does not have enough recent real data to make an evaluation, and goes into INSUFFICIENT_DATA.

In the fourth row, the alarm goes to ALARM state in all cases because the three most recent data points are breaching, and the alarm’s Evaluation Periods and Datapoints to Alarm are both set to 3. In this case, the missing data point is ignored and the setting for how to evaluate missing data is not needed, because there are 3 real data points to evaluate.

Row 5 represents a special case of alarm evaluation called premature alarm state. For more information, see Avoiding premature transitions to alarm state (p. 107).

In the next table, the Period is again set to 5 minutes, and Datapoints to Alarm is only 2 while Evaluation Periods is 3. This is a 2 out of 3, M out of N alarm.

The evaluation range is 5. This is the maximum number of recent data points that are retrieved and can be used in case some data points are missing.

Data points  | # of missing data points | MISSING | IGNORE | BREACHING | NOT BREACHING
--- | --- | --- | --- | --- | ---
0 - X - X | 0 | ALARM | ALARM | ALARM | ALARM
0 0 X 0 X | 0 | ALARM | ALARM | ALARM | ALARM
0 - X - - | 1 | OK | OK | ALARM | OK
--- - - 0 | 2 | OK | OK | ALARM | OK
--- - X - | 2 | ALARM | Retain current state | ALARM | OK

In rows 1 and 2, the alarm always goes to ALARM state because 2 of the 3 most recent data points are breaching. In row 2, the two oldest data points in the evaluation range are not needed because none of the 3 most recent data points are missing, so these two older data points are ignored.
In rows 3 and 4, the alarm goes to ALARM state only if missing data is treated as breaching, in which case the two most recent missing data points are both treated as breaching. In row 4, these two missing data points that are treated as breaching provide the two necessary breaching data points to trigger the ALARM state.

Row 5 represents a special case of alarm evaluation called premature alarm state. For more information, see the following section.

Avoiding premature transitions to alarm state

CloudWatch alarm evaluation includes logic to try to avoid false alarms, where the alarm goes into ALARM state prematurely when data is intermittent. The example shown in row 5 in the tables in the previous section illustrate this logic. In those rows, and in the following examples, the Evaluation Periods is 3 and the evaluation range is 5 data points. Datapoints to Alarm is 3, except for the M out of N example, where Datapoints to Alarm is 2.

Suppose an alarm's most recent data is - - - - X, with four missing data points and then a breaching data point as the most recent data point. Because the next data point may be non-breaching, the alarm does not go immediately into ALARM state when the data is either - - - - X or - - - X - and Datapoints to Alarm is 3. This way, false positives are avoided when the next data point is non-breaching and causes the data to be - - X O or - X - O.

However, if the last few data points are - X - -, the alarm goes into ALARM state even if missing data points are treated as missing. This is because alarms are designed to always go into ALARM state when the oldest available breaching datapoint during the Evaluation Periods number of data points is at least as old as the value of Datapoints to Alarm, and all other more recent data points are breaching or missing. In this case, the alarm goes into ALARM state even if the total number of datapoints available is lower than M (Datapoints to Alarm).

This alarm logic applies to M out of N alarms as well. If the oldest breaching data point during the evaluation range is at least as old as the value of Datapoints to Alarm, and all of the more recent data points are either breaching or missing, the alarm goes into ALARM state no matter the value of M (Datapoints to Alarm).

High-resolution alarms

If you set an alarm on a high-resolution metric, you can specify a high-resolution alarm with a period of 10 seconds or 30 seconds, or you can set a regular alarm with a period of any multiple of 60 seconds. There is a higher charge for high-resolution alarms. For more information about high-resolution metrics, see Publishing custom metrics (p. 74).

Alarms on math expressions

You can set an alarm on the result of a math expression that is based on one or more CloudWatch metrics. A math expression used for an alarm can include as many as 10 metrics. Each metric must be using the same period.

For an alarm based on a math expression, you can specify how you want CloudWatch to treat missing data points for the underlying metrics when evaluating the alarm.

Alarms based on math expressions can't perform Amazon EC2 actions.

For more information about metric math expressions and syntax, see Using metric math (p. 77).
Percentile-based CloudWatch alarms and low data samples

When you set a percentile as the statistic for an alarm, you can specify what to do when there is not enough data for a good statistical assessment. You can choose to have the alarm evaluate the statistic anyway and possibly change the alarm state. Or, you can have the alarm ignore the metric while the sample size is low, and wait to evaluate it until there is enough data to be statistically significant.

For percentiles between 0.5 (inclusive) and 1.00 (exclusive), this setting is used when there are fewer than 10/(1-percentile) data points during the evaluation period. For example, this setting would be used if there were fewer than 1000 samples for an alarm on a p99 percentile. For percentiles between 0 and 0.5 (exclusive), the setting is used when there are fewer than 10/percentile data points.

Common features of CloudWatch alarms

The following features apply to all CloudWatch alarms:

- You can create up to 5000 alarms per Region per AWS account. To create or update an alarm, you use the CloudWatch console, the `PutMetricAlarm` API action, or the `put-metric-alarm` command in the AWS CLI.
- Alarm names must contain only ASCII characters.
- You can list any or all of the currently configured alarms, and list any alarms in a particular state by using the CloudWatch console, the `DescribeAlarms` API action, or the `describe-alarms` command in the AWS CLI.
- You can disable and enable alarms by using the CloudWatch console, the `DisableAlarmActions` and `EnableAlarmActions` API actions, or the `disable-alarm-actions` and `enable-alarm-actions` commands in the AWS CLI.
- You can test an alarm by setting it to any state using the `SetAlarmState` API action or the `set-alarm-state` command in the AWS CLI. This temporary state change lasts only until the next alarm comparison occurs.
- You can create an alarm for a custom metric before you've created that custom metric. For the alarm to be valid, you must include all of the dimensions for the custom metric in addition to the metric namespace and metric name in the alarm definition. To do this, you can use the `PutMetricAlarm` API action, or the `put-metric-alarm` command in the AWS CLI.
- You can view an alarm's history using the CloudWatch console, the `DescribeAlarmHistory` API action, or the `describe-alarm-history` command in the AWS CLI. CloudWatch preserves alarm history for two weeks. Each state transition is marked with a unique timestamp. In rare cases, your history might show more than one notification for a state change. The timestamp enables you to confirm unique state changes.
- The number of evaluation periods for an alarm multiplied by the length of each evaluation period can't exceed one day.

**Note**

Some AWS resources don't send metric data to CloudWatch under certain conditions. For example, Amazon EBS might not send metric data for an available volume that is not attached to an Amazon EC2 instance, because there is no metric activity to be monitored for that volume. If you have an alarm set for such a metric, you might notice its state change to `INSUFFICIENT_DATA`. This might indicate that your resource is inactive, and might not necessarily mean that there is a problem. You can specify how each alarm treats missing data. For more information, see Configuring how CloudWatch alarms treat missing data (p. 104).
Setting 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 when you create the alarm.

Setting 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
2. On the Amazon SNS dashboard, under Common actions, choose Create Topic.
3. In the Create new topic dialog box, for Topic name, enter 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
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, enter 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
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, enter a subject line for your message, and for Message, enter a brief message.
5. Choose Publish Message.
6. Check your email to confirm that you received the message.
Setting up an SNS topic using the AWS CLI

First, you create an SNS topic, and then you 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.

   ```bash
   aws sns create-topic --name my-topic
   ```

   Amazon SNS returns a topic ARN with the following format:

   ```json
   {
   "TopicArn": "arn:aws:sns:us-east-1:111122223333:my-topic"
   }
   ```

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

   ```bash
   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:

   ```json
   {
   "SubscriptionArn": "pending confirmation"
   }
   ```

3. 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.

4. Check the subscription using the `list-subscriptions-by-topic` command.

   ```bash
   ```

   Amazon SNS returns the following:

   ```json
   {
   "Subscriptions": [
   {
   "Owner": "111122223333",
   "Endpoint": "me@mycompany.com",
   "Protocol": "email",
   }
   ]
   }
   ```

5. (Optional) Publish a test message to the topic using the `publish` command.
Create an alarm based on a static threshold

You choose a CloudWatch metric for the alarm to watch, and the threshold for that metric. The alarm goes to ALARM state when the metric breaches the threshold for a specified number of evaluation periods.

To create an alarm based on a single metric

2. In the navigation pane, choose Alarms, All alarms.
3. Choose Create alarm.
4. Choose Select Metric.
5. (Optional) If you have enabled cross-account functionality in the CloudWatch console and the current account is a monitoring account, under Search Metrics choose a different AWS account that contains the metric that you want the alarm to watch. For more information, see Cross-account cross-Region CloudWatch console (p. 242).
6. Do one of the following:
   - Choose the service namespace that contains the metric that you want. Continue choosing options as they appear to narrow the choices. When a list of metrics appears, select the check box next to the metric that you want.
   - In the search box, enter the name of a metric, dimension, or resource ID and press Enter. Then choose one of the results and continue until a list of metrics appears. Select the check box next to the metric that you want.
7. Choose the Graphed metrics tab.
   a. Under Statistic, choose one of the statistics or predefined percentiles, or specify a custom percentile (for example, p95.45).
   b. Under Period, choose the evaluation period for the alarm. When evaluating the alarm, each period is aggregated into one data point.
      You can also choose whether the y-axis legend appears on the left or right while you’re creating the alarm. This preference is used only while you’re creating the alarm.
   c. Choose Select metric.
      The Specify metric and conditions page appears, showing a graph and other information about the metric and statistic you have selected.
8. Under Conditions, specify the following:

```
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"
}
```

6. Check your email to confirm that you received the message.
Creating a CloudWatch alarm based on anomaly detection

You can create an alarm based on CloudWatch anomaly detection, which mines past metric data and creates a model of expected values. The expected values take into account the typical hourly, daily, and weekly patterns in the metric.
You set a value for the anomaly detection threshold, and CloudWatch uses this threshold with the model to determine the "normal" range of values for the metric. A higher value for the threshold produces a thicker band of "normal" values.

You can choose whether the alarm is triggered when the metric value is above the band of expected values, below the band, or either above or below the band.

For more information, see Using CloudWatch anomaly detection (p. 247).

Note

If you create an anomaly detection alarm on a metric that you're already using anomaly detection for in the Metrics console for visualization purposes, the threshold that you set for the alarm doesn't change the threshold that you're already using for visualization. For more information, see Creating a graph (p. 66).

To create an alarm based on anomaly detection

2. In the navigation pane, choose Alarms, All alarms.
3. Choose Create alarm.
4. Choose Select Metric.
5. Choose Select Metric and do one of the following:
   a. Choose the service namespace that contains the metric that you want. To narrow the choices, continue choosing options as they appear. When a list of metrics appears, select the check box next to the metric that you want.
   b. In the search box, enter the name of a metric, dimension, or resource ID and press Enter. Then choose one of the results and continue until a list of metrics appears. Select the check box next to the metric that you want.
6. Choose the Graphed metrics tab.
   a. Under Statistic, choose one of the statistics or predefined percentiles, or specify a custom percentile (for example, p95.45).
   b. Under Period, choose the evaluation period for the alarm. When evaluating the alarm, each period is aggregated into one data point. For anomaly detection alarms, the value must be one minute or longer.

   You can also choose whether the y-axis legend appears on the left or right while you're creating the alarm. This preference is used only while you're creating the alarm.
   c. Choose Select metric.

   The Specify metric and conditions page appears, showing a graph and other information about the metric and statistic you have selected.
7. Under Conditions, specify the following:
   a. Choose Anomaly detection.

   If the model for this metric and statistic already exists, CloudWatch displays the anomaly detection band in the sample graph at the top of the screen. If the model does not already exist, the model will be generated when you finish creating the alarm. It takes up to 15 minutes for the actual anomaly detection band generated by the model to appear in the graph. Before that, the band you see is an approximation of the anomaly detection band. To see the graph in a longer time frame, choose Edit at the top right of the page.
   b. For Whenever metric is, specify whether the metric must be greater than, lower than, or outside (in either direction) the band to trigger the alarm.
   c. For Anomaly detection threshold, choose the number to use for the anomaly detection threshold. A higher number creates a thicker band of "normal" values that is more tolerant of
metric changes, and a lower number creates a thinner band that will go to ALARM state with smaller metric deviations. The number does not have to be a whole number.

d. Choose Additional configuration. For Datapoints to alarm, specify how many evaluation periods (data points) must be in the ALARM state to trigger the alarm. If the two values here match, you create an alarm that goes to ALARM state if that many consecutive periods are breaching.

To create an M out of N alarm, specify a lower number for the first value than you specify for the second value. For more information, see Evaluating an alarm (p. 103).

e. For Missing data treatment, choose how to have the alarm behave when some data points are missing. For more information, see Configuring how CloudWatch alarms treat missing data (p. 104).

f. If the alarm uses a percentile as the monitored statistic, a Percentiles with low samples box appears. Use it to choose whether to evaluate or ignore cases with low sample rates. If you choose ignore (maintain alarm state), the current alarm state is always maintained when the sample size is too low. For more information, see Percentile-based CloudWatch alarms and low data samples (p. 108).

8. Choose Next.

9. Under Notification, select an SNS topic to notify when the alarm is in ALARM state, OK state, or INSUFFICIENT_DATA state.

To have the alarm send multiple notifications for the same alarm state or for different alarm states, choose Add notification.

To have the alarm not send notifications, choose Remove.

10. To have the alarm perform EC2 actions when it changes state or create a Systems Manager OpsItem or incident when it goes into ALARM state, choose the appropriate button and choose the alarm state and action to perform.

For more information about Systems Manager actions, see Configuring CloudWatch to create OpsItems from alarms and Incident creation.

Note
To create an alarm that performs an SSM Incident Manager action, you must have certain permissions. For more information, see Identity-based policy examples for AWS Systems Manager Incident Manager.

11. When finished, choose Next.

12. Enter a name and description for the alarm. The name must contain only ASCII characters. Then choose Next.

13. Under Preview and create, confirm that the information and conditions are what you want, then choose Create alarm.

Modifying an anomaly detection model

Once you have created an alarm, you can adjust the anomaly detection model. You can exclude certain time periods from being used in the model creation. It is critical that you exclude unusual events such as system outages, deployments, and holidays from the training data. You can also specify whether to adjust the model for daylight savings time changes.

To adjust the anomaly detection model for an alarm


2. In the navigation pane, choose Alarms.

3. Choose the name of the alarm. Use the search box to find the alarm if necessary.
4. Choose View in metrics.
5. In the lower part of the screen, choose Edit model.
6. To exclude a time period from being used to produce the model, choose Add another time range to exclude from training. Then select or enter the days and times to exclude from training, and choose Apply.
7. If the metric is sensitive to daylight savings time changes, select the appropriate time zone in the Metric timezone box.
8. Choose Update.

Deleting an anomaly detection model

Using anomaly detection for an alarm accrues AWS charges. If you no longer need an anomaly detection model for an alarm, you should delete the alarm and then the model. If you delete the model without deleting the alarm, the alarm automatically recreates the model.

To delete an alarm
2. In the navigation pane, choose Alarms.
3. Choose the name of the alarm.
4. Choose Actions, Delete.

To delete the anomaly detection model that had been used for an alarm
2. In the navigation pane, choose Metrics.
3. On the All metrics tab, enter a search term in the search field, such as a metric name or resource name, and press Enter.

For example, if you search for the CPUUtilization metric, you see the namespaces and dimensions with this metric.
4. In the results, select the metric that had the anomaly detection model.
5. Choose the Graphed metrics tab.
6. In the lower part of the screen, choose Edit model and then Delete model.

Creating a CloudWatch alarm based on a metric math expression

To create an alarm based on a metric math expression, choose one or more CloudWatch metrics to use in the expression. Then, specify the expression, threshold, and evaluation periods.

To create an alarm based on a math expression
2. In the navigation pane, choose Alarms, All alarms.
3. Choose Create alarm.
4. Choose **Select Metric**.

5. (Optional) If you have enabled cross-account functionality in the CloudWatch console and the current account is a monitoring account, under **Search Metrics** choose choose a different AWS account that contains the metric that you want the alarm to watch. For more information, see [Cross-account cross-Region CloudWatch console (p. 242)](https://docs.aws.amazon.com/AmazonCloudWatch/latest/UserGuide/cross-account-cross-region.html).

6. Choose **Select Metric** and do one of the following:
   - Choose the service namespace that contains a specific metric. Continue choosing options as they appear to narrow the choices. When a list of metrics appears, select the check box next to the right metric.
   - In the search box, enter the name of a metric, dimension, or resource ID and press Enter. Choose one of the results and continue until a list of metrics appears. Select the check box next to the right metric.

   (Optional) To add another metric to use in the math expression, under **All metrics**, choose **All**, find the specific metric, and then select the check box next to it. You can add up to 10 metrics.

7. Choose **Graphed metrics**. For each metric added, do the following:
   - Under **Statistic**, choose one of the statistics or predefined percentiles, or specify a custom percentile (for example, \( p_{95.45} \)).
   - Under **Period**, choose the evaluation period for the alarm. When evaluating the alarm, each period is aggregated into one data point.

     You can also choose whether the y-axis legend appears on the left or right while you're creating the alarm. This preference is used only while you're creating the alarm.

8. Choose **Add a math expression**. A new row appears for the expression.

9. On the new row, under the **Details** column, enter the math expression and press Enter. For information about the functions and syntax that you can use, see [Metric math syntax and functions (p. 78)](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/MetricMathSyntax.html).

   To use a metric or the result of another expression as part of the formula for this expression, use the value shown in the **Id** column: for example, \( m1+m2 \) or \( e1-MIN(e1) \).

   You can change the value of **Id**. It can include numbers, letters, and underscores, and it must start with a lowercase letter. Changing the value of **Id** to a more meaningful name can also make the alarm graph easier to understand.

10. (Optional) Add more math expressions, using both metrics and the results of other math expressions in the formulas of the new math expressions.

11. When you have the expression to use for the alarm, clear the check boxes to the left of every other expression and every metric on the page. Only the check box next to the expression to use for the alarm should be selected. The expression that you choose for the alarm must produce a single time series and show only one line on the graph. Then choose **Select metric**.

    The **Specify metric and conditions** page appears, showing a graph and other information about the math expression that you have selected.

12. For **Whenever expression is**, specify whether the expression must be greater than, less than, or equal to the threshold. Under **than...**, specify the threshold value.

13. Choose **Additional configuration**. For **Datapoints to alarm**, specify how many evaluation periods (data points) must be in the **ALARM** state to trigger the alarm. If the two values here match, you create an alarm that goes to **ALARM** state if that many consecutive periods are breaching.

    To create an **M out of N** alarm, specify a lower number for the first value than you specify for the second value. For more information, see [Evaluating an alarm (p. 103)](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Evaluating-Alarms.html).

14. For **Missing data treatment**, choose how to have the alarm behave when some data points are missing. For more information, see [Configuring how CloudWatch alarms treat missing data (p. 104)](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/Configuring-Missing-Data-Handling.html).
Creating a composite alarm

Composite alarms are alarms that determine their alarm state by watching the alarm states of other alarms.

Using composite alarms can help you reduce alarm noise. If you set up a composite alarm to notify you of state changes, but set up the underlying metric alarms to not send notifications themselves, you will be notified only when the alarm state of the composite alarm changes. For example, you could create metric alarms based on both CPU utilization and disk read operations, and specify for these alarms to never take actions. You could then create a composite alarm that goes into ALARM state and notifies you only when both of those metric alarms are in ALARM state.

In a composite alarm, all underlying alarms must be in the same AWS Region and the same account.

Currently, the only alarm actions that can be taken by composite alarms are notifying SNS topics.

Rule expressions

Each composite alarms includes a rule expression, which specifies which other alarms are to be evaluated to determine the composite alarm’s state. For each alarm that you reference in the rule expression, you designate a function that specifies whether that alarm needs to be in ALARM state, OK state, or INSUFFICIENT_DATA state. You can use operators (AND, OR and NOT) to combine multiple functions in a single expression. You can use parenthesis to logically group the functions in your expression.

A rule expression can refer to both metric alarms and other composite alarms.

Functions can include the following:
• ALARM("alarm-name or alarm-ARN") is TRUE if the named alarm is in ALARM state.
• OK("alarm-name or alarm-ARN") is TRUE if the named alarm is in OK state.
• INSUFFICIENT_DATA("alarm-name or alarm-ARN") is TRUE if the named alarm is in INSUFFICIENT_DATA state.
• TRUE always evaluates to TRUE.
• FALSE always evaluates to FALSE.

TRUE and FALSE are useful for testing a complex AlarmRule structure, and for testing your alarm actions.

The following are some examples of AlarmRule:

• ALARM(CPUUtilizationTooHigh) AND ALARM(DiskReadOpsTooHigh) specifies that the composite alarm goes into ALARM state only if both CPUUtilizationTooHigh and DiskReadOpsTooHigh alarms are in ALARM state.
• ALARM(CPUUtilizationTooHigh) AND NOT ALARM(DeploymentInProgress) specifies that the alarm goes to ALARM state if CPUUtilizationTooHigh is in ALARM state and DeploymentInProgress is not in ALARM state. This example reduces alarm noise during a known deployment window.
• (ALARM(CPUUtilizationTooHigh) OR ALARM(DiskReadOpsTooHigh)) AND OK(NetworkOutTooHigh) goes into ALARM state if CPUUtilizationTooHigh OR DiskReadOpsTooHigh is in ALARM state, and if NetworkOutTooHigh is in OK state. This provides another example of using a composite alarm to prevent noise. This rule ensures that you are not notified with an alarm action on high CPU or disk usage if a known network problem is also occurring.

An AlarmRule expression can specify as many as 100 "child" alarms. The AlarmRule expression can have as many as 500 elements. Elements are child alarms, TRUE or FALSE statements, and parentheses. A pair of parentheses counts as one element.

A rule expression must contain at least one child alarm or at least one TRUE statement or FALSE statement.

To create a composite alarm

2. In the navigation pane, choose Alarms.
3. In the list of alarms, select the check boxes next to each of the existing alarms that you want to reference in your new composite alarm. Then choose Create composite alarm.
4. In the Conditions box, specify the rule expression that the composite alarm will use. Initially, the alarms you selected are listed, joined by the OR logical operator. Each of these alarms has the ALARM state specified.

You can modify the alarm conditions for the composite alarm that you are creating:

a. For each underlying alarm listed, you can change the required state from ALARM to OK or INSUFFICIENT_DATA.

b. You can change each OR operator to AND or NOT. You can also add parentheses to group the logical operators.

c. You can add more alarms to the composite alarm conditions. You can also delete alarms currently listed in the Conditions box.

For example, you could specify the following conditions to create a composite alarm that goes into ALARM state if CPUUtilizationTooHigh OR DiskReadOpsTooHigh is in ALARM state, at the same time that NetworkOutTooHigh is in OK state.
 Editing or deleting a CloudWatch alarm

You can edit or delete an existing alarm.

**To edit an alarm**

2. In the navigation pane, choose **Alarms**.
3. Choose the name of the alarm.
4. Choose **Edit**.
   
   The **Specify metric and conditions** page appears, showing a graph and other information about the metric and statistic that you selected.
5. To change the metric, choose **Edit**, choose the **All metrics** tab, and do one of the following:
• Choose the service namespace that contains the metric that you want. Continue choosing options as they appear to narrow the choices. When a list of metrics appears, select the check box next to the metric that you want.
• In the search box, enter the name of a metric, dimension, or resource ID and press Enter. Then choose one of the results and continue until a list of metrics appears. Select the check box next to the metric that you want.

Choose Select metric.

6. To change other aspects of the alarm, choose the appropriate options. To change how many data points must be breaching for the alarm to go into ALARM state or to change how missing data is treated, choose Additional configuration.
7. Choose Next.
8. Under Notification, Auto Scaling action, and EC2 action, optionally edit the actions taken when the alarm is triggered. Then choose Next.
9. Optionally change the alarm description.

You can’t change the name of an existing alarm. You can copy an alarm and give the new alarm a different name. To copy an alarm, select the check box next to the alarm name in the alarm list and choose Action, Copy.
10. Choose Next.
11. Under Preview and create, confirm that the information and conditions are what you want, then choose Update alarm.

To update an email notification list that was created using the Amazon SNS console

2. In the navigation pane, choose Topics and then select the ARN for your notification list (topic).
3. Do one of the following:
   • To add an email address, choose Create subscription. For Protocol, choose Email. For Endpoint, enter the email address of the new recipient. Choose Create subscription.
   • To remove an email address, choose the Subscription ID. Choose Other subscription actions, Delete subscriptions.
4. Choose Publish to topic.

To delete an alarm

2. In the navigation pane, choose Alarms.
3. Select the check box to the left of the name of the alarm, and choose Actions, Delete.
4. Choose Delete.

Creating a CPU usage alarm

You can create an CloudWatch alarm that sends a notification using Amazon SNS when the alarm changes state from OK to ALARM.

The alarm changes to the ALARM state when the average CPU use of an EC2 instance exceeds a specified threshold for consecutive specified periods.
Setting up a CPU usage alarm using the AWS Management Console

Use these steps to use the AWS Management Console to create a CPU usage alarm.

To create an alarm based on CPU usage

2. In the navigation pane, choose Alarms, Create Alarm.
3. Choose Select metric.
4. In the All metrics tab, choose EC2 metrics.
5. Choose a metric category (for example, Per-Instance Metrics).
6. Find the row with the instance that you want listed in theInstanceId column and CPUUtilization in the Metric Name column. Select the check box next to this row, and choose Select metric.
7. Under Specify metric and conditions, for Statistic choose Average, choose one of the predefined percentiles, or specify a custom percentile (for example, p95.45).
8. Choose a period (for example, 5 minutes).
9. Under Conditions, specify the following:
   a. For Threshold type, choose Static.
   b. For Whenever CPUUtilization is, specify Greater. Under than..., specify the threshold that is to trigger the alarm to go to ALARM state if the CPU utilization exceeds this percentage. For example, 70.
   c. Choose Additional configuration. For Datapoints to alarm, specify how many evaluation periods (data points) must be in the ALARM state to trigger the alarm. If the two values here match, you create an alarm that goes to ALARM state if that many consecutive periods are breaching.
   To create an M out of N alarm, specify a lower number for the first value than you specify for the second value. For more information, see Evaluating an alarm (p. 103).
   d. For Missing data treatment, choose how to have the alarm behave when some data points are missing. For more information, see Configuring how CloudWatch alarms treat missing data (p. 104).
   e. If the alarm uses a percentile as the monitored statistic, a Percentiles with low samples box appears. Use it to choose whether to evaluate or ignore cases with low sample rates. If you choose ignore (maintain alarm state), the current alarm state is always maintained when the sample size is too low. For more information, see Percentile-based CloudWatch alarms and low data samples (p. 108).
10. Choose Next.
11. Under Notification, choose In alarm and select an SNS topic to notify when the alarm is in ALARM state.
   To have the alarm send multiple notifications for the same alarm state or for different alarm states, choose Add notification.
   To have the alarm not send notifications, choose Remove.
12. When finished, choose Next.
13. Enter a name and description for the alarm. The name must contain only ASCII characters. Then choose Next.
14. Under Preview and create, confirm that the information and conditions are what you want, then choose Create alarm.
Setting up a CPU usage alarm using the AWS CLI

Use these steps to use the AWS CLI to create a CPU usage alarm.

To create an alarm based on CPU usage

1. Set up an SNS topic. For more information, see Setting up Amazon SNS notifications (p. 109).
2. Create an alarm using the `put-metric-alarm` command as follows.

```
aws cloudwatch put-metric-alarm --alarm-name cpu-mon --alarm-description "Alarm when CPU exceeds 70%" --metric-name CPUUtilization --namespace AWS/EC2 --statistic Average --period 300 --threshold 70 --comparison-operator GreaterThanThreshold --dimensions Name=InstanceId,Value=i-12345678 --evaluation-periods 2 --alarm-actions arn:aws:sns:us-east-1:1111222333:my-topic --unit Percent
```

3. Test the alarm by forcing an alarm state change using the `set-alarm-state` command.
   a. Change the alarm state from INSUFFICIENT_DATA to OK.
      ```
      aws cloudwatch set-alarm-state --alarm-name cpu-mon --state-reason "initializing" --state-value OK
      ```
   b. Change the alarm state from OK to ALARM.
      ```
      aws cloudwatch set-alarm-state --alarm-name cpu-mon --state-reason "initializing" --state-value ALARM
      ```
   c. Check that you have received a notification about the alarm.

Creating a load balancer latency alarm that sends email

You can set up an Amazon SNS notification and configure an alarm that monitors latency exceeding 100 ms for your Classic Load Balancer.

Setting up a latency alarm using the AWS Management Console

Use these steps to use the AWS Management Console to create a load balancer latency alarm.

To create a load balancer latency alarm

2. In the navigation pane, choose Alarms, Create Alarm.
3. Under CloudWatch Metrics by Category, choose the ELB Metrics category.
4. Select the row with the Classic Load Balancer and the Latency metric.
5. For the statistic, choose Average, choose one of the predefined percentiles, or specify a custom percentile (for example, p95.45).
6. For the period, choose 1 Minute.
7. Choose Next.
8. Under **Alarm Threshold**, enter a unique name for the alarm (for example, `myHighCpuAlarm`) and a description of the alarm (for example, **Alarm when Latency exceeds 100s**). Alarm names must contain only ASCII characters.

9. Under **Whenever**, for **is**, choose > and enter **0.1**. For **for**, enter **3**.

10. Under **Additional settings**, for **Treat missing data as**, choose **ignore (maintain alarm state)** so that missing data points don’t trigger alarm state changes.

    For **Percentiles with low samples**, choose **ignore (maintain the alarm state)** so that the alarm evaluates only situations with adequate numbers of data samples.

11. Under **Actions**, for **Whenever this alarm**, choose **State is ALARM**. For **Send notification to**, choose an existing SNS topic or create a new one.

    To create an SNS topic, choose **New list**. For **Send notification to**, enter a name for the SNS topic (for example, `myHighCpuAlarm`), and for **Email list**, enter a comma-separated list of email addresses to be notified when the alarm changes to the **ALARM** state. Each email address is sent a topic subscription confirmation email. You must confirm the subscription before notifications can be sent.

12. Choose **Create Alarm**.

### Setting up a latency alarm using the AWS CLI

Use these steps to use the AWS CLI to create a load balancer latency alarm.

**To create a load balancer latency alarm**

1. Set up an SNS topic. For more information, see [Setting up Amazon SNS notifications (p. 109)](#).

2. Create the alarm using the `put-metric-alarm` command as follows:

   ```bash
   aws cloudwatch put-metric-alarm --alarm-name lb-mon --alarm-description "Alarm when Latency exceeds 100s" --metric-name Latency --namespace AWS/ELB --statistic Average --period 60 --threshold 100 --comparison-operator GreaterThanThreshold --dimensions Name=LoadBalancerName,Value=my-server --evaluation-periods 3 --alarm-actions arn:aws:sns:us-east-1::11112223333:my-topic --unit Seconds
   ```

3. Test the alarm by forcing an alarm state change using the `set-alarm-state` command.

   a. Change the alarm state from **INSUFFICIENT_DATA** to **OK**.

      ```bash
      aws cloudwatch set-alarm-state --alarm-name lb-mon --state-reason "initializing" --state-value OK
      ```

   b. Change the alarm state from **OK** to **ALARM**.

      ```bash
      aws cloudwatch set-alarm-state --alarm-name lb-mon --state-reason "initializing" --state-value ALARM
      ```

   c. Check that you have received an email notification about the alarm.

### Creating a storage throughput alarm that sends email

You can set up an SNS notification and configure an alarm that is triggered when Amazon EBS exceeds 100 MB throughput.
Setting up a storage throughput alarm using the AWS Management Console

Use these steps to use the AWS Management Console to create an alarm based on Amazon EBS throughput.

To create a storage throughput alarm

2. In the navigation pane, choose Alarms, Create Alarm.
3. Under EBS Metrics, choose a metric category.
4. Select the row with the volume and the VolumeWriteBytes metric.
5. For the statistic, choose Average. For the period, choose 5 Minutes. Choose Next.
6. Under Alarm Threshold, enter a unique name for the alarm (for example, myHighWriteAlarm) and a description of the alarm (for example, VolumeWriteBytes exceeds 100,000 KiB/s). Alarm names must contain only ASCII characters.
7. Under Whenever, for is, choose > and enter 100000. For for, enter 15 consecutive periods.
   A graphical representation of the threshold is shown under Alarm Preview.
8. Under Additional settings, for Treat missing data as, choose ignore (maintain alarm state) so that missing data points don't trigger alarm state changes.
9. Under Actions, for Whenever this alarm, choose State is ALARM. For Send notification to, choose an existing SNS topic or create one.
   To create an SNS topic, choose New list. For Send notification to, enter a name for the SNS topic (for example, myHighCpuAlarm), and for Email list, enter a comma-separated list of email addresses to be notified when the alarm changes to the ALARM state. Each email address is sent a topic subscription confirmation email. You must confirm the subscription before notifications can be sent to an email address.
10. Choose Create Alarm.

Setting up a storage throughput alarm using the AWS CLI

Use these steps to use the AWS CLI to create an alarm based on Amazon EBS throughput.

To create a storage throughput alarm

1. Create an SNS topic. For more information, see Setting up Amazon SNS notifications (p. 109).
2. Create the alarm.
   ```sh
   ```
3. Test the alarm by forcing an alarm state change using the set-alarm-state command.
   a. Change the alarm state from INSUFFICIENT_DATA to OK.
Create alarms to stop, terminate, reboot, or recover an EC2 instance

Using Amazon CloudWatch alarm actions, you can create alarms that automatically stop, terminate, reboot, or recover your EC2 instances. You can use the stop or terminate actions to help you save money when you no longer need an instance to be running. You can use the reboot and recover actions to automatically reboot those instances or recover them onto new hardware if a system impairment occurs.

There are a number of scenarios in which you might want to automatically stop or terminate your instance. For example, you might have instances dedicated to batch payroll processing jobs or scientific computing tasks that run for a period of time and then complete their work. Rather than letting those instances sit idle (and accrue charges), you can stop or terminate them, which helps you to save money. The main difference between using the stop and the terminate alarm actions is that you can easily restart a stopped instance if you need to run it again later. You can also keep the same instance ID and root volume. However, you cannot restart a terminated instance. Instead, you must launch a new instance.

You can add the stop, terminate, reboot, or recover actions to any alarm that is set on an Amazon EC2 per-instance metric, including basic and detailed monitoring metrics provided by Amazon CloudWatch (in the AWS/EC2 namespace), in addition to any custom metrics that include the "InstanceId=" dimension, as long as the InstanceId value refers to a valid running Amazon EC2 instance.

To set up a CloudWatch alarm action that can reboot, stop, or terminate an instance, you must use a service-linked IAM role, AWSServiceRoleForCloudWatchEvents. The AWSServiceRoleForCloudWatchEvents IAM role enables AWS to perform alarm actions on your behalf.

To create the service-linked role for CloudWatch Events, use the following command:

```
aws iam create-service-linked-role --aws-service-name events.amazonaws.com
```

**Console support**

You can create alarms using the CloudWatch console or the Amazon EC2 console. The procedures in this documentation use the CloudWatch console. For procedures that use the Amazon EC2 console, see Create Alarms That Stop, Terminate, Reboot, or Recover an Instance in the Amazon EC2 User Guide for Linux Instances.

**Permissions**

```
aws cloudwatch set-alarm-state --alarm-name ebs-mon --state-reason "initializing" --state-value OK
```

b. Change the alarm state from OK to ALARM.

```
aws cloudwatch set-alarm-state --alarm-name ebs-mon --state-reason "initializing" --state-value ALARM
```

c. Change the alarm state from ALARM to INSUFFICIENT_DATA.

```
aws cloudwatch set-alarm-state --alarm-name ebs-mon --state-reason "initializing" --state-value INSUFFICIENT_DATA
```

d. Check that you have received an email notification about the alarm.
Adding stop actions to Amazon CloudWatch alarms

You can create an alarm that stops an Amazon EC2 instance when a certain threshold has been met. For example, you may run development or test instances and occasionally forget to shut them off. You can create an alarm that is triggered when the average CPU utilization percentage has been lower than 10 percent for 24 hours, signaling that it is idle and no longer in use. You can adjust the threshold, duration, and period to suit your needs, plus you can add an SNS notification, so that you will receive an email when the alarm is triggered.

Amazon EC2 instances that use an Amazon Elastic Block Store volume as the root device can be stopped or terminated, whereas instances that use the instance store as the root device can only be terminated.

To create an alarm to stop an idle instance using the Amazon CloudWatch console

1. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/
2. In the navigation pane, choose Alarms, Create Alarm.
3. For the Select Metric step, do the following:
   a. Under EC2 Metrics, choose Per-Instance Metrics.
   b. Select the row with the instance and the CPUUtilization metric.
   c. For the statistic, choose Average.
   d. Choose a period (for example, 1 Hour).
   e. Choose Next.
4. For the Define Alarm step, do the following:
   a. Under Alarm Threshold, type a unique name for the alarm (for example, Stop EC2 instance) and a description of the alarm (for example, Stop EC2 instance when CPU is idle too long). Alarm names must contain only ASCII characters.
   b. Under Whenever, for is, choose < and type 10. For for, type 24 consecutive periods.

   A graphical representation of the threshold is shown under Alarm Preview.
   c. Under Notification, for Send notification to, choose an existing Alarm SNS topic or create a new one.

      To create an SNS topic, choose New list. For Send notification to, type a name for the SNS topic (for example, Stop_EC2_Instance). For Email list, type a comma-separated list of email addresses to be notified when the alarm changes to the ALARM state. Each email address is sent a topic subscription confirmation email. You must confirm the subscription before notifications can be sent to an email address.

   d. Choose EC2 Action.
   e. For Whenever this alarm, choose State is ALARM. For Take this action, choose Stop this instance.
Adding terminate actions to Amazon CloudWatch alarms

You can create an alarm that terminates an EC2 instance automatically when a certain threshold has been met (as long as termination protection is not enabled for the instance). For example, you might want to terminate an instance when it has completed its work, and you don't need the instance again. If you might want to use the instance later, you should stop the instance instead of terminating it.

For information about enabling and disabling termination protection for an instance, see Enabling Termination Protection for an Instance in the Amazon EC2 User Guide for Linux Instances.

To create an alarm to terminate an idle instance using the Amazon CloudWatch console

2. In the navigation pane, choose Alarms, Create Alarm.
3. For the Select Metric step, do the following:
   a. Under EC2 Metrics, choose Per-Instance Metrics.
   b. Select the row with the instance and the CPUUtilization metric.
   c. For the statistic, choose Average.
   d. Choose a period (for example, 1 Hour).
   e. Choose Next.
4. For the Define Alarm step, do the following:
   a. Under Alarm Threshold, type a unique name for the alarm (for example, Terminate EC2 instance) and a description of the alarm (for example, Terminate EC2 instance when CPU is idle for too long). Alarm names must contain only ASCII characters.
   b. Under Whenever, for is, choose < and type 10. For for, type 24 consecutive periods.
   c. Under Notification, for Send notification to, choose an existing SNS topic or create a new one.
   d. Choose EC2 Action.
   e. For Whenever this alarm, choose State is ALARM. For Take this action, choose Terminate this instance.
   f. Choose Create Alarm.

Adding reboot actions to Amazon CloudWatch alarms

You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically reboots the instance. The reboot alarm action is recommended for Instance Health Check failures (as opposed to the recover alarm action, which is suited for System Health Check failures). An instance reboot is equivalent to an operating system reboot. In most cases, it takes only a few minutes to reboot your instance. When you reboot an instance, it remains on the same physical host, so your instance keeps its public DNS name, private IP address, and any data on its instance store volumes.
Rebooting an instance doesn’t start a new instance billing hour, unlike stopping and restarting your instance. For more information about rebooting an instance, see Reboot Your Instance in the Amazon EC2 User Guide for Linux Instances.

**Important**
To avoid a race condition between the reboot and recover actions, avoid setting the same evaluation period for both a reboot alarm and a recover alarm. We recommend that you set reboot alarms to three evaluation periods of one minute each.

**To create an alarm to reboot an instance using the Amazon CloudWatch console**
2. In the navigation pane, choose Alarms, Create Alarm.
3. For the **Select Metric** step, do the following:
   a. Under EC2 Metrics, choose Per-Instance Metrics.
   b. Select the row with the instance and the StatusCheckFailed_Instance metric.
   c. For the statistic, choose Minimum.
   d. Choose a period (for example, 1 Minute) and choose Next.
4. For the **Define Alarm** step, do the following:
   a. Under Alarm Threshold, type a unique name for the alarm (for example, Reboot EC2 instance) and a description of the alarm (for example, Reboot EC2 instance when health checks fail). Alarm names must contain only ASCII characters.
   b. Under Whenever, for is, choose > and type 0. For for, type 3 consecutive periods.
   A graphical representation of the threshold is shown under Alarm Preview.
   c. Under Notification, for Send notification to, choose an existing SNS topic or create a new one.
   To create an SNS topic, choose New list. For Send notification to, type a name for the SNS topic (for example, Reboot_EC2_Instance). For Email list, type a comma-separated list of email addresses to be notified when the alarm changes to the ALARM state. Each email address is sent a topic subscription confirmation email. You must confirm the subscription before notifications can be sent to an email address.
   d. Choose EC2 Action.
   e. For Whenever this alarm, choose State is ALARM. For Take this action, choose Reboot this instance.
   f. Choose Create Alarm.

**Adding recover actions to Amazon CloudWatch alarms**
You can create an Amazon CloudWatch alarm that monitors an Amazon EC2 instance and automatically recovers the instance if it becomes impaired due to an underlying hardware failure or a problem that requires AWS involvement to repair. Terminated instances cannot be recovered. A recovered instance is identical to the original instance, including the instance ID, private IP addresses, Elastic IP addresses, and all instance metadata.

When the StatusCheckFailed_System alarm is triggered, and the recover action is initiated, you will be notified by the Amazon SNS topic that you chose when you created the alarm and associated the recover action. During instance recovery, the instance is migrated during an instance reboot, and any data that is in-memory is lost. When the process is complete, information is published to the SNS topic you’ve configured for the alarm. Anyone who is subscribed to this SNS topic will receive an email.
notification that includes the status of the recovery attempt and any further instructions. You will notice an instance reboot on the recovered instance.

The recover action can be used only with `StatusCheckFailed_System`, not with `StatusCheckFailed_Instance`.

Examples of problems that cause system status checks to fail include:

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

The recover action is supported only on:

- The A1, C3, C4, C5, C5a, C5n, C6g, Inf1, M3, M4, M5, M5a, M5n, M5zn, M6g, P3, P4, R3, R4, R5, R5a, R5b, R5n, T2, T3, T3a, T4g, X1, and X1e instance types
- Instances in a VPC
- Instances with default or dedicated instance tenancy
- Instances that use Amazon EBS volumes only (do not configure instance store volumes)

If your instance has a public IPv4 address, it retains the public IP address after recovery.

`Important`

To avoid a race condition between the reboot and recover actions, avoid setting the same evaluation period for both a reboot alarm and a recover alarm. We recommend that you set recover alarms to two evaluation periods of one minute each and reboot alarms to three evaluation periods of one minute each.

**To create an alarm to recover an instance using the Amazon CloudWatch console**

2. In the navigation pane, choose **Alarms, Create Alarm**.
3. For the **Select Metric** step, do the following:
   a. Under EC2 Metrics, choose **Per-Instance Metrics**.
   b. Select the row with the instance and the `StatusCheckFailed_System` metric.
   c. For the statistic, choose **Minimum**.
   d. Choose a period (for example, 1 Minute).
      
      `Important`

      To avoid a race condition between the reboot and recover actions, avoid setting the same evaluation period for both a reboot alarm and a recover alarm. We recommend that you set recover alarms to two evaluation periods of one minute each.

   e. Choose **Next**.
4. For the **Define Alarm** step, do the following:
   a. Under **Alarm Threshold**, type a unique name for the alarm (for example, Recover EC2 instance) and a description of the alarm (for example, Recover EC2 instance when health checks fail). Alarm names must contain only ASCII characters.
   b. Under **Whenever**, for is, choose > and type 0. For for, type 2 consecutive periods.
   c. Under **Notification**, for **Send notification to**, choose an existing SNS topic or create a new one.

      To create an SNS topic, choose **New list**. For **Send notification to**, type a name for the SNS topic (for example, Recover_EC2_Instance). For **Email list**, type a comma-separated list of email addresses.
addresses to be notified when the alarm changes to the **ALARM** state. Each email address is sent a topic subscription confirmation email. You must confirm the subscription before notifications can be sent to an email address.

d. Choose **EC2 Action**.

e. For **Whenever this alarm**, choose **State is ALARM**. For **Take this action**, choose **Recover this instance**.

f. Choose **Create Alarm**.

**Viewing the history of triggered alarms and actions**

You can view alarm and action history in the Amazon CloudWatch console. Amazon CloudWatch keeps the last two weeks' worth of alarm and action history.

**To view the history of triggered alarms and actions**

2. In the navigation pane, choose **Alarms** and select an alarm.
3. To view the most recent state transition along with the time and metric values, choose **Details**.
4. To view the most recent history entries, choose **History**.

**Creating a billing alarm to monitor your estimated AWS charges**

You can monitor your estimated AWS charges by using Amazon CloudWatch. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data.

Billing metric data is stored in the US East (N. Virginia) Region and represents worldwide charges. This data includes the estimated charges for every service in AWS that you use, in addition to the estimated overall total of your AWS charges.

The alarm triggers when your account billing exceeds the threshold you specify. It triggers only when actual billing exceeds the threshold. It doesn't use projections based on your usage so far in the month.

If you create a billing alarm at a time when your charges have already exceeded the threshold, the alarm goes to the **ALARM** state immediately.

**Tasks**

- Enabling billing alerts (p. 130)
- Creating a billing alarm (p. 131)
- Deleting a billing alarm (p. 132)

**Enabling billing alerts**

Before you can create an alarm for your estimated charges, you must enable billing alerts, so that you can monitor your estimated AWS charges and create an alarm using billing metric data. After you enable billing alerts, you can't disable data collection, but you can delete any billing alarms that you created.

After you enable billing alerts for the first time, it takes about 15 minutes before you can view billing data and set billing alarms.
Requirements

- You must be signed in using account root user credentials or as an IAM user that has been given permission to view billing information.
- For consolidated billing accounts, billing data for each linked account can be found by logging in as the paying account. You can view billing data for total estimated charges and estimated charges by service for each linked account, in addition to the consolidated account.
- In a consolidated billing account, member linked account metrics are captured only if the payer account enables the Receive Billing Alerts preference. If you change which account is your master/payer account, you must enable the billing alerts in the new master/payer account.
- The account must not be part of the Amazon Partner Network (APN) because billing metrics are not published to CloudWatch for APN accounts. For more information, see AWS Partner Network.

To enable the monitoring of estimated charges

2. In the navigation pane, choose Billing Preferences.
4. Choose Save preferences.

Creating a billing alarm

**Important**
Before you can create a billing alarm, you must enable billing alerts in your account, or in the master/payer account if you are using consolidated billing. For more information, see Enabling billing alerts (p. 130).

In this procedure, you create an alarm that sends a notification when your estimated charges for AWS exceed a specified threshold. This procedure uses the advanced options. For more information about using the simple options, see Create a Billing Alarm (p. 690) in Monitor Your Estimated Charges Using CloudWatch.

To create a billing alarm using the CloudWatch console

2. If necessary, change the Region to US East (N. Virginia). Billing metric data is stored in this Region and represents worldwide charges.
3. In the navigation pane, choose Alarms, Create Alarm.
4. Choose Select metric. In the All metrics tab, choose Billing, Total Estimated Charge.

   If you don't see Billing or the Total Estimated Charge metric, you may need to enable billing alerts. For more information, see Enabling billing alerts (p. 130).
5. Select the check box next to EstimatedCharges, and choose Select metric.
6. Under Conditions, choose Static.
7. For Whenever EstimatedCharges is, choose Greater.
8. For than, enter the monthly amount (for example, 200) that must be exceeded to trigger the alarm.

   **Note**
   The preview graph displays your current charges for the month.
9. Choose Next.
10. For Select an SNS topic, select an SNS topic to notify when the alarm is in ALARM state, or create a new topic to be notified.
To have the alarm send multiple notifications for the same alarm state or for different alarm states, choose Add notification.

11. When finished, choose Next.

12. Enter a name and description for the alarm. The name must contain only ASCII characters. Then choose Next.

13. Under Preview and create, confirm that the information and conditions are what you want, then choose Create alarm.

Deleting a billing alarm

You can delete your billing alarm when you no longer need it.

To delete a billing alarm

2. If necessary, change the Region to US East (N. Virginia). Billing metric data is stored in this Region and reflects worldwide charges.
3. In the navigation pane, choose Alarms.
4. Select the check box next to the alarm and choose Actions, Delete.
5. When prompted for confirmation, choose Yes, Delete.

Hiding Amazon EC2 Auto Scaling alarms

When you view your alarms in the AWS Management Console, you can hide the alarms related to Amazon EC2 Auto Scaling. This feature is available only in the AWS Management Console.

To temporarily hide Amazon EC2 Auto Scaling alarms

2. In the navigation pane, choose Alarms and select Hide all AutoScaling alarms.
Using synthetic monitoring

You can use Amazon CloudWatch Synthetics to create canaries, configurable scripts that run on a schedule, to monitor your endpoints and APIs. Canaries follow the same routes and perform the same actions as a customer, which makes it possible for you to continually verify your customer experience even when you don't have any customer traffic on your applications. By using canaries, you can discover issues before your customers do.

Canaries are scripts written in Node.js or Python. They create Lambda functions in your account that use Node.js or Python as a framework. Canaries work over both HTTP and HTTPS protocols.

Canaries offer programmatic access to a headless Google Chrome Browser via Puppeteer or Selenium Webdriver. For more information about Puppeteer, see Puppeteer. For more information about Selenium, see www.selenium.dev/

Canaries check the availability and latency of your endpoints and can store load time data and screenshots of the UI. They monitor your REST APIs, URLs, and website content, and they can check for unauthorized changes from phishing, code injection and cross-site scripting.

For a video demonstration of canaries, see the Amazon CloudWatch Synthetics Demo video.

You can run a canary once or on a regular schedule. Canaries can run as often as once per minute. You can use both cron and rate expressions to schedule canaries.

For information about security issues to consider before you create and run canaries, see Security considerations for Synthetics canaries (p. 741).

By default, canaries create several CloudWatch metrics in the CloudWatchSynthetics namespace. These metrics have CanaryName as a dimension. Canaries that use the executeStep() or executeHttpStep() function from the function library also have StepName as a dimension. For more information about the canary function library, see Library functions available for canary scripts (p. 162).

CloudWatch Synthetics integrates well with CloudWatch ServiceLens, which uses CloudWatch with AWS X-Ray to provide an end-to-end view of your services to help you more efficiently pinpoint performance bottlenecks and identify impacted users. Canaries that you create with CloudWatch Synthetics appear on the ServiceLens service map. For more information about ServiceLens, see Using ServiceLens to monitor the health of your applications (p. 226).

CloudWatch Synthetics is currently available in all commercial AWS Regions and the GovCloud Regions.

**Note**
In Asia Pacific (Osaka), AWS PrivateLink is not supported.

**Topics**
- Required roles and permissions for CloudWatch canaries (p. 134)
- Creating a canary (p. 138)
- Troubleshooting a failed canary (p. 191)
- Sample code for canary scripts (p. 195)
- Canaries and X-Ray tracing (p. 199)
Required roles and permissions

- Running a canary on a VPC (p. 200)
- Viewing canary statistics and details (p. 200)
- CloudWatch metrics published by canaries (p. 202)
- Editing or deleting a canary (p. 203)
- Monitoring canary events with Amazon EventBridge (p. 204)

Required roles and permissions for CloudWatch canaries

To view canary details and the results of canary runs, you must be signed in as an IAM user who has either the `CloudWatchSyntheticsFullAccess` or the `CloudWatchSyntheticsReadOnlyAccess` policy attached. To read all Synthetics data in the console, you also need the `AmazonS3ReadOnlyAccess` and `CloudWatchReadOnlyAccess` policies. To view the source code used by canaries, you also need the `AWSLambdaReadOnlyAccess` policy.

To create canaries, you must be signed in as an IAM user who has the `CloudWatchSyntheticsFullAccess` policy or a similar set of permissions. To create IAM roles for the canaries, you also need the following inline policy statement:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:CreatePolicy",
        "iam:AttachRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole*",
        "arn:aws:iam::*:policy/service-role/CloudWatchSyntheticsPolicy*"
      ]
    }
  ]
}
```

**Important**

Granting a user the `iam:CreateRole`, `iam:CreatePolicy`, and `iam:AttachRolePolicy` permissions gives that user full administrative access to your AWS account. For example, a user with these permissions can create a policy that has full permissions for all resources and can attach that policy to any role. Be very careful about who you grant these permissions to.

For information about attaching policies and granting permissions to users, see Changing Permissions for an IAM User and To embed an inline policy for a user or role.

**AWS managed policies for CloudWatch Synthetics**

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies AWS managed policies in the IAM User Guide.
AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally change the permissions in an AWS managed policy. This type of update affects all identities (users, groups, and roles) where the policy is attached.

**CloudWatch Synthetics updates to AWS managed policies**

View details about updates to AWS managed policies for CloudWatch Synthetics since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the CloudWatch Document history page.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Redundant actions removed from CloudWatchSyntheticsFullAccess</td>
<td>CloudWatch Synthetics removed the s3:PutBucketEncryption and lambda:GetLayerVersionByArn actions from CloudWatchSyntheticsFullAccess policy because those actions were redundant with other permissions in the policy. The removed actions did not provide any permissions, and there's no net change to the permissions granted by the policy.</td>
<td>March 12, 2021</td>
</tr>
<tr>
<td>CloudWatch Synthetics started tracking changes</td>
<td>CloudWatch Synthetics started tracking changes for its AWS managed policies.</td>
<td>March 10, 2021</td>
</tr>
</tbody>
</table>

**CloudWatchSyntheticsFullAccess**

Here are the contents of the CloudWatchSyntheticsFullAccess policy:

```json
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":
      {
        "synthetics:*"
      },
      "Resource":"
    },
    {
      "Effect":"Allow",
      "Action":
      {
        "s3:CreateBucket",
        "s3:PutEncryptionConfiguration"
      },
      "Resource":
      {
        "arn:aws:s3:::cw-syn-results-*"
      }
    },
    {
      "Effect":"Allow",
      "Action":
      {
        "iam:ListRoles",
        "iam:PassRole",
        "iam:ListAttachedRolePolicies"
      }
    }
  ]
}
```
```json
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObject",
        "s3:ListBucket"
    ],
    "Resource": "arn:aws:s3:::cw-syn-*"
},
{
    "Effect": "Allow",
    "Action": [
        "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::aws-synthetics-library-*"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:PassRole"
    ],
    "Resource": [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole"
    ],
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "lambda.amazonaws.com",
                "synthetics.amazonaws.com"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "iam:GetRole"
    ],
    "Resource": [
        "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:DeleteAlarms"
    ],
    "Resource": [
        "arn:aws:cloudwatch:::*:alarm:Synthetics-*"
    ]
}
```
AWS managed policies for CloudWatch Synthetics

```
},
{  "Effect":"Allow",
   "Action":
      [  "cloudwatch:DescribeAlarms"
      ],
   "Resource":
      [  "arn:aws:cloudwatch::*:*:alarm:*"
      ]
},
{  "Effect":"Allow",
   "Action":
      [  "lambda:CreateFunction",
          "lambda:AddPermission",
          "lambda:PublishVersion",
          "lambda:UpdateFunctionConfiguration",
          "lambda:GetFunctionConfiguration"
      ],
   "Resource":
      [  "arn:aws:lambda::*:*:function:cwsyn-*"
      ]
},
{  "Effect":"Allow",
   "Action":
      [  "lambda:GetLayerVersion",
          "lambda:PublishLayerVersion"
      ],
   "Resource":
      [  "arn:aws:lambda::*:*:layer:cwsyn-*",
          "arn:aws:lambda::*:*:layer:Synthetics:*"
      ]
},
{  "Effect":"Allow",
   "Action":
      [  "ec2:DescribeVpcs",
          "ec2:DescribeSubnets",
          "ec2:DescribeSecurityGroups"
      ],
   "Resource":
      [  "*"
      ]
},
{  "Effect":"Allow",
   "Action":
      [  "sns:ListTopics"
      ],
   "Resource":
      [  "*"
      ]
},
{  "Effect":"Allow",
   "Action":
      [  "sns:CreateTopic",
          "sns:Subscribe",
          "sns:ListSubscriptionsByTopic"
      ],
   "Resource":
      [  "arn::*:sns::*:Synthetics-*"
      ]
}
]```
Creating a canary

Important
Ensure that you use Synthetics canaries to monitor only endpoints and APIs where you have ownership or permissions. Depending on the canary frequency settings, these endpoints might experience increased traffic.

When you use the CloudWatch console to create a canary, you can use a blueprint provided by CloudWatch to create your canary or you can write your own script. For more information, see Using canary blueprints (p. 140).

You can also create a canary using AWS CloudFormation if you are using your own script for the canary. For more information, see AWS::Synthetics::Canary in the AWS CloudFormation User Guide.

If you are writing your own script, you can use several functions that CloudWatch Synthetics has built into a library. For more information, see Synthetics runtime versions (p. 145).

To create a canary
2. In the navigation pane, choose Canaries.
3. Choose Create Canary.
4. Choose one of the following:
   - To base your canary on a blueprint script, choose Use a blueprint, and then choose the type of canary you want to create. For more information about what each type of blueprint does, see Using canary blueprints (p. 140).
   - To upload your own Node.js script to create a custom canary, choose Upload a script.
     You can then drag your script into the Script area or choose Browse files to navigate to the script in your file system.
   - To import your script from an S3 bucket, choose Import from S3. Under Source location, enter the complete path to your canary or choose Browse S3.
You must have s3:GetObject and s3:GetObjectVersion permissions for the S3 bucket that you use. The bucket must be in the same AWS Region where you are creating the canary.

5. Under **Name**, enter a name for your canary. The name is used on many pages, so we recommend that you give it a descriptive name that distinguishes it from other canaries.

6. Under **Application or endpoint URL**, enter the URL that you want the canary to test. This URL must include the protocol (such as https://).

   If you want the canary to test an endpoint on a VPC, you must also enter information about your VPC later in this procedure.

7. If you are using your own script for the canary, under **Lambda handler**, enter the entry point where you want the canary to start. The string that you enter must end with .handler.

8. If you are using environment variables in your script, choose **Environment variables** and then specify a value for each environment variable defined in your script. For more information, see Environment variables (p. 157).

9. Under **Schedule**, choose whether to run this canary just once, run it continuously using a rate expression, or schedule it using a cron expression.
   
   - When you use the CloudWatch console to create a canary that runs continuously, you can choose a rate anywhere between once a minute and once an hour.
   
   - For more information about writing a cron expression for canary scheduling, see Scheduling canary runs using cron (p. 190).

10. Under **Data retention**, specify how long to retain information about both failed and successful canary runs. The range is 1-455 days.

11. Under **Data Storage**, select the S3 bucket to use to store the data from the canary runs. The bucket name can't contain a period (.). If you leave this blank, a default S3 bucket is used or created.

   If you are using the syn-nodejs-puppeteer-3.0 or later runtime, when you enter the URL for the bucket in the text box, you can specify a bucket in the current Region or in a different Region. If you are using an earlier runtime version, the bucket must be in the current Region.

12. Under **Access permissions**, choose whether to create an IAM role to run the canary or use an existing one.

   If you use the CloudWatch console to create a role for a canary when you create the canary, you can't re-use the role for other canaries, because these roles are specific to just one canary. If you have manually created a role that works for multiple canaries, you can use that existing role.

   To use an existing role, you must have the iam:PassRole permission to pass that role to Synthetics and Lambda. You must also have the iam:GetRole permission.

13. (Optional) Under **Alarms**, choose whether you want default CloudWatch alarms to be created for this canary. If you choose to create alarms, they are created with the following name convention: Synthetics-Alarm-canaryName-index

   index is a number representing each different alarm created for this canary. The first alarm has an index of 1, the second alarm has an index of 2, and so on.

14. (Optional) To have this canary test an endpoint that is on a VPC, choose **VPC settings**, and then do the following:

   a. Select the VPC that hosts the endpoint.

   b. Select one or more subnets on your VPC. You must select a private subnet because a Lambda instance can't be configured to run in a public subnet when an IP address can't be assigned to the Lambda instance during execution. For more information, see Configuring a Lambda Function to Access Resources in a VPC.

   c. Select one or more security groups on your VPC.
If the endpoint is on a VPC, you must enable your canary to send information to CloudWatch and Amazon S3. For more information, see Running a canary on a VPC (p. 200).

15. (Optional) Under Tags, add one or more key-value pairs as tags for this canary. Tags can help you identify and organize your AWS resources and track your AWS costs. For more information, see Tagging your Amazon CloudWatch resources (p. 694).

16. (Optional) Under Active tracing, choose whether to enable active X-Ray tracing for this canary. This option is available only if the canary uses runtime version syn-nodejs-2.0 or later. For more information, see Canaries and X-Ray tracing (p. 199).

Resources that are created for canaries

When you create a canary, the following resources are created:

- An IAM role with the name CloudWatchSyntheticsRole-canary-name-uuid (if you use CloudWatch console to create the canary and specify for a new role to be created for the canary)
- An IAM policy with the name CloudWatchSyntheticsPolicy-canary-name-uuid.
- An S3 bucket with the name cw-syn-results-accountID-region.
- Alarms with the name Synthetics-Alarm-MyCanaryName, if you want alarms to be created for the canary.
- Lambda functions and layers, if you use a blueprint to create the canary. These resources have the prefix cwsyn-MyCanaryName.
- CloudWatch Logs log groups with the name /aws/lambda/cwsyn-MyCanaryName.

Using canary blueprints

This section provides details about each of the canary blueprints and the tasks each blueprint is best suited for. Blueprints are provided for the following canary types:

- Heartbeat Monitor
- API Canary
- Broken Link Checker
- Visual Monitoring
- Canary Recorder
- GUI Workflow

When you use a blueprint to create a canary, as you fill out the fields in the CloudWatch console, the Script editor area of the page displays the canary you are creating as a Node.js script. You can also edit your canary in this area to customize it further.

Heartbeat monitoring

Heartbeat scripts load the specified URL and store a screenshot of the page and an HTTP archive file (HAR file). They also store logs of accessed URLs.

You can use the HAR files to view detailed performance data about the web pages. You can analyze the list of web requests and catch performance issues such as time to load for an item.

If your canary uses the syn-nodejs-puppeteer-3.1 or later runtime version, you can use the heartbeat monitoring blueprint to monitor multiple URLs and see the status, duration, associated screenshots, and failure reason or each URL in the step summary of the canary run report.
API canary

API canaries can test the basic Read and Write functions of a REST API. REST stands for *representational state transfer* and is a set of rules that developers follow when creating an API. One of these rules states that a link to a specific URL should return a piece of data.

Canaries can work with any APIs and test all types of functionality. Each canary can make multiple API calls.

In canaries that use runtime version `syn-nodejs-2.0` or later, the API canary blueprint supports multi-step canaries that monitor your APIs as HTTP steps. You can test multiple APIs in a single canary. Each step is a separate request that can access different a URL, use different headers, and use different rules for whether headers and response bodies are captured. By not capturing headers and response body, you can prevent sensitive data from being recorded.

Each request in an API canary consists of the following information:

- The **endpoint**, which is the URL that you request.
- The **method**, which is the type of request that is sent to the server. REST APIs support GET (read), POST (write), PUT (update), PATCH (update), and DELETE (delete) operations.
- The **headers**, which provide information to both the client and the server. They are used for authentication and providing information about the body content. For a list of valid headers, see HTTP Headers.
- The **data (or body)**, which contains information to be sent to the server. This is used only for POST, PUT, PATCH, or DELETE requests.
- The URL that you request.

The API canary blueprint supports GET and POST methods. When you use this blueprint, you must specify headers. For example, you can specify Authorization as a Key and specify the necessary authorization data as the Value for that key.

If you are testing a POST request, you also specify the content to post in the Data field.

Integration with API Gateway

The API blueprint is integrated with Amazon API Gateway. This enables you to select an API Gateway API and stage from the same AWS account and Region as the canary, or to upload a Swagger template from API Gateway for cross-account and cross-Region API monitoring. You can then choose the rest of the details in the console to create the canary, instead of entering them from scratch. For more information about API Gateway, see What is Amazon API Gateway?

Broken link checker

The broken link checker collects all the links inside the URL that you are testing by using `document.getElementsByTagName('a')`. It tests only up to the number of links that you specify, and the URL itself is counted as the first link. For example, if you want to check all the links on a page that contains five links, you must specify for the canary to follow six links.

Broken link checker canaries created using the `syn-nodejs-2.0-beta` runtime or later support the following additional features:

- Provides a report that includes the links that were checked, status code, failure reason (if any), and source and destination page screenshots.
- When viewing canary results, you can filter to see only the broken links and then fix the link based on the reason for failure.
• This version captures annotated source page screenshots for each link and highlights the anchor where the link was found. Hidden components are not annotated.
• You can configure this version to capture screenshots of both source and destination pages, just source pages, or just destination pages.
• This version fixes an issue in the earlier version where the canary script stops after the first broken link even when more links are scraped from the first page.

If you want to update an existing canary using syn-1.0 to use the new runtime, you must delete and re-create the canary. Updating an existing canary to the new runtime does not make these features available.

A broken link checker canary detects the following types of link errors:

• 404 Page Not Found
• Invalid Host Name
• Bad URL. For example, the URL is missing a bracket, has extra slashes, or uses the wrong protocol.
• Invalid HTTP response code.
• The host server returns empty responses with no content and no response code.
• The HTTP requests constantly time out during the canary's run.
• The host consistently drops connections because it is misconfigured or is too busy.

Visual monitoring blueprint

The visual monitoring blueprint includes code to compare screenshots taken during a canary run with screenshots taken during a baseline canary run. If the discrepancy between the two screenshots is beyond a threshold percentage, the canary fails. Visual monitoring is supported in canaries running syn-puppeteer-node-3.2 and later. It is not currently supported in canaries running Python and Selenium.

The visual monitoring blueprint includes the following line of code in the default blueprint canary script, which enables visual monitoring.

```java
syntheticsConfiguration.withVisualCompareWithBaseRun(true);
```

The first time that the canary runs successfully after this line is added to the script, it uses the screenshots taken during that run as the baseline for comparison. After that first canary run, you can use the CloudWatch console to edit the canary to do any of the following:

• Set the next run of the canary as the new baseline.
• Draw boundaries on the current baseline screenshot to designate areas of the screenshot to ignore during visual comparisons.
• Remove a screenshot from being used for visual monitoring.

For more information about using the CloudWatch console to edit a canary, see Editing or deleting a canary (p. 203).

You can also change the canary run that is used as the baseline by using the nextrun or lastrun parameters or specifying a canary run ID in the UpdateCanary API.

When you use the visual monitoring blueprint, you enter the URL where you want the screenshot to be taken, and specify a difference threshold as a percentage. After the baseline run, future runs of the canary that detect a visual difference greater than that threshold trigger a canary failure. After the baseline run, you can also edit the canary to “draw” boundaries on the baseline screenshot that you want to ignore during the visual monitoring.
The visual monitoring feature is powered by the the ImageMagick open source software toolkit. For more information, see ImageMagick.

**Canary recorder**

With the canary recorder blueprint, you can use the CloudWatch Synthetics Recorder to record your click and type actions on a website and automatically generate a Node.js script that can be used to create a canary that follows the same steps. The CloudWatch Synthetics Recorder is a Google Chrome extension provided by Amazon.

**Credits**: The CloudWatch Synthetics Recorder is based on the Headless recorder.

For more information, see Using the CloudWatch Synthetics Recorder for Google Chrome (p. 144).

**GUI workflow builder**

The GUI Workflow Builder blueprint verifies that actions can be taken on your webpage. For example, if you have a webpage with a login form, the canary can populate the user and password fields and submit the form to verify that the webpage is working correctly.

When you use a blueprint to create this type of canary, you specify the actions that you want the canary to take on the webpage. The actions that you can use are the following:

- **Click**— Selects the element that you specify and simulates a user clicking or choosing the element.

  To specify the element in a Node.js script, use `[id=]` or `[@class=]`.

  To specify the element in a Python script, use `xpath //*[id=]` or `//*[class=]`.

- **Verify selector**— Verifies that the specified element exists on the webpage. This test is useful for verifying that a previous action has causes the correct elements to populate the page.

  To specify the element to verify in a Node.js script, use `[id=]` or `[@class=]`.

  To specify the element to verify in a Python script, use `xpath //*[id=]` or `//*[class=]`.

- **Verify text**— Verifies that the specified string is contained within the target element. This test is useful for verifying that a previous action has caused the correct text to be displayed.

  To specify the element in a Node.js script, use a format such as `div[@id=]//h1` because this action uses the `waitForXPath` function in Puppeteer.

  To specify the element in a Python script, use `xpath //*[id=]` or `//*[class=]` because this action uses the `implicitly_wait` function in Selenium.

- **Input text**— Writes the specified text in the target element.

  To specify the element to verify in a Node.js script, use `[id=]` or `[@class=]`.

  To specify the element to verify in a Python script, use `xpath //*[id=]` or `//*[class=]`.

- **Click with navigation**— Waits for the whole page to load after choosing the specified element. This is most useful when you need to reload the page.

  To specify the element in a Node.js script, use `[id=]` or `[@class=]`.

  To specify the element in a Python script, use `xpath //*[id=]` or `//*[class=]`.

For example, the following blueprint uses Node.js. It clicks the **firstButton** on the specified URL, verifies that the expected selector with the expected text appears, inputs the name Test_Customer into the **Name** field, clicks the **Login** button, and then verifies that the login is successful by checking for the **Welcome** text on the next page.
GUI workflow canaries that use the following runtimes also provide a summary of the steps executed for each canary run. You can use the screenshots and error message associated with each step to find the root cause of failure.

- `syn-nodejs-2.0` or later
- `syn-python-selenium-1.0` or later

### Using the CloudWatch Synthetics Recorder for Google Chrome

Amazon provides a CloudWatch Synthetics Recorder to help you create canaries more easily. The recorder is a Google Chrome extension.

The recorder records your click and type actions on a website and automatically generates a Node.js script that can be used to create a canary that follows the same steps.

After you start recording, the CloudWatch Synthetics Recorder detects your actions in the browser and converts them to a script. You can pause and resume the recording as needed. When you stop recording, the recorder produces a Node.js script of your actions, which you can easily copy with the Copy to Clipboard button. You can then use this script to create a canary in CloudWatch Synthetics.

**Credits:** The CloudWatch Synthetics Recorder is based on the Headless recorder.

### Installing the CloudWatch Synthetics Recorder extension for Google Chrome

To use the CloudWatch Synthetics Recorder, you can start creating a canary and choose the Canary Recorder blueprint. If you do this when you haven't already downloaded the recorder, the CloudWatch Synthetics console provides a link to download it.

Alternatively, you can follow these steps to download and install the recorder directly.
To install the CloudWatch Synthetics Recorder

1. Using Google Chrome, go to this website: https://chrome.google.com/webstore/detail/cloudwatch-synthetics-rec/bhdnlmmgplmcdkkdfplenepegfno
2. Choose Add to Chrome, then choose Add extension.

Using the CloudWatch Synthetics Recorder for Google Chrome

To use the CloudWatch Synthetics Recorder to help you create a canary, you can choose Create canary in the CloudWatch console, and then choose Use a blueprint, Canary Recorder. For more information, see Creating a canary (p. 138).

Alternatively, you can use the recorder to record steps without immediately using them to create a canary.

To use the CloudWatch Synthetics Recorder to record your actions on a website

1. Navigate to the page that you want to monitor.
2. Choose the Chrome extensions icon, and then choose CloudWatch Synthetics Recorder.
3. Choose Start Recording.
4. Perform the steps that you want to record. To pause recording, choose Pause.
5. When you are finished recording the workflow, choose Stop recording.
6. Choose Copy to clipboard to copy the generated script to your clipboard. Or, if you want to start over, choose New recording.
7. To create a canary with the copied script, you can paste your copied script into the recorder blueprint inline editor, or save it to an Amazon S3 bucket and import it from there.
8. If you're not immediately creating a canary, you can save your recorded script to a file.

Known limitations of the CloudWatch Synthetics Recorder

The CloudWatch Synthetics Recorder for Google Chrome currently has the following limitations.

- HTML elements that don't have IDs will use CSS selectors. This can break canaries if the webpage structure changes later. We plan to provide some configuration options (such as using data-id) around this in a future version of the recorder.
- The recorder doesn't support actions such as double-click or copy/paste, and doesn't support key combinations such as CMD+0.
- To verify the presence of an element or text on the page, users must add assertions after the script is generated. The recorder doesn't support verifying an element without performing any action on that element. This is similar to the “Verify text” or “Verify element” options in the canary workflow builder. We plan to add some assertions support in a future version of the recorder.
- The recorder records all actions in the tab where the recording is initiated. It doesn't record pop-ups (for instance, to allow location tracking) or navigation to different pages from pop-ups.

Synthetics runtime versions

When you create or update a canary, you choose a Synthetics runtime version for the canary. A Synthetics runtime is a combination of the Synthetics code that calls your script handler, and the Lambda layers of bundled dependencies.

CloudWatch Synthetics currently supports runtimes that use Node.js for scripts and the Puppeteer framework, and runtimes that use Python for scripting and Selenium Webdriver for the framework.
We recommend that you always use the most recent runtime version for your canaries, to be able to use the latest features and updates made to the Synthetics library.

**Topics**
- CloudWatch Synthetics runtime support policy (p. 146)
- Runtime versions using Node.js and Puppeteer (p. 150)
- Runtime versions using Python and Selenium Webdriver (p. 154)

### CloudWatch Synthetics runtime support policy

Synthetics runtime versions are subject to maintenance and security updates. When any component of a runtime version is no longer supported, that Synthetics runtime version is deprecated.

You can’t create canaries using deprecated runtime versions. Canaries that use deprecated runtimes continue to run. You can stop, start, and delete these canaries. You can update an existing canary that uses a deprecated runtime version by updating the canary to use a supported runtime version.

CloudWatch Synthetics notifies you by email if you have canaries that use runtimes that are scheduled to be deprecated in the next 60 days. We recommend that you migrate your canaries to a supported runtime version to benefit from the new functionality, security, and performance enhancements that are included in more recent releases.

**How do I update a canary to a new runtime version?**

You can update a canary's runtime version by using the CloudWatch console, AWS CloudFormation, the AWS CLI or the AWS SDK. When you use the CloudWatch console, you can update up to five canaries at once by selecting them in the canary list page and then choosing **Actions, Update Runtime**.

You can verify the upgrade by first cloning the canary using the CloudWatch console and updating its runtime version. This creates another canary which is a clone of your original canary. Once you have verified your canary with the new runtime version, you can update the runtime version of your original canary and delete the clone canary.

You can also update multiple canaries using an upgrade script. For more information, see Canary runtime upgrade script (p. 146).

If you upgrade a canary and it fails, see Troubleshooting a failed canary (p. 191).

**Runtime deprecation dates**

<table>
<thead>
<tr>
<th>Runtime Version</th>
<th>Deprecation date</th>
</tr>
</thead>
<tbody>
<tr>
<td>syn-nodejs-2.2</td>
<td>May 28, 2021</td>
</tr>
<tr>
<td>syn-nodejs-2.1</td>
<td>May 28, 2021</td>
</tr>
<tr>
<td>syn-nodejs-2.0</td>
<td>May 28, 2021</td>
</tr>
<tr>
<td>syn-nodejs-2.0-beta</td>
<td>February 8, 2021</td>
</tr>
<tr>
<td>syn-1.0</td>
<td>May 28, 2021</td>
</tr>
</tbody>
</table>

**Canary runtime upgrade script**

To upgrade a canary script to a supported runtime version, use the following script.

```javascript
const AWS = require('aws-sdk');
```
You need to configure your AWS credentials and Region.

const synthetics = new AWS.Synthetics();

const DEFAULT_OPTIONS = {
  /**
   * The number of canaries to upgrade during a single run of this script.
   */
  count: 10,
  /**
   * No canaries are upgraded unless force is specified.
   */
  force: false
};

/**
 * The number of milliseconds to sleep between GetCanary calls when
 * verifying that an update succeeded.
 */
const SLEEP_TIME = 5000;

(async () => {
  try {
    const options = getOptions();
    const versions = await getRuntimeVersions();
    const canaries = await getAllCanaries();
    const upgrades = canaries
      .filter(canary => !versions.isLatestVersion(canary.RuntimeVersion))
      .map(canary => {
        return {
          Name: canary.Name,
          FromVersion: canary.RuntimeVersion,
          ToVersion: versions.getLatestVersion(canary.RuntimeVersion)
        }
      });

    if (options.force) {
      const promises = [];
      for (const upgrade of upgrades.slice(0, options.count)) {
        const promise = upgradeCanary(upgrade);
        promises.push(promise);
        // Sleep for 100 milliseconds to avoid throttling.
        await usleep(100);
      }

      const succeeded = [];
      const failed = [];
      for (let i = 0; i < upgrades.slice(0, options.count).length; i++) {
        const upgrade = upgrades[i];
        const promise = promises[i];
        try {
          await promise;
          console.log(`The update of ${upgrade.Name} succeeded.`);
          succeeded.push(upgrade.Name);
        } catch (e) {
          console.log(`The update of ${upgrade.Name} failed with error: ${e}`);
          failed.push({
            Name: upgrade.Name,
            Reason: e
          });
        }
      }
    }
  } catch (error) {
    console.error(`An error occurred: ${error}`);
  }
});
Amazon CloudWatch User Guide
Synthetics runtime versions

}

}

if (succeeded.length) {
console.group('The following canaries were upgraded successfully.');
for (const name of succeeded) {
console.log(name);
}
console.groupEnd()
} else {
console.log('No canaries were upgraded successfully.');
}
if (failed.length) {
console.group('The following canaries were not upgraded successfully.');
for (const failure of failed) {
console.log('\x1b[31m', `${failure.Name}: ${failure.Reason}`, '\x1b[0m');
}
console.groupEnd();
}
} else {
console.log('Run with --force [--count <count>] to perform the first <count> upgrades
shown. The default value of <count> is 10.')
console.table(upgrades);
}
} catch (e) {
console.error(e);
}
})();
function getOptions() {
const force = getFlag('--force', DEFAULT_OPTIONS.force);
const count = getOption('--count', DEFAULT_OPTIONS.count);
return { force, count };

}

function getFlag(key, defaultValue) {
return process.argv.includes(key) || defaultValue;
}
function getOption(key, defaultValue) {
const index = process.argv.indexOf(key);
if (index < 0) {
return defaultValue;
}
const value = process.argv[index + 1];
if (typeof value === 'undefined' || value.startsWith('-')) {
throw `The ${key} option requires a value.`;
}
return value;
}

function getAllCanaries() {
return new Promise((resolve, reject) => {
const canaries = [];
synthetics.describeCanaries().eachPage((err, data) => {
if (err) {
reject(err);
} else {
if (data === null) {
resolve(canaries);
} else {
canaries.push(...data.Canaries);
}
}
});

148


function getRuntimeVersions() {
    return new Promise((resolve, reject) => {
        const jsVersions = [];
        const pythonVersions = [];
        synthetics.describeRuntimeVersions().eachPage((err, data) => {
            if (err) {
                reject(err);
            } else {
                if (data === null) {
                    jsVersions.sort((a, b) => a.ReleaseDate - b.ReleaseDate);
                    pythonVersions.sort((a, b) => a.ReleaseDate - b.ReleaseDate);
                    resolve({
                        isLatestVersion(version) {
                            const latest = this.getLatestVersion(version);
                            return latest === version;
                        },
                        getLatestVersion(version) {
                            if (jsVersions.some(v => v.VersionName === version)) {
                                return jsVersions[jsVersions.length - 1].VersionName;
                            } else if (pythonVersions.some(v => v.VersionName === version)) {
                                return pythonVersions[pythonVersions.length - 1].VersionName;
                            } else {
                                throw Error(`Unknown version ${version}`);
                            }
                        }
                    });
                } else {
                    for (const version of data.RuntimeVersions) {
                        if (version.VersionName === 'syn-1.0') {
                            jsVersions.push(version);
                        } else if (version.VersionName.startsWith('syn-nodejs-2.')) {
                            jsVersions.push(version);
                        } else if (version.VersionName.startsWith('syn-nodejs-puppeteer-')) {
                            jsVersions.push(version);
                        } else if (version.VersionName.startsWith('syn-python-selenium-')) {
                            pythonVersions.push(version);
                        } else {
                            throw Error(`Unknown version ${version.VersionName}`);
                        }
                    }
                }
            }
        });
    });
}

async function upgradeCanary(upgrade) {
    console.log(`Upgrading canary ${upgrade.Name} from ${upgrade.FromVersion} to ${upgrade.ToVersion}`);
    await synthetics.updateCanary({ Name: upgrade.Name, RuntimeVersion: upgrade.ToVersion }).promise();
    while (true) {
        await usleep(SLEEP_TIME);
        console.log(`Getting the state of canary ${upgrade.Name}`);
        const response = await synthetics.getCanary({ Name: upgrade.Name }).promise();
        console.log(`The state of canary ${upgrade.Name} is ${state}`);
        if (state !== 'UPDATING') {
            return;
        }
    }
}
Runtime versions using Node.js and Puppeteer

The first runtime version for Node.js and Puppeteer was named `syn-1.0`. Later runtime versions have the naming convention `syn-language-majorversion.minorversion`. Starting with `syn-nodejs-puppeteer-3.0`, the naming convention is `syn-language-framework-majorversion.minorversion`.

An additional `-beta` suffix shows that the runtime version is currently in a beta preview release.

Runtime versions with the same major version number are backward compatible.

**Notes for all runtime versions**

When using `syn-nodejs-puppeteer-3.0` runtime version, make sure that your canary script is compatible with Node.js 12.x. If you use an earlier version of a `syn-nodejs` runtime version, make sure that your script is compatible with Node.js 10.x.

The Lambda code in a canary is configured to have a maximum memory of 1 GB. Each run of a canary times out after a configured timeout value. If no timeout value is specified for a canary, CloudWatch chooses a timeout value based on the canary’s frequency.

**syn-nodejs-puppeteer-3.2**

The `syn-nodejs-puppeteer-3.2` runtime is the newest runtime version.

**Major dependencies:**

- Lambda runtime Node.js 12.x
- Puppeteer-core version 5.5.0
- Chromium version 88.0.4298.0

**New features in syn-nodejs-puppeteer-3.2:**

- **visual monitoring with screenshots**— Canaries using this runtime or later can compare a screenshot taken during a run with a baseline version of the same screenshot. If the screenshots are more different than a specified percentage threshold, the canary fails. For more information, see [Visual monitoring](p. 171) or [Visual monitoring blueprint](p. 142).

- **New functions regarding sensitive data** You can prevent sensitive data from appearing in canary logs and reports. For more information, see [SyntheticsLogHelper class](p. 173).

- **Deprecated function** The RequestResponseLogHelper class is deprecated in favor of other new configuration options. For more information, see [RequestResponseLogHelper class](p. 178).

**syn-nodejs-puppeteer-3.1**

**Major dependencies:**

- Lambda runtime Node.js 12.x
- Puppeteer-core version 5.5.0
• Chromium version 88.0.4298.0

New features in syn-nodejs-puppeteer-3.1:

• Ability to configure CloudWatch metrics—With this runtime, you can disable the metrics that you do not require. Otherwise, canaries publish various CloudWatch metrics for each canary run.
• Screenshot linking—You can link a screenshot to a canary step after the step has completed. To do this, you take the screenshot by using the `takeScreenshot` method, using the name of the step that you want to associate the screenshot with. For example, you might want to perform a step, add a wait time, and then take the screenshot.
• Heartbeat monitor blueprint can monitor multiple URLs—You can use the heartbeat monitoring blueprint in the CloudWatch console to monitor multiple URLs and see the status, duration, associated screenshots, and failure reason for each URL in the step summary of the canary run report.

**syn-nodejs-puppeteer-3.0**

Major dependencies:

• Lambda runtime Node.js 12.x
• Puppeteer-core version 5.5.0
• Chromium version 88.0.4298.0

New features in syn-nodejs-puppeteer-3.0:

• Upgraded dependencies—This version uses Puppeteer version 5.5.0, Node.js 12.x, and Chromium 88.0.4298.0.
• Cross-Region bucket access—You can now specify an S3 bucket in another Region as the bucket where your canary stores its log files, screenshots, and HAR files.
• New functions available—This version adds library functions to retrieve the canary name and the Synthetics runtime version.

For more information, see Synthetics class (p. 162).

**syn-nodejs-2.2**

This section contains information about the syn-nodejs-2.2 runtime version.

Important
This runtime version is scheduled to be deprecated on May 28, 2021. For more information, see CloudWatch Synthetics runtime support policy (p. 146).

Major dependencies:

• Lambda runtime Node.js 10.x
• Puppeteer-core version 3.3.0
• Chromium version 83.0.4103.0

New features in syn-nodejs-2.2:

• Monitor your canaries as HTTP steps—You can now test multiple APIs in a single canary. Each API is tested as a separate HTTP step, and CloudWatch Synthetics monitors the status of each step using step metrics and the CloudWatch Synthetics step report. CloudWatch Synthetics creates `SuccessPercent` and `Duration` metrics for each HTTP step.
This functionality is implemented by the `executeHttpStep(stepName, requestOptions, callback, stepConfig)` function. For more information, see `executeHttpStep(stepName, requestOptions, [callback], [stepConfig])` (p. 182).

The API canary blueprint is updated to use this new feature.

- **HTTP request reporting**— You can now view detailed HTTP requests reports which capture details such as request/response headers, response body, status code, error and performance timings, TCP connection time, TLS handshake time, first byte time, and content transfer time. All HTTP requests which use the HTTP/HTTPS module under the hood are captured here. Headers and response body are not captured by default but can be enabled by setting configuration options.

- **Global and step-level configuration**— You can set CloudWatch Synthetics configurations at the global level, which are applied to all steps of canaries. You can also override these configurations at the step level by passing configuration key/value pairs to enable or disable certain options.

For more information, see `SyntheticsConfiguration class` (p. 164).

- **Continue on step failure configuration**— You can choose to continue canary execution when a step fails. For the `executeHttpStep` function, this is turned on by default. You can set this option once at global level or set it differently per-step.

**syn-nodejs-2.1**

**Important**
This runtime version is scheduled to be deprecated on May 28, 2021. For more information, see `CloudWatch Synthetics runtime support policy` (p. 146).

**Major dependencies**:
- Lambda runtime Node.js 10.x
- Puppeteer-core version 3.3.0
- Chromium version 83.0.4103.0

**New features in syn-nodejs-2.1**:

- **Configurable screenshot behavior**— Provides the ability to turn off the capturing of screenshots by UI canaries. In canaries that use previous versions of the runtimes, UI canaries always capture screenshots before and after each step. With `syn-nodejs-2.1`, this is configurable. Turning off screenshots can reduce your Amazon S3 storage costs, and can help you comply with HIPAA regulations. For more information, see `SyntheticsConfiguration class` (p. 164).

- **Customize the Google Chrome launch parameters** You can now configure the arguments used when a canary launches a Google Chrome browser window. For more information, see `launch(options)` (p. 178).

There can be a small increase in canary duration when using syn-nodejs-2.0 or later, compared to earlier versions of the canary runtimes.

**syn-nodejs-2.0**

**Important**
This runtime version is scheduled to be deprecated on May 28, 2021. For more information, see `CloudWatch Synthetics runtime support policy` (p. 146).

**Major dependencies**:
- Lambda runtime Node.js 10.x
• Puppeteer-core version 3.3.0
• Chromium version 83.0.4103.0

**New features in syn-nodejs-2.0:**

• **Upgraded dependencies**— This runtime version uses Puppeteer-core version 3.3.0 and Chromium version 83.0.4103.0

• **Support for X-Ray active tracing.** When a canary has tracing enabled, X-Ray traces are sent for all calls made by the canary that use the browser, the AWS SDK, or HTTP or HTTPS modules. Canaries with tracing enabled appear on the service map in both CloudWatch ServiceLens and in X-Ray, even when they don’t send requests to other services or applications that have tracing enabled. For more information, see Canaries and X-Ray tracing (p. 199).

• **Synthetics reporting**— For each canary run, CloudWatch Synthetics creates a report named `SyntheticsReport-PASSED.json` or `SyntheticsReport-FAILED.json` which records data such as start time, end time, status, and failures. It also records the PASSED/FAILED status of each step of the canary script, and failures and screenshots captured for each step.

• **Broken link checker report**— The new version of the broken link checker included in this runtime creates a report that includes the links that were checked, status code, failure reason (if any), and source and destination page screenshots.

• **New CloudWatch metrics**— Synthetics publishes metrics named `2xx`, `4xx`, `5xx`, and `RequestFailed` in the `CloudWatchSynthetics` namespace. These metrics show the number of 200s, 400s, 500s, and request failures in the canary runs. With this runtime version, these metrics are reported only for UI canaries, and are not reported for API canaries. They are also reported for API canaries starting with runtime version `syn-nodejs-puppeteerer-2.2`.

• **Sortable HAR files**— You can now sort your HAR files by status code, request size, and duration.

• **Metrics timestamp**— CloudWatch metrics are now reported based on the Lambda invocation time instead of the canary run end time.

**Bug fixes in syn-nodejs-2.0:**

• Fixed the issue of canary artifact upload errors not being reported. Such errors are now surfaced as execution errors.
• Fixed the issue of redirected requests (3xx) being incorrectly logged as errors.
• Fixed the issue of screenshots being numbered starting from 0. They should now start with 1.
• Fixed the issue of screenshots being garbled for Chinese and Japanese fonts.

There can be a small increase in canary duration when using syn-nodejs-2.0 or later, compared to earlier versions of the canary runtimes.

**syn-nodejs-2.0-beta**

**Important**

This runtime version was deprecated on February 8, 2021. For more information, see CloudWatch Synthetics runtime support policy (p. 146).

**Major dependencies:**

• Lambda runtime Node.js 10.x
• Puppeteer-core version 3.3.0
• Chromium version 83.0.4103.0

**New features in syn-nodejs-2.0-beta:**
- **Upgraded dependencies**— This runtime version uses Puppeteer-core version 3.3.0 and Chromium version 83.0.4103.0
- **Synthetics reporting**— For each canary run, CloudWatch Synthetics creates a report named `SyntheticsReport-PASSED.json` or `SyntheticsReport-FAILED.json` which records data such as start time, end time, status, and failures. It also records the PASSED/FAILED status of each step of the canary script, and failures and screenshots captured for each step.
- **Broken link checker report**— The new version of the broken link checker included in this runtime creates a report that includes the links that were checked, status code, failure reason (if any), and source and destination page screenshots.
- **New CloudWatch metrics**— Synthetics publishes metrics named `2xx`, `4xx`, `5xx`, and `RequestFailed` in the `CloudWatchSynthetics` namespace. These metrics show the number of 200s, 400s, 500s, and request failures in the canary runs. These metrics are reported only for UI canaries, and are not reported for API canaries.
- **Sortable HAR files**— You can now sort your HAR files by status code, request size, and duration.
- **Metrics timestamp**— CloudWatch metrics are now reported based on the Lambda invocation time instead of the canary run end time.

**Bug fixes in syn-nodejs-2.0-beta:**

- Fixed the issue of canary artifact upload errors not being reported. Such errors are now surfaced as execution errors.
- Fixed the issue of redirected requests (3xx) being incorrectly logged as errors.
- Fixed the issue of screenshots being numbered starting from 0. They should now start with 1.
- Fixed the issue of screenshots being garbled for Chinese and Japanese fonts.

**syn-1.0**

**Important**

This runtime version is scheduled to be deprecated on May 28, 2021. For more information, see [CloudWatch Synthetics runtime support policy (p. 146)](https://docs.aws.amazon.com/AWSSDK/latest/APIReference/INDEX.html).

The first Synthetics runtime version is **syn-1.0**.

**Major dependencies:**

- Lambda runtime Node.js 10.x
- Puppeteer-core version 1.14.0
- The Chromium version that matches Puppeteer-core 1.14.0

**Runtime versions using Python and Selenium Webdriver**

The following sections contain information about the CloudWatch Synthetics runtime versions for Python and Selenium Webdriver. Selenium is an open-source browser automation tool. For more information about Selenium, see [www.selenium.dev/](http://www.selenium.dev/)

The naming convention for these runtime versions is `syn-language-framework-majorversion.minorversion`.

**syn-python-selenium-1.0**

**Major dependencies:**

- Python 3.8
• Selenium 3.141.0
• Chromium version 83.0.4103.0

Features:
• **Selenium support**— You can write canary scripts using the Selenium test framework. You can bring your Selenium scripts from elsewhere into CloudWatch Synthetics with minimal changes, and they will work with AWS services.

**Writing a canary script**

The following sections explain how to write a canary script and how to integrate a canary with other AWS Services.

**Topics**
- Writing a Node.js canary script (p. 155)
- Writing a Python canary script (p. 161)

**Writing a Node.js canary script**

**Topics**
- Creating a CloudWatch Synthetics canary from scratch (p. 155)
- Changing an existing Puppeteer script to use as a Synthetics canary (p. 156)
- Environment variables (p. 157)
- Integrating your canary with other AWS services (p. 159)
- Forcing your canary to use a static IP address (p. 160)

**Creating a CloudWatch Synthetics canary from scratch**

Here is an example minimal Synthetics Canary script. This script passes as a successful run, and returns a string. To see what a failing canary looks like, change `let fail = false;` to `let fail = true;`.

You must define an entry point function for the canary script. To see how files are uploaded to the Amazon S3 location specified as the canary's `ArtifactS3Location`, create these files under the `/tmp` folder. After the script runs, the pass/fail status and the duration metrics are published to CloudWatch and the files under `/tmp` are uploaded to S3.

```javascript
const basicCustomEntryPoint = async function () {

    // Insert your code here

    // Perform multi-step pass/fail check

    // Log decisions made and results to /tmp

    // Be sure to wait for all your code paths to complete
    // before returning control back to Synthetics.
    // In that way, your canary will not finish and report success
    // before your code has finished executing

    // Throw to fail, return to succeed
    let fail = false;
    if (fail) {
        throw "Failed basicCanary check."
    }
}
```
Next, we’ll expand the script to use Synthetics logging and make a call using the AWS SDK. For demonstration purposes, this script will create a Amazon DynamoDB client and make a call to the DynamoDB listTables API. It logs the response to the request and logs either pass or fail depending on whether the request was successful.

If you have more than a single .js file or you have a dependency that your script depends on, you can bundle them all into a single ZIP file that contains the folder structure nodejs/node_modules/myCanaryFilename.js file and other folders and files.

Be sure to set your canary's script entry point as myCanaryFilename.handler to match the file name of your script's entry point.

```javascript
const log = require('SyntheticsLogger');
const AWS = require('aws-sdk');
// Require any dependencies that your script needs
// Bundle additional files and dependencies into a .zip file with folder structure
// nodejs/node_modules/additional files and folders

const basicCustomEntryPoint = async function () {
    log.info("Starting DynamoDB:listTables canary.");
    let dynamodb = new AWS.DynamoDB();
    var params = {};
    let request = await dynamodb.listTables(params);
    try {
        let response = await request.promise();
        log.info("listTables response: " + JSON.stringify(response));
    } catch (err) {
        log.error("listTables error: " + JSON.stringify(err), err.stack);
        throw err;
    }
    return "Successfully completed DynamoDB:listTables canary.";
};
exports.handler = async () => {
    return await basicCustomEntryPoint();
};
```

Changing an existing Puppeteer script to use as a Synthetics canary

This section explains how to take Puppeteer scripts and modify them to run as Synthetics canary scripts. For more information about Puppeteer, see Puppeteer API v1.14.0.

We'll start with this example Puppeteer script:

```javascript
const puppeteer = require('puppeteer');
(async () => {
    const browser = await puppeteer.launch();
    const page = await browser.newPage();
    await page.goto('https://example.com');
    console.log("Successfully completed Puppeteer checks.");
    exports.handler = async () => {
        return await basicCustomEntryPoint();
    };
```

```javascript
```

156
Writing a canary script

The conversion steps are as follows:

- Create and export a handler function. The handler is the entry point function for the script.

```javascript
const basicPuppeteerExample = async function () {};
exports.handler = async () => {
  return await basicPuppeteerExample();
};
```

- Use the Synthetics dependency.

```javascript
var synthetics = require('Synthetics');
```

- Use the Synthetics.getPage function to get a Puppeteer Page object.

```javascript
const page = await synthetics.getPage();
```

The page object returned by the Synthetics.getPage function has the page.on request, response and requestfailed events instrumented for logging. Synthetics also sets up HAR file generation for requests and responses on the page, and adds the canary ARN to the user-agent headers of outgoing requests on the page.

The script is now ready to be run as a Synthetics canary. Here is the updated script:

```javascript
var synthetics = require('Synthetics');  // Synthetics dependency

const basicPuppeteerExample = async function () {
  const page = await synthetics.getPage(); // Get instrumented page from Synthetics
  await page.goto('https://example.com');  // Get instrumented page from Synthetics
  await page.screenshot({path: '/tmp/example.png'}); // Write screenshot to /tmp folder
};
exports.handler = async () => {  // Exported handler function
  return await basicPuppeteerExample();
};
```

Environment variables

You can use environment variables when creating canaries. This allows you to write a single canary script and then use that script with different values to quickly create multiple canaries that have a similar task.

For example, suppose your organization has endpoints such as prod, dev, and pre-release for the different stages of your software development, and you need to create canaries to test each of these endpoints. You can write a single canary script that tests your software and then specify different values for the endpoint environment variable when you create each of the three canaries. Then, when you create a canary, you specify the script and the values to use for the environment variables.

The names of environment variables can contain letters, numbers, and the underscore character. They must start with a letter and be at least two characters. The total size of your environment variables can't exceed 4 KB. You can't specify any Lambda reserved environment variables as the names of your environment variables. For more information about reserved environment variables, see Runtime environment variables.
The following example script uses two environment variables. This script is for a canary that checks whether a webpage is available. It uses environment variables to parameterize both the URL that it checks and the CloudWatch Synthetics log level that it uses.

The following function sets LogLevel to the value of the LOG_LEVEL environment variable.

```javascript
synthetics.setLogLevel(process.env.LOG_LEVEL);
```

This function sets URL to the value of the URL environment variable.

```javascript
const URL = process.env.URL;
```

This is the complete script. When you create a canary using this script, you specify values for the LOG_LEVEL and URL environment variables.

```javascript
var synthetics = require('Synthetics');
const log = require('SyntheticsLogger');
const pageLoadEnvironmentVariable = async function () {
  // Setting the log level (0-3)
  synthetics.setLogLevel(process.env.LOG_LEVEL);
  // INSERT URL here
  const URL = process.env.URL;

  let page = await synthetics.getPage();
  //You can customize the wait condition here. For instance,
  //using 'networkidle2' may be less restrictive.
  const response = await page.goto(URL, {waitUntil: 'domcontentloaded', timeout: 30000});
  if (!response) {
    throw "Failed to load page!";
  }
  //Wait for page to render.
  //Increase or decrease wait time based on endpoint being monitored.
  await page.waitFor(15000);
  await synthetics.takeScreenshot('loaded', 'loaded');
  log.info('Page title: ' + pageTitle);
  log.debug('Environment variable:' + process.env.URL);

  //If the response status code is not a 2xx success code
  if (response.status() < 200 || response.status() > 299) {
    throw "Failed to load page!";
  }
};
exports.handler = async () => {
  return await pageLoadEnvironmentVariable();
};
```

### Passing environment variables to your script

To pass environment variables to your script when you create a canary in the console, specify the keys and values of the environment variables in the `Environment variables` section on the console. For more information, see Creating a canary (p. 138).

To pass environment variables through the API or AWS CLI, use the `EnvironmentVariables` parameter in the `RunConfig` section. The following is an example AWS CLI command that creates a canary that uses two environment variables with keys of `Environment` and `Region`.

```bash
aws synthetics create-canary --cli-input-json '{
```

```json
  "EnvironmentVariables": [
    {
      "name": "Environment",
      "value": "production"
    },
    {
      "name": "Region",
      "value": "us-west-2"
    }
  ]
}
```
Integrating your canary with other AWS services

All canaries can use the AWS SDK library. You can use this library when you write your canary to integrate the canary with other AWS services.

To do so, you need to add the following code to your canary. AWS For these examples, AWS Secrets Manager is used as the service that the canary is integrating with.

- Import the AWS SDK.

```javascript
const AWS = require('aws-sdk');
```

- Create a client for the AWS service that you are integrating with.

```javascript
const secretsManager = new AWS.SecretsManager();
```

- Use the client to make API calls to that service.

```javascript
var params = {
    SecretId: secretName
};
return await secretsManager.getSecretValue(params).promise();
```

The following canary script code snippet demonstrates an example of integration with Secrets Manager in more detail.

```javascript
var synthetics = require('Synthetics');
const log = require('SyntheticsLogger');

const AWS = require('aws-sdk');
const secretsManager = new AWS.SecretsManager();

const getSecrets = async (secretName) => {
    var params = {
        SecretId: secretName
```
const secretsExample = async function () {
    let URL = "<URL>";
    let page = await synthetics.getPage();

    log.info('Navigating to URL: ${(URL)}');
    const response = await page.goto(URL, {waitFor: 'domcontentloaded', timeout: 30000});

    // Fetch secrets
    let secrets = await getSecrets("secretname")

    /**
     * Use secrets to login.
     *
     * Assuming secrets are stored in a JSON format like:
     * {
     *   "username": "<USERNAME>",
     *   "password": "<PASSWORD>"
     * }
     */
    let secretsObj = JSON.parse(secrets.SecretString);
    await synthetics.executeStep('login', async function () {
        await page.type("<USERNAME-INPUT-SELECTOR>", secretsObj.username);
        await page.type("<PASSWORD-INPUT-SELECTOR>", secretsObj.password);

        await Promise.all([
            page.waitForNavigation({ timeout: 30000 }),
            await page.click("<SUBMIT-BUTTON-SELECTOR>")
        ]);;
    });

    // Verify login was successful
    await synthetics.executeStep('verify', async function () {
        await page.waitForXPath("<SELECTOR>", { timeout: 30000 });
    });
};

exports.handler = async () => {
    return await secretsExample();
};

Forcing your canary to use a static IP address

You can set up a canary so that it uses a static IP address.

To force a canary to use a static IP address

1. Create a new VPC. For more information, see Using DNS with Your VPC.
2. Create a new internet gateway. For more information, see Adding an internet gateway to your VPC.
3. Create a public subnet inside your new VPC.
4. Add a new route table to the VPC.
5. Add a route in the new route table, that goes from 0.0.0.0/0 to the internet gateway.
6. Associate the new route table with the public subnet.
7. Create an elastic IP address. For more information, see Elastic IP addresses.
8. Create a new NAT gateway and assign it to the public subnet and the elastic IP address.
9. Create a private subnet inside the VPC.
10. Add a route to the VPC default route table, that goes from 0.0.0.0/0 to the NAT gateway.
11. Create your canary.

**Writing a Python canary script**

This script passes as a successful run, and returns a string. To see what a failing canary looks like, change `fail = False` to `fail = True`.

```python
def basic_custom_script():
    # Insert your code here
    # Perform multi-step pass/fail check
    # Log decisions made and results to /tmp
    # Be sure to wait for all your code paths to complete
    # before returning control back to Synthetics.
    # In that way, your canary will not finish and report success
    # before your code has finished executing
    fail = False
    if fail:
        raise Exception("Failed basicCanary check.")
    return "Successfully completed basicCanary checks."

def handler(event, context):
    return basic_custom_script()
```

If you have more than one .py file or your script has a dependency, you can bundle them all into a single ZIP file. The ZIP file must contain your main canary .py file within a `python` folder, such as `python/my_canary_filename.py`. This ZIP file should contain all necessary folders and files, but the other files do not need to be in the `python` folder.

Be sure to set your canary's script entry point as `my_canary_filename.handler` to match the file name of your script's entry point.

**Changing an existing Selenium script to use a Synthetics canary**

You can quickly modify an existing script for Python and Selenium to be used as a canary. For more information about Selenium, see [www.selenium.dev/](http://www.selenium.dev/).

For this example, we'll start with the following Selenium script:

```python
from selenium import webdriver

def basic_selenium_script():
    browser = webdriver.Chrome()
    browser.get('https://example.com')
    browser.save_screenshot('loaded.png')

basic_selenium_script()
```

The conversion steps are as follows.

**To convert a Selenium script to be used as a canary**

1. Change the `import` statement to use Selenium from the `aws_synthetics` module:

   ```python
   from aws_synthetics.selenium import synthetics_webdriver as webdriver
   ```

   The Selenium module from `aws_synthetics` ensures that the canary can emit metrics and logs, generate a HAR file, and work with other CloudWatch Synthetics features.

2. Create a handler function and call your Selenium method. The handler is the entry point function for the script.
def handler(event, context):
    basic_selenium_script()

The script is now updated to be a CloudWatch Synthetics canary. Here is the updated script:

```python
from aws_synthetics.selenium import synthetics_webdriver as webdriver

def basic_selenium_script():
    browser = webdriver.Chrome()
    browser.get('https://example.com')
    browser.save_screenshot('loaded.png')

def handler(event, context):
    basic_selenium_script()
```

Library functions available for canary scripts

CloudWatch Synthetics includes several built-in classes and functions that you can call when writing Node.js scripts to use as canaries.

Some apply to both UI and API canaries. Others apply to UI canaries only. A UI canary is a canary that uses the `getPage()` function and uses Puppeteer as a web driver to navigate and interact with webpages.

**Topics**

- Library functions available for Node.js canary scripts (p. 162)
- Library functions available for Python canary scripts using Selenium (p. 184)

Library functions available for Node.js canary scripts

This section lists the library functions available for Node.js canary scripts.

**Topics**

- Node.js library classes and functions that apply to all canaries (p. 162)
- Node.js library classes and functions that apply to UI canaries only (p. 175)
- Node.js library classes and functions that apply to API canaries only (p. 182)

Node.js library classes and functions that apply to all canaries

The following CloudWatch Synthetics library functions for Node.js are useful for all canaries.

**Topics**

- Synthetics class (p. 162)
- SyntheticsConfiguration class (p. 164)
- Synthetics logger (p. 172)
- SyntheticsLogHelper class (p. 173)

**Synthetics class**

The following functions for all canaries are in the Synthetics class.
addExecutionError(errorMessage, ex);

errorMessage describes the error and ex is the exception that is encountered.

You can use `addExecutionError` to set execution errors for your canary. It fails the canary without interrupting the script execution. It also doesn't impact your `successPercent` metrics.

You should track errors as execution errors only if they are not important to indicate the success or failure of your canary script.

An example of the use of `addExecutionError` is the following. You are monitoring the availability of your endpoint and taking screenshots after the page has loaded. Because the failure of taking a screenshot doesn't determine availability of the endpoint, you can catch any errors encountered while taking screenshots and add them as execution errors. Your availability metrics will still indicate that the endpoint is up and running, but your canary status will be marked as failed. The following sample code block catches such an error and adds it as an execution error.

```javascript
try {
    await synthetics.takeScreenshot(stepName, "loaded");
} catch(ex) {
    synthetics.addExecutionError('Unable to take screenshot ', ex);
}
```

`getCanaryName();`

Returns the name of the canary.

`getRuntimeVersion();`

This function is available in runtime version `syn-nodejs-puppeteer-3.0` and later. It returns the Synthetics runtime version of the canary. For example, the return value could be `syn-nodejs-puppeteer-3.0`.

`getLogLevel();`

Retrieves the current log level for the Synthetics library. Possible values are the following:

- 0 – Debug
- 1 – Info
- 2 – Warn
- 3 – Error

Example:

```javascript
let logLevel = synthetics.getLogLevel();
```

`setLogLevel();`

Sets the log level for the Synthetics library. Possible values are the following:

- 0 – Debug
- 1 – Info
- 2 – Warn
- 3 – Error
Example:

```javascript
synthetics.setLogLevel(0);
```

**SyntheticsConfiguration class**

This class is available only in the `syn-nodejs-2.1` runtime version or later.

You can use the SyntheticsConfiguration class to configure the behavior of Synthetics library functions. For example, you can use this class to configure the `executeStep()` function to not capture screenshots.

You can set CloudWatch Synthetics configurations at the global level, which are applied to all steps of canaries. You can also override these configurations at the step level by passing configuration key/value pairs.

You can pass in options at the step level. For examples, see `async executeStep(stepName, functionToExecute, [stepConfig]);` (p. 176) and `executeHttpStep(stepName, requestOptions, [callback], [stepConfig])` (p. 182)

Function definitions:

```javascript
setConfig(options)
```

`options` is an object, which is a set of configurable options for your canary. The following sections explain the possible fields in `options`.

**setConfig(options) for all canaries**

For canaries using `syn-nodejs-puppeteer-3.2` or later, the (options) for `setConfig` can include the following parameters:

- `includeRequestHeaders` (boolean)— Whether to include request headers in the report. The default is `false`.
- `includeResponseHeaders` (boolean)— Whether to include response headers in the report. The default is `false`.
- `restrictedHeaders` (array)— A list of header values to ignore, if headers are included. This applies to both request and response headers. For example, you can hide your credentials by passing `includeRequestHeaders` as `true` and `restrictedHeaders` as `['Authorization']`.
- `includeRequestBody` (boolean)— Whether to include the request body in the report. The default is `false`.
- `includeResponseBody` (boolean)— Whether to include the response body in the report. The default is `false`.

**setConfig(options) regarding CloudWatch metrics**

For canaries using `syn-nodejs-puppeteer-3.1` or later, the (options) for `setConfig` can include the following Boolean parameters that determine which metrics are published by the canary. The default for each of these options is `true`. The options that start with `aggregated` determine whether the metric is emitted without the `CanaryName` dimension. You can use these metrics to see the aggregated results for all of your canaries. The other options determine whether the metric is emitted with the `CanaryName` dimension. You can use these metrics to see results for each individual canary.

For a list of CloudWatch metrics emitted by canaries, see [CloudWatch metrics published by canaries](p. 202).
• **failedCanaryMetric** (boolean)— Whether to emit the Failed metric (with the CanaryName dimension) for this canary. The default is true.

• **failedRequestsMetric** (boolean)— Whether to emit the Failed requests metric (with the CanaryName dimension) for this canary. The default is true.

• **2xxMetric** (boolean)— Whether to emit the 2xx metric (with the CanaryName dimension) for this canary. The default is true.

• **4xxMetric** (boolean)— Whether to emit the 4xx metric (with the CanaryName dimension) for this canary. The default is true.

• **5xxMetric** (boolean)— Whether to emit the 5xx metric (with the CanaryName dimension) for this canary. The default is true.

• **stepDurationMetric** (boolean)— Whether to emit the Step duration metric (with the CanaryName StepName dimensions) for this canary. The default is true.

• **stepSuccessMetric** (boolean)— Whether to emit the Step success metric (with the CanaryName StepName dimensions) for this canary. The default is true.

• **aggregatedFailedCanaryMetric** (boolean)— Whether to emit the Failed metric (without the CanaryName dimension) for this canary. The default is true.

• **aggregatedFailedRequestsMetric** (boolean)— Whether to emit the Failed Requests metric (without the CanaryName dimension) for this canary. The default is true.

• **aggregated2xxMetric** (boolean)— Whether to emit the 2xx metric (without the CanaryName dimension) for this canary. The default is true.

• **aggregated4xxMetric** (boolean)— Whether to emit the 4xx metric (without the CanaryName dimension) for this canary. The default is true.

• **aggregated5xxMetric** (boolean)— Whether to emit the 5xx metric (without the CanaryName dimension) for this canary. The default is true.

• **visualMonitoringSuccessPercentMetric** (boolean)— Whether to emit the visualMonitoringSuccessPercent metric for this canary. The default is true.

• **visualMonitoringTotalComparisonsMetric** (boolean)— Whether to emit the visualMonitoringTotalComparisons metric for this canary. The default is false.

• **stepsReport** (boolean)— Whether to report a step execution summary. The default is true.

• **includeUrlPassword** (boolean)— Whether to include a password that appears in the URL. By default, passwords that appear in URLs are redacted from logs and reports, to prevent disclosing sensitive data. The default is false.

• **restrictedUrlParameters** (array)— A list of URL path or query parameters to redact. This applies to URLs appearing in logs, reports, and errors. The parameter is case-insensitive. You can pass an asterisk (*) as a value to redact all URL path and query parameter values. The default is an empty array.

• **logRequest** (boolean)— Whether to log every request in canary logs. For UI canaries, this logs each request sent by the browser. The default is true.

• **logResponse** (boolean)— Whether to log every response in canary logs. For UI canaries, this logs each response received by the browser. The default is true.

• **logRequestBody** (boolean)— Whether to log request bodies along with the requests in canary logs. This configuration applies only if logRequest is true. The default is false.

• **logResponseBody** (boolean)— Whether to log response bodies along with the responses in canary logs. This configuration applies only if logResponse is true. The default is false.

• **logRequestHeaders** (boolean)— Whether to log request headers along with the requests in canary logs. This configuration applies only if logRequest is true. The default is false.

• **logResponseHeaders** (boolean)— Whether to log response headers along with the responses in canary logs. This configuration applies only if logResponse is true. The default is false.

Note that includeRequestHeaders enables headers in artifacts.

• **logResponseHeaders** (boolean)— Whether to log response headers along with the responses in canary logs. This configuration applies only if logResponse is true. The default is false.

Note that includeResponseHeaders enables headers in artifacts.
**Note**
The Duration and SuccessPercent metrics are always emitted for each canary, both with and without the CanaryName metric.

**Methods to enable or disable metrics**

*disableAggregatedRequestMetrics()*  
Disables the canary from emitting all request metrics that are emitted with no CanaryName dimension.

*disableRequestMetrics()*  
Disables all request metrics, including both per-canary metrics and metrics aggregated across all canaries.

*enableAggregatedRequestMetrics()*  
Enables the canary to emit all request metrics that are emitted with no CanaryName dimension.

*enableRequestMetrics()*  
Enables all request metrics, including both per-canary metrics and metrics aggregated across all canaries.

*get2xxMetric()*  
Returns whether the canary emits a 2xx metric with the CanaryName dimension.

*get4xxMetric()*  
Returns whether the canary emits a 4xx metric with the CanaryName dimension.

*get5xxMetric()*  
Returns whether the canary emits a 5xx metric with the CanaryName dimension.

*getAggregated2xxMetric()*  
Returns whether the canary emits a 2xx metric with no dimension.

*getAggregated4xxMetric()*  
Returns whether the canary emits a 4xx metric with no dimension.

*getAggregatedFailedCanaryMetric()*  
Returns whether the canary emits a Failed metric with no dimension.

*getAggregatedFailedRequestsMetric()*  
Returns whether the canary emits a Failed requests metric with no dimension.

*getAggregated5xxMetric()*  
Returns whether the canary emits a 5xx metric with no dimension.

*getFailedCanaryMetric()*  
Returns whether the canary emits a Failed metric with the CanaryName dimension.

*getFailedRequestsMetric()*
Returns whether the canary emits a Failed requests metric with the CanaryName dimension.

getStepDurationMetric()

Returns whether the canary emits a Duration metric with the CanaryName dimension for this canary.

getStepSuccessMetric()

Returns whether the canary emits a StepSuccess metric with the CanaryName dimension for this canary.

with2xxMetric(_2xxMetric)

Accepts a Boolean argument, which specifies whether to emit a 2xx metric with the CanaryName dimension for this canary.

with4xxMetric(_4xxMetric)

Accepts a Boolean argument, which specifies whether to emit a 4xx metric with the CanaryName dimension for this canary.

with5xxMetric(_5xxMetric)

Accepts a Boolean argument, which specifies whether to emit a 5xx metric with the CanaryName dimension for this canary.

withAggregated2xxMetric(aggregated2xxMetric)

Accepts a Boolean argument, which specifies whether to emit a 2xx metric with no dimension for this canary.

withAggregated4xxMetric(aggregated4xxMetric)

Accepts a Boolean argument, which specifies whether to emit a 4xx metric with no dimension for this canary.

withAggregated5xxMetric(aggregated5xxMetric)

Accepts a Boolean argument, which specifies whether to emit a 5xx metric with no dimension for this canary.

withAggregatedFailedCanaryMetric(aggregatedFailedCanaryMetric)

Accepts a Boolean argument, which specifies whether to emit a Failed metric with no dimension for this canary.

withAggregatedFailedRequestsMetric(aggregatedFailedRequestsMetric)

Accepts a Boolean argument, which specifies whether to emit a Failed requests metric with no dimension for this canary.

withFailedCanaryMetric(failedCanaryMetric)

Accepts a Boolean argument, which specifies whether to emit a Failed metric with the CanaryName dimension for this canary.

withFailedRequestsMetric(failedRequestsMetric)

Accepts a Boolean argument, which specifies whether to emit a Failed requests metric with the CanaryName dimension for this canary.
**Library functions available for canary scripts**

**withStepDurationMetric(stepSuccessMetric)**

Accepts a Boolean argument, which specifies whether to emit a `Duration` metric with the `CanaryName` dimension for this canary.

**withStepSuccessMetric(stepSuccessMetric)**

Accepts a Boolean argument, which specifies whether to emit a `StepSuccess` metric with the `CanaryName` dimension for this canary.

**Methods to enable or disable other features**

**withHarFile()**

Accepts a Boolean argument, which specifies whether to create a HAR file for this canary.

**withStepsReport()**

Accepts a Boolean argument, which specifies whether to report a step execution summary for this canary.

**withIncludeUrlPassword()**

Accepts a Boolean argument, which specifies whether to include passwords that appear in URLs in logs and reports.

**withRestrictedUrlParameters()**

Accepts an array of URL path or query parameters to redact. This applies to URLs appearing in logs, reports, and errors. You can pass an asterisk (*) as a value to redact all URL path and query parameter values.

**withLogRequest()**

Accepts a Boolean argument, which specifies whether to log every request in the canary's logs.

**withLogResponse()**

Accepts a Boolean argument, which specifies whether to log every response in the canary's logs.

**withLogRequestBody()**

Accepts a Boolean argument, which specifies whether to log every request body in the canary's logs.

**withLogResponseBody()**

Accepts a Boolean argument, which specifies whether to log every response body in the canary's logs.

**withLogRequestHeaders()**

Accepts a Boolean argument, which specifies whether to log every request header in the canary's logs.

**withLogResponseHeaders()**

Accepts a Boolean argument, which specifies whether to log every response header in the canary's logs.

**getHarFile()**

Returns whether the canary creates a HAR file.
getStepsReport()

Returns whether the canary reports a step execution summary.

goingIncludeUrlPassword()

Returns whether the canary includes passwords that appear in URLs in logs and reports.

goingRestrictedUrlParameters()

Returns whether the canary redacts URL path or query parameters.

goingLogRequest()

Returns whether the canary logs every request in the canary's logs.

goingLogResponse()

Returns whether the canary logs every response in the canary's logs.

goingLogRequestBody()

Returns whether the canary logs every request body in the canary's logs.

goingLogResponseBody()

Returns whether the canary logs every response body in the canary's logs.

goingLogRequestHeaders()

Returns whether the canary logs every request header in the canary's logs.

goingLogResponseHeaders()

Returns whether the canary logs every response header in the canary's logs.

Functions for all canaries

- withIncludeRequestHeaders(includeRequestHeaders)
- withIncludeResponseHeaders(includeRequestHeaders)
- withRestrictedHeaders(restrictedHeaders)
- withIncludeRequestBody(includeRequestBody)
- withIncludeResponseBody(includeResponseBody)
- enableReportingOptions()— Enables all reporting options— includeRequestHeaders, includeResponseHeaders, includeRequestBody, and includeResponseBody.
- disableReportingOptions()— Disables all reporting options— includeRequestHeaders, includeResponseHeaders, includeRequestBody, and includeResponseBody.

getConfig( options ) for UI canaries

For UI canaries, getConfig can include the following Boolean parameters:

- continueOnStepFailure (boolean)— Whether to continue with running the canary script after a step fails (this refers to the executeStep function). If any steps fail, the canary run will still be marked as failed. The default is false.
- harFile (boolean)— Whether to create a HAR file. The default is True.
Library functions available for canary scripts

- screenshotOnStepStart (boolean)— Whether to take a screenshot before starting a step.
- screenshotOnStepSuccess (boolean)— Whether to take a screenshot after completing a successful step.
- screenshotOnStepFailure (boolean)— Whether to take a screenshot after a step fails.

Methods to enable or disable screenshots

disableStepScreenshots()

Disables all screenshot options (screenshotOnStepStart, screenshotOnStepSuccess, and screenshotOnStepFailure).

enableStepScreenshots()

Enables all screenshot options (screenshotOnStepStart, screenshotOnStepSuccess, and screenshotOnStepFailure). By default, all these methods are enabled.

getScreenshotOnStepFailure()

Returns whether the canary takes a screenshot after a step fails.

getScreenshotOnStepStart()

Returns whether the canary takes a screenshot before starting a step.

getScreenshotOnStepSuccess()

Returns whether the canary takes a screenshot after completing a step successfully.

withScreenshotOnStepStart(screenshotOnStepStart)

Accepts a Boolean argument, which indicates whether to take a screenshot before starting a step.

withScreenshotOnStepSuccess(screenshotOnStepSuccess)

Accepts a Boolean argument, which indicates whether to take a screenshot after completing a step successfully.

withScreenshotOnStepFailure(screenshotOnStepFailure)

Accepts a Boolean argument, which indicates whether to take a screenshot after a step fails.

Usage in UI canaries

First, import the synthetics dependency and fetch the configuration.

```javascript
// Import Synthetics dependency
const synthetics = require('Synthetics');

// Get Synthetics configuration
const synConfig = synthetics.getConfiguration();
```

Then, set the configuration for each option by calling the setConfig method using one of the following options.

```javascript
// Set configuration values
synConfig.setConfig(
```

Library functions available for canary scripts

```javascript
screenshotOnStepStart: true,
screenshotOnStepSuccess: false,
screenshotOnStepFailure: false
});
```

Or

```javascript
synConfig.withScreenshotOnStepStart(false).withScreenshotOnStepSuccess(true).withScreenshotOnStepFailure(true)
```

To disable all screenshots, use the `disableStepScreenshots()` function as in this example.

```javascript
synConfig.disableStepScreenshots();
```

You can enable and disable screenshots at any point in the code. For example, to disable screenshots only for one step, disable them before running that step and then enable them after the step.

### setConfig(options) for API canaries

For API canaries, `setConfig` can include the following Boolean parameters:

- `continueOnHttpStepFailure` (boolean) — Whether to continue with running the canary script after an HTTP step fails (this refers to the `executeHttpStep` function). If any steps fail, the canary run will still be marked as failed. The default is `true`.

#### Visual monitoring

Visual monitoring compares screenshots taken during a canary run with screenshots taken during a baseline canary run. If the discrepancy between the two screenshots is beyond a threshold percentage, the canary fails and you can see the areas with differences highlighted in color in the canary run report. Visual monitoring is supported in canaries running `syn-puppeteer-node-3.2` and later. It is not currently supported in canaries running Python and Selenium.

To enable visual monitoring, add the following line of code to the canary script. For more details, see `SyntheticsConfiguration` class (p. 164).

```javascript
syntheticsConfiguration.withVisualCompareWithBaseRun(true);
```

The first time that the canary runs successfully after this line is added to the script, it uses the screenshots taken during that run as the baseline for comparison. After that first canary run, you can use the CloudWatch console to edit the canary to do any of the following:

- Set the next run of the canary as the new baseline.
- Draw boundaries on the current baseline screenshot to designate areas of the screenshot to ignore during visual comparisons.
- Remove a screenshot from being used for visual monitoring.

For more information about using the CloudWatch console to edit a canary, see Editing or deleting a canary (p. 203).

#### Other options for visual monitoring

```javascript
syntheticsConfiguration.withVisualVarianceThresholdPercentage(desiredPercentage)
```

Set the acceptable percentage for screenshot variance in visual comparisons.
syntheticsConfiguration.withVisualVarianceHighlightHexColor("#fafa00")

Set the highlight color that designates variance areas when you look at canary run reports that use visual monitoring.

syntheticsConfiguration.withFailCanaryRunOnVisualVariance(failCanary)

Set whether or not the canary fails when there is a visual difference that is more than the threshold. The default is to fail the canary.

Synthetics logger

SyntheticsLogger writes logs out to both the console and to a local log file at the same log level. This log file is written to both locations only if the log level is at or below the desired logging level of the log function that was called.

The logging statements in the local log file are prepended with "DEBUG: ", "INFO: ", and so on to match the log level of the function that was called.

You can use the SyntheticsLogger, assuming you want to run the Synthetics Library at the same log level as your Synthetics canary logging.

Using the SyntheticsLogger is not required to create a log file that is uploaded to your S3 results location. You could instead create a different log file in the /tmp folder. Any files created under the /tmp folder are uploaded to the results location in S3 as artifacts.

To use the Synthetics Library logger:

```javascript
const log = require('SyntheticsLogger');
```

Useful function definitions:

`log.debug(message, ex);`

Parameters: `message` is the message to log. `ex` is the exception, if any, to log.

Example:

```javascript
log.debug("Starting step - login.");
```

`log.error(message, ex);`

Parameters: `message` is the message to log. `ex` is the exception, if any, to log.

Example:

```javascript
try {
  await login();
} catch (ex) {
  log.error("Error encountered in step - login.", ex);
}
```

`log.info(message, ex);`

Parameters: `message` is the message to log. `ex` is the exception, if any, to log.

Example:
log.info("Successfully completed step - login.");

log.log(message, ex);

This is an alias for log.info.

Parameters: message is the message to log. ex is the exception, if any, to log.

Example:

log.log("Successfully completed step - login.");

log.warn(message, ex);

Parameters: message is the message to log. ex is the exception, if any, to log.

Example:

log.warn("Exception encountered trying to publish CloudWatch Metric.", ex);

SyntheticsLogHelper class

The SyntheticsLogHelper class is available in the runtime syn-nodejs-puppeteer-3.2 and later runtimes. It is already initialized in the CloudWatch Synthetics library and is configured with Synthetics configuration. You can add this as a dependency in your script. This class enables you to sanitize URLs, headers, and error messages to redact sensitive information.

Note

Synthetics sanitizes all URLs and error messages it logs before including them in logs, reports, HAR files, and canary run errors based on the Synthetics configuration setting restrictedUrlParameters. You have to use getSanitizedUrl or getSanitizedErrorMessage only if you are logging URLs or errors in your script. Synthetics does not store any canary artifacts except for canary errors thrown by the script. Canary run artifacts are stored in your customer account. For more information, see Security considerations for Synthetics canaries (p. 741).

getSanitizedUrl(url, stepConfig = null)

This function is available in syn-nodejs-puppeteer-3.2 and later. It returns sanitized url strings based on the configuration. You can choose to redact sensitive URL parameters such as password and access_token by setting the property restrictedUrlParameters. By default, passwords in URLs are redacted. You can enable URL passwords if needed by setting includeUrlPassword to true.

This function throws an error if the URL passed in is not a valid URL.

Parameters

- url is a string and is the URL to sanitize.
- stepConfig (Optional) overrides the global Synthetics configuration for this function. If stepConfig is not passed in, the global configuration is used to sanitize the URL.

Example

This example uses the following sample URL: https://example.com/learn/home?access_token=12345&token_type=Bearer&expires_in=1200. In this example, access_token contains your sensitive information which shouldn't be logged. Note that the Synthetics services doesn't
store any canary run artifacts. Artifacts such as logs, screenshots, and reports are all stored in an Amazon S3 bucket in your customer account.

The first step is to set the Synthetics configuration.

```javascript
// Import Synthetics dependency
const synthetics = require('Synthetics');

// Import Synthetics logger for logging url
const log = require('SyntheticsLogger');

// Get Synthetics configuration
const synConfig = synthetics.getConfiguration();

// Set restricted parameters
synConfig.setConfig(
  restrictedUrlParameters: ['access_token'];
);  
```

Next, sanitize and log the URL

```javascript
// Import SyntheticsLogHelper dependency
const syntheticsLogHelper = require('SyntheticsLogHelper');

const sanitizedUrl = synthetics.getSanitizedUrl('https://example.com/learn/home?
access_token=12345&token_type=Bearer&expires_in=1200');

```

This logs the following in your canary log.

```
My example url is: https://example.com/learn/home?
access_token=REDACTED&token_type=Bearer&expires_in=1200
```

You can override the Synthetics configuration for a URL by passing in an optional parameter containing Synthetics configuration options, as in the following example.

```javascript
const urlConfig = {
  restrictedUrlParameters = ['*']
};
const sanitizedUrl = synthetics.getSanitizedUrl('https://example.com/learn/home?
access_token=12345&token_type=Bearer&expires_in=1200', urlConfig);
logger.info('My example url is: ' + sanitizedUrl);
```

The preceding example redacts all query parameters, and is logged as follows:

```
My example url is: https://example.com/learn/home?
access_token=REDACTED&token_type=Bearer&expires_in=REDACTED
```

getSanitizedErrorMessage

This function is available in syn-nodejs-puppeteer-3.2 and later. It returns sanitized error strings by sanitizing any URLs present based on the Synthetics configuration. You can choose to override the global Synthetics configuration when you call this function by passing an optional stepConfig parameter.

**Parameters**

- `error` is the error to sanitize. It can be an Error object or a string.
- `stepConfig` (Optional) overrides the global Synthetics configuration for this function. If stepConfig is not passed in, the global configuration is used to sanitize the URL.
Example

This example uses the following error: Failed to load url: https://example.com/learn/home?access_token=12345&token_type=Bearer.expires_in=1200

The first step is to set the Synthetics configuration.

```javascript
// Import Synthetics dependency
const synthetics = require('Synthetics');

// Import Synthetics logger for logging url
const log = require('SyntheticsLogger');

// Get Synthetics configuration
const synConfig = synthetics.getConfiguration();

// Set restricted parameters
synConfig.setConfig({
  restrictedUrlParameters: ['access_token'];
});
```

Next, sanitize and log the error message

```javascript
// Import SyntheticsLogHelper dependency
const syntheticsLogHelper = require('SyntheticsLogHelper');

try {
  // Your code which can throw an error containing url which your script logs

  // Get sanitized error message
  const sanitizedErrorMessage = synthetics.getSanitizedErrorMessage(errorMessage);
  logger.info(sanitizedErrorMessage);
}
```

This logs the following in your canary log.

```
Failed to load url: https://example.com/learn/home?
access_token=REDACTED&token_type=Bearer&expires_in=1200
```

getSanitizedHeaders(headers, stepConfig=null)

This function is available in syn-nodejs-puppeteer-3.2 and later. It returns sanitized headers based on the restrictedHeaders property of syntheticsConfiguration. The headers specified in the restrictedHeaders property are redacted from logs, HAR files, and reports.

Parameters

- **headers** is an object containing the headers to sanitize.
- **stepConfig** (Optional) overrides the global Synthetics configuration for this function. If stepConfig is not passed in, the global configuration is used to sanitize the headers.

Node.js library classes and functions that apply to UI canaries only

The following CloudWatch Synthetics library functions for Node.js are useful only for UI canaries.

Topics

- Synthetics class (p. 176)
- BrokenLinkCheckerReport class (p. 180)
• **SyntheticsLink class (p. 181)**

**Synthetics class**

The following functions are in the Synthetics class.

`async addUserAgent(page, userAgentString);`

This function appends `userAgentString` to the specified page's user-agent header.

Example:

```javascript
await synthetics.addUserAgent(page, "MyApp-1.0");
```

Results in the page's user-agent header being set to `browsers-user-agent-header-valueMyApp-1.0`

`async executeStep(stepName, functionToExecute, [stepConfig]);`

Executes the provided step, wrapping it with start/pass/fail logging, start/pass/fail screenshots, and pass/fail and duration metrics.

**Note**

If you are using the `syn-nodejs-2.1` or later runtime, you can configure whether and when screenshots are taken. For more information, see **SyntheticsConfiguration class (p. 164)**.

The `executeStep` function also does the following:

- Logs that the step started.
- Takes a screenshot named `<stepName>-starting`.
- Starts a timer.
- Executes the provided function.
- If the function returns normally, it counts as passing. If the function throws, it counts as failing.
- Ends the timer.
- Logs whether the step passed or failed
- Takes a screenshot named `<stepName>-succeeded` or `<stepName>-failed`.
- Emits the `stepName SuccessPercent` metric, 100 for pass or 0 for failure.
- Emits the `stepName Duration` metric, with a value based on the step start and end times.
- Finally, returns what the `functionToExecute` returned or re-throws what `functionToExecute` threw.

If the canary uses the `syn-nodejs-2.0` runtime or later, this function also adds a step execution summary to the canary's report. The summary includes details about each step, such as start time, end time, status (PASSED/FAILED), failure reason (if failed), and screenshots captured during the execution of each step.

Example:

```javascript
await synthetics.executeStep('navigateToUrl', async function (timeoutInMillis = 30000) {
    await page.goto(url, {waitUntil: ['load', 'networkidle0'], timeout: timeoutInMillis});
});
```

Response:

Returns what `functionToExecute` returns.
Updates with syn-nodejs-2.2

Starting with syn-nodejs-2.2, you can optionally pass step configurations to override CloudWatch Synthetics configurations at the step level. For a list of options that you can pass to executeStep, see SyntheticsConfiguration class (p. 164).

The following example overrides the default false configuration for continueOnStepFailure to true and specifies when to take screenshots.

```javascript
var stepConfig = {
    'continueOnStepFailure': true,
    'screenshotOnStepStart': false,
    'screenshotOnStepSuccess': true,
    'screenshotOnStepFailure': false
}

await executeStep('Navigate to amazon', async function (timeoutInMillis = 30000) {
    await page.goto(url, {waitUntil: ['load', 'networkidle0'], timeout: timeoutInMillis});
}, stepConfig);
```

getDefaultLaunchOptions();

The getDefaultLaunchOptions() function returns the browser launch options that are used by CloudWatch Synthetics. For more information, see puppeteer.launch([options])

```javascript
// This function returns default launch options used by Synthetics.
const defaultOptions = await synthetics.getDefaultLaunchOptions();
```

goingPage();

Returns the current open page as a Puppeteer object. For more information, see Puppeteer API v1.14.0.

Example:

```javascript
let page = synthetics.getPage();
```

Response:

The page (Puppeteer object) that is currently open in the current browser session.

goingRequestResponseLogHelper();

Important

In canaries that use the syn-nodejs-puppeteer-3.2 runtime or later, this function is deprecated along with the RequestResponseLogHelper class. Any use of this function causes a warning to appear in your canary logs. This function will be removed in future runtime versions. If you are using this function, use RequestResponseLogHelper class (p. 178) instead.

Use this function as a builder pattern for tweaking the request and response logging flags.

Example:

```javascript
synthetics.setRequestResponseLogHelper(getRequestResponseLogHelper().withLogRequestHeaders(false));
```

Response:

{RequestResponseLogHelper}
launch(options)

The options for this function are available only in the syn-nodejs-2.1 runtime version or later.

This function is used only for UI canaries. It closes the existing browser and launches a new one.

**Note**
CloudWatch Synthetics always launches a browser before starting to run your script. You don't need to call launch() unless you want to launch a new browser with custom options.

(options) is a configurable set of options to set on the browser. For more information, see puppeteer.launch([options]).

If you call this function with no options, Synthetics launches a browser with default arguments, executablePath, and defaultViewport. The default viewport in CloudWatch Synthetics is 1920 by 1080.

You can override launch parameters used by CloudWatch Synthetics and pass additional parameters when launching the browser. For example, the following code snippet launches a browser with default arguments and a default executable path, but with a viewport of 800 x 600.

```javascript
await synthetics.launch({
  defaultViewport: {
    "deviceScaleFactor": 1,
    "width": 800,
    "height": 600
  }
});
```

The following sample code adds a new ignoreHTTPSErrors parameter to the CloudWatch Synthetics launch parameters:

```javascript
await synthetics.launch({
  ignoreHTTPSErrors: true
});
```

You can disable web security by adding a --disable-web-security flag to args in the CloudWatch Synthetics launch parameters:

```javascript
// This function adds the --disable-web-security flag to the launch parameters
const defaultOptions = await synthetics.getDefaultLaunchOptions();
const launchArgs = [...defaultOptions.args, '--disable-web-security'];
await synthetics.launch({
  args: launchArgs
});
```

**RequestResponseLogHelper class**

**Important**
In canaries that use the syn-nodejs-puppeteer-3.2 runtime or later, this class is deprecated. Any use of this class causes a warning to appear in your canary logs. This function will be removed in future runtime versions. If you are using this function, use RequestResponseLogHelper class (p. 178) instead.

Handles the fine-grained configuration and creation of string representations of request and response payloads.

```javascript
class RequestResponseLogHelper {
  constructor () {
```
Library functions available for canary scripts

```javascript
this.request = {url: true, resourceType: false, method: false, headers: false, postData: false};
this.response = {status: true, statusText: true, url: true, remoteAddress: false, headers: false};
}
withLogRequestUrl(logRequestUrl);
withLogRequestResourceType(logRequestResourceType);
withLogRequestMethod(logRequestMethod);
withLogRequestHeaders(logRequestHeaders);
withLogRequestPostData(logRequestPostData);
withLogResponseStatus(logResponseStatus);
withLogResponseStatusText(logResponseStatusText);
withLogResponseUrl(logResponseUrl);
withLogResponseRemoteAddress(logResponseRemoteAddress);
withLogResponseHeaders(logResponseHeaders);
```

Example:

```javascript
synthetics.setRequestResponseLogHelper(getRequestResponseLogHelper()
  .withLogRequestPostData(true)
  .withLogRequestHeaders(true)
  .withLogResponseHeaders(true));
```

Response:

```javascript
{RequestResponseLogHelper}
```

```javascript
setRequestResponseLogHelper();
```

**Important**

In canaries that use the `syn-nodejs-puppeteer-3.2` runtime or later, this function is deprecated along with the `RequestResponseLogHelper` class. Any use of this function causes a warning to appear in your canary logs. This function will be removed in future runtime versions. If you are using this function, use `RequestResponseLogHelper class (p. 178)` instead.

Use this function as a builder pattern for setting the request and response logging flags.

Example:

```javascript
synthetics.setRequestResponseLogHelper().withLogRequestHeaders(true).withLogResponseHeaders(true);
```

Response:

```javascript
{RequestResponseLogHelper}
```

```javascript
async takeScreenshot(name, suffix);
```

Takes a screenshot (.PNG) of the current page with name and suffix (optional).
Example:

```javascript
await synthetics.takeScreenshot("navigateToUrl", "loaded")
```

This example captures and uploads a screenshot named `01-navigateToUrl-loaded.png` to the canary's S3 bucket.

You can take a screenshot for a particular canary step by passing the `stepName` as the first parameter. Screenshots are linked to the canary step in your reports, to help you track each step while debugging.

CloudWatch Synthetics canaries automatically take screenshots before starting a step (the `executeStep` function) and after the step completion (unless you configure the canary to disable screenshots). You can take more screenshots by passing in the step name in the `takeScreenshot` function.

The following example takes screenshot with the `signupForm` as the value of the `stepName`. The screenshot will be named `02-signupForm-address` and will be linked to the step named `signupForm` in the canary report.

```javascript
await synthetics.takeScreenshot('signupForm', 'address')
```

**BrokenLinkCheckerReport class**

This class provides methods to add a synthetics link. It's supported only on canaries that use the `syn-nodejs-2.0-beta` version of the runtime or later.

To use `BrokenLinkCheckerReport`, include the following lines in the script:

```javascript
const BrokenLinkCheckerReport = require('BrokenLinkCheckerReport');
const brokenLinkCheckerReport = new BrokenLinkCheckerReport();
```

Useful function definitions:

**addLink**

```javascript
addLink(syntheticsLink, isBroken)
```

- `syntheticsLink` is a `SyntheticsLink` object representing a link. This function adds the link according to the status code. By default, it considers a link to be broken if the status code is not available or the status code is 400 or higher. You can override this default behavior by passing in the optional parameter `isBrokenLink` with a value of `true` or `false`.

This function does not have a return value.

**getLinks()**

This function returns an array of `SyntheticsLink` objects that are included in the broken link checker report.

**getTotalBrokenLinks()**

This function returns a number representing the total number of broken links.

**getTotalLinksChecked()**

This function returns a number representing the total number of links included in the report.

**How to use BrokenLinkCheckerReport**

The following canary script code snippet demonstrates an example of navigating to a link and adding it to the broken link checker report.
1. **Import** `SyntheticsLink`, `BrokenLinkCheckerReport`, and `Synthetics`.

```javascript
const BrokenLinkCheckerReport = require('BrokenLinkCheckerReport');
const SyntheticsLink = require('SyntheticsLink');

// Synthetics dependency
const synthetics = require('Synthetics');
```

2. **To add a link to the report, create an instance of `BrokenLinkCheckerReport`**.

```javascript
let brokenLinkCheckerReport = new BrokenLinkCheckerReport();
```

3. **Navigate to the URL and add it to the broken link checker report**.

```javascript
let url = "https://amazon.com";

let syntheticsLink = new SyntheticsLink(url);

// Navigate to the url.
let page = await synthetics.getPage();

// Create a new instance of Synthetics Link
let link = new SyntheticsLink(url)

try {
    const response = await page.goto(url, {waitUntil: 'domcontentloaded', timeout: 30000});
} catch (ex) {
    // Add failure reason if navigation fails.
    link.withFailureReason(ex);
}

if (response) {
    // Capture screenshot of destination page
    let screenshotResult = await synthetics.takeScreenshot('amazon-home', 'loaded');

    // Add screenshot result to synthetics link
    link.addScreenshotResult(screenshotResult);

    // Add status code and status description to the link
    link.withStatusCode(response.status()).withStatusText(response.statusText());
}

// Add link to broken link checker report.
brokenLinkCheckerReport.addLink(link);
```

4. **Add the report to Synthetics.** This creates a JSON file named `BrokenLinkCheckerReport.json` in your S3 bucket for each canary run. You can see a links report in the console for each canary run along with screenshots, logs, and HAR files.

```javascript
await synthetics.addReport(brokenLinkCheckerReport);
```

**SyntheticsLink class**

This class provides methods to wrap information. It's supported only on canaries that use the `sy-nodejs-2.0-beta` version of the runtime or later.

To use `SyntheticsLink`, include the following lines in the script:

```javascript
const SyntheticsLink = require('SyntheticsLink');
```
const syntheticsLink = new SyntheticsLink("https://www.amazon.com");

This function returns `syntheticsLinkObject`.

Useful function definitions:

**withUrl(url)**

`url` is a URL string. This function returns `syntheticsLinkObject`.

**withText(text)**

`text` is a string representing anchor text. This function returns `syntheticsLinkObject`. It adds anchor text corresponding to the link.

**withParentUrl(parentUrl)**

`parentUrl` is a string representing the parent (source page) URL. This function returns `syntheticsLinkObject`.

**withStatusCode(statusCode)**

`statusCode` is a string representing the status code. This function returns `syntheticsLinkObject`.

**withFailureReason(failureReason)**

`failureReason` is a string representing the failure reason. This function returns `syntheticsLinkObject`.

**addScreenshotResult(screenshotResult)**

`screenshotResult` is an object. It is an instance of `ScreenshotResult` that was returned by the `Synthetics` function `takeScreenshot`. The object includes the following:

- `fileName`— A string representing the `screenshotFileName`
- `pageUrl` (optional)
- `error` (optional)

**Node.js library classes and functions that apply to API canaries only**

The following CloudWatch Synthetics library functions for Node.js are useful only for API canaries.

**Topics**

- `executeHttpStep(stepName, requestOptions, [callback], [stepConfig])` (p. 182)

**executeHttpStep(stepName, requestOptions, [callback], [stepConfig])**

Executes the provided HTTP request as a step, and publishes `SuccessPercent` (pass/fail) and `Duration` metrics.

`executeHttpStep` uses either HTTP or HTTPS native functions under the hood, depending upon the protocol specified in the request.

This function also adds a step execution summary to the canary's report. The summary includes details about each HTTP request, such as the following:
Library functions available for canary scripts

- Start time
- End time
- Status (PASSED/FAILED)
- Failure reason, if it failed
- HTTP call details such as request/response headers, body, status code, status message, and performance timings.

**Parameters**

**stepName**(*String*)

Specifies the name of the step. This name is also used for publishing CloudWatch metrics for this step.

**requestOptions**(*Object or String*)

The value of this parameter can be a URL, a URL string, or an object. If it is an object, then it must be a set of configurable options to make an HTTP request. It supports all options in `http.request([options[, callback]])` in the Node.js documentation.

In addition to these Node.js options, `requestOptions` supports the additional parameter `body`. You can use the `body` parameter to pass data as a request body.

**callback**(*response*)

(Optional) This is a user function which is invoked with the HTTP response. The response is of the type `Class: http.IncomingMessage`.

**stepConfig**(*object*)

(Optional) Use this parameter to override global synthetics configurations with a different configuration for this step.

**Examples of using executeHttpRequest**

The following series of examples build on each other to illustrate the various uses of this option.

This first example configures request parameters. You can pass a URL as `requestOptions`:

```javascript
let requestOptions = 'https://www.amazon.com';
```

Or you can pass a set of options:

```javascript
let requestOptions = {
  'hostname': 'myproductsEndpoint.com',
  'method': 'GET',
  'path': '/test/product/validProductName',
  'port': 443,
  'protocol': 'https:'
};
```

The next example creates a callback function which accepts a response. By default, if you do not specify `callback`, CloudWatch Synthetics validates that the status is between 200 and 299 inclusive.

```javascript
// Handle validation for positive scenario
const callback = async function(res) {
```

183
return new Promise((resolve, reject) => {
    if (res.statusCode < 200 || res.statusCode > 299) {
        throw res.statusCode + ' ' + res.statusMessage;
    }

    let responseBody = '';
    res.on('data', (d) => {
        responseBody += d;
    });

    res.on('end', () => {
        // Add validation on 'responseBody' here if required. For ex, your status code is 200 but data might be empty
        resolve();
    });
});

The next example creates a configuration for this step that overrides the global CloudWatch Synthetics configuration. The step configuration in this example allows request headers, response headers, request body (post data), and response body in your report and restrict 'X-Amz-Security-Token' and 'Authorization' header values. By default, these values are not included in the report for security reasons. If you choose to include them, the data is only stored in your S3 bucket.

// By default headers, post data, and response body are not included in the report for security reasons.
// Change the configuration at global level or add as step configuration for individual steps
let stepConfig = {
    includeRequestHeaders: true,
    includeResponseHeaders: true,
    includeRequestBody: true,
    includeResponseBody: true
};

This final example passes your request to executeHttpStep and names the step.

await synthetics.executeHttpStep('Verify GET products API', requestOptions, callback, stepConfig);

With this set of examples, CloudWatch Synthetics adds the details from each step in your report and produces metrics for each step using stepName.

You will see successPercent and duration metrics for the Verify GET products API step. You can monitor your API performance by monitoring the metrics for your API call steps.

For a sample complete script that uses these functions, see Multi-step API canary (p. 197).

Library functions available for Python canary scripts using Selenium

This section lists the Selenium library functions available for Python canary scripts.

Topics

- Python and Selenium library classes and functions that apply to all canaries (p. 185)
- Python and Selenium library classes and functions that apply to UI canaries only (p. 188)
Python and Selenium library classes and functions that apply to all canaries

The following CloudWatch Synthetics Selenium library functions for Python are useful for all canaries.

Topics

- SyntheticsConfiguration class (p. 185)
- SyntheticsLogger class (p. 186)

SyntheticsConfiguration class

You can use the SyntheticsConfiguration class to configure the behavior of Synthetics library functions. For example, you can use this class to configure the `executeStep()` function to not capture screenshots.

You can set CloudWatch Synthetics configurations at the global level.

Function definitions:

`set_config(options)`

```python
from aws_synthetics.common import synthetics_configuration

options is an object, which is a set of configurable options for your canary. The following sections explain the possible fields in options.

- screenshot_on_step_start (boolean)— Whether to take a screenshot before starting a step.
- screenshot_on_step_success (boolean)— Whether to take a screenshot after completing a successful step.
- screenshot_on_step_failure (boolean)— Whether to take a screenshot after a step fails.
```

`with_screenshot_on_step_start(screenshot_on_step_start)`

Accepts a Boolean argument, which indicates whether to take a screenshot before starting a step.

`with_screenshot_on_step_success(screenshot_on_step_success)`

Accepts a Boolean argument, which indicates whether to take a screenshot after completing a step successfully.

`with_screenshot_on_step_failure(screenshot_on_step_failure)`

Accepts a Boolean argument, which indicates whether to take a screenshot after a step fails.

`get_screenshot_on_step_start()`

Returns whether to take a screenshot before starting a step.

`get_screenshot_on_step_success()`

Returns whether to take a screenshot after completing a step successfully.

`get_screenshot_on_step_failure()`

Returns whether to take a screenshot after a step fails.

`disable_stepScreenshots()`
Disables all screenshot options (get_screenshot_on_step_start, get_screenshot_on_step_success, and get_screenshot_on_step_failure).

**enable_step_screenshots()**

Enables all screenshot options (get_screenshot_on_step_start, get_screenshot_on_step_success, and get_screenshot_on_step_failure). By default, all these methods are enabled.

**Usage in UI canaries**

First, import the synthetics dependency and fetch the configuration. Then, set the configuration for each option by calling the setConfig method using one of the following options.

```python
from aws_synthetics.common import synthetics_configuration

synthetics_configuration.set_config(
    {
        "screenshot_on_step_start": False,
        "screenshot_on_step_success": False,
        "screenshot_on_step_failure": True
    }
)

or

synthetics_configuration.with_screenshot_on_step_start(False).with_screenshot_on_step_success(False).with_screenshot_on_step_failure(True)
```

To disable all screenshots, use the disableStepScreenshots() function as in this example.

```python
synthetics_configuration.disable_step_screenshots()
```

You can enable and disable screenshots at any point in the code. For example, to disable screenshots only for one step, disable them before running that step and then enable them after the step.

**SyntheticsLogger class**

`synthetics_logger` writes logs out to both the console and to a local log file at the same log level. This log file is written to both locations only if the log level is at or below the desired logging level of the log function that was called.

The logging statements in the local log file are prepended with "DEBUG: ", "INFO: ", and so on to match the log level of the function that was called.

Using `synthetics_logger` is not required to create a log file that is uploaded to your Amazon S3 results location. You could instead create a different log file in the `/tmp` folder. Any files created under the `/tmp` folder are uploaded to the results location in the S3 bucket as artifacts.

**To use synthetics_logger:**

```python
from aws_synthetics.common import synthetics_logger

Useful function definitions:

Get log level:
log_level = synthetics_logger.get_level()

Set log level:

synthetics_logger.set_level()

Log a message with a specified level. The level can be DEBUG, INFO, WARN, or ERROR, as in the following syntax examples:

synthetics_logger.debug(message, *args, **kwargs)
synthetics_logger.info(message, *args, **kwargs)
synthetics_logger.log(message, *args, **kwargs)
synthetics_logger.warn(message, *args, **kwargs)
synthetics_logger.error(message, *args, **kwargs)

For information about debug parameters, see the standard Python documentation at `logging.debug`

In these logging functions, the `message` is the message format string. The `args` are the arguments that are merged into `msg` using the string formatting operator.

There are three keyword arguments in `kwargs`:

- `exc_info`– If not evaluated as false, adds exception information to the logging message.
- `stack_info`– defaults to false. If true, adds stack information to the logging message, including the actual logging call.
- `extra`– The third optional keyword argument, which you can use to pass in a dictionary that is used to populate the `__dict__` of the LogRecord created for the logging event with user-defined attributes.

Examples:

Log a message with the level DEBUG:

```python
synthetics_logger.debug('Starting step - login.')
```

Log a message with the level INFO. `logger.log` is a synonym for `logger.info`:

```python
synthetics_logger.info('Successfully completed step - login.')
```

or

```python
synthetics_logger.log('Successfully completed step - login.')
```

Log a message with the level WARN:

```python
synthetics_logger.warn('Warning encountered trying to publish %s', 'CloudWatch Metric')
```
Log a message with the level ERROR:

```python
synthetics_logger.error('Error encountered trying to publish %s', 'CloudWatch Metric')
```

Log an exception:

```python
synthetics_logger.exception(message, *args, **kwargs)
```

Logs a message with level ERROR. Exception information is added to the logging message. You should call this function only from an exception handler.

For information about exception parameters, see the standard Python documentation at `logging.exception`.

The `message` is the message format string. The `args` are the arguments, which are merged into `msg` using the string formatting operator.

There are three keyword arguments in `kwargs`:

- `exc_info` - If not evaluated as false, adds exception information to the logging message.
- `stack_info` - defaults to false. If true, adds stack information to the logging message, including the actual logging call.
- `extra` - The third optional keyword argument, which you can use to pass in a dictionary that is used to populate the `__dict__` of the LogRecord created for the logging event with user-defined attributes.

Example:

```python
synthetics_logger.exception('Error encountered trying to publish %s', 'CloudWatch Metric')
```

**Python and Selenium library classes and functions that apply to UI canaries only**

The following CloudWatch Synthetics Selenium library functions for Python are useful only for UI canaries.

**Topics**

- SyntheticsBrowser class (p. 188)
- SyntheticsWebDriver class (p. 189)

**SyntheticsBrowser class**

When you create a browser instance by calling `synthetics_webdriver.Chrome()`, the returned browser instance is of the type `SyntheticsBrowser`. The `SyntheticsBrowser` class controls the ChromeDriver, and enables the canary script to drive the browser, allowing the Selenium WebDriver to work with Synthetics.

In addition to the standard Selenium methods, it also provides the following methods:

- `set_viewport_size(width, height)`

Sets the viewport of the browser. Example:

```python
browser.set_viewport_size(1920, 1080)
```
save_screenshot(filename, suffix)

Saves screenshots to the `/tmp` directory. The screenshots are uploaded from there to the canary artifacts folder in the S3 bucket.

`filename` is the file name for the screenshot, and `suffix` is an optional string to be used for naming the screenshot.

Example:

```python
browser.save_screenshot('loaded.png', 'page1')
```

SyntheticsWebDriver class

To use this class, use the following in your script:

```python
from aws_synthetics.selenium import synthetics_webdriver
add_execution_error(errorMessage, ex);
```

`errorMessage` describes the error and `ex` is the exception that is encountered

You can use `add_execution_error` to set execution errors for your canary. It fails the canary without interrupting the script execution. It also doesn't impact your successPercent metrics.

You should track errors as execution errors only if they are not important to indicate the success or failure of your canary script.

An example of the use of `add_execution_error` is the following. You are monitoring the availability of your endpoint and taking screenshots after the page has loaded. Because the failure of taking a screenshot doesn't determine availability of the endpoint, you can catch any errors encountered while taking screenshots and add them as execution errors. Your availability metrics will still indicate that the endpoint is up and running, but your canary status will be marked as failed. The following sample code block catches such an error and adds it as an execution error.

```python
try:
    browser.save_screenshot("loaded.png")
except Exception as ex:
    self.add_execution_error("Unable to take screenshot", ex)
```

add_user_agent(user_agent_str)

Appends the value of `user_agent_str` to the browser's user agent header. You must assign `user_agent_str` before creating the browser instance.

Example:

```python
synthetics_webdriver.add_user_agent('MyApp-1.0')
```

execute_step(step_name, function_to_execute)

Processes one function. It also does the following:

- Logs that the step started.
- Takes a screenshot named `<stepName>-starting`.
- Starts a timer.
-Executes the provided function.
• If the function returns normally, it counts as passing. If the function throws, it counts as failing.
• Ends the timer.
• Logs whether the step passed or failed
• Takes a screenshot named <stepName>-succeeded or <stepName>-failed.
• Emits the stepName SuccessPercent metric, 100 for pass or 0 for failure.
• Emits the stepName Duration metric, with a value based on the step start and end times.
• Finally, returns what the functionToExecute returned or re-throws what functionToExecute threw.

Example:

```python
def custom_actions():
    #verify contains browser.find_element_by_xpath("///[id="id_1"][contains(text(),'login')]")  
    #click a button
    browser.find_element_by_xpath('//[@id="submit"]/a').click()  
    await synthetics_webdriver.execute_step("verify_click", custom_actions)
```

**Chrome()**

Launches an instance of the Chromium browser and returns the created instance of the browser.

Example:

```python
browser = synthetics_webdriver.Chrome()  
browser.get("https://example.com/")
```

### Scheduling canary runs using cron

Using a cron expression gives you flexibility when you schedule a canary. Cron expressions contain five or six fields in the order listed in the following table. The fields are separated by spaces. The syntax differs depending on whether you are using the CloudWatch console to create the canary, or the AWS CLI or AWS SDKs. When you use the console, you specify only the first five fields. When you use the AWS CLI or AWS SDKs, you specify all six fields, and you must specify * for the Year field.

<table>
<thead>
<tr>
<th>Field</th>
<th>Allowed values</th>
<th>Allowed special characters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minutes</td>
<td>0-59</td>
<td>, - * /</td>
</tr>
<tr>
<td>Hours</td>
<td>0-23</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day-of-month</td>
<td>1-31</td>
<td>, - * ? / L W</td>
</tr>
<tr>
<td>Month</td>
<td>1-12 or JAN-DEC</td>
<td>, - * /</td>
</tr>
<tr>
<td>Day-of-week</td>
<td>1-7 or SUN-SAT</td>
<td>, - * ? L #</td>
</tr>
<tr>
<td>Year</td>
<td>*</td>
<td></td>
</tr>
</tbody>
</table>

#### Special characters

- The , (comma) includes multiple values in the expression for a field. For example, in the Month field, JAN,FEB,MAR would include January, February, and March.
• The `-` (dash) special character specifies ranges. In the Day field, `1-15` would include days 1 through 15 of the specified month.

• The `*` (asterisk) special character includes all values in the field. In the Hours field, `*` includes every hour. You cannot use `*` in both the Day-of-month and Day-of-week fields in the same expression. If you use it in one, you must use `?` in the other.

• The `/` (forward slash) specifies increments. In the Minutes field, you can enter `1/10` to specify every tenth minute, starting from the first minute of the hour (for example, the eleventh, twenty-first, and thirty-first minute, and so on).

• The `?` (question mark) specifies one or another. If you enter `7` in the Day-of-month field and you don’t care what day of the week the seventh is, you can enter `?` in the Day-of-week field.

• The `L` wildcard in the Day-of-month or Day-of-week fields specifies the last day of the month or week.

• The `W` wildcard in the Day-of-month field specifies a weekday. In the Day-of-month field, `3W` specifies the weekday closest to the third day of the month.

• The `#` wildcard in the Day-of-week field specifies a certain instance of the specified day of the week within a month. For example, `3#2` is the second Tuesday of the month. The `3` refers to Tuesday because it is the third day of each week, and the `2` refers to the second day of that type within the month.

**Limitations**

• You can’t specify the Day-of-month and Day-of-week fields in the same cron expression. If you specify a value or `*` (asterisk) in one of the fields, you must use a `?` (question mark) in the other.

• Cron expressions that lead to rates faster than one minute are not supported.

• You can’t set a canary to wait for more than a year before running, so you can specify only `*` in the `Year` field.

**Examples**

You can refer to the following sample cron strings when you create a canary. The following examples are the correct syntax for using the AWS CLI or AWS SDKs to create or update a canary. If you are using the CloudWatch console, omit the final `*` in each example.

<table>
<thead>
<tr>
<th>Expression</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>0 10 * * ? *</code></td>
<td>Run at 10:00 am (UTC) every day</td>
</tr>
<tr>
<td><code>15 12 * * ? *</code></td>
<td>Run at 12:15 am (UTC) every day</td>
</tr>
<tr>
<td><code>0 18 ? * MON-FRI</code></td>
<td>Run at 6:00 am (UTC) every Monday through Friday</td>
</tr>
<tr>
<td><code>0 8 1 * ? *</code></td>
<td>Run at 8:00 am (UTC) on the first day of each month</td>
</tr>
<tr>
<td><code>0/10 * ? * MON-SAT</code></td>
<td>Run every 10 minutes Monday through Saturday of each week</td>
</tr>
<tr>
<td><code>0/5 8-17 ? MON-FRI</code></td>
<td>Run every five minutes Monday through Friday between 8:00 am and 5:55 pm (UTC)</td>
</tr>
</tbody>
</table>

**Troubleshooting a failed canary**

If your canary fails, check the following for troubleshooting.

**General troubleshooting**
- Use the canary details page to find more information. In the CloudWatch console, choose Canaries in the navigation pane and then choose the name of the canary to open the canary details page. In the Availability tab, check the SuccessPercent metric to see whether the problem is constant or intermittent.

While still in the Availability tab, choose a failed data point to see screenshots, logs, and step reports (if available) for that failed run.

If a step report is available because steps are part of your script, check to see which step has failed and see the associated screenshots to see the issue that your customers are seeing.

You can also check the HAR files to see if one or more requests are failing. You can dig deeper by using logs to drill down on failed requests and errors. Finally, you can compare these artifacts with the artifacts from a successful canary run to pinpoint the issue.

By default, CloudWatch Synthetics captures screenshots for each step in a UI canary. However, your script might be configured to disable screenshots. During debugging, you may want to enable screenshots again. Similarly, for API canaries you might want to see HTTP request and response headers and body during debugging. For information about how to include this data in the report, see `executeHttpStep(stepName, requestOptions, [callback], [stepConfig])` (p. 182).

- If you had a recent deployment to your application, roll it back and then debug later.
- Connect to your endpoint manually to see if you can reproduce the same issue.

Topics
- Canary runtime version upgrade and downgrade issues (p. 192)
- Waiting for an element to appear (p. 193)
- Node is either not visible or not an HTMLElement for page.click() (p. 193)
- Unable to upload artifacts to S3, Exception: Unable to fetch S3 bucket location: Access Denied (p. 193)
- Canary Failed. Error: No datapoint - Canary Shows timeout error (p. 193)
- Trying to access an internal endpoint (p. 194)
- Cross-origin request sharing (CORS) issue (p. 194)
- Troubleshooting a canary on a VPC (p. 194)

Canary runtime version upgrade and downgrade issues

If you recently upgraded the canary from runtime version `syn-1.0` to a later version, it may be a cross-origin request sharing (CORS) issue. For more information, see Cross-origin request sharing (CORS) issue (p. 194).

If you recently downgraded the canary to an older runtime version, check to make sure that the CloudWatch Synthetics functions that you are using are available in the older runtime version that you downgraded to. For example, the `executeHttpStep` function is available for runtime version `syn-nodejs-2.2` and later. To check on the availability of functions, see Writing a canary script (p. 155).

Note
When you plan to upgrade or downgrade the runtime version for a canary, we recommend that you first clone the canary and update the runtime version in the cloned canary. Once you have verified that the clone with the new runtime version works, you can update the runtime version of your original canary and delete the clone.
Waiting for an element to appear

After analyzing your logs and screenshots, if you see that your script is waiting for an element to appear on screen and times out, check the relevant screenshot to see if the element appears on the page. Verify your xpath to make sure that it is correct.

For Puppeteer-related issues, check Puppeteer's GitHub page or internet forums.

Node is either not visible or not an HTMLElement for page.click()

If a node is not visible or is not an HTMLElement for page.click(), first verify the xpath that you are using to click the element. Also, if your element is at the bottom of the screen, adjust your viewport. CloudWatch Synthetics by default uses a viewport of 1920 * 1080. You can set a different viewport when you launch the browser or by using the Puppeteer function page.setViewport.

Unable to upload artifacts to S3, Exception: Unable to fetch S3 bucket location: Access Denied

This means that CloudWatch Synthetics was unable to upload screenshots, logs, or reports created for the canary because of permission issues. Make sure that canary role has the necessary permissions. For more information, see Required roles and permissions for CloudWatch canaries (p. 134).

Note

Your CloudWatch metrics might show a datapoint as Passed even when the canary has failed with this error. This is because CloudWatch Synthetics publishes the SuccessPercent metric as Passed if your script has passed.

Failure to upload artifacts does not indicate any issues with your script. Therefore, these errors fail the canary but will not trigger any alarms configured on your canary.

You can add your own execution errors by using the CloudWatch Synthetics addExecutionError function. You should only track errors as execution errors if they are not important to indicate the success or failure of your script. For more information about this function, see addExecutionError(errorMessage, ex); (p. 163).

Error: Protocol error (Runtime.callFunctionOn):
Target closed.

This error appears if there are some network requests after the page or browser is closed. You might have forgotten to wait for an asynchronous operation. After executing your script, CloudWatch Synthetics closes the browser. The execution of any asynchronous operation after the browser is closed might cause target closed error.

Canary Failed. Error: No datapoint - Canary Shows timeout error

This means that your canary run exceeded the timeout. The canary execution stopped before CloudWatch Synthetics could publish success percent CloudWatch metrics or update artifacts such as HAR files, logs and screenshots. If your timeout is too low, you can increase it.

By default, a canary timeout value is equal to its frequency. You can manually adjust the timeout value to be less than or equal to the canary frequency. If your canary frequency is low, you must increase the
frequency to increase the timeout. You can adjust both the frequency and the timeout value under **Schedule** when you create or update a canary by using the CloudWatch Synthetics console.

Canary artifacts are not available to view in the CloudWatch Synthetics console when this error happens. You can use CloudWatch Logs to see the canary's logs.

To use CloudWatch Logs to see the logs for a canary

2. In the left navigation pane, choose **Log groups**.
3. Find the log group by typing the canary name in the filter box. Log groups for canaries have the name `/aws/lambda/cwsyn-canaryName-randomId`.

Trying to access an internal endpoint

If you want your canary to access an endpoint on your internal network, we recommend that you set up CloudWatch Synthetics to use VPC. For more information, see Running a canary on a VPC (p. 200).

Cross-origin request sharing (CORS) issue

In a UI canary, if some network requests are failing with `403` or `net::ERR_FAILED`, check whether the canary has active tracing enabled and also uses the Puppeteer function `page.setExtraHTTPHeaders` to add headers. If so, the failed network requests might be caused by cross-origin request sharing (CORS) restrictions. You can confirm whether this is the case by disabling active tracing or removing the extra HTTP headers.

Why does this happen?

When active tracing is used, an extra header is added to all outgoing requests to trace the call. Modifying the request headers by adding a trace header or adding extra headers using Puppeteer's `page.setExtraHTTPHeaders` causes a CORS check for XMLHttpRequest (XHR) requests.

If you don't want to disable active tracing or remove the extra headers, you can update your web application to allow cross-origin access or you can disable web security by using the `disable-web-security` flag when you launch the Chrome browser in your script.

You can override launch parameters used by CloudWatch Synthetics and pass additional `disable-web-security` flag parameters by using the CloudWatch Synthetics launch function. For more information, see Library functions available for Node.js canary scripts (p. 162).

**Note**
You can override launch parameters used by CloudWatch Synthetics when you use runtime version `syn-nodejs-2.1` or later.

Troubleshooting a canary on a VPC

If you have issues after creating or updating a canary on a VPC, one of the following sections might help you troubleshoot the problem.

New canary in error state or canary can't be updated

If you create a canary to run on a VPC and it immediately goes into an error state, or you can't update a canary to run on a VPC, the canary’s role might not have the right permissions. To run on a VPC, a canary must have the permissions `ec2:CreateNetworkInterface`, `ec2:DescribeNetworkInterfaces`, and `ec2:DeleteNetworkInterface`. These permissions are
all contained in the AWSLambdaVPCAccessExecutionRole managed policy. For more information, see Execution Role and User Permissions.

If this issue happened when you created a canary, you must delete the canary, and create a new one. If you use the CloudWatch console to create the new canary, under Access Permissions, select Create a new role. A new role that includes all permissions required to run the canary is created.

If this issue happens when you update a canary, you can update the canary again and provide a new role that has the required permissions.

"No test result returned" error

If a canary displays a "no test result returned" error, one of the following issues might be the cause:

- If your VPC does not have internet access, you must use VPC endpoints to give the canary access to CloudWatch and Amazon S3. You must enable the DNS resolution and DNS hostname options in the VPC for these endpoint addresses to resolve correctly. For more information, see Using DNS with Your VPC.
- Canaries must run in private subnets within a VPC. To check this, open the Subnets page in the VPC console. Check the subnets that you selected when configuring the canary. If they have a path to an internet gateway (igw-), they are not private subnets.

To help you troubleshoot these issues, see the logs for the canary.

To see the log events from a canary

2. In the navigation pane, choose Log groups.
3. Choose the name of the canary's log group. The log group name starts with /aws/lambda/cwsyn-canary-name.

Sample code for canary scripts

This section contains code samples that illustrate some possible functions for CloudWatch Synthetics canary scripts.

Samples for Node.js and Puppeteer

Setting cookies

Web sites rely on cookies to provide custom functionality or track users. By setting cookies in CloudWatch Synthetics scripts, you can mimic this custom behavior and validate it.

For example, a web site might display a Login link for a revisiting user instead of a Register link.

```javascript
var synthetics = require('Synthetics');
const log = require('SyntheticsLogger');

const pageLoadBlueprint = async function () {
    let url = "http://smile.amazon.com/";
    let page = await synthetics.getPage();
}
```
// Set cookies. I found that name, value, and either url or domain are required fields.
const cookies = [
  {
    'name': 'cookie1',
    'value': 'val1',
    'url': url
  },
  {
    'name': 'cookie2',
    'value': 'val2',
    'url': url
  },
  {
    'name': 'cookie3',
    'value': 'val3',
    'url': url
  }];

await page.setCookie(...cookies);

// Navigate to the url
await synthetics.executeStep('pageLoaded_home', async function (timeoutInMillis = 30000) {

  var response = await page.goto(url, {waitUntil: ['load', 'networkidle0'], timeout: timeoutInMillis});

  // Log cookies for this page and this url
  const cookiesSet = await page.cookies(url);
  log.info("Cookies for url: " + url + " are set to: " + JSON.stringify(cookiesSet));
});

exports.handler = async () => {
  return await pageLoadBlueprint();
};

Device emulation

You can write scripts that emulate various devices so that you can approximate how a page looks and behaves on those devices.

The following sample emulates an iPhone 6 device. For more information about emulation, see page.emulate(options) in the Puppeteer documentation.

```javascript
var synthetics = require('Synthetics');
const log = require('SyntheticsLogger');
const puppeteer = require('puppeteer-core');

const pageLoadBlueprint = async function () {
  const iPhone = puppeteer.devices['iPhone 6'];

  // INSERT URL here
  const URL = "https://amazon.com";

  let page = await synthetics.getPage();
  await page.emulate(iPhone);

  // You can customize the wait condition here. For instance, // using 'networkidle2' may be less restrictive.
  const response = await page.goto(URL, {waitUntil: 'domcontentloaded', timeout: 30000});
  if (!response) {
    throw "Failed to load page!";
  }
};
```
await page.waitFor(15000);
await synthetics.takeScreenshot('loaded', 'loaded');

// If the response status code is not a 2xx success code
if (response.status() < 200 || response.status() > 299) {
  throw "Failed to load page!";
}

exports.handler = async () => {
  return await pageLoadBlueprint();
};

Multi-step API canary

This sample code demonstrates an API canary with two HTTP steps: testing the same API for positive and negative test cases. The step configuration is passed to enable reporting of request/response headers. Additionally, it hides the Authorization header and X-Amz-Security-Token, because they contain user credentials.

When this script is used as a canary, you can view details about each step and the associated HTTP requests such as step pass/fail, duration, and performance metrics like DNS look up time and first byte time. You can view the number of 2xx, 4xx and 5xx for your canary run.

var synthetics = require('Synthetics');
const log = require('SyntheticsLogger');

const apiCanaryBlueprint = async function () {

  // Handle validation for positive scenario
  const validatePositiveCase = async function(res) {
    return new Promise((resolve, reject) => {
      if (res.statusCode < 200 || res.statusCode > 299) {
        throw res.statusCode + ' ' + res.statusMessage;
      }
      let responseBody = '';
      res.on('data', (d) => {
        responseBody += d;
      });
      res.on('end', () => {
        // Add validation on 'responseBody' here if required. For ex, your status code is 200 but data might be empty
        resolve();
      });
    });
  }

  // Handle validation for negative scenario
  const validateNegativeCase = async function(res) {
    return new Promise((resolve, reject) => {
      if (res.statusCode < 400) {
        throw res.statusCode + ' ' + res.statusMessage;
      }
      resolve();
    });
  }

  // Other code...
};
let requestOptionsStep1 = {
    'hostname': 'myproductsEndpoint.com',
    'method': 'GET',
    'path': '/test/product/validProductName',
    'port': 443,
    'protocol': 'https:'
};

let headers = {};
headers['User-Agent'] = [synthetics.getCanaryUserAgentString(), headers['User-Agent']].join(' ');

requestOptionsStep1['headers'] = headers;

// By default headers, post data and response body are not included in the report for security reasons.
// Change the configuration at global level or add as step configuration for individual steps
let stepConfig = {
    includeRequestHeaders: true,
    includeResponseHeaders: true,
    includeRequestBody: true,
    includeResponseBody: true
};

await synthetics.executeHttpStep('Verify GET products API with valid name',
requestOptionsStep1, validatePositiveCase, stepConfig);

let requestOptionsStep2 = {
    'hostname': 'myproductsEndpoint.com',
    'method': 'GET',
    'path': '/test/canary/InvalidName(',
    'port': 443,
    'protocol': 'https:'
};

headers = {};
headers['User-Agent'] = [synthetics.getCanaryUserAgentString(), headers['User-Agent']].join(' ');

requestOptionsStep2['headers'] = headers;

// By default headers, post data and response body are not included in the report for security reasons.
// Change the configuration at global level or add as step configuration for individual steps
stepConfig = {
    includeRequestHeaders: true,
    includeResponseHeaders: true,
    includeRequestBody: true,
    includeResponseBody: true
};

await synthetics.executeHttpStep('Verify GET products API with invalid name',
requestOptionsStep2, validateNegativeCase, stepConfig);

});

exports.handler = async () => {
    return await apiCanaryBlueprint();
Samples for Python and Selenium

The following sample Selenium code is a canary that fails with a custom error message when a target element is not loaded.

```python
from aws_synthetics.selenium import synthetics_webdriver as webdriver
from aws_synthetics.common import synthetics_logger as logger
from selenium.webdriver.support.ui import WebDriverWait
from selenium.webdriver.support import expected_conditions as EC
from selenium.webdriver.common.by import By

def custom_selenium_script():
    # create a browser instance
    browser = webdriver.Chrome()
    browser.get('https://www.example.com/)
    logger.info('navigated to home page')
    # set cookie
    browser.add_cookie({'name': 'foo', 'value': 'bar'})
    browser.get('https://www.example.com/)
    # save screenshot
    browser.save_screenshot('signed.png')
    # expected status of an element
    button_condition = EC.element_to_be_clickable((By.CSS_SELECTOR, '.submit-button'))
    # add custom error message on failure
    WebDriverWait(browser, 5).until(button_condition, message='Submit button failed to load').click()
    logger.info('Submit button loaded successfully')

    # entry point for the canary
    def handler(event, context):
        return custom_selenium_script()
```

Canaries and X-Ray tracing

You can choose to enable active AWS X-Ray tracing on canaries that use the `syn-nodejs-2.0` or later runtime. With tracing enabled, traces are sent for all calls made by the canary that use the browser, the AWS SDK, or HTTP or HTTPS modules. Canaries with tracing enabled appear on the service map in both CloudWatch ServiceLens and in X-Ray, even when they don't send requests to other services or applications that have tracing enabled. For more information about X-Ray tracing, see Traces.

When a canary appears on a service map, it appears as a new client node type. You can hover on a canary node to see data about latency, requests, and faults. You can also choose the canary node to see more data at the bottom of the page. From this area of the page, you can choose View in Synthetics to jump to the CloudWatch Synthetics console for more details about the canary, or choose View Traces to see more details about the traces from this canary's runs.

A canary with tracing enabled also has a Tracing tab in its details page, with details about traces and segments from the canary's runs.

Enabling tracing increases canary run time by 2.5% to 7%.

A canary with tracing enabled must use a role with the following permissions. If you use the console to create the role when you create the canary, it is given these permissions.
Running a canary on a VPC

You can run canaries on endpoints on a VPC and public internal endpoints. To run a canary on a VPC, you must have both the DNS Resolution and DNS hostnames options enabled on the VPC. For more information, see Using DNS with Your VPC.

When you run a canary on a VPC endpoint, you must provide a way for it to send its metrics to CloudWatch and its artifacts to Amazon S3. If the VPC is already enabled for internet access, there's nothing more for you to do. The canary executes in your VPC, but can access the internet to upload its metrics and artifacts.

If the VPC is not already enabled for internet access, you have two options:

- Enable it for internet access. For more information, see How do I give internet access to my Lambda function in a VPC? on AWS Support.
- If you want to keep your VPC private, you can configure the canary to send its data to CloudWatch and Amazon S3 through private VPC endpoints. If you have not already done so, you must create endpoints for these services on your VPC. For more information, see Using CloudWatch and CloudWatch Synthetics with interface VPC endpoints (p. 737) and Amazon VPC Endpoints for Amazon S3.

Viewing canary statistics and details

You can view details about your canaries and see statistics about their runs.

To be able to see all the details about your canary run results, you must be logged on to an account that has sufficient permissions. For more information, see Required roles and permissions for CloudWatch canaries (p. 134).

**To view canary statistics and details**

2. In the navigation pane, choose Canaries.
   
   In the details about the canaries that you have created:

   - **Status** visually shows how many of your canaries have passed their most recent runs.
• In the graph under **Canary runs**, each point represents one minute of your canaries' runs. You can pause on a point to see details.

• Near the bottom of the page is a table displaying all canaries. A column on the right shows the alarms created for each canary. Only alarms that conform to the naming standard for canary alarms are displayed. This standard is `Synthetics-Alarm-canaryName-index`. Canary alarms that you create in the **Synthetics** section of the CloudWatch console automatically use this naming convention. If you create canary alarms in the **Alarms** section of the CloudWatch console or by using AWS CloudFormation, and you don't use this naming convention, the alarms work but they do not appear in this list.

3. To see more details about a single canary, choose a point in the **Status** graph or choose the name of the canary in the **Canaries** table.

   In the details about that canary:

   • The **Availability** tab displays information about the recent runs of this canary.

     Under **Canary runs**, you can choose one of the lines to see details about that run.

     Under the graph, you can choose **Links checked**, **Screenshot**, **HAR file**, or **Logs** to see these types of details. If the canary has active tracing enabled, you can also choose **Traces** to see tracing information from the canary's runs.

     The logs for canary runs are stored in S3 buckets and in CloudWatch Logs.

     Screenshots show how your customers view your webpages. You can use the HAR files (HTTP Archive files) to view detailed performance data about the webpages. You can analyze the list of web requests and catch performance issues such as time to load for an item. Log files show the record of interactions between the canary run and the webpage and can be used to identify details of errors.

     If the canary uses the `syn-nodejs-2.0-beta` runtime or later, you can sort the HAR files by status code, request size, or duration.

     If the canary uses the `syn-nodejs-2.0-beta` runtime or later and the canary executes steps in its script, you can choose a **Steps** tab. This tab displays a list of the canary's steps, each step's status, failure reason, URL after step execution, screenshots, and duration of step execution. For API canaries with HTTP steps, you can view steps and corresponding HTTP requests if you are using runtime `syn-nodejs-2.2` or later.

     Choose the **HTTP Requests** tab to view the log of each HTTP request made by the canary. You can view request/response headers, response body, status code, error and performance timings (total duration, TCP connection time, TLS handshake time, first byte time, and content transfer time). All HTTP requests which use the HTTP/HTTPS module under the hood are captured here.

     By default in API canaries, the request header, response header, request body, and response body are not included in the report for security reasons. If you choose to include them, the data is stored only in your S3 bucket. For information about how to include this data in the report, see `executeHttpStep(stepName, requestOptions, [callback], [stepConfig])` (p. 182).

     Response body content types of text, HTML and JSON are supported. Content types like text/html, text/plain, application/JSON and application/x-amz-json-1.0 are supported. Compressed responses are not supported.

   • The **Monitoring** tab displays graphs of the CloudWatch metrics published by this canary. For more information about these metrics, see **CloudWatch metrics published by canaries** (p. 202).

     Below the CloudWatch graphics published by the canary are graphs of Lambda metrics related to the canary's Lambda code.

   • The **Configuration** tab displays configuration and schedule information about the canary.
CloudWatch metrics published by canaries

Canaries publish the following metrics to CloudWatch in the `CloudWatchSynthetics` namespace. For more information about viewing CloudWatch metrics, see Viewing available metrics (p. 51).

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
</table>
| SuccessPercent | The percentage of the runs of this canary that succeed and find no failures.  
Valid Dimensions: CanaryName  
Valid Statistic: Average  
Units: Percent |
| Duration    | The duration in milliseconds of the canary run.  
Valid Dimensions: CanaryName  
Valid Statistic: Average  
Units: Milliseconds |
| 2xx         | The number of network requests performed by the canary that returned OK responses, with response codes between 200 and 299.  
This metric is reported for UI canaries that use runtime version `syn-nodejs-2.0` or later, and is reported for API canaries that use runtime version `syn-nodejs-2.2` or later.  
Valid Dimensions: CanaryName  
Valid Statistic: Sum  
Units: Count |
| 4xx         | The number of network requests performed by the canary that returned Error responses, with response codes between 400 and 499.  
This metric is reported for UI canaries that use runtime version `syn-nodejs-2.0` or later, and is reported for API canaries that use runtime version `syn-nodejs-2.2` or later.  
Valid Dimensions: CanaryName  
Valid Statistic: Sum  
Units: Count |
| 5xx         | The number of network requests performed by the canary that returned Fault responses, with response codes between 500 and 599.  
This metric is reported for UI canaries that use runtime version `syn-nodejs-2.0` or later, and is reported for API canaries that use runtime version `syn-nodejs-2.2` or later.  
Valid Dimensions: CanaryName |
<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed</td>
<td>The number of canary runs that failed to execute. These failures are related to the canary itself.</td>
</tr>
<tr>
<td></td>
<td>Valid Dimensions: CanaryName</td>
</tr>
<tr>
<td></td>
<td>Valid Statistic: Sum</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>Failed requests</td>
<td>The number of HTTP requests executed by the canary on the target website that failed with no response.</td>
</tr>
<tr>
<td></td>
<td>Valid Dimensions: CanaryName</td>
</tr>
<tr>
<td></td>
<td>Valid Statistic: Sum</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
<tr>
<td>VisualMonitoringSuccessPercent</td>
<td>The percentage of visual comparisons that successfully matched the baseline screenshots during a canary run.</td>
</tr>
<tr>
<td></td>
<td>Valid Dimensions: CanaryName</td>
</tr>
<tr>
<td></td>
<td>Valid Statistic: Average</td>
</tr>
<tr>
<td></td>
<td>Units: Percent</td>
</tr>
<tr>
<td>VisualMonitoringTotalComparisons</td>
<td>The total number of visual comparisons that happened during a canary run.</td>
</tr>
<tr>
<td></td>
<td>Valid Dimensions: CanaryName</td>
</tr>
<tr>
<td></td>
<td>Units: Count</td>
</tr>
</tbody>
</table>

**Note**

Canaries that use either the `executeStep()` or `executeHttpStep()` methods from the Synthetics library also publish `SuccessPercent` and `Duration` metrics with the dimensions `CanaryName` and `StepName` for each step.

---

## Editing or deleting a canary

You can edit or delete an existing canary.

**Edit canary**

When you edit a canary, even if you don’t change its schedule, the schedule is reset corresponding to when you edit the canary. For example, if you have a canary that runs every hour, and you edit that canary, the canary will run immediately after the edit is completed and then every hour after that.

**To edit or update a canary**

2. In the navigation pane, choose Canaries.
3. Select the button next to the canary name, and choose Actions, Edit.
4. (Optional) If this canary performs visual monitoring of screenshots and you want to set the next run of the canary as the baseline, select Set next run as new baseline.
5. (Optional) If this canary performs visual monitoring of screenshots and you want to remove a screenshot from visual monitoring or you want to designate parts of the screenshot to be ignored during visual comparisons, under Visual Monitoring choose Edit Baseline.

The screenshot appears, and you can do one of the following:

- To remove the screenshot from being used for visual monitoring, select Remove screenshot from visual test baseline.
- To designate parts of the screenshot to be ignored during visual comparisons, click and drag to draw areas of the screen to ignore. Once you have done this for all the areas that you want to ignore during comparisons, choose Save.

6. Make any other changes to the canary that you'd like, and choose Save.

Delete canary

When you delete a canary, resources used and created by the canary are not automatically deleted. After you delete a canary that you do not intend to use again, you should also delete the following:

- Lambda functions and layers used by this canary. Their prefix is cwsyn-MyCanaryName.
- CloudWatch alarms created for this canary. These alarms have a name that starts with Synthetics-Alarm-MyCanaryName. For more information about deleting alarms, see Editing or deleting a CloudWatch alarm (p. 119).
- Amazon S3 objects and buckets, such as the canary's results location and artifact location.
- IAM roles created for the canary. These have the name role/service-role/CloudWatchSyntheticsRole-MyCanaryName.
- Log groups in CloudWatch Logs created for the canary. These logs groups have the following names: /aws/lambda/cwsyn-MyCanaryName.

Before you delete a canary, you might want to view the canary details and make note of this information. That way, you can delete the correct resources after you delete the canary.

To delete a canary

2. In the navigation pane, choose Canaries.
3. Select the button next to the canary name, and choose Actions, Delete.
4. Enter Delete into the box and choose Delete.
5. Delete the other resources used by and created for the canary, as listed earlier in this section.

Monitoring canary events with Amazon EventBridge

Amazon EventBridge event rules can notify you when canaries change status or complete runs. EventBridge delivers a near-real-time stream of system events that describe changes in AWS resources. CloudWatch Synthetics sends these events to EventBridge on a best effort basis. Best effort delivery
means that CloudWatch Synthetics attempts to send all events to EventBridge, but in some rare cases an event might not be delivered. EventBridge processes all received events at least once. Additionally, your event listeners might not receive the events in the order that the events occurred.

**Note**

Amazon EventBridge is an event bus service that you can use to connect your applications with data from a variety of sources. For more information, see *What is Amazon EventBridge?* in the *Amazon EventBridge User Guide*.

CloudWatch Synthetics emits an event when a canary changes state or completes a run. You can create an EventBridge rule that includes an event pattern to match all event types sent from CloudWatch Synthetics, or that matches only specific event types. When a canary triggers a rule, EventBridge invokes the target actions defined in the rule. This allows you to send notifications, capture event information, and take corrective action, in response to a canary state change or the completion of a canary run. For example, you can create rules for the following use cases:

- Investigating when a canary run fails
- Investigating when a canary has gone into the **ERROR** state
- Tracking a canary's life cycle
- Monitoring canary run success or failure as part of a workflow

**Example events from CloudWatch Synthetics**

This section lists example events from CloudWatch Synthetics. For more information about event format, see *Events and Event Patterns in EventBridge*.

**Canary status change**

In this event type, the values of *current-state* and *previous-state* can be the following:

CREATING | READY | STARTING | RUNNING | UPDATING | STOPPING | STOPPED | ERROR

```json
{
  "version": "0",
  "id": "8a99ca10-1e97-2302-2d64-316c5dedf61",
  "detail-type": "Synthetics Canary Status Change",
  "source": "aws.synthetics",
  "account": "123456789012",
  "time": "2021-02-09T22:19:43Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "account-id": "123456789012",
    "canary-id": "EXAMPLE-dc5a-4f5f-96d1-989b75a94226",
    "canary-name": "events-bb-1",
    "current-state": "STOPPED",
    "previous-state": "UPDATING",
    "source-location": "NULL",
    "updated-on": 1612909161.767,
    "changed-config": {
      "executionArn": {
        "previous-value": "arn:aws:lambda:us-east-1:123456789012:function:cwsyn-events-bb-1-af3e3a05-dc5a-4f5f-96d1-989EXAMPLE:1",
        "current-value": "arn:aws:lambda:us-east-1:123456789012:function:cwsyn-events-bb-1-af3e3a05-dc5a-4f5f-96d1-989EXAMPLE:2"
      }
    }
  }
}
```
Successful canary run completed

```
{
  "version": "0",
  "id": "989EXAMPLE-f4a5-57a7-1a8f-d9cc768a1375",
  "detail-type": "Synthetics Canary TestRun Successful",
  "source": "aws.synthetics",
  "account": "123456789012",
  "time": "2021-02-09T22:24:01Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "account-id": "123456789012",
    "canary-id": "989EXAMPLE-dc5a-4f5f-96d1-989EXAMPLE",
    "canary-name": "events-bb-1",
    "canary-run-id": "c6c39152-8f6a-471c-9810-989EXAMPLE",
    "artifact-location": "cw-syn-results-123456789012/us-east-1/canary/us-east-1/events-bb-1-c6c39152-8f6a-471c-9810-989EXAMPLE/2021/02/09/22/24-21-27",
    "test-run-status": "PASSED",
    "canary-run-timeline": {
      "started": 1612909421,
      "completed": 1612909441
    },
    "message": "Test run result is generated successfully"
  }
}
```

Failed canary run completed

```
{
  "version": "0",
  "id": "2644b18f-3e67-5ebf-cdfb-bf9f91392f41",
  "detail-type": "Synthetics Canary TestRun Failure",
  "source": "aws.synthetics",
  "account": "123456789012",
  "time": "2021-02-09T22:24:27Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "account-id": "123456789012",
    "canary-id": "af3e3a05-dc5a-4f5f-96d1-9989EXAMPLE",
    "canary-name": "events-bb-1",
    "canary-run-id": "0df3823e-7e33-4dal-8194-b04e4d4a2bf6",
    "artifact-location": "cw-syn-results-123456789012/us-east-1/canary/us-east-1/events-bb-1-0df3823e-7e33-4dal-8194-b04e4d4a2bf6/2021/02/09/22/24-21-27",
    "test-run-status": "FAILED",
    "state-reason": "Error: net::ERR_NAME_NOT_RESOLVED"
  }
}
```
It's possible that events might be duplicated or out of order. To determine the order of events, use the time property.

Prerequisites for creating EventBridge rules

Before you create an EventBridge rule for CloudWatch Synthetics, you should do the following:

- Familiarize yourself with events, rules, and targets in EventBridge.
- Create and configure the targets invoked by your EventBridge rules. Rules can invoke many types of targets, including:
  - Amazon SNS topics
  - AWS Lambda functions
  - Kinesis streams
  - Amazon SQS queues

For more information, see What is Amazon EventBridge? and Getting started with Amazon EventBridge in the Amazon EventBridge User Guide.

Create an EventBridge rule (CLI)

The steps in the following example create an EventBridge rule that publishes an Amazon SNS topic when the canary named my-canary-name in us-east-1 completes a run or changes state.

1. Create the rule.

   ```bash
   aws events put-rule \
   --name TestRule \
   --region us-east-1 \
   --event-pattern "{"source": ["aws.synthetics"], "detail": {"canary-name": ["my-canary-name"]}}"
   ```

   Any properties you omit from the pattern are ignored.

2. Add the topic as a rule target.

   - Replace `topic-arn` with the Amazon Resource Name (ARN) of your Amazon SNS topic.

   ```bash
   aws events put-targets \
   --rule TestRule \
   --targets "Id"="1", "Arn"="topic-arn"
   ```

   **Note**

   To allow Amazon EventBridge to call your target topic, you must add a resource-based policy to your topic. For more information, see Amazon SNS permissions in the Amazon EventBridge User Guide.
For more information, see Events and event patterns in EventBridge in the Amazon EventBridge User Guide.
Using metric streams

You can use metric streams to continually stream CloudWatch metrics to a destination of your choice, with near-real-time delivery and low latency. Supported destinations include AWS destinations such as Amazon Simple Storage Service and several third-party service provider destinations.

There are two main usage scenarios for CloudWatch metric streams:

- **Data lake**— Create a metric stream and direct it to an Amazon Kinesis Data Firehose delivery stream that delivers your CloudWatch metrics to a data lake such as Amazon S3. This enables you to continually update monitoring data, or to combine this CloudWatch metric data with billing and performance data to create rich datasets. You can then use tools such as Amazon Athena to get insight into cost optimization, resource performance, and resource utilization.

- **Third-party providers**— Use third-party service providers to monitor, troubleshoot, and analyze your applications using the streamed CloudWatch data.

By using filtering options with metric streams, you can stream all your CloudWatch metrics, all your CloudWatch metrics except for namespaces that you choose to omit, or a narrower set of only the namespaces that you select. Each metric stream can include up to 1000 filters that either include or exclude metric namespaces. A single metric stream can have only include or exclude filters, but not both.

After a metric stream is created, if new metrics are created that match the filters in place, the new metrics are automatically included in the stream.

There is no limit on the number of metric streams per account or per Region, and no limit on the number of metric updates being streamed.

Each stream can use either JSON format or OpenTelemetry 0.7.0 format.

Metric streams pricing is based on the number of metric updates. You will also incur charges from Kinesis Data Firehose for the delivery stream used for the metric stream. For more information, see Amazon CloudWatch Pricing.

**Topics**

- Setting up a metric stream (p. 209)
- Metric stream operation and maintenance (p. 212)
- Monitoring your metric streams with CloudWatch metrics (p. 213)
- Trust between CloudWatch and Kinesis Data Firehose (p. 214)
- Metric streams output formats (p. 214)
- Troubleshooting (p. 224)

Setting up a metric stream

Use the steps in the following sections to set up a CloudWatch metric stream.

After a metric stream is created, the time it takes for metric data to appear at the destination depends on the configured buffering settings on the Kinesis Data Firehose delivery stream. The buffering is expressed in maximum payload size or maximum wait time, whichever is reached first. If these are set to the minimum values (60 seconds, 1MB) the expected latency is within 3 minutes if the selected CloudWatch namespaces have active metric updates.
In a CloudWatch metric stream, data is sent every minute. Data might arrive at the final destination out of order. All metrics in the specified namespaces are sent in the metric stream, except metrics with a timestamp that is more than two hours old.

To create and manage metric streams, you must be logged on to an account that has the CloudWatchFullAccess policy and the iam:PassRole permission, or an account that has the following list of permissions:

- iam:PassRole
- cloudwatch:PutMetricStream
- cloudwatch:DeleteMetricStream
- cloudwatch:GetMetricStream
- cloudwatch:ListMetricStreams
- cloudwatch:StartMetricStreams
- cloudwatch:StopMetricStreams

If you're going to have CloudWatch set up the IAM role needed for metric streams, you must also have the iam:CreateRole and iam:PutRolePolicy permissions.

Important
A user with the cloudwatch:PutMetricStream has access the CloudWatch metric data that is being streamed, even if they don't have the cloudwatch:GetMetricData permission.

Topics
- Setting up a metric stream to an AWS service (data lake scenario) (p. 210)
- Setting up a metric stream to a third-party solution (p. 212)

## Setting up a metric stream to an AWS service (data lake scenario)

You can use the CloudWatch console, the AWS CLI, AWS CloudFormation, or the AWS Cloud Development Kit (CDK) to set up a metric stream.

The Kinesis Data Firehose delivery stream that you use for your metric stream must be in the same account and the same Region where you set up the metric stream. To achieve cross-Region functionality, you can configure the Kinesis Data Firehose delivery stream to stream to a final destination that is in a different account or a different Region.

### CloudWatch console

This section describes how to use the CloudWatch console to set up a metric stream to another AWS service.

When you use the console to set up a metric stream, you have the option of choosing the Quick S3 Setup. This method works well if want the final output as JSON or to be queried by Amazon Athena. If you want the final format to be Parquet format or Optimized Row Columnar (ORC), you should create your own Kinesis Data Firehose delivery stream and choose Select an existing Firehose owned by your account instead of choosing Quick S3 Setup.

**To set up a metric stream to an AWS service**

2. In the navigation pane, choose Streams, Create stream.
3. Choose the CloudWatch metric namespaces to include in the metric stream.
   - To include all or most of your metric namespaces in the metric stream, choose All metrics.
     Then, if you want to exclude some metric namespaces from the stream, choose Exclude metric namespaces and select the namespaces to exclude.
   - To include only a few metric namespaces in the metric stream, choose Selected namespaces and then select the namespaces to include.

   **Note**
   Consider carefully whether to stream all metrics, because the more metrics that you stream the higher your metric stream charges will be.

4. Choose one of the following:
   - For a quick setup, choose Quick S3 setup. CloudWatch will create all necessary resources including the Kinesis Data Firehose delivery stream and the necessary IAM roles. The default format for this option is JSON, but you can change the format later in this procedure.
   - To use a Kinesis Data Firehose delivery stream that already exists, choose Select an existing Firehose owned by your account. The Kinesis Data Firehose delivery stream must be in the same account. The default format for this option is OpenTelemetry, but you can change the format later in this procedure.

   Then select the Kinesis Data Firehose delivery stream to use under Select your Kinesis Data Firehose delivery stream.

5. (Optional) If you're using Quick S3 Setup, you can choose Select existing resources to use an existing S3 bucket or existing IAM roles instead of having CloudWatch create new ones for you.

6. (Optional) If you're using Select an existing Firehose owned by your account, you can choose Select existing service role to use an existing IAM role instead of having CloudWatch create a new one for you.

7. (Optional) To change the output format from the default format for your scenario, choose Change output format. The supported formats are JSON and OpenTelemetry 0.7.0.

8. (Optional) Customize the name of the new metric stream under Metric stream name.

9. Choose Create metric stream.

**AWS CLI or AWS API**

Use the following steps to create a CloudWatch metric stream to another AWS service.

**To use the AWS CLI or AWS API to create a metric stream**

1. If you're streaming to Amazon S3, first create the bucket. For more information, see Creating a bucket.

2. Create the Kinesis Data Firehose delivery stream. For more information, see Creating an Amazon Kinesis Data Firehose Delivery Stream.

3. Create an IAM role that enables CloudWatch to write to the Kinesis Data Firehose delivery stream. For more information about the contents of this role, see Trust between CloudWatch and Kinesis Data Firehose (p. 214).

4. Use the `aws cloudwatch put-metric-stream` CLI command or the PutMetricStream API to create the CloudWatch metric stream.

**AWS CloudFormation**

You can use AWS CloudFormation to set up a metric stream. For more information, see AWS::CloudWatch::MetricStream.
To use AWS CloudFormation to create a metric stream

1. If you're streaming to Amazon S3, first create the bucket. For more information, see Creating a bucket.
2. Create the Kinesis Data Firehose delivery stream. For more information, see Creating an Amazon Kinesis Data Firehose Delivery Stream.
3. Create an IAM role that enables CloudWatch to write to the Kinesis Data Firehose delivery stream. For more information about the contents of this role, see Trust between CloudWatch and Kinesis Data Firehose (p. 214).
4. Create the stream in AWS CloudFormation. For more information, see AWS::CloudWatch::MetricStream.

AWS Cloud Development Kit (CDK)

You can use AWS Cloud Development Kit (CDK) to set up a metric stream.

To use the AWS CDK to create a metric stream

1. If you're streaming to Amazon S3, first create the bucket. For more information, see Creating a bucket.
2. Create the Kinesis Data Firehose delivery stream. For more information, see Creating an Amazon Kinesis Data Firehose Delivery Stream.
3. Create an IAM role that enables CloudWatch to write to the Kinesis Data Firehose delivery stream. For more information about the contents of this role, see Trust between CloudWatch and Kinesis Data Firehose (p. 214).
4. Create the metric stream. The metric stream resource is available in AWS CDK as a Level 1 (L1) Construct named CfnMetricStream. For more information, see Using L1 constructs.

Setting up a metric stream to a third-party solution

To set up a CloudWatch metric stream to stream metrics to a third-party solution, follow the instructions provided by that third-party provider.

Metric stream operation and maintenance

Metric streams are always in one of two states, Running or Stopped.

- **Running**— The metric stream is running correctly. There might not be any metric data streamed to the destination because of the filters on the stream.
- **Stopped**— The metric stream has been explicitly stopped by someone, and not because of an error. It might be useful to stop your stream to temporarily pause the streaming of data without deleting the stream.

If you stop and restart a metric stream, the metric data that was published to CloudWatch while the metric stream was stopped is not backfilled to the metric stream.

If you change the output format of a metric stream, in certain cases you might see a small amount of metric data written to the destination in both the old format and the new format. To avoid this situation, you can create a new Kinesis Data Firehose delivery stream with the same configuration as your current
Monitoring your metric streams

Metric streams emit CloudWatch metrics about their health and operation in the AWS/CloudWatch/MetricStreams namespace. The following metrics are emitted. Both metrics are emitted with a MetricStreamName dimension and with no dimension. You can use the metrics with no dimensions to see aggregated metrics for all of your metric streams. You can use the metrics with the MetricStreamName dimension to see the metrics about only that metric stream.

For both of these metrics, values are emitted only for metric streams that are in the Running state.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetricUpdate</td>
<td>The number metric updates sent to the metric stream. If no metric updates are streamed during a time period, a value of 0 is emitted for this metric. If you stop the metric stream, this metric stops being emitted until the metric stream is started again. Valid Statistic: Sum Units: None</td>
</tr>
<tr>
<td>PublishErrorRate</td>
<td>The number of unrecoverable errors that occur when putting data into the Kinesis Data Firehose delivery stream. If no errors occur during a time period, a value of 0 is emitted for this metric. If you stop the metric stream, this metric stops being emitted until the metric stream is started again. Valid Statistic: Average to see the rate of metric updates unable to be written. This value will be between 0.0 and 1.0. Units: None</td>
</tr>
</tbody>
</table>
Trust between CloudWatch and Kinesis Data Firehose

The Kinesis Data Firehose delivery stream must trust CloudWatch through an IAM role that has write permissions to Kinesis Data Firehose. These permissions can be limited to the single Kinesis Data Firehose delivery stream that the CloudWatch metric stream uses. The IAM role must trust the streams.metrics.cloudwatch.amazonaws.com service principal.

If you use the CloudWatch console to create a metric stream, you can have CloudWatch create the role with the correct permissions. If you use another method to create a metric stream, or you want to create the IAM role itself, it must contain the following permissions policy and trust policy.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": ["firehose:PutRecord", "firehose:PutRecordBatch"],
         "Effect": "Allow",
      }
   ]
}
```

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "Service": "streams.metrics.cloudwatch.amazonaws.com"
         },
         "Action": "sts:AssumeRole"
      }
   ]
}
```

Metric data is streamed by CloudWatch to the destination Kinesis Data Firehose delivery stream on behalf of the source that owns the metric stream resource.

Metric streams output formats

The data in a CloudWatch metric stream can be in the JSON format or the OpenTelemetry format. Currently, the version of OpenTelemetry format supported is 0.7.0.

**JSON format**

In a CloudWatch metric stream that uses the JSON format, each Kinesis Data Firehose record contains multiple JSON objects separated by a newline character (\n). Each object includes a single data point of a single metric.

The JSON format that is used is fully compatible with AWS Glue and with Amazon Athena. If you have a Kinesis Data Firehose delivery stream and an AWS Glue table formatted correctly, the format can be
automatically transformed into Parquet format or Optimized Row Columnar (ORC) format before being stored in S3. For more information about transforming the format, see Converting Your Input Record Format in Kinesis Data Firehose. For more information about the correct format for AWS Glue, see Which AWS Glue schema should I use for JSON output format? (p. 215).

In the JSON format, the valid values for `unit` are the same as for the value of `unit` in the `MetricDatum` API structure. For more information, see MetricDatum. The value for the `timestamp` field is in epoch milliseconds, such as 1616004674229.

The following is an example of the format. In this example, the JSON is formatted for easy reading, but in practice the whole format is on a single line.

```json
{
    "metric_stream_name": "MyMetricStream",
    "account_id": "1234567890",
    "region": "us-east-1",
    "namespace": "AWS/EC2",
    "metric_name": "DiskWriteOps",
    "dimensions": {
        "InstanceId": "i-123456789012"
    },
    "timestamp": 1611929698000,
    "value": {
        "count": 3.0,
        "sum": 20.0,
        "max": 18.0,
        "min": 0.0
    },
    "unit": "Seconds"
}
```

Which AWS Glue schema should I use for JSON output format?

The following is an example of a JSON representation of the `StorageDescriptor` for an AWS Glue table, which would then be used by Kinesis Data Firehose. For more information about `StorageDescriptor`, see StorageDescriptor.

```json
{
    "Columns": [
        {
            "Name": "metric_stream_name",
            "Type": "string"
        },
        {
            "Name": "account_id",
            "Type": "string"
        },
        {
            "Name": "region",
            "Type": "string"
        },
        {
            "Name": "namespace",
            "Type": "string"
        },
        {
            "Name": "metric_name",
            "Type": "string"
        },
        {
            "Name": "timestamp",
            "Type": "timestamp"
        }
    ]
}
```
The preceding example is for data written on Amazon S3 in JSON format. Replace the values in the following fields with the indicated values to store the data in Parquet format or Optimized Row Columnar (ORC) format.

- **Parquet:**
  - SerDeInfo.serializationLib: org.apache.hadoop.hive.ql.io.parquet.serde.ParquetHiveSerDe
  - parameters.classification: parquet

- **ORC:**
  - SerDeInfo.serializationLib: org.apache.hadoop.hive.ql.io.orc.OrcSerde
  - parameters.classification: orc

**OpenTelemetry 0.7.0 format**

OpenTelemetry is a collection of tools, APIs, and SDKs. You can use it to instrument, generate, collect, and export telemetry data (metrics, logs, and traces) for analysis. OpenTelemetry is part of the Cloud Native Computing Foundation. For more information, see [OpenTelemetry](#).

For information about the full OpenTelemetry 0.7.0 specification, see [v0.7.0 release](#).

**Note**

While metric streams is in general availability, the OpenTelemetry format 0.7.0 is not yet generally available. Metric streams will continue to offer OpenTelemetry format 0.7.0 even when the OpenTelemetry format version 1.0 becomes available.

A Kinesis record can contain one or more `ExportMetricsServiceRequest` OpenTelemetry data structures. Each data structure starts with a header with an `UnsignedVarInt32` indicating the record length in bytes. Each `ExportMetricsServiceRequest` may contain data from multiple metrics at once.
The following is a string representation of the message of the `ExportMetricsServiceRequest` OpenTelemetry data structure. OpenTelemetry serializes the use of the Google Protocol Buffers binary protocol, which is not human-readable.

```yaml
resource_metrics {
  resource {
    attributes {
      key: "cloud.provider"
      value {
        string_value: "aws"
      }
    }
    attributes {
      key: "cloud.account.id"
      value {
        string_value: "2345678901"
      }
    }
    attributes {
      key: "cloud.region"
      value {
        string_value: "us-east-1"
      }
    }
    attributes {
      key: "aws.exporter.arn"
      value {
        string_value: "arn:aws:cloudwatch:us-east-1:123456789012:metric-stream/MyMetricStream"
      }
    }
  }
  instrumentation_library_metrics {
    metrics {
      name: "amazonaws.com/AWS/DynamoDB/ConsumedReadCapacityUnits"
      unit: "1"
      double_summary {
        data_points {
          labels {
            key: "Namespace"
            value: "AWS/DynamoDB"
          }
          labels {
            key: "MetricName"
            value: "ConsumedReadCapacityUnits"
          }
          labels {
            key: "TableName"
            value: "MyTable"
          }
          start_time_unix_nano: 1604948400000000000
          time_unix_nano: 1604948460000000000
          count: 1
          sum: 1.0
          quantile_values {
            quantile: 0.0
            value: 1.0
          }
          quantile_values {
            quantile: 1.0
            value: 1.0
          }
        }
      }
    }
  }
```

217
key: "Namespace"
  value: "AWS/DynamoDB"
}
layers {
  key: "MetricName"
  value: "ConsumedReadCapacityUnits"
}
layers {
  key: "TableName"
  value: "MyTable"
}
start_time_unix_nano: 1604948460000000000
time_unix_nano: 1604948520000000000
count: 2
sum: 5.0
quantile_values {
  quantile: 0.0
  value: 2.0
}
quantile_values {
  quantile: 1.0
  value: 3.0
}
}

Top-level object to serialize OpenTelemetry metric data

ExportMetricsServiceRequest is the top-level wrapper to serialize an OpenTelemetry exporter payload. It contains one or more ResourceMetrics.

message ExportMetricsServiceRequest {
  // An array of ResourceMetrics.
  // For data coming from a single resource this array will typically contain one
  // element. Intermediary nodes (such as OpenTelemetry Collector) that receive
  // data from multiple origins typically batch the data before forwarding further and
  // in that case this array will contain multiple elements.
  repeated opentelemetry.proto.metrics.v1.ResourceMetrics resource_metrics = 1;
}

ResourceMetrics is the top-level object to represent MetricData objects.

// A collection of InstrumentationLibraryMetrics from a Resource.
message ResourceMetrics {
  // The resource for the metrics in this message.
  // If this field is not set then no resource info is known.
  opentelemetry.proto.resource.v1.Resource resource = 1;

  // A list of metrics that originate from a resource.
  repeated opentelemetry.proto.metrics.v1.InstrumentationLibraryMetrics instrumentation_library_metrics = 2;
}

The Resource object

A Resource object is a value-pair object that contains some information about the resource that generated the metrics. For metrics created by AWS, the data structure contains the Amazon Resource Name (ARN) of the resource related to the metric, such as an EC2 instance or an S3 bucket.

The Resource object contains an attribute called attributes, which store a list of key-value pairs.
- cloud.account.id contains the account ID
- cloud.region contains the Region
- aws.exporter.arn contains the metric stream ARN
- cloud.provider is always aws.

```protobuf
// Resource information.
message Resource {
  // Set of labels that describe the resource.
  repeated opentelemetry.proto.common.v1.KeyValue attributes = 1;

  // dropped_attributes_count is the number of dropped attributes. If the value is 0,
  // no attributes were dropped.
  uint32 dropped_attributes_count = 2;
}
```

The `InstrumentationLibraryMetrics` object

The `instrumentation_library` field will not be filled. We will fill only the metrics field that we are exporting.

```protobuf
// A collection of Metrics produced by an InstrumentationLibrary.
message InstrumentationLibraryMetrics {
  // The instrumentation library information for the metrics in this message.
  // If this field is not set then no library info is known.
  opentelemetry.proto.common.v1.InstrumentationLibrary instrumentation_library = 1;

  // A list of metrics that originate from an instrumentation library.
  repeated Metric metrics = 2;
}
```

The `Metric` object

The metric object contains a `DoubleSummary` data field that contains a list of `DoubleSummaryDataPoint`.

```protobuf
message Metric {
  // name of the metric, including its DNS name prefix. It must be unique.
  string name = 1;

  // description of the metric, which can be used in documentation.
  string description = 2;

  // unit in which the metric value is reported. Follows the format
  // described by http://unitsofmeasure.org/ucum.html.
  string unit = 3;

  oneof data {
    IntGauge int_gauge = 4;
    DoubleGauge double_gauge = 5;
    IntSum int_sum = 6;
    DoubleSum double_sum = 7;
    IntHistogram int_histogram = 8;
    DoubleHistogram double_histogram = 9;
    DoubleSummary double_summary = 11;
  }
}

message DoubleSummary {
  repeated DoubleSummaryDataPoint data_points = 1;
}
```
The MetricDescriptor object

The MetricDescriptor object contains metadata. For more information, see metrics.proto on GitHub.

For metric streams, the MetricDescriptor has the following contents:

- **name** will be `amazonaws.com/metric_namespace/metric_name`
- **description** will be blank.
- **unit** will be filled by mapping the metric datum's unit to the case-sensitive variant of the Unified code for Units of Measure. For more information, see Translations with OpenTelemetry 0.7.0 format (p. 221) and The Unified Code For Units of Measure.
- **type** will be SUMMARY.

The DoubleSummaryDataPoint object

The DoubleSummaryDataPoint object contains the value of a single data point in a time series in a DoubleSummary metric.

```protobuf
// DoubleSummaryDataPoint is a single data point in a timeseries that describes the // time-varying values of a Summary metric.
message DoubleSummaryDataPoint {
  // The set of labels that uniquely identify this timeseries.
  repeated opentelemetry.proto.common.v1.StringKeyValue labels = 1;

  // start_time_unix_nano is the last time when the aggregation value was reset // to "zero". For some metric types this is ignored, see data types for more // details.
  // The aggregation value is over the time interval [start_time_unix_nano, // time_unix_nano].
  // Value is UNIX Epoch time in nanoseconds since 00:00:00 UTC on 1 January // 1970.
  // Value of 0 indicates that the timestamp is unspecified. In that case the // timestamp may be decided by the backend.
  fixed64 start_time_unix_nano = 2;

  // time_unix_nano is the moment when this aggregation value was reported.
  // Value is UNIX Epoch time in nanoseconds since 00:00:00 UTC on 1 January // 1970.
  fixed64 time_unix_nano = 3;

  // count is the number of values in the population. Must be non-negative.
  fixed64 count = 4;

  // sum of the values in the population. If count is zero then this field // must be zero.
  double sum = 5;

  // Represents the value at a given quantile of a distribution.
  // To record Min and Max values following conventions are used:
  // - The 1.0 quantile is equivalent to the maximum value observed.
  // - The 0.0 quantile is equivalent to the minimum value observed.
}
message ValueAtQuantile {
  // The quantile of a distribution. Must be in the interval // [0.0, 1.0].
  double quantile = 1;

  // The value at the given quantile of a distribution.
}
```
For more information, see Translations with OpenTelemetry 0.7.0 format (p. 221).

Translations with OpenTelemetry 0.7.0 format

CloudWatch performs some transformations to put CloudWatch data into OpenTelemetry format.

Translating namespace, metric name, and dimensions

These attributes are key-value pairs encoded in the mapping.

- One pair contains the namespace of the metric
- One pair contains the name of the metric
- For each dimension, CloudWatch stores the following pair: `metricDatum.Dimensions[i].Name`, `metricDatum.Dimensions[i].Value`

Translating Average, Sum, SampleCount, Min and Max

The Summary datapoint enables CloudWatch to export all of these statistics using one datapoint.

- `startTimeUnixNano` contains the CloudWatch `startTime`
- `timeUnixNano` contains the CloudWatch `endTime`
- `sum` contains the Sum statistic.
- `count` contains the SampleCount statistic.
- `quantile_values` contains two `valueAtQuantile.value` objects:
  - `valueAtQuantile.quantile = 0.0` with `valueAtQuantile.value = Min value`
  - `valueAtQuantile.quantile = 1.0` with `valueAtQuantile.value = Max value`

Resources that consume the metric stream can calculate the Average statistic as **Sum/SampleCount**.

Translating units

CloudWatch units are mapped to the case-sensitive variant of the Unified code for Units of Measure, as shown in the following table. For more information, see The Unified Code For Units of Measure.

<table>
<thead>
<tr>
<th>CloudWatch</th>
<th>OpenTelemetry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Second</td>
<td>s</td>
</tr>
<tr>
<td>Second or Seconds</td>
<td>s</td>
</tr>
<tr>
<td>Microsecond</td>
<td>us</td>
</tr>
<tr>
<td>Milliseconds</td>
<td>ms</td>
</tr>
<tr>
<td>Bytes</td>
<td>By</td>
</tr>
<tr>
<td>Kilobytes</td>
<td>kBy</td>
</tr>
</tbody>
</table>
Units that are combined with a slash are mapped by applying the OpenTelemetry conversion of both the units. For example, Bytes/Second is mapped to By/s.

### How to parse OpenTelemetry 0.7.0 messages

This section provides information to help you get started with parsing OpenTelemetry 0.7.0.

First, you should get language-specific bindings, which enable you to parse OpenTelemetry 0.7.0 messages in your preferred language.

#### To get language-specific bindings

- The steps depend on your preferred language.
  - To use Java, add the following Maven dependency to your Java project: [OpenTelemetry Java]
    ```
    opentelemetry/java/jre/0.14.1.
    ```
  - To use any other language, follow these steps:
    a. Make sure that your language is supported by checking the list at [Generating Your Classes](https://www.example.com/generating-your-classes).
    b. Install the Protobuf compiler by following the steps at [Download Protocol Buffers](https://www.example.com/download-protocol-buffers).
    c. Download the OpenTelemetry 0.7.0 ProtoBuf definitions at [v0.7.0 release](https://www.example.com/v0.7.0-release).
    d. Confirm that you are in the root folder of the downloaded OpenTelemetry 0.7.0 ProtoBuf definitions, and run the command to generate language-specific bindings. For more information, see [Generating Your Classes](https://www.example.com/generating-your-classes).

    The following is an example for how to generate Javascript bindings.
    ```
    protoc --proto_path=./ --js_out=import_style=commonjs,binary:src \
    opentelemetry/proto/common/v1/common.proto \
    opentelemetry/proto/resource/v1/resource.proto \
    opentelemetry/proto/metrics/v1/metrics.proto
    ```

    The following section includes examples of using the language-specific bindings that you can build using the previous instructions.
Java

```java
package com.example;

import io.opentelemetry.proto.collector.metrics.v1.ExportMetricsServiceRequest;
import java.io.IOException;
import java.io.InputStream;
import java.util.ArrayList;
import java.util.List;

public class MyOpenTelemetryParser {

    public List<ExportMetricsServiceRequest> parse(InputStream inputStream) throws IOException {
        List<ExportMetricsServiceRequest> result = new ArrayList<>();
        ExportMetricsServiceRequest request;
        /* A Kinesis record can contain multiple `ExportMetricsServiceRequest` records, each of them starting with a header with an UnsignedVarInt32 indicating the record length in bytes:
         ------ --------------------------- ------ -----------------------
         |UINT32|ExportMetricsServiceRequest|UINT32|ExportMetricsService...
         ------ --------------------------- ------ -----------------------
        */
        while ((request = ExportMetricsServiceRequest.parseDelimitedFrom(inputStream)) != null) {
            // Do whatever we want with the parsed message
            result.add(request);
        }
        return result;
    }
}
```

Javascript

This example assumes that the root folder with the bindings generated is ./

The data argument of the function `parseRecord` can be one of the following types:

- `Uint8Array` this is optimal
- `Buffer` optimal under node
- `Array`, `number` 8-bit integers

```javascript
const pb = require('google-protobuf')
const pbMetrics = require('./opentelemetry/proto/collector/metrics/v1/metrics_service_pb')

function parseRecord(data) {
    const result = []
    // Loop until we've read all the data from the buffer
    while (data.length) {
        /* A Kinesis record can contain multiple `ExportMetricsServiceRequest` records, each of them starting with a header with an
         UnsignedVarInt32 indicating the record length in bytes:
          ------ --------------------------- ------ -----------------------
          |UINT32|ExportMetricsServiceRequest|UINT32|ExportMetricsService...
          ------ --------------------------- ------ -----------------------
        */
        const reader = new pb.BinaryReader(data)
```
const messageLength = reader.decoder_.readUnsignedVarint32()
const messageFrom = reader.decoder_.cursor_
const messageTo = messageFrom + messageLength

// Extract the current `ExportMetricsServiceRequest` message to parse
const message = data.subarray(messageFrom, messageTo)

// Parse the current message using the ProtoBuf library
const parsed = pbMetrics.ExportMetricsServiceRequest.deserializeBinary(message)

// Do whatever we want with the parsed message
result.push(parsed.toObject())

// Shrink the remaining buffer, removing the already parsed data
data = data.subarray(messageTo)
}
return result
}

**Python**

You must read the var-int delimiters yourself or use the internal methods `_VarintBytes(size)` and `_DecodeVarint32(buffer, position)`. These return the position in the buffer just after the size bytes. The read-side constructs a new buffer that is limited to reading only the bytes of the message.

```python
size = my_metric.ByteSize()
f.write(_VarintBytes(size))
f.write(my_metric.SerializeToString())
msg_len, new_pos = _DecodeVarint32(buf, 0)
msg_buf = buf[new_pos:new_pos+msg_len]
request = metrics_service_pb.ExportMetricsServiceRequest()
request.ParseFromString(msg_buf)
```

**Go**

Use `Buffer.DecodeMessage()`.

**C#**

Use `CodedInputStream`. This class can read size-delimited messages.

**C++**

The functions described in `google/protobuf/util/delimited_message_util.h` can read size-delimited messages.

**Other languages**

For other languages, see [Download Protocol Buffers](https://cloud.google.com/protocol-buffers/docs/download).

When implementing the parser, consider that a Kinesis record can contain multiple `ExportMetricsServiceRequest` Protocol Buffers messages, each of them starting with a header with an `UnsignedVarInt32` that indicates the record length in bytes.

**Troubleshooting**

If you're not seeing metric data at your final destination, check the following:
• Check that the metric stream is in the running state. For steps on how to use the CloudWatch console to do this, see Metric stream operation and maintenance (p. 212).

• Check the metrics emitted by the metric stream. In the CloudWatch console, under Metrics, look at the AWS/CloudWatch/MetricStreams namespace for the MetricUpdate and PublishErrorRate metrics.

• If the PublishErrorRate metric is high, confirm that the destination that is used by the Kinesis Data Firehose delivery stream exists and that the IAM role specified in the metric stream's configuration grants the CloudWatch service principal permissions to write to it. For more information, see Trust between CloudWatch and Kinesis Data Firehose (p. 214).

• Check that the Kinesis Data Firehose delivery stream has permission to write to the final destination.

• In the Kinesis Data Firehose console, view the Kinesis Data Firehose delivery stream that is used for the metric stream and check the Monitoring tab to see whether the Kinesis Data Firehose delivery stream is receiving data.

• Confirm that you have configured your Kinesis Data Firehose delivery stream with the correct details.

• Check any available logs or metrics for the final destination that the Kinesis Data Firehose delivery stream writes to.

• To get more detailed information, enable CloudWatch Logs error logging on the Kinesis Data Firehose delivery stream. For more information, see Monitoring Kinesis Data Firehose Using CloudWatch Logs.
Using ServiceLens to monitor the health of your applications

CloudWatch ServiceLens enhances the observability of your services and applications by enabling you to integrate traces, metrics, logs, alarms, and other resource health information into one place. ServiceLens integrates CloudWatch with AWS X-Ray to provide an end-to-end view of your application to help you more efficiently pinpoint performance bottlenecks and identify impacted users. A service map displays your service endpoints and resources as “nodes” and highlights the traffic, latency, and errors for each node and its connections. You can choose a node to see detailed insights about the correlated metrics, logs, and traces associated with that part of the service. This enables you to investigate problems and their effect on the application.

To fully take advantage of ServiceLens and correlated metrics, logs, and traces, you must update the X-Ray SDK and the instrumentation of your application. ServiceLens supports logs correlation for Lambda.
functions, API Gateway, Java-based applications running on Amazon EC2, and Java-based applications running on Amazon EKS or Kubernetes with Container Insights deployed.

ServiceLens integrates with Amazon CloudWatch Synthetics, a fully-managed service that enables you to create canaries to monitor your endpoints and APIs from the outside-in. Canaries that you create appear on the ServiceLens service map. For more information, see Using synthetic monitoring (p. 133).

ServiceLens is available in every Region where X-Ray is available.

Topics
- Deploying ServiceLens (p. 227)
- Using the service map in ServiceLens (p. 235)
- Using the traces view in ServiceLens (p. 237)
- Using the resource health view in ServiceLens (p. 237)
- ServiceLens troubleshooting (p. 239)

Deploying ServiceLens

Deploying ServiceLens requires two steps:
- Deploy AWS X-Ray so that you can view the service map.
- Deploy the CloudWatch agent and the X-Ray daemon to enable the service map integration with CloudWatch metrics and CloudWatch Logs.

Topics
- Deploying AWS X-Ray (p. 227)
- Deploying the CloudWatch agent and the X-Ray daemon (p. 229)

Deploying AWS X-Ray

You can use any AWS X-Ray SDK to enable X-Ray. However, the correlation of logs and metrics with your traces is supported only if you use the Java SDK.

To deploy X-Ray, follow the standard X-Ray setup. For more information, see the following:
- AWS X-Ray SDK for Java (supports logs correlations)
- The X-Ray SDK for Node.js
- AWS X-Ray SDK for .NET
- AWS X-Ray SDK for Go
- AWS X-Ray SDK for Python
- AWS X-Ray SDK for Ruby

After completing the X-Ray setup, follow the steps in the following sections to integrate X-Ray with CloudWatch Logs and enable segment metrics.

Topics
- Integrating with CloudWatch Logs (p. 228)
- Enabling segment metrics from X-Ray (p. 228)
Integrating with CloudWatch Logs

To enable integration with CloudWatch Logs, there are two steps:

- Enable trace to logs correlation. This is supported only using the SDK for Java.
- Configure trace ID injection.

Enabling trace to logs correlation

The SDK for Java supports both a set of standard application logging frameworks and CloudWatch Logs native support. Before completing the following steps, you must have completed a standard setup of the AWS X-Ray SDK for Java.

The supported runtimes are Amazon EC2, Amazon ECS with CloudWatch Container Insights enabled, and Lambda.

- To enable trace to logs correlation on Amazon EC2, enable the X-Ray EC2 Plugin. For more information, see Service Plugins
- To enable trace to logs correlation on Amazon EKS, first enable Container Insights if you have not already done so. For more information, see Using Container Insights (p. 262).

Then, enable the X-Ray SDK EKS Plugin. For more information, see Service Plugins.
- To enable trace to logs correlation on Lambda, you must enable X-Ray on Lambda. For more information, see AWS Lambda and AWS X-Ray.

Enabling trace ID injection

For information about how to enable trace ID injection, see Logging.

Enabling segment metrics from X-Ray

The AWS X-Ray SDK for Java can emit several metrics about segments into CloudWatch to give an unsampled view of latency, throttle, error, and fault rates. It uses the CloudWatch agent to emit these metrics to minimize the impact on application performance. For more information about segments, see Segments.

If you enable segment metrics, a log group called `XRayApplicationMetrics` is created, and the metrics `ErrorRate`, `FaultRate`, `ThrottleRate`, and `Latency`, are published into a custom CloudWatch metric namespace called `Observability`.

Segment metrics are not currently supported in Lambda.

To enable the AWS X-Ray SDK for Java to publish segment metrics, use the following example.

```java
AWSXRayRecorderBuilder builder = AWSXRayRecorderBuilder.standard().withSegmentListener(new MetricsSegmentListener());
```

If you are using ServiceLens with Amazon EKS and Container Insights, add the `AWS_XRAY_METRICS_DAEMON_ADDRESS` environment variable to the `HOST_IP` as shown in the following example.

```yaml
env:
  - name: HOST_IP
    valueFrom:
      fieldRef:
        apiVersion: v1
```
Deploying the CloudWatch agent and the X-Ray daemon

This section explains how to deploy the CloudWatch agent and the X-Ray daemon. You can deploy the agent and the daemon in the following environments:

- Amazon ECS or Fargate
- Amazon EKS or Kubernetes hosted on Amazon EC2
- Amazon EC2

The deployment steps for each of these environments are explained in the following sections.

Topics
- Deploying the CloudWatch agent and the X-Ray daemon on Amazon ECS (p. 229)
- Deploying the CloudWatch agent and the X-Ray daemon on Amazon EKS or Kubernetes (p. 233)
- Deploying the CloudWatch agent and the X-Ray daemon on Amazon EC2 (p. 235)

Deploying the CloudWatch agent and the X-Ray daemon on Amazon ECS

On Amazon ECS, you deploy the CloudWatch agent as a sidecar to your application container to collect metrics. You can configure the CloudWatch Agent through SSM parameter store.

Creating IAM roles

You must create two IAM roles. If you already have created these roles, you may need to add permissions to them.

- **ECS task role**— Containers use this role to run. The permissions should be whatever your applications need, plus CloudWatchAgentServerPolicy and AWSXRayDaemonWriteAccess.
- **ECS task definition role**— Amazon ECS uses this role to launch and execute your containers. If you have already created this role, attach the AmazonSSMReadOnlyAccess, AmazonECSTaskExecutionRolePolicy, and CloudWatchAgentServerPolicy policies to it.

If you need to store more sensitive data for Amazon ECS to use, see Specifying Sensitive Data for more information.

For more information about creating IAM roles, see Creating IAM Roles.

Store the agent configuration in SSM Parameter Store

You need to make sure your agent configuration file has the following section, and then upload it to the SSM parameter store.

```json
{
  "logs": {
    "fieldPath": status.hostIP
    - name: AWS_XRAY_METRICS_DAEMON_ADDRESS
      value: #(HOST_IP):25888
  }
}
```

For more information, see Enable X-Ray CloudWatch Metrics.
"metrics_collected": {
  "emf": {} 
}
}

To upload the agent configuration to the SSM parameter store

1. Put the agent configuration content into a local file /tmp/ecs-cwagent.json
2. Enter the following command. Replace region with the Region of your cluster.

```bash
aws ssm put-parameter \\
--name "ecs-cwagent" \\
--type "String" \\
--value "\`cat /tmp/ecs-cwagent.json`" \\
--region "region"
```

Create a task definition and launch the task

The steps for this task depend on whether you want to use the EC2 launch type or the Fargate launch type.

**EC2 launch type**

First, create the task definition. In this example, the container "demo-app" sends X-Ray SDK metrics to the CloudWatch agent and sends trace information to the X-Ray daemon.

Copy the following task definition to a local JSON file such as /tmp/ecs-cwagent-ec2.json. Replace the following placeholders:

- Replace `{{ecs-task-role}}` with the ARN of your ECS task role.
- Replace `{{ecs-task-execution-role}}` with the ARN of your ECS task execution role.
- Replace `{{demo-app-image}}` with your application image that has X-Ray SDK integration enabled. Change the name from demo-app to your own application name.
- Replace `{{region}}` with the name of the AWS Region where you want to send the logs for containers. For example, us-west-2.

```json
{
  "family": "ecs-cwagent-ec2",
  "taskRoleArn": "{{ecs-task-role}}",
  "executionRoleArn": "{{ecs-task-execution-role}}",
  "networkMode": "bridge",
  "containerDefinitions": [ 
    {
      "name": "demo-app",
      "image": "{{demo-app-image}}",
      "links": [ 
        "cloudwatch-agent",
        "xray-daemon"
      ],
      "logConfiguration": {
        "logDriver": "awslogs",
        "options": {
          "awslogs-create-group": "True",
          "awslogs-group": "/ecs/ecs-cwagent-ec2",
          "awslogs-region": "{{region}}",
          "awslogs-stream-prefix": "ecs"
        }
      }
    }
  ]
}
```
Deploying the CloudWatch agent and the X-Ray daemon

Enter the following command to create the task definition. Replace `{{region}}` with the Region of your cluster.

```
aws ecs register-task-definition \
  --cli-input-json file:///tmp/ecs-cwagent-ec2.json \
  --region {{region}}
```

Enter the following command to launch the task. Replace `{{cluster-name}}` and `{{region}}` with the name and Region of your cluster.

```
aws ecs run-task \
  --cluster {{cluster-name}} \
  --task-definition ecs-cwagent-ec2 \
  --region {{region}} \
  --launch-type EC2
```

**Fargate launch type**

First, create the task definition. In this example, the container “demo-app” sends X-Ray SDK metrics to the CloudWatch agent and sends trace information to the X-Ray daemon.
Copy the following task definition to a local JSON file such as /tmp/ecs-cwagent-ec2.json. Replace the following placeholders:

- Replace `{\{ecs-task-role\}}` with the Amazon Resource Name (ARN) of your ECS task role.
- Replace `{\{ecs-task-execution-role\}}` with the ARN of your ECS task execution role.
- Replace `{\{demo-app-image\}}` with your application image that has X-Ray SDK integration enabled. Change the name from demo-app to your own application name.
- Replace `{\{region\}}` with the name of the AWS Region where you want to send the logs for containers. For example, `us-west-2`.

```json
{
    "family": "ecs-cwagent-fargate",
    "taskRoleArn": "\{\{ecs-task-role\}\}",
    "executionRoleArn": "\{\{ecs-task-execution-role\}\}",
    "networkMode": "awsvpc",
    "containerDefinitions": [
        {
            "name": "demo-app",
            "image": "\{\{demo-app-image\}\}",
            "logConfiguration": {
                "logDriver": "awslogs",
                "options": {
                    "awslogs-create-group": "True",
                    "awslogs-group": "/ecs/ecs-cwagent-fargate",
                    "awslogs-region": "\{\{region\}\}"
                },
                "awslogs-stream-prefix": "ecs"
            }
        },
        {
            "name": "xray-daemon",
            "image": "public.ecr.aws/xray/aws-xray-daemon:latest",
            "logConfiguration": {
                "logDriver": "awslogs",
                "options": {
                    "awslogs-create-group": "True",
                    "awslogs-group": "/ecs/ecs-cwagent-fargate",
                    "awslogs-region": "\{\{region\}\}"
                },
                "awslogs-stream-prefix": "ecs"
            }
        },
        {
            "name": "cloudwatch-agent",
            "image": "public.ecr.aws/cloudwatch-agent/cloudwatch-agent:latest",
            "secrets": [
                {
                    "name": "CW_CONFIG_CONTENT",
                    "valueFrom": "ecs-cwagent"
                }],
            "logConfiguration": {
                "logDriver": "awslogs",
                "options": {
                    "awslogs-create-group": "True",
                    "awslogs-group": "/ecs/ecs-cwagent-fargate",
                    "awslogs-region": "\{\{region\}\}"
                },
                "awslogs-stream-prefix": "ecs"
            }
        }
    ]
}
```
Enter the following command to create the task definition. Replace \{\{region\}\} with the Region of your cluster.

```bash
aws ecs register-task-definition \
--cli-input-json file:///tmp/ecs-cwagent-fargate.json \
--region \{\{region\}\}
```

If you already have a Fargate cluster set up, you can use the task definition you just created to launch the task. If you do not yet have any Fargate clusters, see Configure the Service for more information about the rest of the steps to set up Fargate.

**Deploying the CloudWatch agent and the X-Ray daemon on Amazon EKS or Kubernetes**

These topics explain how to install the X-Ray daemon and the CloudWatch agent on Amazon EKS or Kubernetes.

**Deploying the X-Ray daemon on Amazon EKS or Kubernetes**

To install the CloudWatch agent and the X-Ray daemon on Amazon EKS or Kubernetes, you can use a quick setup.

**To install the CloudWatch agent and the X-Ray daemon on Amazon EKS or Kubernetes**

1. Ensure that the IAM role that is attached to the EC2 instance, or the Kubernetes worker node, has the `CloudWatchAgentServerPolicy` and `AWSXRayDaemonWriteAccess` policies attached.
2. Enter the following command:

```bash
curl https://raw.githubusercontent.com/aws-samples/amazon-cloudwatch-container-insights/master/k8s-deployment-manifest-templates/deployment-mode/daemonset/cwagent-fluentd-xray/cwagent-fluentd-xray-quickstart.yaml | sed "s/{{cluster_name}}/cluster-name/;s/{{region_name}}/region/" | kubectl apply -f -
```

**What the Quick Start does**

This section describes the quick setup of the CloudWatch agent and the X-Ray daemon.

- The quick setup specifies inbound ports and protocols. Outbound connections do not have to be explicitly opened.
- The quick setup installs the X-Ray daemon via the `kubectl apply -f` command with the following file content.

```yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  name: xray-daemon
  namespace: amazon-cloudwatch
spec:
  selector:
```
The quick setup updates the CloudWatch agent using the Docker image version/label 1.231221.0 or later, or the latest version. You can find the image at https://hub.docker.com/r/amazon/cloudwatch-agent.

To enable the X-Ray SDK to read cluster name and Region information, the quick setup updates the CloudWatch agent using the Docker image version/label 1.231221.0, or later, or the latest. You can find the image at https://hub.docker.com/r/amazon/cloudwatch-agent.

To enable the X-Ray SDK to read cluster name and Region information, the quick setup created a file with the following content, and then applied it with the `kubectl apply -f` command.

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  name: container-insights-discovery-role
  namespace: amazon-cloudwatch
rules:
- apiGroups:
  - ""
  resourceNames:
  - cluster-info
  resources:
  - configmaps
  verbs:
  - get
---

apiVersion: rbac.authorization.k8s.io/v1
kind: RoleBinding
metadata:
  name: service-users-cloudwatch-discovery-role-binding
  namespace: amazon-cloudwatch
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: container-insights-discovery-role
subjects:
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccount:amazon-cloudwatch:service-users
```
• The quick setup exposes the CloudWatch agent port that receives X-Ray SDK metrics. The default port is UDP 25888.

```
ports:
  - containerPort: 25888
    hostPort: 25888
    protocol: UDP
```

• The quick setup merges the agent configuration JSON with the X-Ray SDK metrics configuration with the following JSON.

```
{
  "logs": {
  "metrics_collected": {
    "emf": {}
  }
}
}
```

### Deploying the CloudWatch agent and the X-Ray daemon on Amazon EC2

Standard installations of the CloudWatch agent and the X-Ray daemon are sufficient to enable ServiceLens on Amazon EC2, with the addition of the following CloudWatch agent configuration section example. For more information about installing the agent, see Installing the CloudWatch agent (p. 429). For more information about the CloudWatch agent configuration file, see Manually create or edit the CloudWatch agent configuration file (p. 471).

When you configure the CloudWatch agent, include this section in your configuration file:

```
{
  "logs": {
    "metrics_collected": {
      "emf": {}
    }
  }
}
```

For more information about installing the X-Ray daemon, see X-Ray Daemon Configuration.

### Using the service map in ServiceLens

This section introduces the service map and helps you learn to navigate it.

To see a service map, you must have installed AWS X-Ray and completed the other ServiceLens deployment steps. For more information, see Deploying ServiceLens (p. 227).

You must also be signed in to an account that has the AWSXrayReadOnlyAccess managed policy, as well as permissions that enable you to view the CloudWatch console. For more information, see How AWS X-Ray Works with IAM and Using Amazon CloudWatch dashboards (p. 17).
To begin using the service map

2. In the navigation pane, choose ServiceLens, Service Map.

A service map appears. It has the following parts:

- The AWS services and your custom applications that you have enabled tracing for are shown as circles or "nodes." The size of each node indicates the relative number of traced requests that are going to that service.
- Edges, or connections between nodes, are shown as lines connecting the nodes. By default, the thickness of a line indicates the relative number of traced requests between those nodes.

You can use the dropdown menu in the top right to choose whether the number of traced requests or the average latency is used for node and edge sizing. You can also select to use constant size for all nodes and edges.
- The entry point to your nodes is shown on the left as a "Client." A "Client" represents both web server traffic and traced API operation requests.
- A node outlined partially in red, orange, or purple has issues. Some traced requests to these nodes have faults, errors, or throttling. The percentage of the color outline indicates the percentage of traced requests that are having issues.
- If a node has a triangle with an exclamation point next to it, at least one CloudWatch alarm related to that node is in alarm state.

3. By default, the data in the map is for the most recent 6-hour time window. To change the timeframe of the window, use the controls at the upper right of the screen. The time range to be shown can be up to 6 hours, and can be as much as 30 days in the past.
4. If you have enabled X-Ray groups, you can filter the map by selecting an X-ray group in the filter.
5. To view metrics for a node, choose the node. To then see more information about that node, choose View logs, View traces, or View dashboard.
6. To focus on the incoming and outgoing connections for a node, select the node and choose View connections near the top of the service map.
7. To see a pop-up displaying latency, errors, requests, and alarm summary statistics for a node, pause on that node.
8. To see latency statistics for an edge connection, pause on the line representing that edge.
9. To display alarm status for a service, along with line charts for latency, errors, and trace counts, choose that service node on the map.

For more information about this view, see the following procedures.
10. To view the service map as a table, choose List view near the top of the screen. In this view, you can filter and sort the nodes and alarms that are displayed on the map.
11. To see a dashboard with metrics for a specific node, select the node and then choose View dashboard near the bottom of the screen.

To view traces for a service or application on the service map

2. In the navigation pane, choose ServiceLens, Service Map.
3. Choose the node that represents the service or application that you want to investigate.

CloudWatch displays line charts of latency, errors, and trace counts for that service, along with a summary of alarm status.

Above those charts are options to dive down to logs and traces for the service.
4. To view traces related to the service, choose **View traces**.

The console switches to the **Traces** view, focused on the service that you are investigating. For more information, see **Using the traces view in ServiceLens** (p. 237).

---

**Using the traces view in ServiceLens**

The traces view enables you to view recent X-Ray traces in your application.

**To view traces and dive down for more information**

2. In the navigation pane, choose **ServiceLens, Traces**.
3. Under **Filter type**, you can choose different criteria to sort the traces by. As you do, CloudWatch displays the success rate and response time of the traces according to your choice. The list of traces displayed at the bottom of the page is narrowed to traces that match your filter. The first 1000 traces that match your filter are retrieved.

The values in the filter table are populated by the traces that the filter returns, and update as you refine your choices in the filter.

Use the **Custom query** option under **Filter type** to add a custom expression as a filter. Custom expressions can contain keywords, unary or binary operators, and comparison values for the keywords. Keywords can correspond to parts of a trace, such as `responsetime`, `duration`, and status codes. For more information, see **Filter Expression Syntax**.

You can focus your filter further by selecting the check box next to a row under **Traces by** and choosing **Add to filter**. The filter value from the selected row is added to the filter.

4. To see a histogram representing the response time distribution of the traces returned by the current filter, and a table displaying each individual trace, scroll to the bottom of the screen.

Choose one of the traces in the table to view detailed information about the trace.

The trace details page displays a timeline that includes each of the segments that comprise the trace. Choose a segment to view additional associated metadata, including errors where applicable. For traces where the logs can be associated, the log lines associated with the trace are displayed under the timeline.

You can then optionally view those log entries in CloudWatch Logs Insights. To do that, choose **View in CloudWatch Logs Insights** and then choose **Run query**.

Some traces do not have associated log entries.

- If you don’t see log entries for Amazon EC2 or Amazon EKS, you need to update to the latest version of the X-Ray SDK. For more information, see **Deploying AWS X-Ray** (p. 227).
- ServiceLens shows log entries for Amazon ECS only if there are 20 or fewer log groups with names that start with `/ecs/`.
- Currently, log entries for Fargate traces are not available.

---

**Using the resource health view in ServiceLens**

You can use the resource health view to automatically discover, manage, and visualize the health and performance of hosts across their applications in a single view. You can visualize the health of their hosts
by a performance dimension such as CPU or memory, and slice and dice hundreds of hosts in a single view using filters. You can filter by tags or by use cases, such as hosts in the same Auto Scaling group or hosts that use the same load balancer,

**Prerequisites**

To make sure that you get the full benefit of the resource health view, check that you have the following prerequisites.

- To see the memory utilization of your hosts and use it as a filter, you must install the CloudWatch agent on your hosts and set it up to send a memory metric to CloudWatch in the default CWAgent namespace. On Linux and macOS instances, the CloudWatch agent must send the `mem_used_percent` metric. On Windows instances, the agent must send the `Memory % Committed Bytes in Use` metric. These metrics are included if you use the wizard to create the CloudWatch agent configuration file and select any of the pre-defined sets of metrics. Metrics collected by the CloudWatch agent are billed as custom metrics. For more information, see Installing the CloudWatch agent (p. 429).

When you use the CloudWatch agent to collect these memory metrics to use with the resource health view, you must include the following section in the CloudWatch agent configuration file. This section contains the default dimension settings and is created by default, so do not change any part of this section to anything different than what is shown in the following example.

```json
"append_dimensions": {
  "ImageId": "${aws:ImageId}"
  "InstanceId": "${aws:InstanceId}"
  "InstanceType": "${aws:InstanceType}"
  "AutoScalingGroupName": "${aws:AutoScalingGroupName}"
},
```

- To view all the information available in the resource health view, you must be signed in to an account that has the following permissions. If you are signed on with fewer permissions, you can still use the resource health view but some performance data will not be visible.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "autoscaling:Describe*",
        "cloudwatch:Describe*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:Describe*",
        "sns:Get*",
        "sns:List*",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeRegions"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```
To view resource health in your account

2. In the navigation pane, choose ServiceLens, Resource Health.

   The resource health page appears, showing a square for each host in your account. Each square is colored based on the current status of that host, based on the setting for Color by. Host squares with an alarm symbol have one or more alarms currently in ALARM state.

   You can see up to 500 hosts in a single view. If you have more hosts in your account, use the filter settings in step 6 of this procedure.
3. To change what criteria is used to show each host's health, choose a setting for Color by. You can choose CPU Utilization, Memory Utilization, or Status check. Memory utilization metrics are available only for hosts that are running the CloudWatch agent and have it configured to collect memory metrics and send them to the default CWAgent namespace. For more information, see Collecting metrics and logs from Amazon EC2 instances and on-premises servers with the CloudWatch agent (p. 428).
4. To change the thresholds and the colors that are used for the health indicators in the grid, choose the gear icon above the grid.
5. To toggle whether to show alarms in the host grid, choose or clear Show alarms across all metrics.
6. To split the hosts in the map into groups, choose a grouping criteria for Group by.
7. To narrow the view to fewer hosts, choose a filter criteria for Filter by. You can filter by tags and by resource groupings such as Auto Scaling group, instance type, security group, and more.
8. To sort hosts, choose a sorting criteria for Sort by. You can sort by status check results, instance state, CPU or memory utilization, and the number of alarms that are in ALARM state.
9. To see more information about a host, choose the square that represents that host. A popup pane appears. To then dive deeper into information about that host, choose View dashboard or View on list.

ServiceLens troubleshooting

The following sections can help if you're having issues with CloudWatch ServiceLens.

I don't see all my logs

How to configure logs to appear in ServiceLens depends on the service.

- API Gateway logs appear if logging is turned on in API Gateway.
- Amazon ECS and Amazon EKS logs appear if you are using the latest versions of the X-Ray SDK and the CloudWatch agent. For more information, see Deploying ServiceLens (p. 227).
- Lambda logs appear if the request ID is in the log entry. This happens automatically for the situations listed in the following table. For other cases, where the runtime does not automatically include the trace ID, you can manually include the trace ID.

<table>
<thead>
<tr>
<th>Runtime</th>
<th>Method</th>
<th>Request ID automatically in log entry?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java</td>
<td>context.getLogger.log</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>aws-lambda-java-log4j2</td>
<td></td>
</tr>
<tr>
<td>Java</td>
<td>System.out.println</td>
<td>No</td>
</tr>
</tbody>
</table>
I don't see all my alarms on the service map

ServiceLens shows only the alert icon for a node if any alarms associated with that node are in the ALARM state.

ServiceLens associates alarms with nodes using the following logic:

- If the node represents an AWS service, then all alarms with the namespace associated with that service are associated with the node. For example, a node of type `AWS::Kinesis` is linked with all alarms that are based on metrics in the CloudWatch namespace `AWS/Kinesis`.
- If the node represents an AWS resource, then the alarms on that specific resource are linked. For example, a node of type `AWS::DynamoDB::Table` with the name "MyTable" is linked to all alarms that are based on a metric with the namespace `AWS/DynamoDB` and have the `TableName` dimension set to `MyTable`.
- If the node is of unknown type, which is identified by a dashed border around the name, then no alarms are associated with that node.

I don't see some AWS resources on the service map

For AWS resources to be traced on the service map, the AWS SDK must be captured using the X-Ray SDK. For more information about X-Ray, see What Is AWS X-Ray.

Not every AWS resource is represented by a dedicated node. Some AWS services are represented by a single node for all requests to the service. The following resource types are displayed with a node per resource:

- `AWS::DynamoDB::Table`
- `AWS::Lambda::Function`

Lambda functions are represented by two nodes— one for the Lambda Container, and one for the function. This helps to identify cold start problems with Lambda functions. Lambda container nodes are associated with alarms and dashboards in the same way as Lambda function nodes.

- `AWS::ApiGateway::Stage`
There are too many nodes on my service map

Use X-Ray groups to break your map into multiple maps. For more information, see Using Filter Expressions with Groups.
Cross-account cross-Region CloudWatch console

You can add *cross-account* functionality to your CloudWatch console. This functionality provides you with cross-account visibility to your dashboards, alarms, metrics, and automatic dashboards without having to log in and log out of different accounts.

You can then create dashboards that summarize CloudWatch data from multiple AWS accounts and multiple AWS Regions into a single dashboard. You can also create an alarm in one account that watches a metric located in a different account.

Many organizations have their AWS resources deployed in multiple accounts, to provide billing and security boundaries. In this case, we recommend that you designate one or more of your accounts as your monitoring accounts, and build your cross-account dashboards in these accounts.

Cross-account functionality is integrated with AWS Organizations, to help you efficiently build your cross-account dashboards.

**Cross-Region functionality**

Cross-Region functionality is now built in automatically. You do not need to take any extra steps to be able to display metrics from different Regions in a single account on the same graph or the same dashboard.

**Topics**

- Enabling cross-account functionality in CloudWatch (p. 242)
- (Optional) Integrate with AWS Organizations (p. 245)
- Troubleshooting your CloudWatch cross-account setup (p. 245)
- Disabling and cleaning up after using cross-account (p. 246)

Enabling cross-account functionality in CloudWatch

To set up cross-account functionality in your CloudWatch console, use the CloudWatch console to set up your sharing accounts and monitoring accounts.

**Set up a sharing account**

You must enable sharing in each account that will make data available to the monitoring account.

This will grant the read-only permissions that you choose in step 5 to all users that view a cross account dashboard in the account that you share with, if the user has corresponding permissions in the account that you share with.

**To enable your account to share CloudWatch data with other accounts**

2. In the navigation pane, choose *Settings*, then choose *Configure.*
3. Choose **Share data**.

4. For **Sharing**, choose **Specific accounts** and enter the IDs of the accounts that you want to share data with.

   Any accounts that you specify here can view your account's CloudWatch data. Specify the IDs only of accounts that you know and trust.

5. For **Permissions**, specify how to share your data with one of the following options:

   - **Provide read-only access to your CloudWatch metrics, dashboards, and alarms.** This option enables the monitoring accounts to create cross-account dashboards that include widgets that contain CloudWatch data from your account.
   - **Include CloudWatch automatic dashboards.** If you select this option, users in the monitoring account can also view the information in this account's automatic dashboards. For more information, see [Getting started with Amazon CloudWatch](p. 11).
   - **Include X-Ray read-only access for ServiceLens.** If you select this option, users in the monitoring account can also view the ServiceLens service map and X-Ray trace information in this account. For more information, see [Using ServiceLens to monitor the health of your applications](p. 226).
   - **Full read-only access to everything in your account.** This option enables the accounts that you use for sharing to create cross-account dashboards that include widgets that contain CloudWatch data from your account. It also enables those accounts to look deeper into your account and view your account's data in the consoles of other AWS services.

6. Choose **Launch CloudFormation template**.

   In the confirmation screen, type **Confirm**, and choose **Launch template**.

7. Select the **I acknowledge...** check box, and choose **Create stack**.

**Sharing with an entire organization**

Completing the preceding procedure creates an IAM role which enables your account to share data with one account. You can create or edit an IAM role that shares your data with all accounts in an organization. Do this only if you know and trust all accounts in the organization.

This will grant the read-only permissions listed in the policies shown in step 5 of the previous procedure to all users that view a cross-account dashboard in the account that you share with, if the user has corresponding permissions in the account that you share with.

**To share your CloudWatch account data with all accounts in an organization**

1. If you haven't already, complete the preceding procedure to share your data with one AWS account.
2. Sign in to the AWS Management Console and open the IAM console at [https://console.aws.amazon.com/iam/](https://console.aws.amazon.com/iam/).
3. In the navigation pane, choose **Roles**.
4. In the list of roles, choose **CloudWatch-CrossAccountSharingRole**.
5. Choose **Trust relationships**, **Edit trust relationship**.

   You see a policy like this:

   ```json
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "AWS": "arn:aws:iam::123456789012:root"
         },
       }
     ]
   }
   ```
6. Change the policy to the following, replacing `org-id` with the ID of your organization.

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Principal": {
            "AWS": "*"
         },
         "Action": "sts:AssumeRole",
         "Condition": {
            "StringEquals": {
               "aws:PrincipalOrgID": "org-id"
            }
         }
      }
   ]
}
```

7. Choose **Update Trust Policy**.

**Set up a monitoring account**

Enable each monitoring account if you want to view cross-account CloudWatch data.

When you complete the following procedure, CloudWatch creates a service-linked role that CloudWatch uses in the monitoring account to access data shared from your other accounts. This service-linked role is called **AWSServiceRoleForCloudWatchCrossAccount**. For more information, see Using service-linked roles for CloudWatch (p. 717).

**To enable your account to view cross-account CloudWatch data**

2. In the navigation pane, choose **Settings**, then in the **Cross-account cross-region** section, choose **Configure**.
3. Select **Show selector in the console** to enable an account selector to appear in the CloudWatch console when you are graphing a metric or creating an alarm.
4. Under **View cross-account cross-region**, choose one of the following options:
   - **Account Id Input**. This option prompts you to manually input an account ID each time that you want to switch accounts when you view cross-account data.
   - **AWS Organization account selector**. This option causes the accounts that you specified when you completed your cross-account integration with Organizations to appear. When you next use the console, CloudWatch displays a dropdown list of these accounts for you to select from when you are viewing cross-account data.

To do this, you must have first used your organization management account to allow CloudWatch to see a list of accounts in your organization. For more information, see (Optional) Integrate with AWS Organizations (p. 245).

   - **Custom account selector**. This option prompts you to enter a list of account IDs. When you next use the console, CloudWatch displays a dropdown list of these accounts for you to select from when you are viewing cross-account data.
You can also enter a label for each of these accounts to help you identify them when choosing accounts to view.

The account selector settings that a user makes here are retained only for that user, not for all other users in the monitoring account.

5. Choose Enable.

After you complete this setup, you can create cross-account dashboards. For more information, see Cross-account cross-Region dashboards (p. 18).

(Optional) Integrate with AWS Organizations

If you want to integrate cross-account functionality with AWS Organizations, you must make a list of all accounts in the organization available to the monitoring accounts.

To enable cross-account CloudWatch functionality to access a list of all accounts in your organization

1. Sign in to your organization's management account.
2. Open the CloudWatch console at https://console.aws.amazon.com/cloudwatch/.
3. In the navigation pane, choose Settings, then choose Configure.
4. For Grant permission to view the list of accounts in the organization, choose Specific accounts to be prompted to enter a list of account IDs. The list of accounts in your organization are shared with only the accounts that you specify here.
5. Choose Share organization account list.
6. Choose Launch CloudFormation template.

In the confirmation screen, type Confirm, and choose Launch template.

Troubleshooting your CloudWatch cross-account setup

This section contains troubleshooting tips for cross-account, console deployment in CloudWatch.

I am getting access denied errors displaying cross-account data

Check the following:

- Your monitoring account should have a role named AWSServiceRoleForCloudWatchCrossAccount. If it does not, you need to create this role. For more information, see Set Up a Monitoring Account (p. 244).
- Each sharing account should have a role named CloudWatch-CrossAccountSharingRole. If it does not, you need to create this role. For more information, see Set Up A Sharing Account (p. 242).
- The sharing role must trust the monitoring account.

To confirm that your roles are set up properly for the CloudWatch cross-account console

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Roles.
3. In the list of roles, make sure the needed role exists. In a sharing account, look for CloudWatch-CrossAccountSharingRole. In a monitoring account, look for AWSServiceRoleForCloudWatchCrossAccount.
4. If you are in a sharing account and CloudWatch-CrossAccountSharingRole already exists, choose CloudWatch-CrossAccountSharingRole.
5. Choose Trust relationships, Edit trust relationship.
6. Confirm that the policy lists either the account ID of the monitoring account, or the organization ID of an organization that contains the monitoring account.

I don't see an account dropdown in the console

First, check that you have created the correct IAM roles, as discussed in the preceding troubleshooting section. If those are set up correctly, make sure that you have enabled this account to view cross-account data, as described in Enable Your Account to View Cross-Account Data (p. 244).

Disabling and cleaning up after using cross-account

To disable cross-account functionality for CloudWatch, follow these steps.

Step 1: Remove the cross-account stacks or roles

The best method is to remove the AWS CloudFormation stacks that were used to enable cross-account functionality.

- In each of the sharing accounts, remove the CloudWatch-CrossAccountSharingRole stack.
- If you used AWS Organizations to enable cross-account functionality with all accounts in an organization, remove the CloudWatch-CrossAccountListAccountsRole stack in the organization's management account.

If you didn't use the AWS CloudFormation stacks to enable cross-account functionality, do the following:

- In each of the sharing accounts, delete the CloudWatch-CrossAccountSharingRole IAM role.
- If you used AWS Organizations to enable cross-account functionality with all accounts in an organization, delete the CloudWatch-CrossAccountSharing-ListAccountsRole IAM role in the organization's management account.

Step 2: Remove the service-linked role

In the monitoring account, delete the AWSServiceRoleForCloudWatchCrossAccount service-linked IAM role.
Using CloudWatch anomaly detection

When you enable anomaly detection for a metric, CloudWatch applies statistical and machine learning algorithms. These algorithms continuously analyze metrics of systems and applications, determine normal baselines, and surface anomalies with minimal user intervention.

The algorithms generate an anomaly detection model. The model generates a range of expected values that represent normal metric behavior.

You can use the model of expected values in two ways:

- Create anomaly detection alarms based on a metric's expected value. These types of alarms don't have a static threshold for determining alarm state. Instead, they compare the metric's value to the expected value based on the anomaly detection model.

  You can choose whether the alarm is triggered when the metric value is above the band of expected values, below the band, or both.

  For more information, see Creating a CloudWatch alarm based on anomaly detection (p. 112).

- When viewing a graph of metric data, overlay the expected values onto the graph as a band. This makes it visually clear which values in the graph are out of the normal range. For more information, see Creating a graph (p. 66).

  You can enable anomaly detection using the AWS Management Console, the AWS CLI, AWS CloudFormation, or the AWS SDK. You can enable anomaly detection on metrics vended by AWS and also on custom metrics.

  You can also retrieve the upper and lower values of the model's band by using the GetMetricData API request with the ANOMALY_DETECTION_BAND metric math function. For more information, see GetMetricData.

In a graph with anomaly detection, the expected range of values is shown as a gray band. If the metric's actual value goes beyond this band, it is shown as red during that time.

Anomaly detection algorithms account for the seasonality and trend changes of metrics. The seasonality changes could be hourly, daily, or weekly, as shown in the following examples.
The longer-range trends could be downward or upward.

Seconds

Anomaly detections also works well with metrics with flat patterns.
How CloudWatch anomaly detection works

When you enable anomaly detection for a metric, CloudWatch applies machine learning algorithms to the metric’s past data to create a model of the metric’s expected values. The model assesses both trends and hourly, daily, and weekly patterns of the metric. The algorithm trains on up to two weeks of metric data, but you can enable anomaly detection on a metric even if the metric does not have a full two weeks of data.

You specify a value for the anomaly detection threshold that CloudWatch uses along with the model to determine the “normal” range of values for the metric. A higher value for the anomaly detection threshold produces a thicker band of “normal” values.

The machine learning model is specific to a metric and a statistic. For example, if you enable anomaly detection for a metric using the AVG statistic, the model is specific to the AVG statistic.

When CloudWatch creates a model for many common metrics from AWS services, it ensures that the band doesn’t extend outside of logical values. For example, a band for a statistic that can’t be negative will never extend below zero, and a band for a percentage metric will stay between 0 and 100.

After you create a model, CloudWatch anomaly detection continually evaluates the model and makes adjustments to it to ensure that it is as accurate as possible. This includes re-training the model to adjust if the metric values evolve over time or have sudden changes, and also includes predictors to improve the models of metrics that are seasonal, spiky, or sparse.

After you enable anomaly detection on a metric, you can choose to exclude specified time periods of the metric from being used to train the model. This way, you can exclude deployments or other unusual events from being used for model training, ensuring the most accurate model is created.

Using anomaly detection models for alarms incurs charges on your AWS account. For more information, see Amazon CloudWatch Pricing.
Using Contributor Insights to analyze high-cardinality data

You can use Contributor Insights to analyze log data and create time series that display contributor data. You can see metrics about the top-N contributors, the total number of unique contributors, and their usage. This helps you find top talkers and understand who or what is impacting system performance. For example, you can find bad hosts, identify the heaviest network users, or find the URLs that generate the most errors.

You can build your rules from scratch, and when you use the AWS Management Console you can also use sample rules that AWS has created. Rules define the log fields that you want to use to define contributors, such as ipaddress. You can also filter the log data to find and analyze the behavior of individual contributors.

CloudWatch also provides built-in rules that you can use to analyze metrics from other AWS services. Currently, built-in rules are available for Amazon DynamoDB.

All rules analyze incoming data in real time.

Note
If you use Contributor Insights, you are charged for each occurrence of a log event that matches a rule. For more information, see Amazon CloudWatch Pricing.

Topics
• Creating a Contributor Insights rule (p. 250)
• Contributor Insights rule syntax (p. 253)
• Contributor Insights rule examples (p. 256)
• Viewing Contributor Insights reports (p. 258)
• Graphing metrics generated by rules (p. 259)
• Using Contributor Insights built-in rules (p. 261)

Creating a Contributor Insights rule

You can create rules to analyze log data. Any logs in JSON or Common Log Format (CLF) can be evaluated. This includes your custom logs that follow one of these formats and logs from AWS services such as Amazon VPC flow logs, Amazon Route 53 DNS query logs, Amazon ECS container logs, and logs from AWS CloudTrail, Amazon SageMaker, Amazon RDS, AWS AppSync and API Gateway.

In a rule, when you specify field names or values, all matching is case sensitive.

You can use built-in sample rules when you create a rule or you can create your own rule from scratch. Contributor Insights includes sample rules for the following types of logs:

• Amazon API Gateway logs
• Amazon Route 53 public DNS query logs
• Amazon Route 53 resolver query logs
• CloudWatch Container Insights logs
• VPC flow logs
Important
When you grant a user the `cloudwatch:PutInsightRule` permission, by default that user can create a rule that evaluates any log group in CloudWatch Logs. You can add IAM policy conditions that limit these permissions for a user to include and exclude specific log groups. For more information, see Using condition keys to limit Contributor Insights users’ access to log groups (p. 715).

To create a rule using a built-in sample rule
2. In the navigation pane, choose Contributor Insights.
3. Choose Create rule.
4. Choose Sample rule, and from Select sample rule, select the rule.
5. For Rule name, enter a name. Valid characters are A-Z, a-z, 0-9, "-", ",", and ".".
6. For Log group(s), select the log groups that you want the rule to monitor. You can select as many as 20 log groups.
   
   To select all log groups with names that start with a certain string, choose Select by prefix match and enter the prefix.
   
   If you use Select by prefix match, be aware of how many log groups will match your prefix and be analyzed by the rule. You incur charges for each log event that matches a rule. If you accidentally search more log groups than you intend, you might incur unexpected charges. For more information, see Amazon CloudWatch Pricing.
7. The sample rule has filled out the Fields, Contribution, Filters, and Aggregate on fields. You can adjust those values, if you like.
8. Choose whether to create the rule in a disabled or enabled state. If you choose to enable it, the rule immediately starts analyzing your data. You incur costs when you run enabled rules. For more information, see Amazon CloudWatch Pricing.
   
   Contributor Insights analyzes only new log events after a rule is created. A rule cannot process logs events that were previously processed by CloudWatch Logs.
9. Choose Create.

To create a rule from scratch
2. In the navigation pane, choose Contributor Insights.
3. Choose Create rule.
4. In the Create rule wizard, choose Custom rule.
5. For Rule name, enter a name. Valid characters are A-Z, a-z, 0-9, "-", ",", and ".".
6. You can finish creating the rule by using the wizard or by choosing the Syntax tab and specifying your rule syntax manually.

   To continue using the wizard, do the following:
   
   a. For Log group(s), select the log groups that you want the rule to monitor. You can select as many as 20 log groups.

   To select all log groups with names that start with a certain string, choose Select by prefix match and enter that prefix.

   251
If you use **Select by prefix match**, be aware of how many log groups will match your prefix and be analyzed by the rule. You incur charges for each log event that matches a rule. If you accidentally search more log groups than you intend, you might incur unexpected charges. For more information, see Amazon CloudWatch Pricing.

b. For **Log format**, choose **JSON** or **CLF**.

c. For **Contribution, Key**, enter a contributor type that you want to report on. The report displays the top-N values for this contributor type.

Valid entries are any log field that has values. Examples include **requestId**, **sourceIPAddress**, and **containerID**.

For information about finding the log field names for the logs in a certain log group, see Finding Log Fields (p. 253).

Keys larger than 1 KB are truncated to 1KB.

d. (Optional) Add more values for **Contribution, Key**. You can include as many as four keys in a rule. If you enter more than one key, the contributors in the report are defined by unique value combinations of the keys. For example, if you specify three keys, each unique combination of values for the three keys is counted as a unique contributor.

e. (Optional) If you want to rank contributors by the value of a numerical log field, instead of by number of occurrences in log events, use the **Contribution, Value** field. Enter the name of a numerical log field that you want to sum to determine contributor ranking. For example, if you want to find the source IP addresses that are sending the most bytes over the network, you would add **bytes** as the value, assuming that **bytes** is the correct keyword for that field in the log events.

f. If you want to filter the results to a narrower scope, choose **Add filter**. For **Match**, enter the log field that you want to filter by. For **Condition**, choose the comparison operator and enter a value that you want to filter this field for. You can use * as a wildcard in the value.

For example, if you want to analyze only the log events in an Apache log that contain errors, for **Match**, you would specify **RESPONSE_CODE**, for **Condition**, you would specify **EqualTo**, and then you would enter 5** as the value to filter for.

You can add as many as 10 filters in a rule. Multiple filters are joined by AND logic, so only log events that match all filters are evaluated.

g. For **Aggregate on**, choose **Count** or **Sum**. Choosing **Count** causes the contributor ranking to be based on the number of occurrences. Choosing **Sum** causes the ranking to be based on the aggregated sum of the values of the field that you specify for **Contribution, Value**.

7. To enter your rule as a JSON object instead of using the wizard, do the following:

a. Choose the **Syntax** tab.

b. In **Rule body**, enter the JSON object for your rule. For information about rule syntax, see Contributor Insights rule syntax (p. 253).

8. Choose whether to create the rule in a disabled or enabled state. If you choose to enable it, the rule immediately starts analyzing your data. You incur costs when you run enabled rules. For more information, see Amazon CloudWatch Pricing.

Contributor Insights analyzes only new log events after a rule is created. A rule cannot process logs events that were previously processed by CloudWatch Logs.

9. Choose **Create**.

You can disable, enable, or delete rules that you have created.
To enable, disable, or delete a rule in Contributor Insights

2. In the navigation pane, choose **Contributor Insights**.
3. In the list of rules, select the check box next to a single rule.
   - Built-in rules are created by AWS services and can’t be edited, disabled, or deleted.
4. Choose **Actions**, and then choose the option you want.

Finding log fields

When you create a rule, you need to know the names of fields in the log entries in a log group.

**To find the log fields in a log group**

2. In the navigation pane, under **Logs**, choose **Insights**.
3. Above the query editor, select one or more log groups to query.
   - When you select a log group, CloudWatch Logs Insights automatically detects fields in the data in the log group and displays them in the right pane in **Discovered fields**.

Contributor Insights rule syntax

This section explains the syntax for Contributor Insights rules. Use this syntax only when you are creating a rule by entering a JSON block. If you use the wizard to create a rule, you don’t need to know the syntax. For more information about creating rules using the wizard, see Creating a Contributor Insights rule (p. 250).

All matching of rules to log event field names and values is case sensitive.

The following example illustrates the syntax for JSON logs.

```json
{
  "Schema": {
    "Name": "CloudWatchLogRule",
    "Version": 1
  },
  "LogGroupNames": [
    "API-Gateway-Access-Logs*",
    "Log-group-name2"
  ],
  "LogFormat": "JSON",
  "Contribution": {
    "Keys": [
      "$.ip"
    ],
    "ValueOf": "$.requestBytes",
    "Filters": [
      {
        "Match": "$.httpMethod",
        "In": [
          "PUT"
        ]
      }
    ]
  }
}
```
"AggregateOn": "Sum"
}

Fields in Contributor Insights rules

Schema

The value of Schema for a rule that analyzes CloudWatch Logs data must always be {"Name": "CloudWatchLogRule", "Version": 1}

LogGroupNames

An array of strings. For each element in the array, you can optionally use * at the end of a string to include all log groups with names that start with that prefix.

Be careful about using wildcards with log group names. You incur charges or each log event that matches a rule. If you accidentally search more log groups than you intend, you might incur unexpected charges. For more information, see Amazon CloudWatch Pricing.

LogFormat

Valid values are JSON and CLF.

Contribution

This object includes a Keys array with as many as four members, optionally a single ValueOf, and optionally an array of as many as four Filters.

Keys

An array of up to four log fields that are used as dimensions to classify contributors. If you enter more than one key, each unique combination of values for the keys is counted as a unique contributor. The fields must be specified using JSON property format notation.

ValueOf

(Optional) Specify this only when you are specifying sum as the value of AggregateOn. ValueOf specifies a log field with numerical values. In this type of rule, the contributors are ranked by their sum of the value of this field, instead of their number of occurrences in the log entries. For example, if you want to sort contributors by their total BytesSent over a period, you would set ValueOf to BytesSent and specify Sum for AggregateOn.

Filters

(Optional) Specifies an array of as many as four filters to narrow the log events that are included in the report. If you specify multiple filters, Contributor Insights evaluates them with a logical AND operator. You can use this to filter out irrelevant log events in your search or you can use it to select a single contributor to analyze their behavior.

Each member in the array must include a Match field and a field indicating the type of matching operator to use.

The Match field specifies a log field to evaluate in the filter. The log field is specified using JSON property format notation.

The matching operator field must be one of the following: In, NotIn, StartsWith, GreaterThan, LessThan, EqualTo, NotEqualTo, or IsPresent. If the operator field is In, NotIn, or StartsWith, it is followed by an array of string values to check for. Contributor Insights evaluates the array of string values with an OR operator. The array can include as many as 10 string values.

If the operator field is GreaterThan, LessThan, EqualTo, or NotEqualTo, it is followed by a single numerical value to compare with.

If the operator field is IsPresent, it is followed by either true or false. This operator matches log events based on whether the specified log field is present in the log event. The IsPresent works
Amazon CloudWatch User Guide
Contributor Insights rule syntax

only with values in the leaf node of JSON properties. For example, a ﬁlter that looks for matches to
c-count does not evaluate a log event with a value of details.c-count.c1.
See the following for ﬁlter examples:
{"Match":
{"Match":
{"Match":
{"Match":

"$.httpMethod", "In": [ "PUT", ] }
"$.StatusCode", "EqualTo": 200 }
"$.BytesReceived", "GreaterThan": 10000}
"$.eventSource", "StartsWith": [ "ec2", "ecs" ] }

AggregateOn
Valid values are Count and Sum. Speciﬁes whether to aggregate the report based on a count of
occurrences or a sum of the values of the ﬁeld that is speciﬁed in the ValueOf ﬁeld.
JSON property format notation
The Keys, ValueOf, and Match ﬁelds follow JSON property format with dot notation, where $
represents the root of the JSON object. This is followed by a period and then an alphanumeric string with
the name of the subproperty. Multiple property levels are supported.
The following list illustrates valid examples of JSON property format:
$.userAgent
$.endpoints[0]
$.users[1].name
$.requestParameters.instanceId

Additional ﬁeld in rules for CLF logs
Common Log Format (CLF) log events do not have names for the ﬁelds like JSON does. To provide the
ﬁelds to use for Contributor Insights rules, a CLF log event can be treated as array with an index starting
from 1. You can specify the ﬁrst ﬁeld as "1", the second ﬁeld as "2", and so on.
To make a rule for a CLF log easier to read, you can use Fields. This enables you to provide a naming
alias for CLF ﬁeld locations. For example, you can specify that the location "4" is an IP address. Once
speciﬁed, IpAddress can be used as property in the Keys, ValueOf, and Filters in the rule.
The following is an example of a rule for a CLF log that uses the Fields ﬁeld.
{

"Schema": {
"Name": "CloudWatchLogRule",
"Version": 1
},
"LogGroupNames": [
"API-Gateway-Access-Logs*"
],
"LogFormat": "CLF",
"Fields": {
"4": "IpAddress",
"7": "StatusCode"
},
"Contribution": {
"Keys": [
"IpAddress"
],
"Filters": [
{
"Match": "StatusCode",
"EqualTo": 200

255


Contribution Insights rule examples

This section contains examples that illustrate use cases for Contributor Insights rules.

VPC Flow Logs: Byte transfers by source and destination IP address

```json
{
    "Schema": {
        "Name": "CloudWatchLogRule",
        "Version": 1
    },
    "LogGroupNames": [
        "/aws/containerinsights/sample-cluster-name/flowlogs"
    ],
    "LogFormat": "CLF",
    "Fields": {
        "4": "srcaddr",
        "5": "dstaddr",
        "10": "bytes"
    },
    "Contribution": {
        "Keys": ["srcaddr", "dstaddr"],
        "ValueOf": "bytes",
        "Filters": []
    },
    "AggregateOn": "Sum"
}
```

VPC Flow Logs: Highest number of HTTPS requests

```json
{
    "Schema": {
        "Name": "CloudWatchLogRule",
        "Version": 1
    },
    "LogGroupNames": [
        "/aws/containerinsights/sample-cluster-name/flowlogs"
    ],
    "LogFormat": "CLF",
    "Fields": {
        "5": "destination address",
        "7": "destination port",
        "9": "packet count"
    },
    "Contribution": {
        "Keys": ["destination address"],
        "ValueOf": "packet count",
        "Filters": [
            {
                "Match": "destination port",
            }
        ]
    }
}
```
Example rules

"EqualTo": 443
]
},
"AggregateOn": "Sum"
}

VPC Flow Logs: Rejected TCP connections

{
  "Schema": {
    "Name": "CloudWatchLogRule",
    "Version": 1
  },
  "LogGroupNames": [
    "/aws/containerinsights/sample-cluster-name/flowlogs"
  ],
  "LogFormat": "CLF",
  "Fields": {
    "3": "interfaceID",
    "4": "sourceAddress",
    "8": "protocol",
    "13": "action"
  },
  "Contribution": {
    "Keys": [
      "interfaceID",
      "sourceAddress"
    ],
    "Filters": [
      {
        "Match": "protocol",
        "EqualTo": 6
      },
      {
        "Match": "action",
        "In": [
          "REJECT"
        ]
      }
    ],
    "AggregateOn": "Sum"
  }
}

Route 53 NXDomain responses by source address

{
  "Schema": {
    "Name": "CloudWatchLogRule",
    "Version": 1
  },
  "AggregateOn": "Count",
  "Contribution": {
    "Filters": [
      {
        "Match": "$rcode",
        "StartsWith": [
          "NXDOMAIN"
        ]
      }
    ],
    "Keys": [
      "sourceAddress"
    ]
  }
}

257
Viewing Contributor Insights reports

To view graphs of report data and a ranked list of contributors found by your rules, follow these steps.

To view your rule reports

2. In the navigation pane, choose Contributor Insights.
3. In the list of rules, choose the name of a rule.

The graph displays the results of the rule over the last three hours. The table under the graph shows the top 10 contributors.

4. To change the number of contributors shown in the table, choose **Top 10 contributors** at the top of the graph.

5. To filter the graph to show only the results from a single contributor, choose that contributor in the table legend. To again show all contributors, choose that same contributor again in the legend.

6. To change the time range shown in the report, choose **15m, 30m, 1h, 2h, 3h, or custom** at the top of the graph.

The maximum time range for the report is 24 hours, but you can choose a 24-hour window that occurred up to 15 days ago. To choose a time window in the past, choose **custom, absolute**, and then specify your time window.

7. To change the length of the time period used for the aggregation and ranking of contributors, choose **period** at the top of the graph. Viewing a longer time period generally shows a smoother report with few spikes. Choosing a shorter time period is more likely to display spikes.

8. To add this graph to a CloudWatch dashboard, choose **Add to dashboard**.

9. To open the CloudWatch Logs Insights query window, with the log groups in this report already loaded in the query box, choose **View logs**.

10. To export the report data to your clipboard or a CSV file, choose **Export**.

**Graphing metrics generated by rules**

Contributor Insights provides a metric math function, **INSIGHT_RULE_METRIC**. You can use this function to add data from a Contributor Insights report to a graph in the **Metrics** tab of the CloudWatch console. You can also set an alarm based on this math function. For more information about metric math functions, see [Using metric math](p. 77)

To use this metric math function, you must be signed in to an account that has both the `cloudwatch:GetMetricData` and `cloudwatch:GetInsightRuleReport` permissions.

The syntax is `INSIGHT_RULE_METRIC(ruleName, metricName)`. `ruleName` is the name of a Contributor Insights rule. `metricName` is one of the values in the following list. The value of `metricName` determines which type of data the math function returns.

- **UniqueContributors** — the number of unique contributors for each data point.
- **MaxContributorValue** — the value of the top contributor for each data point. The identity of the contributor might change for each data point in the graph.

If this rule aggregates by **Count**, the top contributor for each data point is the contributor with the most occurrences in that period. If the rule aggregates by **Sum**, the top contributor is the contributor with the greatest sum in the log field specified by the rule’s **Value** during that period.

- **SampleCount** — the number of data points matched by the rule.
- **Sum** — the sum of the values from all contributors during the time period represented by that data point.
- **Minimum** — the minimum value from a single observation during the time period represented by that data point.
- **Maximum** — the maximum value from a single observation during the time period represented by that data point.
- **Average** — the average value from all contributors during the time period represented by that data point.
Setting an alarm on Contributor Insights metric data

You can set alarms on metrics generated by Contributor Insights by using \texttt{INSIGHT\_RULE\_METRIC}. For example, you can create an alarm based on the percentage of TCP connections that have been rejected. First, create two rules like the following:

```
{
    "Schema": {
        "Name": "CloudWatchLogRule",
        "Version": 1
    },
    "LogGroupNames": [
        "/aws/containerinsights/sample-cluster-name/flowlogs"
    ],
    "LogFormat": "CLF",
    "Fields": {
        "3": "interfaceID",
        "4": "sourceAddress",
        "8": "protocol",
        "13": "action"
    },
    "Contribution": {
        "Keys": [
            "interfaceID",
            "sourceAddress"
        ],
        "Filters": [
            {
                "Match": "protocol",
                "EqualTo": 6
            },
            {
                "Match": "action",
                "In": [
                    "REJECT"
                ]
            }
        ],
        "AggregateOn": "Sum"
    }
}
```

```
{
    "Schema": {
        "Name": "CloudWatchLogRule",
        "Version": 1
    },
    "LogGroupNames": [
        "/aws/containerinsights/sample-cluster-name/flowlogs"
    ],
    "LogFormat": "CLF",
    "Fields": {
        "3": "interfaceID",
        "4": "sourceAddress",
        "8": "protocol",
        "13": "action"
    },
    "Contribution": {
        "Keys": [
            "interfaceID",
            "sourceAddress"
        ],
        "Filters": [
```
Using Contributor Insights built-in rules

Other AWS services create built-in Contributor Insights rules that evaluate metrics from those AWS services. Currently, Amazon DynamoDB supports built-in rules.

For more information, see Contributor Insights for Amazon DynamoDB.
Using Container Insights

Use CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices. Container Insights is available for Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), and Kubernetes platforms on Amazon EC2. Amazon ECS support includes support for Fargate.

CloudWatch automatically collects metrics for many resources, such as CPU, memory, disk, and network. Container Insights also provides diagnostic information, such as container restart failures, to help you isolate issues and resolve them quickly. You can also set CloudWatch alarms on metrics that Container Insights collects.

Container Insights collects data as performance log events using embedded metric format (p. 668). These performance log events are entries that use a structured JSON schema that enables high-cardinality data to be ingested and stored at scale. From this data, CloudWatch creates aggregated metrics at the cluster, node, pod, task, and service level as CloudWatch metrics. The metrics that Container Insights collects are available in CloudWatch automatic dashboards, and also viewable in the Metrics section of the CloudWatch console.

CloudWatch does not automatically create all possible metrics from the log data, to help you manage your Container Insights costs. However, you can view additional metrics and additional levels of granularity by using CloudWatch Logs Insights to analyze the raw performance log events.

Metrics collected by Container Insights are charged as custom metrics. For more information about CloudWatch pricing, see Amazon CloudWatch Pricing.

In Amazon EKS and Kubernetes, Container Insights uses a containerized version of the CloudWatch agent to discover all of the running containers in a cluster. It then collects performance data at every layer of the performance stack.

Container Insights supports encryption with the customer master key (CMK) for the logs and metrics that it collects. To enable this encryption, you must manually enable KMS encryption for the log group that receives Container Insights data. This results in Container Insights encrypting this data using the provided CMK. Only symmetric CMKs are supported. Do not use asymmetric CMKs to encrypt your log groups.

For more information, see Encrypt Log Data in CloudWatch Logs Using AWS KMS.

Supported platforms

Container Insights is available for Amazon Elastic Container Service, Amazon Elastic Kubernetes Service, and Kubernetes platforms on Amazon EC2 instances.

- For Amazon ECS, Container Insights collects metrics at the cluster, task and service levels on both Linux and Windows Server instances. It can collect metrics at the instance-level only on Linux instances.

  For Amazon ECS, network metrics are available only for containers in bridge network mode. They are not available for containers in awsvpc network mode or host network mode.

- For Amazon Elastic Kubernetes Service, and Kubernetes platforms on Amazon EC2 instances, Container Insights is supported only on Linux instances.

- Currently, Container Insights isn't supported in AWS Batch.
CloudWatch agent container image

Amazon provides a CloudWatch agent container image on Amazon Elastic Container Registry. For more information, see cloudwatch-agent on Amazon ECR.

Supported Regions

Container Insights for Amazon ECS is supported in the following Regions:

- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)
- Africa (Cape Town)
- Asia Pacific (Mumbai)
- Asia Pacific (Hong Kong)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Tokyo)
- Asia Pacific (Sydney)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- Middle East (Bahrain)
- South America (São Paulo)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)
- China (Beijing)
- China (Ningxia)

Supported Regions for Amazon EKS and Kubernetes

Container Insights for Amazon EKS and Kubernetes is supported in the following Regions:

- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Hong Kong)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
Setting up Container Insights

The Container Insights setup process is different for Amazon ECS and Amazon EKS and Kubernetes.

Topics
- Setting up Container Insights on Amazon ECS (p. 264)
- Setting up Container Insights on Amazon EKS and Kubernetes (p. 275)

Setting up Container Insights on Amazon ECS

You can use one or both of the following options to enable Container Insights on Amazon ECS clusters:

- Use the AWS Management Console or the AWS CLI to start collecting cluster-level, task-level, and service-level metrics.
- Deploy the CloudWatch agent as a DaemonSet to start collecting instance-level metrics on clusters that are hosted on Amazon EC2 instances.

Topics
- Setting up Container Insights on Amazon ECS for cluster- and service-level metrics (p. 264)
- Setting up Container Insights on Amazon ECS using AWS Distro for OpenTelemetry (p. 266)
- Deploying the CloudWatch agent to collect EC2 instance-level metrics on Amazon ECS (p. 268)
- Set up Firelens to send logs to CloudWatch Logs (p. 274)

Setting up Container Insights on Amazon ECS for cluster- and service-level metrics

You can enable Container Insights on new and existing Amazon ECS clusters. Container Insights collects metrics at the cluster, task, and service levels. For existing clusters, you use the AWS CLI. For new clusters, use either the Amazon ECS console or the AWS CLI.

If you’re using Amazon ECS on an Amazon EC2 instance, and you want to collect network and storage metrics from Container Insights, launch that instance using an AMI that includes Amazon ECS agent version 1.29. For information about updating your agent version, see Updating the Amazon ECS Container Agent
You can use the AWS CLI to set account-level permission to enable Container Insights for any new Amazon ECS clusters created in your account. To do so, enter the following command.

```
aws ecs put-account-setting --name "containerInsights" --value "enabled"
```

### Setting up Container Insights on existing Amazon ECS clusters

To enable Container Insights on an existing Amazon ECS cluster, enter the following command. You must be running version 1.16.200 or later of the AWS CLI for the following command to work.

```
aws ecs update-cluster-settings --cluster myCICluster --settings name=containerInsights,value=enabled
```

### Setting up Container Insights on new Amazon ECS clusters

There are two ways to enable Container Insights on new Amazon ECS clusters. You can configure Amazon ECS so that all new clusters are enabled for Container Insights by default. Otherwise, you can enable a new cluster when you create it.

#### Using the AWS Management Console

You can enable Container Insights on all new clusters by default, or on an individual cluster as you create it.

**To enable Container Insights on all new clusters by default**

1. Open the Amazon ECS console at [https://console.aws.amazon.com/ecs/](https://console.aws.amazon.com/ecs/).
2. In the navigation pane, choose **Account Settings**.
3. Select the check box at the bottom of the page to enable the Container Insights default.

If you haven't used the preceding procedure to enable Container Insights on all new clusters by default, use the following steps to create a cluster with Container Insights enabled.

**To create a cluster with Container Insights enabled**

1. Open the Amazon ECS console at [https://console.aws.amazon.com/ecs/](https://console.aws.amazon.com/ecs/).
2. In the navigation pane, choose **Clusters**.
3. Choose **Create cluster**.
4. On the next page, do the following:
   a. Name your cluster.
   b. If you don't have a VPC already, select the check box to create one. You can use the default values for the VPC.
   c. Fill out all other needed information, including instance type.
   d. Select **Enabled Container Insights**.
   e. Choose **Create**.

You can now create task definitions, run tasks, and launch services in the cluster. For more information, see the following:

- Creating a task definition
- Running tasks
Creating a service

Setting up Container Insights on new Amazon ECS clusters using the AWS CLI

To enable Container Insights on all new clusters by default, enter the following command.

```
aws ecs put-account-setting --name "containerInsights" --value "enabled"
```

If you didn't use the preceding command to enable Container Insights on all new clusters by default, enter the following command to create a new cluster with Container Insights enabled. You must be running version 1.16.200 or later of the AWS CLI for the following command to work.

```
aws ecs create-cluster --cluster-name myCICluster --settings "name=containerInsights,value=enabled"
```

Disabling Container Insights on Amazon ECS clusters

To disable Container Insights on an existing Amazon ECS cluster, enter the following command.

```
aws ecs update-cluster-settings --cluster myCICluster --settings name=containerInsights,value=disabled
```

Setting up Container Insights on Amazon ECS using AWS Distro for OpenTelemetry

Use this section if you want to use AWS Distro for OpenTelemetry to set up CloudWatch Container Insights on an Amazon ECS cluster. For more information about AWS Distro for Open Telemetry, see AWS Distro for OpenTelemetry.

These steps assume that you already have a cluster running Amazon ECS. For more information about using AWS Distro for OpenTelemetry with Amazon ECS and setting up an Amazon ECS cluster for this purpose, see Setting up AWS Distro for OpenTelemetry Collector in Amazon Elastic Container Service.

Step 1: Create a task role

The first step is creating a task role in the cluster that the AWS OpenTelemetry Collector will use.

To create a task role for AWS Distro for OpenTelemetry

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Policies and then choose Create policy.
3. Choose the JSON tab and copy in the following policy:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:DescribeLogStreams",
                "logs:DescribeLogGroups",
                "ssm:GetParameters"
            ],
            "Resource": "*"
        }
    ]
}
```
Step 2: Create a task execution role

The next step is creating a task execution role for the AWS OpenTelemetry Collector.

**To create a task execution role for AWS Distro for OpenTelemetry**

1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the left navigation pane, choose Roles and then choose Create role.
3. In the list of services, choose Elastic Container Service.
4. Lower on the page, choose Elastic Container Service Task and then choose Next: Permissions.
5. In the list of policies, search for AWSDistroOpenTelemetryPolicy and then select the check box next to AWSDistroOpenTelemetryPolicy.
6. Choose Next: Tags and then choose Next: Review.
7. For Role name enter AWSOpenTelemetryTaskRole and then choose Create role.

Step 3: Create a task definition

The next step is creating a task definition.

**To create a task definition for AWS Distro for OpenTelemetry**

1. Open the Amazon ECS console at https://console.aws.amazon.com/ecs/.
2. In the left navigation pane, choose Task Definitions and then choose Create new Task Definition.
3. Select either FARGATE or EC2 and then choose Next step.
4. Enter a task definition name such as aws-otel.
5. For Task Role, select AWSOpenTelemetryTaskRole which you created earlier.
6. For Task execution role, select AWSOpenTelemetryTaskExecutionRole which you created earlier.
7. Fill in the Task memory and Task CPU.
8. Under Container Definitions, choose Add container.
10. Under **ENVIRONMENT**, for **Command** enter `--config=/etc/ecs/container-insights/otel-task-metrics-config.yaml`

   This YAML file is included in the Docker image, and includes the configuration to consume container metrics.

11. If you're using the EC2 launch type, enter a port mapping of 55680 for TCP.

12. Finish the steps for adding the container.

For more information about using the AWS OpenTelemetry collector with Amazon ECS, see Setting up AWS Distro for OpenTelemetry Collector in Amazon Elastic Container Service.

**Step 4: Run the task**

The final step is running the task that you've created.

**To run the task for AWS Distro for OpenTelemetry**

1. Open the Amazon ECS console at https://console.aws.amazon.com/ecs/.
2. In the left navigation pane, choose **Task Definitions** and then select the task that you just created.
3. Choose **Actions, Run Task**.

   Next, you can check for the new metrics in the CloudWatch console.
5. In the left navigation pane, choose **Metrics**.

   You should see a **ECS/ContainerInsights** namespace. Choose that namespace and you should see eight metrics.

**Deploying the CloudWatch agent to collect EC2 instance-level metrics on Amazon ECS**

To deploy the CloudWatch agent to collect instance-level metrics from Amazon ECS clusters that are hosted on EC2 instance, use a quick start setup with a default configuration, or install the agent manually to be able to customize it.

Both methods require that you already have at least one Amazon ECS cluster deployed with an EC2 launch type. These methods also assume that you have the AWS CLI installed. Additionally, to run the commands in the following procedures, you must be logged on to an account or role that has the IAMFullAccess and AmazonECS_FullAccess policies.

**Topics**
- Quick setup using AWS CloudFormation (p. 268)
- Manual and custom setup (p. 270)

**Quick setup using AWS CloudFormation**

To use the quick setup, enter the following command to use AWS CloudFormation to install the agent. Replace `cluster-name` and `cluster-region` with the name and Region of your Amazon ECS cluster.

This command creates the IAM roles **CWAgentECSTaskRole** and **CWAgentECSExecutionRole**. If these roles already exist in your account, use `ParameterKey=CreateIAMRoles,ParameterValue=False` instead of `ParameterKey=CreateIAMRoles,ParameterValue=True` when you enter the command. Otherwise, the command will fail.
Note

The following setup step pulls the container image from Docker Hub as an anonymous user by default. This pull may be subject to a rate limit. For more information, see CloudWatch agent container image (p. 263).

```bash
ClusterName=cluster-name
Region=cluster-region
  --parameters ParameterKey=ClusterName,ParameterValue=#{ClusterName} \
  ParameterKey=CreateIAMRoles,ParameterValue=True \
  --capabilities CAPABILITY_NAMED_IAM \
  --region #{Region}
```

(Alternative) Using your own IAM roles

If you want to use your own custom ECS task role and ECS task execution role instead of the CWAgentECSTaskRole and CWAgentECSExecutionRole roles, first make sure that the role to be used as the ECS task role has CloudWatchAgentServerPolicy attached. Also, make sure that the role to be used as the ECS task execution role has both the CloudWatchAgentServerPolicy and AmazonECSTaskExecutionRolePolicy policies attached. Then enter the following command. In the command, replace task-role-arn with the ARN of your custom ECS task role, and replace execution-role-arn with the ARN of your custom ECS task execution role.

```bash
ClusterName=cluster-name
Region=cluster-region
TaskRoleArn=task-role-arn
ExecutionRoleArn=execution-role-arn
  --parameters ParameterKey=ClusterName,ParameterValue=#{ClusterName} \
  ParameterKey=TaskRoleArn,ParameterValue=#{TaskRoleArn} \
  ParameterKey=ExecutionRoleArn,ParameterValue=#{ExecutionRoleArn} \
  --capabilities CAPABILITY_NAMED_IAM \
  --region #{Region}
```

Troubleshooting the quick setup

To check the status of the AWS CloudFormation stack, enter the following command.

```bash
ClusterName=cluster-name
Region=cluster-region
aws cloudformation describe-stacks --stack-name CWAgentECS-#{ClusterName}-${Region} --region #{Region}
```

If you see the StackStatus is other than CREATE_COMPLETE or CREATE_IN_PROGRESS, check the stack events to find the error. Enter the following command.

```bash
ClusterName=cluster-name
Region=cluster-region
aws cloudformation describe-stack-events --stack-name CWAgentECS-#{ClusterName}-${Region} --region #{Region}
```
To check the status of the `cwagent` daemon service, enter the following command. In the output, you should see that the `runningCount` is equal to the `desiredCount` in the deployment section. If it isn’t equal, check the `failures` section in the output.

```
ClusterName=cluster-name
Region=cluster-region
aws ecs describe-services --services cwagent-daemon-service --cluster $ClusterName --region $Region
```

You can also use the CloudWatch Logs console to check the agent log. Look for the `/ecs/ecs-cwagent-daemon-service` log group.

**Deleting the AWS CloudFormation stack for the CloudWatch agent**

If you need to delete the AWS CloudFormation stack, enter the following command.

```
ClusterName=cluster-name
Region=cluster-region
aws cloudformation delete-stack --stack-name CWAgentECS-${ClusterName}-${Region} --region ${Region}
```

**Manual and custom setup**

Follow the steps in this section to manually deploy the CloudWatch agent to collect instance-level metrics from your Amazon ECS clusters that are hosted on EC2 instances.

**Necessary IAM roles and policies**

Two IAM roles are required. You must create them if they don’t already exist. For more information about these roles, see Amazon ECS Task Role and Amazon ECS Task Execution Role.

- An **ECS task role**, which is used by the CloudWatch agent to publish metrics. If this role already exists, you must make sure it has the `CloudWatchAgentServerPolicy` policy attached.
- An **ECS task execution role**, which is used by Amazon ECS agent to launch the CloudWatch agent. If this role already exists, you must make sure it has the `AmazonECSTaskExecutionRolePolicy` and `CloudWatchAgentServerPolicy` policies attached.

If you do not already have these roles, you can use the following commands to create them and attach the necessary policies. This first command creates the ECS task role.

```
aws iam create-role --role-name CWAgentECSTaskRole \
  --assume-role-policy-document "{"Version": "2012-10-17","Statement": [{"Sid": ","Effect": "Allow","Principal": {"Service": "ecs-tasks.amazonaws.com"}, "Action": "sts:AssumeRole"}]}"
```

After you enter the previous command, note the value of `Arn` from the command output as `TaskRoleArn`. You’ll need to use it later when you create the task definition. Then enter the following command to attach the necessary policies.

```
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy \
  --role-name CWAgentECSTaskRole
```

This next command creates the ECS task execution role.

```
aws iam create-role --role-name CWAgentECSExecutionRole \
  --assume-role-policy-document "{"Version": "2012-10-17","Statement": [{"Sid": ","Effect": "Allow","Principal": {"Service": "ecs-tasks.amazonaws.com"}, "Action": "sts:AssumeRole"}]}"
```
After you enter the previous command, note the value of Arn from the command output as "ExecutionRoleArn". You'll need to use it later when you create the task definition. Then enter the following commands to attach the necessary policies.

```bash
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy
   --role-name CWAgentECSExecutionRole
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/service-role/AmazonECSTaskExecutionRolePolicy
   --role-name CWAgentECSExecutionRole
```

Create the task definition and launch the daemon service

Create a task definition and use it to launch the CloudWatch agent as a daemon service. To create the task definition, enter the following command. In the first lines, replace the placeholders with the actual values for your deployment. `logs-region` is the Region where CloudWatch Logs is located, and `cluster-region` is the Region where your cluster is located. `task-role-arn` is the Arn of the ECS task role that you are using, and `execution-role-arn` is the Arn of the ECS task execution role.

```bash
TaskRoleArn=task-role-arn
ExecutionRoleArn=execution-role-arn
AWSLogsRegion=logs-region
Region=cluster-region
   | sed "s|\{{task-role-arn}\}|${TaskRoleArn}|;s|\{{execution-role-arn}\}|${ExecutionRoleArn}|;s|\{{awslogs-region}\}|${AWSLogsRegion}|" 
   | xargs -0 aws ecs register-task-definition --region ${Region} --cli-input-json
```

Then run the following command to launch the daemon service. Replace `cluster-name` and `cluster-region` with the name and Region of your Amazon ECS cluster.

```bash
ClusterName=cluster-name
Region=cluster-region
aws ecs create-service 
   --cluster ${ClusterName} 
   --service-name cwagent-daemon-service 
   --task-definition ecs-cwagent-daemon-service 
   --scheduling-strategy DAEMON 
   --region ${Region}
```

If you see this error message, An error occurred (InvalidParameterException) when calling the CreateService operation: Creation of service was not idempotent, you have already created a daemon service named cwagent-daemon-service. You must delete that service first, using the following command as an example.

```bash
ClusterName=cluster-name
Region=cluster-region
aws ecs delete-service 
   --cluster ${ClusterName} 
   --service cwagent-daemon-service 
   --region ${Region} 
   --force
```
(Optional) Advanced configuration

Optionally, you can use SSM to specify other configuration options for the CloudWatch agent in your Amazon ECS clusters that are hosted on EC2 instances. These options are as follows:

- **metrics_collection_interval** – How often in seconds that the CloudWatch agent collects metrics. The default is 60. The range is 1–172,000.
- **endpoint_override** – (Optional) Specifies a different endpoint to send logs to. You might want to do this if you're publishing from a cluster in a VPC and you want the logs data to go to a VPC endpoint.

The value of endpoint_override must be a string that is a URL.

- **force_flush_interval** – Specifies in seconds the maximum amount of time that logs remain in the memory buffer before being sent to the server. No matter the setting for this field, if the size of the logs in the buffer reaches 1 MB, the logs are immediately sent to the server. The default value is 5 seconds.
- **region** – By default, the agent publishes metrics to the same Region where the Amazon ECS container instance is located. To override this, you can specify a different Region here. For example, "region" : "us-east-1"

The following is an example of a customized configuration:

```json
{
   "agent": {
      "region": "us-east-1"
   },
   "logs": {
      "metrics_collected": {
         "ecs": {
            "metrics_collection_interval": 30
         }
      },
      "force_flush_interval": 5
   }
}
```

To customize your CloudWatch agent configuration in your Amazon ECS containers

1. Make sure that the `AmazonSSMReadOnlyAccess` policy is attached to your Amazon ECS Task Execution role. You can enter the following command to do so. This example assumes that your Amazon ECS Task Execution role is CWAgentECSExecutionRole. If you are using a different role, substitute that role name in the following command.

   ```bash
   aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess --role-name CWAgentECSExecutionRole
   
   272
   ```

2. Create the customized configuration file similar to the preceding example. Name this file `/tmp/ecs-cwagent-daemon-config.json`.

3. Run the following command to put this configuration into the Parameter Store. Replace `cluster-region` with the Region of your Amazon ECS cluster. To run this command, you must be logged on to a user or role that has the `AmazonSSMFullAccess` policy.

   ```bash
   Region=cluster-region
   aws ssm put-parameter \ 
   --name "ecs-cwagent-daemon-service" \ 
   --type "String" \ 
   --value "cat /tmp/ecs-cwagent-daemon-config.json"
   ```
4. Download the task definition file to a local file, such as /tmp/cwagent-ecs-instance-metric.json

```
```

5. Modify the task definition file. Remove the following section:

```
"environment": [
    {
      "name": "USE_DEFAULT_CONFIG",
      "value": "True"
    }
  ],
```

Replace that section with the following:

```
"secrets": [
  {
    "name": "CW_CONFIG_CONTENT",
    "valueFrom": "ecs-cwagent-daemon-service"
  }
],
```

6. Restart the agent as a daemon service by following these steps:

   a. Run the following command.

```
TaskRoleArn=task-role-arn
ExecutionRoleArn=execution-role-arn
AWSLogsRegion=logs-region
Region=cluster-region
cat /tmp/cwagent-ecs-instance-metric.json \
  | sed "s|{{task-role-arn}}|${TaskRoleArn}|;s|{{execution-role-arn}}|" \ 
  | sed "s|{{awslogs-region}}|${AWSLogsRegion}|" | xargs -0 aws ecs register-task-definition --region ${Region} --cli-input-json
```

   b. Run the following command to launch the daemon service. Replace `cluster-name` and `cluster-region` with the name and Region of your Amazon ECS cluster.

```
ClusterName=cluster-name
Region=cluster-region
aws ecs create-service \
  --cluster ${ClusterName} \ 
  --service-name cwagent-daemon-service \ 
  --task-definition ecs-cwagent-daemon-service \ 
  --scheduling-strategy DAEMON \ 
  --region ${Region}
```

If you see this error message, an error occurred (InvalidParameterException) when calling the CreateService operation: Creation of service was not idempotent, you have already created a daemon service named cwagent-daemon-service. You must delete that service first, using the following command as an example.

```
ClusterName=cluster-name
Region=Region
```
Set up Firelens to send logs to CloudWatch Logs

FireLens for Amazon ECS enables you to use task definition parameters to route logs to Amazon CloudWatch Logs for log storage and analytics. FireLens works with Fluent Bit and Fluentd. We provide an AWS for Fluent Bit image, or you can use your own Fluent Bit or Fluentd image. Creating Amazon ECS task definitions with a FireLens configuration is supported using the AWS SDKs, AWS CLI, and AWS Management Console. For more information about CloudWatch Logs, see What is CloudWatch Logs?

There are key considerations when using FireLens for Amazon ECS. For more information, see Considerations.

To find the AWS for Fluent Bit images, see Using the AWS for Fluent Bit image.

To create a task definition that uses a FireLens configuration, see Creating a task definition that uses a FireLens configuration.

Example

The following task definition example demonstrates how to specify a log configuration that forwards logs to a CloudWatch Logs log group. For more information, see What Is Amazon CloudWatch Logs? in the Amazon CloudWatch Logs User Guide.

In the log configuration options, specify the log group name and the Region it exists in. To have Fluent Bit create the log group on your behalf, specify "auto_create_group": "true". You can also specify the task ID as the log stream prefix, which assists in filtering. For more information, see Fluent Bit Plugin for CloudWatch Logs.

```json
{
  "family": "firelens-example-cloudwatch",
  "taskRoleArn": "arn:aws:iam::123456789012:role/ecs_task_iam_role",
  "containerDefinitions": [
    {
      "essential": true,
      "image": "906394416424.dkr.ecr.us-west-2.amazonaws.com/aws-for-fluent-bit:latest",
      "name": "log_router",
      "firelensConfiguration": {
        "type": "fluentbit"
      },
      "logConfiguration": {
        "logDriver": "awslogs",
        "options": {
          "awslogs-group": "firelens-container",
          "awslogs-region": "us-west-2",
          "awslogs-create-group": "true",
          "awslogs-stream-prefix": "firelens"
        }
      },
      "memoryReservation": 50
    },
    {
      "essential": true,
      "image": "nginx",
      "name": "app",
      "logConfiguration": {
        "logDriver": "awslogs",
        "options": {
          "awslogs-group": "firelens-container",
          "awslogs-region": "us-west-2",
          "awslogs-create-group": "true",
          "awslogs-stream-prefix": "firelens"
        }
      }
    }
  ]
}
```
Setting up Container Insights on Amazon EKS and Kubernetes

The overall process for setting up Container Insights on Amazon EKS or Kubernetes is as follows:

1. Verify that you have the necessary prerequisites.
2. Set up the CloudWatch agent or the AWS Distro for OpenTelemetry as a DaemonSet on your cluster to send metrics to CloudWatch.
   
   Set up Fluent Bit or FluentD to send logs to CloudWatch Logs.
   
   You can perform these steps at once as part of the quick start setup if you are using the CloudWatch agent, or do them separately.
3. (Optional) Set up Amazon EKS control plane logging.
4. (Optional) Set up the CloudWatch agent as a StatsD endpoint on the cluster to send StatsD metrics to CloudWatch.

Topics

- Verify prerequisites (p. 275)
- Using the CloudWatch agent (p. 277)
- Using AWS Distro for OpenTelemetry (p. 282)
- Send logs to CloudWatch Logs (p. 283)
- Updating or deleting Container Insights on Amazon EKS and Kubernetes (p. 294)

Verify prerequisites

Before you install Container Insights on Amazon EKS or Kubernetes, verify the following. These prerequisites apply whether you are using the CloudWatch agent or AWS Distro for OpenTelemetry to set up Container Insights on Amazon EKS clusters.

- You have a functional Amazon EKS or Kubernetes cluster with nodes attached in one of the Regions that supports the Container Insights for Amazon EKS and Kubernetes. For the list of supported Regions, see Using Container Insights (p. 262).
- You have `kubectl` installed and running. For more information, see Installing `kubectl` in the Amazon EKS User Guide.
• If you're using Kubernetes running on AWS instead of using Amazon EKS, the following prerequisites are also necessary:
  • Be sure that your Kubernetes cluster has enabled role-based access control (RBAC). For more information, see Using RBAC Authorization in the Kubernetes Reference.
  • Your kubelet has enabled Webhook authorization mode. For more information, see Kubelet authentication/authorization in the Kubernetes Reference.
  • Your container runtime is Docker.

You must also grant IAM permissions to enable your Amazon EKS worker nodes to send metrics and logs to CloudWatch. There are two ways to do this:

• Attach a policy to the IAM role of your worker nodes. This works for both Amazon EKS clusters and other Kubernetes clusters.
• Use an IAM role for service accounts for the cluster, and attach the policy to this role. This works only for Amazon EKS clusters.

The first option grants permissions to CloudWatch for the entire node, while using an IAM role for the service account gives CloudWatch access to only the appropriate daemonset pods.

**Attaching a policy to the IAM role of your worker nodes**

Follow these steps to attach the policy to the IAM role of your worker nodes. This works for both Amazon EKS clusters and Kubernetes clusters outside of Amazon EKS.

**To attach the necessary policy to the IAM role for your worker nodes**

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. Select one of the worker node instances and choose the IAM role in the description.
3. On the IAM role page, choose **Attach policies**.
4. In the list of policies, select the check box next to **CloudWatchAgentServerPolicy**. If necessary, use the search box to find this policy.
5. Choose **Attach policies**.

If you're running a Kubernetes cluster outside Amazon EKS, you might not already have an IAM role attached to your worker nodes. If not, you must first attach an IAM role to the instance and then add the policy as explained in the previous steps. For more information on attaching a role to an instance, see Attaching an IAM Role to an Instance in the Amazon EC2 User Guide for Windows Instances.

If you're running a Kubernetes cluster outside Amazon EKS and you want to collect EBS volume IDs in the metrics, you must add another policy to the IAM role attached to the instance. Add the following as an inline policy. For more information, see Adding and Removing IAM Identity Permissions in the IAM User Guide.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeVolumes"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```
Using an IAM service account role

This method works only on Amazon EKS clusters.

**To grant permission to CloudWatch using an IAM service account role**

1. If you haven't already, enable IAM roles for service accounts on your cluster. For more information, see [Enabling IAM roles for service accounts on your cluster](#).
2. If you haven't already, create the IAM role for your service account. For more information, see [Creating an IAM role and policy for your service account](#).

   When you create the role, attach the **CloudWatchAgentServerPolicy** IAM policy to the role in addition to the policy that you create for the role.
3. If you haven't already, associate the IAM role with a service account in your cluster. For more information, see [Specifying an IAM role for your service account](#).

**Using the CloudWatch agent**

Use the instructions in these sections to set up Container Insights on an Amazon EKS cluster by using the CloudWatch agent.

**Topics**

- Quick Start setup for Container Insights on Amazon EKS and Kubernetes (p. 277)
- Set up the CloudWatch agent to collect cluster metrics (p. 279)

**Quick Start setup for Container Insights on Amazon EKS and Kubernetes**

To complete the setup of Container Insights, you can follow the quick start instructions in this section.

**Important**

Before completing the steps in this section, you must have verified the prerequisites including IAM permissions. For more information, see [Verify prerequisites](#).

Alternatively, you can instead follow the instructions in the following two sections, **Set up the CloudWatch agent to collect cluster metrics** (p. 279) and **Send logs to CloudWatch Logs** (p. 283). Those sections provide more configuration details on how the CloudWatch agent works with Amazon EKS and Kubernetes, but require you to perform more installation steps.

**Note**

Amazon has now launched Fluent Bit as the default log solution for Container Insights with significant performance gains. We recommend that you use Fluent Bit instead of Fluentd.

**Quick Start with the CloudWatch agent and Fluent Bit**

There are two configurations for Fluent Bit: an optimized version and a version that provides an experience more similar to FluentD. The Quick Start configuration uses the optimized version. For more details about the FluentD-compatible configuration, see [Set up Fluent Bit as a DaemonSet to send logs to CloudWatch Logs](#).

To deploy Container Insights using the quick start, enter the following command.

**Note**

The following setup step pulls the container image from Docker Hub as an anonymous user by default. This pull may be subject to a rate limit. For more information, see [CloudWatch agent container image](#).

---

277
In this command, `my-cluster-name` is the name of your Amazon EKS or Kubernetes cluster, and `my-cluster-region` is the name of the Region where the logs are published. We recommend that you use the same Region where your cluster is deployed to reduce the AWS outbound data transfer costs.

For example, to deploy Container Insights on the cluster named `MyCluster` and publish the logs and metrics to US West (Oregon), enter the following command.

```bash
ClusterName='MyCluster'
LogRegion='us-west-2'
FluentBitHttpPort='2020'
FluentBitReadFromHead='Off'
[ [ #{$FluentBitReadFromHead} = 'On' ] ] && FluentBitReadFromTail='Off'||
FluentBitReadFromTail='On'
[ [ -z #{$FluentBitHttpPort} ] ] && FluentBitHttpServer='Off' || FluentBitHttpServer='On'
curl https://raw.githubusercontent.com/aws-samples/amazon-cloudwatch-container-insights/latest/k8s-deployment-manifest-templates/deployment-mode/daemonset/container-insights-monitoring/quickstart/cwagent-fluent-bit-quickstart.yaml | sed 's/{{cluster_name}}/'${ClusterName}'/;s/{{region_name}}/'${LogRegion}'/;s/{{http_server_toggle}}/'$FluentBitHttpServer'/;s/{{http_server_port}}/'$FluentBitHttpPort'/;s/{{read_from_head}}/'$FluentBitReadFromHead'/;s/{{read_from_tail}}/'$FluentBitReadFromTail'/' | kubectl apply -f -
```

Migrating from Fluentd

If you already have Fluentd configured and want to move to Fluent Bit, you must delete the FluentD pods after you install Fluent Bit. You can use the following command to delete FluentD.

```bash
kubectl delete configmap cluster-info -n amazon-cloudwatch
```

Deleting Container Insights

If you want to remove Container Insights after using the quick start setup, enter the following command.

```bash
curl https://raw.githubusercontent.com/aws-samples/amazon-cloudwatch-container-insights/latest/k8s-deployment-manifest-templates/deployment-mode/daemonset/container-insights-monitoring/quickstart/cwagent-fluent-bit-quickstart.yaml | sed 's/{{cluster_name}}/'${ClusterName}'/;s/{{region_name}}/'${LogRegion}'/;s/{{http_server_toggle}}/'$FluentBitHttpServer'/;s/{{http_server_port}}/'$FluentBitHttpPort'/;s/
```

```bash
```
### Quick Start with the CloudWatch agent and Fluentd

If you are already using Fluentd in your Kubernetes cluster and want to extend it to be the log solution for Container Insights, we provide a FluentD configuration for you to do so.

To deploy the CloudWatch agent and Fluentd using the quick start, use the following command. The following setup contains a community supported FluentD container image. You can replace the image with your own FluentD image as long as it meets the FluentD image requirements. For more information, see (Optional) Set up FluentD as a DaemonSet to send logs to CloudWatch Logs (p. 289).

```
curl https://raw.githubusercontent.com/aws-samples/amazon-cloudwatch-container-insights/latest/kubernetes-deployment-manifest-templates/deployment-mode/daemonset/container-insights-monitoring/quickstart/cwagent-fluentd-quickstart.yaml | sed "s/\{{cluster_name}\}/cluster-name/;s/\{{region_name}\}/cluster-region/" | kubectl apply -f -
```

In this command, `cluster-name` is the name of your Amazon EKS or Kubernetes cluster, and `cluster-region` is the name of the Region where the logs are published. We recommend that you use the same Region where your cluster is deployed to reduce the AWS outbound data transfer costs.

For example, to deploy Container Insights on the cluster named `MyCluster` and publish the logs and metrics to US West (Oregon), enter the following command.

```
```

### Deleting Container Insights

If you want to remove Container Insights after using the quick start setup, enter the following command.

```
curl https://raw.githubusercontent.com/aws-samples/amazon-cloudwatch-container-insights/latest/kubernetes-deployment-manifest-templates/deployment-mode/daemonset/container-insights-monitoring/quickstart/cwagent-fluentd-quickstart.yaml | sed "s/\{{cluster_name}\}/cluster-name/;s/\{{region_name}\}/cluster-region/" | kubectl delete -f -
```

### Set up the CloudWatch agent to collect cluster metrics

To set up Container Insights to collect metrics, you can follow the steps in Quick Start setup for Container Insights on Amazon EKS and Kubernetes (p. 277) or you can follow the steps in this section. In the following steps, you set up the CloudWatch agent to be able to collect metrics from your clusters.

#### Step 1: Create a namespace for CloudWatch

Use the following step to create a Kubernetes namespace called `amazon-cloudwatch` for CloudWatch.

You can skip this step if you have already created this namespace.

To create a namespace for CloudWatch

- Enter the following command.

  ```
  ```
Step 2: Create a service account in the cluster

Use the following step to create a service account for the CloudWatch agent, if you do not already have one.

To create a service account for the CloudWatch agent

- Enter the following command.

```bash
```

If you didn't follow the previous steps, but you already have a service account for the CloudWatch agent that you want to use, you must ensure that it has the following rules. Additionally, in the rest of the steps in the Container Insights installation, you must use the name of that service account instead of `cloudwatch-agent`.

```
rules:
  - apiGroups: [""]
    resources: ["pods", "nodes", "endpoints"]
    verbs: ["watch", "list"]
  - apiGroups: [""]
    resources: ["nodes/proxy"]
    verbs: ["get"]
  - apiGroups: [""]
    resources: ["nodes/stats", "configmaps", "events"]
    verbs: ["create"]
  - apiGroups: [""]
    resources: ["configmaps"]
    resourceNames: ["cwagent-clusterleader"]
    verbs: ["get", "update"]
  - nonResourceURLs: ["/metrics"]
    verbs: ["get"]
```

Step 3: Create a ConfigMap for the CloudWatch agent

Use the following steps to create a ConfigMap for the CloudWatch agent.

To create a ConfigMap for the CloudWatch agent

1. Download the ConfigMap YAML to your `kubectl` client host by running the following command:

```bash
```

2. Edit the downloaded YAML file, as follows:

   - **cluster_name** – In the `kubernetes` section, replace `{{cluster-name}}` with the name of your cluster. Remove the `{{}}` characters. Alternatively, if you're using an Amazon EKS cluster, you can delete the "cluster_name" field and value. If you do, the CloudWatch agent detects the cluster name from the Amazon EC2 tags.

3. (Optional) Make further changes to the ConfigMap based on your monitoring requirements, as follows:

   - **metrics_collection_interval** – In the `kubernetes` section, you can specify how often the agent collects metrics. The default is 60 seconds. The default cadvisor collection interval in kubelet is 15 seconds, so don't set this value to less than 15 seconds.
• **endpoint_override** – In the logs section, you can specify the CloudWatch Logs endpoint if you want to override the default endpoint. You might want to do this if you’re publishing from a cluster in a VPC and you want the data to go to a VPC endpoint.

• **force_flush_interval** – In the logs section, you can specify the interval for batching log events before they are published to CloudWatch Logs. The default is 5 seconds.

• **region** – By default, the agent published metrics to the Region where the worker node is located. To override this, you can add a region field in the agent section: for example, "region": "us-west-2".

• **statsd** section – If you want the CloudWatch Logs agent to also run as a StatsD listener in each worker node of your cluster, you can add a statsd section to the metrics section, as in the following example. For information about other StatsD options for this section, see Retrieve custom metrics with StatsD (p. 503).

```json
"metrics": {
    "metrics_collected": {
        "statsd": {
            "service_address": "8125"
        }
    }
}
```

A full example of the JSON section is as follows.

```json
{
    "agent": {
        "region": "us-east-1"
    },
    "logs": {
        "metrics_collected": {
            "kubernetes": {
                "cluster_name": "MyCluster",
                "metrics_collection_interval": 60
            }
        },
        "force_flush_interval": 5,
        "endpoint_override": "logs.us-east-1.amazonaws.com"
    },
    "metrics": {
        "metrics_collected": {
            "statsd": {
                "service_address": "8125"
            }
        }
    }
}
```

4. Create the ConfigMap in the cluster by running the following command.

```bash
kubectl apply -f cwagent-configmap.yaml
```

**Step 4: Deploy the CloudWatch agent as a DaemonSet**

To finish the installation of the CloudWatch agent and begin collecting container metrics, use the following steps.

**To deploy the CloudWatch agent as a DaemonSet**

1. • If you do not want to use StatsD on the cluster, enter the following command.
If you do want to use StatsD, follow these steps:

a. Download the DaemonSet YAML to your kubectl client host by running the following command.

```bash
```

b. Uncomment the `port` section in the `cwagent-daemonset.yaml` file as in the following:

```yaml
ports:
  - containerPort: 8125
    hostPort: 8125
    protocol: UDP
```

c. Deploy the CloudWatch agent in your cluster by running the following command.

```bash
kubectl apply -f cwagent-daemonset.yaml
```

2. Validate that the agent is deployed by running the following command.

```bash
kubectl get pods -n amazon-cloudwatch
```

When complete, the CloudWatch agent creates a log group named `/aws/containerinsights/Cluster_Name/performance` and sends the performance log events to this log group. If you also set up the agent as a StatsD listener, the agent also listens for StatsD metrics on port 8125 with the IP address of the node where the application pod is scheduled.

**Troubleshooting**

If the agent doesn't deploy correctly, try the following:

- Run the following command to get the list of pods.

```bash
kubectl get pods -n amazon-cloudwatch
```

- Run the following command and check the events at the bottom of the output.

```bash
kubectl describe pod pod-name -n amazon-cloudwatch
```

- Run the following command to check the logs.

```bash
kubectl logs pod-name -n amazon-cloudwatch
```

**Using AWS Distro for OpenTelemetry**

Use the instructions in this section to set up Container Insights on an Amazon EKS cluster by using the AWS Distro for OpenTelemetry collector. For more information about the AWS Distro for OpenTelemetry, see [AWS Distro for OpenTelemetry](#).
First, deploy the AWS Distro for OpenTelemetry collector as a DaemonSet by entering the following command.

```
curl https://raw.githubusercontent.com/aws-observability/aws-otel-collector/main/deployment-template/eks/otel-container-insights-infra.yaml | kubectl apply -f -
```

To confirm that the collector is running, enter the following command.

```
kubectl get pods -l name=aws-otel-eks-ci -n aws-otel-eks
```

If the output of this command includes multiple pods in the Running state, the collector is running and collecting metrics from the cluster. The collector creates a log group named `aws/containerinsights/cluster-name/performance` and sends the performance log events to it.

For information about how to see your Container Insights metrics in CloudWatch, see Viewing Container Insights metrics (p. 296).

AWS has also provided documentation on GitHub for this scenario. If you want to customize the metrics and logs published by Container Insights, see https://aws-otel.github.io/docs/getting-started/container-insights/eks-infra.

### Send logs to CloudWatch Logs

To send logs from your containers to Amazon CloudWatch Logs, you can use Fluent Bit or Fluentd. For more information, see Fluent Bit and Fluentd.

If you are not already using Fluentd, we recommend that you use Fluent Bit for the following reasons:

- Fluent Bit has a smaller resource footprint and is more resource-efficient with memory and CPU usage than FluentD. For a more detailed comparison, see Fluent Bit and Fluentd performance comparison (p. 283).
- The Fluent Bit image is developed and maintained by AWS. This gives AWS the ability to adopt new Fluent Bit image features and respond to issues much quicker.

**Topics**

- Fluent Bit and Fluentd performance comparison (p. 283)
- Set up Fluent Bit as a DaemonSet to send logs to CloudWatch Logs (p. 284)
- (Optional) Set up FluentD as a DaemonSet to send logs to CloudWatch Logs (p. 289)
- (Optional) Set up Amazon EKS control plane logging (p. 294)
- (Optional) Enable App Mesh Envoy access logs (p. 294)

### Fluent Bit and Fluentd performance comparison

The following tables show the performance advantage that Fluent Bit has over FluentD in memory and CPU usages. The following numbers are just for reference and might change depending on the environment.

<table>
<thead>
<tr>
<th>Logs per second</th>
<th>Fluentd CPU usage</th>
<th>Fluent Bit CPU usage with Fluentd-compatible configuration</th>
<th>Fluent Bit CPU usage with optimized configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>0.35 vCPU</td>
<td>0.02 vCPU</td>
<td>0.02 vCPU</td>
</tr>
</tbody>
</table>
### Differences if you’re already using Fluentd

If you are already using Fluentd to send logs from containers to CloudWatch Logs, read this section to see the differences between Fluentd and Fluent Bit. If you are not already using Fluentd with Container Insights, you can skip to Setting up Fluent Bit (p. 285).

We provide two default configurations for Fluent Bit:

- **Fluent Bit optimized configuration** — A configuration aligned with Fluent Bit best practices.
- **Fluentd-compatible configuration** — A configuration that is aligned with Fluentd behavior as much as possible.

The following list explains the differences between Fluentd and each Fluent Bit configuration in detail.

- **Differences in log stream names** — If you use the Fluent Bit optimized configuration, the log stream names will be different.
Under /aws/containerinsights/Cluster_Name/application

- Fluent Bit optimized configuration sends logs to `kubernetes-nodeName-application.var.log.containers.kubernetes-podName_kubernetes-namespace_kubernetes-containers-container-name-kubernetes-containers-containerID`
- Fluentd sends logs to `kubernetes-podName_kubernetes-namespace_kubernetes-containers-containerName-kubernetes-containers-containerID`

Under /aws/containerinsights/Cluster_Name/host

- Fluent Bit optimized configuration sends logs to `kubernetes-nodeName.host-log-file`
- Fluentd sends logs to `host-log-file-Kubernetes-NodePrivateIp`

Under /aws/containerinsights/Cluster_Name/dataplane

- Fluent Bit optimized configuration sends logs to `kubernetes-nodeName.dataplaneServiceLog`
- Fluentd sends logs to `dataplaneServiceLog-Kubernetes-nodeName`
- The kube-proxy and aws-node log files that Container Insights writes are in different locations. In FluentD configuration, they are in /aws/containerinsights/Cluster_Name/application. In the Fluent Bit optimized configuration, they are in /aws/containerinsights/Cluster_Name/dataplane.
- Most metadata such as pod_name and namespace_name are the same in Fluent Bit and Fluentd, but the following are different.
  - The Fluent Bit optimized configuration uses docker_id and Fluentd use Docker.container_id.
  - Both Fluent Bit configurations do not use the following metadata. They are present only in Fluentd: container_image_id, master_url, namespace_id, and namespace_labels.

### Setting up Fluent Bit

To set up Fluent Bit to collect logs from your containers, you can follow the steps in Quick Start setup for Container Insights on Amazon EKS and Kubernetes (p. 277) or you can follow the steps in this section.

In the following steps, you set up Fluent Bit as a daemonSet to send logs to CloudWatch Logs. When you complete this step, Fluent Bit creates the following log groups if they don't already exist.

<table>
<thead>
<tr>
<th>Log group name</th>
<th>Log source</th>
</tr>
</thead>
<tbody>
<tr>
<td>/aws/containerinsights/Cluster_Name/application</td>
<td>All log files in /var/log/containers</td>
</tr>
<tr>
<td>/aws/containerinsights/Cluster_Name/host</td>
<td>Logs from /var/log/dmesg, /var/log/secure, and /var/log/messages</td>
</tr>
<tr>
<td>/aws/containerinsights/Cluster_Name/dataplane</td>
<td>The logs in /var/log/journal for kubelet.service, kubeproxy.service, and docker.service.</td>
</tr>
</tbody>
</table>

### To install Fluent Bit to send logs from containers to CloudWatch Logs

1. If you don't already have a namespace called amazon-cloudwatch, create one by entering the following command:

   ```bash
   ```
2. Run the following command to create a ConfigMap named `cluster-info` with the cluster name and the Region to send logs to. Replace `cluster-name` and `cluster-region` with your cluster's name and Region.

```bash
ClusterName=cluster-name
RegionName=cluster-region
FluentBitHttpPort='2020'
FluentBitReadFromHead='Off'
[[ #($FluentBitReadFromHead) = 'On' ]] && FluentBitReadFromTail='Off' &&
FluentBitReadFromTail='On'
[[ -z #($FluentBitHttpPort) ]] && FluentBitHttpServer='Off' || FluentBitHttpServer='On'
kubectl create configmap fluent-bit-cluster-info
  --from-literal=cluster.name=${ClusterName} \n  --from-literal=http.server=${FluentBitHttpServer} \n  --from-literal=http.port=${FluentBitHttpPort} \n  --from-literal=read.head=${FluentBitReadFromHead} \n  --from-literal=read.tail=${FluentBitReadFromTail} \n  --from-literal=logs.region=${RegionName} -n amazon-cloudwatch
```

In this command, the `FluentBitHttpServer` for monitoring plugin metrics is on by default. To turn it off, change the third line in the command to `FluentBitHttpPort=''` (empty string) in the command.

Also by default, Fluent Bit reads log files from the tail, and will capture only new logs after it is deployed. If you want the opposite, set `FluentBitReadFromHead='On'` and it will collect all logs in the file system.

3. Download and deploy the Fluent Bit daemonset to the cluster by running one of the following commands.

   • If you want the Fluent Bit optimized configuration, run this command.

```bash
```

   • If you want the Fluent Bit configuration that is more similar to Fluentd, run this command.

```bash
```

4. Validate the deployment by entering the following command. Each node should have one pod named `fluent-bit-*`.

```bash
kubectl get pods -n amazon-cloudwatch
```

The above steps create the following resources in the cluster:

- A service account named `Fluent-Bit` in the `amazon-cloudwatch` namespace. This service account is used to run the Fluent Bit daemonSet. For more information, see Managing Service Accounts in the Kubernetes Reference.
- A cluster role named `Fluent-Bit-role` in the `amazon-cloudwatch` namespace. This cluster role grants `get`, `list`, and `watch` permissions on pod logs to the `Fluent-Bit` service account. For more information, see API Overview in the Kubernetes Reference.
- A ConfigMap named `Fluent-Bit-config` in the `amazon-cloudwatch` namespace. This ConfigMap contains the configuration to be used by Fluent Bit. For more information, see Configure a Pod to Use a ConfigMap in the Kubernetes Tasks documentation.
If you want to verify your Fluent Bit setup, follow these steps.

Verify the Fluent Bit setup

2. In the navigation pane, choose Logs.
3. Make sure that you're in the Region where you deployed Fluent Bit.
4. Check the list of log groups in the Region. You should see the following:
   - /aws/containerinsights/Cluster_Name/application
   - /aws/containerinsights/Cluster_Name/host
   - /aws/containerinsights/Cluster_Name/dataplane
5. Navigate to one of these log groups and check the Last Event Time for the log streams. If it is recent relative to when you deployed Fluent Bit, the setup is verified.

There might be a slight delay in creating the /dataplane log group. This is normal as these log groups only get created when Fluent Bit starts sending logs for that log group.

Multiline log support

By default, the multiline log entry starter is any character with no white space. This means that all log lines that start with a character that does not have white space are considered as a new multiline log entry.

If your own application logs use a different multiline starter, you can support them by making two changes in the Fluent-Bit.yaml file.

First, exclude them from the default input by adding the pathnames of your log files to an exclude_path field in the containers section of Fluent-Bit.yaml. The following is an example.

```
[INPUT]
Name        tail
Tag         application.*
Exclude_Path full_pathname_of_log_file*, full_pathname_of_log_file2*
Path        /var/log/containers/*.log
```

Next, add a block for your log files to the Fluent-Bit.yaml file. Refer to the cloudwatch-agent log configuration example below which uses a timestamp regular expression as the multiline starter.

```
application-log.conf: |
[INPUT]
    Name        tail
    Tag         application.*
    Path        /var/log/containers/cloudwatch-agent*
    Docker_Mode On
    Docker_Mode_Flush 5
    Docker_Mode_Parser cwagent_firstline
    Parser       docker
    DB           /fluent-bit/state/flb_cwagent.db
    Mem_Buf_Limit 5MB
    Skip_Long_Lines On
    Refresh_Interval 10

parsers.conf: |
[PARSER]
    Name        cwagent_firstline
    Format      regex
```
(Optional) Reducing the log volume from Fluent Bit

By default, we send Fluent Bit application logs and Kubernetes metadata to CloudWatch. If you want to reduce the volume of data being sent to CloudWatch, you can stop one or both of these data sources from being sent to CloudWatch.

To stop Fluent Bit application logs, remove the following section from the `Fluent-Bit.yaml` file.

<table>
<thead>
<tr>
<th>INPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Tag</td>
</tr>
<tr>
<td>Path</td>
</tr>
<tr>
<td>Parser</td>
</tr>
<tr>
<td>DB</td>
</tr>
<tr>
<td>Mem_Buf_Limit</td>
</tr>
<tr>
<td>Skip_Long_Lines</td>
</tr>
<tr>
<td>Refresh_Interval</td>
</tr>
</tbody>
</table>

To remove Kubernetes metadata from being appended to log events that are sent to CloudWatch, add the following filters to the `application-log.conf` section in the `Fluent-Bit.yaml` file.

```
[FILTER]
Name | nest
Match | application.*
Operation | lift
Nested_under | kubernetes
Add_prefix | Kube.

[FILTER]
Name | modify
Match | application.*
Remove | Kube.<Metadata_1>
Remove | Kube.<Metadata_2>
Remove | Kube.<Metadata_3>

[FILTER]
Name | nest
Match | application.*
Operation | nest
Wildcard | Kube.*
Nested_under | kubernetes
Remove_prefix | Kube.
```

Troubleshooting

If you don’t see these log groups and are looking in the correct Region, check the logs for the Fluent Bit daemonSet pods to look for the error.

Run the following command and make sure that the status is Running.

```
kubectl get pods -n amazon-cloudwatch
```

If the logs have errors related to IAM permissions, check the IAM role that is attached to the cluster nodes. For more information about the permissions required to run an Amazon EKS cluster, see For more...
information about the permissions required to run an Amazon EKS cluster, see Amazon EKS IAM Policies, Roles, and Permissions in the Amazon EKS User Guide.

If the pod status is CreateContainerConfigError, get the exact error by running the following command.

```
kubectl describe pod pod_name -n amazon-cloudwatch
```

Dashboard

You can create a dashboard to monitor metrics of each running plugin. You can see data for input and output bytes and for record processing rates as well as output errors and retry/failed rates. To view these metrics, you will need to install the CloudWatch agent with Prometheus metrics collection for Amazon EKS and Kubernetes clusters. For more information about how to set up the dashboard, see Install the CloudWatch agent with Prometheus metrics collection on Amazon EKS and Kubernetes clusters (p. 366).

**Note**
Before you can set up this dashboard, you must set up Container Insights for Prometheus metrics. For more information, see Container Insights Prometheus metrics monitoring (p. 326).

To create a dashboard for the Fluent Bit Prometheus metrics

1. Create environment variables, replacing the values on the right in the following lines to match your deployment.

```
DASHBOARD_NAME=your_cw_dashboard_name
REGION_NAME=your_metric_region_such_as_us-west-1
CLUSTER_NAME=your_kubernetes_cluster_name
```

2. Create the dashboard by running the following command.

```
| sed "s/{{YOUR_AWS_REGION}}/${REGION_NAME}/g"
| sed "s/{{YOUR_CLUSTER_NAME}}/${CLUSTER_NAME}/g"
|xargs -0 aws cloudwatch put-dashboard --dashboard-name ${DASHBOARD_NAME} --dashboard-body
```

(Optional) Set up FluentD as a DaemonSet to send logs to CloudWatch Logs

**Warning**
Container Insights Support for FluentD is now in maintenance mode, which means that AWS will not provide any further updates for FluentD and that we are planning to deprecate it in near future. Additionally, the current FluentD configuration for Container Insights is using an old version of the FluentD Image fluent/fluentd-kubernetes-daemonset:v1.7.3-debian-cloudwatch-1.0 which does not have the latest improvement and security patches. For the latest FluentD image supported by the open source community, see fluentd-kubernetes-daemonset.

We strongly recommend that you migrate to use FluentBit with Container Insights whenever possible. Using FluentBit as the log forwarder for Container Insights provides significant performance gains.

For more information, see Set up Fluent Bit as a DaemonSet to send logs to CloudWatch Logs (p. 284) and Differences if you’re already using Fluentd (p. 284).

To set up FluentD to collect logs from your containers, you can follow the steps in Quick Start setup for Container Insights on Amazon EKS and Kubernetes (p. 277) or you can follow the steps in this section.
In the following steps, you set up FluentD as a DaemonSet to send logs to CloudWatch Logs. When you complete this step, FluentD creates the following log groups if they don't already exist.

<table>
<thead>
<tr>
<th>Log group name</th>
<th>Log source</th>
</tr>
</thead>
<tbody>
<tr>
<td>/aws/containerinsights/Cluster_Name/ application</td>
<td>All log files in /var/log/containers</td>
</tr>
<tr>
<td>/aws/containerinsights/Cluster_Name/ host</td>
<td>Logs from /var/log/dmesg, /var/log/secure, and /var/log/messages</td>
</tr>
<tr>
<td>/aws/containerinsights/Cluster_Name/ dataplane</td>
<td>The logs in /var/log/journal for kubelet.service, kubeproxy.service, and docker.service.</td>
</tr>
</tbody>
</table>

**Step 1: Create a namespace for CloudWatch**

Use the following step to create a Kubernetes namespace called `amazon-cloudwatch` for CloudWatch. You can skip this step if you have already created this namespace.

**To create a namespace for CloudWatch**

- Enter the following command.

```
```

**Step 2: Install FluentD**

Start this process by downloading FluentD. When you finish these steps, the deployment creates the following resources on the cluster:

- A service account named `fluentd` in the `amazon-cloudwatch` namespace. This service account is used to run the FluentD DaemonSet. For more information, see Managing Service Accounts in the Kubernetes Reference.
- A cluster role named `fluentd` in the `amazon-cloudwatch` namespace. This cluster role grants `get`, `list`, and `watch` permissions on pod logs to the `fluentd` service account. For more information, see API Overview in the Kubernetes Reference.
- A ConfigMap named `fluentd-config` in the `amazon-cloudwatch` namespace. This ConfigMap contains the configuration to be used by FluentD. For more information, see Configure a Pod to Use a ConfigMap in the Kubernetes Tasks documentation.

**To install FluentD**

1. Create a ConfigMap named `cluster-info` with the cluster name and the AWS Region that the logs will be sent to. Run the following command, updating the placeholders with your cluster and Region names.

```
kubectl create configmap cluster-info \   --from-literal=cluster.name=cluster_name \   --from-literal=logs.region=region_name -n amazon-cloudwatch
```

2. Download and deploy the FluentD DaemonSet to the cluster by running the following command. Make sure that you are using the container image with correct architecture. The example manifest
only works on x86 instances and will enter CrashLoopBackOff if you have Advanced RISC Machine (ARM) instances in your cluster. The Fluentd daemonSet does not have an official multi-architecture Docker image that enables you to use one tag for multiple underlying images and let the container runtime pull the right one. The FluentD ARM image uses a different tag with an arm64 suffix.

```
```

**Note**

Because of a recent change to optimize the FluentD configuration and minimize the impact of FluentD API requests on Kubernetes API endpoints, the "Watch" option for Kubernetes filters has been disabled by default. For more details, see fluent-plugin-kubernetes_metadata_filter.

3. Validate the deployment by running the following command. Each node should have one pod named fluentd-cloudwatch-*.

```
kubectl get pods -n amazon-cloudwatch
```

**Step 3: Verify the FluentD setup**

To verify your FluentD setup, use the following steps.

**To verify the FluentD setup for Container Insights**

2. In the navigation pane, choose **Logs**. Make sure that you're in the Region where you deployed FluentD to your containers.

   In the list of log groups in the Region, you should see the following:

   - /aws/containerinsights/Cluster_Name/application
   - /aws/containerinsights/Cluster_Name/host
   - /aws/containerinsights/Cluster_Name/dataplane

   If you see these log groups, the FluentD setup is verified.

**Multiline log support**

On August 19 2019, we added multiline log support for the logs collected by FluentD.

By default, the multiline log entry starter is any character with no white space. This means that all log lines that start with a character that does not have white space are considered as a new multiline log entry.

If your own application logs use a different multiline starter, you can support them by making two changes in the fluentd.yaml file.

First, exclude them from the default multiline support by adding the pathnames of your log files to an exclude_path field in the containers section of fluentd.yaml. The following is an example.

```
<source>
```
Next, add a block for your log files to the `fluentd.yaml` file. The example below is used for the CloudWatch agent's log file, which uses a timestamp regular expression as the multiline starter. You can copy this block and add it to `fluentd.yaml`. Change the indicated lines to reflect your application log file name and the multiline starter that you want to use.

```xml
<source>
  @type tail
  @id in_tail_container_logs
  @label @containers
  path /var/log/containers/*.log
  exclude_path ["full_pathname_of_log_file", "full_pathname_of_log_file2"]
</source>

```xml
<source>
  @type tail
  @id in_tail_cwagent_logs
  @label @cwagentlogs
  path /var/log/containers/cloudwatch-agent*
  pos_file /var/log/cloudwatch-agent.log.pos
  tag *
  read_from_head true
  <parse>
    @type json
    time_format %Y-%m-%dT%H:%M:%S.%NZ
  </parse>
</source>

```xml
<label @cwagentlogs>
  <filter **>
    @type kubernetes_metadata
    @id filter_kube_metadata_cwagent
  </filter>
  <filter **>
    @type record_transformer
    @id filter_cwagent_stream_transformer
    <record>
      stream_name ${tag_parts[3]}
    </record>
  </filter>
  <filter **>
    @type concat
    key log
    multiline_start_regexp /^\d{4}[-/]\d{1,2}[-/]\d{1,2}/
    separator 
    flush_interval 5
    timeout_label @NORMAL
  </filter>
  <match **>
    @type relabel
    @label @NORMAL
  </match>
</label>

(Optional) Reducing the log volume from FluentD

By default, we send FluentD application logs and Kubernetes metadata to CloudWatch. If you want to reduce the volume of data being sent to CloudWatch, you can stop one or both of these data sources from being sent to CloudWatch.
To stop FluentD application logs, remove the following section from the `fluentd.yaml` file.

```yaml
<source>
  @type tail
  @id in_tail_fluentd_logs
  @label @fluentdlogs
  path /var/log/containers/fluentd*
  pos_file /var/log/fluentd.log.pos
  tag *
  read_from_head true
  <parse>
    @type json
    time_format %Y-%m-%dT%H:%M:%S.%NZ
  </parse>
</source>

To remove Kubernetes metadata from being appended to log events that are sent to CloudWatch, add one line to the `record_transformer` section in the `fluentd.yaml` file. In the log source where you want to remove this metadata, add the following line.

```yaml
remove_keys $.kubernetes.pod_id, $.kubernetes.master_url, $.kubernetes.container_image_id, $.kubernetes.namespace_id
```

For example:

```yaml
<filter **>
  @type record_transformer
  @id filter_containers_stream_transformer
  <record>
    stream_name $(tag_parts[3])
  </record>
</filter>

remove_keys $.kubernetes.pod_id, $.kubernetes.master_url, $.kubernetes.container_image_id, $.kubernetes.namespace_id
```

**Troubleshooting**

If you don't see these log groups and are looking in the correct Region, check the logs for the FluentD DaemonSet pods to look for the error.
Run the following command and make sure that the status is Running.

```
kubectl get pods -n amazon-cloudwatch
```

In the results of the previous command, note the pod name that starts with fluentd-cloudwatch. Use this pod name in the following command.

```
kubectl logs pod_name -n amazon-cloudwatch
```

If the logs have errors related to IAM permissions, check the IAM role attached to the cluster nodes. For more information about the permissions required to run an Amazon EKS cluster, see Amazon EKS IAM Policies, Roles, and Permissions in the Amazon EKS User Guide.

If the pod status is CreateContainerConfigError, get the exact error by running the following command.

```
kubectl describe pod pod_name -n amazon-cloudwatch
```

If the pod status is CrashLoopBackOff, make sure that the architecture of the Fluentd container image is the same as the node when you installed Fluentd. If your cluster has both x86 and ARM64 nodes, you can use a kubernetes.io/arch label to place the images on the correct node. For more information, see kubernetes.io/arch.

(Optional) Set up Amazon EKS control plane logging

If you're using Amazon EKS, you can optionally enable Amazon EKS control plane logging, to provide audit and diagnostic logs directly from the Amazon EKS control plane to CloudWatch Logs. For more information, see Amazon EKS Control Plane Logging.

(Optional) Enable App Mesh Envoy access logs

You can set up Container Insights FluentD to send App Mesh Envoy access logs to CloudWatch Logs. For more information, see Access logs.

To have Envoy access logs sent to CloudWatch Logs

1. Set up FluentD in the cluster. For more information, see (Optional) Set up FluentD as a DaemonSet to send logs to CloudWatch Logs (p. 289).
2. Configure Envoy access logs for your virtual nodes. For instructions, see Configure Envoy access logs. Be sure to configure the log path to be /dev/stdout in each virtual node.

When you have finished, the envoy access logs are sent to the /aws/containerinsights/Cluster_Name/application log group.

Updating or deleting Container Insights on Amazon EKS and Kubernetes

Use the steps in these sections to update your CloudWatch agent container image, or to remove Container Insights from an Amazon EKS or Kubernetes cluster.

Topics

- Updating the CloudWatch agent container image (p. 295)
• Deleting the CloudWatch agent and FluentD for Container Insights (p. 296)

Updating the CloudWatch agent container image

If you need to update your container image to the latest version, use the steps in this section.

To update your container image

1. Apply the latest `cwagent-serviceaccount.yaml` file by entering the following command.

   ```bash
   ```

2. This step is necessary only for customers who upgraded their containerized CloudWatch agent from a version earlier than 1.226589.0, which was released on August 20, 2019.

   In the Configmap file `cwagentconfig`, change the keyword `structuredlogs` to `logs`
   
   a. First, open the existing `cwagentconfig` in edit mode by entering the following command.

   ```bash
   kubectl edit cm cwagentconfig -n amazon-cloudwatch
   ```

   In the file, if you see the keyword `structuredlogs`, change it to `logs`

   b. Enter `wq` to save the file and exit edit mode.

3. Apply the latest `cwagent-daemonset.yaml` file by entering the following command.

   ```bash
   ```

You can achieve rolling updates of the CloudWatch agent DaemonSet anytime that you change your configuration in `cwagent-configmap.yaml`. To do so, you must make sure the `.spec.template` section in the `cwagent-daemonset.yaml` file has changes. Otherwise, Kubernetes treats the DaemonSet as unchanged. A common practice is to add the hash value of the ConfigMap into `.spec.template.metadata.annotations.configHash`, as in the following example.

```bash
yq w -i cwagent-daemonset.yaml spec.template.metadata.annotations.configHash $(kubectl get cm/cwagentconfig -n amazon-cloudwatch -o yaml | sha256sum)
```

This adds a hash value into the `cwagent-daemonset.yaml` file, as in the following example.

```
spec:
  selector:
    matchLabels:
      name: cloudwatch-agent
  template:
    metadata:
      labels:
        name: cloudwatch-agent
      annotations:
        configHash: 88915de4cf9c3551a8dc74c0137a3e83569d28c71044b0359c2578d2e0461825
```

Then if you run the following command, the new configuration is picked up.
For more information about yq, see yq.

Deleting the CloudWatch agent and FluentD for Container Insights

To delete all resources related to the CloudWatch agent and Fluentd, enter the following command. In this command, `Cluster` is the name of your Amazon EKS or Kubernetes cluster, and `Region` is the name of the Region where the logs are published.

```
curl https://raw.githubusercontent.com/aws-samples/amazon-cloudwatch-container-insights/latest/k8s-deployment-manifest-templates/deployment-mode/daemonset/container-insights-monitoring/quickstart/cwagent-fluentd-quickstart.yaml | sed "s/{{cluster_name}}/Cluster_Name/;s/{{region_name}}/Region/" | kubectl delete -f -
```

Viewing Container Insights metrics

After you have Container Insights set up and it is collecting metrics, you can view those metrics in the CloudWatch console.

For Container Insights metrics to appear on your dashboard, you must complete the Container Insights setup. For more information, see Setting up Container Insights (p. 264).

This procedure explains how to view the metrics that Container Insights automatically generates from the collected log data. The rest of this section explains how to further dive into your data and use CloudWatch Logs Insights to see more metrics at more levels of granularity.

**To view Container Insights metrics**

2. In the navigation pane, choose Performance Monitoring.
3. Use the drop-down boxes near the top to select the type of resource to view, as well as the specific resource.

You can set a CloudWatch alarm on any metric that Container Insights collects. For more information, see Using Amazon CloudWatch alarms (p. 102)

Viewing the top contributors

For some of the views in Container Insights performance monitoring, you can also see the top contributors by memory or CPU, or the most recently active resources. This is available when you select any of the following dashboards in the drop-down box near the top of the page:

- ECS Services
- ECS Tasks
- EKS Namespaces
- EKS Services
- EKS Pods

When you are viewing one of these types of resources, the bottom of the page displays a table sorted initially by CPU usage. You can change it to sort by memory usage or recent activity. To see more about
one of the rows in the table, you can select the checkbox next to that row and then choose Actions and choose one of the options in the Actions menu.

Using CloudWatch Logs Insights to view Container Insights data

Container Insights collects metrics by using performance log events with using embedded metric format (p. 668). The logs are stored in CloudWatch Logs. CloudWatch generates several metrics automatically from the logs which you can view in the CloudWatch console. You can also do a deeper analysis of the performance data that is collected by using CloudWatch Logs Insights queries.

For more information about CloudWatch Logs Insights, see Analyze Log Data with CloudWatch Logs Insights. For more information about the log fields you can use in queries, see Container Insights performance log events for Amazon EKS and Kubernetes (p. 309).

To use CloudWatch Logs Insights to query your container metric data

2. In the navigation pane, choose Insights.

   Near the top of the screen is the query editor. When you first open CloudWatch Logs Insights, this box contains a default query that returns the 20 most recent log events.
3. In the box above the query editor, select one of the Container Insights log groups to query. For the following example queries to work, the log group name must end with performance.

   When you select a log group, CloudWatch Logs Insights automatically detects fields in the data in the log group and displays them in Discovered fields in the right pane. It also displays a bar graph of log events in this log group over time. This bar graph shows the distribution of events in the log group that matches your query and time range, not only the events displayed in the table.
4. In the query editor, replace the default query with the following query and choose Run query.

   ```
   STATS avg(node_cpu_utilization) as avg_node_cpu_utilization by NodeName
   | SORT avg_node_cpu_utilization DESC
   ```

   This query shows a list of nodes, sorted by average node CPU utilization.
5. To try another example, replace that query with another query and choose Run query. More sample queries are listed later on this page.

   ```
   STATS avg(number_of_container_restarts) as avg_number_of_container_restarts by PodName
   | SORT avg_number_of_container_restarts DESC
   ```

   This query displays a list of your pods, sorted by average number of container restarts.
6. If you want to try another query, you can use include fields in the list at the right of the screen. For more information about query syntax, see CloudWatch Logs Insights Query Syntax.

To see lists of your resources

2. In the navigation pane, choose Resources.
3. The default view is a list of your resources being monitored by Container Insights, and alarms that you have set on these resources. To see a visual map of the resources, choose Map view.
4. From the map view, you can pause your pointer over any resource in the map to see basic metrics about that resource. You can choose any resource to see more detailed graphs about the resource.
Use case: Seeing task-level metrics in Amazon ECS containers

The following example illustrates how to use CloudWatch Logs Insights to dive deeper into your Container Insights logs. For more examples, see the blog Introducing Amazon CloudWatch Container Insights for Amazon ECS.

Container Insights does not automatically generate metrics at the Task level of granularity. The following query displays task-level metrics for CPU and memory usage.

```
stats avg(CpuUtilized) as CPU, avg(MemoryUtilized) as Mem by TaskId, ContainerName
| sort Mem, CPU desc
```

Other sample queries for Container Insights

List of your pods, sorted by average number of container restarts

```
STATS avg(number_of_container_restarts) as avg_number_of_container_restarts by PodName
| SORT avg_number_of_container_restarts DESC
```

Pods requested vs. pods running

```
fields @timestamp, @message
| sort @timestamp desc
| filter Type="Pod"
| stats min(pod_number_of_containers) as requested, min(pod_number_of_running_containers) as running, ceil(avg(pod_number_of_containers-pod_number_of_running_containers)) as pods_missing by kubernetes.pod_name
| sort pods_missing desc
```

Count of cluster node failures

```
stats avg(cluster_failed_node_count) as CountOfNodeFailures
| filter Type="Cluster"
| sort @timestamp desc
```

Application log errors by container name

```
stats count() as countoferrors by kubernetes.container_name
| filter stream="stderr"
| sort countoferrors desc
```

Disk usage by container name

```
stats floor(avg(container_filesystem_usage/1024)) as container_filesystem_usage_avg_kb by InstanceId, kubernetes.container_name, device
| filter Type="ContainerFS"
| sort container_filesystem_usage_avg_kb desc
```

CPU usage by container name

```
stats pct(container_cpu_usage_total, 50) as CPUPercMedian by kubernetes.container_name
```
Metrics collected by Container Insights

Container Insights collects one set of metrics for Amazon ECS and AWS Fargate, and a different set for Amazon EKS and Kubernetes.

Topics
- Amazon ECS Container Insights metrics (p. 299)
- Amazon EKS and Kubernetes Container Insights metrics (p. 303)

Amazon ECS Container Insights metrics

The following table lists the metrics and dimensions that Container Insights collects for Amazon ECS. These metrics are in the ECS/ContainerInsights namespace. For more information, see Metrics (p. 3).

If you do not see any Container Insights metrics in your console, be sure that you have completed the setup of Container Insights. Metrics do not appear before Container Insights has been set up completely. For more information, see Setting up Container Insights (p. 264).

When you use Container Insights to collect the following metrics, the metrics are charged as custom metrics. For more information about CloudWatch pricing, see Amazon CloudWatch Pricing. Amazon ECS also automatically sends several free metrics to CloudWatch. For more information, see Available metrics and dimensions.

The following metrics are available when you complete the steps in Setting up Container Insights on Amazon ECS for cluster- and service-level metrics (p. 264)

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ContainerInstanceCount</td>
<td>ClusterName</td>
<td>The number of EC2 instances running the Amazon ECS agent that are registered with a cluster. Unit: Count</td>
</tr>
<tr>
<td>CpuUtilized</td>
<td>TaskDefinitionFamily, ClusterName, ServiceName, ClusterName</td>
<td>The CPU units used by tasks in the resource that is specified by the dimension set that you’re using. This metric is collected only for tasks that have a defined CPU reservation in their container definition.</td>
</tr>
<tr>
<td>CpuReserved</td>
<td>TaskDefinitionFamily, ClusterName, ServiceName, ClusterName</td>
<td>The CPU units reserved by tasks in the resource that is specified by the</td>
</tr>
<tr>
<td>Metric name</td>
<td>Dimensions</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ClusterName</td>
<td>ClusterName</td>
<td>dimension set that you're using.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This metric is collected only for tasks that have a defined CPU reservation in their task definition.</td>
</tr>
<tr>
<td>DeploymentCount</td>
<td>ServiceName, ClusterName</td>
<td>The number of deployments in an Amazon ECS service.</td>
</tr>
<tr>
<td>DesiredTaskCount</td>
<td>ServiceName, ClusterName</td>
<td>The desired number of tasks for an Amazon ECS service.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>MemoryUtilized</td>
<td>TaskDefinitionFamily, ClusterName, ServiceName, ClusterName, ClusterName</td>
<td>The memory being used by tasks in the resource that is specified by the dimension set that you're using.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This metric is collected only for tasks that have a defined memory reservation in their task definition.</td>
</tr>
<tr>
<td>MemoryReserved</td>
<td>TaskDefinitionFamily, ClusterName, ServiceName, ClusterName, ClusterName</td>
<td>The memory that is reserved by tasks in the resource that is specified by the dimension set that you're using.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This metric is collected only for tasks that have a defined memory reservation in their task definition.</td>
</tr>
<tr>
<td>NetworkRxBytes</td>
<td>TaskDefinitionFamily, ClusterName, ServiceName, ClusterName, ClusterName</td>
<td>The number of bytes received by the resource that is specified by the dimensions that you're using.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This metric is available only for containers in tasks using the awsvpc or bridge network modes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes/Second</td>
</tr>
<tr>
<td>Metric name</td>
<td>Dimensions</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>NetworkTxBytes</td>
<td>TaskDefinitionFamily, ClusterName, ServiceName, ClusterName</td>
<td>The number of bytes transmitted by the resource that is specified by the dimensions that you're using. This metric is available only for containers in tasks using the awsvpc or bridge network modes. Unit: Bytes/Second</td>
</tr>
<tr>
<td>PendingTaskCount</td>
<td>ServiceName, ClusterName</td>
<td>The number of tasks currently in the PENDING state. Unit: Count</td>
</tr>
<tr>
<td>RunningTaskCount</td>
<td>ServiceName, ClusterName</td>
<td>The number of tasks currently in the RUNNING state. Unit: Count</td>
</tr>
<tr>
<td>ServiceCount</td>
<td>ClusterName</td>
<td>The number of services in the cluster. Unit: Count</td>
</tr>
<tr>
<td>StorageReadBytes</td>
<td>TaskDefinitionFamily, ServiceName, ClusterName, ClusterName</td>
<td>The number of bytes read from storage in the resource that is specified by the dimensions that you're using. Unit: Bytes</td>
</tr>
<tr>
<td>StorageWriteBytes</td>
<td>TaskDefinitionFamily, ServiceName, ClusterName, ClusterName</td>
<td>The number of bytes written to storage in the resource that is specified by the dimensions that you're using. Unit: Bytes</td>
</tr>
<tr>
<td>TaskCount</td>
<td>ClusterName</td>
<td>The number of tasks running in the cluster. Unit: Count</td>
</tr>
</tbody>
</table>
### Amazon CloudWatch User Guide

#### Amazon ECS Container Insights metrics

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TaskSetCount</td>
<td>ServiceName, ClusterName</td>
<td>The number of task sets in the service. Unit: Count</td>
</tr>
</tbody>
</table>

The following metrics are available when you complete the steps in Deploying the CloudWatch agent to collect EC2 instance-level metrics on Amazon ECS (p. 268)

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>instance_cpu_limit</td>
<td>ClusterName</td>
<td>The maximum number of CPU units that can be assigned to a single EC2 Instance in the cluster.</td>
</tr>
<tr>
<td>instance_cpu_reserved_capacity</td>
<td>ClusterName, Instanceld, ContainerInstanceID,ClusterName</td>
<td>The percentage of CPU currently being reserved on a single EC2 instance in the cluster.</td>
</tr>
<tr>
<td>instance_cpu_usage</td>
<td>ClusterName</td>
<td>The number of CPU units being used on a Single EC2 instance in the cluster.</td>
</tr>
<tr>
<td>instance_cpu_utilization</td>
<td>ClusterName, Instanceld, ContainerInstanceID,ClusterName</td>
<td>The total percentage of CPU units being used on a single EC2 instance in the cluster.</td>
</tr>
<tr>
<td>instance_filesystem_utilization</td>
<td>ClusterName, Instanceld, ContainerInstanceID,ClusterName</td>
<td>The total percentage of file system capacity being used on a single EC2 instance in the cluster.</td>
</tr>
<tr>
<td>instance_memory_limit</td>
<td>ClusterName</td>
<td>The maximum amount of memory, in bytes, that can be assigned to a single EC2 Instance in this cluster.</td>
</tr>
<tr>
<td>instance_memory_reserved_capacity</td>
<td>ClusterName, Instanceld, ContainerInstanceID,ClusterName</td>
<td>The percentage of Memory currently being reserved on a single EC2 Instance in the cluster.</td>
</tr>
<tr>
<td>instance_memory_utilization</td>
<td>ClusterName, Instanceld, ContainerInstanceID,ClusterName</td>
<td>The total percentage of memory being used on a single EC2 Instance in the cluster.</td>
</tr>
<tr>
<td>Metric name</td>
<td>Dimensions</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>instance_memory_working_set</td>
<td>ClusterName</td>
<td>The amount of memory, in bytes, being used on a single EC2 Instance in the cluster.</td>
</tr>
<tr>
<td>instance_network_total_bytes</td>
<td>ClusterName</td>
<td>The total number of bytes per second transmitted and received over the network on a single EC2 Instance in the cluster.</td>
</tr>
<tr>
<td>instance_number_of_running_tasks</td>
<td>ClusterName</td>
<td>The number of running tasks on a single EC2 Instance in the cluster.</td>
</tr>
</tbody>
</table>

### Amazon EKS and Kubernetes Container Insights metrics

The following table lists the metrics and dimensions that Container Insights collects for Amazon EKS and Kubernetes. These metrics are in the `ContainerInsights` namespace. For more information, see Metrics (p. 3).

If you do not see any Container Insights metrics in your console, be sure that you have completed the setup of Container Insights. Metrics do not appear before Container Insights has been set up completely. For more information, see Setting up Container Insights (p. 264).

When you use Container Insights to collect the following metrics, the metrics are charged as custom metrics. For more information about CloudWatch pricing, see Amazon CloudWatch Pricing.

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cluster_failed_node_count</td>
<td>ClusterName</td>
<td>The number of failed worker nodes in the cluster. A node is considered failed if it is suffering from any node conditions. For more information, see Conditions in the Kubernetes documentation.</td>
</tr>
<tr>
<td>cluster_node_count</td>
<td>ClusterName</td>
<td>The total number of worker nodes in the cluster.</td>
</tr>
<tr>
<td>namespace_number_of_running_pods</td>
<td>Namespace ClusterName</td>
<td>The number of pods running per namespace in the resource that is specified by the dimensions that you're using.</td>
</tr>
<tr>
<td>Metric name</td>
<td>Dimensions</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>node_cpu_limit</td>
<td>ClusterName</td>
<td>The maximum number of CPU units that can be assigned to a single node in this cluster.</td>
</tr>
<tr>
<td>node_cpu_reserved_capacity</td>
<td>NodeName, ClusterName, InstanceId, ClusterName</td>
<td>The percentage of CPU units that are reserved for node components, such as kubelet, kube-proxy, and Docker.</td>
</tr>
<tr>
<td>node_cpu_usage_total</td>
<td>ClusterName</td>
<td>The number of CPU units being used on the nodes in the cluster.</td>
</tr>
<tr>
<td>node_cpu_utilization</td>
<td>NodeName, ClusterName, InstanceId, ClusterName</td>
<td>The total percentage of CPU units being used on the nodes in the cluster.</td>
</tr>
<tr>
<td>node_filesystem_utilization</td>
<td>NodeName, ClusterName, InstanceId, ClusterName</td>
<td>The total percentage of file system capacity being used on nodes in the cluster.</td>
</tr>
<tr>
<td>node_memory_limit</td>
<td>ClusterName</td>
<td>The maximum amount of memory, in bytes, that can be assigned to a single node in this cluster.</td>
</tr>
<tr>
<td>node_memory_reserved_capacity</td>
<td>NodeName, ClusterName, InstanceId, ClusterName</td>
<td>The percentage of memory currently being used on the nodes in the cluster.</td>
</tr>
<tr>
<td>node_memory_utilization</td>
<td>NodeName, ClusterName, InstanceId, ClusterName</td>
<td>The percentage of memory currently being used by the node or nodes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>node_memory_utilization is calculated by node_memory_working_set / node_memory_limit. It is the percentage of node memory usage over the node memory limitation.</td>
</tr>
<tr>
<td>node_memory_working_set</td>
<td>ClusterName</td>
<td>The amount of memory, in bytes, being used in the working set of the nodes in the cluster.</td>
</tr>
<tr>
<td>Metric name</td>
<td>Dimensions</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>node_network_total_bytes</td>
<td>NodeName, ClusterName, InstanceId</td>
<td>The total number of bytes per second transmitted and received over the network per node in a cluster.</td>
</tr>
<tr>
<td>node_number_of_running_containers</td>
<td>NodeName, ClusterName, InstanceId</td>
<td>The number of running containers per node in a cluster.</td>
</tr>
<tr>
<td>node_number_of_running_pods</td>
<td>NodeName, ClusterName, InstanceId</td>
<td>The number of running pods per node in a cluster.</td>
</tr>
<tr>
<td>pod_cpu_reserved_capacity</td>
<td>PodName, Namespace, ClusterName</td>
<td>The CPU capacity that is reserved per pod in a cluster.</td>
</tr>
<tr>
<td>pod_cpu_utilization</td>
<td>PodName, Namespace, ClusterName</td>
<td>The percentage of CPU units being used by pods.</td>
</tr>
<tr>
<td>pod_cpu_utilization</td>
<td>PodName, Namespace, ClusterName</td>
<td>The percentage of CPU units being used by pods that is over the pod limit.</td>
</tr>
<tr>
<td>pod_memory_reserved_capacity</td>
<td>PodName, Namespace, ClusterName</td>
<td>The percentage of memory that is reserved for pods.</td>
</tr>
<tr>
<td>pod_memory_utilization</td>
<td>PodName, Namespace, ClusterName</td>
<td>The percentage of memory currently being used by the pod or pods.</td>
</tr>
<tr>
<td>pod_memory_utilization</td>
<td>PodName, Namespace, ClusterName</td>
<td>The percentage of memory that is being used by pods that is over the pod limit.</td>
</tr>
<tr>
<td>pod_number_of_container_restarts</td>
<td>PodName, Namespace, ClusterName</td>
<td>The total number of container restarts in a pod.</td>
</tr>
</tbody>
</table>
Container Insights performance log reference

This section includes reference information about how Container Insights uses performance log events to collect metrics.

Topics

- Container Insights performance log events for Amazon ECS (p. 306)
- Container Insights performance log events for Amazon EKS and Kubernetes (p. 309)
- Relevant fields in performance log events for Amazon EKS and Kubernetes (p. 320)

Container Insights performance log events for Amazon ECS

The following are examples of the performance log events that Container Insights collects from Amazon ECS.

Type: Container

```json
{
  "Version":"0",
  "Type":"Container",
  "ContainerName":"sleep",
  "TaskId":"7ac4dfba69214411b4783a3b8189c9ba",
  "TaskDefinitionFamily":"sleep360",
  "TaskDefinitionRevision":"1",
  "ContainerInstanceId":"0d7650e6dec34c1a9200f72098071e8f",
  "EC2InstanceId":"i-0c47379d9bdc6f30",
  "ClusterName":"MyCluster",
  "Image":"busybox",
  "ContainerKnownStatus":"RUNNING",
  "Timestamp":1623963900000,
  "CpuUtilized":0.0,
  "PodName":null,
  "PodNamespace":null,
  "PodClusterName":null,
  "Namespace":null,
  "ClusterName":null,
  "Service":null,
  "Namespace":null,
  "ClusterName":null,
  "Dimensions":null
}
```
Type: Task

```json
{
  "Version": "0",
  "Type": "Task",
  "TaskId": "7ac4dfba69214411b4783a3b8189c9ba",
  "TaskDefinitionFamily": "sleep360",
  "TaskDefinitionRevision": "1",
  "ContainerInstanceARN": "9d7650e6dec34c1a9200f72098071e8f",
  "EC2InstanceId": "i-0c470579dbd2f3",
  "ClusterName": "MyCluster",
  "AccountID": "637146863587",
  "Region": "us-west-2",
  "AvailabilityZone": "us-west-2b",
  "KnownStatus": "RUNNING",
  "LaunchType": "EC2",
  "PullStartedAt": 1623963608201,
  "PullStoppedAt": 1623963610065,
  "CreatedAt": 1623963607094,
  "StartedAt": 1623963610382,
  "Timestamp": 1623963900000,
  "CpuUtilized": 0.0,
  "CpuReserved": 10.0,
  "MemoryUtilized": 0,
  "MemoryReserved": 10,
  "StorageReadBytes": 0,
  "StorageWriteBytes": 0,
  "NetworkRxBytes": 0,
  "NetworkRxDropped": 0,
  "NetworkRxErrors": 0,
  "NetworkRxPackets": 14,
  "NetworkTxBytes": 0,
  "NetworkTxDropped": 0,
  "NetworkTxErrors": 0,
  "NetworkTxPackets": 0,
  "CloudWatchMetrics": [
    {
      "Namespace": "ECS/ContainerInsights",
      "Metrics": [
        {
          "Name": "CpuUtilized",
          "Unit": "None"
        },
        {
          "Name": "CpuReserved",
          "Unit": "None"
        },
        {
          "Name": "MemoryUtilized",
          "Unit": "Megabytes"
        }
      ]
    }
  ]
}
```
"Name": "MemoryReserved",
"Unit": "Megabytes"
},
{
"Name": "StorageReadBytes",
"Unit": "Bytes/Second"
},
{
"Name": "StorageWriteBytes",
"Unit": "Bytes/Second"
},
{
"Name": "NetworkRxBytes",
"Unit": "Bytes/Second"
},
{
"Name": "NetworkTxBytes",
"Unit": "Bytes/Second"
}
],
"Dimensions": [
[
"ClusterName"
],
[
"ClusterName",
"TaskDefinitionFamily"
]
]
}
}

**Type: Service**

{
"Version": "0",
"Type": "Service",
"ServiceName": "myCIService",
"ClusterName": "myCICluster",
"Timestamp": 1561586460000,
"DesiredTaskCount": 2,
"RunningTaskCount": 2,
"PendingTaskCount": 0,
"DeploymentCount": 1,
"TaskSetCount": 0,
"CloudWatchMetrics": [
{
"Namespace": "ECS/ContainerInsights",
"Metrics": [
{
"Name": "DesiredTaskCount",
"Unit": "Count"
},
{
"Name": "RunningTaskCount",
"Unit": "Count"
},
{
"Name": "PendingTaskCount",
"Unit": "Count"
},
{
"Name": "DeploymentCount",
"Unit": "Count"
}
]}
}
Container Insights performance log events for Amazon EKS and Kubernetes

The following are examples of the performance log events that Container Insights collects from Amazon EKS and Kubernetes clusters.

**Type: Node**

```json
{}
```
"AutoScalingGroupName": "eksctl-myCICluster-nodegroup-standard-workers-
NodeGroup-1174PV2WHZAYU",
"CloudWatchMetrics": [
{
  "Metrics": [
    {
      "Unit": "Percent",
      "Name": "node_cpu_utilization"
    },
    {
      "Unit": "Percent",
      "Name": "node_memory_utilization"
    },
    {
      "Unit": "Bytes/Second",
      "Name": "node_network_total_bytes"
    },
    {
      "Unit": "Percent",
      "Name": "node_cpu_reserved_capacity"
    },
    {
      "Unit": "Percent",
      "Name": "node_memory_reserved_capacity"
    },
    {
      "Unit": "Count",
      "Name": "node_number_of_running_pods"
    },
    {
      "Unit": "Count",
      "Name": "node_number_of_running_containers"
    }
  ],
  "Dimensions": [
    [
      "NodeName",
      "InstanceId",
      "ClusterName"
    ]
  ],
  "Namespace": "ContainerInsights"
},
{
  "Metrics": [
    {
      "Unit": "Percent",
      "Name": "node_cpu_utilization"
    },
    {
      "Unit": "Percent",
      "Name": "node_memory_utilization"
    },
    {
      "Unit": "Bytes/Second",
      "Name": "node_network_total_bytes"
    },
    {
      "Unit": "Percent",
      "Name": "node_cpu_reserved_capacity"
    },
    {
      "Unit": "Percent",
      "Name": "node_memory_reserved_capacity"
    }
  ]}
```
"Unit": "Count",
"Name": "node_number_of_running_pods"
},

"Unit": "Count",
"Name": "node_number_of_running_containers"
},

"Name": "node_cpu_usage_total"
},

"Name": "node_cpu_limit"
},

"Unit": "Bytes",
"Name": "node_memory_working_set"
},

"Unit": "Bytes",
"Name": "node_memory_limit"
],
"Dimensions": [

"ClusterName"
]
},
"Namespace": "ContainerInsights"
},

"ClusterName": "myCICluster",
"InstanceId": "i-1234567890123456",
"InstanceType": "t3.xlarge",
"NodeName": "ip-192-0-2-0.us-west-2.compute.internal",
"Sources": [

"cadvisor",
"/proc",
"pod",
"calculated"
],
"Timestamp": "1567096682364",
"Type": "Node",
"Version": "0",
"kubernetes": {

"host": "ip-192-168-75-26.us-west-2.compute.internal",

"node_cpu_limit": 4000,
"node_cpu_request": 1130,
"node_cpu_reserved_capacity": 28.249999999999996,
"node_cpu_usage_system": 33.794636630852764,
"node_cpu_usage_total": 136.47852169244098,
"node_cpu_usage_user": 71.67075111567326,
"node_cpu_utilization": 3.4119630423110245,
"node_memory_cache": 3103297536,
"node_memory_failcnt": 0,
"node_memory_hierarchical_pgfault": 0,
"node_memory_hierarchical_pgmajfault": 0,
"node_memory_limit": 16624865280,
"node_memory_mapped_file": 406646784,
"node_memory_max_usage": 4230746112,
"node_memory_pgfault": 0,
"node_memory_pgfault": 0,
"node_memory_pgmajfault": 0,
"node_memory_request": 1115684864,
"node_memory_reserved_capacity": 6.7109407818311055,
"node_memory_rss": 798146560,
"node_memory_swap": 0,
```
"node_memory_usage": 3901444096,
"node_memory_utilization": 6.601302600149552,
"node_memory_working_set": 1097457664,
"node_network_rx_bytes": 35918.392817386324,
"node_network_rx_dropped": 0,
"node_network_rx_errors": 0,
"node_network_rx_packets": 157.6756524548117,
"node_network_total_bytes": 68264.20276554905,
"node_network_tx_bytes": 32345.80994816272,
"node_network_tx_dropped": 0,
"node_network_tx_errors": 0,
"node_network_tx_packets": 154.21455923431654,
"node_number_of_running_containers": 16,
"node_number_of_running_pods": 13
}

Type: NodeFS

```json
{
    "AutoScalingGroupName": "eksctl-myCICluster-nodegroup-standard-workers-NodeGroup-1174PV2WHZAYU",
    "CloudWatchMetrics": [
        {
            "Metrics": [
                {
                    "Unit": "Percent",
                    "Name": "node_filesystem_utilization"
                }
            ],
            "Dimensions": [
                [
                    "NodeName",
                    "InstanceId",
                    "ClusterName"
                ],
                [
                    "ClusterName"
                ]
            ],
            "Namespace": "ContainerInsights"
        }
    ],
    "ClusterName": "myCICluster",
    "EBSVolumeId": "aws://us-west-2b/vol-0a53108976d4a2fda",
    "InstanceId": "i-1234567890123456",
    "InstanceType": "t3.xlarge",
    "NodeName": "ip-192-0-2-0.us-west-2.compute.internal",
    "Sources": [
        "cadvisor",
        "calculated"
    ],
    "Timestamp": "1567097939726",
    "Type": "NodeFS",
    "Version": "0",
    "device": "/dev/nvme0n1p1",
    "fstype": "vfs",
    "kubernetes": {
        "host": "ip-192-168-75-26.us-west-2.compute.internal"
    },
    "node_filesystem_available": 17298395136,
    "node_filesystem_capacity": 21462233088,
    "node_filesystem_inodes": 10484720,
    "node_filesystem_inodes_free": 10367158,
    "node_filesystem_usage": 4163837952,
    "node_filesystem_utilization": 19.400767547940255
}
Type: NodeDiskIO

```
{
  "AutoScalingGroupName": "eksctl-myCICluster-nodegroup-standard-workers-
  NodeGroup-1174FV2WHZAYU",
  "ClusterName": "myCICluster",
  "EBSVolumeId": "aws://us-west-2b/vol-0a53108976d4a2fda",
  "InstanceId": "i-1234567890123456",
  "InstanceType": "t3.xlarge",
  "NodeName": "ip-192-0-2-0.us-west-2.compute.internal",
  "Sources": [
    "cadvisor",
  ],
  "Timestamp": "1567096928131",
  "Type": "NodeDiskIO",
  "Version": "0",
  "device": "/dev/nvme0n1",
  "kubernetes": {
    "host": "ip-192-168-75-26.us-west-2.compute.internal"
  },
  "node_diskio_io_service_bytes_async": 9750.505814277016,
  "node_diskio_io_service_bytes_read": 0,
  "node_diskio_io_service_bytes_sync": 230.6174506688036,
  "node_diskio_io_service_bytes_total": 9981.123264945818,
  "node_diskio_io_service_bytes_write": 9981.123264945818,
  "node_diskio_io_serviced_async": 1.153087253344018,
  "node_diskio_ioserviced_read": 0,
  "node_diskio_io_serviced_sync": 0.03603397666700056,
  "node_diskio_io_serviced_total": 1.1891212300110185,
  "node_diskio_io_serviced_write": 1.1891212300110185
}
```

Type: NodeNet

```
{
  "AutoScalingGroupName": "eksctl-myCICluster-nodegroup-standard-workers-
  NodeGroup-1174FV2WHZAYU",
  "ClusterName": "myCICluster",
  "InstanceId": "i-1234567890123456",
  "InstanceType": "t3.xlarge",
  "NodeName": "ip-192-0-2-0.us-west-2.compute.internal",
  "Sources": [
    "cadvisor",
    "calculated"
  ],
  "Timestamp": "1567096928131",
  "Type": "NodeNet",
  "Version": "0",
  "interface": "eni972f6bfa9a0",
  "kubernetes": {
    "host": "ip-192-168-75-26.us-west-2.compute.internal"
  },
  "node_interface_network_rx_bytes": 3163.008420864309,
  "node_interface_network_rx_dropped": 0,
  "node_interface_network_rx_errors": 0,
  "node_interface_network_rx_packets": 16.575629266800258,
  "node_interface_network_total_bytes": 3518.3935157426017,
  "node_interface_network_tx_bytes": 355.3850947872893,
  "node_interface_network_tx_dropped": 0,
  "node_interface_network_tx_errors": 0,
  "node_interface_network_tx_packets": 3.9997714100370625
}
```
Type: Pod

```json
{
   "AutoScalingGroupName": "eksctl-myCICluster-nodegroup-standard-workers-
NodeGroup-1174PV2WHZAYU",
   "CloudWatchMetrics": [
      {
         "Metrics": [
            {
               "Unit": "Percent",
               "Name": "pod_cpu_utilization"
            },
            {
               "Unit": "Percent",
               "Name": "pod_memory_utilization"
            },
            {
               "Unit": "Bytes/Second",
               "Name": "pod_network_rx_bytes"
            },
            {
               "Unit": "Bytes/Second",
               "Name": "pod_network_tx_bytes"
            },
            {
               "Unit": "Percent",
               "Name": "pod_cpu_utilization_over_pod_limit"
            },
            {
               "Unit": "Percent",
               "Name": "pod_memory_utilization_over_pod_limit"
            }
         ],
         "Dimensions": [
            [
               "PodName",
               "Namespace",
               "ClusterName"
            ],
            [
               "Service",
               "Namespace",
               "ClusterName"
            ],
            [
               "Namespace",
               "ClusterName"
            ],
            [
               "ClusterName"
            ],
            "Namespace": "ContainerInsights"
         ],
      },
      {"Metrics": [
         {
            "Unit": "Percent",
            "Name": "pod_cpu_reserved_capacity"
         },
         {"Unit": "Percent",
            "Name": "pod_memory_reserved_capacity"
         }
      ]
   }
}
```
"Dimensions": [  [    "PodName",    "Namespace",    "ClusterName"  ],  [    "ClusterName"  ]  ],  "Namespace": "ContainerInsights"},  "Metrics": [  {    "Unit": "Count",    "Name": "pod_number_of_container restarts"  }],  "Dimensions": [  [    "PodName",    "Namespace",    "ClusterName"  ]],  "Namespace": "ContainerInsights"},  "ClusterName": "myCICluster",  "InstanceId": "i-1234567890123456",  "InstanceType": "t3.xlarge",  "Namespace": "amazon-cloudwatch",  "NodeName": "ip-192-0-2-0.us-west-2.compute.internal",  "PodName": "cloudwatch-agent-statsd",  "Service": "cloudwatch-agent-statsd",  "Sources": [    "cadvisor",    "pod",    "calculated"  ],  "Timestamp": "1567097351092",  "Type": "Pod",  "Version": "0",  "kubernetes": {    "host": "ip-192-168-75-26.us-west-2.compute.internal",    "labels": {      "app": "cloudwatch-agent-statsd",      "pod-template-hash": "df44f855f"    },    "namespace_name": "amazon-cloudwatch",    "pod_id": "2f4ff5ac-c813-11e9-a31d-06e9ddee32928",    "pod_name": "cloudwatch-agent-statsd-df44f855f-ts4q2",    "pod_owners": [      {        "owner_kind": "Deployment",        "owner_name": "cloudwatch-agent-statsd"      }    ],    "service_name": "cloudwatch-agent-statsd"  },  "pod_cpu_limit": 200,  "pod_cpu_request": 200,  "pod_cpu_reserved_capacity": 5,
"pod_cpu_usage_system": 1.4504841104992765,
"pod_cpu_usage_total": 5.817016867430125,
"pod_cpu_usage_user": 1.1281543081661038,
"pod_cpu_utilization": 0.1454254216857600,
"pod_cpu_utilization_over_pod_limit": 2.9085084337150624,
"pod_memory_cache": 8192,
"pod_memory_failcnt": 0,
"pod_memory_hierarchical_pgfault": 0,
"pod_memory_hierarchical_pgmajfault": 0,
"pod_memory_limit": 104857600,
"pod_memory_mapped_file": 0,
"pod_memory_max_usage": 25268224,
"pod_memory_pgfault": 0,
"pod_memory_pgmajfault": 0,
"pod_memory_request": 104857600,
"pod_memory_reserved_capacity": 0.6307275170893897,
"pod_memory_rss": 22777856,
"pod_memory_swap": 0,
"pod_memory_swap_usage": 25141248,
"pod_memory_total_bytes": 10158.829201483635,
"pod_network_rx_bytes": 9880.697124714186,
"pod_network_rx_dropped": 0,
"pod_network_rx_errors": 0,
"pod_network_rx_packets": 107.80005532263283,
"pod_network_total_bytes": 10158.829201483635,
"pod_network_tx_bytes": 278.13207676944796,
"pod_network_tx_dropped": 0,
"pod_network_tx_errors": 0,
"pod_number_of_container_restarts": 0,
"pod_number_of_containers": 1,
"pod_number_of_running_containers": 1,
"pod_status": "Running"}

**Type: PodNet**

```json
{
    "AutoScalingGroupName": "eksctl-myCICluster-nodegroup-standard-workers-
NodeGroup-1174PVZWHZAYU",
    "ClusterName": "myCICluster",
    "InstanceId": "i-1234567890123456",
    "InstanceType": "t3.xlarge",
    "Namespace": "amazon-cloudwatch",
    "NodeName": "ip-192-0-2-0.us-west-2.compute.internal",
    "PodName": "cloudwatch-agent-statsd",
    "Service": "cloudwatch-agent-statsd",
    "Sources": [
        "cadvisor",
        "calculated"
    ],
    "Timestamp": "1567097351092",
    "Type": "PodNet",
    "Version": "0",
    "interface": "eth0",
    "kubernetes": {
        "host": "ip-192-168-75-26.us-west-2.compute.internal",
        "labels": {
            "app": "cloudwatch-agent-statsd",
            "pod-template-hash": "df4f855f"
        },
        "namespace_name": "amazon-cloudwatch",
        "pod_id": "2f4ff5ac-c813-11e9-a31d-06e9dde32928",
```
"pod_name": "cloudwatch-agent-statsd-df44f855f-ts4q2",
"pod_owners": [
  {
    "owner_kind": "Deployment",
    "owner_name": "cloudwatch-agent-statsd"
  }
],
"service_name": "cloudwatch-agent-statsd",
"pod_interface_network_rx_bytes": 9880.697124714186,
"pod_interface_network_rx_dropped": 0,
"pod_interface_network_rx_errors": 0,
"pod_interface_network_rx_packets": 107.80005532263283,
"pod_interface_network_total_bytes": 10158.829201483635,
"pod_interface_network_tx_bytes": 278.13207676944796,
"pod_interface_network_tx_dropped": 0,
"pod_interface_network_tx_errors": 0,
"pod_interface_network_tx_packets": 1.146027574644318
}

Type: Container

{
  "AutoScalingGroupName": "eksctl-myCICluster-nodegroup-standard-workers-NodeGroup-sample",
  "ClusterName": "myCICluster",
  "InstanceId": "i-1234567890123456",
  "InstanceType": "t3.xlarge",
  "Namespace": "amazon-cloudwatch",
  "NodeName": "ip-192-0-2-0.us-west-2.compute.internal",
  "PodName": "cloudwatch-agent-statsd",
  "Service": "cloudwatch-agent-statsd",
  "Sources": [
  "cadvisor",
  "pod",
  "calculated"
  ],
  "Timestamp": "1567097399912",
  "Type": "Container",
  "Version": "0",
  "container_cpu_limit": 200,
  "container_cpu_request": 200,
  "container_cpu_usage_system": 1.87958283771964,
  "container_cpu_usage_total": 6.159993652997942,
  "container_cpu_usage_user": 1.6707403001952357,
  "container_cpu_utilization": 0.15399984132494854,
  "container_memory_cache": 8192,
  "container_memory_failcnt": 0,
  "container_memory_hierarchical_pgfault": 0,
  "container_memory_hierarchical_pgmajfault": 0,
  "container_memory_limit": 104857600,
  "container_memory_mapped_file": 0,
  "container_memory_max_usage": 24580096,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_max_usage": 24580096,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
  "container_memory_majpage": 0,
},
"host": "ip-192-168-75-26.us-west-2.compute.internal",
"labels": {
  "app": "cloudwatch-agent-statsd",
  "pod-template-hash": "df44f855f"
},
"namespace_name": "amazon-cloudwatch",
"pod_id": "2f4ff3ac-c813-11e9-a31d-06e9de32928",
"pod_name": "cloudwatch-agent-statsd-df44f855f-ts4q2",
"pod_owners": [
  {
    "owner_kind": "Deployment",
    "owner_name": "cloudwatch-agent-statsd"
  }
],
"service_name": "cloudwatch-agent-statsd",
"number_of_container_restarts": 0
}

Type: ContainerFS

{
"AutoScalingGroupName": "eksctl-myCICluster-nodegroup-standard-workers-NodeGroup-1174F52W8ZAYU",
"ClusterName": "myCICluster",
"EBSVolumeId": "aws://us-west-2b/vol-0a53108976d4a2fda",
"InstanceType": "t3.xlarge",
"Namespace": "amazon-cloudwatch",
"NodeName": "ip-192-0-2-0.us-west-2.compute.internal",
"PodName": "cloudwatch-agent-statsd",
"Service": "cloudwatch-agent-statsd",
"Sources": [
  {"cadvisor",
  "calculated"
},
"Timestamp": "1567097399912",
"Type": "ContainerFS",
"Version": "0",
"container_filesystem_available": 0,
"container_filesystem_capacity": 21462233088,
"container_filesystem_usage": 24576,
"container_filesystem_utilization": 0.0001145081217748071,
"device": "/dev/nvme0n1p1",
"fstype": "vfs",
"kubernetes": {
  "container_name": "cloudwatch-agent",
  "docker": {
    "container_id": "8967b6b37da239dfad197c9fdeaa3e5dfd35a8a759ec86e2e4c3f7b401e232706"
  },
  "host": "ip-192-168-75-26.us-west-2.compute.internal",
  "labels": {
    "app": "cloudwatch-agent-statsd",
    "pod-template-hash": "df44f855f"
  },
  "namespace_name": "amazon-cloudwatch",
  "pod_id": "2f4ff3ac-c813-11e9-a31d-06e9de32928",
  "pod_name": "cloudwatch-agent-statsd-df44f855f-ts4q2",
  "pod_owners": [
    {
      "owner_kind": "Deployment",
      "owner_name": "cloudwatch-agent-statsd"
    }
  ]
},

318
"service_name": "cloudwatch-agent-statsd"
}
}

Type: Cluster

{
"CloudWatchMetrics": [
{
"Metrics": [
{
"Unit": "Count",
"Name": "cluster_node_count"
},
{
"Unit": "Count",
"Name": "cluster_failed_node_count"
}
],
"Dimensions": [
["ClusterName"
],
"Namespace": "ContainerInsights"
},
"ClusterName": "myCICluster",
"Sources": ["apiserver"
],
"Timestamp": "1567097534160",
"Type": "Cluster",
"Version": "0",
"cluster_failed_node_count": 0,
"cluster_node_count": 3
}

Type: ClusterService

{
"CloudWatchMetrics": [
{
"Metrics": [
{
"Unit": "Count",
"Name": "service_number_of_running_pods"
}
],
"Dimensions": [
["Service",
"Namespace",
"ClusterName"
],
["ClusterName"
],
"Namespace": "ContainerInsights"
},
"ClusterName": "myCICluster",
"Namespace": "amazon-cloudwatch",
"version": "0.0.1"
]
Relevant fields in performance log events for Amazon EKS and Kubernetes

For Amazon EKS and Kubernetes, the containerized CloudWatch agent emits data as performance log events. This enables CloudWatch to ingest and store high-cardinality data. CloudWatch uses the data in the performance log events to create aggregated CloudWatch metrics at the cluster, node, and pod levels without the need to lose granular details.

The following table lists the fields in these performance log events that are relevant to the collection of Container Insights metric data. You can use CloudWatch Logs Insights to query for any of these fields.
to collect data or investigate issues. For more information, see Analyze Log Data With CloudWatch Logs Insights.

<table>
<thead>
<tr>
<th>Type</th>
<th>Log field</th>
<th>Source</th>
<th>Formula or notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pod</td>
<td>pod_cpu_utilization</td>
<td>Calculated</td>
<td>Formula: pod_cpu_usage_total / node_cpu_limit</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_cpu_usage_total</td>
<td>cadvisor</td>
<td></td>
</tr>
<tr>
<td>Pod</td>
<td>pod_cpu_limit</td>
<td>Calculated</td>
<td>Formula: sum(container_cpu_limit)</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_cpu_request</td>
<td>Calculated</td>
<td>Formula: sum(container_cpu_request)</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_cpu_utilization_over_pod_limit</td>
<td>Calculated</td>
<td>Formula: pod_cpu_usage_total / pod_cpu_limit</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_cpu_reserved_capacity</td>
<td>Calculated</td>
<td>Formula: pod_cpu_request / node_cpu_limit</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_memory_utilization</td>
<td>Calculated</td>
<td>Formula: pod_memory_working_set / node_memory_limit</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_memory_working_set</td>
<td>cadvisor</td>
<td></td>
</tr>
<tr>
<td>Pod</td>
<td>pod_memory_limit</td>
<td>Calculated</td>
<td>Formula: sum(container_memory_limit)</td>
</tr>
<tr>
<td>Type</td>
<td>Log field</td>
<td>Source</td>
<td>Formula or notes</td>
</tr>
<tr>
<td>------</td>
<td>-----------</td>
<td>--------</td>
<td>-----------------</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_memory_request</td>
<td>Calculated</td>
<td>Formula: (\text{sum(container_memory_request)}) &lt;br&gt; Container_memory_request isn't guaranteed to be set. Only the ones that are set are included in the sum.</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_memory_utilization_over_pod_limit</td>
<td>Calculated</td>
<td>Formula: (\frac{\text{pod_memory_working_set}}{\text{pod_memory_limit}}) &lt;br&gt; If any containers in the pod don't have a memory limit defined, this field doesn't appear in the log event.</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_memory_reserved_capacity</td>
<td>Calculated</td>
<td>Formula: (\frac{\text{pod_memory_request}}{\text{node_memory_limit}})</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_network_tx_bytes</td>
<td>Calculated</td>
<td>Formula: (\text{sum(pod_interface_network_tx_bytes)}) &lt;br&gt; This data is available for all the network interfaces per pod. The CloudWatch agent calculates the total and adds metric extraction rules.</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_network_rx_bytes</td>
<td>Calculated</td>
<td>Formula: (\text{sum(pod_interface_network_rx_bytes)})</td>
</tr>
<tr>
<td>Pod</td>
<td>pod_network_total_bytes</td>
<td>Calculated</td>
<td>Formula: (\text{pod_network_rx_bytes} + \text{pod_network_tx_bytes})</td>
</tr>
</tbody>
</table>
## Relevant fields in performance log events for Amazon EKS and Kubernetes

<table>
<thead>
<tr>
<th>Type</th>
<th>Log field</th>
<th>Source</th>
<th>Formula or notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PodNet</td>
<td>pod_interface_network_rx_bytes</td>
<td>cadvisor</td>
<td>This data is network rx bytes per second of a pod network interface.</td>
</tr>
<tr>
<td>PodNet</td>
<td>pod_interface_network_tx_bytes</td>
<td>cadvisor</td>
<td>This data is network tx bytes per second of a pod network interface.</td>
</tr>
<tr>
<td>Container</td>
<td>container_cpu_usage_total</td>
<td>cadvisor</td>
<td></td>
</tr>
<tr>
<td>Container</td>
<td>container_cpu_limit</td>
<td>cadvisor</td>
<td>Not guaranteed to be set. It's not emitted if it's not set.</td>
</tr>
<tr>
<td>Container</td>
<td>container_cpu_request</td>
<td>cadvisor</td>
<td>Not guaranteed to be set. It's not emitted if it's not set.</td>
</tr>
<tr>
<td>Container</td>
<td>container_memory_working_set</td>
<td>cadvisor</td>
<td></td>
</tr>
<tr>
<td>Container</td>
<td>container_memory_limit</td>
<td>pod</td>
<td>Not guaranteed to be set. It's not emitted if it's not set.</td>
</tr>
<tr>
<td>Container</td>
<td>container_memory_request</td>
<td>pod</td>
<td>Not guaranteed to be set. It's not emitted if it's not set.</td>
</tr>
<tr>
<td>ContainerFS</td>
<td>container_filesystem_capacity</td>
<td>pod</td>
<td>This data is available per disk device.</td>
</tr>
<tr>
<td>ContainerFS</td>
<td>container_filesystem_usage</td>
<td>pod</td>
<td>This data is available per disk device.</td>
</tr>
<tr>
<td>ContainerFS</td>
<td>container_filesystem_utilization</td>
<td>Calculated</td>
<td>Formula: container_filesystem_usage / container_filesystem_capacity</td>
</tr>
<tr>
<td>Node</td>
<td>node_cpu_utilization</td>
<td>Calculated</td>
<td>Formula: node_cpu_usage_total / node_cpu_limit</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Type</th>
<th>Log field</th>
<th>Source</th>
<th>Formula or notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>node_cpu_usage_total</td>
<td>cadvisor</td>
<td></td>
</tr>
<tr>
<td>Node</td>
<td>node_cpu_limit</td>
<td>/proc</td>
<td></td>
</tr>
<tr>
<td>Node</td>
<td>node_cpu_request</td>
<td>Calculated</td>
<td>Formula: sum(pod_cpu_request)</td>
</tr>
<tr>
<td>Node</td>
<td>node_cpu_reserved_capacity</td>
<td>Calculated</td>
<td>Formula: node_cpu_request / node_cpu_limit</td>
</tr>
<tr>
<td>Node</td>
<td>node_memory_utilization</td>
<td>Calculated</td>
<td>Formula: node_memory_working_set / node_memory_limit</td>
</tr>
<tr>
<td>Node</td>
<td>node_memory_working_set</td>
<td>cadvisor</td>
<td></td>
</tr>
<tr>
<td>Node</td>
<td>node_memory_limit</td>
<td>/proc</td>
<td></td>
</tr>
<tr>
<td>Node</td>
<td>node_memory_request</td>
<td>Calculated</td>
<td>Formula: sum(pod_memory_request)</td>
</tr>
<tr>
<td>Node</td>
<td>node_memory_reserved_capacity</td>
<td>Calculated</td>
<td>Formula: node_memory_request / node_memory_limit</td>
</tr>
<tr>
<td>Node</td>
<td>node_network_rx_bytes</td>
<td>Calculated</td>
<td>Formula: sum(node_interface_network_rx_bytes)</td>
</tr>
<tr>
<td>Node</td>
<td>node_network_tx_bytes</td>
<td>Calculated</td>
<td>Formula: sum(node_interface_network_tx_bytes)</td>
</tr>
<tr>
<td>Node</td>
<td>node_network_total_bytes</td>
<td>Calculated</td>
<td>Formula: node_network_rx_bytes + node_network_tx_bytes</td>
</tr>
<tr>
<td>Node</td>
<td>node_number_of_running_pods</td>
<td>Pod List</td>
<td></td>
</tr>
<tr>
<td>Node</td>
<td>node_number_of_running_containers</td>
<td>Pod List</td>
<td></td>
</tr>
<tr>
<td>NodeNet</td>
<td>node_interface_network_rx_bytes</td>
<td>cadvisor</td>
<td>This data is network rx bytes per second of a worker node network interface.</td>
</tr>
<tr>
<td>NodeNet</td>
<td>node_interface_network_tx_bytes</td>
<td>cadvisor</td>
<td>This data is network tx bytes per second of a worker node network interface.</td>
</tr>
<tr>
<td>NodeFS</td>
<td>node_filesystem_capacity</td>
<td>cadvisor</td>
<td></td>
</tr>
</tbody>
</table>
Relevant fields in performance log events for Amazon EKS and Kubernetes

<table>
<thead>
<tr>
<th>Type</th>
<th>Log field</th>
<th>Source</th>
<th>Formula or notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>NodeFS</td>
<td>node_filesystem_usage</td>
<td>cadvisor</td>
<td></td>
</tr>
<tr>
<td>NodeFS</td>
<td>node_filesystem_utilization</td>
<td>Calculated</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Formula: node_filesystem_usage / node_filesystem_capacity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This data is available per device name.</td>
</tr>
<tr>
<td>Cluster</td>
<td>cluster_failed_node_count</td>
<td>API Server</td>
<td></td>
</tr>
<tr>
<td>Cluster</td>
<td>cluster_node_count</td>
<td>API Server</td>
<td></td>
</tr>
<tr>
<td>Service</td>
<td>service_number_of_running_pods</td>
<td>API Server</td>
<td></td>
</tr>
<tr>
<td>Namespace</td>
<td>namespace_number_of_running_pods</td>
<td>API Server</td>
<td></td>
</tr>
</tbody>
</table>

Metrics calculation examples

This section includes examples that show how some of the values in the preceding table are calculated.

Suppose that you have a cluster in the following state.

```plaintext
Node1
  node_cpu_limit = 4
  node_cpu_usage_total = 3

Pod1
  pod_cpu_usage_total = 2

  Container1
    container_cpu_limit = 1
    container_cpu_request = 1
    container_cpu_usage_total = 0.8

  Container2
    container_cpu_limit = null
    container_cpu_request = null
    container_cpu_usage_total = 1.2

Pod2
  pod_cpu_usage_total = 0.4

  Container3
    container_cpu_limit = 1
    container_cpu_request = 0.5
    container_cpu_usage_total = 0.4

Node2
  node_cpu_limit = 8
  node_cpu_usage_total = 1.5

Pod3
  pod_cpu_usage_total = 1

  Container4
    container_cpu_limit = 2
```
Container Insights Prometheus metrics monitoring

CloudWatch Container Insights monitoring for Prometheus automates the discovery of Prometheus metrics from containerized systems and workloads. Prometheus is an open-source systems monitoring and alerting toolkit. For more information, see What is Prometheus? in the Prometheus documentation.

Discovering Prometheus metrics is supported for Amazon Elastic Container Service, Amazon Elastic Kubernetes Service and Kubernetes clusters running on Amazon EC2 instances. The Prometheus counter, gauge, and summary metric types are collected. Support for histogram metrics is planned for an upcoming release.

For Amazon ECS and Amazon EKS clusters, both the EC2 and Fargate launch types are supported. Container Insights automatically collects metrics from several workloads, and you can configure it to collect metrics from any workload.

You can adopt Prometheus as an open-source and open-standard method to ingest custom metrics in CloudWatch. The CloudWatch agent with Prometheus support discovers and collects Prometheus metrics to monitor, troubleshoot, and alarm on application performance degradation and failures faster. This also reduces the number of monitoring tools required to improve observability.

Container Insights Prometheus support involves pay-per-use of metrics and logs, including collecting, storing, and analyzing. For more information, see Amazon CloudWatch Pricing.

Pre-built dashboards for some workloads
Set up and configure Prometheus metrics collection on Amazon ECS clusters

To collect Prometheus metrics from Amazon ECS clusters, you can use the CloudWatch agent as a collector or use the AWS Distro for OpenTelemetry collector. For information about using the AWS Distro for OpenTelemetry collector, see [https://aws-otel.github.io/docs/getting-started/container-insights/ecs-prometheus](https://aws-otel.github.io/docs/getting-started/container-insights/ecs-prometheus).

The following sections explain how to use the CloudWatch agent as the collector to retrieve Prometheus metrics. You install the CloudWatch agent with Prometheus monitoring on clusters running Amazon ECS, and you can optionally configure the agent to scrape additional targets. These sections also provide optional tutorials for setting up sample workloads to use for testing with Prometheus monitoring.

Container Insights on Amazon ECS supports the following launch type and network mode combinations for Prometheus metrics:

<table>
<thead>
<tr>
<th>Amazon ECS launch type</th>
<th>Network modes supported</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2 (Linux)</td>
<td>bridge, host, and awsvpc</td>
</tr>
<tr>
<td>Fargate</td>
<td>awsvpc</td>
</tr>
</tbody>
</table>

**VPC security group requirements**

The ingress rules of the security groups for the Prometheus workloads must open the Prometheus ports to the CloudWatch agent for scraping the Prometheus metrics by the private IP.

The egress rules of the security group for the CloudWatch agent must allow the CloudWatch agent to connect to the Prometheus workloads' port by private IP.
Topics

- Install the CloudWatch agent with Prometheus metrics collection on Amazon ECS clusters (p. 328)
- Scraping additional Prometheus sources and importing those metrics (p. 332)
- (Optional) Set up sample containerized Amazon ECS workloads for Prometheus metric testing (p. 341)

Install the CloudWatch agent with Prometheus metrics collection on Amazon ECS clusters

This section explains how to set up the CloudWatch agent with Prometheus monitoring in a cluster running Amazon ECS. After you do this, the agent automatically scrapes and imports metrics for the following workloads running in that cluster.

- AWS App Mesh
- Java/JMX

You can also configure the agent to scrape and import metrics from additional Prometheus workloads and sources.

Set up IAM roles

You need two IAM roles for the CloudWatch agent task definition. If you specify `CreateIAMRoles=True` in the AWS CloudFormation stack to have Container Insights create these roles for you, the roles will be created with the correct permissions. If you want to create them yourself or use existing roles, the following roles and permissions are required.

- **CloudWatch agent ECS task role**— The CloudWatch agent container uses this role. It must include the `CloudWatchAgentServerPolicy` policy and a customer-managed policy which contains the following read-only permissions:
  - ec2:DescribeInstances
  - ecs:ListTasks
  - ecs:ListServices
  - ecs:DescribeContainerInstances
  - ecs:DescribeServices
  - ecs:DescribeTasks
  - ecs:DescribeTaskDefinition

- **CloudWatch agent ECS task execution role**— This is the role that Amazon ECS requires to launch and execute your containers. Ensure that your task execution role has the `AmazonSSMReadOnlyAccess`, `AmazonECSTaskExecutionRolePolicy`, and `CloudWatchAgentServerPolicy` policies attached. If you want to store more sensitive data for Amazon ECS to use, see Specifying sensitive data.

Install the CloudWatch agent with Prometheus monitoring by using AWS CloudFormation

You use AWS CloudFormation to install the CloudWatch agent with Prometheus monitoring for Amazon ECS clusters. The following list shows the parameters you will use in the AWS CloudFormation template.

- **ECSClusterName**— Specifies the target Amazon ECS cluster.
- **CreateIAMRoles**— Specify `True` to create new roles for the Amazon ECS task role and Amazon ECS task execution role. Specify `False` to reuse existing roles.
• **TaskRoleName**— If you specified `True` for `CreateIAMRoles`, this specifies the name to use for the new Amazon ECS task role. If you specified `False` for `CreateIAMRoles`, this specifies the existing role to use as the Amazon ECS task role.

• **ExecutionRoleName**— If you specified `True` for `CreateIAMRoles`, this specifies the name to use for the new Amazon ECS task execution role. If you specified `False` for `CreateIAMRoles`, this specifies the existing role to use as the Amazon ECS task execution role.

• **ECSNetworkMode**— If you are using EC2 launch type, specify the network mode here. It must be either `bridge` or `host`.

• **ECSLaunchType**— Specify either `fargate` or `EC2`.

• **SecurityGroupID**— If the `ECSNetworkMode` is `awsvpc`, specify the security group ID here.

• **SubnetID**— If the `ECSNetworkMode` is `awsvpc`, specify the subnet ID here.

**Command samples**

This section includes sample AWS CloudFormation commands to install Container Insights with Prometheus monitoring in various scenarios.

**Note**

The following setup step pulls the container image from Docker Hub as an anonymous user by default. This pull may be subject to a rate limit. For more information, see CloudWatch agent container image (p. 263).

Create AWS CloudFormation stack for an Amazon ECS cluster in bridge network mode

```bash
export AWS_PROFILE=${your_aws_config_profile_eg_default}
export AWS_DEFAULT_REGION=${your_aws_region_eg_ap-southeast-1}
export ECS_CLUSTER_NAME=${your_ec2 ecs_cluster_name}
export ECS_NETWORK_MODE=bridge
export CREATE_IAM_ROLES=True
export ECS_TASK_ROLE_NAME=${your_selected_ecs_task_role_name}
export ECS_EXECUTION_ROLE_NAME=${your_selected_ecs_execution_role_name}
aws cloudformation create-stack --stack-name CWAgent-Prometheus-ECS-#{ECS_CLUSTER_NAME}-EC2-#{ECS_NETWORK_MODE} --template-body file://cwagent-ecs-prometheus-metric-for-bridge-host.yaml --parameters ParameterKey=ECSClusterName,ParameterValue=#{ECS_CLUSTER_NAME} ParameterKey=CreateIAMRoles,ParameterValue=#{CREATE_IAM_ROLES} ParameterKey=ECSNetworkMode,ParameterValue=#{ECS_NETWORK_MODE} ParameterKey=TaskRoleName,ParameterValue=#{ECS_TASK_ROLE_NAME} ParameterKey=ExecutionRoleName,ParameterValue=#{ECS_EXECUTION_ROLE_NAME} --capabilities CAPABILITY_NAMED_IAM --region #{AWS_DEFAULT_REGION} --profile ${AWS_PROFILE}
```

Create AWS CloudFormation stack for an Amazon ECS cluster in host network mode

```bash
export AWS_PROFILE=${your_aws_config_profile_eg_default}
export AWS_DEFAULT_REGION=${your_aws_region_eg_ap-southeast-1}
export ECS_CLUSTER_NAME=${your_ec2 ecs_cluster_name}
export ECS_NETWORK_MODE=host
export CREATE_IAM_ROLES=True
export ECS_TASK_ROLE_NAME=${your_selected_ecs_task_role_name}
export ECS_EXECUTION_ROLE_NAME=${your_selected_ecs_execution_role_name}
```

aws cloudformation create-stack --stack-name CWAgent-Prometheus-ECS-#{ECS_CLUSTER_NAME}-EC2-#{ECS_NETWORK_MODE} \
   --template-body file://cwagent-ecs-prometheus-metric-for-bridge-host.yaml \
   --parameters ParameterKey=ECSClusterName,ParameterValue=#{ECS_CLUSTER_NAME} \
   ParameterKey=CreateIAMRoles,ParameterValue=#{CREATE_IAM_ROLES} \
   ParameterKey=TaskRoleName,ParameterValue=#{ECS_TASK_ROLE_NAME} \
   ParameterKey=ExecutionRoleName,ParameterValue=#{ECS_EXECUTION_ROLE_NAME} \
   --capabilities CAPABILITY_NAMED_IAM \
   --region #{AWS_DEFAULT_REGION} \
   --profile #{AWS_PROFILE}

Create AWS CloudFormation stack for an Amazon ECS cluster in awsvpc network mode

export AWS_PROFILE=your_aws_config_profile_eg_default
export AWS_DEFAULT_REGION=your_aws_region_eg_ap-southeast-1
export ECS_CLUSTER_NAME=your_ec2_ecs_cluster_name
export ECS_LAUNCH_TYPE=EC2
export CREATE_IAM_ROLES=True
export ECS_CLUSTER_SECURITY_GROUP=your_security_group_eg-xxxxxxxxxx
export ECS_CLUSTER_SUBNET=your_subnet_eg_subnet-xxxxxxxxxx
export ECS_TASK_ROLE_NAME=your_selected_ecs_task_role_name
export ECS_EXECUTION_ROLE_NAME=your_selected_ecs_execution_role_name


aws cloudformation create-stack --stack-name CWAgent-Prometheus-ECS-#{ECS_CLUSTER_NAME}-#{ECS_LAUNCH_TYPE}-awsvpc \
   --template-body file://cwagent-ecs-prometheus-metric-for-awsvpc.yaml \
   --parameters ParameterKey=ECSClusterName,ParameterValue=#{ECS_CLUSTER_NAME} \
   ParameterKey=CreateIAMRoles,ParameterValue=#{CREATE_IAM_ROLES} \
   ParameterKey=ECSLaunchType,ParameterValue=#{ECS_LAUNCH_TYPE} \
   ParameterKey=SecurityGroupId,ParameterValue=#{ECS_SECURITY_GROUP_ID} \
   ParameterKey=SubnetId,ParameterValue=#{ECS_CLUSTER_SUBNET} \
   ParameterKey=TaskRoleName,ParameterValue=#{ECS_TASK_ROLE_NAME} \
   ParameterKey=ExecutionRoleName,ParameterValue=#{ECS_EXECUTION_ROLE_NAME} \
   --capabilities CAPABILITY_NAMED_IAM \
   --region #{AWS_DEFAULT_REGION} \
   --profile #{AWS_PROFILE}

Create AWS CloudFormation stack for a Fargate cluster in awsvpc network mode

export AWS_PROFILE=your_aws_config_profile_eg_default
export AWS_DEFAULT_REGION=your_aws_region_eg_ap-southeast-1
export ECS_CLUSTER_NAME=your_ec2_ecs_cluster_name
export ECS_LAUNCH_TYPE=FARGATE
export CREATE_IAM_ROLES=True
export ECS_CLUSTER_SECURITY_GROUP=your_security_group_eg-xxxxxxxxxx
export ECS_CLUSTER_SUBNET=your_subnet_eg_subnet-xxxxxxxxxx
export ECS_TASK_ROLE_NAME=your_selected_ecs_task_role_name
export ECS_EXECUTION_ROLE_NAME=your_selected_ecs_execution_role_name

aws cloudformation create-stack --stack-name CWAgent-Prometheus-ECS-#{ECS_CLUSTER_NAME}-#{ECS_LAUNCH_TYPE}-awsvpc \
--template-body file://cwagent-ecs-prometheus-metric-for-awsvpc.yaml \
--parameters ParameterKey=ECSClusterName,ParameterValue=#{ECS_CLUSTER_NAME} \
    ParameterKey=CreateIAMRoles,ParameterValue=#{CREATE_IAM_ROLES} \
    ParameterKey=ECSLaunchType,ParameterValue=#{ECS_LAUNCH_TYPE} \
    ParameterKey=SecurityGroupID,ParameterValue=#{ECS_CLUSTER_SECURITY_GROUP} \
    ParameterKey=SubnetID,ParameterValue=#{ECS_CLUSTER_SUBNET} \
    ParameterKey=TaskRoleName,ParameterValue=#{ECS_TASK_ROLE_NAME} \
    ParameterKey=ExecutionRoleName,ParameterValue=#{ECS_EXECUTION_ROLE_NAME} \
--capabilities CAPABILITY_NAMED_IAM \
--region #{AWS_DEFAULT_REGION} \
--profile #{AWS_PROFILE}

AWS resources created by the AWS CloudFormation stack

The following table lists the AWS resources that are created when you use AWS CloudFormation to set up Container Insights with Prometheus monitoring on an Amazon ECS cluster.

<table>
<thead>
<tr>
<th>Resource type</th>
<th>Resource name</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS::SSM::Parameter</td>
<td>AmazonCloudWatch-CWAgentConfig-#{ECS_CLUSTER_NAME}-#{ECS_LAUNCH_TYPE}-#{ECS_NETWORK_MODE}</td>
<td>This is the CloudWatch agent with the default App Mesh and Java/JMX embedded metric format definition.</td>
</tr>
<tr>
<td>AWS::SSM::Parameter</td>
<td>AmazonCloudWatch-PrometheusConfigName-#{ECS_CLUSTER_NAME}-#{ECS_LAUNCH_TYPE}-#{ECS_NETWORK_MODE}</td>
<td>This is the Prometheus scraping configuration.</td>
</tr>
<tr>
<td>AWS::IAM::Role</td>
<td>ECS_TASK_ROLE_NAME</td>
<td>The Amazon ECS task role. This is created only if you specified True for CREATE_IAM_ROLES.</td>
</tr>
<tr>
<td>AWS::IAM::Role</td>
<td>ECS_EXECUTION_ROLE_NAME</td>
<td>The Amazon ECS task execution role. This is created only if you specified True for CREATE_IAM_ROLES.</td>
</tr>
<tr>
<td>AWS::ECS::TaskDefinition</td>
<td>prometheus-#{ECS_CLUSTER_NAME}-#{ECS_LAUNCH_TYPE}-#{ECS_NETWORK_MODE}</td>
<td></td>
</tr>
<tr>
<td>AWS::ECS::Service</td>
<td>CWAgent-prometheus-replica-service-#{ECS_LAUNCH_TYPE}-#{ECS_NETWORK_MODE}</td>
<td></td>
</tr>
</tbody>
</table>

Deleting the AWS CloudFormation stack for the CloudWatch agent with Prometheus monitoring

To delete the CloudWatch agent from an Amazon ECS cluster, enter these commands.

```bash
export AWS_PROFILE=your_aws_config_profile_eg_default
export AWS_DEFAULT_REGION=your_aws_region_eg_ap-southeast-1
export CLOUDFORMATION_STACK_NAME=your_cloudformation_stack_name
```
Scraping additional Prometheus sources and importing those metrics

The CloudWatch agent with Prometheus monitoring needs two configurations to scrape the Prometheus metrics. One is for the standard Prometheus configurations as documented in `<scrape_config>` in the Prometheus documentation. The other is for the CloudWatch agent configuration.

For Amazon ECS clusters, the configurations are integrated with the Parameter Store of AWS Systems Manager by the secrets in the Amazon ECS task definition:

- The secret `PROMETHEUS_CONFIG_CONTENT` is for the Prometheus scrape configuration.
- The secret `CW_CONFIG_CONTENT` is for the CloudWatch agent configuration.

To scrape additional Prometheus metrics sources and import those metrics to CloudWatch, you modify both the Prometheus scrape configuration and the CloudWatch agent configuration, and then re-deploy the agent with the updated configuration.

**VPC security group requirements**

The ingress rules of the security groups for the Prometheus workloads must open the Prometheus ports to the CloudWatch agent for scraping the Prometheus metrics by the private IP.

The egress rules of the security group for the CloudWatch agent must allow the CloudWatch agent to connect to the Prometheus workloads' port by private IP.

**Prometheus scrape configuration**

The CloudWatch agent supports the standard Prometheus scrape configurations as documented in `<scrape_config>` in the Prometheus documentation. You can edit this section to update the configurations that are already in this file, and add additional Prometheus scraping targets. By default, the sample configuration file contains the following global configuration lines:

```yaml
global:
  scrape_interval: 1m
  scrape_timeout: 10s
```

- **scrape_interval**— Defines how frequently to scrape targets.
- **scrape_timeout**— Defines how long to wait before a scrape request times out.

You can also define different values for these settings at the job level, to override the global configurations.

**Prometheus scraping jobs**

The CloudWatch agent YAML files already have some default scraping jobs configured. For example, in the YAML files for Amazon ECS such as `cwagent-ecs-prometheus-metric-for-bridge-host.yaml`, the default scraping jobs are configured in the `ecs_service_discovery` section.

```yaml
"ecs_service_discovery": {
  "sd_frequency": "1m",
```
Each of these default targets are scraped, and the metrics are sent to CloudWatch in log events using embedded metric format. For more information, see Ingesting high-cardinality logs and generating metrics with CloudWatch embedded metric format (p. 668).

Log events from Amazon ECS clusters are stored in the /aws/ecs/containerinsights/cluster_name/prometheus log group.

Each scraping job is contained in a different log stream in this log group.

To add a new scraping target, you add a new entry in the task_definition_list section under the ecs_service_discovery section of the YAML file, and restart the agent. For an example of this process, see Tutorial for adding a new Prometheus scrape target: Prometheus API Server metrics (p. 374).

CloudWatch agent configuration for Prometheus

The CloudWatch agent configuration file has a prometheus section under metrics_collected for the Prometheus scraping configuration. It includes the following configuration options:

- **cluster_name**— specifies the cluster name to be added as a label in the log event. This field is optional. If you omit it, the agent can detect the Amazon ECS cluster name.
- **log_group_name**— specifies the log group name for the scraped Prometheus metrics. This field is optional. If you omit it, CloudWatch uses /aws/ecs/containerinsights/cluster_name/prometheus for logs from Amazon ECS clusters.
- **prometheus_config_path**— specifies the Prometheus scrape configuration file path. If the value of this field starts with env: the Prometheus scrape configuration file contents will be retrieved from the container's environment variable. Do not change this field.
- **ecs_service_discovery**— is the section to specify the configurations of the Amazon ECS Prometheus target auto-discovery functions. Two modes are supported to discover the Prometheus targets: discovery based on the container's docker label or discovery based on the Amazon ECS task definition ARN regular expression. You can use the two modes together and the CloudWatch agent will de-duplicate the discovered targets based on: {private_ip}:{port}/{metrics_path}.

The ecs_service_discovery section can contain the following fields:

- **sd_frequency** is the frequency to discover the Prometheus exporters. Specify a number and a unit suffix. For example, 1m for once per minute or 30s for once per 30 seconds. Valid unit suffixes are ns, us, ms, s, m, and h.

This field is optional. The default is 60 seconds (1 minute).
• **sd_target_cluster** is the target Amazon ECS cluster name for auto-discovery. This field is optional. The default is the name of the Amazon ECS cluster where the CloudWatch agent is installed.

• **sd_cluster_region** is the target Amazon ECS cluster's Region. This field is optional. The default is the Region of the Amazon ECS cluster where the CloudWatch agent is installed.

• **sd_result_file** is the path of the YAML file for the Prometheus target results. The Prometheus scrape configuration will refer to this file.

• **docker_label** is an optional section that you can use to specify the configuration for docker label-based service discovery. If you omit this section, docker label-based discovery is not used. This section can contain the following fields:
  - **sd_port_label** is the container's docker label name that specifies the container port for Prometheus metrics. The default value is `ECS_PROMETHEUS_EXPORTER_PORT`. If the container does not have this docker label, the CloudWatch agent will skip it.
  - **sd_metrics_path_label** is the container's docker label name that specifies the Prometheus metrics path. The default value is `ECS_PROMETHEUS_METRICS_PATH`. If the container does not have this docker label, the agent assumes the default path `/metrics`.
  - **sd_job_name_label** is the container's docker label name that specifies the Prometheus scrape job name. The default value is `job`. If the container does not have this docker label, the CloudWatch agent uses the job name in the Prometheus scrape configuration.

• **task_definition_list** is an optional section that you can use to specify the configuration of task definition-based service discovery. If you omit this section, task definition-based discovery is not used. This section can contain the following fields:
  - **sd_task_definition_arn_pattern** is the pattern to use to specify the Amazon ECS task definitions to discover. This is a regular expression.
  - **sd_metrics_ports** lists the containerPort for the Prometheus metrics. Separate the containerPorts with semicolons.
  - **sd_container_name_pattern** specifies the Amazon ECS task container names. This is a regular expression.
  - **sd_metrics_path** specifies the Prometheus metric path. If you omit this, the agent assumes the default path `/metrics`.
  - **sd_job_name** specifies the Prometheus scrape job name. If you omit this field, the CloudWatch agent uses the job name in the Prometheus scrape configuration.

• **service_name_list_for_tasks** is an optional section that you can use to specify the configuration of service name-based discovery. If you omit this section, service name-based discovery is not used. This section can contain the following fields:
  - **sd_service_name_pattern** is the pattern to use to specify the Amazon ECS service where tasks are to be discovered. This is a regular expression.
  - **sd_metrics_ports** lists the containerPort for the Prometheus metrics. Separate multiple containerPorts with semicolons.
  - **sd_container_name_pattern** specifies the Amazon ECS task container names. This is a regular expression.
  - **sd_metrics_path** specifies the Prometheus metrics path. If you omit this, the agent assumes the default path `/metrics`.
  - **sd_job_name** specifies the Prometheus scrape job name. If you omit this field, the CloudWatch agent uses the job name in the Prometheus scrape configuration.

• **metric_declaration** are sections that specify the array of logs with embedded metric format to be generated. There are `metric_declaration` sections for each Prometheus source that the CloudWatch agent imports from by default. These sections each include the following fields:
  - **label_matcher** is a regular expression that checks the value of the labels listed in `source_labels`. The metrics that match are enabled for inclusion in the embedded metric format sent to CloudWatch.
If you have multiple labels specified in `source_labels`, we recommend that you do not use `^` or `$` characters in the regular expression for `label_matcher`.

- `source_labels` specifies the value of the labels that are checked by the `label_matcher` line.
- `label_separator` specifies the separator to be used in the `label_matcher` line if multiple `source_labels` are specified. The default is `;`. You can see this default used in the `label_matcher` line in the following example.
- `metric_selectors` is a regular expression that specifies the metrics to be collected and sent to CloudWatch.
- `dimensions` is the list of labels to be used as CloudWatch dimensions for each selected metric.

See the following `metric_declaration` example.

```json
"metric_declaration": [ 
  { 
    "source_labels": [ "Service", "Namespace"], 
    "label_matcher": "(.*node-exporter.*|.*kube-dns.*);kube-system$", 
    "dimensions": [ 
      [ "Service", "Namespace" ] 
    ], 
    "metric_selectors": [ 
      "^coredns_dns_request_type_count_total$" 
    ] 
  } 
]
```

This example configures an embedded metric format section to be sent as a log event if the following conditions are met:

- The value of `Service` contains either `node-exporter` or `kube-dns`.
- The value of `Namespace` is `kube-system`.
- The Prometheus metric `coredns_dns_request_type_count_total` contains both `Service` and `Namespace` labels.

The log event that is sent includes the following highlighted section:

```json
{ 
  "CloudWatchMetrics": [ 
    { 
      "Metrics": [ 
        { 
          "Name": "coredns_dns_request_type_count_total" 
        } 
      ], 
      "Dimensions": [ 
        [ 
          "Namespace", 
          "Service" 
        ] 
      ], 
      "Namespace": "ContainerInsights/Prometheus" 
    } 
  ], 
  "Namespace": "kube-system", 
  "Service": "kube-dns", 
  "coredns_dns_request_type_count_total": 2562, 
  "eks_amazonaws_com_component": "kube-dns", 
  "instance": "192.168.61.254:9153"
}
```
Detailed guide for autodiscovery on Amazon ECS clusters

Prometheus provides dozens of dynamic service-discovery mechanisms as described in `<scrape_config>`. However, there is no built-in service discovery for Amazon ECS. The CloudWatch agent adds this mechanism.

When the Amazon ECS Prometheus service discovery is enabled, the CloudWatch agent periodically makes the following API calls to Amazon ECS and Amazon EC2 frontends to retrieve the metadata of the running ECS tasks in the target ECS cluster.

```
EC2:DescribeInstances
ECS:ListTasks
ECS:ListServices
ECS:DescribeContainerInstances
ECS:DescribeServices
ECS:DescribeTasks
ECS:DescribeTaskDefinition
```

The metadata is used by the CloudWatch agent to scan the Prometheus targets within the ECS cluster. The CloudWatch agent supports three service discovery modes:

- Container docker label-based service discovery
- ECS task definition ARN regular expression-based service discovery
- ECS service name regular expression-based service discovery

All modes can be used together. CloudWatch agent de-duplicates the discovered targets based on:

```
{private_ip}:{port}/{metrics_path}
```

All discovered targets are written into a result file specified by the `sd_result_file` configuration field within the CloudWatch agent container. The following is a sample result file:

```yaml
- targets:
  - 10.6.1.95:32785
    labels:
      __metrics_path__: /metrics
      ECS_PROMETHEUS_EXPORTER_PORT: "9406"
      ECS_PROMETHEUS_JOB_NAME: demo-jar-ec2-bridge-dynamic
      ECS_PROMETHEUS_METRICS_PATH: /metrics
      InstanceType: t3.medium
      LaunchType: EC2
      SubnetId: subnet-123456789012
      TaskDefinitionFamily: demo-jar-ec2-bridge-dynamic-port
      TaskGroupName: family:demo-jar-ec2-bridge-dynamic-port
      TaskRevision: "7"
      VpcId: vpc-0123456789012
      container_name: demo-jar-ec2-bridge-dynamic-port
      job: demo-jar-ec2-bridge-dynamic
  - targets:
    - 10.6.3.193:9404
    labels:
      __metrics_path__: /metrics
      ECS_PROMETHEUS_EXPORTER_PORT_SUBSET_B: "9404"
      ECS_PROMETHEUS_JOB_NAME: demo-tomcat-ec2-bridge-mapped-port
      ECS_PROMETHEUS_METRICS_PATH: /metrics
      InstanceType: t3.medium
```
You can directly integrate this result file with Prometheus file-based service discovery. For more information about Prometheus file-based service discovery, see `<file_sd_config>`.

Suppose the result file is written to `/tmp/cwagent_ecs_auto_sd.yaml` The following Prometheus scrape configuration will consume it.

```yaml
global:
  scrape_interval: 1m
  scrape_timeout: 10s
scrape_configs:
- job_name: cwagent-ecs-file-sd-config
  sample_limit: 10000
  file_sd_configs:
    - files: ["/tmp/cwagent_ecs_auto_sd.yaml"]
```

The CloudWatch agent also adds the following additional labels for the discovered targets.

- `container_name`
- `TaskDefinitionFamily`
- `TaskRevision`
- `TaskGroup`
- `StartedBy`
- `LaunchType`
- `job`
- `__metrics_path__`
- Docker labels

When the cluster has the EC2 launch type, the following three labels are added.

- `InstanceType`
- `VpcId`
- `SubnetId`

**Note**
Docker labels that don't match the regular expression `[a-zA-Z_][a-zA-Z0-9_]` are filtered out. This matches the Prometheus conventions as listed in `label_name` in Configuration file in the Prometheus documentation.

**ECS service discovery configuration examples**

This section includes examples that demonstrate ECS service discovery.

**Example 1**

```
"ecs_service_discovery": {
```
This example enables docker label-based service discovery. The CloudWatch agent will query the ECS tasks' metadata once per minute and write the discovered targets into the `/tmp/cwagent_ecs_auto_sd.yaml` file within the CloudWatch agent container.

The default value of `sd_port_label` in the `docker_label` section is `ECS_PROMETHEUS_EXPORTER_PORT`. If any running container in the ECS tasks has a `ECS_PROMETHEUS_EXPORTER_PORT` docker label, the CloudWatch agent uses its value as container port to scan all exposed ports of the container. If there is a match, the mapped host port plus the private IP of the container are used to construct the Prometheus exporter target in the following format: `private_ip:host_port`.

The default value of `sd_metrics_path_label` in the `docker_label` section is `ECS_PROMETHEUS_METRICS_PATH`. If the container has this docker label, its value will be used as the `__metrics_path__`. If the container does not have this label, the default value `/metrics` is used.

The default value of `sd_job_name_label` in the `docker_label` section is `job`. If the container has this docker label, its value will be appended as one of the labels for the target to replace the default job name specified in the Prometheus configuration. The value of this docker label is used as the log stream name in the CloudWatch Logs log group.

**Example 2**

```json
"ecs_service_discovery": {
  "sd_frequency": "15s",
  "sd_result_file": "/tmp/cwagent_ecs_auto_sd.yaml",
  "docker_label": {
    "sd_port_label": "ECS_PROMETHEUS_EXPORTER_PORT_SUBSET_A",
    "sd_job_name_label": "ECS_PROMETHEUS_JOB_NAME"
  }
}
```

This example enables docker label-based service discovery. The CloudWatch agent will query the ECS tasks' metadata every 15 seconds and write the discovered targets into the `/tmp/cwagent_ecs_auto_sd.yaml` file within the CloudWatch agent container. The containers with a docker label of `ECS_PROMETHEUS_EXPORTER_PORT_SUBSET_A` will be scanned. The value of the docker label `ECS_PROMETHEUS_JOB_NAME` is used as the job name.

**Example 3**

```json
"ecs_service_discovery": {
  "sd_frequency": "5m",
  "sd_result_file": "/tmp/cwagent_ecs_auto_sd.yaml",
  "task_definition_list": [
    {
      "sd_job_name": "java-prometheus",
      "sd_metrics_path": "/metrics",
      "sd_metrics_ports": "9404; 9406",
      "sd_task_definition_name_pattern": ".*:task-definition/.*javajmx.*:[0-9]+"
    },
    {
      "sd_job_name": "envoy-prometheus",
      "sd_metrics_path": "/stats/prometheus",
      "sd_container_name_pattern": "^envoy$"
    }
  ]
}
```

The `task_definition_list` field allows specifying task definitions that the CloudWatch agent should scan. This example includes two task definitions:

1. `java-prometheus`: Selects containers with any task definition name containing `javajmx` and defined ports `9404` and `9406`.
2. `envoy-prometheus`: Selects containers with the docker label `envoy-prometheus` and the `envoy` container name pattern.
This example enables ECS task definition ARN regular expression-based service discovery. The CloudWatch agent will query the ECS tasks' metadata every five minutes and write the discovered targets into the /tmp/cwagent_ecs_auto_sd.yaml file within the CloudWatch agent container.

Two task definition ARN regular expression sections are defined:

- For the first section, the ECS tasks with javajmx in their ECS task definition ARN are filtered for the container port scan. If the containers within these ECS tasks expose the container port on 9404 or 9406, the mapped host port along with the private IP of the container are used to create the Prometheus exporter targets. The value of `sd_metrics_path` sets __metrics_path__ to /metrics. So the CloudWatch agent will scrape the Prometheus metrics from `private_ip:host_port/metrics`, the scraped metrics are sent to the java-prometheus log stream in CloudWatch Logs in the log group /aws/ecs/containerinsights/cluster_name/prometheus.

- For the second section, the ECS tasks with appmesh in their ECS task definition ARN and with version of :23 are filtered for the container port scan. For containers with a name of envoy that expose the container port on 9901, the mapped host port along with the private IP of the container are used to create the Prometheus exporter targets. The value within these ECS tasks expose the container port on 9404 or 9406, the mapped host port along with the private IP of the container are used to create the Prometheus exporter targets. The value of `sd_metrics_path` sets __metrics_path__ to /stats/prometheus. So the CloudWatch agent will scrape the Prometheus metrics from `private_ip:host_port/stats/prometheus`, and send the scraped metrics to the envoy-prometheus log stream in CloudWatch Logs in the log group /aws/ecs/containerinsights/cluster_name/prometheus.

**Example 4**

```json
"ecs_service_discovery": {
  "sd_frequency": "5m",
  "sd_result_file": "/tmp/cwagent_ecs_auto_sd.yaml",
  "service_name_list_for_tasks": [
    {
      "sd_job_name": "nginx-prometheus",
      "sd_metrics_path": "/metrics",
      "sd_metrics_ports": "9113",
      "sd_service_name_pattern": "^nginx-.*"
    },
    {
      "sd_job_name": "haproxy-prometheus",
      "sd_metrics_path": "/stats/metrics",
      "sd_container_name_pattern": "^haproxy$",
      "sd_metrics_ports": "8404",
      "sd_service_name_pattern": ".*haproxy-service.*"
    }
  ]
}
```

This example enables ECS service name regular expression-based service discovery. The CloudWatch agent will query the ECS services' metadata every five minutes and write the discovered targets into the /tmp/cwagent_ecs_auto_sd.yaml file within the CloudWatch agent container.

Two service name regular expression sections are defined:
For the first section, the ECS tasks that are associated with ECS services that have names matching the regular expression `^nginx-.*` are filtered for the container port scan. If the containers within these ECS tasks expose the container port on 9113, the mapped host port along with the private IP of the container are used to create the Prometheus exporter targets. The value of `sd_metrics_path` sets `__metrics_path__` to `/metrics`. So the CloudWatch agent will scrape the Prometheus metrics from `private_ip:host_port/metrics`, and the scraped metrics are sent to the `nginx-prometheus` log stream in CloudWatch Logs in the log group `/aws/ecs/containerinsights/cluster_name/prometheus`.

For the second section, the ECS tasks that are associated with ECS services that have names matching the regular expression `.*haproxy-service.*` are filtered for the container port scan. For containers with a name of `haproxy` expose the container port on 8404, the mapped host port along with the private IP of the container are used to create the Prometheus exporter targets. The value of `sd_metrics_path` sets `__metrics_path__` to `/stats/metrics`. So the CloudWatch agent will scrape the Prometheus metrics from `private_ip:host_port/stats/metrics`, and the scraped metrics are sent to the `haproxy-prometheus` log stream in CloudWatch Logs in the log group `/aws/ecs/containerinsights/cluster_name/prometheus`.

**Example 5**

```json
"ecs_service_discovery": {
"sd_frequency": "1m30s",
"sd_result_file": "/tmp/cwagent_ecs_auto_sd.yaml",
"docker_label": {
"sd_port_label": "MY_PROMETHEUS_EXPORTER_PORT_LABEL",
"sd_metrics_path_label": "MY_PROMETHEUS_METRICS_PATH_LABEL",
"sd_job_name_label": "MY_PROMETHEUS_METRICS_NAME_LABEL"
}
"task_definition_list": [
{
"sd_metrics_ports": "9150",
"sd_task_definition_name_pattern": "*memcached.*"
}
]
}
```

This example enables both ECS service discovery modes. The CloudWatch agent will query the ECS tasks' metadata every 90 seconds and write the discovered targets into the `/tmp/cwagent_ecs_auto_sd.yaml` file within the CloudWatch agent container.

**For the docker-based service discovery configuration:**

- The ECS tasks with docker label `MY_PROMETHEUS_EXPORTER_PORT_LABEL` will be filtered for Prometheus port scan. The target Prometheus container port is specified by the value of the label `MY_PROMETHEUS_EXPORTER_PORT_LABEL`.
- The value of the docker label `MY_PROMETHEUS_EXPORTER_PORT_LABEL` is used for `__metrics_path__`. If the container does not have this docker label, the default value `/metrics` is used.
- The value of the docker label `MY_PROMETHEUS_EXPORTER_PORT_LABEL` is used as the job label. If the container does not have this docker label, the job name defined in the Prometheus configuration is used.

**For the ECS task definition ARN regular expression-based service discovery configuration:**

- The ECS tasks with `memcached` in the ECS task definition ARN are filtered for container port scan. The target Prometheus container port is 9150 as defined by `sd_metrics_ports`. The default metrics path `/metrics` is used. The job name defined in the Prometheus configuration is used.
(Optional) Set up sample containerized Amazon ECS workloads for Prometheus metric testing

To test the Prometheus metric support in CloudWatch Container Insights, you can set up one or more of the following containerized workloads. The CloudWatch agent with Prometheus support automatically collects metrics from each of these workloads. To see the metrics that are collected by default, see Prometheus metrics collected by the CloudWatch agent (p. 392).

Before you can install any of these workloads, you must install Helm 3.x by entering the following commands:

```
brew install helm
```

For more information, see Helm.

Topics

- Sample App Mesh workload for Amazon ECS clusters (p. 341)
- Sample Java/JMX workload for Amazon ECS clusters (p. 342)
- Sample NGINX workload for Amazon ECS clusters (p. 343)
- Sample NGINX Plus workload for Amazon ECS clusters (p. 348)
- Tutorial for adding a new Prometheus scrape target: Memcached on Amazon ECS (p. 355)
- Tutorial for scraping Redis Prometheus metrics on Amazon ECS Fargate (p. 360)

Sample App Mesh workload for Amazon ECS clusters

To collect metrics from a sample Prometheus workload for Amazon ECS, you must be running Container Insights in the cluster. For information about installing Container Insights, see Setting up Container Insights on Amazon ECS (p. 264).

First, follow this walkthrough to deploy the sample color app on your Amazon ECS cluster. After you finish, you will have App Mesh Prometheus metrics exposed on port 9901.

Next, follow these steps to install the CloudWatch agent with Prometheus monitoring on the same Amazon ECS cluster where you installed the color app. The steps in this section install the CloudWatch agent in bridge network mode.

The environment variables `ENVIRONMENT_NAME`, `AWS_PROFILE`, and `AWS_DEFAULT_REGION` that you set in the walkthrough will also be used in the following steps.

**To install the CloudWatch agent with Prometheus monitoring for testing**

1. Download the AWS CloudFormation template by entering the following command.

   ```
   ```

2. Set the network mode by entering the following commands.

   ```
   export ECS_CLUSTER_NAME=${ENVIRONMENT_NAME}
   export ECS_NETWORK_MODE=bridge
   ```

3. Create the AWS CloudFormation stack by entering the following commands.
aws cloudformation create-stack --stack-name CWAgent-Prometheus-ECS-$(ECS_CLUSTER_NAME)-EC2-$(ECSNETWORK_MODE) \
   --template-body file://cwagent-ecs-prometheus-metric-for-bridge-host.yaml \
   --parameters ParameterKey=ECSClusterName,ParameterValue=\$(ECS_CLUSTER_NAME) \
   ParameterKey=ECSNetworkMode,ParameterValue=\$(ECS_NETWORK_MODE) \
   ParameterKey=TaskRoleName,ParameterValue=CWAgent-Prometheus-TaskRole-\$(ECS_CLUSTER_NAME) \
   ParameterKey=ExecutionRoleName,ParameterValue=CWAgent-Prometheus-\$(ECS_CLUSTER_NAME) \
   --capabilities CAPABILITY_NAMED_IAM \
   --region ${AWS_DEFAULT_REGION} \
   --profile ${AWS_PROFILE}

4. (Optional) When the AWS CloudFormation stack is created, you see a CREATE_COMPLETE message. If you to check the status before you see that message, enter the following command.

aws cloudformation describe-stacks \
   --stack-name CWAgent-Prometheus-ECS-\$(ECS_CLUSTER_NAME)-EC2-\$(ECS_NETWORK_MODE) \
   --query 'Stacks[0].StackStatus' \
   --region \$(AWS_DEFAULT_REGION) \
   --profile \$(AWS_PROFILE)

Troubleshooting

The steps in the walkthrough use jq to parse the output result of the AWS CLI. For more information about installing jq, see jq. Use the following command to set the default output format of your AWS CLI to JSON so jq can parse it correctly.

```
$ aws configure
When the response gets to Default output format, enter json.
```

Uninstall the CloudWatch agent with Prometheus monitoring

When you are finished testing, enter the following command to uninstall the CloudWatch agent by deleting the AWS CloudFormation stack.

aws cloudformation delete-stack \
   --stack-name CWAgent-Prometheus-ECS-\$(ECS_CLUSTER_NAME)-EC2-\$(ECS_NETWORK_MODE) \
   --region \$(AWS_DEFAULT_REGION) \
   --profile \$(AWS_PROFILE)

Sample Java/JMX workload for Amazon ECS clusters

JMX Exporter is an official Prometheus exporter that can scrape and expose JMX mBeans as Prometheus metrics. For more information, see prometheus/jmx_exporter.

The CloudWatch agent with Prometheus support scrapes the Java/JMX Prometheus metrics based on the service discovery configuration in the Amazon ECS cluster. You can configure the JMX Exporter to expose the metrics on a different port or metrics_path. If you do change the port or path, update the default ecs_service_discovery section in the CloudWatch agent configuration.

To collect metrics from a sample Prometheus workload for Amazon ECS, you must be running Container Insights in the cluster. For information about installing Container Insights, see Setting up Container Insights on Amazon ECS (p. 264).
To install the Java/JMX sample workload for Amazon ECS clusters

1. Follow the steps in these sections to create your Docker images.
   - Example: Java Jar Application Docker image with Prometheus metrics (p. 386)
   - Example: Apache Tomcat Docker image with Prometheus metrics (p. 384)

2. Specify the following two docker labels in the Amazon ECS task definition file. You can then run the task definition as an Amazon ECS service or Amazon ECS task in the cluster.
   - Set `ECS_PROMETHEUS_EXPORTER_PORT` to point to the containerPort where the Prometheus metrics are exposed.
   - Set `Java_EMF_Metrics` to `true`. The CloudWatch agent uses this flag to generated the embedded metric format in the log event.

The following is an example:

```json
{
    "family": "workload-java-ec2-bridge",
    "taskRoleArn": "{{task-role-arn}}",
    "executionRoleArn": "{{execution-role-arn}}",
    "networkMode": "bridge",
    "containerDefinitions": [
        {
            "name": "tomcat-prometheus-workload-java-ec2-bridge-dynamic-port",
            "image": "your_docker_image_tag_for_tomcat_with_prometheus_metrics",
            "portMappings": [
                {
                    "hostPort": 0,
                    "protocol": "tcp",
                    "containerPort": 9404
                }
            ],
            "dockerLabels": {
                "ECS_PROMETHEUS_EXPORTER_PORT": "9404",
                "Java_EMF_Metrics": "true"
            }
        }
    ],
    "requiresCompatibilities": ["EC2"],
    "cpu": "256",
    "memory": "512"
}
```

The default setting of the CloudWatch agent in the AWS CloudFormation template enables both docker label-based service discovery and task definition ARN-based service discovery. To view these default settings, see line 65 of the CloudWatch agent YAML configuration file. The containers with the `ECS_PROMETHEUS_EXPORTER_PORT` label will be auto-discovered based on the specified container port for Prometheus scraping.

The default setting of the CloudWatch agent also has the `metric_declaration` setting for Java/JMX at line 112 of the same file. All docker labels of the target containers will be added as additional labels in the Prometheus metrics and sent to CloudWatch Logs. For the Java/JMX containers with docker label `Java_EMF_Metrics="true"`, the embedded metric format will be generated.

Sample NGINX workload for Amazon ECS clusters

The NGINX Prometheus exporter can scrape and expose NGINX data as Prometheus metrics. This example uses the exporter in tandem with the NGINX reverse proxy service for Amazon ECS.
For more information about the NGINX Prometheus exporter, see `nginx-prometheus-exporter` on Github. For more information about the NGINX reverse proxy, see `ecs-nginx-reverse-proxy` on Github.

The CloudWatch agent with Prometheus support scrapes the NGINX Prometheus metrics based on the service discovery configuration in the Amazon ECS cluster. You can configure the NGINX Prometheus Exporter to expose the metrics on a different port or path. If you change the port or path, update the `ecs_service_discovery` section in the CloudWatch agent configuration file.

Install the NGINX reverse proxy sample workload for Amazon ECS clusters

Follow these steps to install the NGINX reverse proxy sample workload.

Create the Docker images

To create the Docker images for the NGINX reverse proxy sample workload

1. Download the following folder from the NGINX reverse proxy repo: `https://github.com/awslabs/ecs-nginx-reverse-proxy/tree/master/reverse-proxy/`.
2. Find the `app` directory and build an image from that directory:
   ```bash
docker build -t web-server-app .
```
3. Build a custom image for NGINX. First, create a directory with the following two files:
   - A sample Dockerfile:
     ```dockerfile
     FROM nginx
     COPY nginx.conf /etc/nginx/nginx.conf
     ```
   - An `nginx.conf` file, modified from `https://github.com/awslabs/ecs-nginx-reverse-proxy/tree/master/reverse-proxy/`:
     ```nginx
     events {
       worker_connections 768;
     }

     http {
       # Nginx will handle gzip compression of responses from the app server
       gzip on;
       gzip_proxied any;
       gzip_types text/plain application/json;
       gzip_min_length 1000;

       server {
         listen 8080;
         location /stub_status {
           stub_status on;
         }
       }

       server {
         listen 80;

         # Nginx will reject anything not matching /api
         location /api {
           # Reject requests with unsupported HTTP method
           if ($request_method !~ ^(GET|POST|HEAD|OPTIONS|PUT|DELETE)$) {
             return 405;
           }

           # Only requests matching the whitelist expectations will
           # get sent to the application server
        }
     }
     ```
proxy_pass http://app:3000;
proxy_http_version 1.1;
proxy_set_header Upgrade $http_upgrade;
proxy_set_header Connection 'upgrade';
proxy_set_header Host $host;
proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
proxy_cache_bypass $http_upgrade;
}
}
}

**Note**

stub_status must be enabled on the same port that nginx-prometheus-exporter is configured to scrape metrics from. In our example task definition, nginx-prometheus-exporter is configured to scrape metrics from port 8080.

4. Build an image from files in your new directory:

```bash
docker build -t nginx-reverse-proxy ./path-to-your-directory
```

5. Upload your new images to an image repository for later use.

### Create the task definition to run NGINX and the web server app in Amazon ECS

Next, you set up the task definition.

This task definition enables the collection and export of NGINX Prometheus metrics. The NGINX container tracks input from the app, and exposes that data to port 8080, as set in nginx.conf. The NGINX prometheus exporter container scrapes these metrics, and posts them to port 9113, for use in CloudWatch.

**To set up the task definition for the NGINX sample Amazon ECS workload**

1. Create a task definition JSON file with the following content. Replace `your-customized-nginx-image` with the image URI for your customized NGINX image, and replace `your-web-server-app-image` with the image URI for your web server app image.

```json
{
  "containerDefinitions": [
    {
      "name": "nginx",
      "image": "your-customized-nginx-image",
      "memory": 256,
      "cpu": 256,
      "essential": true,
      "portMappings": [
        {
          "containerPort": 80,
          "protocol": "tcp"
        }
      ],
      "links": [
        "app"
      ]
    },
    {
      "name": "app",
      "image": "your-web-server-app-image",
      "memory": 256,
      "cpu": 256,
      "essential": true
    }
  ]
}
```
Configure the CloudWatch agent to scrape NGINX Prometheus metrics

The final step is to configure the CloudWatch agent to scrape the NGINX metrics. In this example, the CloudWatch agent discovers the task via the service name pattern, and the port 9113, where the exporter exposes the Prometheus metrics for NGINX. With the task discovered and the metrics available, the CloudWatch agent begins posting the collected metrics to the log stream `nginx-prometheus-exporter`.

**To configure the CloudWatch agent to scrape the NGINX metrics**

1. Download the latest version of the necessary YAML file by entering the following command.

   ```bash
   ```
2. Open the file with a text editor, and find the full CloudWatch agent configuration in the value key in the resource: CWAgentConfigSSMParameter section. Then, in the ecs_service_discovery section, add the following service_name_list_for_tasks section.

```
"service_name_list_for_tasks": [
  {
    "sd_job_name": "nginx-prometheus-exporter",
    "sd_metrics_path": "/metrics",
    "sd_metrics_ports": "9113",
    "sd_service_name_pattern": "^nginx-service$"
  }
],
```

3. In the same file, add the following section in the metric_declaration section to allow NGINX metrics. Be sure to follow the existing indentation pattern.

```
{ "source_labels": ["job"],
  "label_matcher": ".*nginx.*",
  "dimensions": ["ClusterName", "TaskDefinitionFamily", "ServiceName"],
  "metric_selectors": ["^nginx_.*$"],
}
```

4. If you don't already have the CloudWatch agent deployed in this cluster, skip to step 8.

If you already have the CloudWatch agent deployed in the Amazon ECS cluster by using AWS CloudFormation, you can create a change set by entering the following commands:

```
ECS_CLUSTER_NAME=your_cluster_name
AWS_REGION=your_aws_region
ECS_NETWORK_MODE=bridge
CREATE_IAM_ROLES=True
ECS_TASK_ROLE_NAME=your_selected_ecs_task_role_name
ECS_EXECUTION_ROLE_NAME=your_selected_ecs_execution_role_name

aws cloudformation create-change-set --stack-name CWAgent-Prometheus-ECS-#{ECS_CLUSTER_NAME}-EC2-#{ECS_NETWORK_MODE} --parameters ParameterKey=ECSClusterName,ParameterValue=$ECS_CLUSTER_NAME ParameterKey=CreateIAMRoles,ParameterValue=$CREATE_IAM_ROLES
ParameterKey=ECSNetworkMode,ParameterValue=$ECS_NETWORK_MODE
ParameterKey=TaskRoleName,ParameterValue=$ECS_TASK_ROLE_NAME
ParameterKey=ExecutionRoleName,ParameterValue=$ECS_EXECUTION_ROLE_NAME

```


6. Review the newly-created changeset nginx-scraping-support. You should see one change applied to the CWAgentConfigSSMParameter resource. Run the changeset and restart the CloudWatch agent task by entering the following command:

```
aws ecs update-service --cluster $ECS_CLUSTER_NAME --desired-count 0 --service cwagent-prometheus-replica-service-EC2-#ECS_NETWORK_MODE
```

7. Wait about 10 seconds, and then enter the following command.

347
aws ecs update-service --cluster $ECS_CLUSTER_NAME \\ 
--desired-count 1 \\ 
--service cwagent-prometheus-replica-service-EC2--$ECS_NETWORK_MODE \\ 
--region $AWS_REGION

8. If you are installing the CloudWatch agent with Prometheus metric collecting on the cluster for the first time, enter the following commands.

```bash
aws cloudformation create-stack --stack-name CWAgent-Prometheus-ECS-#(ECS_CLUSTER_NAME)-EC2-#(ECS_NETWORK_MODE) \\ 
--template-body file://cwagent-ecs-prometheus-metric-for-bridge-host.yaml \\ 
--parameters ParameterKey=ECSClusterName,ParameterValue=$ECS_CLUSTER_NAME \\ 
ParameterKey=CreateIAMRoles,ParameterValue=$CREATE_IAM_ROLES \\ 
ParameterKey=ECSNetworkMode,ParameterValue=$ECS_NETWORK_MODE \\ 
ParameterKey=TaskRoleName,ParameterValue=$ECS_TASK_ROLE_NAME \\ 
ParameterKey=ExecutionRoleName,ParameterValue=$ECS_EXECUTION_ROLE_NAME \\ 
--capabilities CAPABILITY_NAMED_IAM \\ 
--region $AWS_REGION
```

Viewing your NGINX metrics and logs

You can now view the NGINX metrics being collected.

**To view the metrics for your sample NGINX workload**

2. In the Region where your cluster is running, choose Metrics in the left navigation pane. Find the ContainerInsights/Prometheus namespace to see the metrics.
3. To see the CloudWatch Logs events, choose Log groups in the navigation pane. The events are in the log group `/aws/containerinsights/your_cluster_name/prometheus`, in the log stream `nginx-prometheus-exporter`.

Sample NGINX Plus workload for Amazon ECS clusters

NGINX Plus is the commercial version of NGINX. You must have a licence to use it. For more information, see [NGINX Plus](#). The NGINX Prometheus exporter can scrape and expose NGINX data as Prometheus metrics. This example uses the exporter in tandem with the NGINX Plus reverse proxy service for Amazon ECS.

For more information about the NGINX Prometheus exporter, see [nginx-prometheus-exporter](#) on Github. For more information about the NGINX reverse proxy, see [ecs-nginx-reverse-proxy](#) on Github.

The CloudWatch agent with Prometheus support scrapes the NGINX Plus Prometheus metrics based on the service discovery configuration in the Amazon ECS cluster. You can configure the NGINX Prometheus Exporter to expose the metrics on a different port or path. If you change the port or path, update the ecs_service_discovery section in the CloudWatch agent configuration file.
Install the NGINX Plus reverse proxy sample workload for Amazon ECS clusters

Follow these steps to install the NGINX reverse proxy sample workload.

Create the Docker images

To create the Docker images for the NGINX Plus reverse proxy sample workload

1. Download the following folder from the NGINX reverse proxy repo: https://github.com/awslabs/ecs-nginx-reverse-proxy/tree/master/reverse-proxy/.
2. Find the app directory and build an image from that directory:

   ```
   docker build -t web-server-app ./path-to-app-directory
   ```
3. Build a custom image for NGINX Plus. Before you can build the image for NGINX Plus, you need to obtain the key named nginx-repo.key and the SSL certificate nginx-repo.crt for your licensed NGINX Plus. Create a directory and store in it your nginx-repo.key and nginx-repo.crt files.

In the directory that you just created, create the following two files:

- A sample Dockerfile with the following content. This docker file is adopted from a sample file provided at https://docs.nginx.com/nginx/admin-guide/installing-nginx/installing-nginx-docker/#docker_plus_image. The important change that we make is that we load a separate file, called nginx.conf, which will be created in the next step.

```bash
FROM debian:buster-slim
LABEL maintainer="NGINX Docker Maintainers <docker-maint@nginx.com>"

# Define NGINX versions for NGINX Plus and NGINX Plus modules
# Uncomment this block and the versioned nginxPackages block in the main RUN
# instruction to install a specific release
# ENV NGINX_VERSION 21
# ENV NJS_VERSION 0.3.9
# ENV PKG_RELEASE 1~buster

# Download certificate and key from the customer portal (https://cs.nginx.com) (https://cs.nginx.com/)
# and copy to the build context
COPY nginx-repo.crt /etc/ssl/nginx/
COPY nginx-repo.key /etc/ssl/nginx/
# COPY nginx.conf /etc/ssl/nginx/nginx.conf

RUN set -x 
# Create nginx user/group first, to be consistent throughout Docker variants 
&& addgroup --system --gid 101 nginx 
&& adduser --system --disabled-login --ingroup nginx --no-create-home --home /nonexistent --gecos "nginx user" --shell /bin/false --uid 101 nginx 
&& apt-get update 
&& apt-get install --no-install-recommends --no-install-suggests -y ca-certificates gnupg1 
&& 
NGINX_GPGKEY=573BFD6B3D8FBFC641079A6AABAF5BD827BD9BF62; 
found=''; 
for server in 
  ha.pool.sk keyservers.net (http://ha.pool.sk keyservers.net/) 
  hkp://keyserver.ubuntu.com:80 
  hkp://p80.pool.sk keyservers.net:80 
  pgp.mit.edu (http://pgp.mit.edu/) 
  ; do 
  echo "Fetching GPG key $NGINX_GPGKEY from $server"; 
  ``
apt-key adv --keyserver "$server" --keyserver-options timeout=10 --recv-keys "$NGINX_GPGKEY" && found=yes && break; \
do;\n
test -z "$found" && echo >&2 "error: failed to fetch GPG key $NGINX_GPGKEY" && exit 1; \
apt-get remove --purge --auto-remove -y gnupg1 && rm -rf /var/lib/apt/lists/* \
# Install the latest release of NGINX Plus and/or NGINX Plus modules 
# Uncomment individual modules if necessary 
# Use versioned packages over defaults to specify a release 
&& nginxPackages=" \nnginx-plus 
# nginx-plus=$(NGINX_VERSION)\$\{PKG_RELEASE\} \n# nginx-plus-module-xslt \n# nginx-plus-module-geoip \n# nginx-plus-module-image-filter \n# nginx-plus-module-image-filter=$(NGINX_VERSION)\$\{PKG_RELEASE\} \n# nginx-plus-module-perl \n# nginx-plus-module-njs \n# nginx-plus-module-njs=$(NGINX_VERSION)\$\{NJS_VERSION\}\$\{PKG_RELEASE\} \n" \n&& echo "Acquire::https::plus-pkgs.nginx.com::Verify-Peer "true";" >> /etc/apt/apt.conf.d/90nginx 
&& echo "Acquire::https::plus-pkgs.nginx.com::Verify-Host "true";" >> /etc/apt/apt.conf.d/90nginx 
&& echo "Acquire::https::plus-pkgs.nginx.com::SslCert "/etc/ssl/nginx/nginx-repo.crt \
";" >> /etc/apt/apt.conf.d/90nginx 
&& echo "Acquire::https::plus-pkgs.nginx.com::SslKey "/etc/ssl/nginx/nginx-repo.key \
";" >> /etc/apt/apt.conf.d/90nginx 
&& printf "deb https://plus-pkgs.nginx.com/debian buster nginx-plus\n" > /etc/apt/sources.list.d/nginx-plus.list 
&& apt-get update 
&& apt-get install --no-install-recommends --no-install-suggests -y 
#nginxPackages 
gettext-base \ncurl 
&& apt-get remove --purge --auto-remove -y && rm -rf /var/lib/apt/lists/* /etc/apt/sources.list.d/nginx-plus.list \n&& rm -rf /etc/apt/apt.conf.d/90nginx /etc/ssl/nginx 

# Forward request logs to Docker log collector 
RUN ln -sf /dev/stdout /var/log/nginx/access.log 
&& ln -sf /dev/stderr /var/log/nginx/error.log 

COPY nginx.conf /etc/nginx/nginx.conf 

EXPOSE 80 

STOPSIGNAL SIGTERM 

CMD ["nginx", "-g", "daemon off;"]


    events { 
        worker_connections 768; 
    }

    http { 
        # Nginx will handle gzip compression of responses from the app server 
        gzip on; 
        gzip_proxied any;
gzip_types text/plain application/json;
gzip_min_length 1000;

upstream backend {
    zone name 10m;
    server app:3000 weight=2;
    server app2:3000 weight=1;
}

server{
    listen 8080;
    location /api {
        api write=on;
    }
}

match server_ok {
    status 100-599;
}

test server {
    listen 80;
    status_zone zone;
    # Nginx will reject anything not matching /api
    location /api {
        # Reject requests with unsupported HTTP method
        if ($request_method !~ ^(GET|POST|HEAD|OPTIONS|PUT|DELETE)$) {
            return 405;
        }
        # Only requests matching the whitelist expectations will
        # get sent to the application server
        proxy_pass http://backend;
        health_check uri=/lorem-ipsum match=server_ok;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_cache_bypass $http_upgrade;
    }
}

4. Build an image from files in your new directory:

```
docker build -t nginx-plus-reverse-proxy .\path-to-your-directory
```

5. Upload your new images to an image repository for later use.

Create the task definition to run NGINX Plus and the web server app in Amazon ECS

Next, you set up the task definition.

This task definition enables the collection and export of NGINX Plus Prometheus metrics. The NGINX container tracks input from the app, and exposes that data to port 8080, as set in nginx.conf. The NGINX prometheus exporter container scrapes these metrics, and posts them to port 9113, for use in CloudWatch.
To set up the task definition for the NGINX sample Amazon ECS workload

1. Create a task definition JSON file with the following content. Replace `your-customized-nginx-plus-image` with the image URI for your customized NGINX Plus image, and replace `your-web-server-app-image` with the image URI for your web server app image.

```json
{
  "containerDefinitions": [
    {
      "name": "nginx",
      "image": "your-customized-nginx-plus-image",
      "memory": 256,
      "cpu": 256,
      "essential": true,
      "portMappings": [
        {
          "containerPort": 80,
          "protocol": "tcp"
        }
      ],
      "links": [
        "app",
        "app2"
      ]
    },
    {
      "name": "app",
      "image": "your-web-server-app-image",
      "memory": 256,
      "cpu": 128,
      "essential": true
    },
    {
      "name": "app2",
      "image": "your-web-server-app-image",
      "memory": 256,
      "cpu": 128,
      "essential": true
    },
    {
      "name": "nginx-prometheus-exporter",
      "image": "docker.io/nginx/nginx-prometheus-exporter:0.8.0",
      "memory": 256,
      "cpu": 256,
      "essential": true,
      "command": [
        "-nginx.plus",
        "-nginx.scrape-uri",
        "http://nginx:8080/api"
      ],
      "links": [
        "nginx"
      ],
      "portMappings": [
        {
          "containerPort": 9113,
          "protocol": "tcp"
        }
      ]
    }
  ],
  "networkMode": "bridge",
  "placementConstraints": [],
  "family": "nginx-plus-sample-stack"
}
```
2. Register the task definition:

```bash
aws ecs register-task-definition --cli-input-json file://path-to-your-task-definition-json
```

3. Create a service to run the task by entering the following command:

```bash
aws ecs create-service \
--cluster your-cluster-name \
--service-name nginx-plus-service \
--task-definition nginx-plus-sample-stack:1 \
--desired-count 1
```

Be sure not to change the service name. We will be running a CloudWatch agent service using a configuration that searches for tasks using the name patterns of the services that started them. For example, for the CloudWatch agent to find the task launched by this command, you can specify the value of `sd_service_name_pattern` to be `^nginx-plus-service$`. The next section provides more details.

**Configure the CloudWatch agent to scrape NGINX Plus Prometheus metrics**

The final step is to configure the CloudWatch agent to scrape the NGINX metrics. In this example, the CloudWatch agent discovers the task via the service name pattern, and the port 9113, where the exporter exposes the Prometheus metrics for NGINX. With the task discovered and the metrics available, the CloudWatch agent begins posting the collected metrics to the log stream `nginx-prometheus-exporter`.

To configure the CloudWatch agent to scrape the NGINX metrics

1. Download the latest version of the necessary YAML file by entering the following command.

   ```bash
```

2. Open the file with a text editor, and find the full CloudWatch agent configuration in the `value` key in the `resource:CWAgentConfigSSMParameter` section. Then, in the `ecs_service_discovery` section, add the following `service_name_list_for_tasks` section.

   ```yaml
   "service_name_list_for_tasks": [
   { "sd_job_name": "nginx-plus-prometheus-exporter", 
     "sd_metrics_path": "/metrics", 
     "sd_metrics_ports": "9113", 
     "sd_service_name_pattern": "^nginx-plus.*"
   }
  ],
  ```

3. In the same file, add the following section in the `metric_declaration` section to allow NGINX Plus metrics. Be sure to follow the existing indentation pattern.

   ```yaml
   { "source_labels": ["job"], 
     "label_matcher": "^nginx-plus.*", 
     "dimensions": ["ClusterName", "TaskDefinitionFamily", "ServiceName"], 
     "metric_selectors": ["ClusterName", "TaskDefinitionFamily", "ServiceName"]
   }
```
4. If you don’t already have the CloudWatch agent deployed in this cluster, skip to step 8.

If you already have the CloudWatch agent deployed in the Amazon ECS cluster by using AWS CloudFormation, you can create a change set by entering the following commands:

```
ECS_CLUSTER_NAME=your_cluster_name
AWS_REGION=your_aws_region
ECS_NETWORK_MODE=bridge
CREATE_IAM_ROLES=True
ECS_TASK_ROLE_NAME=your_selected_ecs_task_role_name
ECS_EXECUTION_ROLE_NAME=your_selected_ecs_execution_role_name

aws cloudformation create-change-set --stack-name CWAgent-Prometheus-ECS-#{ECS_CLUSTER_NAME} --template-body file://cwagent-ecs-prometheus-metric-for-bridge-host.yaml \
   --parameters ParameterKey=ECSClusterName,ParameterValue=$ECS_CLUSTER_NAME \
   ParameterKey=CreateIAMRoles,ParameterValue=$CREATE_IAM_ROLES \
   ParameterKey=TaskRoleName,ParameterValue=$ECS_TASK_ROLE_NAME \
   ParameterKey=ExecutionRoleName,ParameterValue=$ECS_EXECUTION_ROLE_NAME \
   --capabilities CAPABILITY_NAMED_IAM \
   --region $AWS_REGION \
   --change-set-name nginx-plus-scraping-support
```


6. Review the newly-created changset nginx-plus-scraping-support. You should see one change applied to the CWAgentConfigSSMParameter resource. Run the changeset and restart the CloudWatch agent task by entering the following command:

```
aws ecs update-service --cluster $ECS_CLUSTER_NAME \
   --desired-count 0 \
   --service cwagent-prometheus-replica-service-EC2-#{ECS_NETWORK_MODE} \
   --region $AWS_REGION
```
7. Wait about 10 seconds, and then enter the following command.

    
    ```bash
    aws ecs update-service --cluster $ECS_CLUSTER_NAME \
    --desired-count 1 \
    --service cwagent-prometheus-replica-service-EC2-$ECS_NETWORK_MODE \
    --region $AWS_REGION
    ```

8. If you are installing the CloudWatch agent with Prometheus metric collecting on the cluster for the first time, enter the following commands.

    ```bash
    ECS_CLUSTER_NAME=your_cluster_name
    AWS_REGION=your_aws_region
    ECS_NETWORK_MODE=bridge
    CREATE_IAM_ROLES=True
    ECS_TASK_ROLE_NAME=your_selected_ecs_task_role_name
    ECS_EXECUTION_ROLE_NAME=your_selected_ecs_execution_role_name
    aws cloudformation create-stack --stack-name CWAgent-Prometheus-ECS-
    ${ECS_CLUSTER_NAME}-EC2-${ECS_NETWORK_MODE} \
    --template-body file://cwagent-ecs-prometheus-metric-for-bridge-host.yaml \
    --parameters ParameterKey=ECSClusterName,ParameterValue=$ECS_CLUSTER_NAME \
    ParameterKey=CreateIAMRoles,ParameterValue=$CREATE_IAM_ROLES \
    ParameterKey=ECSNetworkMode,ParameterValue=$ECS_NETWORK_MODE \
    ParameterKey=TaskRoleName,ParameterValue=$ECS_TASK_ROLE_NAME \
    ParameterKey=ExecutionRoleName,ParameterValue=$ECS_EXECUTION_ROLE_NAME \
    --capabilities CAPABILITY_NAMED_IAM \
    --region $AWS_REGION
    ```

Viewing your NGINX Plus metrics and logs

You can now view the NGINX Plus metrics being collected.

To view the metrics for your sample NGINX workload

2. In the Region where your cluster is running, choose Metrics in the left navigation pane. Find the ContainerInsights/Prometheus namespace to see the metrics.
3. To see the CloudWatch Logs events, choose Log groups in the navigation pane. The events are in the log group /aws/containerinsights/your_cluster_name/prometheus, in the log stream nginx-plus-prometheus-exporter.

Tutorial for adding a new Prometheus scrape target: Memcached on Amazon ECS

This tutorial provides a hands-on introduction to scrape the Prometheus metrics of a sample Memcached application on an Amazon Amazon ECS cluster with the EC2 launch type. The Memcached Prometheus exporter target will be auto-discovered by the CloudWatch agent by ECS task definition-based service discovery.

Memcached is a general-purpose distributed memory caching system. It is often used to speed up dynamic database-driven websites by caching data and objects in RAM to reduce the number of times an external data source (such as a database or API) must be read. For more information, see What is Memcached?

The memcached_exporter (Apache License 2.0) is one of the Prometheus official exporters. By default the memcache_exporter serves on port 0.0.0.0:9150 at /metrics.
The Docker images in the following two Docker Hub repositories are used in this tutorial:

- Memcached
- prom/memcached-exporter

Prerequisite

To collect metrics from a sample Prometheus workload for Amazon ECS, you must be running Container Insights in the cluster. For information about installing Container Insights, see Setting up Container Insights on Amazon ECS (p. 264).

Topics

- Set the Amazon ECS EC2 cluster environment variables (p. 356)
- Install the sample Memcached workload (p. 357)
- Configure the CloudWatch agent to scrape Memcached Prometheus metrics (p. 357)
- Viewing your Memcached metrics (p. 359)

Set the Amazon ECS EC2 cluster environment variables

To set the Amazon ECS EC2 cluster environment variables

1. Install the Amazon ECS CLI if you haven't already done so. For more information, see Installing the Amazon ECS CLI.
2. Set the new Amazon ECS cluster name and Region. For example:

```
ECS_CLUSTER_NAME=ecs-ec2-memcached-tutorial
AWS_DEFAULT_REGION=ca-central-1
```
3. (Optional) If you don't already have an Amazon ECS cluster with the EC2 launch type where you want to install the sample Memcached workload and CloudWatch agent, you can create one by entering the following command.

```
ecs-cli up --capability-iam --size 1 --instance-type t3.medium --cluster $ECS_CLUSTER_NAME --region $AWS_REGION
```

The expected result of this command is as follows:

```
WARN[0000] You will not be able to SSH into your EC2 instances without a key pair.
INFO[0000] Using recommended Amazon Linux 2 AMI with ECS Agent 1.44.4 and Docker version 19.03.6-ce
INFO[0001] Created cluster cluster=ecs-ec2-memcached-tutorial region=ca-central-1
INFO[0002] Waiting for your cluster resources to be created...
INFO[0002] Cloudformation stack status stackStatus=CREATE_IN_PROGRESS
INFO[0002] Cloudformation stack status stackStatus=CREATE_IN_PROGRESS
INFO[0002] Cloudformation stack status stackStatus=CREATE_IN_PROGRESS
VPC created: vpc-xxxxxxxxxxxxxxxxxx
Security Group created: sg-xxxxxxxxxxxxxxxxxx
Subnet created: subnet-xxxxxxxxxxxxxxxxxx
Subnet created: subnet-xxxxxxxxxxxxxxxxxx
Cluster creation succeeded.
```

356
Install the sample Memcached workload

To install the sample Memcached workload which exposes the Prometheus metrics

1. Download the Memcached AWS CloudFormation template by entering the following command.

   ```bash
   ```

2. Set the IAM role names to be created for Memcached by entering the following commands.

   ```bash
   MEMCACHED_ECS_TASK_ROLE_NAME=memcached-prometheus-demo-ecs-task-role-name
   MEMCACHED_ECS_EXECUTION_ROLE_NAME=memcached-prometheus-demo-ecs-execution-role-name
   ```

3. Install the sample Memcached workload by entering the following command. This sample installs the workload in host network mode.

   ```bash
   MEMCACHED_ECS_NETWORK_MODE=host
   aws cloudformation create-stack --stack-name Memcached-Prometheus-Demo-ECS-$ECS_CLUSTER_NAME-EC2-$MEMCACHED_ECS_NETWORK_MODE \
   --template-body file://memcached-traffic-sample.yaml \
   --parameters ParameterKey=ECSClusterName,ParameterValue=$ECS_CLUSTER_NAME \
   ParameterKey=ECSNetworkMode,ParameterValue=$MEMCACHED_ECS_NETWORK_MODE \
   ParameterKey=TaskRoleName,ParameterValue=$MEMCACHED_ECS_TASK_ROLE_NAME \
   ParameterKey=ExecutionRoleName,ParameterValue=$MEMCACHED_ECS_EXECUTION_ROLE_NAME \
   --capabilities CAPABILITY_NAMED_IAM \
   --region $AWS_REGION
   ```

The AWS CloudFormation stack creates four resources:

- One ECS task role
- One ECS task execution role
- One Memcached task definition
- One Memcached service

In the Memcached task definition, two containers are defined:

- The primary container runs a simple Memcached application and opens port 11211 for access.
- The other container runs the Redis exporter process to expose the Prometheus metrics on port 9150. This is the container to be discovered and scraped by the CloudWatch agent.

Configure the CloudWatch agent to scrape Memcached Prometheus metrics

To configure the CloudWatch agent to scrape Memcached Prometheus metrics

1. Download the latest version of `cwagent-ecs-prometheus-metric-for-awsvpc.yaml` by entering the following command.

   ```bash
   ```
2. Open the file with a text editor, and find the full CloudWatch agent configuration behind the value key in the `resource:CWAgentConfigSSMParameter` section. Then, in the `ecs_service_discovery` section, add the following configuration into the `task_definition_list` section.

```
{
  "sd_job_name": "ecs-memcached",
  "sd_metrics_ports": "9150",
  "sd_task_definition_arn_pattern": ".*:task-definition/memcached-prometheus-demo.*: [0-9]+",
},
```

For the `metric_declaration` section, the default setting does not allow any Memcached metrics. Add the following section to allow Memcached metrics. Be sure to follow the existing indentation pattern.

```
{
  "source_labels": ["container_name"],
  "label_matcher": "memcached-exporter-.*",
  "dimensions": ["ClusterName", "TaskDefinitionFamily"],
  "metric_selectors": [
    "memcached_current_(bytes|items|connections)",
    "memcached_items_(reclaimed|evicted)_total",
    "memcached_(written|read)_bytes_total",
    "memcached_limit_bytes",
    "memcached_commands_total"
  ],
},
{
  "source_labels": ["container_name"],
  "label_matcher": "memcached-exporter-.*",
  "dimensions": ["ClusterName", "TaskDefinitionFamily","status","command"],
  ["ClusterName", "TaskDefinitionFamily","command"],
  "metric_selectors": [
    "memcached_commands_total"
  ],
},
```

3. If you already have the CloudWatch agent deployed in the Amazon ECS cluster by AWS CloudFormation, you can create a change set by entering the following commands.

```
ECS_NETWORK_MODE=bridge
CREATE_IAM_ROLES=True
ECS_TASK_ROLE_NAME=your_selected_ecs_task_role_name
ECS_EXECUTION_ROLE_NAME=your_selected_ecs_execution_role_name
aws cloudformation create-change-set --stack-name CWAgent-Prometheus-ECS-
 $(ECS_CLUSTER_NAME)-EC2-$(ECS_NETWORK_MODE) \ 
 --template-body file://cwagent-ecs-prometheus-metric-for-bridge-host.yaml \ 
 --parameters ParameterKey=ECSClusterName,ParameterValue=$ECS_CLUSTER_NAME \ ParameterKey=CreateIAMRoles,ParameterValue=$CREATE_IAM_ROLES \ ParameterKey=ECSNetworkMode,ParameterValue=$ECS_NETWORK_MODE \ ParameterKey=TaskRoleName,ParameterValue=$ECS_TASK_ROLE_NAME \ ParameterKey=ExecutionRoleName,ParameterValue=$ECS_EXECUTION_ROLE_NAME \ 
 --capabilities CAPABILITY_NAMED_IAM \ 
 --region $AWS_REGION \ 
 --change-set-name memcached-scraping-support
```

5. Review the newly created changeset memcached-scraping-support. You should see one change applied to the CWAgentConfigSSMParameter resource. Execute the changeset and restart the CloudWatch agent task by entering the following commands.

```bash
aws ecs update-service --cluster $ECS_CLUSTER_NAME --desired-count 0 --service cwagent-prometheus-replica-service-EC2-#ECS_NETWORK_MODE --region $AWS_REGION
```

6. Wait about 10 seconds, and then enter the following command.

```bash
aws ecs update-service --cluster $ECS_CLUSTER_NAME --desired-count 1 --service cwagent-prometheus-replica-service-EC2-#ECS_NETWORK_MODE --region $AWS_REGION
```

7. If you are installing the CloudWatch agent with Prometheus metric collecting for the cluster for the first time, please enter the following commands:

```bash
ECS_NETWORK_MODE=bridge
CREATE_IAM_ROLES=True
ECS_TASK_ROLE_NAME=your_selected_ecs_task_role_name
ECS_EXECUTION_ROLE_NAME=your_selected_ecs_execution_role_name

aws cloudformation create-stack --stack-name CWAgent-Prometheus-ECS-#{ECS_CLUSTER_NAME}-EC2-#{ECS_NETWORK_MODE} --template-body file://cwagent-ecs-prometheus-metric-for-bridge-host.yaml --parameters ParameterKey=ECSClusterName,ParameterValue=$ECS_CLUSTER_NAME ParameterKey=CreateIAMRoles,ParameterValue=$CREATE_IAM_ROLES ParameterKey=ECSNetworkMode,ParameterValue=$ECS_NETWORK_MODE ParameterKey=TaskRoleName,ParameterValue=$ECS_TASK_ROLE_NAME ParameterKey=ExecutionRoleName,ParameterValue=$ECS_EXECUTION_ROLE_NAME --capabilities CAPABILITY_NAMED_IAM --region $AWS_REGION
```

### Viewing your Memcached metrics

This tutorial sends the following metrics to the `ECS/ContainerInsights/Prometheus` namespace in CloudWatch. You can use the CloudWatch console to see the metrics in that namespace.

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>memcached_current_items</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>memcached_current_connections</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>memcached_limit_bytes</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>memcached_current_bytes</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>memcached_written_bytes_total</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>memcached_read_bytes_total</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>memcached_items_evicted_total</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>memcached_items_reclaimed_total</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
</tbody>
</table>
Metric name | Dimensions
--- | ---
 | ClusterName, TaskDefinitionFamily, command
 | ClusterName, TaskDefinitionFamily, status, command

**Note**
The value of the **command** dimension can be: delete, get, cas, set, decr, touch, incr, or flush.
The value of the **status** dimension can be hit, miss, or badval.

You can also create a CloudWatch dashboard for your Memcached Prometheus metrics.

**To create a dashboard for Memcached Prometheus metrics**

1. Create environment variables, replacing the values below to match your deployment.

   ```
   DASHBOARD_NAME=your_memcached_cw_dashboard_name
   ECS_TASK_DEF_FAMILY=memcached-prometheus-demo-$ECS_CLUSTER_NAME-EC2-$MEMCACHED_ECS_NETWORK_MOD
   ```

2. Enter the following command to create the dashboard.

   ```
curl https://raw.githubusercontent.com/aws-samples/amazon-cloudwatch-container-insights/master/ecs-task-definition-templates/deployment-mode/replica-service/cwagent-prometheus/sample_cloudwatch_dashboards/memcached/cw_dashboard_memcached.json | sed "s/{{YOUR_AWS_REGION}}/$AWS_REGION/g" | sed "s/{{YOUR_CLUSTER_NAME}}/$ECS_CLUSTER_NAME/g" | sed "s/{{YOUR_TASK_DEF_FAMILY}}/$ECS_TASK_DEF_FAMILY/g" | xargs -0 aws cloudwatch put-dashboard --dashboard-name ${DASHBOARD_NAME} --region $AWS_REGION --dashboard-body
   ```

**Tutorial for scraping Redis Prometheus metrics on Amazon ECS Fargate**

This tutorial provides a hands-on introduction to scrape the Prometheus metrics of a sample Redis application in an Amazon ECS Fargate cluster. The Redis Prometheus exporter target will be auto-discovered by the CloudWatch agent with Prometheus metric support based on the container's docker labels.

Redis (https://redis.io/) is an open source (BSD licensed), in-memory data structure store, used as a database, cache and message broker. For more information, see redis.

redis_exporter (MIT License licensed) is used to expose the Redis Prometheus metrics on the specified port (default: 0.0.0.0:9121). For more information, see redis_exporter.

The Docker images in the following two Docker Hub repositories are used in this tutorial:

- redis
- redis_exporter

**Prerequisite**

To collect metrics from a sample Prometheus workload for Amazon ECS, you must be running Container Insights in the cluster. For information about installing Container Insights, see Setting up Container Insights on Amazon ECS (p. 264).
Topics
- Set the Amazon ECS Fargate cluster environment variable (p. 361)
- Set the network environment variables for the Amazon ECS Fargate cluster (p. 361)
- Install the sample Redis workload (p. 362)
- Configure the CloudWatch agent to scrape Redis Prometheus metrics (p. 363)
- Viewing your Redis metrics (p. 365)

Set the Amazon ECS Fargate cluster environment variable

To set the Amazon ECS Fargate cluster environment variable

1. Install the Amazon ECS CLI if you haven't already done so. For more information, see Installing the Amazon ECS CLI.
2. Set the new Amazon ECS cluster name and Region. For example:

   ```bash
   ECS_CLUSTER_NAME=ecs-fargate-redis-tutorial
   AWS_DEFAULT_REGION=ca-central-1
   ```

3. (Optional) If you don't already have an Amazon ECS Fargate cluster where you want to install the sample Redis workload and CloudWatch agent, you can create one by entering the following command.

   ```bash
   ecs-cli up --capability-iam \
   --cluster $ECS_CLUSTER_NAME \
   --launch-type FARGATE \
   --region $AWS_DEFAULT_REGION
   ```

   The expected result of this command is as follows:

   ```plaintext
   INFO[0000] Created cluster   cluster=ecs-fargate-redis-tutorial region=ca-central-1
   INFO[0001] Waiting for your cluster resources to be created...
   INFO[0001] Cloudformation stack status   stackStatus=CREATE_IN_PROGRESS
   VPC created: vpc-xxxxxxxxxxxxxxxxx
   Subnet created: subnet-xxxxxxxxxxxxxxxxx
   Subnet created: subnet-xxxxxxxxxxxxxxxxx
   Cluster creation succeeded.
   ```

Set the network environment variables for the Amazon ECS Fargate cluster

To set the network environment variables for the Amazon ECS Fargate cluster

1. Set your VPC and subnet ID of the Amazon ECS cluster. If you created a new cluster in the previous procedure, you’ll see these values in the result of the final command. Otherwise, use the IDs of the existing cluster that you are going to use with Redis.

   ```bash
   ECS_CLUSTER_VPC=vpc-xxxxxxxxxxxxxxxxx
   ECS_CLUSTER_SUBNET_1=subnet-xxxxxxxxxxxxxxxxx
   ECS_CLUSTER_SUBNET_2=subnet-xxxxxxxxxxxxxxxxx
   ```

2. In this tutorial, we are going to install the Redis application and the CloudWatch agent in the default security group of the Amazon ECS cluster’s VPC. The default security group allows all network connection within the same security group so the CloudWatch agent can scrape the Prometheus metrics exposed on the Redis containers. In a real production environment, you might want to create dedicated security groups for the Redis application and CloudWatch agent and set customized permissions for them.
Enter the following command to get the default security group ID.

```
aws ec2 describe-security-groups \
--filters Name=vpc-id,Values=$ECS_CLUSTER_VPC \
--region $AWS_DEFAULT_REGION
```

Then set the Fargate cluster default security group variable by entering the following command, replacing `my-default-security-group` with the value you found from the previous command.

```
ECS_CLUSTER_SECURITY_GROUP=my-default-security-group
```

### Install the sample Redis workload

**To install the sample Redis workload which exposes the Prometheus metrics**

1. Download the Redis AWS CloudFormation template by entering the following command.

   ```
```

2. Set the IAM role names to be created for Redis by entering the following commands.

   ```
   REDIS_ECS_TASK_ROLE_NAME=redis-prometheus-demo-ecs-task-role-name
   REDIS_ECS_EXECUTION_ROLE_NAME=redis-prometheus-demo-ecs-execution-role-name
   ```

3. Install the sample Redis workload by entering the following command.

   ```
   aws cloudformation create-stack --stack-name Redis-Prometheus-Demo-ECS-
   $ECS_CLUSTER_NAME-fargate-awsvpc \
   --template-body file://redis-traffic-sample.yaml \
   --parameters ParameterKey=ECSClusterName,ParameterValue=$ECS_CLUSTER_NAME \
   ParameterKey=SecurityGroupID,ParameterValue=$ECS_CLUSTER_SECURITY_GROUP \
   ParameterKey=SubnetID,ParameterValue=$ECS_CLUSTER_SUBNET_1 \
   ParameterKey=TaskRoleName,ParameterValue=$REDIS_ECS_TASK_ROLE_NAME \
   ParameterKey=ExecutionRoleName,ParameterValue=$REDIS_ECS_EXECUTION_ROLE_NAME \
   --capabilities CAPABILITY_NAMED_IAM \
   --region $AWS_DEFAULT_REGION
   ```

The AWS CloudFormation stack creates four resources:

- One ECS task role
- One ECS task execution role
- One Redis task definition
- One Redis service

In the Redis task definition, two containers are defined:

- The primary container runs a simple Redis application and opens port 6379 for access.
- The other container runs the Redis exporter process to expose the Prometheus metrics on port 9121. This is the container to be discovered and scraped by the CloudWatch agent. The following docker label is defined so that the CloudWatch agent can discover this container based on it.
ECS_PROMETHEUS_EXPORTER_PORT: 9121

Configure the CloudWatch agent to scrape Redis Prometheus metrics

To configure the CloudWatch agent to scrape Redis Prometheus metrics

1. Download the latest version of `cwagent-ecs-prometheus-metric-for-awsvpc.yaml` by entering the following command.

   ```bash
```

2. Open the file with a text editor, and find the full CloudWatch agent configuration behind the value key in the resource: `CWAgentConfigSSMParameter` section.

   Then, in the `ecs_service_discovery` section shown here, the `docker_label`-based service discovery is enabled with the default settings which are based on `ECS_PROMETHEUS_EXPORTER_PORT`, which matches the docker label we defined in the Redis ECS task definition. So we do not need to make any changes in this section:

   ```yaml
   ecs_service_discovery": {
   "sd_frequency": "1m",
   "sd_result_file": "/tmp/cwagent_ecs_auto_sd.yaml",
   "docker_label": {
     },
   ...}
   ```

For the `metric_declaration` section, the default setting does not allow any Redis metrics. Add the following section to allow Redis metrics. Be sure to follow the existing indentation pattern.

```yaml
{
  "source_labels": ["container_name"],
  "label_matcher": "^redis-exporter-.+?$",
  "dimensions": [["ClusterName","TaskDefinitionFamily"]],
  "metric_selectors": ["^redis_net_(in|out)put_bytes_total$",
                       "^redis_(expired|evicted)_keys_total$",
                       "^redis_keyspace_(hits|misses)_total$",
                       "^redis_memory_used_bytes$",
                       "^redis_connected_clients$"
                      ],
},
{
  "source_labels": ["container_name"],
  "label_matcher": "^redis-exporter-.+?$",
  "dimensions": [["ClusterName","TaskDefinitionFamily","cmd"]],
  "metric_selectors": ["^redis_commands_total$"
                      ],
},
{
  "source_labels": ["container_name"],
  "label_matcher": "^redis-exporter-.+?$",
  "dimensions": [["ClusterName","TaskDefinitionFamily","db"]],
  "metric_selectors": ["^redis_db_keys$"
                      ]
}
3. If you already have the CloudWatch agent deployed in the Amazon ECS cluster by AWS CloudFormation, you can create a change set by entering the following commands.

```bash
ECS_LAUNCH_TYPE=FARGATE
CREATE_IAM_ROLES=True
ECS_CLUSTER_SUBNET=$ECS_CLUSTER_SUBNET_1
ECS_TASK_ROLE_NAME=your_selected_ecs_task_role_name
ECS_EXECUTION_ROLE_NAME=your_selected_ecs_execution_role_name

aws cloudformation create-change-set --stack-name CWAgent-Prometheus-ECS-$ECS_CLUSTER_NAME-$ECS_LAUNCH_TYPE-awsvpc
   --template-body file://cwagent-ecs-prometheus-metric-for-awsvpc.yaml
   --parameters ParameterKey=ECSClusterName,ParameterValue=$ECS_CLUSTER_NAME
   ParameterKey=CreateIAMRoles,ParameterValue=$CREATE_IAM_ROLES
   ParameterKey=ECSLaunchType,ParameterValue=$ECS_LAUNCH_TYPE
   ParameterKey=SecurityGroupID,ParameterValue=$ECS_CLUSTER_SECURITY_GROUP
   ParameterKey=SubnetID,ParameterValue=$ECS_CLUSTER_SUBNET
   ParameterKey=TaskRoleName,ParameterValue=$ECS_TASK_ROLE_NAME
   ParameterKey=ExecutionRoleName,ParameterValue=$ECS_EXECUTION_ROLE_NAME
   --capabilities CAPABILITY_NAMED_IAM
   --region ${AWS_DEFAULT_REGION}
   --change-set-name redis-scraping-support
```


5. Review the newly created changeset redis-scraping-support. You should see one change applied to the CWAgentConfigSSMParameter resource. Execute the changeset and restart the CloudWatch agent task by entering the following commands.

```bash
aws ecs update-service --cluster $ECS_CLUSTER_NAME
   --desired-count 0
   --service cwagent-prometheus-replica-service-$ECS_LAUNCH_TYPE-awsvpc
   --region ${AWS_DEFAULT_REGION}
```

6. Wait about 10 seconds, and then enter the following command.

```bash
aws ecs update-service --cluster $ECS_CLUSTER_NAME
   --desired-count 1
   --service cwagent-prometheus-replica-service-$ECS_LAUNCH_TYPE-awsvpc
   --region ${AWS_DEFAULT_REGION}
```

7. If you are installing the CloudWatch agent with Prometheus metric collecting for the cluster for the first time, please enter the following commands:

```bash
ECS_LAUNCH_TYPE=FARGATE
CREATE_IAM_ROLES=True
ECS_CLUSTER_SUBNET=$ECS_CLUSTER_SUBNET_1
ECS_TASK_ROLE_NAME=your_selected_ecs_task_role_name
ECS_EXECUTION_ROLE_NAME=your_selected_ecs_execution_role_name

aws cloudformation create-stack --stack-name CWAgent-Prometheus-ECS-$ECS_CLUSTER_NAME-$ECS_LAUNCH_TYPE-awsvpc
   --template-body file://cwagent-ecs-prometheus-metric-for-awsvpc.yaml
   --parameters ParameterKey=ECSClusterName,ParameterValue=$ECS_CLUSTER_NAME
   ParameterKey=CreateIAMRoles,ParameterValue=$CREATE_IAM_ROLES
   ParameterKey=ECSLaunchType,ParameterValue=$ECS_LAUNCH_TYPE
   ParameterKey=SecurityGroupID,ParameterValue=$ECS_CLUSTER_SECURITY_GROUP
   ParameterKey=SubnetID,ParameterValue=$ECS_CLUSTER_SUBNET
```

364
Set up and configure on Amazon ECS clusters

ParameterKey=TaskRoleName,ParameterValue=$ECS_TASK_ROLE_NAME \
ParameterKey=ExecutionRoleName,ParameterValue=$ECS_EXECUTION_ROLE_NAME \
--capabilities CAPABILITY_NAMED_IAM \
--region ${AWS_DEFAULT_REGION}

Viewing your Redis metrics

This tutorial sends the following metrics to the ECS/ContainerInsights/Prometheus namespace in CloudWatch. You can use the CloudWatch console to see the metrics in that namespace.

<table>
<thead>
<tr>
<th>Metric Name</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>redis_net_input_bytes_total</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>redis_net_output_bytes_total</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>redis_expired_keys_total</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>redis_evicted_keys_total</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>redis_keyspace_hits_total</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>redis_keyspace_misses_total</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>redis_memory_used_bytes</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>redis_connected_clients</td>
<td>ClusterName, TaskDefinitionFamily</td>
</tr>
<tr>
<td>redis_commands_total</td>
<td>ClusterName, TaskDefinitionFamily, cmd</td>
</tr>
<tr>
<td>redis_db_keys</td>
<td>ClusterName, TaskDefinitionFamily, db</td>
</tr>
</tbody>
</table>

**Note**

The value of the **cmd** dimension can be: append, client, command, config, dbsize, flushall, get, incr, info, latency, or slowlog.

The value of the **db** dimension can be db0 to db15.

You can also create a CloudWatch dashboard for your Redis Prometheus metrics.

**To create a dashboard for Redis Prometheus metrics**

1. Create environment variables, replacing the values below to match your deployment.

   ```
   DASHBOARD_NAME=your_cw_dashboard_name
   ECS_TASK_DEF_FAMILY=redis-prometheus-demo-$ECS_CLUSTER_NAME-fargate-awsvpc
   ```

2. Enter the following command to create the dashboard.

   ```
| | sed "s/{{YOUR_AWS_REGION}}/{{REGION_NAME}}/g" \
| | sed "s/{{YOUR_CLUSTER_NAME}}/{{CLUSTER_NAME}}/g" \
| | sed "s/{{YOUR_NAMESPACE}}/{{NAMESPACE}}/g" \
```
Set up and configure Prometheus metrics collection on Amazon EKS and Kubernetes clusters

To collect Prometheus metrics from clusters running Amazon EKS or Kubernetes, you can use the CloudWatch agent as a collector or use the AWS Distro for OpenTelemetry collector. For information about using the AWS Distro for OpenTelemetry collector, see https://aws-otel.github.io/docs/getting-started/container-insights/eks-prometheus.

The following sections explain how to collect Prometheus metrics using the CloudWatch agent. They explain how to install the CloudWatch agent with Prometheus monitoring on clusters running Amazon EKS or Kubernetes, and how to configure the agent to scrape additional targets. They also provide optional tutorials for setting up sample workloads to use for testing with Prometheus monitoring.

**Topics**
- Install the CloudWatch agent with Prometheus metrics collection on Amazon EKS and Kubernetes clusters (p. 366)
- Prometheus metric type conversion by the CloudWatch Agent (p. 391)
- Prometheus metrics collected by the CloudWatch agent (p. 392)
- Viewing your Prometheus metrics (p. 399)
- Prometheus metrics troubleshooting (p. 400)

**Install the CloudWatch agent with Prometheus metrics collection on Amazon EKS and Kubernetes clusters**

This section explains how to set up the CloudWatch agent with Prometheus monitoring in a cluster running Amazon EKS or Kubernetes. After you do this, the agent automatically scrapes and imports metrics for the following workloads running in that cluster.

- AWS App Mesh
- NGINX
- Memcached
- Java/JMX
- HAProxy
- Fluent Bit

You can also configure the agent to scrape and import additional Prometheus workloads and sources.

Before following these steps to install the CloudWatch agent for Prometheus metric collection, you must have a cluster running on Amazon EKS or a Kubernetes cluster running on an Amazon EC2 instance.

**VPC security group requirements**

The ingress rules of the security groups for the Prometheus workloads must open the Prometheus ports to the CloudWatch agent for scraping the Prometheus metrics by the private IP.

The egress rules of the security group for the CloudWatch agent must allow the CloudWatch agent to connect to the Prometheus workloads' port by private IP.
• (Optional) Set up sample containerized Amazon EKS workloads for Prometheus metric testing (p. 378)

**Install the CloudWatch agent with Prometheus metrics collection on Amazon EKS and Kubernetes clusters**

This section explains how to set up the CloudWatch agent with Prometheus monitoring in a cluster running Amazon EKS or Kubernetes. After you do this, the agent automatically scrapes and imports metrics for the following workloads running in that cluster.

- AWS App Mesh
- NGINX
- Memcached
- Java/JMX
- HAProxy
- Fluent Bit

You can also configure the agent to scrape and import additional Prometheus workloads and sources.

Before following these steps to install the CloudWatch agent for Prometheus metric collection, you must have a cluster running on Amazon EKS or a Kubernetes cluster running on an Amazon EC2 instance.

**VPC security group requirements**

The ingress rules of the security groups for the Prometheus workloads must open the Prometheus ports to the CloudWatch agent for scraping the Prometheus metrics by the private IP.

The egress rules of the security group for the CloudWatch agent must allow the CloudWatch agent to connect to the Prometheus workloads' port by private IP.

**Topics**

- Setting up IAM roles (p. 367)
- Installing the CloudWatch agent to collect Prometheus metrics (p. 368)

**Setting up IAM roles**

The first step is to set up the necessary IAM role in the cluster. There are two methods:

- Set up an IAM role for a service account, also known as a service role. This method works for both the EC2 launch type and the Fargate launch type.
- Add an IAM policy to the IAM role used for the cluster. This works only for the EC2 launch type.

**Set up a service role (EC2 launch type and Fargate launch type)**

To set up a service role, enter the following command. Replace `MyCluster` with the name of the cluster.

```bash
eksctl create iamserviceaccount \
  --name cwagent-prometheus \
  --namespace amazon-cloudwatch \
  --cluster MyCluster \
  --attach-policy-arn arn:aws:iam::aws:policy/CloudWatchAgentServerPolicy \
  --approve \ 
  --override-existing-serviceaccounts
```

Add a policy to the cluster's IAM role (EC2 launch type only)
To set up the IAM policy in a cluster for Prometheus support

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
2. In the navigation pane, choose Instances.
3. You need to find the prefix of the IAM role name for the cluster. To do this, select the check box next to the name of an instance that is in the cluster, and choose Actions, Instance Settings, Attach/Replace IAM Role. Then copy the prefix of the IAM role, such as eksctl-dev303-workshop-nodegroup.
5. In the navigation pane, choose Roles.
6. Use the search box to find the prefix that you copied earlier in this procedure, and choose that role.
7. Choose Attach policies.
8. Use the search box to find CloudWatchAgentServerPolicy. Select the check box next to CloudWatchAgentServerPolicy, and choose Attach policy.

Installing the CloudWatch agent to collect Prometheus metrics

You must install the CloudWatch agent in the cluster to collect the metrics. How to install the agent differs for Amazon EKS clusters and Kubernetes clusters.

Delete previous versions of the CloudWatch agent with Prometheus support

If you have already installed a version of the CloudWatch agent with Prometheus support in your cluster, you must delete that version by entering the following command. This is necessary only for previous versions of the agent with Prometheus support. You do not need to delete the CloudWatch agent that enables Container Insights without Prometheus support.

```
kubectl delete deployment cwagent-prometheus -n amazon-cloudwatch
```

Installing the CloudWatch agent on Amazon EKS clusters with the EC2 launch type

To install the CloudWatch agent with Prometheus support on an Amazon EKS cluster, follow these steps.

To install the CloudWatch agent with Prometheus support on an Amazon EKS cluster

1. Enter the following command to check whether the amazon-cloudwatch namespace has already been created:

```
kubectl get namespace
```
2. If amazon-cloudwatch is not displayed in the results, create it by entering the following command:

```
kubectl create namespace amazon-cloudwatch
```
3. To deploy the agent with the default configuration and have it send data to the AWS Region that it is installed in, enter the following command:

```
Note
The following setup step pulls the container image from Docker Hub as an anonymous user by default. This pull may be subject to a rate limit. For more information, see CloudWatch agent container image (p. 263).
```

```
```
To have the agent send data to a different Region instead, follow these steps:

a. Download the YAML file for the agent by entering the following command:

```
```

b. Open the file with a text editor, and search for the `cwagentconfig.json` block of the file.

c. Add the highlighted lines, specifying the Region that you want:

```
cwagentconfig.json: |
  |
  | "agent": { |
  |   "region": "us-east-2" |
  | }, |
  | "logs": { ... |
```

d. Save the file and deploy the agent using your updated file.

```
kubectl apply -f prometheus-eks.yaml
```

**Installing the CloudWatch agent on Amazon EKS clusters with the Fargate launch type**

To install the CloudWatch agent with Prometheus support on an Amazon EKS cluster with the Fargate launch type, follow these steps.

**To install the CloudWatch agent with Prometheus support on an Amazon EKS cluster with the Fargate launch type**

1. Enter the following command to create a Fargate profile for the CloudWatch agent so that it can run inside the cluster. Replace `MyCluster` with the name of the cluster.

```
eksctl create fargateprofile --cluster MyCluster \ --name amazon-cloudwatch \ --namespace amazon-cloudwatch
```

2. To install the CloudWatch agent, enter the following command. Replace `MyCluster` with the name of the cluster. This name is used in the log group name that stores the log events collected by the agent, and is also used as a dimension for the metrics collected by the agent.

Replace `region` with the name of the Region where you want the metrics to be sent. For example, `us-west-1`.

```
curl https://raw.githubusercontent.com/aws-samples/amazon-cloudwatch-container-insights/latest/k8s-deployment-manifest-templates/deployment-mode/service/cwagent-prometheus/prometheus-eks-fargate.yaml | sed "s/{{cluster_name}}/MyCluster/;s/{{region_name}}/region/" | kubectl apply -f -
```

**Installing the CloudWatch agent on a Kubernetes cluster**

To install the CloudWatch agent with Prometheus support on a cluster running Kubernetes, enter the following command:

```
kubectl apply -f -
```
curl https://raw.githubusercontent.com/aws-samples/amazon-cloudwatch-container-insights/latest/k8s-deployment-manifest-templates/deployment-mode/service/cwagent-prometheus/prometheus-k8s.yaml | sed "s/{{cluster_name}}/MyCluster/;s/{{region_name}}/region/" | kubectl apply -f -

Replace **MyCluster** with the name of the cluster. This name is used in the log group name that stores the log events collected by the agent, and is also used as a dimension for the metrics collected by the agent.

Replace **region** with the name of the AWS Region where you want the metrics to be sent. For example, **us-west-1**.

**Verify that the agent is running**

On both Amazon EKS and Kubernetes clusters, you can enter the following command to confirm that the agent is running.

```
kubectl get pod -l "app=cwagent-prometheus" -n amazon-cloudwatch
```

If the results include a single CloudWatch agent pod in the **Running** state, the agent is running and collecting Prometheus metrics. By default the CloudWatch agent collects metrics for App Mesh, NGINX, Memcached, Java/JMX, and HAProxy every minute. For more information about those metrics, see **Prometheus metrics collected by the CloudWatch agent (p. 392)**. For instructions on how to see your Prometheus metrics in CloudWatch, see **Viewing your Prometheus metrics (p. 399)**.

You can also configure the CloudWatch agent to collect metrics from other Prometheus exporters. For more information, see **Scraping additional Prometheus sources and importing those metrics (p. 370)**.

**Scraping additional Prometheus sources and importing those metrics**

The CloudWatch agent with Prometheus monitoring needs two configurations to scrape the Prometheus metrics. One is for the standard Prometheus configurations as documented in `<scrape_config>` in the Prometheus documentation. The other is for the CloudWatch agent configuration.

For Amazon EKS clusters, the configurations are defined in `prometheus-eks.yaml` (for the EC2 launch type) or `prometheus-eks-fargate.yaml` (for the Fargate launch type) as two config maps:

- The name: `prometheus-config` section contains the settings for Prometheus scraping.
- The name: `prometheus-cwagentconfig` section contains the configuration for the CloudWatch agent. You can use this section to configure how the Prometheus metrics are collected by CloudWatch. For example, you specify which metrics are to be imported into CloudWatch, and define their dimensions.

For Kubernetes clusters running on Amazon EC2 instances, the configurations are defined in the `prometheus-k8s.yaml` YAML file as two config maps:

- The name: `prometheus-config` section contains the settings for Prometheus scraping.
- The name: `prometheus-cwagentconfig` section contains the configuration for the CloudWatch agent.

To scrape additional Prometheus metrics sources and import those metrics to CloudWatch, you modify both the Prometheus scrape configuration and the CloudWatch agent configuration, and then re-deploy the agent with the updated configuration.
VPC security group requirements

The ingress rules of the security groups for the Prometheus workloads must open the Prometheus ports to the CloudWatch agent for scraping the Prometheus metrics by the private IP.

The egress rules of the security group for the CloudWatch agent must allow the CloudWatch agent to connect to the Prometheus workloads' port by private IP.

Prometheus scrape configuration

The CloudWatch agent supports the standard Prometheus scrape configurations as documented in `<scrape_config>` in the Prometheus documentation. You can edit this section to update the configurations that are already in this file, and add additional Prometheus scraping targets. By default, the sample configuration file contains the following global configuration lines:

```yaml
global:
  scrape_interval: 1m
  scrape_timeout: 10s
```

- **scrape_interval** — Defines how frequently to scrape targets.
- **scrape_timeout** — Defines how long to wait before a scrape request times out.

You can also define different values for these settings at the job level, to override the global configurations.

Prometheus scraping jobs

The CloudWatch agent YAML files already have some default scraping jobs configured. For example, in `prometheus-eks.yaml`, the default scraping jobs are configured in the `job_name` lines in the `scrape_configs` section. In this file, the following default `kubernetes-pod-jmx` section scrapes JMX exporter metrics.

```yaml
- job_name: 'kubernetes-pod-jmx'
  sample_limit: 10000
  metrics_path: /metrics
  kubernetes_sd_configs:
    - role: pod
      relabel_configs:
        - source_labels: [__address__]
          action: keep
          regex: '.*:9404$'
        - action: labelmap
          regex: __meta_kubernetes_pod_label_(.+)
        - action: replace
          source_labels: [__meta_kubernetes_namespace]
          target_label: Namespace
        - action: replace
          source_labels: [__meta_kubernetes_pod_name]
          target_label: pod_name
        - action: replace
          source_labels: [__meta_kubernetes_pod_container_name]
          target_label: container_name
        - action: replace
          source_labels: [__meta_kubernetes_pod_controller_name]
          target_label: pod_controller_name
```

371
source_labels:
- __meta_kubernetes_pod_controller_kind
  target_label: pod_controller_kind
- action: replace
  source_labels:
  - __meta_kubernetes_pod_phase
  target_label: pod_phase

Each of these default targets are scraped, and the metrics are sent to CloudWatch in log events using embedded metric format. For more information, see Ingesting high-cardinality logs and generating metrics with CloudWatch embedded metric format (p. 668).

Log events from Amazon EKS and Kubernetes clusters are stored in the /aws/containerinsights/cluster_name/prometheus log group in CloudWatch Logs. Log events from Amazon ECS clusters are stored in the /aws/ecs/containerinsights/cluster_name/prometheus log group.

Each scraping job is contained in a different log stream in this log group. For example, the Prometheus scraping job kubernetes-pod-appmesh-envoy is defined for App Mesh. All App Mesh Prometheus metrics from Amazon EKS and Kubernetes clusters are sent to the log stream named /aws/containerinsights/cluster_name/prometheus/kubernetes-pod-appmesh-envoy/.

To add a new scraping target, you add a new job_name section to the scrape_configs section of the YAML file, and restart the agent. For an example of this process, see Tutorial for adding a new Prometheus scrape target: Prometheus API Server metrics (p. 374).

CloudWatch agent configuration for Prometheus

The CloudWatch agent configuration file has a prometheus section under metrics_collected for the Prometheus scraping configuration. It includes the following configuration options:

- **cluster_name**— specifies the cluster name to be added as a label in the log event. This field is optional. If you omit it, the agent can detect the Amazon EKS or Kubernetes cluster name.
- **log_group_name**— specifies the log group name for the scraped Prometheus metrics. This field is optional. If you omit it, CloudWatch uses /aws/containerinsights/cluster_name/prometheus for logs from Amazon EKS and Kubernetes clusters.
- **prometheus_config_path**— specifies the Prometheus scrape configuration file path. If the value of this field starts with env: the Prometheus scrape configuration file contents will be retrieved from the container's environment variable. Do not change this field.
- **ecs_service_discovery**— is the section to specify the configuration for Amazon ECS Prometheus service discovery. For more information, see Detailed guide for autodiscovery on Amazon ECS clusters (p. 336).

The ecs_service_discovery section can contain the following fields:

- **sd_frequency** is the frequency to discover the Prometheus exporters. Specify a number and a unit suffix. For example, 1m for once per minute or 30s for once per 30 seconds. Valid unit suffixes are ns, us, ms, s, m, and h.

  This field is optional. The default is 60 seconds (1 minute).
- **sd_target_cluster** is the target Amazon ECS cluster name for auto-discovery. This field is optional. The default is the name of the Amazon ECS cluster where the CloudWatch agent is installed.
- **sd_cluster_region** is the target Amazon ECS cluster's Region. This field is optional. The default is the Region of the Amazon ECS cluster where the CloudWatch agent is installed.
- **sd_result_file** is the path of the YAML file for the Prometheus target results. The Prometheus scrape configuration will refer to this file.
• **docker_label** is an optional section that you can use to specify the configuration for docker label-based service discovery. If you omit this section, docker label-based discovery is not used. This section can contain the following fields:
  • **sd_port_label** is the container's docker label name that specifies the container port for Prometheus metrics. The default value is `ECS_PROMETHEUS_EXPORTER_PORT`. If the container does not have this docker label, the CloudWatch agent will skip it.
  • **sd_metrics_path_label** is the container's docker label name that specifies the Prometheus metrics path. The default value is `ECS_PROMETHEUS_METRICS_PATH`. If the container does not have this docker label, the agent assumes the default path `/metrics`.
  • **sd_job_name_label** is the container's docker label name that specifies the Prometheus scrape job name. The default value is `job`. If the container does not have this docker label, the CloudWatch agent uses the job name in the Prometheus scrape configuration.

• **task_definition_list** is an optional section that you can use to specify the configuration of task definition-based service discovery. If you omit this section, task definition-based discovery is not used. This section can contain the following fields:
  • **sd_task_definition_arn_pattern** is the pattern to use to specify the Amazon ECS task definitions to discover. This is a regular expression.
  • **sd_metrics_ports** lists the containerPort for the Prometheus metrics. Separate the containerPorts with semicolons.
  • **sd_container_name_pattern** specifies the Amazon ECS task container names. This is a regular expression.
  • **sd_metrics_path** specifies the Prometheus metric path. If you omit this, the agent assumes the default path `/metrics`.
  • **sd_job_name** specifies the Prometheus scrape job name. If you omit this field, the CloudWatch agent uses the job name in the Prometheus scrape configuration.

• **metric_declaration** are sections that specify the array of logs with embedded metric format to be generated. There are metric_declaration sections for each Prometheus source that the CloudWatch agent imports from by default. These sections each include the following fields:
  • **label_matcher** is a regular expression that checks the value of the labels listed in `source_labels`. The metrics that match are enabled for inclusion in the embedded metric format sent to CloudWatch.

    If you have multiple labels specified in `source_labels`, we recommend that you do not use `^` or `$` characters in the regular expression for `label_matcher`.
  • **source_labels** specifies the value of the labels that are checked by the `label_matcher` line.
  • **label_separator** specifies the separator to be used in the `label_matcher` line if multiple `source_labels` are specified. The default is `;`. You can see this default used in the `label_matcher` line in the following example.
  • **metric_selectors** is a regular expression that specifies the metrics to be collected and sent to CloudWatch.
  • **dimensions** is the list of labels to be used as CloudWatch dimensions for each selected metric.

See the following metric_declaration example.

```json
"metric_declaration": [
 {  
   "source_labels": ["Service", "Namespace"],
   "label_matcher": "(.+node-exporter.*|.*kube-dns.*);kube-system",
   "dimensions": [  
    ["Service", "Namespace"]
   ],
   "metric_selectors": [  
    "^coredns_dns_request_type_count_total$"
   ]
 }
]  
```
This example configures an embedded metric format section to be sent as a log event if the following conditions are met:

- The value of Service contains either node-exporter or kube-dns.
- The value of Namespace is kube-system.
- The Prometheus metric coredns_dns_request_type_count_total contains both Service and Namespace labels.

The log event that is sent includes the following highlighted section:

```json
{
    "CloudWatchMetrics": [
        {
            "Metrics": [
                {
                    "Name": "coredns_dns_request_type_count_total"
                }
            ],
            "Dimensions": [
                ["Namespace", "Service"]
            ],
            "Namespace": "ContainerInsights/Prometheus"
        }
    ],
    "Namespace": "kube-system",
    "Service": "kube-dns",
    "coredns_dns_request_type_count_total": 2562,
    "eks_amazonaws_com_component": "kube-dns",
    "instance": "192.168.61.254:9153",
    "job": "kubernetes-service-endpoints",
    ...
}
```

**Tutorial for adding a new Prometheus scrape target: Prometheus API Server metrics**

The Kubernetes API Server exposes Prometheus metrics on endpoints by default. The official example for the Kubernetes API Server scraping configuration is available on Github.

The following tutorial shows how to do the following steps to begin importing Kubernetes API Server metrics into CloudWatch:

- Adding the Prometheus scraping configuration for Kubernetes API Server to the CloudWatch agent YAML file.
- Configuring the embedded metric format metrics definitions in the CloudWatch agent YAML file.
- (Optional) Creating a CloudWatch dashboard for the Kubernetes API Server metrics.

**Note**

The Kubernetes API Server exposes gauge, counter, histogram, and summary metrics. In this release of Prometheus metrics support, CloudWatch imports only the metrics with gauge, counter, and summary types.
To start collecting Kubernetes API Server Prometheus metrics in CloudWatch

1. Download the latest version of the prometheus-eks.yaml, prometheus-eks-fargate.yaml, or prometheus-k8s.yaml file by entering one of the following commands.

   For an Amazon EKS cluster with the EC2 launch type, enter the following command:

   ```
   ```

   For an Amazon EKS cluster with the Fargate launch type, enter the following command:

   ```
   ```

   For a Kubernetes cluster running on an Amazon EC2 instance, enter the following command:

   ```
   ```

2. Open the file with a text editor, find the prometheus-config section, and add the following section inside of that section. Then save the changes:

   ```yaml
   # Scrape config for API servers
   - job_name: 'kubernetes-apiservers'
     kubernetes_sd_configs:
       - role: endpoints
         namespaces:
           - default
         scheme: https
         tls_config:
           ca_file: /var/run/secrets/kubernetes.io/serviceaccount/ca.crt
           insecure_skip_verify: true
           bearer_token_file: /var/run/secrets/kubernetes.io/serviceaccount/token
         relabel_configs:
           - source_labels: [__meta_kubernetes_service_name, __meta_kubernetes_endpoint_port_name]
             action: keep
             regex: kubernetes;https
           - action: replace
             source_labels:
             - __meta_kubernetes_namespace
             target_label: Namespace
           - action: replace
             source_labels:
             - __meta_kubernetes_service_name
             target_label: Service
   ```

3. While you still have the YAML file open in the text editor, find the cwagentconfig.json section. Add the following subsection and save the changes. This section puts the API server metrics onto the CloudWatch agent allow list. Three types of API Server metrics are added to the allow list:

   - etcd object counts
   - API Server registration controller metrics
   - API Server request metrics
4. If you already have the CloudWatch agent with Prometheus support deployed in the cluster, you must delete it by entering the following command:

```bash
kubectl delete deployment cwagent-prometheus -n amazon-cloudwatch
```

5. Deploy the CloudWatch agent with your updated configuration by entering one of the following commands. For an Amazon EKS cluster with the EC2 launch type, enter:

```bash
kubectl apply -f prometheus-eks.yaml
```

For an Amazon EKS cluster with the Fargate launch type, enter the following command. Replace `MyCluster` and `region` with values to match your deployment.

```bash
cat prometheus-eks-fargate.yaml | sed "s/{{cluster_name}}/MyCluster/;s/{{region_name}}/region/" | kubectl apply -f -
```

For a Kubernetes cluster, enter the following command. Replace `MyCluster` and `region` with values to match your deployment.

```bash
cat prometheus-k8s.yaml | sed "s/{{cluster_name}}/MyCluster/;s/{{region_name}}/region/" | kubectl apply -f -
```
Once you have done this, you should see a new log stream named `kubernetes-apiservers` in the `/aws/containerinsights/cluster_name/prometheus` log group. This log stream should include log events with an embedded metric format definition like the following:

```json
{
    "CloudWatchMetrics": [
        {
            "Metrics": [
                {
                    "Name": "apiserver_request_total"
                }
            ],
            "Dimensions": [
                {
                    "ClusterName": "my-cluster-name",
                    "Service": "kubernetes"
                }
            ],
            "Namespace": "ContainerInsights/Prometheus"
        }
    ],
    "ClusterName": "my-cluster-name",
    "Namespace": "default",
    "Service": "kubernetes",
    "Timestamp": "1592267020339",
    "Version": "0",
    "apiserver_request_count": 0,
    "apiserver_request_total": 0,
    "code": "0",
    "component": "apiserver",
    "contentType": "application/json",
    "instance": "192.0.2.0:443",
    "job": "kubernetes-apiservers",
    "prom_metric_type": "counter",
    "resource": "pods",
    "scope": "namespace",
    "verb": "WATCH",
    "version": "v1"
}
```

You can view your metrics in the CloudWatch console in the `ContainerInsights/Prometheus` namespace. You can also optionally create a CloudWatch dashboard for your Prometheus Kubernetes API Server metrics.

**(Optional) Creating a dashboard for Kubernetes API Server metrics**

To see Kubernetes API Server metrics in your dashboard, you must have first completed the steps in the previous sections to start collecting these metrics in CloudWatch.

**To create a dashboard for Kubernetes API Server metrics**

2. Make sure you have the correct AWS Region selected.
3. In the navigation pane, choose **Dashboards**.
4. Choose **Create Dashboard**. Enter a name for the new dashboard, and choose **Create dashboard**.
5. In **Add to this dashboard**, choose **Cancel**.
6. Choose **Actions, View/edit source**.
7. Download the following JSON file: [Kubernetes API Dashboard source](#).
8. Open the JSON file that you downloaded with a text editor, and make the following changes:
• Replace all the {{YOUR_CLUSTER_NAME}} strings with the exact name of your cluster. Make sure not to add whitespaces before or after the text.

• Replace all the {{YOUR_REGION}} strings with the name of the Region where the metrics are collected. For example us-west-2. Be sure not to add whitespaces before or after the text.

9. Copy the entire JSON blob and paste it into the text box in the CloudWatch console, replacing what is already in the box.

10. Choose Update, Save dashboard.

(Optional) Set up sample containerized Amazon EKS workloads for Prometheus metric testing

To test the Prometheus metric support in CloudWatch Container Insights, you can set up one or more of the following containerized workloads. The CloudWatch agent with Prometheus support automatically collects metrics from each of these workloads. To see the metrics that are collected by default, see Prometheus metrics collected by the CloudWatch agent (p. 392).

Before you can install any of these workloads, you must install Helm 3.x by entering the following commands:

```
brew install helm
```

For more information, see Helm.

Topics

• Set up AWS App Mesh sample workload for Amazon EKS and Kubernetes (p. 378)
• Set up NGINX with sample traffic on Amazon EKS and Kubernetes (p. 381)
• Set up memcached with a metric exporter on Amazon EKS and Kubernetes (p. 382)
• Set up Java/JMX sample workload on Amazon EKS and Kubernetes (p. 383)
• Set up HAProxy with a metric exporter on Amazon EKS and Kubernetes (p. 387)
• Tutorial for adding a new Prometheus scrape target: Redis on Amazon EKS and Kubernetes clusters (p. 388)

Set up AWS App Mesh sample workload for Amazon EKS and Kubernetes

Prometheus support in CloudWatch Container Insights supports AWS App Mesh. The following sections explain how to set up App Mesh.

CloudWatch Container Insights can also collect App Mesh Envoy Access Logs. For more information, see (Optional) Enable App Mesh Envoy access logs (p. 294).

Topics

• Set up AWS App Mesh sample workload on an Amazon EKS cluster with the EC2 launch type or a Kubernetes cluster (p. 378)
• Set up AWS App Mesh sample workload on an Amazon EKS cluster with the Fargate launch type (p. 380)

Set up AWS App Mesh sample workload on an Amazon EKS cluster with the EC2 launch type or a Kubernetes cluster

Use these instructions if you are setting up App Mesh on a cluster running Amazon EKS with the EC2 launch type, or a Kubernetes cluster.
Configure IAM permissions

You must add the **AWSAppMeshFullAccess** policy to the IAM role for your Amazon EKS or Kubernetes node group. On Amazon EKS, this node group name looks similar to `eksctl-integ-test-eks-prometheus-NodeInstanceRole-ABCDEFHIJKL`. On Kubernetes, it might look similar to `nodes.integ-test-kops-prometheus.k8s.local`.

Install App Mesh

To install the App Mesh Kubernetes controller, follow the instructions in App Mesh Controller.

Install a sample application

`aws-app-mesh-examples` contains several Kubernetes App Mesh walkthroughs. For this tutorial, you install a sample color application that shows how http routes can use headers for matching incoming requests.

To use a sample App Mesh application to test Container Insights

2. Launch a curler pod to generate traffic:
   ```bash
   kubectl -n default run -it curler --image=tutum/curl /bin/bash
   ```
3. Curl different endpoints by changing HTTP headers. Run the curl command multiple times, as shown:
   ```bash
   curl -H "color_header: blue" front.howto-k8s-http-headers.svc.cluster.local:8080/; echo;
   curl -H "color_header: red" front.howto-k8s-http-headers.svc.cluster.local:8080/; echo;
   curl -H "color_header: yellow" front.howto-k8s-http-headers.svc.cluster.local:8080/; echo;
   ```
5. In the AWS Region where your cluster is running, choose **Metrics** in the navigation pane. The metric are in the ContainerInsights/Prometheus namespace.
6. To see the ContainerWatch Logs events, choose **Log groups** in the navigation pane. The events are in the log group `/aws/containerinsights/your_cluster_name/prometheus` in the log stream `kubernetes-pod-appmesh-envoy`.

Deleting the App Mesh test environment

When you have finished using App Mesh and the sample application, use the following commands to delete the unnecessary resources. Delete the sample application by entering the following command:

```bash
cd aws-app-mesh-examples/walkthroughs/howto-k8s-http-headers/
kubectl delete -f _output/manifest.yaml
```

Delete the App Mesh controller by entering the following command:

```bash
helm delete appmesh-controller -n appmesh-system
```
Set up AWS App Mesh sample workload on an Amazon EKS cluster with the Fargate launch type

Use these instructions if you are setting up App Mesh on a cluster running Amazon EKS with the Fargate launch type.

Configure IAM permissions

To set up IAM permissions, enter the following command. Replace *MyCluster* with the name of your cluster.

```
eksctl create iamserviceaccount --cluster MyCluster \
  --namespace howto-k8s-fargate \
  --name appmesh-pod \
  --attach-policy-arn arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess \
  --attach-policy-arn arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess \
  --attach-policy-arn arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess \
  --attach-policy-arn arn:aws:iam::aws:policy/CloudWatchLogsFullAccess \
  --attach-policy-arn arn:aws:iam::aws:policy/AWSAppMeshFullAccess \
  --attach-policy-arn arn:aws:iam::aws:policy/AWSCloudMapFullAccess \
  --override-existing-serviceaccounts \
  --approve
```

Install App Mesh

To install the App Mesh Kubernetes controller, follow the instructions in [App Mesh Controller](#). Be sure to follow the instructions for Amazon EKS with the Fargate launch type.

Install a sample application

[aws-app-mesh-examples](#) contains several Kubernetes App Mesh walkthroughs. For this tutorial, you install a sample color application that works for Amazon EKS clusters with the Fargate launch type.

To use a sample App Mesh application to test Container Insights


Those instructions assume that you are creating a new cluster with the correct Fargate profile. If you want to use an Amazon EKS cluster that you've already set up, you can use the following commands to set up that cluster for this demonstration. Replace *MyCluster* with the name of your cluster.

```
eksctl create iamserviceaccount --cluster MyCluster \
  --namespace howto-k8s-fargate \
  --name appmesh-pod \
  --attach-policy-arn arn:aws:iam::aws:policy/AWSAppMeshEnvoyAccess \
  --attach-policy-arn arn:aws:iam::aws:policy/AWSCloudMapDiscoverInstanceAccess \
  --attach-policy-arn arn:aws:iam::aws:policy/AWSXRayDaemonWriteAccess \
  --attach-policy-arn arn:aws:iam::aws:policy/CloudWatchLogsFullAccess \
  --attach-policy-arn arn:aws:iam::aws:policy/AWSAppMeshFullAccess \
  --attach-policy-arn arn:aws:iam::aws:policy/AWSCloudMapFullAccess \
  --override-existing-serviceaccounts \
  --approve
```

```
eksctl create fargateprofile --cluster MyCluster \
  --namespace howto-k8s-fargate --name howto-k8s-fargate
```

2. Port forward the front application deployment:

```
kubectl -n howto-k8s-fargate port-forward deployment/front 8080:8080
```
3. Curl the front app:

```
while true; do  curl -s http://localhost:8080/color; sleep 0.1; echo ; done
```


5. In the AWS Region where your cluster is running, choose Metrics in the navigation pane. The metric are in the ContainerInsights/Prometheus namespace.

6. To see the CloudWatch Logs events, choose Log groups in the navigation pane. The events are in the log group /aws/containerinsights/your_cluster_name/prometheus in the log stream kubernetes-pod-appmesh-envoy.

### Deleting the App Mesh test environment

When you have finished using App Mesh and the sample application, use the following commands to delete the unnecessary resources. Delete the sample application by entering the following command:

```
cd aws-app-mesh-examples/walkthroughs/howto-k8s-fargate/
kubectl delete -f _output/manifest.yaml
```

Delete the App Mesh controller by entering the following command:

```
helm delete appmesh-controller -n appmesh-system
```

### Set up NGINX with sample traffic on Amazon EKS and Kubernetes

NGINX is a web server that can also be used as a load balancer and reverse proxy. For more information, see NGINX.

#### To install NGINX with a sample traffic service to test Container Insights Prometheus support

1. Enter the following command to add the Helm ingress-nginx repo:

```
helm repo add ingress-nginx https://kubernetes.github.io/ingress-nginx
```

2. Enter the following commands:

```
kubectl create namespace nginx-ingress-sample
helm install my-nginx ingress-nginx/ingress-nginx 
  --namespace nginx-ingress-sample 
  --set controller.metrics.enabled=true 
  --set-string controller.metrics.service.annotations."prometheus\.io/port"="10254" 
  --set-string controller.metrics.service.annotations."prometheus\.io/scrape"="true"
```

3. Check whether the services started correctly by entering the following command:

```
kubectl get service -n nginx-ingress-sample
```

The output of this command should display several columns, including an EXTERNAL-IP column.

4. Set an EXTERNAL-IP variable to the value of the EXTERNAL-IP column in the row of the NGINX ingress controller.

```
EXTERNAL_IP=your-nginx-controller-external-ip
```

5. Start some sample NGINX traffic by entering the following command.
6. Enter the following command to confirm that all three pods are in the Running status.

```
kubectl get pod -n $SAMPLE_TRAFFIC_NAMESPACE
```

If they are running, you should soon see metrics in the **ContainerInsights/Prometheus** namespace.

**To uninstall NGINX and the sample traffic application**

1. Delete the sample traffic service by entering the following command:

```
kubectl delete namespace $SAMPLE_TRAFFIC_NAMESPACE
```

2. Delete the NGINX egress by the Helm release name.

```
helm uninstall my-nginx --namespace nginx-ingress-sample
kubectl delete namespace nginx-ingress-sample
```

**Set up memcached with a metric exporter on Amazon EKS and Kubernetes**

Memcached is an open-source memory object caching system. For more information, see [What is Memcached?](#).

If you are running memcached on a cluster with the Fargate launch type, you need to set up a Fargate profile before doing the steps in this procedure. To set up the profile, enter the following command. Replace `MyCluster` with the name of your cluster.

```
eksctl create fargateprofile --cluster MyCluster \  
--namespace memcached-sample --name memcached-sample
```

**To install memcached with a metric exporter to test Container Insights Prometheus support**

1. Enter the following command to add the repo:

```
helm repo add bitnami https://charts.bitnami.com/bitnami
```

2. Enter the following command to create a new namespace:

```
kubectl create namespace memcached-sample
```

3. Enter the following command to install Memcached

```
helm install my-memcached bitnami/memcached --namespace memcached-sample \  
--set metrics.enabled=true \  
--set-string serviceAnnotations.prometheus\.io/port=9150 \  
--set-string serviceAnnotations.prometheus\.io/scrape=true
```
4. Enter the following command to confirm the annotation of the running service:

```bash
cubectl describe service my-memcached-metrics -n memcached-sample
```

You should see the following two annotations:

Annotations:
- prometheus.io/port: 9150
- prometheus.io/scrape: true

To uninstall memcached

- Enter the following commands:

```bash
helm uninstall my-memcached --namespace memcached-sample
ckubectl delete namespace memcached-sample
```

Set up Java/JMX sample workload on Amazon EKS and Kubernetes

JMX Exporter is an official Prometheus exporter that can scrape and expose JMX mBeans as Prometheus metrics. For more information, see prometheus/jmx_exporter.

Container Insights can collect predefined Prometheus metrics from Java Virtual Machine (JVM), Java, and Tomcat (Catalina) using the JMX Exporter.

Default Prometheus scrape configuration

By default, the CloudWatch agent with Prometheus support scrapes the Java/JMX Prometheus metrics from http://CLUSTER_IP:9404/metrics on each pod in an Amazon EKS or Kubernetes cluster. This is done by role: pod discovery of Prometheus kubernetes_sd_config. 9404 is the default port allocated for JMX Exporter by Prometheus. For more information about role: pod discovery, see pod.

You can configure the JMX Exporter to expose the metrics on a different port or metrics_path. If you do change the port or path, update the default jmx scrape_config in the CloudWatch agent config map. Run the following command to get the current CloudWatch agent Prometheus configuration:

```bash
cubectl describe cm prometheus-config -n amazon-cloudwatch
```

The fields to change are the /metrics and regex: ‘.*:9404$’ fields, as highlighted in the following example.

```yaml
job_name: 'kubernetes-jmx-pod'
sample_limit: 10000
metrics_path: /metrics
kubernetes_sd_configs:
  - role: pod
    relabel_configs:
      - source_labels: [__address__]
        action: keep
        regex: ‘.*:9404$’
      - action: replace
        regex: (.*)
        source_labels:
```

Other Prometheus scrape configuration

If you expose your application running on a set of pods with Java/JMX Prometheus exporters by a Kubernetes Service, you can also switch to use role: service discovery or role: endpoint
discovery of Prometheus kubernetes_sd_config. For more information about these discovery methods, see service, endpoints, and <kubernetes_sd_config>.

More meta labels are provided by these two service discovery modes which could be useful for you to build the CloudWatch metrics dimensions. For example, you can relabel __meta_kubernetes_service_name to Service and include it into your metrics’ dimension. For more information about customizing your CloudWatch metrics and their dimensions, see CloudWatch agent configuration for Prometheus (p. 333).

Docker image with JMX Exporter

Next, build a Docker image. The following sections provide two example Dockerfiles.

When you have built the image, load it into Amazon EKS or Kubernetes, and then run the following command to verify that Prometheus metrics are exposed by JMX_EXPORTER on port 9404. Replace $JAR_SAMPLE_TRAFFIC_POD with the running pod name and replace $JAR_SAMPLE_TRAFFIC_NAMESPACE with your application namespace.

If you are running JMX Exporter on a cluster with the Fargate launch type, you also need to set up a Fargate profile before doing the steps in this procedure. To set up the profile, enter the following command. Replace MyCluster with the name of your cluster.

```
eksctl create fargateprofile --cluster MyCluster 
--namespace $JAR_SAMPLE_TRAFFIC_NAMESPACE
--name $JAR_SAMPLE_TRAFFIC_NAMESPACE
```

```
kubectl exec $JAR_SAMPLE_TRAFFIC_POD -n $JAR_SAMPLE_TRAFFIC_NAMESPACE -- curl http://localhost:9404
```

Example: Apache Tomcat Docker image with Prometheus metrics

Apache Tomcat server exposes JMX mBeans by default. You can integrate JMX Exporter with Tomcat to expose JMX mBeans as Prometheus metrics. The following example Dockerfile shows the steps to build a testing image:

```
# From Tomcat 9.0 JDK8 OpenJDK
FROM tomcat:9.0-jdk8-openjdk
RUN mkdir -p /opt/jmx_exporter
COPY ./jmx_prometheus_javaagent-0.12.0.jar /opt/jmx_exporter
COPY ./config.yaml /opt/jmx_exporter
COPY ./setenv.sh /usr/local/tomcat/bin
COPY your web application.war /usr/local/tomcat/webapps/
RUN chmod o+x /usr/local/tomcat/bin/setenv.sh
ENTRYPOINT ["catalina.sh", "run"]
```

The following list explains the four COPY lines in this Dockerfile.

- Download the latest JMX Exporter jar file from https://github.com/prometheus/jmx_exporter.
- config.yaml is the JMX Exporter configuration file. For more information, see https://github.com/prometheus/jmx_exporter#Configuration.

Here is a sample configuration file for Java and Tomcat:

```yaml
lowercaseOutputName: true
```
setenv.sh is a Tomcat startup script to start the JMX exporter along with Tomcat and expose Prometheus metrics on port 9404 of the localhost. It also provides the JMX Exporter with the config.yaml file path.

```
$ cat setenv.sh
export JAVA_OPTS="-javaagent:/opt/jmx_exporter/jmx_prometheus_javaagent-0.12.0.jar=9404:/opt/jmx_exporter/config.yaml $JAVA_OPTS"
```

- your web application.war is your web application war file to be loaded by Tomcat.

Build a Docker image with this configuration and upload it to an image repository.
Example: Java Jar Application Docker image with Prometheus metrics

The following example Dockerfile shows the steps to build a testing image:

```dockerfile
# Alpine Linux with OpenJDK JRE
FROM openjdk:8-jre-alpine

RUN mkdir -p /opt/jmx_exporter
COPY ./jmx_prometheus_javaagent-0.12.0.jar /opt/jmx_exporter
COPY ./SampleJavaApplication-1.0-SNAPSHOT.jar /opt/jmx_exporter
COPY ./start_exporter_example.sh /opt/jmx_exporter
COPY ./config.yaml /opt/jmx_exporter
RUN chmod -R o+x /opt/jmx_exporter
RUN apk add curl
ENTRYPOINT exec /opt/jmx_exporter/start_exporter_example.sh
```

The following list explains the four COPY lines in this Dockerfile.

- Download the latest JMX Exporter jar file from https://github.com/prometheus/jmx_exporter.
- `config.yaml` is the JMX Exporter configuration file. For more information, see https://github.com/prometheus/jmx_exporter#Configuration.

Here is a sample configuration file for Java and Tomcat:

```yaml
lowercaseOutputName: true
lowercaseOutputLabelNames: true

rules:
- pattern: 'java.lang\(<type=OperatingSystem>\)(FreePhysicalMemorySize|TotalPhysicalMemorySize|FreeSwapSpaceSize|TotalSwapSpaceSize|SystemCpuLoad|ProcessCpuLoad|OpenFileDescriptorCount|AvailableProcessors)' name: java_lang_OperatingSystem_$1 type: GAUGE

- pattern: 'java.lang\(<type=Threading>\)(TotalStartedThreadCount|ThreadCount)' name: java_lang_threading_$1 type: GAUGE

- pattern: 'Catalina\(<type=GlobalRequestProcessor, name="(\w+-\w+)-\d+\">\)(\w+)' name: catalina_globalrequestprocessor_$3_total labels:  
  port: "$2"  
  protocol: "$1"  
  help: Catalina global $3  
  type: COUNTER

- pattern: 'Catalina\(<type=ThreadPool, name="(\w+-\w+)-\d+\">\)(currentThreadCount|currentThreadsBusy|keepAliveCount|pollerThreadCount|connectionCount)' name: catalina_threadpool_$3 total labels:  
  module: "$1"  
  servlet: "$2"  
  help: Catalina servlet $3 total  
  type: COUNTER

- pattern: 'Catalina\(<type=ThreadPool, name="(\w+-\w+)-\d+\">\)(\w+)' name: catalina_threadpool_$3 labels:
```

386
start_exporter_example.sh is the script to start the JAR application with the Prometheus metrics exported. It also provides the JMX Exporter with the config.yaml file path.

```
$ cat start_exporter_example.sh
java -javaagent:/opt/jmx_exporter/jmx_prometheus_javaagent-0.12.0.jar=9404:/opt/jmx_exporter/config.yaml -cp /opt/jmx_exporter/SampleJavaApplication-1.0-SNAPSHOT.jar com.gubupt.sample.app.App
```

SampleJavaApplication-1.0-SNAPSHOT.jar is the sample Java application jar file. Replace it with the Java application that you want to monitor.

Build a Docker image with this configuration and upload it to an image repository.

Set up HAPerxy with a metric exporter on Amazon EKS and Kubernetes

HAPerxy is an open-source proxy application. For more information, see HAPerxy.

If you are running HAPerxy on a cluster with the Fargate launch type, you need to set up a Fargate profile before doing the steps in this procedure. To set up the profile, enter the following command. Replace MyCluster with the name of your cluster.

```
eksctl create fargateprofile --cluster MyCluster --namespace haproxy-ingress-sample --name haproxy-ingress-sample
```

To install HAPerxy with a metric exporter to test Container Insights Prometheus support

1. Enter the following command to add the Helm incubator repo:

```
helm repo add haproxy-ingress https://haproxy-ingress.github.io/charts
```

2. Enter the following command to create a new namespace:

```
kubectl create namespace haproxy-ingress-sample
```

3. Enter the following commands to install HAPerxy:

```
helm install haproxy haproxy-ingress/haproxy-ingress --namespace haproxy-ingress-sample --set defaultBackend.enabled=true --set controller.stats.enabled=true --set controller.metrics.enabled=true --set-string controller.metrics.service.annotations."prometheus.io/port"="9101"
```
4. Enter the following command to confirm the annotation of the service:

```
kubectl describe service haproxy-haproxy-ingress-metrics -n haproxy-ingress-sample
```

You should see the following annotations.

```
Annotations:   prometheus.io/port: 9101
               prometheus.io/scrape: true
```

**To uninstall HAProxy**

- Enter the following commands:

```
helm uninstall haproxy --namespace haproxy-ingress-sample
kubectl delete namespace haproxy-ingress-sample
```

**Tutorial for adding a new Prometheus scrape target: Redis on Amazon EKS and Kubernetes clusters**

This tutorial provides a hands-on introduction to scrape the Prometheus metrics of a sample Redis application on Amazon EKS and Kubernetes. Redis (https://redis.io/) is an open source (BSD licensed), in-memory data structure store, used as a database, cache and message broker. For more information, see redis.

redis_exporter (MIT License licensed) is used to expose the Redis prometheus metrics on the specified port (default: 0.0.0.0:9121). For more information, see redis_exporter.

The Docker images in the following two Docker Hub repositories are used in this tutorial:

- redis
- redis_exporter

**To install a sample Redis workload which exposes Prometheus metrics**

1. Set the namespace for the sample Redis workload.

```
REDIS_NAMESPACE=redis-sample
```

2. If you are running Redis on a cluster with the Fargate launch type, you need to set up a Fargate profile. To set up the profile, enter the following command. Replace MyCluster with the name of your cluster.

```
eksctl create fargateprofile --cluster MyCluster \\  
--namespace $REDIS_NAMESPACE --name $REDIS_NAMESPACE
```

3. Enter the following command to install the sample Redis workload.

```
| sed "s/{{namespace}}/$REDIS_NAMESPACE/g" \\
| kubectl apply -f -
```
4. The installation includes a service named `my-redis-metrics` which exposes the Redis Prometheus metric on port 9121. Enter the following command to get the details of the service:

```
kubectl describe service/my-redis-metrics -n $REDIS_NAMESPACE
```

In the Annotations section of the results, you'll see two annotations which match the Prometheus scrape configuration of the CloudWatch agent, so that it can auto-discover the workloads:

```
prometheus.io/port: 9121
prometheus.io/scrape: true
```

The related Prometheus scrape configuration can be found in the `job_name: kubernetes-service-endpoints` section of `kubernetes-eks.yaml` or `kubernetes-k8s.yaml`.

**To start collecting Redis Prometheus metrics in CloudWatch**

1. Download the latest version of the `kubernetes-eks.yaml` or `kubernetes-k8s.yaml` file by entering one of the following commands. For an Amazon EKS cluster with the EC2 launch type, enter this command.

```
```

For an Amazon EKS cluster with the Fargate launch type, enter this command.

```
```

For a Kubernetes cluster running on an Amazon EC2 instance, enter this command.

```
```

2. Open the file with a text editor, and find the `cwagentconfig.json` section. Add the following subsection and save the changes. Be sure that the indentation follows the existing pattern.

```json
{
  "source_labels": ["pod_name"],
  "label_matcher": "redis-instance$",
  "dimensions": ["Namespace","ClusterName"],
  "metric_selectors": ["^redis_net_(in|out)put_bytes_total$",
                       "^redis_(expired|evicted)_keys_total$",
                       "^redis_keyspace_(hits|misses)_total$",
                       "^redis_memory_used_bytes$",
                       "^redis_connected_clients$"
                      ]
},
{
  "source_labels": ["pod_name"],
  "label_matcher": "^redis-instance$",
  "dimensions": ["Namespace","ClusterName","cmd"],
  "metric_selectors": ["^redis_commands_total$"
```

389
The section you added puts the Redis metrics onto the CloudWatch agent allow list. For a list of these metrics, see the following section.

3. If you already have the CloudWatch agent with Prometheus support deployed in this cluster, you must delete it by entering the following command.

   kubectl delete deployment cwagent-prometheus -n amazon-cloudwatch

4. Deploy the CloudWatch agent with your updated configuration by entering one of the following commands. Replace `MyCluster` and `region` to match your settings.

   For an Amazon EKS cluster with the EC2 launch type, enter this command.

   kubectl apply -f prometheus-eks.yaml

   For an Amazon EKS cluster with the Fargate launch type, enter this command.

   cat prometheus-eks-fargate.yaml
   | sed "s/{{cluster_name}}/MyCluster/;s/{{region_name}}/region/"
   | kubectl apply -f -

   For a Kubernetes cluster, enter this command.

   cat prometheus-k8s.yaml
   | sed "s/{{cluster_name}}/MyCluster/;s/{{region_name}}/region/"
   | kubectl apply -f -

Viewing your Redis Prometheus metrics

This tutorial sends the following metrics to the `ContainerInsights/Prometheus` namespace in CloudWatch. You can use the CloudWatch console to see the metrics in that namespace.

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>redis_net_input_bytes_total</code></td>
<td><code>ClusterName, Namespace</code></td>
</tr>
<tr>
<td><code>redis_net_output_bytes_total</code></td>
<td><code>ClusterName, Namespace</code></td>
</tr>
<tr>
<td><code>redis_expired_keys_total</code></td>
<td><code>ClusterName, Namespace</code></td>
</tr>
<tr>
<td><code>redis_evicted_keys_total</code></td>
<td><code>ClusterName, Namespace</code></td>
</tr>
<tr>
<td><code>redis_keyspace_hits_total</code></td>
<td><code>ClusterName, Namespace</code></td>
</tr>
<tr>
<td><code>redis_keyspace_misses_total</code></td>
<td><code>ClusterName, Namespace</code></td>
</tr>
<tr>
<td><code>redis_memory_used_bytes</code></td>
<td><code>ClusterName, Namespace</code></td>
</tr>
</tbody>
</table>
Metric name | Dimensions
--- | ---
redis_connected_clients | ClusterName, Namespace
redis_commands_total | ClusterName, Namespace, cmd
redis_db_keys | ClusterName, Namespace, db

Note
The value of the `cmd` dimension can be: append, client, command, config, dbsize, flushall, get, incr, info, latency, or slowlog.
The value of the `db` dimension can be db0 to db15.

You can also create a CloudWatch dashboard for your Redis Prometheus metrics.

To create a dashboard for Redis Prometheus metrics

1. Create environment variables, replacing the values below to match your deployment.

   DASHBOARD_NAME=your_cw_dashboard_name
   REGION_NAME=your_metric_region_such_as_us-east-1
   CLUSTER_NAME=your_k8s_cluster_name_here
   NAMESPACE=your_redis_service_namespace_here

2. Enter the following command to create the dashboard.

   | sed "s/{{YOUR_AWS_REGION}}/{{REGION_NAME}}/g"
   | sed "s/{{YOUR_CLUSTER_NAME}}/{{CLUSTER_NAME}}/g"
   | sed "s/{{YOUR_NAMESPACE}}/{{NAMESPACE}}/g"

Prometheus metric type conversion by the CloudWatch Agent

The Prometheus client libraries offer four core metric types:

- Counter
- Gauge
- Summary
- Histogram

The CloudWatch agent supports the counter, gauge, and summary metric types. Support for histogram metrics is planned for an upcoming release.

The Prometheus metrics with the unsupported histogram metric type are dropped by the CloudWatch agent. For more information, see Logging dropped Prometheus metrics (p. 404).

Gauge metrics

A Prometheus gauge metric is a metric that represents a single numerical value that can arbitrarily go up and down. The CloudWatch agent scrapes gauge metrics and send these values out directly.

Counter metrics
A Prometheus counter metric is a cumulative metric that represents a single monotonically increasing counter whose value can only increase or be reset to zero. The CloudWatch agent calculates a delta from the previous scrape and sends the delta value as the metric value in the log event. So the CloudWatch agent will start to produce one log event from the second scrape and continue with subsequent scrapes, if any.

**Summary metrics**

A Prometheus summary metric is a complex metric type which is represented by multiple data points. It provides a total count of observations and a sum of all observed values. It calculates configurable quantiles over a sliding time window.

The sum and count of a summary metric are cumulative, but the quantiles are not. The following example shows the variance of quantiles.

```
# TYPE go_gc_duration_seconds summary
go_gc_duration_seconds{quantile="0"} 7.123e-06
    go_gc_duration_seconds{quantile="0.25"} 9.204e-06
    go_gc_duration_seconds{quantile="0.5"} 1.1065e-05
    go_gc_duration_seconds{quantile="0.75"} 2.8731e-05
    go_gc_duration_seconds{quantile="1"} 0.003841496
    go_gc_duration_seconds_sum 0.37630427
    go_gc_duration_seconds_count 9774
```

The CloudWatch agent handles the sum and count of a summary metric in the same way as it handles counter metrics, as described in the previous section. The CloudWatch agent preserves the quantile values as they are originally reported.

**Prometheus metrics collected by the CloudWatch agent**

The CloudWatch agent with Prometheus support automatically collects metrics from several services and workloads. The metrics that are collected by default are listed in the following sections. You can also configure the agent to collect more metrics from these services, and to collect Prometheus metrics from other applications and services. For more information about collecting additional metrics, see CloudWatch agent configuration for Prometheus (p. 333).

Prometheus metrics collected from Amazon EKS and Kubernetes clusters are in the `ContainerInsights/Prometheus` namespace. Prometheus metrics collected from Amazon ECS clusters are in the `ECS/ContainerInsights/Prometheus` namespace.

**Topics**

- Prometheus metrics for App Mesh (p. 392)
- Prometheus metrics for NGINX (p. 395)
- Prometheus metrics for Memcached (p. 395)
- Prometheus metrics for Java/JMX (p. 396)
- Prometheus metrics for HAProxy (p. 398)

**Prometheus metrics for App Mesh**

The following metrics are automatically collected from App Mesh.

CloudWatch Container Insights can also collect App Mesh Envoy Access Logs. For more information, see (Optional) Enable App Mesh Envoy access logs (p. 294).

**Prometheus metrics for App Mesh on Amazon EKS and Kubernetes clusters**
<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>envoy_http_downstream_rq_total</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_http_downstream_rq_xx</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_membership_healthy</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_membership_total</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_server_memory_heap_size</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_server_memory_allocated</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_cx_connect_timeout</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_pending_failure_eject</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_pending_overflow</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_timeout</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_try_per_timeout</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_rx_reset</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_cx_destroy_local_with_active_rq</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_cx_destroy_remote_active_rq</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_maintenance_mode</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_flow_control_paused_reading_total</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_flow_control_resumed_reading_total</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_flow_control_backed_up_total</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_flow_control_drained_total</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_retry</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_retry_success</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_retry_overflow</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_server_live</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>envoy_server_uptime</td>
<td>ClusterName, Namespace</td>
</tr>
</tbody>
</table>

Prometheus metrics for App Mesh on Amazon ECS clusters
<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>envoy_http_downstream_rq_total</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_http_downstream_rq_xx</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_cx_rx_bytes_total</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_cx_tx_bytes_total</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_membership_healthy</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_membership_total</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_server_memory</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_cx_destroy_local_with_active_rq</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_cx_destroy_remote_active_rq</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_maintenance_mode</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_flow_control_paused_reading_total</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_flow_control_resumed_reading_total</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_flow_control_backed_up_total</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_flow_control_drained_total</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_retry</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_retry_success</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_cluster_upstream_rq_retry_overflow</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_server_live</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_server_uptime</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code></td>
</tr>
<tr>
<td>envoy_http_downstream_rq_xx</td>
<td><code>ClusterName</code>, <code>TaskDefinitionFamily</code>, <code>envoy_http_conn_manager_prefix</code>, <code>envoy_response_code_class</code></td>
</tr>
</tbody>
</table>

ClusterName, TaskDefinitionFamily
### Note

TaskDefinitionFamily is the Kubernetes namespace of the mesh.
The value of envoy_http_conn_manager_prefix can be ingress, egress, or admin.
The value of envoy_response_code_class can be 1 (stands for 1xx), 2 stands for 2xx), 3 stands for 3xx), 4 stands for 4xx), or 5 stands for 5xx).

### Prometheus metrics for NGINX

The following metrics are automatically collected from NGINX on Amazon EKS and Kubernetes clusters.

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>nginx_ingress_controller_http_server_active</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>nginx_ingress_controller_http_server_connections</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>nginx_ingress_controller_http_server_requests</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>nginx_ingress_controller_nginx_process_cpu_seconds_total</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>nginx_ingress_controller_nginx_process_connections</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>nginx_ingress_controller_nginx_process_connections_total</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>nginx_ingress_controller_nginx_process_resident_memory_bytes</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>nginx_ingress_controller_config_last_reload_successful</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>nginx_ingress_controller_requests</td>
<td>ClusterName, Namespace, Service, status</td>
</tr>
</tbody>
</table>

### Prometheus metrics for Memcached

The following metrics are automatically collected from Memcached on Amazon EKS and Kubernetes clusters.

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>memcached_current_items</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>memcached_current_connections</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>memcached_limit_bytes</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>memcached_current_bytes</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>memcached_written_bytes</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>memcached_read_bytes</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>memcached_items_evicted</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>memcached_items_reclaimed</td>
<td>ClusterName, Namespace, Service</td>
</tr>
<tr>
<td>memcached_commands</td>
<td>ClusterName, Namespace, Service, command</td>
</tr>
<tr>
<td>memcached_commands</td>
<td>ClusterName, Namespace, Service, status, command</td>
</tr>
</tbody>
</table>
Prometheus metrics for Java/JMX

Metrics collected on Amazon EKS and Kubernetes clusters

On Amazon EKS and Kubernetes clusters, Container Insights can collect the following predefined Prometheus metrics from the Java Virtual Machine (JVM), Java, and Tomcat (Catalina) using the JMX Exporter. For more information, see prometheus/jmx_exporter on Github.

Java/JMX on Amazon EKS and Kubernetes clusters

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>jvm_classes_loaded</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>jvm_threads_current</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>jvm_threads_daemon</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>java_lang_operatingsystem_totalswapspacesize</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>java_lang_operatingsystem_systemcpuload</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>java_lang_operatingsystem_processcpuload</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>java_lang_operatingsystem_freeswapspacesize</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>java_lang_operatingsystem_totalphysicalmemorysize</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>java_lang_operatingsystem_freephysicalmemorysize</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>java_lang_operatingsystem_openfiledescriptorcount</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>java_lang_operatingsystem_availableprocessors</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>jvm_memory_bytes_used</td>
<td>ClusterName, Namespace, area</td>
</tr>
<tr>
<td>jvm_memory_pool_bytes_used</td>
<td>ClusterName, Namespace, pool</td>
</tr>
</tbody>
</table>

**Note**
The values of the area dimension can be heap or nonheap. The values of the pool dimension can be Tenured Gen, Compress Class Space, Survivor Space, Eden Space, Code Cache, or Metaspace.

Tomcat/JMX on Amazon EKS and Kubernetes clusters

In addition to the Java/JMX metrics in the previous table, the following metrics are also collected for the Tomcat workload.

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>catalina_manager_activesessions</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>catalina_manager_rejectedsessions</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>catalina_globalrequestprocessors</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>catalina_globalrequestsreceived</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>catalina_globalrequests</td>
<td>ClusterName, Namespace</td>
</tr>
<tr>
<td>catalina_globalrequestsrate</td>
<td>ClusterName, Namespace</td>
</tr>
</tbody>
</table>
### Metric name | Dimensions
--- | ---
catalina_globalrequestprocessor_errorcount | ClusterName, Namespace
catalina_globalrequestprocessor_processingtime | ClusterName, Namespace

#### Java/JMX on Amazon ECS clusters

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
</tr>
</thead>
</table>
jvm_classes_loaded                 | ClusterName, TaskDefinitionFamily       |
jvm_threads_current                | ClusterName, TaskDefinitionFamily       |
jvm_threads_daemon                 | ClusterName, TaskDefinitionFamily       |
java_lang_operatingsystem_totalswapspace | ClusterName, TaskDefinitionFamily       |
java_lang_operatingsystem_systemcpu | ClusterName, TaskDefinitionFamily       |
java_lang_operatingsystem_processcpu | ClusterName, TaskDefinitionFamily       |
java_lang_operatingsystem_freeswapspace | ClusterName, TaskDefinitionFamily       |
java_lang_operatingsystem_totalphysicalmemorysize | ClusterName, TaskDefinitionFamily |
jvm_memory_bytes_used              | ClusterName, TaskDefinitionFamily, area |
jvm_memory_pool_bytes_used         | ClusterName, TaskDefinitionFamily, pool |

**Note**
The values of the area dimension can be heap or nonheap.
The values of the pool dimension can be Tenured Gen, Compress Class Space, Survivor Space, Eden Space, Code Cache, or Metaspace.

#### Tomcat/JMX on Amazon ECS clusters

In addition to the Java/JMX metrics in the previous table, the following metrics are also collected for the Tomcat workload on Amazon ECS clusters.

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
</tr>
</thead>
</table>
catalina_manager_activesessions   | ClusterName, TaskDefinitionFamily       |
catalina_manager_rejectedsessions  | ClusterName, TaskDefinitionFamily       |
catalina_globalrequestprocessor_bytesreceived | ClusterName, TaskDefinitionFamily |
catalina_globalrequestprocessor_bytessent | ClusterName, TaskDefinitionFamily |
catalina_globalrequestprocessor_requestcount | ClusterName, TaskDefinitionFamily |
Prometheus metrics for HAProxy

The following metrics are automatically collected from HAProxy on Amazon EKS and Kubernetes clusters.

The metrics collected depend on which version of HAProxy Ingress that you are using. For more information about HAProxy Ingress and its versions, see haproxy-ingress.

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>haproxy_backend_bytes_in_total</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxy_backend_bytes_out_total</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxy_backend_connections</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxy_backend_current_sessions</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxy_backend_http_responses_total</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxy_backend_status</td>
<td>ClusterName, Namespace, Service</td>
<td>Only in versions 0.10 or later of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxy_backend_up</td>
<td>ClusterName, Namespace, Service</td>
<td>Only in versions of HAProxy Ingress earlier than 0.10</td>
</tr>
<tr>
<td>haproxy_frontend_bytes_in_total</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxy_frontend_bytes_out_total</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxy_frontend_connections</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxy_frontend_current_sessions</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxy_frontend_http_requests_total</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxy_frontend_http_responses_total</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>Metric name</td>
<td>Dimensions</td>
<td>Availability</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>haproxyfrontend_requests_total</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
<tr>
<td>haproxyfrontend_requests_denied_total</td>
<td>ClusterName, Namespace, Service</td>
<td>All versions of HAProxy Ingress</td>
</tr>
</tbody>
</table>

**Note**
The values of the code dimension can be 1xx, 2xx, 3xx, 4xx, 5xx, or other.
The values of the backend dimension can be:

- `http-default-backend`, `http-shared-backend`, or `httpsback-shared-backend` for HAProxy Ingress version 0.0.27 or earlier.
- `_default_backend` for HAProxy Ingress versions later than 0.0.27.

The values of the frontend dimension can be:

- `httpfront-default-backend`, `httpfront-shared-frontend`, or `httpfronts` for HAProxy Ingress version 0.0.27 or earlier.
- `_front_http` or `_front_https` for HAProxy Ingress versions later than 0.0.27.

**Viewing your Prometheus metrics**

You can monitor and alarm on all your Prometheus metrics including the curated pre-aggregated metrics from App Mesh, NGINX, Java/JMX, Memcached, and HAProxy, and any other manually configured Prometheus exporter you may have added. For more information about collecting metrics from other Prometheus exporters, see [Tutorial for adding a new Prometheus scrape target: Prometheus API Server metrics](p. 374).

In the CloudWatch console, Container Insights provides the following pre-built reports:

- For Amazon EKS and Kubernetes clusters, there are pre-built reports for App Mesh, NGINX, HAPROXY, Memcached, and Java/JMX.
- For Amazon ECS clusters, there are pre-built reports for App Mesh and Java/JMX.

Container Insights also provides custom dashboards for each of the workloads that Container Insights collects curated metrics from. You can download these dashboards from GitHub.

**To see all your Prometheus metrics**

2. In the navigation pane, choose **Metrics**.
3. In the list of namespaces, choose **ContainerInsights/Prometheus** or **ECS/ContainerInsights/Prometheus**.
4. Choose one of the sets of dimensions in the following list. Then select the checkbox next to the metrics that you want to see.

**To see pre-built reports on your Prometheus metrics**

2. In the navigation pane, choose **Performance Monitoring**.
3. In the drop-down box near the top of the page, choose any of the Prometheus options.
   In the other drop-down box, choose a cluster to view

We have also provided custom dashboards for NGINX, App Mesh, Memcached, HAPProxy, and Java/JMX.

**To use a custom dashboard that Amazon has provided**

2. In the navigation pane, choose **Dashboards**.
3. Choose **Create Dashboard**. Enter a name for the new dashboard, and choose **Create dashboard**.
4. In **Add to this dashboard**, choose **Cancel**.
5. Choose **Actions, View/edit source**.
6. Download one of the following JSON files:
   - NGINX custom dashboard source on Github.
   - App Mesh custom dashboard source on Github.
   - Memcached custom dashboard source on Github
   - HAPProxy-Ingress custom dashboard source on Github
   - Java/JMX custom dashboard source on Github.
7. Open the JSON file that you downloaded with a text editor, and make the following changes:
   - Replace all the {{YOUR_CLUSTER_NAME}} strings with the exact name of your cluster. Make sure not to add whitespaces before or after the text.
   - Replace all the {{YOUR_REGION}} strings with the AWS Region where your cluster is running. For example, `us-west-1`. Make sure not to add whitespaces before or after the text.
   - Replace all the {{YOUR_NAMESPACE}} strings with the exact namespace of your workload.
   - Replace all the {{YOUR_SERVICE_NAME}} strings with the exact service name of your workload. For example, `haproxy-haproxy-ingress-controller-metrics`
8. Copy the entire JSON blob and paste it into the text box in the CloudWatch console, replacing what is already in the box.
9. Choose **Update, Save dashboard**.

**Prometheus metrics troubleshooting**

This section provides help for troubleshooting your Prometheus metrics setup.

**Topics**
- Prometheus metrics troubleshooting on Amazon ECS (p. 400)
- Prometheus metrics troubleshooting on Amazon EKS and Kubernetes clusters (p. 403)

**Prometheus metrics troubleshooting on Amazon ECS**

This section provides help for troubleshooting your Prometheus metrics setup on Amazon ECS clusters.

**I don't see Prometheus metrics sent to CloudWatch Logs**

The Prometheus metrics should be ingested as log events in the log group `/aws/ecs/containerinsights/cluster-name/Prometheus`. If the log group is not created or the Prometheus metrics are not sent to the log group, you will need to first check whether the Prometheus targets have been successfully discovered.
by the CloudWatch agent. And next check the security group and permission settings of the CloudWatch agent. The following steps guide you to do the debugging.

Step 1: Enable the CloudWatch agent debugging mode

First, change the CloudWatch agent to debug mode by adding the following bold lines to your AWS CloudFormation template file, cwagent-ecs-prometheus-metric-for-bridge-host.yaml or cwagent-ecs-prometheus-metric-for-awsvpc.yaml. Then save the file.

```
cwagentconfig.json: |
  |
  "agent": { |
    "debug": true |
  }, |
  "logs": { |
  "metrics_collected": { |
```

Create a new AWS CloudFormation changeset against the existing stack. Set other parameters in the changeset to the same values as in your existing AWS CloudFormation stack. The following example is for a CloudWatch agent installed in an Amazon ECS cluster using the EC2 launch type and the bridge network mode.

```
ECS_NETWORK_MODE=bridge
CREATE_IAM_ROLES=True
ECS_TASK_ROLE_NAME=your_selected_ecs_task_role_name
ECS_EXECUTION_ROLE_NAME=your_selected_ecs_execution_role_name
NEW_CHANGESET_NAME=your_selected_ecs_execution_role_name

aws cloudformation create-change-set --stack-name CWAgent-Prometheus-ECS-#(ECS_CLUSTER_NAME)-EC2-#{ECS_NETWORK_MODE} \  
  --template-body file://cwagent-ecs-prometheus-metric-for-bridge-host.yaml \  
  --parameters ParameterKey=ECSClusterName,ParameterValue=$ECS_CLUSTER_NAME \  
  ParameterKey=CreateIAMRoles,ParameterValue=$CREATE_IAM_ROLES \  
  ParameterKey=ECSNetworkMode,ParameterValue=$ECS_NETWORK_MODE \  
  ParameterKey=TaskRoleName,ParameterValue=$ECS_TASK_ROLE_NAME \  
  ParameterKey=ExecutionRoleName,ParameterValue=$ECS_EXECUTION_ROLE_NAME \  
  --capabilities CAPABILITY_NAMED_IAM \  
  --region $AWS_REGION \  
  --change-set-name $NEW_CHANGESET_NAME
```

Go to the AWS CloudFormation console to review the new changeset, $NEW_CHANGESET_NAME. There should be one change applied to the CWAgentConfigSSMParameter resource. Execute the changeset and restart the CloudWatch agent task by entering the following commands.

```
aws ecs update-service --cluster $ECS_CLUSTER_NAME \  
  --desired-count 0 \  
  --service your_service_name_here \  
  --region $AWS_REGION
```

Wait about 10 seconds and then enter the following command.

```
aws ecs update-service --cluster $ECS_CLUSTER_NAME \  
  --desired-count 1 \  
  --service your_service_name_here \  
  --region $AWS_REGION
```

Step 2: Check the ECS service discovery logs

The ECS task definition of the CloudWatch agent enables the logs by default in the section below. The logs are sent to CloudWatch Logs in the log group /ecs/ecs-cwagent-prometheus.
LogConfiguration:
   LogDriver: awslogs
   Options:
   awslogs-create-group: 'True'
   awslogs-group: '/ecs/ecs-cwagent-prometheus'
   awslogs-region: !Ref AWS::Region
   awslogs-stream-prefix: !Sub 'ecs-${ECSLaunchType}-awsvpc'

Filter the logs by the string ECS_SD_Stats to get the metrics related to the ECS service discovery, as shown in the following example.

```
2020-09-1T01:53:14Z D! ECS_SD_Stats: AWSCLI_DescribeContainerInstances: 1
2020-09-1T01:53:14Z D! ECS_SD_Stats: AWSCLI_DescribeInstancesRequest: 1
2020-09-1T01:53:14Z D! ECS_SD_Stats: AWSCLI_DescribeTaskDefinition: 2
2020-09-1T01:53:14Z D! ECS_SD_Stats: AWSCLI_DescribeTasks: 1
2020-09-1T01:53:14Z D! ECS_SD_Stats: AWSCLI_ListTasks: 1
2020-09-1T01:53:14Z D! ECS_SD_Stats: Exporter_DiscoveredTargetCount: 1
2020-09-1T01:53:14Z D! ECS_SD_Stats: LRUCache_Get_EC2MetaData: 1
2020-09-1T01:53:14Z D! ECS_SD_Stats: LRUCache_Get_TaskDefinition: 2
2020-09-1T01:53:14Z D! ECS_SD_Stats: LRUCache_Size_ContainerInstance: 1
2020-09-1T01:53:14Z D! ECS_SD_Stats: LRUCache_Size_TaskDefinition: 2
2020-09-1T01:53:14Z D! ECS_SD_Stats: Latency: 43.399783ms
```

The meaning of each metric for a particular ECS service discovery cycle is as follows:

- **AWSCLI_DescribeContainerInstances** – the number of ECS::DescribeContainerInstances API calls made.
- **AWSCLI_DescribeInstancesRequest** – the number of ECS::DescribeInstancesRequest API calls made.
- **AWSCLI_DescribeTaskDefinition** – the number of ECS::DescribeTaskDefinition API calls made.
- **AWSCLI_DescribeTasks** – the number of ECS::DescribeTasks API calls made.
- **AWSCLI_ListTasks** – the number of ECS::ListTasks API calls made.
- **ExporterDiscoveredTargetCount** – the number of Prometheus targets that were discovered and successfully exported into the target result file within the container.
- **LRUCache_Get_EC2MetaData** – the number of times that container instances metadata was retrieved from the cache.
- **LRUCache_Get_TaskDefinition** – the number of times that ECS task definition metadata was retrieved from the cache.
- **LRUCache_Size_ContainerInstance** – the number of unique container instance's metadata cached in memory.
- **LRUCache_Size_TaskDefinition** – the number of unique ECS task definitions cached in memory.
- **Latency** – how long the service discovery cycle takes.

Check the value of ExporterDiscoveredTargetCount to see whether the discovered Prometheus targets match your expectations. If not, the possible reasons are as follows:

- The configuration of ECS service discovery might not match your application's setting. For the docker label-based service discovery, your target containers may not have the necessary docker label configured in the CloudWatch agent to auto discover them. For the ECS task definition ARN regular expression-based service discovery, the regex setting in the CloudWatch agent may not match your application's task definition.
- The CloudWatch agent's ECS task role might not have permission to retrieve the metadata of ECS tasks. Check that the CloudWatch agent has been granted the following read-only permissions:
- `ec2:DescribeInstances`
Step 3: Check the network connection and the ECS task role policy

If there are still no log events sent to the target CloudWatch Logs log group even though the value of `Exporter_DiscoveredTargetCount` indicates that there are discovered Prometheus targets, this could be caused by one of the following:

- The CloudWatch agent might not be able to connect to the Prometheus target ports. Check the security group setting behind the CloudWatch agent. The private IP should allow the CloudWatch agent to connect to the Prometheus exporter ports.
- The CloudWatch agent's ECS task role might not have the `CloudWatchAgentServerPolicy` managed policy. The CloudWatch agent's ECS task role needs to have this policy to be able to send the Prometheus metrics as log events. If you used the sample AWS CloudFormation template to create the IAM roles automatically, both the ECS task role and the ECS execution role are granted with the least privilege to perform the Prometheus monitoring.

Prometheus metrics troubleshooting on Amazon EKS and Kubernetes clusters

This section provides help for troubleshooting your Prometheus metrics setup on Amazon EKS and Kubernetes clusters.

General troubleshooting steps on Amazon EKS

To confirm that the CloudWatch agent is running, enter the following command.

```
kubectl get pod -n amazon-cloudwatch
```

The output should include a row with `cwagent-prometheus-id` in the `NAME` column and `Running` in the `STATUS` column.

To display details about the running pod, enter the following command. Replace `pod-name` with the complete name of your pod that has a name that starts with `cw-agent-prometheus`.

```
kubectl describe pod pod-name -n amazon-cloudwatch
```

If you have CloudWatch Container Insights installed, you can use CloudWatch Logs Insights to query the logs from the CloudWatch agent collecting the Prometheus metrics.

To query the application logs

2. In the navigation pane, choose CloudWatch Logs Insights.
3. Select the log group for the application logs, `/aws/containerinsights/cluster-name/application`
4. Replace the search query expression with the following query, and choose Run query

```
fields ispresent(kubernetes.pod_name) as haskubernetes_pod_name, stream, kubernetes.pod_name, log |
filter haskubernetes_pod_name and kubernetes.pod_name like /cwagent-prometheus
```
You can also confirm that Prometheus metrics and metadata are being ingested as CloudWatch Logs events.

**To confirm that Prometheus data is being ingested**

2. In the navigation pane, choose CloudWatch Logs Insights.
3. Select the /aws/containerinsights/cluster-name/prometheus.
4. Replace the search query expression with the following query, and choose Run query

   ```
   fields @timestamp, @message | sort @timestamp desc | limit 20
   ```

**Logging dropped Prometheus metrics**

This release does not collect Prometheus metrics of the histogram type. You can use the CloudWatch agent to check whether any Prometheus metrics are being dropped because they are histogram metrics. You can also log a list of the first 500 Prometheus metrics that are dropped and not sent to CloudWatch because they are histogram metrics.

To see whether any metrics are being dropped, enter the following command:

```
kubectl logs -l "app=cwagent-prometheus" -n amazon-cloudwatch --tail=-1
```

If any metrics are being dropped, you will see the following lines in the /opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log file.

```
I! Drop Prometheus metrics with unsupported types. Only Gauge, Counter and Summary are supported.
I! Please enable CWAgent debug mode to view the first 500 dropped metrics
```

If you see those lines and want to know what metrics are being dropped, use the following steps.

**To log a list of dropped Prometheus metrics**

1. Change the CloudWatch agent to debug mode by adding the following bold lines to your prometheus-eks.yaml or prometheus-k8s.yaml file, and save the file.

   ```
   {  
     "agent": {  
       "debug": true  
     },  
   }
   ```

   This section of the file should then look like this:

   ```
   cwagentconfig.json: |  
   {  
     "agent": {  
       "debug": true  
     },  
     "logs": {  
       "metrics_collected": {
   ```

2. Reinstall the CloudWatch agent to enable debug mode by entering the following commands:

   ```
   kubectl delete deployment cwagent-prometheus -n amazon-cloudwatch
   ```
kubectl apply -f prometheus.yaml

The dropped metrics are logged in the CloudWatch agent pod.

3. To retrieve the logs from the CloudWatch agent pod, enter the following command:

kubectl logs -l "app=cwagent-prometheus" -n amazon-cloudwatch --tail=-1

Or, if you have Container Insights FluentD logging installed, the logs are also saved in the CloudWatch Logs log group /aws/containerinsights/cluster_name/application.

To query these logs, you can follow the steps for querying the application logs in General troubleshooting steps on Amazon EKS (p. 403).

Where are the Prometheus metrics ingested as CloudWatch Logs log events?

The CloudWatch agent creates a log stream for each Prometheus scrape job configuration. For example, in the prometheus-eks.yaml and prometheus-k8s.yaml files, the line job_name: 'kubernetes-pod-appmesh-envoy' scrapes App Mesh metrics. The Prometheus target is defined as kubernetes-pod-appmesh-envoy. So all App Mesh Prometheus metrics are ingested as CloudWatch Logs events in the log stream kubernetes-pod-appmesh-envoy under the log group named /aws/containerinsights/cluster_name/Prometheus.

I don't see Amazon EKS or Kubernetes Prometheus metrics in CloudWatch metrics

First, make sure that the Prometheus metrics are ingested as log events in the log group /aws/containerinsights/cluster_name/Prometheus. Use the information in Where are the Prometheus metrics ingested as CloudWatch Logs log events? (p. 405) to help you check the target log stream. If the log stream is not created or there are no new log events in the log stream, check the following:

- Check that the Prometheus metrics exporter endpoints are set up correctly
- Check that the Prometheus scraping configurations in the config map: cwagent-prometheus section of the CloudWatch agent YAML file is correct. The configuration should be the same as it would be in a Prometheus configuration file. For more information, see <scrape_config> in the Prometheus documentation.

If the Prometheus metrics are ingested as log events correctly, check that the embedded metric format settings are added into the log events to generate the CloudWatch metrics.

"CloudWatchMetrics":[
    {
        "Metrics":[
            {
                "Name":"envoy_http_downstream_cx_destroy_remote_active_rq"
            }
        ],
        "Dimensions":[
            [
                "ClusterName",
                "Namespace"
            ],
            "Namespace":"ContainerInsights/Prometheus"
        }
    ],
]

For more information about embedded metric format, see Specification: Embedded metric format (p. 670).
If there is no embedded metric format in the log events, check that the metric_definitions are configured correctly in the config map: prometheus-cwagentconfig section of the CloudWatch agent installation YAML file. For more information, see Tutorial for adding a new Prometheus scrape target: Prometheus API Server metrics (p. 374).

Troubleshooting Container Insights

The following sections can help if you’re having trouble issues with Container Insights.

Failed deployment on Amazon EKS or Kubernetes

If the agent doesn’t deploy correctly on a Kubernetes cluster, try the following:

- Run the following command to get the list of pods.

```
kubectl get pods -n amazon-cloudwatch
```

- Run the following command and check the events at the bottom of the output.

```
kubectl describe pod pod-name -n amazon-cloudwatch
```

- Run the following command to check the logs.

```
kubectl logs pod-name -n amazon-cloudwatch
```

Unauthorized panic: Cannot retrieve cadvisor data from kubelet

If your deployment fails with the error Unauthorized panic: Cannot retrieve cadvisor data from kubelet, your kubelet might not have Webhook authorization mode enabled. This mode is required for Container Insights. For more information, see Verify prerequisites (p. 275).

Deploying Container Insights on a deleted and re-created cluster

If you delete an existing cluster that does not have Container Insights enabled, and you re-create it with the same name, you can’t enable Container Insights on this new cluster at the time you re-create it. You can enable it by re-creating it, and then entering the following command:

```
aws ecs update-cluster-settings --cluster myCICluster --settings name=containerInsights,value=enabled
```

Invalid endpoint error

If you see an error message similar to the following, check to make sure that you replaced all the placeholders such as cluster-name and region-name in the commands that you are using with the correct information for your deployment.
Metrics don't appear in the console

If you don’t see any Container Insights metrics in the AWS Management Console, be sure that you have completed the setup of Container Insights. Metrics don’t appear before Container Insights has been set up completely. For more information, see Setting up Container Insights (p. 264).

Pod metrics missing on Amazon EKS or Kubernetes after upgrading cluster

This section might be useful if you all or some pod metrics are missing after you deploy the CloudWatch agent as a daemonset on a new or upgraded cluster, or you see an error log with the message W! No pod metric collected.

These errors can be caused by changes in the container runtime, such as containerd or the docker systemd cgroup driver. You can usually solve this by updating your deployment manifest so that the containerd socket from the host is mounted into the container. See the following example:

```yaml
apiVersion: apps/v1
class: DaemonSet
metadata:
  name: cloudwatch-agent
  namespace: amazon-cloudwatch
spec:
  template:
    spec:
      containers:
        - name: cloudwatch-agent
          # ...
          volumeMounts:
            # ...
            - name: dockersock
              mountPath: /var/run/docker.sock
              readOnly: true
            - name: varlibdocker
              mountPath: /var/lib/docker
              readOnly: true
            - name: containerdsock # NEW mount
              mountPath: /run/containerd/containerd.sock
              readOnly: true
            # ...
            volumes:
              # ...
              - name: dockersock
                hostPath:
                  path: /var/run/docker.sock
              - name: varlibdocker
                hostPath:
                  path: /var/lib/docker
              - name: containerdsock # NEW volume
                hostPath:
```
No pod metrics when using Bottlerocket for Amazon EKS

Bottlerocket is a Linux-based open source operating system that is purpose-built by AWS for running containers.

Bottlerocket uses a different containerd path on the host, so you need to change the volumes to its location. If you don't, you see an error in the logs that includes W! No pod metric collected. See the following example.

```yaml
volumes:
  # ...
  - name: containerdsock
    hostPath:
      # path: /run/containerd/containerd.sock
      # bottlerocket does not mount containerd sock at normal place
      # https://github.com/bottlerocket-os/bottlerocket/
      # commit/91b10c85b3f4c3660b496e243ef8b55df0973b
      path: /run/dockershim.sock
```

No container filesystem metrics when using the containerd runtime for Amazon EKS or Kubernetes

This is a known issue and is being worked on by community contributors. For more information, see Disk usage metric for containerd and container file system metrics is not supported by cadvisor for containerd on GitHub.

Unexpected log volume increase from CloudWatch agent when collecting Prometheus metrics

This was a regression introduced in version 1.247347.6b250880 of the CloudWatch agent. This regression has already been fixed in more recent versions of the agent. It's impact was limited to scenarios where customers collected the logs of the CloudWatch agent itself and were also using Prometheus. For more information, see [prometheus] agent is printing all the scraped metrics in log on GitHub.

Latest docker image mentioned in release notes not found from Dockerhub

We update the release note and tag on Github before we start the actual release internally. It usually takes 1-2 weeks to see the latest docker image on registries after we bump the version number on Github. There is no nightly release for the CloudWatch agent container image. You can build the image directly from source at the following location: https://github.com/aws/amazon-cloudwatch-agent/tree/master/amazon-cloudwatch-container-insights/cloudwatch-agent-dockerfile

CrashLoopBackoff error on the CloudWatch agent

If you see a CrashLoopBackOff error for the CloudWatch agent, make sure that your IAM permissions are set correctly. For more information, see Verify prerequisites (p. 275).
CloudWatch agent or FluentD pod stuck in pending

If you have a CloudWatch agent or FluentD pod stuck in Pending or with a FailedScheduling error, determine if your nodes have enough compute resources based on the number of cores and amount of RAM required by the agents. Enter the following command to describe the pod:

```
kubectl describe pod cloudwatch-agent-85ppg -n amazon-cloudwatch
```

Building your own CloudWatch agent Docker image


The Dockerfile supports building multi-architecture images directly using `docker buildx`.

Deploying other CloudWatch agent features in your containers

You can deploy additional monitoring features in your containers using the CloudWatch agent. These features include the following:

- **Embedded Metric Format**— For more information, see Ingesting high-cardinality logs and generating metrics with CloudWatch embedded metric format (p. 668).
- **StatsD**— For more information, see Retrieve custom metrics with StatsD (p. 503).

Instructions and necessary files are located on GitHub at the following locations:

- For Amazon ECS containers, see Example Amazon ECS task definitions based on deployment modes.
- For Amazon EKS and Kubernetes containers, see Example Kubernetes YAML files based on deployment modes.
Using Lambda Insights

CloudWatch Lambda Insights is a monitoring and troubleshooting solution for serverless applications running on AWS Lambda. The solution collects, aggregates, and summarizes system-level metrics including CPU time, memory, disk, and network. It also collects, aggregates, and summarizes diagnostic information such as cold starts and Lambda worker shutdowns to help you isolate issues with your Lambda functions and resolve them quickly.

Lambda Insights uses a new CloudWatch Lambda extension, which is provided as a Lambda layer. When you install this extension on a Lambda function, it collects system-level metrics and emits a single performance log event for every invocation of that Lambda function. CloudWatch uses embedded metric formatting to extract metrics from the log events.

For more information about Lambda extensions, see Using AWS Lambda extensions. For more information about embedded metric format, see Ingesting high-cardinality logs and generating metrics with CloudWatch embedded metric format (p. 668).

You can use Lambda Insights with any Lambda function that uses a Lambda runtime that supports Lambda extensions. For a list of these runtimes, see Lambda Extensions API.

Pricing

For each Lambda function enabled for Lambda Insights, you only pay for what you use for metrics and logs. For a pricing example, see Amazon CloudWatch Pricing.

You are charged for the execution time consume by the Lambda extension, in 1ms increments. For more information about Lambda pricing, see AWS Lambda Pricing.

Getting started with Lambda Insights

To enable Lambda Insights on a Lambda function, you can use a one-click toggle in the Lambda console. Alternatively, you can use the AWS CLI, AWS CloudFormation, the AWS Serverless Application Model CLI, or the AWS Cloud Development Kit (CDK).

The following sections provide detailed instructions for completing these steps.

Topics
- Available versions of the Lambda Insights extension (p. 410)
- Using the console to enable Lambda Insights on an existing Lambda function (p. 415)
- Using the AWS CLI to enable Lambda Insights on an existing Lambda function (p. 416)
- Using the AWS SAM CLI to enable Lambda Insights on an existing Lambda function (p. 416)
- Using AWS CloudFormation to enable Lambda Insights on an existing Lambda function (p. 418)
- Using the AWS CDK to enable Lambda Insights on an existing Lambda function (p. 418)
- Using Serverless Framework to enable Lambda Insights on an existing Lambda function (p. 419)
- Enabling Lambda Insights on a Lambda container image deployment (p. 420)

Available versions of the Lambda Insights extension

This section lists the versions of the Lambda Insights extension, and the ARNs to use for these extensions in each AWS Region.
1.0.98.0

This version removes unnecessary logging and also addresses an issue with the AWS Serverless Application Model CLI local invokes. For more information about this issue, see Adding LambdaInsightsExtension results in timeout with 'sam local invoke'.

**ARNs for version 1.0.98.0**

The following table lists the ARNs to use for this version of the extension in each AWS Region where it is available.

<table>
<thead>
<tr>
<th>Region</th>
<th>ARN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Africa (Cape Town)</td>
<td>arn:aws:lambda:af-south-1:012438385374:layer:LambdaInsightsExtension:8</td>
</tr>
<tr>
<td>Asia Pacific (Hong Kong)</td>
<td>arn:aws:lambda:ap-east-1:519774774795:layer:LambdaInsightsExtension:8</td>
</tr>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>arn:aws:lambda:ap-south-1:580247275435:layer:LambdaInsightsExtension:14</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>arn:aws:lambda:ap-southeast-1:580247275435:layer:LambdaInsightsExtension:14</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>arn:aws:lambda:ca-central-1:580247275435:layer:LambdaInsightsExtension:14</td>
</tr>
<tr>
<td>China (Beijing)</td>
<td>arn:aws-cn:lambda:cn-north-1:488211338238:layer:LambdaInsightsExtension:8</td>
</tr>
<tr>
<td>China (Ningxia)</td>
<td>arn:aws-cn:lambda:cn-northwest-1:488211338238:layer:LambdaInsightsExtension:8</td>
</tr>
<tr>
<td>Region</td>
<td>ARN</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Europe (Milan)</td>
<td>arn:aws:lambda:eu-south-1:133924923099:layer:LambdaInsightsExtension:8</td>
</tr>
<tr>
<td>Middle East (Bahrain)</td>
<td>arn:aws:lambda:me-south-1:285320876703:layer:LambdaInsightsExtension:8</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>arn:aws:lambda:sa-east-1:580247275435:layer:LambdaInsightsExtension:14</td>
</tr>
</tbody>
</table>

**1.0.89.0**

This version corrects the performance event timestamp to always represent the start of the invocation of the function.

**ARNs for version 1.0.89.0**

The following table lists the ARNs to use for this version of the extension in each AWS Region where it is available.

<table>
<thead>
<tr>
<th>Region</th>
<th>ARN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>arn:aws:lambda:ap-south-1:580247275435:layer:LambdaInsightsExtension:12</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>arn:aws:lambda:ap-southeast-1:580247275435:layer:LambdaInsightsExtension:12</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>arn:aws:lambda:ap-southeast-2:580247275435:layer:LambdaInsightsExtension:12</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>arn:aws:lambda:ap-northeast-1:580247275435:layer:LambdaInsightsExtension:12</td>
</tr>
<tr>
<td>Region</td>
<td>ARN</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>arn:aws:lambda:ca-central-1:580247275435:layer:LambdaInsightsExtension:12</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>arn:aws:lambda:eu-central-1:580247275435:layer:LambdaInsightsExtension:12</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>arn:aws:lambda:eu-west-1:580247275435:layer:LambdaInsightsExtension:12</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>arn:aws:lambda:sa-east-1:580247275435:layer:LambdaInsightsExtension:12</td>
</tr>
</tbody>
</table>

1.0.86.0

With version 1.0.54.0 of the extension, memory metrics were sometimes reported incorrectly and sometimes were higher than 100%. Version 1.0.86.0 corrects the memory measurement issue by using the same event data as Lambda platform metrics. This means that you may see a dramatic change in the recorded memory metric values. This is achieved by using the new Lambda Logs API. This provides a more accurate measurement of Lambda sandbox memory usage. However, something to be aware of is that the Lambda Logs API can't deliver platform report events if a function sandbox times out and is subsequently spun down. In this case, Lambda Insights is unable to record the invocation metrics. For more information about Lambda Logs API, see AWS Lambda Logs API.

New features in version 1.0.86.0

- Uses the Lambda Logs API to correct the memory metric. This solves the previous issue where memory statistics were greater than 100%.
- Introduces Init Duration as a new CloudWatch metric.
- Uses the invocation ARN to add a version dimension for aliases and invoked versions. If you are using Lambda aliases or versions to achieve incremental deployments (such as blue-green deployments), you can view your metrics based on the invoked alias. The version dimension is not applied if the function doesn't use an alias or version. For more information, see Lambda function aliases.
- Adds a billed_mb_ms field to the performance events to display the cost per invoke. This does not consider any cost associated with provisioned concurrency.
- Adds billed_duration and duration fields to the performance events.

ARNs for version 1.0.86.0

The following table lists the ARNs to use for this version of the extension in each AWS Region where it is available.
<table>
<thead>
<tr>
<th>Region</th>
<th>ARN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>arn:aws:lambda:ap-south-1:580247275435:layer:LambdaInsightsExtension:11</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>arn:aws:lambda:ap-southeast-1:580247275435:layer:LambdaInsightsExtension:11</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>arn:aws:lambda:ap-southeast-2:580247275435:layer:LambdaInsightsExtension:11</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>arn:aws:lambda:ap-northeast-1:580247275435:layer:LambdaInsightsExtension:11</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>arn:aws:lambda:ca-central-1:580247275435:layer:LambdaInsightsExtension:11</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>arn:aws:lambda:eu-central-1:580247275435:layer:LambdaInsightsExtension:11</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>arn:aws:lambda:eu-west-1:580247275435:layer:LambdaInsightsExtension:11</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>arn:aws:lambda:sa-east-1:580247275435:layer:LambdaInsightsExtension:11</td>
</tr>
</tbody>
</table>

**1.0.54.0**

Version 1.0.54.0 was the initial release of the Lambda Insights extension.

**ARNs for version 1.0.54.0**

The following table lists the ARNs to use for this version of the extension in each AWS Region where it is available.
<table>
<thead>
<tr>
<th>Region</th>
<th>ARN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia Pacific (Mumbai)</td>
<td>arn:aws:lambda:ap-south-1:580247275435:layer:LambdaInsightsExtension:2</td>
</tr>
<tr>
<td>Asia Pacific (Seoul)</td>
<td>arn:aws:lambda:ap-northeast-2:580247275435:layer:LambdaInsightsExtension:2</td>
</tr>
<tr>
<td>Asia Pacific (Singapore)</td>
<td>arn:aws:lambda:ap-southeast-1:580247275435:layer:LambdaInsightsExtension:2</td>
</tr>
<tr>
<td>Asia Pacific (Sydney)</td>
<td>arn:aws:lambda:ap-southeast-2:580247275435:layer:LambdaInsightsExtension:2</td>
</tr>
<tr>
<td>Asia Pacific (Tokyo)</td>
<td>arn:aws:lambda:ap-northeast-1:580247275435:layer:LambdaInsightsExtension:2</td>
</tr>
<tr>
<td>Canada (Central)</td>
<td>arn:aws:lambda:ca-central-1:580247275435:layer:LambdaInsightsExtension:2</td>
</tr>
<tr>
<td>Europe (Frankfurt)</td>
<td>arn:aws:lambda:eu-central-1:580247275435:layer:LambdaInsightsExtension:2</td>
</tr>
<tr>
<td>Europe (Ireland)</td>
<td>arn:aws:lambda:eu-west-1:580247275435:layer:LambdaInsightsExtension:2</td>
</tr>
<tr>
<td>South America (São Paulo)</td>
<td>arn:aws:lambda:sa-east-1:580247275435:layer:LambdaInsightsExtension:2</td>
</tr>
</tbody>
</table>

### Using the console to enable Lambda Insights on an existing Lambda function

Follow these steps to use the console to enable Lambda Insights on an existing Lambda function.

**To enable Lambda Insights on a Lambda function**

2. Choose the name of the function, and then choose the Configuration tab.
3. In the Monitoring tools section of the Configuration page, choose Edit.
4. Under CloudWatch Lambda Insights, choose Enhanced monitoring and then choose Save.

Using the AWS CLI to enable Lambda Insights on an existing Lambda function

Follow these steps to use the AWS CLI to enable Lambda Insights on an existing Lambda function.

Step 1: Update function permissions

To update the function's permissions

• Attach the CloudWatchLambdaInsightsExecutionRolePolicy managed IAM policy to the function's execution role by entering the following command.

```bash
aws iam attach-role-policy 
  --role-name function-execution-role 
  --policy-arn "arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy"
```

Step 2: Install the Lambda extension

Install the Lambda extension by entering the following command. Replace the ARN value for the layers parameter with the ARN matching your Region and the extension version that you want to use. For more information, see Available versions of the Lambda Insights extension (p. 410).

```bash
aws lambda update-function-configuration 
  --function-name function-name 
```

Step 3: Enable the CloudWatch Logs VPC endpoint

This step is necessary only for functions running in a private subnet with no internet access, and if you have not already configured a CloudWatch Logs virtual private cloud (VPC) endpoint.

If you need to do this step, enter the following command, replacing the placeholders with information for your VPC.

For more information, see Using CloudWatch Logs with Interface VPC Endpoints.

```bash
aws ec2 create-vpc-endpoint 
  --vpc-id vpcId 
  --vpc-endpoint-type Interface 
  --service-name com.amazonaws.region.logs 
  --subnet-id subnetId 
  --security-group-id securitygroupId
```

Using the AWS SAM CLI to enable Lambda Insights on an existing Lambda function

Follow these steps to use the AWS SAM AWS CLI to enable Lambda Insights on an existing Lambda function.
If you don't already have the latest version of the AWS SAM CLI installed, you must first install or upgrade it. For more information, see Installing the AWS SAM CLI.

**Step 1: Install the layer**

To make the Lambda Insights extension available to all of your Lambda functions, add a `Layers` property to the `Globals` section of your SAM template with the ARN of the Lambda Insights layer. The example below uses the layer for the initial release of Lambda Insights. For the latest release version of the Lambda Insights extension layer, see Available versions of the Lambda Insights extension (p. 410).

```yaml
Globals:
  Function:
    Layers:
    - !Sub "arn:aws:lambda:${AWS::Region}:580247275435:layer:LambdaInsightsExtension:14"
```

To enable this layer for only a single function, add the `Layers` property to the function as shown in this example.

```yaml
Resources:
  MyFunction:
    Type: AWS::Serverless::Function
    Properties:
      Layers:
      - !Sub "arn:aws:lambda:${AWS::Region}:580247275435:layer:LambdaInsightsExtension:14"
```

**Step 2: Add the managed policy**

For each function, add the `CloudWatchLambdaInsightsExecutionRolePolicy` IAM policy.

AWS SAM doesn't support global policies, so you must enable those on each function individually, as shown in this example. For more information about globals, see Globals Section.

```yaml
Resources:
  MyFunction:
    Type: AWS::Serverless::Function
    Properties:
      Policies:
      - CloudWatchLambdaInsightsExecutionRolePolicy
```

**Invoking locally**

The AWS SAM CLI supports Lambda extensions. However, every locally executed invocation resets the runtime environment. Lambda Insights data won't be available from local invocations because the runtime is restarted without a shutdown event. For more information, see Release 1.6.0 - Add support for local testing of AWS Lambda extensions.

**Troubleshooting**

To troubleshoot your Lambda Insights installation, add the following environment variable to your Lambda function to enable debug logging.

```yaml
Resources:
  MyFunction:
    Type: AWS::Serverless::Function
    Properties:
      Environment:
        Variables:
          LAMBDA_INSIGHTS_LOG_LEVEL: info
```
Using AWS CloudFormation to enable Lambda Insights on an existing Lambda function

Follow these steps to use AWS CloudFormation to enable Lambda Insights on an existing Lambda function.

**Step 1: Install the layer**

Add the Lambda Insights layer to the `Layers` property within the Lambda Insights layer ARN. The example below uses the layer for the initial release of Lambda Insights. For the latest release version of the Lambda Insights extension layer, see Available versions of the Lambda Insights extension (p. 410).

### Resources:

```
MyFunction:
  Type: AWS::Lambda::Function
  Properties:
    Layers:
      - !Sub "arn:aws:lambda:${AWS::Region}:580247275435:layer:LambdaInsightsExtension:14"
```

**Step 2: Add the managed policy**

Add the `CloudWatchLambdaInsightsExecutionRolePolicy` IAM policy to your function execution role.

### Resources:

```
MyFunctionExecutionRole:
  Type: 'AWS::IAM::Role'
  Properties:
    ManagedPolicyArns:
      - 'arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy'
```

**Step 3: (Optional) Add VPC endpoint**

This step is necessary only for functions running in a private subnet with no internet access, and if you have not already configured a CloudWatch Logs virtual private cloud (VPC) endpoint. For more information, see Using CloudWatch Logs with Interface VPC Endpoints.

### Resources:

```
CloudWatchLogsVpcPrivateEndpoint:
  Type: AWS::EC2::VPC Endpoint
  Properties:
    PrivateDnsEnabled: 'true'
    VpcEndpointType: Interface
    VpcId: !Ref VPC
    ServiceName: !Sub com.amazonaws.${AWS::Region}.logs
    SecurityGroupIds:
      - !Ref InterfaceVpcEndpointSecurityGroup
    SubnetIds:
      - !Ref PublicSubnet01
      - !Ref PublicSubnet02
      - !Ref PublicSubnet03
```

**Using the AWS CDK to enable Lambda Insights on an existing Lambda function**

Follow these steps to use the AWS CDK to enable Lambda Insights on an existing Lambda function. To use these steps, you must already be using the AWS CDK to manage your resources.
The commands in this section are in TypeScript.

First, update the function permissions.

```typescript
executionRole.addManagedPolicy(
  ManagedPolicy.fromAwsManagedPolicyName('CloudWatchLambdaInsightsExecutionRolePolicy')
);
```

Next, install the extension on the Lambda function. Replace the ARN value for the `layerArn` parameter with the ARN matching your Region and the extension version that you want to use. For more information, see Available versions of the Lambda Insights extension (p. 410).

```typescript
import lambda = require('@aws-cdk/aws-lambda');
const layer = lambda.LayerVersion.fromLayerVersionArn(this, 'LayerFromArn', layerArn);
```

If necessary, enable the virtual private cloud (VPC) endpoint for CloudWatch Logs. This step is necessary only for functions running in a private subnet with no internet access, and if you have not already configured a CloudWatch Logs VPC endpoint.

```typescript
const cloudWatchLogsEndpoint = vpc.addInterfaceEndpoint('cwl-gateway', {
  service: InterfaceVpcEndpointAwsService.CLOUDWATCH_LOGS,
});
cloudWatchLogsEndpoint.connections.allowDefaultPortFromAnyIpv4();
```

### Using Serverless Framework to enable Lambda Insights on an existing Lambda function

Follow these steps to use Serverless Framework to enable Lambda Insights on an existing Lambda function. For more information about Serverless Framework, see serverless.com.

This is done through a Lambda Insights plugin for Serverless. For more information, see serverless-plugin-lambda-insights.

If you don’t already have the latest version of the Serverless command-line interface installed, you must first install or upgrade it. For more information, see Get started with Serverless Framework Open Source & AWS.

#### To use Serverless Framework to enable Lambda Insights on a Lambda function

1. Install the Serverless plugin for Lambda Insights by running the following command in your Serverless directory:

   ```bash
   npm install --save-dev serverless-plugin-lambda-insights
   ```

2. In your `serverless.yml` file, add the plugin in the `plugins` section as shown:

   ```yaml
   provider:
     name: aws
     plugins:
       - serverless-plugin-lambda-insights
   ```

3. Enable Lambda Insights.
You can enable Lambda Insights individually per function by adding the following property to the serverless.yml file:

```yaml
functions:
  myLambdaFunction:
    handler: src/app/index.handler
    lambdaInsights: true #enables Lambda Insights for this function

You can enable Lambda Insights for all functions within the serverless.yml file by adding the following custom section:

```yaml
custom:
  lambdaInsights:
    defaultLambdaInsights: true #enables Lambda Insights for all functions
```

4. Re-deploy the Serverless service by entering the following command:

```
serverless deploy
```

This re-deploys all functions and enables Lambda Insights for those functions that you have specified. It enables Lambda Insights by adding the Lambda Insights layer and attaching the necessary permissions using the `arn:aws:iam::aws:policy/CloudWatchLambdaInsightsExecutionRolePolicy` IAM policy.

## Enabling Lambda Insights on a Lambda container image deployment

To enable Lambda Insights on a Lambda function that is deployed as a container image, add the following lines in your Dockerfile. These lines install the Lambda Insights agent as an extension in your container image.

```bash
RUN curl -O https://lambda-insights-extension.s3-ap-northeast-1.amazonaws.com/amazon_linux/lambda-insights-extension.rpm && \
    rpm -U lambda-insights-extension.rpm && \
    rm -f lambda-insights-extension.rpm
```

After you create your Lambda function, assign the `CloudWatchLambdaInsightsExecutionRolePolicy` IAM policy to the function's execution role, and Lambda Insights is enabled on the container image-based Lambda function.

**Note**

To use an older version of the Lambda Insights extension, replace the URL in the previous commands with this URL: `https://lambda-insights-extension.s3-ap-northeast-1.amazonaws.com/amazon_linux/lambda-insights-extension.1.0.111.0.rpm`. Currently, only Lambda Insights versions 1.0.111.0 and later are available. For more information, see Available versions of the Lambda Insights extension (p. 410).

### To verify the signature of the Lambda Insights agent package on a Linux server

1. Enter the following command to download the public key.

```
shell$ wget https://lambda-insights-extension.s3-ap-northeast-1.amazonaws.com/lambda-insights-extension.gpg
```
2. Enter the following command to import the public key into your keyring.

```
shell$ gpg --import lambda-insights-extension.gpg
```

The output will be similar to the following. Make a note of the key value, you will need it in the next step. In this example output, the key value is 848ABDC8.

```
gpg: key 848ABDC8: public key "Amazon Lambda Insights Extension" imported
gpg: Total number processed: 1
```

3. Verify the fingerprint by entering the following command. Replace key-value with the value of the key from the preceding step.

```
shell$ gpg --fingerprint key-value
```

The fingerprint string in the output of this command should be E0AF FA11 FFF3 5BD7 349E E222 479C 97A1 848A BDC8. If the string doesn't match, don't install the agent and contact AWS.

4. After you have verified the fingerprint, you can use it to verify the Lambda Insights agent package. Download the package signature file by entering the following command.

```
shell$ wget https://lambda-insights-extension.s3-ap-northeast-1.amazonaws.com/amazon_linux/lambda-insights-extension.rpm.sig
```

5. Verify the signature by entering the following command.

```
shell$ gpg --verify lambda-insights-extension.rpm.sig lambda-insights-extension.rpm
```

The output should look like the following:

```
gpg: Signature made Thu 08 Apr 2021 06:41:00 PM UTC using RSA key ID 848ABDC8
gpg: Good signature from "Amazon Lambda Insights Extension"
gpg: WARNING: This key is not certified with a trusted signature!
gpg:         There is no indication that the signature belongs to the owner.
Primary key fingerprint: E0AF FA11 FFF3 5BD7 349E E222 479C 97A1 848A BDC8
```

In the expected output, there might be a warning about a trusted signature. A key is trusted only if you or someone who you trust has signed it. This doesn't mean that the signature is invalid, only that you have not verified the public key.

If the output contains BAD signature, check whether you performed the steps correctly. If you continue to get a BAD signature response, contact AWS and avoid using the downloaded file.

**Example**

This section includes an example of enabling Lambda Insights on a container image-based Python Lambda function.

**An example of enabling Lambda Insights on a Lambda container image**

1. Create a Dockerfile that is similar to the following:

```
FROM public.ecr.aws/lambda/python:3.8
// extra lines to install the agent here
```
RUN curl -O https://lambda-insights-extension.s3-ap-northeast-1.amazonaws.com/amazon_linux/lambda-insights-extension.rpm && \
    rpm -U lambda-insights-extension.rpm && \
    rm -f lambda-insights-extension.rpm
COPY index.py ${LAMBDA_TASK_ROOT}
CMD [ "index.handler" ]

2. Create a Python file named `index.py` that is similar to the following:

   ```python
   def handler(event, context):
       return {
           'message': 'Hello World!'  
       }
   ```

3. Put the Dockerfile and `index.py` in the same directory. Then, in that directory, run the following steps to build the docker image and upload it to Amazon ECR.

   ```bash
   // create an ECR repository
   aws ecr create-repository --repository-name test-repository
   // build the docker image
   docker build -t test-image .
   // sign in to AWS
   aws ecr get-login-password | docker login --username AWS --password-stdin
   "${ACCOUNT_ID}".dkr.ecr."${REGION}".amazonaws.com
   // tag the image
   docker tag test-image:latest "${ACCOUNT_ID}".dkr.ecr."${REGION}".amazonaws.com/test-repository:latest
   // push the image to ECR
   docker push "${ACCOUNT_ID}".dkr.ecr."${REGION}".amazonaws.com/test-repository:latest
   ```

4. Use that Amazon ECR image that you just created to create the Lambda function.

5. Assign the `CloudWatchLambdaInsightsExecutionRolePolicy` IAM policy to the function's execution role.

### Viewing your Lambda Insights metrics

After you have installed the Lambda Insights extension on a Lambda function that has been invoked, you can use the CloudWatch console to see your metrics. You can see a multi-function overview, or focus on a single function.

For a list of Lambda Insights metrics, see Metrics collected by Lambda Insights (p. 423).

#### To view the multi-function overview for your Lambda Insights metrics


2. In the left navigation pane, under Lambda Insights, choose Multi-function.

   The top part of the page displays graphs with aggregated metrics of all your Lambda functions in the Region that have Lambda Insights enabled. Lower on the page is a table that lists the functions.

3. To filter by function name to reduce the number of functions displayed, type part of the function name in the box near the top of the page.

4. To add this view to a dashboard as a widget, choose Add to dashboard.

#### To view metrics for a single function


422
2. In the left navigation pane, under **Lambda Insights**, choose **Single-function**.
   
   The top part of the page displays graphs with metrics for the selected function.

3. If you have X-Ray enabled, you can choose a single trace ID. This opens CloudWatch ServiceLens for that invocation, and from there you can zoom out to see the distributed trace and the other services involved in handling that specific transaction. For more information about ServiceLens, see Using ServiceLens to monitor the health of your applications (p. 226).

4. To open CloudWatch Logs Insights and zoom in on a specific error, choose **View logs** by the table at the bottom of the page.

5. To add this view to a dashboard as a widget, choose **Add to dashboard**.

---

### Metrics collected by Lambda Insights

Lambda Insights collects several metrics from the Lambda functions where it is installed. Some of these metrics are available as time series aggregated data in CloudWatch Metrics. Other metrics are not aggregated into time series data but can be found in the embedded metric format log entries by using CloudWatch Logs Insights.

The following metrics are available as time series aggregated data in CloudWatch Metrics in the **LambdaInsights** namespace.

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_total_time</td>
<td>function_name</td>
<td>Sum of cpu_system_time and cpu_user_time.</td>
</tr>
<tr>
<td></td>
<td>function_name, version</td>
<td>Unit: Milliseconds</td>
</tr>
<tr>
<td>init_duration</td>
<td>function_name</td>
<td>The amount of time spent in the <em>init</em> phase of the Lambda execution environment lifecycle.</td>
</tr>
<tr>
<td></td>
<td>function_name, version</td>
<td>Unit: Milliseconds</td>
</tr>
<tr>
<td>memory_utilization</td>
<td>function_name</td>
<td>The maximum memory measured as a percentage of the memory allocated to the function.</td>
</tr>
<tr>
<td></td>
<td>function_name, version</td>
<td>Unit: Percent</td>
</tr>
<tr>
<td>rx_bytes</td>
<td>function_name</td>
<td>The number of bytes received by the function.</td>
</tr>
<tr>
<td></td>
<td>function_name, version</td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>tx_bytes</td>
<td>function_name</td>
<td>The number of bytes sent by the function.</td>
</tr>
<tr>
<td></td>
<td>function_name, version</td>
<td>Unit: Bytes</td>
</tr>
</tbody>
</table>
## Metrics collected by Lambda Insights

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Dimensions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>total_memory</strong></td>
<td>function_name</td>
<td>The amount of memory allocated to your Lambda function. This is the same as your function's memory size.</td>
</tr>
<tr>
<td></td>
<td>function_name, version</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Megabytes</td>
</tr>
<tr>
<td><strong>total_network</strong></td>
<td>function_name</td>
<td>Sum of rx_bytes and tx_bytes. Even for functions that don't perform I/O tasks, this value is usually greater than zero because of network calls made by the Lambda runtime.</td>
</tr>
<tr>
<td></td>
<td>function_name, version</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td><strong>used_memory_max</strong></td>
<td>function_name</td>
<td>The measured memory of the function sandbox.</td>
</tr>
<tr>
<td></td>
<td>function_name, version</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Megabytes</td>
</tr>
</tbody>
</table>

The following metrics can be found in the embedded metric format log entries by using CloudWatch Logs Insights. For more information about CloudWatch Logs Insights, see Analyzing Log Data with CloudWatch Logs Insights.

For more information about embedded metric format, see Ingesting high-cardinality logs and generating metrics with CloudWatch embedded metric format (p. 668).

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>cpu_system_time</strong></td>
<td>The amount of time the CPU spent executing kernel code.</td>
</tr>
<tr>
<td></td>
<td>Unit: Milliseconds</td>
</tr>
<tr>
<td><strong>cpu_total_time</strong></td>
<td>Sum of cpu_system_time and cpu_user_time.</td>
</tr>
<tr>
<td></td>
<td>Unit: Milliseconds</td>
</tr>
<tr>
<td><strong>cpu_user_time</strong></td>
<td>The amount of time the CPU spent executing user code.</td>
</tr>
<tr>
<td></td>
<td>Unit: Milliseconds</td>
</tr>
<tr>
<td><strong>fd_max</strong></td>
<td>The maximum number of file descriptors available.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td><strong>fd_use</strong></td>
<td>The maximum number of file descriptors in use.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
</tbody>
</table>
### Metric name | Description
--- | ---
memory_utilization | The maximum memory measured as a percentage of the memory allocated to the function. Unit: Percent
rx_bytes | The number of bytes received by the function. Unit: Bytes
tx_bytes | The number of bytes sent by the function. Unit: Bytes
threads_max | The number of threads in use by the function process. As a function author, you don't control the initial number of threads created by the runtime. Unit: Count
tmp_max | The amount of space available in the /tmp directory. Unit: Bytes
tmp_used | The amount of space used in the /tmp directory. Unit: Bytes
total_memory | The amount of memory allocated to your Lambda function. This is the same as your function's memory size. Unit: Megabytes
total_network | Sum of rx_bytes and tx_bytes. Even for functions that don't perform I/O tasks, this value is usually greater than zero because of network calls made by the Lambda runtime. Unit: Bytes
used_memory_max | The measured memory of the function sandbox. Unit: Bytes

## Troubleshooting and known issues

The first step to troubleshooting any issues is to enable debug logging on the Lambda Insights extension. To do this, set the following environment variable on your Lambda function: LAMBDA_INSIGHTS_LOG_LEVEL=info. For more information, see Using AWS Lambda environment variables.

The extension emits logs into the same log group as your function (/aws/lambda/function-name). Review those logs to see if the error might be related to a setup issue.
I don't see any metrics from Lambda Insights

If you don’t see Lambda Insights metrics that you expect to see, check the following possibilities:

• **The metrics might just be delayed**— If the function has not yet been invoked or the data has not been flushed yet, you won’t see the metrics in CloudWatch. For more information, see Known Issues later in this section.

• **Confirm that the Lambda function has the correct permissions**—Make sure that the CloudWatchLambdaInsightsExecutionRolePolicy IAM policy is assigned to the function's execution role.

• **Check the Lambda runtime**—Lambda Insights supports only certain Lambda runtimes. For a list of supported runtimes, see Using Lambda Insights (p. 410).

  For example, to use Lambda Insights on Java 8, you must use the java8.al2 runtime, not the java8 runtime.

• **Check network access**—The Lambda function might be on a VPC private subnet with no internet access and you don't have a VPC endpoint configured for CloudWatch Logs. To help debug this issue, you can set the environment variable LAMBDA_INSIGHTS_LOG_LEVEL=info.

Known issues

Data delay can be as high as 20 minutes. When a function handler completes, Lambda freezes the sandbox, which also freezes the Lambda Insights extension. While the function is running, we use an adaptive batching strategy based on the function TPS to output data. However, if the function stops being invoked for an extended period and there is still event data in the buffer, this data can be delayed until Lambda shuts down the idle sandbox. When Lambda shuts down the sandbox, we flush the buffered data.

Example telemetry event

Each invocation of a Lambda function that has Lambda Insights enabled writes a single log event to the /aws/lambda-insights log group. Each log event contains metrics in embedded metric format. For more information about embedded metric format, see Ingesting high-cardinality logs and generating metrics with CloudWatch embedded metric format (p. 668).

To analyze these log events, you can use the following methods:

• The Lambda Insights section of the CloudWatch console, as explained in Viewing your Lambda Insights metrics (p. 422).

• Log event queries using CloudWatch Logs Insights. For more information, see Analyzing Log Data with CloudWatch Logs Insights.

• Metrics collected in the LambdaInsights namespace, which you graph by using CloudWatch metrics.

The following is an example of a Lambda Insights log event with embedded metric format.

```json
{
  "_aws": {
    "Timestamp": 1605034324256,
    "CloudWatchMetrics": [
      {
        "Namespace": "LambdaInsights",
        "Dimensions": [
```

426
Example telemetry event

```
[ "function_name" ],
[ "function_name", "version" ]
],
"Metrics": [
  { "Name": "memory_utilization", "Unit": "Percent" },
  { "Name": "total_memory", "Unit": "Megabytes" },
  { "Name": "used_memory_max", "Unit": "Megabytes" },
  { "Name": "cpu_total_time", "Unit": "Milliseconds" },
  { "Name": "tx_bytes", "Unit": "Bytes" },
  { "Name": "rx_bytes", "Unit": "Bytes" },
  { "Name": "total_network", "Unit": "Bytes" },
  { "Name": "init_duration", "Unit": "Milliseconds" }
],
"LambdaInsights": {
  "ShareTelemetry": true
},
"event_type": "performance",
"function_name": "cpu-intensive",
"version": "Blue",
"request_id": "12345678-8bcc-42f7-b1de-123456789012",
"trace_id": "1-5faae118-12345678901234567890",
"duration": 45191,
"billed_duration": 45200,
"billed_mb_ms": 11571200,
"cold_start": true,
"init_duration": 130,
"tmp_free": 538329088,
"tmp_max": 551346176,
"threads_max": 11,
"used_memory_max": 63,
"total_memory": 256,
"memory_utilization": 24,
"cpu_user_time": 6640,
"cpu_system_time": 50,
"cpu_total_time": 6690,
"fd_use": 416,
"fd_max": 32642,
"tx_bytes": 4434,
"rx_bytes": 6911,
"timeout": true,
"shutdown_reason": "Timeout",
"total_network": 11345,
"agent_version": "1.0.72.0",
"agent_memory_avg": 10,
"agent_memory_max": 10
}
Collecting metrics and logs from Amazon EC2 instances and on-premises servers with the CloudWatch agent

The unified CloudWatch agent enables you to do the following:

- Collect internal system-level metrics from Amazon EC2 instances across operating systems. The metrics can include in-guest metrics, in addition to the metrics for EC2 instances. The additional metrics that can be collected are listed in Metrics collected by the CloudWatch agent (p. 516).
- Collect system-level metrics from on-premises servers. These can include servers in a hybrid environment as well as servers not managed by AWS.
- Retrieve custom metrics from your applications or services using the StatsD and collectd protocols. StatsD is supported on both Linux servers and servers running Windows Server. collectd is supported only on Linux servers.
- Collect logs from Amazon EC2 instances and on-premises servers, running either Linux or Windows Server.

Note
The CloudWatch agent does not support collecting logs from FIFO pipes.

You can store and view the metrics that you collect with the CloudWatch agent in CloudWatch just as you can with any other CloudWatch metrics. The default namespace for metrics collected by the CloudWatch agent is CWAgent, although you can specify a different namespace when you configure the agent.

The logs collected by the unified CloudWatch agent are processed and stored in Amazon CloudWatch Logs, just like logs collected by the older CloudWatch Logs agent. For information about CloudWatch Logs pricing, see Amazon CloudWatch Pricing.

Metrics collected by the CloudWatch agent are billed as custom metrics. For more information about CloudWatch metrics pricing, see Amazon CloudWatch Pricing.

The CloudWatch agent is open-source under the MIT license, and is hosted on GitHub. If you would like to build, customize or contribute to the CloudWatch agent, see the GitHub repository for the latest instructions. If you think you’ve found a potential security issue, do not post it on GitHub or any public forum. Instead, please follow the instructions at Vulnerability Reporting or email AWS security directly.

The steps in this section explain how to install the unified CloudWatch agent on Amazon EC2 instances and on-premises servers. For more information about the metrics that the CloudWatch agent can collect, see Metrics collected by the CloudWatch agent (p. 516).

Supported operating systems
The CloudWatch agent is supported on x86-64 architecture on the following operating systems:
• Amazon Linux version 2014.03.02 or later
• Amazon Linux 2
• Ubuntu Server versions 20.04, 18.04, 16.04, and 14.04
• CentOS versions 8.0, 7.6, 7.2, and 7.0
• Red Hat Enterprise Linux (RHEL) versions 8, 7.7, 7.6, 7.5, 7.4, 7.2, and 7.0
• Debian version 10 and version 8.0
• SUSE Linux Enterprise Server (SLES) version 15 and version 12
• Oracle Linux versions 7.8, 7.6, and 7.5
• macOS, including EC2 Mac1 instances

The agent is supported on ARM64 architecture on the following operating systems:
• Amazon Linux 2
• Ubuntu Server versions 20.04 and 18.04
• Red Hat Enterprise Linux (RHEL) version 7.6
• SUSE Linux Enterprise Server 15

Installation process overview
You can download and install the CloudWatch agent manually using the command line, or you can integrate it with SSM. The general flow of installing the CloudWatch agent using either method is as follows:

1. Create IAM roles or users that enable the agent to collect metrics from the server and optionally to integrate with AWS Systems Manager.
2. Download the agent package.
3. Modify the CloudWatch agent configuration file and specify the metrics that you want to collect.
4. Install and start the agent on your servers. As you install the agent on an EC2 instance, you attach the IAM role that you created in step 1. As you install the agent on an on-premises server, you specify a named profile that contains the credentials of the IAM user that you created in step 1.

Contents
• Installing the CloudWatch agent (p. 429)
• Create the CloudWatch agent configuration file (p. 466)
• Metrics collected by the CloudWatch agent (p. 516)
• OpenTelemetry support in the CloudWatch agent (p. 527)
• Common scenarios with the CloudWatch agent (p. 532)
• Troubleshooting the CloudWatch agent (p. 539)

Installing the CloudWatch agent
The CloudWatch agent is available as a package in Amazon Linux 2. If you are using this operating system, you can install the package by entering the following command. You must also make sure that the IAM role attached to the instance has the `CloudWatchAgentServerPolicy` attached. For more information, see Create IAM roles to use with the CloudWatch agent on Amazon EC2 instances (p. 444).
sudo yum install amazon-cloudwatch-agent

On all supported operating systems, you can download and install the CloudWatch agent using either the command line with an Amazon S3 download link, using SSM, or using an AWS CloudFormation template.

Contents

• Installing the CloudWatch agent using the command line (p. 430)
• Installing the CloudWatch agent using AWS Systems Manager (p. 443)
• Installing the CloudWatch agent on new instances using AWS CloudFormation (p. 455)
• Verifying the signature of the CloudWatch agent package (p. 460)

Installing the CloudWatch agent using the command line

Use the following topics to download, configure, and install the CloudWatch agent package.

Topics

• Download and configure the CloudWatch agent using the command line (p. 430)
• Create IAM roles and users for use with CloudWatch agent (p. 435)
• Installing and running the CloudWatch agent on your servers (p. 436)

Download and configure the CloudWatch agent using the command line

Use the following steps to download the CloudWatch agent package, create IAM roles or users, and optionally modify the common configuration file.

Download the CloudWatch agent package

The CloudWatch agent is available as a package in Amazon Linux 2. If you are using this operating system, you can install the package by entering the following command. You must also make sure that the IAM role attached to the instance has the CloudWatchAgentServerPolicy attached. For more information, see Create IAM roles and users for use with CloudWatch agent (p. 435).

sudo yum install amazon-cloudwatch-agent

On all supported operating systems, you can download and install the CloudWatch agent using the command line.

For each download link, there is a general link as well as links for each Region. For example, for Amazon Linux and Amazon Linux 2 and the x86-64 architecture, three of the valid download links are:

• https://s3.amazonaws.com/amazoncloudwatch-agent/amazon_linux/amd64/latest/amazon-cloudwatch-agent.rpm
• https://s3.us-east-1.amazonaws.com/amazoncloudwatch-agent-us-east-1/amazon_linux/amd64/latest/amazon-cloudwatch-agent.rpm

430
You can also download a README file about the latest changes to the agent, and a file that indicates the version number that is available for download. These files are in the following locations:


<table>
<thead>
<tr>
<th>Architecture</th>
<th>Platform</th>
<th>Download link</th>
<th>Signature file link</th>
</tr>
</thead>
<tbody>
<tr>
<td>x86-64</td>
<td>Centos</td>
<td><a href="https://s3.amazonaws.com/amazoncloudwatch-agent/centos/amd64/latest/amazon-cloudwatch-agent.rpm">https://s3.amazonaws.com/amazoncloudwatch-agent/centos/amd64/latest/amazon-cloudwatch-agent.rpm</a></td>
<td></td>
</tr>
<tr>
<td>x86-64</td>
<td>Redhat</td>
<td><a href="https://s3.amazonaws.com/amazoncloudwatch-agent/redhat/amd64/latest/amazon-cloudwatch-agent.rpm">https://s3.amazonaws.com/amazoncloudwatch-agent/redhat/amd64/latest/amazon-cloudwatch-agent.rpm</a></td>
<td></td>
</tr>
<tr>
<td>x86-64</td>
<td>SUSE</td>
<td><a href="https://s3.amazonaws.com/amazoncloudwatch-agent/suse/amd64/latest/amazon-cloudwatch-agent.rpm">https://s3.amazonaws.com/amazoncloudwatch-agent/suse/amd64/latest/amazon-cloudwatch-agent.rpm</a></td>
<td></td>
</tr>
</tbody>
</table>
### Installing the CloudWatch agent using the command line

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Platform</th>
<th>Download link</th>
<th>Signature file link</th>
</tr>
</thead>
</table>
|              |          | https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-
|              |          | <region>/debian/amd64/latest/amazon-cloudwatch-agent.deb                        |                                                                                      |
|              |          | https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-
|              |          | <region>/debian/amd64/latest/amazon-cloudwatch-agent.deb.sig                    |                                                                                      |
|              |          | https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-
|              |          | <region>/ubuntu/amd64/latest/amazon-cloudwatch-agent.deb                        |                                                                                      |
|              |          | https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-
|              |          | <region>/ubuntu/amd64/latest/amazon-cloudwatch-agent.deb.sig                    |                                                                                      |
|              |          | https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-
|              |          | <region>/oracle_linux/amd64/latest/amazon-cloudwatch-agent.rpm                 |                                                                                      |
|              |          | https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-
|              |          | <region>/oracle_linux/amd64/latest/amazon-cloudwatch-agent.rpm.sig            |                                                                                      |
|              |          | https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-
|              |          | <region>/darwin/amd64/latest/amazon-cloudwatch-agent.pkg                        |                                                                                      |
|              |          | https://s3.<region>.amazonaws.com/amazoncloudwatch-agent-
<p>|              |          | &lt;region&gt;/darwin/amd64/latest/amazon-cloudwatch-agent.pkg.sig                    |                                                                                      |</p>
<table>
<thead>
<tr>
<th>Architecture</th>
<th>Platform</th>
<th>Download link</th>
<th>Signature file link</th>
</tr>
</thead>
</table>
To use the command line to download and install the CloudWatch agent package

1. Download the CloudWatch agent.

On a Linux server, enter the following. For `download-link`, use the appropriate download link from the previous table.

```
wget download-link
```

On a server running Windows Server, download the following file:

```
```

2. After you have downloaded the package, you can optionally verify the package signature. For more information, see Verifying the signature of the CloudWatch agent package (p. 460).

3. Install the package. If you downloaded an RPM package on a Linux server, change to the directory containing the package and enter the following:

```
sudo rpm -U ./amazon-cloudwatch-agent.rpm
```

If you downloaded a DEB package on a Linux server, change to the directory containing the package and enter the following:

```
sudo dpkg -i -E ./amazon-cloudwatch-agent.deb
```

If you downloaded an MSI package on a server running Windows Server, change to the directory containing the package and enter the following:

```
msiexec /i amazon-cloudwatch-agent.msi
```

This command also works from within PowerShell. For more information about MSI command options, see Command-Line Options in the Microsoft Windows documentation.

Create and modify the agent configuration file

After you have downloaded the CloudWatch agent, you must create the configuration file before you start the agent on any servers. For more information, see Create the CloudWatch agent configuration file (p. 466).
Create IAM roles and users for use with CloudWatch agent

Access to AWS resources requires permissions. You create an IAM role, an IAM user, or both to grant permissions that the CloudWatch agent needs to write metrics to CloudWatch. If you're going to use the agent on Amazon EC2 instances, you must create an IAM role. If you're going to use the agent on on-premises servers, you must create an IAM user.

Note
We recently modified the following procedures by using new CloudWatchAgentServerPolicy and CloudWatchAgentAdminPolicy policies created by Amazon, instead of requiring customers to create these policies themselves. For writing files to and downloading files from the Parameter Store, the policies created by Amazon support only files with names that start with AmazonCloudWatch-. If you have a CloudWatch agent configuration file with a file name that doesn't start with AmazonCloudWatch-, these policies can't be used to write the file to Parameter Store or download it from Parameter Store.

If you're going to run the CloudWatch agent on Amazon EC2 instances, use the following steps to create the necessary IAM role. This role provides permissions for reading information from the instance and writing it to CloudWatch.

To create the IAM role necessary to run the CloudWatch agent on EC2 instances

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane on the left, choose Roles and then Create role.
3. Make sure that AWS service is selected under Select type of trusted entity.
4. For Choose a use case, choose EC2 under Common use cases,
5. Choose Next: Permissions.
6. In the list of policies, select the check box next to CloudWatchAgentServerPolicy. If necessary, use the search box to find the policy.
7. Choose Next: Review.
8. Confirm that CloudWatchAgentServerPolicy appears next to Policies. In Role name, enter a name for the role, such as CloudWatchAgentServerRole. Optionally give it a description. Then choose Create role.

The role is now created.

If you're going to run the CloudWatch agent on on-premises servers, use the following steps to create the necessary IAM user.

To create the IAM user necessary for the CloudWatch agent to run on on-premises servers

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane on the left, choose Users and then Add user.
3. Enter the user name for the new user.
4. Select Programmatic access and choose Next: Permissions.
5. Choose Attach existing policies directly.
6. In the list of policies, select the check box next to CloudWatchAgentServerPolicy. If necessary, use the search box to find the policy.
7. Choose Next: Review.
8. Confirm that the correct policies are listed, and choose Create user.
9. Next to the name of the new user, choose Show. Copy the access key and secret key to a file so that you can use them when installing the agent. Choose Close.
Installing and running the CloudWatch agent on your servers

After you have created the agent configuration file that you want and created an IAM role or IAM user, use the following steps to install and run the agent on your servers, using that configuration. First, attach an IAM role or IAM user to the server that will run the agent. Then, on that server, download the agent package and start it using the agent configuration you created.

Download the CloudWatch agent package using an S3 download link

You need to install the agent on each server where you will run the agent. The CloudWatch agent is available as a package in Amazon Linux 2. If you are using this operating system, you can install the package by entering the following command. You must also make sure that the IAM role attached to the instance has the CloudWatchAgentServerPolicy attached. For more information, see Create IAM roles to use with the CloudWatch agent on Amazon EC2 instances (p. 444).

```
sudo yum install amazon-cloudwatch-agent
```

On all supported operating systems, you can download and install the CloudWatch agent using the command line with an Amazon S3 download link as described in the following steps.

For each download link, there is a general link as well as links for each Region. For example, for Amazon Linux and Amazon Linux 2 and the x86-64 architecture, three of the valid download links are:


<table>
<thead>
<tr>
<th>Architecture</th>
<th>Platform</th>
<th>Download link</th>
<th>Signature file link</th>
</tr>
</thead>
<tbody>
<tr>
<td>x86-64</td>
<td>Amazon Linux and Amazon Linux 2</td>
<td><a href="https://s3.amazonaws.com/amazoncloudwatch-agent/amazon_linux/amd64/latest/amazon-cloudwatch-agent.rpm">Link</a></td>
<td><a href="https://s3.amazonaws.com/amazoncloudwatch-agent/amazon_linux/amd64/latest/amazon-cloudwatch-agent.rpm.sig">Link</a></td>
</tr>
</tbody>
</table>

436
<table>
<thead>
<tr>
<th>Architecture</th>
<th>Platform</th>
<th>Download link</th>
<th>Signature file link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture</td>
<td>Platform</td>
<td>Download link</td>
<td>Signature file link</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| x86-64       | Oracle       | https://s3.amazonaws.com/amazoncloudwatch-agent/oracle_linux/amd64/latest/amazon-cloudwatch-agent.rpm  
| x86-64       | macOS        | https://s3.amazonaws.com/amazoncloudwatch-agent/darwin/amd64/latest/amazon-cloudwatch-agent.pkg  
| ARM64        | Amazon Linux 2 | https://s3.amazonaws.com/amazoncloudwatch-agent/amazon_linux/arm64/latest/amazon-cloudwatch-agent.rpm  
<table>
<thead>
<tr>
<th>Architecture</th>
<th>Platform</th>
<th>Download link</th>
<th>Signature file link</th>
</tr>
</thead>
</table>

**To use the command line to install the CloudWatch agent on an Amazon EC2 instance**

1. Download the CloudWatch agent. For a Linux server, enter the following. For `download-link`, use the appropriate download link from the previous table.

   ```bash
   wget download-link
   ```

   For a server running Windows Server, download the following file:

   ```text
   ```

2. After you have downloaded the package, you can optionally verify the package signature. For more information, see [Verifying the signature of the CloudWatch agent package](p. 460).

3. Install the package. If you downloaded an RPM package on a Linux server, change to the directory containing the package and enter the following:
Installing the CloudWatch agent using the command line

```
sudo rpm -U ./amazon-cloudwatch-agent.rpm
```

If you downloaded a DEB package on a Linux server, change to the directory containing the package and enter the following:

```
sudo dpkg -i -E ./amazon-cloudwatch-agent.deb
```

If you downloaded an MSI package on a server running Windows Server, change to the directory containing the package and enter the following:

```
msiexec /i amazon-cloudwatch-agent.msi
```

This command also works from within PowerShell. For more information about MSI command options, see Command-Line Options in the Microsoft Windows documentation.

(Installing on an EC2 instance) Attaching an IAM role

To enable the CloudWatch agent to send data from the instance, you must attach an IAM role to the instance. The role to attach is **CloudWatchAgentServerRole**.

For more information on attaching an IAM role to an instance, see Attaching an IAM Role to an Instance in the *Amazon EC2 User Guide for Windows Instances*.

(Installing on an on-premises server) Specify IAM credentials and AWS Region

To enable the CloudWatch agent to send data from an on-premises server, you must specify the access key and secret key of the IAM user that you created earlier. For more information about creating this user, see Create IAM roles and users for use with CloudWatch agent (p. 435).

You also must specify the AWS Region to send the metrics to, using the `region` field in the `[AmazonCloudWatchAgent]` section of the AWS config file, as in the following example.

```
[profile AmazonCloudWatchAgent]
region = us-west-1
```

The following is an example of using the `aws configure` command to create a named profile for the CloudWatch agent. This example assumes that you are using the default profile name of `AmazonCloudWatchAgent`.

**To create the AmazonCloudWatchAgent profile for the CloudWatch agent**

1. If you haven't already done so, install the AWS Command Line Interface on the server. For more information, see Installing the AWS CLI.
2. On Linux servers, enter the following command and follow the prompts:

```
sudo aws configure --profile AmazonCloudWatchAgent
```

On Windows Server, open PowerShell as an administrator, enter the following command, and follow the prompts.

```
aws configure --profile AmazonCloudWatchAgent
```
Verify internet access

Your Amazon EC2 instances must have outbound internet access to send data to CloudWatch or CloudWatch Logs. For more information about how to configure internet access, see Internet Gateways in the Amazon VPC User Guide.

The endpoints and ports to configure on your proxy are as follows:

- If you’re using the agent to collect metrics, you must whitelist the CloudWatch endpoints for the appropriate Regions. These endpoints are listed in Amazon CloudWatch in the Amazon Web Services General Reference.
- If you’re using the agent to collect logs, you must whitelist the CloudWatch Logs endpoints for the appropriate Regions. These endpoints are listed in Amazon CloudWatch Logs in the Amazon Web Services General Reference.
- If you’re using Systems Manager to install the agent or Parameter Store to store your configuration file, you must whitelist the Systems Manager endpoints for the appropriate Regions. These endpoints are listed in AWS Systems Manager in the Amazon Web Services General Reference.

(Optional) Modify the common configuration for proxy or Region information

The CloudWatch agent includes a configuration file called `common-config.toml`. You can optionally use this file to specify proxy and Region information.

On a server running Linux, this file is in the `/opt/aws/amazon-cloudwatch-agent/etc` directory. On a server running Windows Server, this file is in the `C:\ProgramData\Amazon\AmazonCloudWatchAgent` directory.

The default `common-config.toml` is as follows.

```
# This common-config is used to configure items used for both ssm and cloudwatch access

## Configuration for shared credential.
## Default credential strategy will be used if it is absent here:
## Instance role is used for EC2 case by default.
## AmazonCloudWatchAgent profile is used for onPremise case by default.
## [credentials]
#    shared_credential_profile = "{profile_name}"
#    shared_credential_file = "{file_name}"

## Configuration for proxy.
## System-wide environment-variable will be read if it is absent here.
## i.e. HTTP_PROXY/http_proxy; HTTPS_PROXY/https_proxy; NO_PROXY/no_proxy
## Note: system-wide environment-variable is not accessible when using ssm run-command.
## Absent in both here and environment-variable means no proxy will be used.
## [proxy]
#    http_proxy = "{http_url}"
#    https_proxy = "{https_url}"
#    no_proxy = "{domain}"
```

All lines are commented out initially. To set the credential profile or proxy settings, remove the `#` from that line and specify a value. You can edit this file manually or by using the RunShellScript Run Command in Systems Manager:

- `shared_credential_profile` – For on-premises servers, this line specifies the IAM user credential profile to use to send data to CloudWatch. If you keep this line commented out, `AmazonCloudWatchAgent` is used. For more information about creating this profile, see (Installing on an on-premises server) Specify IAM credentials and AWS Region (p. 440).

441
On an EC2 instance, you can use this line to have the CloudWatch agent send data from this instance to CloudWatch in a different AWS Region. To do so, specify a named profile that includes a region field specifying the name of the Region to send to.

If you specify a shared_credential_profile, you must also remove the # from the beginning of the [credentials] line.

- shared_credential_file – To have the agent look for credentials in a file located in a path other than the default path, specify that complete path and file name here. The default path is /root/.aws on Linux and is C:\Users\Administrator\.aws on Windows Server.

The first example below shows the syntax of a valid shared_credential_file line for Linux servers, and the second example is valid for Windows Server. On Windows Server, you must escape the \ characters.

| shared_credential_file= "/usr/username/credentials" |
| shared_credential_file= "C:\\Documents and Settings\\username\\aws\\credentials" |

If you specify a shared_credential_file, you must also remove the # from the beginning of the [credentials] line.

- Proxy settings – If your servers use HTTP or HTTPS proxies to contact AWS services, specify those proxies in the http_proxy and https_proxy fields. If there are URLs that should be excluded from proxying, specify them in the no_proxy field, separated by commas.

**Start the CloudWatch agent using the command line**

Follow these steps to use the command line to start the CloudWatch agent on a server.

**To use the command line to start the CloudWatch agent on a server**

1. Copy the agent configuration file that you want to use to the server where you’re going to run the agent. Note the pathname where you copy it to.
2. In this command, -a fetch-config causes the agent to load the latest version of the CloudWatch agent configuration file, and -s starts the agent.

Enter one of the following commands. Replace configuration-file-path with the path to the agent configuration file. This file is called config.json if you created it with the wizard, and might be called amazon-cloudwatch-agent.json if you created it manually.

On an EC2 instance running Linux, enter the following command.

```bash
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:configuration-file-path
```

On an on-premises server running Linux, enter the following:

```bash
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m onPremise -s -c file:configuration-file-path
```

On an EC2 instance running Windows Server, enter the following from the PowerShell console:

```bash
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m ec2 -s -c file:configuration-file-path
```
On an on-premises server running Windows Server, enter the following from the PowerShell console:

```
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m onPremise -s -c file:configuration-file-path
```

### Installing the CloudWatch agent using AWS Systems Manager

Use the following topics to install and run the CloudWatch agent using AWS Systems Manager.

**Topics**
- Create IAM roles and users for use with the CloudWatch agent (p. 443)
- Download and configure the CloudWatch agent (p. 446)
- Installing the CloudWatch agent on EC2 instances using your agent configuration (p. 448)
- Installing the CloudWatch agent on on-premises servers (p. 452)

### Create IAM roles and users for use with the CloudWatch agent

Access to AWS resources requires permissions. You can create IAM roles and users that include the permissions that you need for the CloudWatch agent to write metrics to CloudWatch and for the CloudWatch agent to communicate with Amazon EC2 and AWS Systems Manager. You use IAM roles on Amazon EC2 instances, and you use IAM users with on-premises servers.

One role or user enables CloudWatch agent to be installed on a server and send metrics to CloudWatch. The other role or user is needed to store your CloudWatch agent configuration in Systems Manager Parameter Store. Parameter Store enables multiple servers to use one CloudWatch agent configuration.

The ability to write to Parameter Store is a broad and powerful permission. You should use it only when you need it, and it shouldn't be attached to multiple instances in your deployment. If you store your CloudWatch agent configuration in Parameter Store, we recommend the following:

- Set up one instance where you perform this configuration.
- Use the IAM role with permissions to write to Parameter Store only on this instance.
- Use the IAM role with permissions to write to Parameter Store only while you are working with and saving the CloudWatch agent configuration file.

**Note**

We recently modified the following procedures by using new CloudWatchAgentServerPolicy and CloudWatchAgentAdminPolicy policies created by Amazon, instead of requiring customers to create these policies themselves. To use these policies to write the agent configuration file to Parameter Store and then download it from Parameter Store, your agent configuration file must have a name that starts with AmazonCloudWatch-. If you have a CloudWatch agent configuration file with a file name that doesn't start with AmazonCloudWatch-, these policies can't be used to write the file to Parameter Store or to download the file from Parameter Store.
Create IAM roles to use with the CloudWatch agent on Amazon EC2 instances

The first procedure creates the IAM role that you must attach to each Amazon EC2 instance that runs the CloudWatch agent. This role provides permissions for reading information from the instance and writing it to CloudWatch.

The second procedure creates the IAM role that you must attach to the Amazon EC2 instance being used to create the CloudWatch agent configuration file. This step is necessary if you're going to store this file in Systems Manager Parameter Store so that other servers can use it. This role provides permissions for writing to Parameter Store, in addition to the permissions for reading information from the instance and writing it to CloudWatch. This role includes permissions sufficient to run the CloudWatch agent as well as to write to Parameter Store.

Note
Parameter Store supports parameters in Standard and Advanced tiers. These parameter tiers are not related to the Basic, Standard, and Advanced levels of details available with the CloudWatch Agent predefined metric sets.

To create the IAM role necessary for each server to run the CloudWatch agent

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Roles and then choose Create role.
3. Under Select type of trusted entity, choose AWS service.
4. Immediately under Common use cases, choose EC2, and then choose Next: Permissions.
5. In the list of policies, select the check box next to CloudWatchAgentServerPolicy. If necessary, use the search box to find the policy.
6. To use Systems Manager to install or configure the CloudWatch agent, select the box next to AmazonSSMManagedInstanceCore. This AWS managed policy enables an instance to use Systems Manager service core functionality. If necessary, use the search box to find the policy. This policy isn't necessary if you start and configure the agent only through the command line.
7. Choose Next: Tags.
8. (Optional) Add one or more tag-key value pairs to organize, track, or control access for this role, and then choose Next: Review.
9. For Role name, enter a name for your new role, such as CloudWatchAgentServerRole or another name that you prefer.
10. (Optional) For Role description, enter a description.
11. Confirm that CloudWatchAgentServerPolicy and optionally AmazonSSMManagedInstanceCore appear next to Policies.
12. Choose Create role.

The role is now created.

The following procedure creates the IAM role that can also write to Parameter Store. You can use this role to store the agent configuration file in Parameter Store so that other servers can retrieve it.

The permissions for writing to Parameter Store provide broad access. This role shouldn't be attached to all your servers, and only administrators should use it. After you create the agent configuration file and copy it to Parameter Store, you should detach this role from the instance and use CloudWatchAgentServerRole instead.

To create the IAM role for an administrator to write to Parameter Store

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Roles and then choose Create role.
3. Under Select type of trusted entity, choose AWS service.
4. Immediately under Choose the service that will use this role, choose EC2, and then choose Next: Permissions.
5. In the list of policies, select the check box next to CloudWatchAgentAdminPolicy. If necessary, use the search box to find the policy.
6. To use Systems Manager to install or configure the CloudWatch agent, select the box next to AmazonSSMManagedInstanceCore. This AWS managed policy enables an instance to use Systems Manager service core functionality. If necessary, use the search box to find the policy. This policy isn't necessary if you start and configure the agent only through the command line.
7. Choose Next: Tags.
8. (Optional) Add one or more tag-key value pairs to organize, track, or control access for this role, and then choose Next: Review.
9. For Role name, enter a name for your new role, such as CloudWatchAgentAdminRole or another name that you prefer.
10. (Optional) For Role description, enter a description.
11. Confirm that CloudWatchAgentAdminPolicy and optionally AmazonSSMManagedInstanceCore appear next to Policies.
12. Choose Create role.

The role is now created.

Create IAM users to use with the CloudWatch agent on on-premises servers

The first procedure creates the IAM user that you need to run the CloudWatch agent. This user provides permissions to send data to CloudWatch.

The second procedure creates the IAM user that you can use when creating the CloudWatch agent configuration file. Use this procedure to store this file in Systems Manager Parameter Store so that other servers can use it. This user provides permissions to write to Parameter Store, in addition to the permissions to write data to CloudWatch.

**Note**
Parameter Store supports parameters in Standard and Advanced tiers. These parameter tiers are not related to the Basic, Standard, and Advanced levels of details available with the CloudWatch Agent predefined metric sets.

To create the IAM user necessary for the CloudWatch agent to write data to CloudWatch

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Users, and then choose Add user.
3. Enter the user name for the new user.
4. For Access type, select Programmatic access, and then choose Next: Permissions.
5. For Set permissions, choose Attach existing policies directly.
6. In the list of policies, select the check box next to CloudWatchAgentServerPolicy. If necessary, use the search box to find the policy.
7. To use Systems Manager to install or configure the CloudWatch agent, select the box next to AmazonSSMManagedInstanceCore. This AWS managed policy enables an instance to use Systems Manager service core functionality. (If necessary, use the search box to find the policy. This policy isn't necessary if you start and configure the agent only through the command line.)
8. Choose Next: Tags.
9. (Optional) Add one or more tag-key value pairs to organize, track, or control access for this role, and then choose **Next: Review**.

10. Confirm that the correct policies are listed, and then choose **Create user**.

11. In the row for the new user, choose **Show**. Copy the access key and secret key to a file so that you can use them when installing the agent. Choose **Close**.

The following procedure creates the IAM user that can also write to Parameter Store. If you’re going to store the agent configuration file in Parameter Store so that other servers can use it, you need to use this IAM user. This IAM user provides permissions for writing to Parameter Store. This user also provides the permissions for reading information from the instance and writing it to CloudWatch. The permissions for writing to Systems Manager Parameter Store provide broad access. This IAM user shouldn’t be attached to all your servers, and only administrators should use it. You should use this IAM user only when you are storing the agent configuration file in Parameter Store.

**To create the IAM user necessary to store the configuration file in Parameter Store and send information to CloudWatch**

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.

2. In the navigation pane, choose **Users**, and then choose **Add user**.

3. Enter the user name for the new user.

4. For **Access type**, select **Programmatic access**, and then choose **Next: Permissions**.

5. For **Set permissions**, choose **Attach existing policies directly**.

6. In the list of policies, select the check box next to **CloudWatchAgentAdminPolicy**. If necessary, use the search box to find the policy.

7. To use Systems Manager to install or configure the CloudWatch agent, select the check box next to **AmazonSSMManagedInstanceCore**. This AWS managed policy enables an instance to use Systems Manager service core functionality. (If necessary, use the search box to find the policy. This policy isn’t necessary if you start and configure the agent only through the command line.)

8. Choose **Next: Tags**.

9. (Optional) Add one or more tag-key value pairs to organize, track, or control access for this role, and then choose **Next: Review**.

10. Confirm that the correct policies are listed, and then choose **Create user**.

11. In the row for the new user, choose **Show**. Copy the access key and secret key to a file so that you can use them when installing the agent. Choose **Close**.

**Download and configure the CloudWatch agent**

This section explains how to use Systems Manager to download the agent and then how to create your agent configuration file. Before you can use Systems Manager to download the agent, you must make sure that the instance is configured correctly for Systems Manager.

**Installing or updating SSM Agent**

On an Amazon EC2 instance, the CloudWatch agent requires that the instance is running version 2.2.93.0 or later. Before you install the CloudWatch agent, update or install SSM Agent on the instance if you haven’t already done so.

For information about installing or updating SSM Agent on an instance running Linux, see **Installing and Configuring SSM Agent on Linux Instances** in the *AWS Systems Manager User Guide*.

For information about installing or updating the SSM Agent, see **Working with SSM Agent** in the *AWS Systems Manager User Guide*.
(Optional) Verify Systems Manager prerequisites

Before you use Systems Manager Run Command to install and configure the CloudWatch agent, verify that your instances meet the minimum Systems Manager requirements. For more information, see Systems Manager Prerequisites in the AWS Systems Manager User Guide.

Verify internet access

Your Amazon EC2 instances must have outbound internet access to send data to CloudWatch or CloudWatch Logs. For more information about how to configure internet access, see Internet Gateways in the Amazon VPC User Guide.

The endpoints and ports to configure on your proxy are as follows:

- If you’re using the agent to collect metrics, you must whitelist the CloudWatch endpoints for the appropriate Regions. These endpoints are listed in Amazon CloudWatch in the Amazon Web Services General Reference.
- If you’re using the agent to collect logs, you must whitelist the CloudWatch Logs endpoints for the appropriate Regions. These endpoints are listed in Amazon CloudWatch Logs in the Amazon Web Services General Reference.
- If you’re using Systems Manager to install the agent or Parameter Store to store your configuration file, you must whitelist the Systems Manager endpoints for the appropriate Regions. These endpoints are listed in AWS Systems Manager in the Amazon Web Services General Reference.

Use the following steps to download the CloudWatch agent package using Systems Manager.

To download the CloudWatch agent using Systems Manager

2. In the navigation pane, choose Run Command.
   - or -
   If the AWS Systems Manager home page opens, scroll down and choose Explore Run Command.
3. Choose Run command.
4. In the Command document list, choose AWS-ConfigureAWSPackage.
5. In the Targets area, choose the instance to install the CloudWatch agent on. If you don’t see a specific instance, it might not be configured as a managed instance for use with Systems Manager. For more information, see Setting Up AWS Systems Manager for Hybrid Environments in the AWS Systems Manager User Guide.
6. In the Action list, choose Install.
7. In the Name field, enter AmazonCloudWatchAgent.
8. Keep Version set to latest to install the latest version of the agent.
10. Optionally, in the Targets and outputs areas, select the button next to an instance name and choose View output. Systems Manager should show that the agent was successfully installed.

Create and modify the agent configuration file

After you have downloaded the CloudWatch agent, you must create the configuration file before you start the agent on any servers.

If you’re going to save your agent configuration file in the Systems Manager Parameter Store, you must use an EC2 instance to save to the Parameter Store. Additionally, you must first attach to that instance.
the CloudWatchAgentAdminRole IAM role. For more information about attaching roles, see Attaching an IAM Role to an Instance in the Amazon EC2 User Guide for Windows Instances.

For more information about creating the CloudWatch agent configuration file, see Create the CloudWatch agent configuration file (p. 466).

Installing the CloudWatch agent on EC2 instances using your agent configuration

After you have a CloudWatch agent configuration saved in Parameter Store, you can use it when you install the agent on other servers.

Topics

• Attach an IAM role to the instance (p. 448)
• Download the CloudWatch agent package on an Amazon EC2 instance (p. 448)
• (Optional) Modify the common configuration and named profile for CloudWatch agent (p. 449)
• Start the CloudWatch agent (p. 450)

Attach an IAM role to the instance

You must attach the CloudWatchAgentServerRole IAM role to the EC2 instance to be able to run the CloudWatch agent on the instance. This role enables the CloudWatch agent to perform actions on the instance.

For more information, see Attaching an IAM Role to an Instance in the Amazon EC2 User Guide for Windows Instances.

Download the CloudWatch agent package on an Amazon EC2 instance

You need to install the agent on each server where you will run the agent. The CloudWatch agent is available as a package in Amazon Linux 2. If you are using this operating system, you can install the package by entering the following command. You must also make sure that the IAM role attached to the instance has the CloudWatchAgentServerPolicy attached. For more information, see Create IAM roles to use with the CloudWatch agent on Amazon EC2 instances (p. 444).

```bash
sudo yum install amazon-cloudwatch-agent
```

On all supported operating systems, you can download the CloudWatch agent package using either Systems Manager Run Command or an Amazon S3 download link. For information about using an Amazon S3 download link, see Download the CloudWatch agent package (p. 430).

Download the CloudWatch agent on an Amazon EC2 instance Using Systems Manager

Before you can use Systems Manager to install the CloudWatch agent, you must make sure that the instance is configured correctly for Systems Manager.

Installing or updating SSM Agent

On an Amazon EC2 instance, the CloudWatch agent requires that the instance is running version 2.2.93.0 or later. Before you install the CloudWatch agent, update or install SSM Agent on the instance if you haven’t already done so.

For information about installing or updating SSM Agent on an instance running Linux, see Installing and Configuring the SSM Agent on Linux Instances in the AWS Systems Manager User Guide.

For information about installing or updating SSM Agent on an instance running Windows Server, see Installing and Configuring SSM Agent on Windows Instances in the AWS Systems Manager User Guide.
Install the CloudWatch agent using Systems Manager

(Optional) Verify Systems Manager prerequisites

Before you use Systems Manager Run Command to install and configure the CloudWatch agent, verify that your instances meet the minimum Systems Manager requirements. For more information, see Setting Up AWS Systems Manager in the AWS Systems Manager User Guide.

Verify internet access

Your Amazon EC2 instances must have outbound internet access in order to send data to CloudWatch or CloudWatch Logs. For more information about how to configure internet access, see Internet Gateways in the Amazon VPC User Guide.

Download the CloudWatch agent package

Systems Manager Run Command enables you to manage the configuration of your instances. You specify a Systems Manager document, specify parameters, and execute the command on one or more instances. SSM Agent on the instance processes the command and configures the instance as specified.

To download the CloudWatch agent using Run Command

2. In the navigation pane, choose Run Command.
   -or-
   If the AWS Systems Manager home page opens, scroll down and choose Explore Run Command.
3. Choose Run command.
4. In the Command document list, choose AWS-ConfigureAWSPackage.
5. In the Targets area, choose the instance on which to install the CloudWatch agent. If you do not see a specific instance, it might not be configured for Run Command. For more information, see Setting Up AWS Systems Manager for Hybrid Environments in the AWS Systems Manager User Guide.
6. In the Action list, choose Install.
7. In the Name box, enter AmazonCloudWatchAgent.
8. Keep Version set to latest to install the latest version of the agent.
10. Optionally, in the Targets and outputs areas, select the button next to an instance name and choose View output. Systems Manager should show that the agent was successfully installed.

(Optional) Modify the common configuration and named profile for CloudWatch agent

The CloudWatch agent includes a configuration file called common-config.toml. You can use this file optionally specify proxy and Region information.

On a server running Linux, this file is in the /opt/aws/amazon-cloudwatch-agent/etc directory. On a server running Windows Server, this file is in the C:\ProgramData\Amazon\AmazonCloudWatchAgent directory.

The default common-config.toml is as follows:

```
# This common-config is used to configure items used for both ssm and cloudwatch access

## Configuration for shared credential.
## Default credential strategy will be used if it is absent here:
## Instance role is used for EC2 case by default.
## AmazonCloudWatchAgent profile is used for onPremise case by default.
```
All lines are commented out initially. To set the credential profile or proxy settings, remove the # from that line and specify a value. You can edit this file manually, or by using the RunShellScript Run Command in Systems Manager:

- **shared_credential_profile** – For on-premises servers, this line specifies the IAM user credential profile to use to send data to CloudWatch. If you keep this line commented out, AmazonCloudWatchAgent is used.

  On an EC2 instance, you can use this line to have the CloudWatch agent send data from this instance to CloudWatch in a different AWS Region. To do so, specify a named profile that includes a region field specifying the name of the Region to send to.

  If you specify a shared_credential_profile, you must also remove the # from the beginning of the [credentials] line.

- **shared_credential_file** – To have the agent look for credentials in a file located in a path other than the default path, specify that complete path and file name here. The default path is /root/.aws on Linux and is C:\Users\Administrator\.aws on Windows Server.

  The first example below shows the syntax of a valid shared_credential_file line for Linux servers, and the second example is valid for Windows Server. On Windows Server, you must escape the \ characters.

    shared_credential_file= "/usr/username/credentials"

    shared_credential_file= "C:\\Documents and Settings\\username\\.aws\\credentials"

  If you specify a shared_credential_file, you must also remove the # from the beginning of the [credentials] line.

- **Proxy settings** – If your servers use HTTP or HTTPS proxies to contact AWS services, specify those proxies in the http_proxy and https_proxy fields. If there are URLs that should be excluded from proxying, specify them in the no_proxy field, separated by commas.

  **Start the CloudWatch agent**

  You can start the agent using Systems Manager Run Command or the command line.

  **Start the CloudWatch agent using Systems Manager Run Command**

  Follow these steps to start the agent using Systems Manager Run Command.

  **To start the CloudWatch agent using Run Command**

2. In the navigation pane, choose Run Command.

-or-

If the AWS Systems Manager home page opens, scroll down and choose Explore Run Command.

3. Choose Run command.

4. In the Command document list, choose AmazonCloudWatch-ManageAgent.

5. In the Targets area, choose the instance where you installed the CloudWatch agent.

6. In the Action list, choose configure.

7. In the Optional Configuration Source list, choose ssm.

8. In the Optional Configuration Location box, enter the name of the agent configuration file that you created and saved to Systems Manager Parameter Store, as explained in Create the CloudWatch agent configuration file (p. 466).

9. In the Optional Restart list, choose yes to start the agent after you have finished these steps.


11. Optionally, in the Targets and outputs areas, select the button next to an instance name and choose View output. Systems Manager should show that the agent was successfully started.

Start the CloudWatch agent on an Amazon EC2 instance using the command line

Follow these steps to use the command line to install the CloudWatch agent on an Amazon EC2 instance.

To use the command line to start the CloudWatch agent on an Amazon EC2 instance

- In this command, -a fetch-config causes the agent to load the latest version of the CloudWatch agent configuration file, and -s starts the agent.

Linux and macOS: If you saved the configuration file in the Systems Manager Parameter Store, enter the following:

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c ssm:configuration-parameter-store-name
```

Linux and macOS: If you saved the configuration file on the local computer, enter the following command. Replace configuration-file-path with the path to the agent configuration file. This file is called config.json if you created it with the wizard, and might be called amazon-cloudwatch-agent.json if you created it manually.

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:configuration-file-path
```

Windows Server: If you saved the agent configuration file in Systems Manager Parameter Store, enter the following from the PowerShell console:

```
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m ec2 -s -c ssm:configuration-parameter-store-name
```

Windows Server: If you saved the agent configuration file on the local computer, enter the following from the PowerShell console:

```
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m ec2 -s -c file:"C:\Program Files\Amazon\AmazonCloudWatchAgent\config.json"
```
Installing the CloudWatch agent on on-premises servers

If you have downloaded the CloudWatch agent on one computer and created the agent configuration file you want, you can use that configuration file to install the agent on other on-premises servers.

Download the CloudWatch agent on an on-premises server

You can download the CloudWatch agent package using either Systems Manager Run Command or an Amazon S3 download link. For information about using an Amazon S3 download link, see Download the CloudWatch agent package (p. 430).

Download using Systems Manager

To use Systems Manager Run Command, you must register your on-premises server with Amazon EC2 Systems Manager. For more information, see Setting Up Systems Manager in Hybrid Environments in the AWS Systems Manager User Guide.

If you have already registered your server, update SSM Agent to the latest version.

For information about updating SSM Agent on a server running Linux, see Install SSM Agent for a Hybrid Environment (Linux) in the AWS Systems Manager User Guide.

For information about updating the SSM Agent on a server running Windows Server, see Install SSM Agent for a Hybrid Environment (Windows) in the AWS Systems Manager User Guide.

To use the SSM Agent to download the CloudWatch agent package on an on-premises server

2. In the navigation pane, choose Run Command.
   -or-
   If the AWS Systems Manager home page opens, scroll down and choose Explore Run Command.
3. Choose Run command.
4. In the Command document list, select the button next to AWS-ConfigureAWSPackage.
5. In the Targets area, select the server to install the CloudWatch agent on. If you don't see a specific server, it might not be configured for Run Command. For more information, see Setting Up AWS Systems Manager for Hybrid Environments in the AWS Systems Manager User Guide.
6. In the Action list, choose Install.
7. In the Name box, enter AmazonCloudWatchAgent.
8. Keep Version blank to install the latest version of the agent.

The agent package is downloaded, and the next steps are to configure and start it.

(Installing on an on-premises server) Specify IAM credentials and AWS Region

To enable the CloudWatch agent to send data from an on-premises server, you must specify the access key and secret key of the IAM user that you created earlier. For more information about creating this user, see Create IAM roles and users for use with the CloudWatch agent (p. 443).

You also must specify the AWS Region to send the metrics to, using the region field.

Following is an example of this file.

452
Install the CloudWatch agent using Systems Manager

```
[AmazonCloudWatchAgent]
aws_access_key_id=my_access_key
aws_secret_access_key=my_secret_key
region = us-west-1
```

For `my_access_key` and `my_secret_key`, use the keys from the IAM user that doesn’t have the permissions to write to Systems Manager Parameter Store. For more information about the IAM users needed for CloudWatch agent, see Create IAM users to use with the CloudWatch agent on on-premises servers (p. 445).

If you name this profile AmazonCloudWatchAgent, you don’t need to do anything more. Optionally, you can give it a different name and specify that name as the value for `shared_credential_profile` in the `common-config.toml` file, which is explained in the following section.

Following is an example of using the `aws configure` command to create a named profile for the CloudWatch agent. This example assumes that you’re using the default profile name of AmazonCloudWatchAgent.

**To create the AmazonCloudWatchAgent profile for the CloudWatch agent**

1. If you haven’t already done so, install the AWS Command Line Interface on the server. For more information, see Installing the AWS CLI.
2. On Linux servers, enter the following command and follow the prompts:

   ```
   sudo aws configure --profile AmazonCloudWatchAgent
   ```

   On Windows Server, open PowerShell as an administrator, enter the following command, and follow the prompts.

   ```
   aws configure --profile AmazonCloudWatchAgent
   ```

   *(Optional) Modifying the common configuration and named profile for CloudWatch agent*

   The CloudWatch agent includes a configuration file called `common-config.toml`. You can optionally use this file to specify proxy and Region information.

   On a server running Linux, this file is in the `/opt/aws/amazon-cloudwatch-agent/etc` directory. On a server running Windows Server, this file is in the `C:\ProgramData\Amazon\AmazonCloudWatchAgent` directory.

   The default `common-config.toml` is as follows:

   ```
   # This common-config is used to configure items used for both ssm and cloudwatch access
   
   ## Configuration for shared credential.
   ## Default credential strategy will be used if it is absent here:
   ##            Instance role is used for EC2 case by default.
   ##            AmazonCloudWatchAgent profile is used for onPremise case by default.
   # [credentials]
   #   shared_credential_profile = "{profile_name}"
   #   shared_credential_file = "{file_name}"
   
   ## Configuration for proxy.
   ## System-wide environment-variable will be read if it is absent here.
   ```

453
Install the CloudWatch agent using Systems Manager

## i.e. HTTP_PROXY/http_proxy; HTTPS_PROXY/https_proxy; NO_PROXY/no_proxy
## Note: system-wide environment-variable is not accessible when using ssm run-command.
## Absent in both here and environment-variable means no proxy will be used.

```yaml
# [proxy]
#    http_proxy = "{http_url}"
#    https_proxy = "{https_url}"
#    no_proxy = "{domain}"
```

All lines are commented out initially. To set the credential profile or proxy settings, remove the `#` from that line and specify a value. You can edit this file manually, or by using the RunShellScript Run Command in Systems Manager:

- **shared_credential_profile** – For on-premises servers, this line specifies the IAM user credential profile to use to send data to CloudWatch. If you keep this line commented out, AmazonCloudWatchAgent is used. For more information about creating this profile, see (Installing on an on-premises server) Specify IAM credentials and AWS Region (p. 452).

On an EC2 instance, you can use this line to have the CloudWatch agent send data from this instance to CloudWatch in a different AWS Region. To do so, specify a named profile that includes a `region` field specifying the name of the Region to send to.

If you specify a `shared_credential_profile`, you must also remove the `#` from the beginning of the `[credentials]` line.

- **shared_credential_file** – To have the agent look for credentials in a file located in a path other than the default path, specify that complete path and file name here. The default path is `/root/.aws` on Linux and is `C:\Users\Administrator\aws` on Windows Server.

The first example below shows the syntax of a valid `shared_credential_file` line for Linux servers, and the second example is valid for Windows Server. On Windows Server, you must escape the `\` characters.

```ini
shared_credential_file= "/usr/username/credentials"
```

```ini
shared_credential_file= "C:\\Documents and Settings\\username\\.aws\\credentials"
```

If you specify a `shared_credential_file`, you must also remove the `#` from the beginning of the `[credentials]` line.

- **Proxy settings** – If your servers use HTTP or HTTPS proxies to contact AWS services, specify those proxies in the `http_proxy` and `https_proxy` fields. If there are URLs that should be excluded from proxying, specify them in the `no_proxy` field, separated by commas.

### Starting the CloudWatch agent

You can start the CloudWatch agent using either Systems Manager Run Command or the command line.

**To use SSM Agent to start the CloudWatch agent on an on-premises server**

2. In the navigation pane, choose Run Command.
   - or -
3. Choose Run command.
4. In the **Command document** list, select the button next to AmazonCloudWatch-ManageAgent.
5. In the **Targets** area, select the instance where you installed the agent.
6. In the **Action** list, choose **configure**.
7. In the **Mode** list, choose **onPremise**.
8. In the **Optional Configuration Location** box, enter the name of the agent configuration file that you created with the wizard and stored in the Parameter Store.
9. Choose **Run**.

The agent starts with the configuration you specified in the configuration file.

**To use the command line to start the CloudWatch agent on an on-premises server**

- In this command, `-a fetch-config` causes the agent to load the latest version of the CloudWatch agent configuration file, and `-s` starts the agent.

Linux: If you saved the configuration file in the Systems Manager Parameter Store, enter the following:

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m onPremise -s -c ssm:configuration-parameter-store-name
```

Linux: If you saved the configuration file on the local computer, enter the following command. Replace `configuration-file-path` with the path to the agent configuration file. This file is called `config.json` if you created it with the wizard, and might be called `amazon-cloudwatch-agent.json` if you created it manually.

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m onPremise -s -c file:configuration-file-path
```

Windows Server: If you saved the agent configuration file in Systems Manager Parameter Store, enter the following from the PowerShell console:

```
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m onPremise -s -c ssm:configuration-parameter-store-name
```

Windows Server: If you saved the agent configuration file on the local computer, enter the following from the PowerShell console. Replace `configuration-file-path` with the path to the agent configuration file. This file is called `config.json` if you created it with the wizard, and might be called `amazon-cloudwatch-agent.json` if you created it manually.

```
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m onPremise -s -c file:configuration-file-path
```

**Installing the CloudWatch agent on new instances using AWS CloudFormation**

Amazon has uploaded several AWS CloudFormation templates to GitHub to help you install and update the CloudWatch agent on new Amazon EC2 instances. For more information about using AWS CloudFormation, see [What is AWS CloudFormation?](#).

The template location is [Deploy the Amazon CloudWatch agent to EC2 instances using AWS CloudFormation](#). This location includes both inline and ssm directories. Each of these directories contains templates for both Linux and Windows instances.
• The templates in the `inline` directory have the CloudWatch agent configuration embedded into the AWS CloudFormation template. By default, the Linux templates collect the metrics `mem_used_percent` and `swap_used_percent`, and the Windows templates collect `Memory % Committed Bytes In Use` and `Paging File % Usage`.

To modify these templates to collect different metrics, modify the following section of the template. The following example is from the template for Linux servers. Follow the format and syntax of the agent configuration file to make these changes. For more information, see [Manually create or edit the CloudWatch agent configuration file](p. 471).

```json
{
  "metrics":{
    "append_dimensions":{
      "AutoScalingGroupName":"${!aws:AutoScalingGroupName}",
      "ImageId":"${!aws:ImageId}",
      "InstanceId":"${!aws:InstanceId}",
      "InstanceType":"${!aws:instanceType}"
    },
    "metrics_collected":{
      "mem":{
        "measurement":[
          "mem_used_percent"
        ]
      },
      "swap":{
        "measurement":[
          "swap_used_percent"
        ]
      }
    }
  }
}
```

**Note**

In the inline templates, all placeholder variables must have an exclamation mark (!) before them as an escape character. You can see this in the example template. If you add other placeholder variables, be sure to add an exclamation mark before the name.

• The templates in the `ssm` directory load an agent configuration file from Parameter Store. To use these templates, you must first create a configuration file and upload it to Parameter Store. You then provide the Parameter Store name of the file in the template. You can create the configuration file manually or by using the wizard. For more information, see [Create the CloudWatch agent configuration file](p. 466).

You can use both types of templates for installing the CloudWatch agent and for updating the agent configuration.

**Tutorial: Install and configure the CloudWatch agent using an AWS CloudFormation inline template**

This tutorial walks you through using AWS CloudFormation to install the CloudWatch agent on a new Amazon EC2 instance. This tutorial installs on a new instance running Amazon Linux 2 using the inline templates, which don't require the use of the JSON configuration file or Parameter Store. The inline template includes the agent configuration in the template. In this tutorial, you use the default agent configuration contained in the template.

After the procedure for installing the agent, the tutorial continues with how to update the agent.
To use AWS CloudFormation to install the CloudWatch agent on a new instance

1. Download the template from GitHub. In this tutorial, download the inline template for Amazon Linux 2 as follows:

   ```bash
   ```


3. Choose **Create stack**.

4. For **Choose a template**, select **Upload a template to Amazon S3**, choose the downloaded template, and choose **Next**.

5. On the **Specify Details** page, fill out the following parameters and choose **Next**:
   - **Stack name**: Choose a stack name for your AWS CloudFormation stack.
   - **IAMRole**: Choose an IAM role that has permissions to write CloudWatch metrics and logs. For more information, see Create IAM roles to use with the CloudWatch agent on Amazon EC2 instances (p. 435).
   - **InstanceAMI**: Choose an AMI that is valid in the Region where you're going to launch your stack.
   - **InstanceType**: Choose a valid instance type.
   - **KeyName**: To enable SSH access to the new instance, choose an existing Amazon EC2 key pair. If you don't already have an Amazon EC2 key pair, you can create one in the AWS Management Console. For more information, see Amazon EC2 Key Pairs in the Amazon EC2 User Guide for Linux Instances.
   - **SSHLocation**: Specifies the IP address range that can be used to connect to the instance using SSH. The default allows access from any IP address.

6. On the **Options** page, you can choose to tag your stack resources. Choose **Next**.

7. On the **Review** page, review your information, acknowledge that the stack might create IAM resources, and then choose **Create**.

   If you refresh the console, you see that the new stack has the **CREATE_IN_PROGRESS** status.

8. When the instance is created, you can see it in the Amazon EC2 console. Optionally, you can connect to the host and check the progress.

Use the following command to confirm that the agent is installed:

   ```bash
   rpm -qa amazon-cloudwatch-agent
   ```

Use the following command to confirm that the agent is running:

   ```bash
   ps aux | grep amazon-cloudwatch-agent
   ```

The next procedure demonstrates using AWS CloudFormation to update the CloudWatch agent using an inline template. The default inline template collects the `mem_used_percent` metric. In this tutorial, you change the agent configuration to stop collecting that metric.

To use AWS CloudFormation to update the CloudWatch agent

1. In the template that you downloaded in the previous procedure, remove the following lines and then save the template:

   ```json
   "mem": {
   ```
3. On the AWS CloudFormation dashboard, select the stack that you created and choose Update Stack.
4. For Select Template, select Upload a template to Amazon S3, choose the template that you modified, and choose Next.
5. On the Options page, choose Next and then Next.
6. On the Review page, review your information and choose Update.

After some time, you see UPDATE_COMPLETE.

Tutorial: Install the CloudWatch agent using AWS CloudFormation and Parameter Store

This tutorial walks you through using AWS CloudFormation to install the CloudWatch agent on a new Amazon EC2 instance. This tutorial installs on a new instance running Amazon Linux 2 using an agent configuration file that you create and save in Parameter Store.

After the procedure for installing the agent, the tutorial continues with how to update the agent.

To use AWS CloudFormation to install the CloudWatch agent on a new instance using a configuration from Parameter Store

1. If you haven't done so already, download the CloudWatch agent package to one of your computers so that you can create the agent configuration file. For more information and downloading the agent using Parameter Store, see Download and configure the CloudWatch agent (p. 446). For more information on downloading the package using the command line, see Download and configure the CloudWatch agent using the command line (p. 430).
2. Create the agent configuration file and save it in Parameter Store. For more information, see Create the CloudWatch agent configuration file (p. 466).
3. Download the template from GitHub as follows:


5. Choose Create stack.
6. For Choose a template, select Upload a template to Amazon S3, choose the template that you downloaded, and choose Next.
7. On the Specify Details page, fill out the following parameters accordingly and choose Next:
   - Stack name: Choose a stack name for your AWS CloudFormation stack.
   - IAMRole: Choose an IAM role that has permissions to write CloudWatch metrics and logs. For more information, see Create IAM roles to use with the CloudWatch agent on Amazon EC2 instances (p. 444).
   - InstanceAMI: Choose an AMI that is valid in the Region where you're going to launch your stack.
   - InstanceType: Choose a valid instance type.
   - KeyName: To enable SSH access to the new instance, choose an existing Amazon EC2 key pair. If you don't already have an Amazon EC2 key pair, you can create one in the AWS Management Console.
Installing the CloudWatch agent on new instances using AWS CloudFormation

Console. For more information, see Amazon EC2 Key Pairs in the Amazon EC2 User Guide for Linux Instances.

- **SSHLocation**: Specifies the IP address range that can be used to connect to the instance using SSH. The default allows access from any IP address.
- **SSMKey**: Specifies the agent configuration file that you created and saved in Parameter Store.

8. On the **Options** page, you can choose to tag your stack resources. Choose **Next**.

9. On the **Review** page, review your information, acknowledge that the stack might create IAM resources, and then choose **Create**.

If you refresh the console, you see that the new stack has the CREATE_IN_PROGRESS status.

10. When the instance is created, you can see it in the Amazon EC2 console. Optionally, you can connect to the host and check the progress.

Use the following command to confirm that the agent is installed:

```
rpm -qa amazon-cloudwatch-agent
```

Use the following command to confirm that the agent is running:

```
ps aux | grep amazon-cloudwatch-agent
```

The next procedure demonstrates using AWS CloudFormation to update the CloudWatch agent, using an agent configuration that you saved in Parameter Store.

**To use AWS CloudFormation to update the CloudWatch agent using a configuration in Parameter Store**

1. Change the agent configuration file stored in Parameter Store to the new configuration that you want.

2. In the AWS CloudFormation template that you downloaded in the section called “Tutorial: Install the CloudWatch agent using AWS CloudFormation and Parameter Store” (p. 458) topic, change the version number. For example, you might change `VERSION=1.0` to `VERSION=2.0`.


4. On the AWS CloudFormation dashboard, select the stack that you created and choose **Update Stack**.

5. For **Select Template**, select **Upload a template to Amazon S3**, select the template that you just modified, and choose **Next**.

6. On the **Options** page, choose **Next** and then **Next**.

7. On the **Review** page, review your information and choose **Update**.

After some time, you see UPDATE_COMPLETE.

**Troubleshooting installation of the CloudWatch agent with AWS CloudFormation**

This section helps you troubleshoot issues with installing and updating the CloudWatch agent using AWS CloudFormation.

**Detecting when an update fails**

If you use AWS CloudFormation to update your CloudWatch agent configuration, and use an invalid configuration, the agent stops sending any metrics to CloudWatch. A quick way to check whether an agent configuration update succeeded is to look at the `cfn-init-cmd.log` file. On a Linux server, the
file is located at /var/log/cfn-init-cmd.log. On a Windows instance, the file is located at C:\cfn\log\cfn-init-cmd.log.

Metrics are missing

If you don’t see metrics that you expect to see after installing or updating the agent, confirm that the agent is configured to collect that metric. To do this, check the `amazon-cloudwatch-agent.json` file to make sure that the metric is listed, and check that you are looking in the correct metric namespace. For more information, see CloudWatch agent files and locations (p. 542).

Verifying the signature of the CloudWatch agent package

GPG signature files are included for CloudWatch agent packages on Linux servers. You can use a public key to verify that the agent download file is original and unmodified.

For Windows Server, you can use the MSI to verify the signature.

For macOS computers, the signature is included in the agent download package.

To find the correct signature file, see the following table. For each architecture and operating system there is a general link as well as links for each Region. For example, for Amazon Linux and Amazon Linux 2 and the x86-64 architecture, three of the valid links are:


<table>
<thead>
<tr>
<th>Architecture</th>
<th>Platform</th>
<th>Download link</th>
<th>Signature file link</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architecture</td>
<td>Platform</td>
<td>Download link</td>
<td>Signature file link</td>
</tr>
<tr>
<td>--------------</td>
<td>---------</td>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Architecture</td>
<td>Platform</td>
<td>Download link</td>
<td>Signature file link</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>x86-64</td>
<td>Oracle</td>
<td><a href="https://s3.amazonaws.com/amazoncloudwatch-agent/oracle_linux/amd64/latest/amazon-cloudwatch-agent.rpm">https://s3.amazonaws.com/amazoncloudwatch-agent/oracle_linux/amd64/latest/amazon-cloudwatch-agent.rpm</a></td>
<td></td>
</tr>
<tr>
<td>x86-64</td>
<td>macOS</td>
<td><a href="https://s3.amazonaws.com/amazoncloudwatch-agent/darwin/amd64/latest/amazon-cloudwatch-agent.pkg">https://s3.amazonaws.com/amazoncloudwatch-agent/darwin/amd64/latest/amazon-cloudwatch-agent.pkg</a></td>
<td></td>
</tr>
<tr>
<td>ARM64</td>
<td>Amazon Linux 2</td>
<td><a href="https://s3.amazonaws.com/amazoncloudwatch-agent/amazon_linux/arm64/latest/amazon-cloudwatch-agent.rpm">https://s3.amazonaws.com/amazoncloudwatch-agent/amazon_linux/arm64/latest/amazon-cloudwatch-agent.rpm</a></td>
<td></td>
</tr>
</tbody>
</table>
To verify the CloudWatch agent package on a Linux server

1. Download the public key.

   shell$ wget https://s3.amazonaws.com/amazoncloudwatch-agent/assets/amazon-cloudwatch-agent.gpg

2. Import the public key into your keyring.

   shell$ gpg --import amazon-cloudwatch-agent.gpg
   gpg: key 3B789C72: public key "Amazon CloudWatch Agent" imported
   gpg: Total number processed: 1
   gpg: imported: 1 (RSA: 1)

   Make a note of the key value, as you need it in the next step. In the preceding example, the key value is 3B789C72.

3. Verify the fingerprint by running the following command, replacing key-value with the value from the preceding step:
Verifying the signature of the CloudWatch agent package

```
shell$ gpg --fingerprint key-value
```

The fingerprint string should be equal to the following:

```
9376 16F3 450B 7D80 6CBD 9725 D581 6730 3B78 9C72
```

If the fingerprint string doesn't match, don't install the agent. Contact Amazon Web Services.

After you have verified the fingerprint, you can use it to verify the signature of the CloudWatch agent package.

4. Download the package signature file using `wget`. To determine the correct signature file, see the preceding table.

```
wget Signature File Link
```

5. To verify the signature, run `gpg --verify`.

```
shell$ gpg --verify signature-filename agent-download-filename
```

If the output includes the phrase `BAD signature`, check whether you performed the procedure correctly. If you continue to get this response, contact Amazon Web Services and avoid using the downloaded file.

Note the warning about trust. A key is trusted only if you or someone who you trust has signed it. This doesn't mean that the signature is invalid, only that you have not verified the public key.

To verify the CloudWatch agent package on a server running Windows Server

1. Download and install GnuPG for Windows from https://gnupg.org/download/. When installing, include the Shell Extension (GpgEx) option.

   You can perform the remaining steps in Windows PowerShell.

2. Download the public key.

   
   ```
   ```

3. Import the public key into your keyring.

   ```
   PS> gpg --import amazon-cloudwatch-agent.gpg
   gpg: key 3B789C72: public key "Amazon CloudWatch Agent" imported
   gpg: Total number processed: 1
   gpg: imported: 1 (RSA: 1)
   ```

   Make a note of the key value because you need it in the next step. In the preceding example, the key value is 3B789C72.
4. Verify the fingerprint by running the following command, replacing `key-value` with the value from the preceding step:

```
PS> gpg --fingerprint key-value
pub   rsa2048 2017-11-14 [SC]
     9376 16F3 450B 7D80 6CBD 9725 D581 6730 3B78 9C72
uid           [ unknown] Amazon CloudWatch Agent
```

The fingerprint string should be equal to the following:

```
9376 16F3 450B 7D80 6CBD 9725 D581 6730 3B78 9C72
```

If the fingerprint string doesn't match, don't install the agent. Contact Amazon Web Services.

After you have verified the fingerprint, you can use it to verify the signature of the CloudWatch agent package.

5. Download the package signature file using `wget`. To determine the correct signature file, see CloudWatch Agent Download Links (p. 430).

6. To verify the signature, run `gpg --verify`.

```
PS> gpg --verify sig-filename agent-download-filename
```

If the output includes the phrase `BAD signature`, check whether you performed the procedure correctly. If you continue to get this response, contact Amazon Web Services and avoid using the downloaded file.

Note the warning about trust. A key is trusted only if you or someone who you trust has signed it. This doesn't mean that the signature is invalid, only that you have not verified the public key.

**To verify the CloudWatch agent package on a macOS computer**

- There are two methods for signature verification on macOS.
  - Verify the fingerprint by running the following command.

```
pkgutil --check-signature amazon-cloudwatch-agent.pkg
```

You should see a result similar to the following.

```
Package "amazon-cloudwatch-agent.pkg":
  Status: signed by a developer certificate issued by Apple for distribution
  Signed with a trusted timestamp on: 2020-10-02 18:13:24 +0000
  Certificate Chain:
  1. Developer ID Installer: AMZN Mobile LLC (94KV3E626L)
     Expires: 2024-10-18 22:31:30 +0000
     SHA256 Fingerprint:
     81 B4 6F AF 1C CA E1 E8 3C 6F FB 9E 52 5E 84 02 6E 7F 17 21 8E FB
     0C 40 79 13 66 8D 9F 1F 10 1C
  2. Developer ID Certification Authority
     Expires: 2027-02-01 22:12:15 +0000
     SHA256 Fingerprint:
```

465
Create the CloudWatch agent configuration file

Before running the CloudWatch agent on any servers, you must create a CloudWatch agent configuration file.

The agent configuration file is a JSON file that specifies the metrics and logs that the agent is to collect, including custom metrics. You can create it by using the wizard or by creating it yourself from scratch. You could also use the wizard to initially create the configuration file and then modify it manually. If you create or modify the file manually, the process is more complex, but you have more control over the metrics collected and can specify metrics not available through the wizard.

Any time you change the agent configuration file, you must then restart the agent to have the changes take effect. To restart the agent, follow the instructions in Start the CloudWatch agent (p. 450).

After you have created a configuration file, you can save it manually as a JSON file and then use this file when installing the agent on your servers. Alternatively, you can store it in Systems Manager Parameter Store if you're going to use Systems Manager when you install the agent on servers.

Contents

• Create the CloudWatch agent configuration file with the wizard (p. 467)
• Manually create or edit the CloudWatch agent configuration file (p. 471)
Create the CloudWatch agent configuration file with the wizard

The agent configuration file wizard, `amazon-cloudwatch-agent-config-wizard`, asks a series of questions, including the following:

- Are you installing the agent on an Amazon EC2 instance or an on-premises server?
- Is the server running Linux or Windows Server?
- Do you want the agent to also send log files to CloudWatch Logs? If so, do you have an existing CloudWatch Logs agent configuration file? If yes, the CloudWatch agent can use this file to determine the logs to collect from the server.
- If you're going to collect metrics from the server, do you want to monitor one of the default sets of metrics or customize the list of metrics that you collect?
- Do you want to collect custom metrics from your applications or services, using StatsD or collectd?
- Are you migrating from an existing SSM Agent?

The wizard can autodetect the credentials and AWS Region to use if you have the AWS credentials and configuration files in place before you start the wizard. For more information about these files, see Configuration and Credential Files in the AWS Systems Manager User Guide.

In the AWS credentials file, the wizard checks for default credentials and also looks for an `AmazonCloudWatchAgent` section such as the following:

```
[AmazonCloudWatchAgent]
aws_access_key_id = my_access_key
aws_secret_access_key = my_secret_key
```

The wizard displays the default credentials, the credentials from the `AmazonCloudWatchAgent`, and an Others option. You can select which credentials to use. If you choose Others, you can input credentials.

For `my_access_key` and `my_secret_key`, use the keys from the IAM user that has the permissions to write to Systems Manager Parameter Store. For more information about the IAM users needed for the CloudWatch agent, see Create IAM users to use with the CloudWatch agent on on-premises servers (p. 445).

In the AWS configuration file, you can specify the Region that the agent sends metrics to if it's different than the `[default]` section. The default is to publish the metrics to the Region where the Amazon EC2 instance is located. If the metrics should be published to a different Region, specify the Region here. In the following example, the metrics are published to the `us-west-1` Region.

```
[AmazonCloudWatchAgent]
region = us-west-1
```

CloudWatch agent predefined metric sets

The wizard is configured with predefined sets of metrics, with different detail levels. These sets of metrics are shown in the following tables. For more information about these metrics, see Metrics collected by the CloudWatch agent (p. 516).

**Note**
Parameter Store supports parameters in Standard and Advanced tiers. These parameter tiers are not related to the Basic, Standard, and Advanced levels of metric details that are described in these tables.

Amazon EC2 instances running Linux
### Basic

<table>
<thead>
<tr>
<th>Metrics included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mem: mem_used_percent</td>
</tr>
<tr>
<td>Disk: disk_used_percent</td>
</tr>
</tbody>
</table>

The disk metrics such as disk_used_percent have a dimension for Partition, which means that the number of custom metrics generated is dependent on the number of partitions associated with your instance. The number of disk partitions you have depends on which AMI you are using and the number of Amazon EBS volumes you attach to the server.

### Standard

<table>
<thead>
<tr>
<th>Metrics included</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU:</strong> cpu_usage_idle, cpu_usage_iowait, cpu_usage_user, cpu_usage_system</td>
</tr>
<tr>
<td>Disk: disk_used_percent, disk_inodes_free</td>
</tr>
<tr>
<td>Diskio: diskio_io_time</td>
</tr>
<tr>
<td>Mem: mem_used_percent</td>
</tr>
<tr>
<td>Swap: swap_used_percent</td>
</tr>
</tbody>
</table>

### Advanced

<table>
<thead>
<tr>
<th>Metrics included</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU:</strong> cpu_usage_idle, cpu_usage_iowait, cpu_usage_user, cpu_usage_system</td>
</tr>
<tr>
<td>Disk: disk_used_percent, disk_inodes_free</td>
</tr>
<tr>
<td>Diskio: diskio_io_time, diskio_write_bytes, diskio_read_bytes, diskio_writes, diskio_reads</td>
</tr>
<tr>
<td>Mem: mem_used_percent</td>
</tr>
<tr>
<td>Netstat: netstat_tcp_established, netstat_tcp_time_wait</td>
</tr>
<tr>
<td>Swap: swap_used_percent</td>
</tr>
</tbody>
</table>

On-premises servers running Linux

<table>
<thead>
<tr>
<th>Metrics included</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic</td>
</tr>
<tr>
<td>Disk: disk_used_percent</td>
</tr>
<tr>
<td>Diskio: diskio_write_bytes, diskio_read_bytes, diskio_writes, diskio_reads</td>
</tr>
<tr>
<td>Mem: mem_used_percent</td>
</tr>
<tr>
<td>Net: net_bytes_sent, net_bytes_recv, net_packets_sent, net_packets_recv</td>
</tr>
<tr>
<td>Swap: swap_used_percent</td>
</tr>
</tbody>
</table>

### Standard

<table>
<thead>
<tr>
<th>Metrics included</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CPU:</strong> cpu_usage_idle, cpu_usage_iowait</td>
</tr>
<tr>
<td>Disk: disk_used_percent, disk_inodes_free</td>
</tr>
<tr>
<td>Diskio: diskio_io_time, diskio_write_bytes, diskio_read_bytes, diskio_writes, diskio_reads</td>
</tr>
</tbody>
</table>
### Create the CloudWatch agent configuration file with the wizard

<table>
<thead>
<tr>
<th>Detail level</th>
<th>Metrics included</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mem:</strong> mem_used_percent</td>
<td></td>
</tr>
<tr>
<td><strong>Net:</strong> net_bytes_sent, net_bytes_recv, net_packets_sent, net_packets_recv</td>
<td></td>
</tr>
<tr>
<td><strong>Swap:</strong> swap_used_percent</td>
<td></td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td></td>
</tr>
<tr>
<td><strong>CPU:</strong> cpu_usage_guest, cpu_usage_idle, cpu_usage_iowait, cpu_usage_steal, cpu_usage_user, cpu_usage_system</td>
<td></td>
</tr>
<tr>
<td><strong>Disk:</strong> disk_used_percent, disk_inodes_free</td>
<td></td>
</tr>
<tr>
<td><strong>Diskio:</strong> diskio_io_time, diskio_write_bytes, diskio_read_bytes, diskio_writes, diskio_reads</td>
<td></td>
</tr>
<tr>
<td><strong>Mem:</strong> mem_used_percent</td>
<td></td>
</tr>
<tr>
<td><strong>Net:</strong> net_bytes_sent, net_bytes_recv, net_packets_sent, net_packets_recv</td>
<td></td>
</tr>
<tr>
<td><strong>Netstat:</strong> netstat_tcp_established, netstat_tcp_time_wait</td>
<td></td>
</tr>
<tr>
<td><strong>Swap:</strong> swap_used_percent</td>
<td></td>
</tr>
</tbody>
</table>

### Amazon EC2 instances running Windows Server

<table>
<thead>
<tr>
<th>Detail level</th>
<th>Metrics included</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Memory:</strong> Memory % Committed Bytes In Use</td>
<td></td>
</tr>
<tr>
<td><strong>LogicalDisk:</strong> LogicalDisk % Free Space</td>
<td></td>
</tr>
<tr>
<td><strong>Standard</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Memory:</strong> Memory % Committed Bytes In Use</td>
<td></td>
</tr>
<tr>
<td><strong>Paging:</strong> Paging File % Usage</td>
<td></td>
</tr>
<tr>
<td><strong>Processor:</strong> Processor % Idle Time, Processor % Interrupt Time, Processor % User Time</td>
<td></td>
</tr>
<tr>
<td><strong>PhysicalDisk:</strong> PhysicalDisk % Disk Time</td>
<td></td>
</tr>
<tr>
<td><strong>LogicalDisk:</strong> LogicalDisk % Free Space</td>
<td></td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Memory:</strong> Memory % Committed Bytes In Use</td>
<td></td>
</tr>
<tr>
<td><strong>Paging:</strong> Paging File % Usage</td>
<td></td>
</tr>
<tr>
<td><strong>Processor:</strong> Processor % Idle Time, Processor % Interrupt Time, Processor % User Time</td>
<td></td>
</tr>
<tr>
<td><strong>LogicalDisk:</strong> LogicalDisk % Free Space</td>
<td></td>
</tr>
<tr>
<td><strong>PhysicalDisk:</strong> PhysicalDisk % Disk Time, PhysicalDisk Disk Write Bytes/sec, PhysicalDisk Disk Read Bytes/sec, PhysicalDisk Disk Writes/sec, PhysicalDisk Disk Reads/sec</td>
<td></td>
</tr>
</tbody>
</table>
Create the CloudWatch agent configuration file with the wizard

<table>
<thead>
<tr>
<th>Detail level</th>
<th>Metrics included</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>TCPv4 Connections Established, TCPv6 Connections Established</td>
</tr>
</tbody>
</table>

### On-premises server running Windows Server

<table>
<thead>
<tr>
<th>Detail level</th>
<th>Metrics included</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Basic</strong></td>
<td><strong>Paging:</strong> Paging File % Usage</td>
</tr>
<tr>
<td></td>
<td><strong>Processor:</strong> Processor % Processor Time</td>
</tr>
<tr>
<td></td>
<td><strong>LogicalDisk:</strong> LogicalDisk % Free Space</td>
</tr>
<tr>
<td></td>
<td><strong>PhysicalDisk:</strong> PhysicalDisk Disk Write Bytes/sec, PhysicalDisk Disk Read Bytes/sec, PhysicalDisk Disk Writes/sec, PhysicalDisk Disk Reads/sec</td>
</tr>
<tr>
<td></td>
<td><strong>Memory:</strong> Memory % Committed Bytes In Use</td>
</tr>
<tr>
<td></td>
<td><strong>Network Interface:</strong> Network Interface Bytes Sent/sec, Network Interface Bytes Received/sec, Network Interface Packets Sent/sec, Network Interface Packets Received/sec</td>
</tr>
<tr>
<td><strong>Standard</strong></td>
<td><strong>Paging:</strong> Paging File % Usage</td>
</tr>
<tr>
<td></td>
<td><strong>Processor:</strong> Processor % Processor Time, Processor % Idle Time, Processor % Interrupt Time</td>
</tr>
<tr>
<td></td>
<td><strong>LogicalDisk:</strong> LogicalDisk % Free Space</td>
</tr>
<tr>
<td></td>
<td><strong>PhysicalDisk:</strong> PhysicalDisk % Disk Time, PhysicalDisk Disk Write Bytes/sec, PhysicalDisk Disk Read Bytes/sec, PhysicalDisk Disk Writes/sec, PhysicalDisk Disk Reads/sec</td>
</tr>
<tr>
<td></td>
<td><strong>Memory:</strong> Memory % Committed Bytes In Use</td>
</tr>
<tr>
<td></td>
<td><strong>Network Interface:</strong> Network Interface Bytes Sent/sec, Network Interface Bytes Received/sec, Network Interface Packets Sent/sec, Network Interface Packets Received/sec</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td><strong>Paging:</strong> Paging File % Usage</td>
</tr>
<tr>
<td></td>
<td><strong>Processor:</strong> Processor % Processor Time, Processor % Idle Time, Processor % Interrupt Time, Processor % User Time</td>
</tr>
<tr>
<td></td>
<td><strong>LogicalDisk:</strong> LogicalDisk % Free Space</td>
</tr>
<tr>
<td></td>
<td><strong>PhysicalDisk:</strong> PhysicalDisk % Disk Time, PhysicalDisk Disk Write Bytes/sec, PhysicalDisk Disk Read Bytes/sec, PhysicalDisk Disk Writes/sec, PhysicalDisk Disk Reads/sec</td>
</tr>
<tr>
<td></td>
<td><strong>Memory:</strong> Memory % Committed Bytes In Use</td>
</tr>
<tr>
<td></td>
<td><strong>Network Interface:</strong> Network Interface Bytes Sent/sec, Network Interface Bytes Received/sec, Network Interface Packets Sent/sec, Network Interface Packets Received/sec</td>
</tr>
</tbody>
</table>
Run the CloudWatch agent configuration wizard

To create the CloudWatch agent configuration file

1. Start the CloudWatch agent configuration wizard by entering the following:

   ```bash
   sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
   ```

   On a server running Windows Server, enter the following:

   ```bash
   cd "C:\Program Files\Amazon\AmazonCloudWatchAgent"
   amazon-cloudwatch-agent-config-wizard.exe
   ```

2. Answer the questions to customize the configuration file for your server.

3. If you're storing the configuration file locally, the configuration file `config.json` is stored in `/opt/aws/amazon-cloudwatch-agent/bin/` on Linux servers, and is stored in `C:\Program Files\Amazon\AmazonCloudWatchAgent` on Windows Server. You can then copy this file to other servers where you want to install the agent.

   If you're going to use Systems Manager to install and configure the agent, be sure to answer Yes when prompted whether to store the file in Systems Manager Parameter Store. You can also choose to store the file in Parameter Store even if you aren't using the SSM Agent to install the CloudWatch agent. To be able to store the file in Parameter Store, you must use an IAM role with sufficient permissions. For more information, see Create IAM roles and users for use with the CloudWatch agent (p. 443).

Manually create or edit the CloudWatch agent configuration file

The CloudWatch agent configuration file is a JSON file with three sections: agent, metrics, and logs.

- The agent section includes fields for the overall configuration of the agent. If you use the wizard, it doesn't create an agent section.
- The metrics section specifies the custom metrics for collection and publishing to CloudWatch. If you're using the agent only to collect logs, you can omit the metrics section from the file.
- The logs section specifies what log files are published to CloudWatch Logs. This can include events from the Windows Event Log if the server runs Windows Server.

The following sections explain the structure and fields of this JSON file. You can also view the schema definition for this configuration file. The schema definition is located at `installation-directory/doc/amazon-cloudwatch-agent-schema.json` on Linux servers, and at `installation-directory/amazon-cloudwatch-agent-schema.json` on servers running Windows Server.

If you create or edit the agent configuration file manually, you can give it any name. For simplicity in troubleshooting, we recommend that you name it `/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json` on a Linux server and `$Env:ProgramData\Amazon`
After you have created the file, you can copy it to other servers where you want to install the agent.

CloudWatch agent configuration file: Agent section

The agent section can include the following fields. The wizard doesn’t create an agent section. Instead, the wizard omits it and uses the default values for all fields in this section.

- **metrics_collection_interval**: Optional. Specifies how often all metrics specified in this configuration file are to be collected. You can override this value for specific types of metrics. This value is specified in seconds. For example, specifying 10 sets metrics to be collected every 10 seconds, and setting it to 300 specifies metrics to be collected every 5 minutes.

  If you set this value below 60 seconds, each metric is collected as a high-resolution metric. For more information about high-resolution metrics, see High-resolution metrics (p. 74).

  The default value is 60.

- **region**: Specifies the Region to use for the CloudWatch endpoint when an Amazon EC2 instance is being monitored. The metrics collected are sent to this Region, such as us-west-1. If you omit this field, the agent sends metrics to the Region where the Amazon EC2 instance is located.

  If you are monitoring an on-premises server, this field isn’t used, and the agent reads the Region from the AmazonCloudWatchAgent profile of the AWS configuration file.

- **credentials**: Specifies an IAM role to use when sending metrics and logs to a different AWS account. If specified, this field contains one parameter, role_arn.

- **role_arn**: Specifies the Amazon Resource Name (ARN) of an IAM role to use for authentication when sending metrics and logs to a different AWS account. For more information, see Sending metrics and logs to a different account (p. 537).

- **debug**: Optional. Specifies running the CloudWatch agent with debug log messages. The default value is false.

- **logfile**: Specifies the location where the CloudWatch agent writes log messages. If you specify an empty string, the log goes to stderr. If you don’t specify this option, the default locations are the following:
  - **Linux**: /opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
  - **Windows Server**: C:\ProgramData\Amazon\CloudWatchAgent\Logs\amazon-cloudwatch-agent.log

  The CloudWatch agent automatically rotates the log file that it creates. A log file is rotated out when it reaches 100 MB in size. The agent keeps the rotated log files for up to seven days, and it keeps as many as five backup log files that have been rotated out. Backup log files have a timestamp appended to their filename. The timestamp shows the date and time that the file was rotated out: for example, amazon-cloudwatch-agent-2018-06-08T21-01-50.247.log.gz.

- **omit_hostname**: Optional. By default, the hostname is published as a dimension of metrics that are collected by the agent, unless you are using the append_dimensions field in the metrics section. Set omit_hostname to true to prevent the hostname from being published as a dimension even if you are not using append_dimensions. The default value is false.

- **run_as_user**: Optional. Specifies a user to use to run the CloudWatch agent. If you don’t specify this parameter, the root user is used. This option is valid only on Linux servers.

  If you specify this option, the user must exist before you start the CloudWatch agent. For more information, see Running the CloudWatch agent as a different user (p. 532).

- **user_agent**: Optional. Specifies the user-agent string that is used by the CloudWatch agent when it makes API calls to the CloudWatch backend. The default value is a string consisting of the agent version, the version of the Go programming language that was used to compile the agent, the runtime operating system and architecture, the build time, and the plugins enabled.
The following is an example of an agent section.

```
"agent": {  
  "metrics_collection_interval": 60,  
  "region": "us-west-1",  
  "debug": false,  
  "run_as_user": "cwagent"  
}
```

**CloudWatch agent configuration file: Metrics section**

On servers running either Linux or Windows Server, the *metrics* section includes the following fields:

- **namespace** – Optional. The namespace to use for the metrics collected by the agent. The default value is *CWAgent*. The maximum length is 255 characters. The following is an example:

```
{
  "metrics": {
      "namespace": "Development/Product1Metrics",
      ......  
  },
}
```

- **append_dimensions** – Optional. Adds Amazon EC2 metric dimensions to all metrics collected by the agent. This also causes the agent to not publish the hostname as a dimension. The only supported key-value pairs for `append_dimensions` are shown in the following list. Any other key-value pairs are ignored.

  - "ImageID":"${aws:ImageId}" sets the instance's AMI ID as the value of the ImageID dimension.
  - "InstanceId":"${aws:InstanceId}" sets the instance's instance ID as the value of the InstanceID dimension.
  - "InstanceType":"${aws:InstanceType}" sets the instance's instance type as the value of the InstanceType dimension.
  - "AutoScalingGroupName":"${aws:AutoScalingGroupName}" sets the instance's Auto Scaling group name as the value of the AutoScalingGroupName dimension.

  If you want to append dimensions to metrics with arbitrary key-value pairs, use the `append_dimensions` parameter in the field for that particular type of metric.

  If you specify a value that depends on Amazon EC2 metadata and you use proxies, you must make sure that the server can access the endpoint for Amazon EC2. For more information about these endpoints, see Amazon Elastic Compute Cloud (Amazon EC2) in the Amazon Web Services General Reference.

- **aggregation_dimensions** – Optional. Specifies the dimensions that collected metrics are to be aggregated on. For example, if you roll up metrics on the AutoScalingGroupName dimension, the metrics from all instances in each Auto Scaling group are aggregated and can be viewed as a whole.

  You can roll up metrics along single or multiple dimensions. For example, specifying `[["InstanceId"], ["InstanceType"], ["InstanceId","InstanceType"]]]` aggregates metrics for instance ID singly, instance type singly, and for the combination of the two dimensions.

  You can also specify `[]` to roll up all metrics into one collection, disregarding all dimensions.

- **endpoint_override** – Specifies a FIPS endpoint or private link to use as the endpoint where the agent sends metrics. Specifying this and setting a private link enables you to send the metrics to an Amazon VPC endpoint. For more information, see What Is Amazon VPC?.

  The value of `endpoint_override` must be a string that is a URL.
Manually create or edit the CloudWatch agent configuration file

For example, the following part of the metrics section of the configuration file sets the agent to use a VPC Endpoint when sending metrics.

```json
{
  "metrics": {
    "endpoint_override": "vpce-XXXXXXXXXXXXXXXXXXXXXXXXX.monitoring.us-east-1.vpce.amazonaws.com",
    ...
  },
}
```

- **metrics_collected** – Required. Specifies which metrics are to be collected, including custom metrics collected through StatsD or collectd. This section includes several subsections.

  The contents of the metrics_collected section depend on whether this configuration file is for a server running Linux or Windows Server.

  - **force_flush_interval** – Specifies in seconds the maximum amount of time that metrics remain in the memory buffer before being sent to the server. No matter the setting for this, if the size of the metrics in the buffer reaches 40 KB or 20 different metrics, the metrics are immediately sent to the server.
    
    The default value is 60.

  - **credentials** – Specifies an IAM role to use when sending metrics to a different account. If specified, this field contains one parameter, role_arn.

    - **role_arn** – Specifies the ARN of an IAM role to use for authentication when sending metrics to a different account. For more information, see Sending metrics and logs to a different account (p. 537). If specified here, this value overrides the role_arn specified in the agent section of the configuration file, if any.

**Linux**

On servers running Linux, the metrics_collected section of the configuration file can also contain the following fields.

Many of these fields can include a measurement sections that lists the metrics you want to collect for that resource. These measurement sections can either specify the complete metric name such as swap_used, or just the part of the metric name that will be appended to the type of resource. For example, specifying reads in the measurement section of the diskio section causes the diskio_reads metric to be collected.

- **collectd** – Optional. Specifies that you want to retrieve custom metrics using the collectd protocol. You use collectd software to send the metrics to the CloudWatch agent. For more information about the configuration options available for collectd, see Retrieve custom metrics with collectd (p. 505).

- **ethtool** – Optional. Specifies that you want to retrieve network metrics using the ethtool plugin. This plugin can import both the metrics collected by the standard ethtool utility, as well as network performance metrics from Amazon EC2 instances. For more information about the configuration options available for ethtool, see Collect network performance metrics (p. 492).

- **cpu** – Optional. Specifies that CPU metrics are to be collected. This section is valid only for Linux instances. You must include at least one of the resources and totalcpu fields for any CPU metrics to be collected. This section can include the following fields:

  - **resources** – Optional. Specify this field with a value of * to cause per-cpu metrics are to be collected. The only allowed value is *.

  - **totalcpu** – Optional. Specifies whether to report cpu metrics aggregated across all cpu cores. The default is true.
• **measurement** – Specifies the array of cpu metrics to be collected. Possible values are:
  - `time_active`
  - `time_guest`
  - `time_guest_nice`
  - `time_idle`
  - `time_iowait`
  - `time_irq`
  - `time_nice`
  - `time_softirq`
  - `time_steal`
  - `time_system`
  - `time_user`
  - `usage_active`
  - `usage_guest`
  - `usage_guest_nice`
  - `usage_idle`
  - `usage_iowait`
  - `usage_irq`
  - `usage_nice`
  - `usage_softirq`
  - `usage_steal`
  - `usage_system`
  - `usage_user`

By default, the unit for `cpu_usage_*` metrics is `Percent`, and `cpu_time_*` metrics don't have a unit.

Within the entry for each individual metric, you might optionally specify one or both of the following:

• **rename** – Specifies a different name for this metric.

• **unit** – Specifies the unit to use for this metric, overriding the default unit for the metric. The unit that you specify must be a valid CloudWatch metric unit, as listed in the `Unit` description in `MetricDatum`.

• **metrics_collection_interval** – Optional. Specifies how often to collect the cpu metrics, overriding the global `metrics_collection_interval` specified in the agent section of the configuration file.

This value is specified in seconds. For example, specifying 10 sets metrics to be collected every 10 seconds, and setting it to 300 specifies metrics to be collected every 5 minutes.

If you set this value below 60 seconds, each metric is collected as a high-resolution metric. For more information about high-resolution metrics, see `High-resolution metrics (p. 74)`.

• **append_dimensions** – Optional. Additional dimensions to use for only the cpu metrics. If you specify this field, it's used in addition to dimensions specified in the global `append_dimensions` field that is used for all types of metrics that the agent collects.

• **disk** – Optional. Specifies that disk metrics are to be collected. This section is valid only for Linux instances. This section can include as many as two fields:

  • **resources** – Optional. Specifies an array of disk mount points. This field limits CloudWatch to collect metrics from only the listed mount points. You can specify `*` as the value to collect metrics from all mount points. The default value is to collect metrics from all mount points.

  • **measurement** – Specifies the array of disk metrics to be collected. Possible values are `free`, `total`, `used`, `used_percent`, `inodes_free`, `inodes_used`, and `inodes_total`. This field is required if you include disk.

  **Note**
  The disk metrics have a dimension for `Partition`, which means that the number of custom metrics generated is dependent on the number of partitions associated with your instance. The number of disk partitions you have depends on which AMI you are using and the number of Amazon EBS volumes you attach to the server.

To see the default units for each disk metric, see `Metrics collected by the CloudWatch agent on Linux and macOS instances (p. 518)`.

Within the entry for each individual metric, you might optionally specify one or both of the following:

• **rename** – Specifies a different name for this metric.

• **unit** – Specifies the unit to use for this metric, overriding the default unit for the metric. The unit that you specify must be a valid CloudWatch metric unit, as listed in the `Unit` description in `MetricDatum`.

• **ignore_file_system_types** – Specifies file system types to exclude when collecting disk metrics. Valid values include `sysfs`, `devtmpfs`, and so on.
• **drop_device** – Setting this to `true` causes `Device` to not be included as a dimension for disk metrics.

Preventing `Device` from being used as a dimension can be useful on instances that use the Nitro system because on those instances the device names change for each disk mount when the instance is rebooted. This can cause inconsistent data in your metrics and cause alarms based on these metrics to go to `INSUFFICIENT_DATA` state.

The default is `false`.

• **metrics_collection_interval** – Optional. Specifies how often to collect the disk metrics, overriding the global `metrics_collection_interval` specified in the agent section of the configuration file.

This value is specified in seconds.

If you set this value below 60 seconds, each metric is collected as a high-resolution metric. For more information, see High-resolution metrics (p. 74).

• **append_dimensions** – Optional. Additional dimensions to use for only the disk metrics. If you specify this field, it is used in addition to dimensions specified in the `append_dimensions` field that is used for all types of metrics collected by the agent.

• **diskio** – Optional. Specifies that disk i/o metrics are to be collected. This section is valid only for Linux instances. This section can include as many as two fields:

  • **resources** – Optional. If you specify an array of devices, CloudWatch collects metrics from only those devices. Otherwise, metrics for all devices are collected. You can also specify `*` as the value to collect metrics from all devices.

  • **measurement** – Specifies the array of diskio metrics to be collected. Possible values are `reads`, `writes`, `read_bytes`, `write_bytes`, `read_time`, `write_time`, `io_time`, and `iops_in_progress`. This field is required if you include `diskio`.

Within the entry for each individual metric, you might optionally specify one or both of the following:

  • **rename** – Specifies a different name for this metric.

  • **unit** – Specifies the unit to use for this metric, overriding the default unit for the metric. The unit that you specify must be a valid CloudWatch metric unit, as listed in the `Unit description` in `MetricDatum`.

• **metrics_collection_interval** – Optional. Specifies how often to collect the diskio metrics, overriding the global `metrics_collection_interval` specified in the agent section of the configuration file.

This value is specified in seconds.

If you set this value below 60 seconds, each metric is collected as a high-resolution metric. For more information about high-resolution metrics, see High-resolution metrics (p. 74).

• **append_dimensions** – Optional. Additional dimensions to use for only the diskio metrics. If you specify this field, it is used in addition to dimensions specified in the `append_dimensions` field that is used for all types of metrics collected by the agent.

• **swap** – Optional. Specifies that swap memory metrics are to be collected. This section is valid only for Linux instances. This section can include as many as three fields:

  • **measurement** – Specifies the array of swap metrics to be collected. Possible values are `free`, `used`, and `used_percent`. This field is required if you include `swap`.

To see the default units for each `swap` metric, see Metrics collected by the CloudWatch agent on Linux and macOS instances (p. 518).
Within the entry for each individual metric, you might optionally specify one or both of the following:

- **rename** – Specifies a different name for this metric.
- **unit** – Specifies the unit to use for this metric, overriding the default unit for the metric. The unit that you specify must be a valid CloudWatch metric unit, as listed in the `Unit description in MetricDatum`.
- **metrics_collection_interval** – Optional. Specifies how often to collect the swap metrics, overriding the global `metrics_collection_interval` specified in the agent section of the configuration file.

This value is specified in seconds.

If you set this value below 60 seconds, each metric is collected as a high-resolution metric. For more information about high-resolution metrics, see [High-resolution metrics](p. 74).

- **append_dimensions** – Optional. Additional dimensions to use for only the swap metrics. If you specify this field, it is used in addition to dimensions specified in the global `append_dimensions` field that is used for all types of metrics collected by the agent. It's collected as a high-resolution metric.
- **mem** – Optional. Specifies that memory metrics are to be collected. This section is valid only for Linux instances. This section can include as many as three fields:
  - **measurement** – Specifies the array of memory metrics to be collected. Possible values are `active`, `available`, `available_percent`, `buffered`, `cached`, `free`, `inactive`, `total`, `used`, and `used_percent`. This field is required if you include `mem`.

To see the default units for each `mem` metric, see [Metrics collected by the CloudWatch agent on Linux and macOS instances](p. 518).

Within the entry for each individual metric, you might optionally specify one or both of the following:

- **rename** – Specifies a different name for this metric.
- **unit** – Specifies the unit to use for this metric, overriding the default unit for the metric. The unit that you specify must be a valid CloudWatch metric unit, as listed in the `Unit description in MetricDatum`.
- **metrics_collection_interval** – Optional. Specifies how often to collect the mem metrics, overriding the global `metrics_collection_interval` specified in the agent section of the configuration file.

This value is specified in seconds.

If you set this value below 60 seconds, each metric is collected as a high-resolution metric. For more information about high-resolution metrics, see [High-resolution metrics](p. 74).

- **append_dimensions** – Optional. Additional dimensions to use for only the mem metrics. If you specify this field, it's used in addition to dimensions specified in the global `append_dimensions` field that is used for all types of metrics that the agent collects.
- **net** – Optional. Specifies that networking metrics are to be collected. This section is valid only for Linux instances. This section can include as many as four fields:
  - **resources** – Optional. If you specify an array of network interfaces, CloudWatch collects metrics from only those interfaces. Otherwise, metrics for all devices are collected. You can also specify `*` as the value to collect metrics from all interfaces.
  - **measurement** – Specifies the array of networking metrics to be collected. Possible values are `bytes_sent`, `bytes_recv`, `drop_in`, `drop_out`, `err_in`, `err_out`, `packets_sent`, and `packets_recv`. This field is required if you include `net`.
Manually create or edit the CloudWatch agent configuration file

To see the default units for each `net` metric, see Metrics collected by the CloudWatch agent on Linux and macOS instances (p. 518).

Within the entry for each individual metric, you might optionally specify one or both of the following:

- **rename** – Specifies a different name for this metric.
- **unit** – Specifies the unit to use for this metric, overriding the default unit for the metric. The unit that you specify must be a valid CloudWatch metric unit, as listed in the `Unit` description in `MetricDatum`.
- **metrics_collection_interval** – Optional. Specifies how often to collect the net metrics, overriding the global `metrics_collection_interval` specified in the agent section of the configuration file.

This value is specified in seconds. For example, specifying 10 sets metrics to be collected every 10 seconds, and setting it to 300 specifies metrics to be collected every 5 minutes.

If you set this value below 60 seconds, each metric is collected as a high-resolution metric. For more information about high-resolution metrics, see High-resolution metrics (p. 74).

- **append_dimensions** – Optional. Additional dimensions to use for only the net metrics. If you specify this field, it's used in addition to dimensions specified in the `append_dimensions` field that is used for all types of metrics collected by the agent.
- **netstat** – Optional. Specifies that TCP connection state and UDP connection metrics are to be collected. This section is valid only for Linux instances. This section can include as many as three fields:
  - **measurement** – Specifies the array of netstat metrics to be collected. Possible values are `tcp_close`, `tcp_close_wait`, `tcp_closing`, `tcp_established`, `tcp_fin_wait1`, `tcp_fin_wait2`, `tcp_last_ack`, `tcp_listen`, `tcp_none`, `tcp_syn_sent`, `tcp_syn_recv`, `tcp_time_wait`, and `udp_socket`. This field is required if you include `netstat`.

To see the default units for each `netstat` metric, see Metrics collected by the CloudWatch agent on Linux and macOS instances (p. 518).

Within the entry for each individual metric, you might optionally specify one or both of the following:

- **rename** – Specifies a different name for this metric.
- **unit** – Specifies the unit to use for this metric, overriding the default unit for the metric. The unit that you specify must be a valid CloudWatch metric unit, as listed in the `Unit` description in `MetricDatum`.
- **metrics_collection_interval** – Optional. Specifies how often to collect the netstat metrics, overriding the global `metrics_collection_interval` specified in the agent section of the configuration file.

This value is specified in seconds.

If you set this value below 60 seconds, each metric is collected as a high-resolution metric. For more information about high-resolution metrics, see High-resolution metrics (p. 74).

- **append_dimensions** – Optional. Additional dimensions to use for only the netstat metrics. If you specify this field, it's used in addition to dimensions specified in the `append_dimensions` field that is used for all types of metrics collected by the agent.
- **processes** – Optional. Specifies that process metrics are to be collected. This section is valid only for Linux instances. This section can include as many as three fields:
  - **measurement** – Specifies the array of processes metrics to be collected. Possible values are `blocked`, `dead`, `idle`, `paging`, `running`, `sleeping`, `stopped`, `total`, `total_threads`, `wait`, and `zombies`. This field is required if you include `processes`.  

478
For all processes metrics, the default unit is Count.

Within the entry for each individual metric, you might optionally specify one or both of the following:

- **rename** – Specifies a different name for this metric.
- **unit** – Specifies the unit to use for this metric, overriding the default unit for the metric. The unit that you specify must be a valid CloudWatch metric unit, as listed in the Unit description in MetricDatum.
- **metrics_collection_interval** – Optional. Specifies how often to collect the processes metrics, overriding the global metrics_collection_interval specified in the agent section of the configuration file.

This value is specified in seconds. For example, specifying 10 sets metrics to be collected every 10 seconds, and setting it to 300 specifies metrics to be collected every 5 minutes.

If you set this value below 60 seconds, each metric is collected as a high-resolution metric. For more information, see High-resolution metrics (p. 74).

- **append_dimensions** – Optional. Additional dimensions to use for only the process metrics. If you specify this field, it’s used in addition to dimensions specified in the append_dimensions field that is used for all types of metrics collected by the agent.

- **procstat** – Optional. Specifies that you want to retrieve metrics from individual processes. For more information about the configuration options available for procstat, see Collect process metrics with the procstat plugin (p. 495).

- **statsd** – Optional. Specifies that you want to retrieve custom metrics using the StatsD protocol. The CloudWatch agent acts as a daemon for the protocol. You use any standard StatsD client to send the metrics to the CloudWatch agent. For more information about the configuration options available for StatsD, see Retrieve custom metrics with StatsD  (p. 503).

- **ethtool** – Optional. Specifies that you want to import ethtool statistics into CloudWatch. For more information, see Collect network performance metrics (p. 492).

The following is an example of a metrics section for a Linux server. In this example, three CPU metrics, three netstat metrics, three process metrics, and one disk metric are collected, and the agent is set up to receive additional metrics from a collectd client.

```
"metrics": {
  "metrics_collected": {
    "collectd": {},
    "cpu": {
      "resources": ["*"]
    },
    "measurement": [
      {
        "name": "cpu_usage_idle", "rename": "CPU_USAGE_IDLE", "unit": "Percent"},
      {
        "name": "cpu_usage_nice", "unit": "Percent"},
      {
        "name": "cpu_usage_guest"
      },
      "totalcpu": false,
      "metrics_collection_interval": 10,
      "append_dimensions": {
        "test": "test1",
        "date": "2017-10-01"
      }
    },
    "netstat": {
      "measurement": [
        "tcp_established",
        "tcp_syn_sent",
```
"tcp_close",
"metrics_collection_interval": 60
},
"disk": {
  "measurement": [
    "used_percent"
  ],
  "resources": [
    "*"
  ],
  "drop_device": true
},
"processes": {
  "measurement": [
    "running",
    "sleeping",
    "dead"
  ]
}
},
"append_dimensions": {
  "ImageId": "${aws:ImageId}",
  "InstanceId": "${aws:InstanceId}",
  "InstanceType": "${aws:InstanceType}",
  "AutoScalingGroupName": "${aws:AutoScalingGroupName}"}
},
"aggregation_dimensions" : [["AutoScalingGroupName"], ["InstanceId", "InstanceType"], []]}

Windows Server

In the metrics_collected section for Windows Server, you can have subsections for each Windows performance object, such as Memory, Processor, and LogicalDisk. For information about what objects and counters are available, see the Microsoft Windows documentation.

Within the subsection for each object, you specify a measurement array of the counters to collect. The measurement array is required for each object that you specify in the configuration file. You can also specify a resources field to name the instances to collect metrics from. You can also specify * for resources to collect separate metrics for every instance. If you omit resources, the data for all instances is aggregated into one set. For objects that don't have instances, omit resources.

Within each object section, you can also specify the following optional fields:

- metrics_collection_interval – Optional. Specifies how often to collect the metrics for this object, overriding the global metrics_collection_interval specified in the agent section of the configuration file.

  This value is specified in seconds. For example, specifying 10 sets metrics to be collected every 10 seconds, and setting it to 300 specifies metrics to be collected every 5 minutes.

  If you set this value below 60 seconds, each metric is collected as a high-resolution metric. For more information, see High-resolution metrics (p. 74).

- append_dimensions – Optional. Specifies additional dimensions to use for only the metrics for this object. If you specify this field, it's used in addition to dimensions specified in the global append_dimensions field that is used for all types of metrics collected by the agent.

Within each counter section, you can also specify the following optional fields:

- rename – Specifies a different name to be used in CloudWatch for this metric.
• **unit** – Specifies the unit to use for this metric. The unit that you specify must be a valid CloudWatch metric unit, as listed in the Unit description in MetricDatum.

There are two other optional sections that you can include in `metrics_collected`:

• **statsd** – Enables you to retrieve custom metrics using the StatsD protocol. The CloudWatch agent acts as a daemon for the protocol. You use any standard StatsD client to send the metrics to the CloudWatch agent. For more information, see Retrieve custom metrics with StatsD (p. 503).

• **procstat** – Enables you to retrieve metrics from individual processes. For more information, see Collect process metrics with the procstat plugin (p. 495).

The following is an example `metrics` section for use on Windows Server. In this example, many Windows metrics are collected, and the computer is also set to receive additional metrics from a StatsD client.

```json
"metrics": {
    "metrics_collected": {
        "statsd": {},
        "Processor": {
            "measurement": [ {
                "name": "% Idle Time", "rename": "CPU_IDLE", "unit": "Percent"},
                "% Interrupt Time",
                "% User Time",
                "% Processor Time"
            },
            "resources": [ 
                "\*"
            ],
            "append_dimensions": {
                "d1": "win_foo",
                "d2": "win_bar"
            }
        },
        "LogicalDisk": {
            "measurement": [ {
                "name": "% Idle Time", "unit": "Percent"},
                {"name": "% Disk Read Time", "rename": "DISK_READ"},
                "% Disk Write Time"
            ],
            "resources": [ 
                "\*"
            ],
            "append_dimensions": {
                "d3": "win_bo"
            }
        },
        "Memory": {
            "metrics_collection_interval": 5,
            "measurement": [ 
                "Available Bytes",
                "Cache Faults/sec",
                "Page Faults/sec",
                "Pages/sec"
            ],
            "append_dimensions": {
                "d3": "win_bo"
            }
        },
        "Network Interface": {
            "metrics_collection_interval": 5,
            "measurement": [ 
                "Bytes Received/sec",
                "Bytes Sent/sec",
                "Packets Received/sec",
                "Packets Sent/sec"
            ],
            "append_dimensions": {
                "d4": "win_net"
            }
        },
        "Process": {
            "measurement": [ 
                "CPU Time"],
            "append_dimensions": {
                "d5": "win_process"
            }
        }
    }
}```
Manually create or edit the CloudWatch agent configuration file

```
"Packets Sent/sec",
"resources": [
  "*"
],
"append_dimensions": {
  "d3": "win_bo"
},
"System": {
  "measurement": [
    "Context Switches/sec",
    "System Calls/sec",
    "Processor Queue Length"
  ],
  "append_dimensions": {
    "d1": "win_foo",
    "d2": "win_bar"
  }
},
"append_dimensions": {
  "ImageId": "${aws:ImageId}"
},
"aggregate_dimensions" : [["ImageId"], ["InstanceId", "InstanceType"], ["d1"],[]]
```

### CloudWatch agent configuration file: Logs section

The logs section includes the following fields:

- **logs_collected** – Required if the logs section is included. Specifies which log files and Windows event logs are to be collected from the server. It can include two fields, `files` and `windows_events`.
- **files** – Specifies which regular log files the CloudWatch agent is to collect. It contains one field, `collect_list`, which further defines these files.
  - **collect_list** – Required if `files` is included. Contains an array of entries, each of which specifies one log file to collect. Each of these entries can include the following fields:
    - **file_path** – Specifies the path of the log file to upload to CloudWatch Logs. Standard Unix glob matching rules are accepted, with the addition of ** as a super asterisk. For example, specifying `/var/log/**.log` causes all `.log` files in the `/var/log` directory tree to be collected. For more examples, see Glob Library.

      You can also use the standard asterisk as a standard wildcard. For example, `/var/log/system.log*` matches files such as `system.log_1111`, `system.log_2222`, and so on in `/var/log`.

      Only the latest file is pushed to CloudWatch Logs based on file modification time. We recommend that you use wildcards to specify a series of files of the same type, such as `access_log.2018-06-01-01` and `access_log.2018-06-01-02`, but not multiple kinds of files, such as `access_log_80` and `access_log_443`. To specify multiple kinds of files, add another log stream entry to the agent configuration file so that each kind of log file goes to a different log stream.

    - **auto_removal** – Optional. If this is true, the CloudWatch agent automatically removes old log files after they are uploaded to CloudWatch Logs. The agent only removes complete files from logs that create multiple files, such as logs that create separate files for each date. If a log continuously writes to a single file, it is not removed.
If you already have a log file rotation or removal method in place, we recommend that you omit this field or set it to `false`.

If you omit this field, the default value of `false` is used.

- **log_group_name** – Optional. Specifies what to use as the log group name in CloudWatch Logs. As part of the name, you can use `{instance_id}`, `{hostname}`, `{local_hostname}`, and `{ip_address}` as variables within the name. `{hostname}` retrieves the hostname from the EC2 metadata, and `{local_hostname}` uses the hostname from the network configuration file.

If you use these variables to create many different log groups, keep in mind the limit of 5000 log groups per account per Region.

Allowed characters include a–z, A–Z, 0–9, '_' (underscore), '-' (hyphen), '/' (forward slash), and '.' (period).

We recommend that you specify this field to prevent confusion. If you omit this field, the file path up to the final dot is used as the log group name. For example, if the file path is `/tmp/TestLogFile.log.2017-07-11-14`, the log group name is `/tmp/TestLogFile.log`.

- **log_stream_name** – Optional. Specifies what to use as the log stream name in CloudWatch Logs. As part of the name, you can use `{instance_id}`, `{hostname}`, `{local_hostname}`, and `{ip_address}` as variables within the name. `{hostname}` retrieves the hostname from the EC2 metadata, and `{local_hostname}` uses the hostname from the network configuration file.

If you omit this field, the value of the `log_stream_name` parameter in the global logs section is used. If that is also omitted, the default value of `{instance_id}` is used.

If a log stream doesn't already exist, it's created automatically.

- **timezone** – Optional. Specifies the time zone to use when putting timestamps on log events. The valid values are `UTC` and `Local`. The default value is `Local`.

This parameter is ignored if you don't specify a value for `timestamp_format`.

- **timestamp_format** – Optional. Specifies the timestamp format, using plaintext and special symbols that start with `%`. If you omit this field, the current time is used. If you use this field, you can use the symbols in the following list as part of the format.

If a single log entry contains two time stamps that match the format, the first time stamp is used.

This list of symbols is different than the list used by the older CloudWatch Logs agent. For a summary of these differences, see [Timestamp differences between the unified CloudWatch agent and the earlier CloudWatch Logs agent](#).

- `%y`
  
  Year without century as a zero-padded decimal number. For example, 19 to represent 2019.

- `%Y`
  
  Year with century as a decimal number. For example, 2019.

- `%b`
  
  Month as the locale's abbreviated name

- `%B`
  
  Month as the locale's full name
%m

Month as a zero-padded decimal number

%-m

Month as a decimal number (not zero-padded)

%d

Day of the month as a zero-padded decimal number

%-d

Day of the month as a decimal number (not zero-padded)

%A

Full name of weekday, such as Monday

%a

Abbreviation of weekday, such as Mon

%H

Hour (in a 24-hour clock) as a zero-padded decimal number

%H

Hour (in a 12-hour clock) as a zero-padded decimal number

%-I

Hour (in a 12-hour clock) as a decimal number (not zero-padded)

%p

AM or PM

%M

Minutes as a zero-padded decimal number

%-M

Minutes as a decimal number (not zero-padded)

%S

Seconds as a zero-padded decimal number

%-S

Seconds as a decimal number (not zero padded)

%f

Fractional seconds as a decimal number (1-9 digits), zero-padded on the left.

%Z

Time zone, for example PST

%z

Time zone, expressed as the offset between the local time zone and UTC. For example, -0700. Only this format is supported. For example, -07:00 isn’t a valid format.
• **multi_line_start_pattern** – Specifies the pattern for identifying the start of a log message. A log message is made of a line that matches the pattern and any subsequent lines that don't match the pattern.

If you omit this field, multi-line mode is disabled, and any line that begins with a non-whitespace character closes the previous log message and starts a new log message.

If you include this field, you can specify `{timestamp_format}` to use the same regular expression as your timestamp format. Otherwise, you can specify a different regular expression for CloudWatch Logs to use to determine the start lines of multi-line entries.

• **encoding** – Specifies the encoding of the log file so that it can be read correctly. If you specify an incorrect coding, there might be data loss because characters that can't be decoded are replaced with other characters.

The default value is `utf-8`. The following are all possible values:

```text
```

• The **windows_events** section specifies the type of Windows events to collect from servers running Windows Server. It includes the following fields:

  • **collect_list** – Required if `windows_events` is included. Specifies the types and levels of Windows events to be collected. Each log to be collected has an entry in this section, which can include the following fields:

    • **event_name** – Specifies the type of Windows events to log. This is equivalent to the Windows event log channel name: for example, `system`, `security`, `application`, and so on. This field is required for each type of Windows event to log.

    **Note**
    When CloudWatch retrieves messages from a Windows log channel, it looks up the log channel based on its Full Name property. Meanwhile, the Windows Event Viewer navigation pane displays the Log Name property of log channels. The Full Name and Log Name do not always match. To confirm the Full Name of a channel, right-click on it in the Windows Event viewer and open Properties.

    • **event_levels** – Specifies the levels of event to log. You must specify each level to log. Possible values include `INFORMATION`, `WARNING`, `ERROR`, `CRITICAL`, and `VERBOSE`. This field is required for each type of Windows event to log.

    • **log_group_name** – Required. Specifies what to use as the log group name in CloudWatch Logs.

    • **log_stream_name** – Optional. Specifies what to use as the log stream name in CloudWatch Logs. As part of the name, you can use `{instance_id}`, `{hostname}`, `{local_hostname}`, and `{ip_address}` as variables within the name. `{hostname}` retrieves the hostname from the EC2 metadata, and `{local_hostname}` uses the hostname from the network configuration file.

      If you omit this field, the value of the log_stream_name parameter in the global logs section is used. If that is also omitted, the default value of `{instance_id}` is used.

      If a log stream doesn't already exist, it's created automatically.

    • **event_format** – Optional. Specifies the format to use when storing Windows events in CloudWatch Logs. `xml` uses the XML format as in Windows Event Viewer. `text` uses the legacy CloudWatch Logs agent format.
• log_stream_name – Required. Specifies the default log stream name to be used for any logs or Windows events that don't have individual log stream names defined in the log_stream_name parameter within their entry in collect_list.

• endpoint_override – Specifies a FIPS endpoint or private link to use as the endpoint where the agent sends logs. Specifying this field and setting a private link enables you to send the logs to an Amazon VPC endpoint. For more information, see What Is Amazon VPC?

The value of endpoint_override must be a string that is a URL.

For example, the following part of the logs section of the configuration file sets the agent to use a VPC Endpoint when sending logs.

```json
{  
  "logs": {  
    "endpoint_override": "vpce-XXXXXXXXXXXXXXXXXXXXXXXXX.logs.us-east-1.vpce.amazonaws.com",
    .......
  },
}
```

• force_flush_interval – Specifies in seconds the maximum amount of time that logs remain in the memory buffer before being sent to the server. No matter the setting for this field, if the size of the logs in the buffer reaches 1 MB, the logs are immediately sent to the server. The default value is 5.

• credentials – Specifies an IAM role to use when sending logs to a different AWS account. If specified, this field contains one parameter, role_arn.

• role_arn – Specifies the ARN of an IAM role to use for authentication when sending logs to a different AWS account. For more information, see Sending metrics and logs to a different account (p. 537). If specified here, this overrides the role_arn specified in the agent section of the configuration file, if any.

• metrics_collected – Specifies that the agent is to collect metrics embedded in logs. Currently, the metrics_collected field can contain only the emf field.

• emf – Specifies that the agent is to collect logs that are in embedded metric format. You can generate metric data from these logs. For more information, see Ingesting high-cardinality logs and generating metrics with CloudWatch embedded metric format (p. 668).

The following is an example of a logs section.

```json
"logs": {
  "logs_collected": {
    "files": {
      "collect_list": [
      {
        "file_path": "c:\ProgramData\Amazon\AmazonCloudWatchAgent\Logs\amazon-cloudwatch-agent.log",
        "log_group_name": "amazon-cloudwatch-agent.log",
        "log_stream_name": "my_log_stream_name_1",
        "timestamp_format": "%H: %M: %S%y%b%-d"
      },
      {
        "file_path": "c:\ProgramData\Amazon\AmazonCloudWatchAgent\Logs\test.log",
        "log_group_name": "test.log",
        "log_stream_name": "my_log_stream_name_2"
      }
    ],
    "windows_events": {
      "collect_list": [
```
How the CloudWatch agent handles sparse log files

Sparse files are files with both empty blocks and real contents. A sparse file uses disk space more efficiently by writing brief information representing the empty blocks to disk instead of the actual null bytes which makes up the block. This makes the actual size of a sparse file usually much smaller than its apparent size.

However, the CloudWatch agent doesn't treat sparse files differently than it treats normal files. When the agent reads a sparse file, the empty blocks are treated as "real" blocks filled with null bytes. Because of this, the CloudWatch agent publishes as many bytes as the apparent size of a sparse file to CloudWatch.

Configuring the CloudWatch agent to publish a sparse file can cause higher than expected CloudWatch costs, so we recommend not to do so. For example, `/var/logs/lastlog` in Linux is usually a very sparse file, and we recommend that you don't publish it to CloudWatch.

CloudWatch agent configuration file: Complete examples

The following is an example of a complete CloudWatch agent configuration file for a Linux server.

The items listed in the measurement sections for the metrics you want to collect can either specify the complete metric name such or just the part of the metric name that will be appended to the type of resource. For example, specifying either `reads` or `diskio_reads` in the measurement section of the `diskio` section will cause the `diskio_reads` metric to be collected.

This example includes both ways of specifying metrics in the measurement section.
Manually create or edit the CloudWatch agent configuration file.

```
{
  "measurement": [
    {
      "name": "cpu_usage_idle", "rename": "CPU_USAGE_IDLE", "unit": "Percent"},
    {
      "name": "cpu_usage_nice", "unit": "Percent"},
    {
      "name": "cpu_usage_guest"
    },
    "totalcpu": false,
    "metrics_collection_interval": 10,
    "append_dimensions": {
      "customized_dimension_key_1": "customized_dimension_value_1",
      "customized_dimension_key_2": "customized_dimension_value_2"
    }
  },
  "disk": {
    "resources": [
      "/",
      "/tmp"
    ],
    "measurement": [
      {
        "name": "free", "rename": "DISK_FREE", "unit": "Gigabytes"},
      "total",
      "used"
    ],
    "ignore_file_system_types": [
      "sysfs", "devtmpfs"
    ],
    "metrics_collection_interval": 60,
    "append_dimensions": {
      "customized_dimension_key_3": "customized_dimension_value_3",
      "customized_dimension_key_4": "customized_dimension_value_4"
    }
  },
  "diskio": {
    "resources": [
      "*"
    ],
    "measurement": [
      "reads",
      "writes",
      "read_time",
      "write_time",
      "io_time"
    ],
    "metrics_collection_interval": 60
  },
  "swap": {
    "measurement": [
      "swap_used",
      "swap_free",
      "swap_used_percent"
    ]
  },
  "mem": {
    "measurement": [
      "mem_used",
      "mem_cached",
      "mem_total"
    ],
    "metrics_collection_interval": 1
  },
  "net": {
    "resources": [
      "eth0"
    ],
    "measurement": [
      "bytes_sent",
      "bytes_recv",
      "packets_sent",
      "packets_recv",
      "errin",
      "errout",
      "dropin",
      "dropout"
    ],
    "metrics_collection_interval": 1
  }
}
```
The following is an example of a complete CloudWatch agent configuration file for a server running Windows Server.

```json
{
    "agent": {
        "metrics_collection_interval": 60,
        "logfile": "C:\ProgramData\Amazon\AmazonCloudWatchAgent\Logs\amazon-cloudwatch-agent.log"
    }
}
```
Manually create or edit the CloudWatch agent configuration file

```
{
"metrics": {
  "namespace": "MyCustomNamespace",
  "metrics_collected": {
    "Processor": {
      "measurement": [
        {"name": "% Idle Time", "rename": "CPU_IDLE", "unit": "Percent"},
        {"name": "% Interrupt Time"},
        {"name": "% User Time"},
        {"name": "% Processor Time"}
      ],
      "resources": ["*"],
      "append_dimensions": {
        "customized_dimension_key_1": "customized_dimension_value_1",
        "customized_dimension_key_2": "customized_dimension_value_2"
      }
    },
    "LogicalDisk": {
      "measurement": [
        {"name": "% Idle Time", "unit": "Percent"},
        {"name": "% Disk Read Time", "rename": "DISK_READ"},
        {"name": "% Disk Write Time"}
      ],
      "resources": ["*"],
      "append_dimensions": {
        "customized_dimension_key_3": "customized_dimension_value_3"
      }
    },
    "customizedObjectName": {
      "metrics_collection_interval": 60,
      "customizedCounterName": [
        "metric1",
        "metric2"
      ],
      "resources": ["customizedInstances"
    },
    "Memory": {
      "metrics_collection_interval": 5,
      "measurement": [
        {"name": "Available Bytes"},
        {"name": "Cache Faults/sec"},
        {"name": "Page Faults/sec"},
        {"name": "Pages/sec"}
      ],
      "resources": ["*"],
      "append_dimensions": {
        "customized_dimension_key_3": "customized_dimension_value_3"
      }
    },
    "System": {
      "measurement": [
        {"name": "Context Switches/sec",
```
Manually create or edit the CloudWatch agent configuration file

```

"System Calls/sec",
"Processor Queue Length"
]
},

"append_dimensions": {
"ImageId": "${aws:ImageId}",
"InstanceId": "${aws:InstanceId}",
"InstanceType": "${aws:InstanceType}",
"AutoScalingGroupName": "${aws:AutoScalingGroupName}"}
},

"aggregation_dimensions": [["ImageId"], ["InstanceId", "InstanceType"], ["di"],[]]
},

"logs": {
"logs_collected": {
"files": {
"collect_list": [
{
"file_path": "c:\ProgramData\Amazon\AmazonCloudWatchAgent\Logs\amazon-cloudwatch-agent.log",
"log_group_name": "amazon-cloudwatch-agent.log",
"timezone": "UTC"
},
{
"file_path": "c:\ProgramData\Amazon\AmazonCloudWatchAgent\Logs\test.log",
"log_group_name": "test.log",
"timezone": "Local"
}
]
},

"windows_events": {
"collect_list": [
{
"event_name": "System",
"event_levels": [
"INFORMATION",
"ERROR"
],
"log_group_name": "System",
"log_stream_name": "System",
"event_format": "xml"
}
],
{
"event_name": "CustomizedName",
"event_levels": [
"WARNING",
"ERROR"
],
"log_group_name": "CustomizedLogGroup",
"log_stream_name": "CustomizedLogStream",
"event_format": "xml"
}
]
},

"log_stream_name": "example_log_stream_name"
}
```

Save the CloudWatch agent configuration file manually

If you create or edit the CloudWatch agent configuration file manually, you can give it any name. For simplicity in troubleshooting, we recommend that you name it /opt/aws/amazon-cloudwatch-
Manually create or edit the CloudWatch agent configuration file

agent/etc/amazon-cloudwatch-agent.json on a Linux server and %Env:ProgramData\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent.json on servers running Windows Server. After you have created the file, you can copy it to other servers where you want to run the agent.

Uploading the CloudWatch agent configuration file to Systems Manager Parameter Store

If you plan to use the SSM Agent to install the CloudWatch agent on servers, after you manually edit the CloudWatch agent configuration file, you can upload it to Systems Manager Parameter Store. To do so, use the Systems Manager put-parameter command.

To be able to store the file in Parameter Store, you must use an IAM role with sufficient permissions. For more information, see Create IAM roles and users for use with the CloudWatch agent (p. 443).

Use the following command, where parameter name is the name to be used for this file in Parameter Store and configuration_file_pathname is the path and file name of the configuration file that you edited.

```
aws ssm put-parameter --name "parameter name" --type "String" --value file://configuration_file_pathname
```

Collect network performance metrics

EC2 instances running on Linux that use the Elastic Network Adapter (ENA) publish network performance metrics. Version 1.246396.0 and later of the CloudWatch agent enable you to import these network performance metrics into CloudWatch. When you import these network performance metrics into CloudWatch, they are charged as CloudWatch custom metrics.

For more information about the ENA driver, see Enabling enhanced networking with the Elastic Network Adapter (ENA) on Linux instances and Enabling enhanced networking with the Elastic Network Adapter (ENA) on Windows instances.

How you set up the collection of network performance metrics differs on Linux servers and Windows servers.

The following table lists these network performance metrics enabled by the ENA adapter. When the CloudWatch agent imports these metrics into CloudWatch from Linux instances, it prepends `ethtool_` at the beginning of each of these metric names.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name on Linux servers: <code>bw_in_allowance_exceeded</code></td>
<td>The number of packets queued and/or dropped because the inbound aggregate bandwidth exceeded the maximum for the instance.</td>
</tr>
<tr>
<td>Name on Windows servers: <code>Aggregate inbound BW allowance exceeded</code></td>
<td>This metric is collected only if you have listed it in the <code>ethtool</code> subsection of the <code>metrics_collected</code> section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492)</td>
</tr>
<tr>
<td>Name on Linux servers: <code>bw_out_allowance_exceeded</code></td>
<td>The number of packets queued and/or dropped because the outbound aggregate bandwidth exceeded the maximum for the instance.</td>
</tr>
</tbody>
</table>
Manually create or edit the CloudWatch agent configuration file

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name on Windows servers: <strong>Aggregate outbound BW allowance exceeded</strong></td>
<td>This metric is collected only if you have listed it in the <code>ethtool</code> subsection of the <code>metrics_collected</code> section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492)</td>
</tr>
<tr>
<td>Name on Linux servers: <code>conntrack_allowance_exceeded</code></td>
<td>The number of packets dropped because connection tracking exceeded the maximum for the instance and new connections could not be established. This can result in packet loss for traffic to or from the instance.</td>
</tr>
<tr>
<td>Name on Windows servers: <strong>Connection tracking allowance exceeded</strong></td>
<td>This metric is collected only if you have listed it in the <code>ethtool</code> subsection of the <code>metrics_collected</code> section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492)</td>
</tr>
<tr>
<td>Name on Linux servers: <strong>linklocal_allowance_exceeded</strong></td>
<td>The number of packets dropped because the PPS of the traffic to local proxy services exceeded the maximum for the network interface. This impacts traffic to the DNS service, the Instance Metadata Service, and the Amazon Time Sync Service.</td>
</tr>
<tr>
<td>Name on Windows servers: <strong>Link local packet rate allowance exceeded</strong></td>
<td>This metric is collected only if you have listed it in the <code>ethtool</code> subsection of the <code>metrics_collected</code> section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492)</td>
</tr>
<tr>
<td>Name on Linux servers: <strong>pps_allowance_exceeded</strong></td>
<td>The number of packets queued and/or dropped because the bidirectional PPS exceeded the maximum for the instance.</td>
</tr>
<tr>
<td>Name on Windows servers: <strong>PPS allowance exceeded</strong></td>
<td>This metric is collected only if you have listed it in the <code>ethtool</code> subsection of the <code>metrics_collected</code> section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492)</td>
</tr>
</tbody>
</table>

**Linux setup**

On Linux servers, the `ethtool plugin` enables you to import the network performance metrics into CloudWatch.

`ethtool` is a standard Linux utility that can collect statistics about Ethernet devices on Linux servers. The statistics it collects depend on the network device and driver. Examples of these statistics include `tx_packets`, `rx_bytes`, `tx_errors`, and `align_errors`. When you use the `ethtool` plugin with the
CloudWatch agent, you can also import these statistics into CloudWatch, along with the EC2 network performance metrics listed earlier in this section.

When the CloudWatch agent imports metrics into CloudWatch, it adds an `ethtool_` prefix to the names of all imported metrics. So the standard ethtool statistic `rx_bytes` is called `ethtool_rx_bytes` in CloudWatch, and the EC2 network performance metric `bw_in_allowance_exceeded` is called `ethtool_bw_in_allowance_exceeded` in CloudWatch.

On Linux servers, to import ethtool metrics, add an `ethtool` section to the `metrics_collected` section of the CloudWatch agent configuration file. The `ethtool` section can include the following subsections:

- **interface_include**— Including this section causes the agent to collect metrics from only the interfaces that have names listed in this section. If you omit this section, metrics are collected from all Ethernet interfaces that aren’t listed in `interface_exclude`.

  The default ethernet interface is `eth0`.

- **interface_exclude**— If you include this section, list the Ethernet interfaces that you don’t want to collect metrics from.

  The `ethtool` plugin always ignores loopback interfaces.

- **metrics_include**— This section lists the metrics to import into CloudWatch. It can include both standard statistics collected by ethtool and Amazon EC2 high-resolution network metrics.

The following example displays part of the CloudWatch agent configuration file. This configuration collects the standard ethtool metrics `rx_packets` and `tx_packets`, and the Amazon EC2 network performance metrics from only the `eth1` interface.

For more information about the CloudWatch agent configuration file, see [Manually create or edit the CloudWatch agent configuration file](p. 471).

```json
"metrics": {
    "append_dimensions": {
        "InstanceId": "${aws:InstanceId}"
    },
    "metrics_collected": {
        "ethtool": {
            "interface_include": ["eth1"],
            "metrics_include": ["rx_packets", "tx_packets", "bw_in_allowance_exceeded", "bw_out_allowance_exceeded", "conntrack_allowance_exceeded", "linklocal_allowance_exceeded", "pps_allowance_exceeded" ]
        }
    }
}
```

**Viewing network performance metrics**

After importing network performance metrics into CloudWatch, you can view these metrics as time series graphs, and create alarms that can watch these metrics and notify you if they breach a threshold that you specify. The following procedure shows how to view ethtool metrics as a time series graph. For more information about setting alarms, see [Using Amazon CloudWatch alarms](p. 102).
Because all of these metrics are aggregate counters, you can use CloudWatch metric math functions such as `RATE(METRICS())` to calculate the rate for these metrics in graphs or use them to set alarms. For more information about metric math functions, see Using metric math (p. 77).

**To view network performance metrics in the CloudWatch console**

2. In the navigation pane, choose **Metrics**.
3. Choose the namespace for the metrics collected by the agent. By default, this is **CWAgent**, but you may have specified a different namespace in the CloudWatch agent configuration file.
4. Choose 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 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.
   b. To sort the table, use the column heading.
   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**.
6. (Optional) To add this graph to a CloudWatch dashboard, choose **Actions**, and then choose **Add to dashboard**.

**Collect process metrics with the procstat plugin**

The **procstat** plugin enables you to collect metrics from individual processes. It is supported on Linux servers and on servers running Windows Server 2012 or later.

**Topics**

- Configuring the CloudWatch agent for procstat (p. 495)
- Metrics collected by procstat (p. 497)
- Viewing process metrics imported by the CloudWatch agent (p. 502)

**Configuring the CloudWatch agent for procstat**

To use the procstat plugin, add a **procstat** section in the **metrics_collected** section of the CloudWatch agent configuration file. There are three ways to specify the processes to monitor. You can use only one of these methods, but you can use that method to specify one or more processes to monitor.

- **pid_file**: Selects processes by the names of the process identification number (PID) files they create.
- **exe**: Selects the processes that have process names that match the string that you specify, using regular expression matching rules. The match is a "contains" match, meaning that if you specify agent as the term to match, processes with names like `cloudwatchagent` match the term. For more information, see **Syntax**.
- **pattern**: Selects processes by the command lines used to start the processes. All processes are selected that have command lines matching the specified string using regular expression matching rules. The entire command line is checked, including parameters and options used with the command.

The match is a "contains" match, meaning that if you specify `-c` as the term to match, processes with parameters like `-config` match the term.
The CloudWatch agent uses only one of these methods, even if you include more than one of the above sections. If you specify more than one section, the CloudWatch agent uses the `pid_file` section if it is present. If not, it uses the `exe` section.

On Linux servers, the strings that you specify in an `exe` or `pattern` section are evaluated as regular expressions. On servers running Windows Server, these strings are evaluated as WMI queries. An example would be pattern: "%apache%". For more information, see LIKE Operator.

Whichever method you use, you can include an optional `metrics_collection_interval` parameter, which specifies how often in seconds to collect those metrics. If you omit this parameter, the default value of 60 seconds is used.

In the examples in the following sections, the `procstat` section is the only section included in the `metrics_collected` section of the agent configuration file. Actual configuration files can also include other sections in `metrics_collected`. For more information, see Manually create or edit the CloudWatch agent configuration file (p. 471).

### Configuring with `pid_file`

The following example `procstat` section monitors the processes that create the PID files `example1.pid` and `example2.pid`. Different metrics are collected from each process. Metrics collected from the process that creates `example2.pid` are collected every 10 seconds, and the metrics collected from the `example1.pid` process are collected every 60 seconds, the default value.

```json
{
    "metrics": {
        "metrics_collected": {
            "procstat": [
                {
                    "pid_file": "/var/run/example1.pid",
                    "measurement": [
                        "cpu_usage",
                        "memory_rss"
                    ]
                },
                {
                    "pid_file": "/var/run/example2.pid",
                    "measurement": [
                        "read_bytes",
                        "read_count",
                        "write_bytes"
                    ],
                    "metrics_collection_interval": 10
                }
            ]
        }
    }
}
```

### Configuring with `exe`

The following example `procstat` section monitors all processes with names that match the strings `agent` or `plugin`. The same metrics are collected from each process.

```json
{
    "metrics": {
        "metrics_collected": {
            "procstat": [
                {
                    "exe": "agent",
                    "measurement": [
                        "cpu_time",
                        "system_time"
                    ]
                }
            ]
        }
    }
}
```
Manually create or edit the CloudWatch agent configuration file

```
{
  "metrics": {
    "metrics_collected": {
      "procstat": [
        {
          "pattern": "config",
          "measurement": ["rlimit_memory_data_hard",
                           "rlimit_memory_data_soft",
                           "rlimit_memory_stack_hard",
                           "rlimit_memory_stack_soft"
                        ]
        },
        {
          "pattern": "-c",
          "measurement": ["rlimit_memory_data_hard",
                           "rlimit_memory_data_soft",
                           "rlimit_memory_stack_hard",
                           "rlimit_memory_stack_soft"
                        ]
        }
      ]
    }
  }
}
```

## Configuring with pattern

The following example `procstat` section monitors all processes with command lines that match the strings `config` or `-c`. The same metrics are collected from each process.

```
{
  "pattern": "config",
  "measurement": ["rlimit_memory_data_hard",
                   "rlimit_memory_data_soft",
                   "rlimit_memory_stack_hard",
                   "rlimit_memory_stack_soft"
                ]
},
{
  "pattern": "-c",
  "measurement": ["rlimit_memory_data_hard",
                   "rlimit_memory_data_soft",
                   "rlimit_memory_stack_hard",
                   "rlimit_memory_stack_soft"
                ]
}
```

## Metrics collected by procstat

The following table lists the metrics that you can collect with the `procstat` plugin.

The CloudWatch agent adds `procstat` to the beginning of the following metric names. There is a different syntax depending on whether it was collected from a Linux server or a server running Windows Server. For example, the `cpu_time` metric appears as `procstat_cpu_time` when collected from Linux and as `procstat cpu_time` when collected from Windows Server.

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Available on</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_time</td>
<td>Linux</td>
<td>The amount of time that the</td>
</tr>
</tbody>
</table>
Manually create or edit the CloudWatch agent configuration file

<table>
<thead>
<tr>
<th>Metric name</th>
<th>Available on</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>process uses the CPU. This metric is measured in hundredths of a second. Unit: Count</td>
</tr>
<tr>
<td>cpu_time_system</td>
<td>Linux, Windows Server, macOS</td>
<td>The amount of time that the process is in system mode. This metric is measured in hundredths of a second. Type: Float Unit: Count</td>
</tr>
<tr>
<td>cpu_time_user</td>
<td>Linux, Windows Server, macOS</td>
<td>The amount of time that the process is in user mode. This metric is measured in hundredths of a second. Unit: Count</td>
</tr>
<tr>
<td>cpu_usage</td>
<td>Linux, Windows Server, macOS</td>
<td>The percentage of time that the process is active in any capacity. Unit: Percent</td>
</tr>
<tr>
<td>memory_data</td>
<td>Linux, macOS</td>
<td>The amount of memory that the process uses for data. Unit: Bytes</td>
</tr>
<tr>
<td>memory_locked</td>
<td>Linux, macOS</td>
<td>The amount of memory that the process has locked. Unit: Bytes</td>
</tr>
<tr>
<td>Metric name</td>
<td>Available on</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>memory_rss</td>
<td>Linux, Windows Server, macOS</td>
<td>The amount of real memory (resident set) that the process is using.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>memory_stack</td>
<td>Linux, macOS</td>
<td>The amount of stack memory that the process is using.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>memory_swap</td>
<td>Linux, macOS</td>
<td>The amount of swap memory that the process is using.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>memory_vms</td>
<td>Linux, Windows Server, macOS</td>
<td>The amount of virtual memory that the process is using.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>pid</td>
<td>Linux, Windows Server, macOS</td>
<td>Process identifier (ID).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>pid_count</td>
<td>Linux, Windows Server, macOS</td>
<td>The number of process IDs associated with the process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On Linux servers and macOS computers the full name of this metric is procstat_lookup_pid_count and on Windows Server it is procstat_lookup_pid_count.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>Metric name</td>
<td>Available on</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>read_bytes</td>
<td>Linux, Windows Server</td>
<td>The number of bytes that the process has read from disks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>write_bytes</td>
<td>Linux, Windows Server</td>
<td>The number of bytes that the process has written to disks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>read_count</td>
<td>Linux, Windows Server</td>
<td>The number of disk read operations that the process has executed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>write_count</td>
<td>Linux, Windows Server</td>
<td>The number of disk write operations that the process has executed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>involuntary_context_switches</td>
<td>Linux</td>
<td>The number of times that the process was involuntarily context-switched.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>voluntary_context_switches</td>
<td>Linux</td>
<td>The number of times that the process was context-switched voluntarily.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>realtime_priority</td>
<td>Linux</td>
<td>The current usage of real-time priority for the process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>Metric name</td>
<td>Available on</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>nice_priority</td>
<td>Linux</td>
<td>The current usage of nice priority for the process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>signals_pending</td>
<td>Linux</td>
<td>The number of signals pending to be handled by the process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>rlimit_cpu_time_hard</td>
<td>Linux</td>
<td>The hard CPU time resource limit for the process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>rlimit_cpu_time_soft</td>
<td>Linux</td>
<td>The soft CPU time resource limit for the process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>rlimit_file_locks_hard</td>
<td>Linux</td>
<td>The hard file locks resource limit for the process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>rlimit_file_locks_soft</td>
<td>Linux</td>
<td>The soft file locks resource limit for the process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>rlimit_memory_data_hard</td>
<td>Linux</td>
<td>The hard resource limit on the process for memory used for data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>rlimit_memory_data_soft</td>
<td>Linux</td>
<td>The soft resource limit on the process for memory used for data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>Metric name</td>
<td>Available on</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>rlimit_memory_locked_hard</td>
<td>Linux</td>
<td>The hard resource limit on the process for locked memory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>rlimit_memory_locked_soft</td>
<td>Linux</td>
<td>The soft resource limit on the process for locked memory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>rlimit_memory_rss_hard</td>
<td>Linux</td>
<td>The hard resource limit on the process for physical memory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>rlimit_memory_rss_soft</td>
<td>Linux</td>
<td>The soft resource limit on the process for physical memory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>rlimit_memory_stack_hard</td>
<td>Linux</td>
<td>The hard resource limit on the process stack.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>rlimit_memory_stack_soft</td>
<td>Linux</td>
<td>The soft resource limit on the process stack.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>rlimit_memory_vms_hard</td>
<td>Linux</td>
<td>The hard resource limit on the process for virtual memory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unit: Bytes</td>
</tr>
</tbody>
</table>

**Viewing process metrics imported by the CloudWatch agent**

After importing process metrics into CloudWatch, you can view these metrics as time series graphs, and create alarms that can watch these metrics and notify you if they breach a threshold that you specify.
The following procedure shows how to view process metrics as a time series graph. For more information about setting alarms, see Using Amazon CloudWatch alarms (p. 102).

**To view process metrics in the CloudWatch console**

2. In the navigation pane, choose Metrics.
3. Choose the namespace for the metrics collected by the agent. By default, this is CWAgent, but you may have specified a different namespace in the CloudWatch agent configuration file.
4. Choose 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 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.
   b. To sort the table, use the column heading.
   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.
6. (Optional) To add this graph to a CloudWatch dashboard, choose Actions, Add to dashboard.

**Retrieve custom metrics with StatsD**

You can retrieve additional custom metrics from your applications or services using the CloudWatch agent with the StatsD protocol. StatsD is a popular open-source solution that can gather metrics from a wide variety of applications. StatsD is especially useful for instrumenting your own metrics. For an example of using the CloudWatch agent and StatsD together, see How to better monitor your custom application metrics using Amazon CloudWatch Agent.

StatsD is supported on both Linux servers and servers running Windows Server. CloudWatch supports the following StatsD format:

```
MetricName:value|type|@sample_rate|#tag1:
value,tag1...
```

- **MetricName** – A string with no colons, bars, # characters, or @ characters.
- **value** – This can be either integer or float.
- **type** – Specify c for counter, g for gauge, ms for timer, h for histogram, or s for set.
- **sample_rate** – (Optional) A float between 0 and 1, inclusive. Use only for counter, histogram, and timer metrics. The default value is 1 (sampling 100% of the time).
- **tags** – (Optional) A comma-separated list of tags. StatsD tags are similar to dimensions in CloudWatch. Use colons for key/value tags, such as env:prod.

You can use any StatsD client that follows this format to send the metrics to the CloudWatch agent. For more information about some of the available StatsD clients, see the StatsD client page on GitHub.

To collect these custom metrics, add a "statsd": {} line to the metrics_collected section of the agent configuration file. You can add this line manually. If you use the wizard to create the configuration file, it's done for you. For more information, see Create the CloudWatch agent configuration file (p. 466).

The StatsD default configuration works for most users. There are three optional fields that you can add to the statsd section of the agent configuration file as needed:
Manually create or edit the CloudWatch agent configuration file

- **service_address** – The service address to which the CloudWatch agent should listen. The format is `ip:port`. If you omit the IP address, the agent listens on all available interfaces. Only the UDP format is supported, so you don't need to specify a UDP prefix.

  The default value is `:8125`.

- **metrics_collection_interval** – How often in seconds that the StatsD plugin runs and collects metrics. The default value is 10 seconds. The range is 1–172,000.

- **metrics_aggregation_interval** – How often in seconds CloudWatch aggregates metrics into single data points. The default value is 60 seconds.

  For example, if `metrics_collection_interval` is 10 and `metrics_aggregation_interval` is 60, CloudWatch collects data every 10 seconds. After each minute, the six data readings from that minute are aggregated into a single data point, which is sent to CloudWatch.

  The range is 0–172,000. Setting `metrics_aggregation_interval` to 0 disables the aggregation of StatsD metrics.

The following is an example of the `statsd` section of the agent configuration file, using the default port and custom collection and aggregation intervals.

```json
{
  "metrics":{
    "metrics_collected":{
      "statsd":{
        "service_address":":8125",
        "metrics_collection_interval":60,
        "metrics_aggregation_interval":300
      }
    }
  }
}
```

**Viewing StatsD metrics imported by the CloudWatch agent**

After importing StatsD metrics into CloudWatch, you can view these metrics as time series graphs, and create alarms that can watch these metrics and notify you if they breach a threshold that you specify. The following procedure shows how to view StatsD metrics as a time series graph. For more information about setting alarms, see Using Amazon CloudWatch alarms (p. 102).

**To view StatsD metrics in the CloudWatch console**

2. In the navigation pane, choose **Metrics**.
3. Choose the namespace for the metrics collected by the agent. By default, this is **CWAgent**, but you may have specified a different namespace in the CloudWatch agent configuration file.
4. Choose 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 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.
   b. To sort the table, use the column heading.
   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**.
6. (Optional) To add this graph to a CloudWatch dashboard, choose **Actions, Add to dashboard**.
Retrieve custom metrics with collectd

You can retrieve additional metrics from your applications or services using the CloudWatch agent with the collectd protocol, which is supported only on Linux servers. Collectd is a popular open-source solution with plugins that can gather system statistics for a wide variety of applications. By combining the system metrics that the CloudWatch agent can already collect with the additional metrics from collectd, you can better monitor, analyze, and troubleshoot your systems and applications. For more information about collectd, see collectd - The system statistics collection daemon.

You use the collectd software to send the metrics to the CloudWatch agent. For the collectd metrics, the CloudWatch agent acts as the server while the collectd plugin acts as the client.

The collectd software is not installed automatically on every server. On a server running Amazon Linux 2, follow these steps to install collectd:

```bash
sudo yum install -y collectd
```

For information about installing collectd on other systems, see the Download page for collectd.

To collect these custom metrics, add a "collectd": {} line to the metrics_collected section of the agent configuration file. You can add this line manually. If you use the wizard to create the configuration file, it is done for you. For more information, see Create the CloudWatch agent configuration file (p. 466).

Optional parameters are also available. If you are using collectd and you do not use /etc/collectd/auth_file as your collectd_auth_file, you must set some of these options.

- **service_address**: The service address to which the CloudWatch agent should listen. The format is "udp://ip:port. The default is udp://127.0.0.1:25826.
- **name_prefix**: A prefix to attach to the beginning of the name of each collectd metric. The default is collectd_. The maximum length is 255 characters.
- **collectd_security_level**: Sets the security level for network communication. The default is encrypt. encrypt specifies that only encrypted data is accepted. sign specifies that only signed and encrypted data is accepted. none specifies that all data is accepted. If you specify a value for collectd_auth_file, encrypted data is decrypted if possible.

For more information, see Client setup and Possible interactions in the collectd Wiki.

- **collectd_auth_file** Sets a file in which user names are mapped to passwords. These passwords are used to verify signatures and to decrypt encrypted network packets. If given, signed data is verified and encrypted packets are decrypted. Otherwise, signed data is accepted without checking the signature and encrypted data cannot be decrypted.

The default is /etc/collectd/auth_file.

If collectd_security_level is set to none, this is optional. If you set collectd_security_level to encrypt or sign, you must specify collectd_auth_file.

For the format of the auth file, each line is a user name followed by a colon and any number of spaces followed by the password. For example:

```plaintext
user1: user1_password
user2: user2_password
```

- **collectd_typesdb**: A list of one or more files that contain the dataset descriptions. The list must be surrounded by brackets, even if there is just one entry in the list. Each entry in the list must be
surrounded by double quotes. If there are multiple entries, separate them with commas. The default on Linux servers is "[/usr/share/collectd/types.db". The default on macOS computers depends on the version of collectd. For example, "[/usr/local/Cellar/collectd/5.12.0/share/collectd/types.db". For more information, see https://collectd.org/documentation/manpages/types.db.5.shtml.

- **metrics_aggregation_interval**: How often in seconds CloudWatch aggregates metrics into single data points. The default is 60 seconds. The range is 0 to 172,000. Setting it to 0 disables the aggregation of collectd metrics.

The following is an example of the collectd section of the agent configuration file.

```json
{
  "metrics":{
    "metrics_collected":{
      "collectd":{
        "name_prefix":"My_collectd_metrics_",
        "metrics_aggregation_interval":120
      }
    }
  }
}
```

**Viewing collectd metrics imported by the CloudWatch agent**

After importing collectd metrics into CloudWatch, you can view these metrics as time series graphs, and create alarms that can watch these metrics and notify you if they breach a threshold that you specify. The following procedure shows how to view collectd metrics as a time series graph. For more information about setting alarms, see Using Amazon CloudWatch alarms (p. 102).

**To view collectd metrics in the CloudWatch console**

2. In the navigation pane, choose **Metrics**.
3. Choose the namespace for the metrics collected by the agent. By default, this is **CWAgent**, but you may have specified a different namespace in the CloudWatch agent configuration file.
4. Choose 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 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.
   b. To sort the table, use the column heading.
   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**.
6. (Optional) To add this graph to a CloudWatch dashboard, choose **Actions, Add to dashboard**.

**Set up and configure Prometheus metrics collection on Amazon EC2 instances**

The following sections explain how to install the CloudWatch agent with Prometheus monitoring on EC2 instances, and how to configure the agent to scrape additional targets. It also provides tutorials for setting up sample workloads to use testing with Prometheus monitoring.
VPC security group requirements

If you are using a VPC, the following requirements apply.

- The ingress rules of the security groups for the Prometheus workloads must open the Prometheus ports to the CloudWatch agent for scraping the Prometheus metrics by the private IP.
- The egress rules of the security group for the CloudWatch agent must allow the CloudWatch agent to connect to the Prometheus workloads' port by private IP.

Topics

- Step 1: Install the CloudWatch agent (p. 507)
- Step 2: Scrape Prometheus sources and import metrics (p. 507)
- Example: Set up Java/JMX sample workloads for Prometheus metric testing (p. 511)

Step 1: Install the CloudWatch agent

The first step is to install the CloudWatch agent on the EC2 instance. For instructions, see Installing the CloudWatch agent (p. 429).

Step 2: Scrape Prometheus sources and import metrics

The CloudWatch agent with Prometheus monitoring needs two configurations to scrape the Prometheus metrics. One is for the standard Prometheus configurations as documented in <scrape_config> in the Prometheus documentation. The other is for the CloudWatch agent configuration.

Prometheus scrape configuration

The CloudWatch agent supports the standard Prometheus scrape configurations as documented in <scrape_config> in the Prometheus documentation. You can edit this section to update the configurations that are already in this file, and add additional Prometheus scraping targets. A sample configuration file contains the following global configuration lines:

```
[global]
scrape_interval: 1m
scrape_timeout: 10s

[scrape_configs]
- job_name: MY_JOB
  sample_limit: 10000
  file_sd_configs:
    - files: ["C:\ProgramData\Amazon\AmazonCloudWatchAgent\prometheus_sd_1.yaml", "C:\ProgramData\Amazon\AmazonCloudWatchAgent\prometheus_sd_2.yaml"]
```

The global section specifies parameters that are valid in all configuration contexts. They also serve as defaults for other configuration sections. It contains the following parameters:

- `scrape_interval`—Defines how frequently to scrape targets.
- `scrape_timeout`—Defines how long to wait before a scrape request times out.

The `scrape_configs` section specifies a set of targets and parameters that define how to scrape them. It contains the following parameters:
• **job_name**— The job name assigned to scraped metrics by default.
• **sample_limit**— Per-scan limit on the number of scraped samples that will be accepted.
• **file_sd_configs**— List of file service discovery configurations. It reads a set of files containing a list of zero or more static configs. The `file_sd_configs` section contains a `files` parameter which defines patterns for files from which target groups are extracted.

The CloudWatch agent supports the following service discovery configuration types.

**static_config** Allows specifying a list of targets and a common label set for them. It is the canonical way to specify static targets in a scan configuration.

The following is a sample static config to scrape Prometheus metrics from a local host. Metrics can also be scraped from other servers if the Prometheus port is open to the server where the agent runs.

```yaml
PS C:\ProgramData\Amazon\AmazonCloudWatchAgent> cat prometheus_sd_1.yaml
- targets:
  - 127.0.0.1:9404
labels:
  key1: value1
  key2: value2
```

This example contains the following parameters:

• **targets**— The targets scraped by the static config.
• **labels**— Labels assigned to all metrics that are scraped from the targets.

**ec2_sd_config** Allows retrieving scrape targets from Amazon EC2 instances. The following is a sample `ec2_sd_config` to scrape Prometheus metrics from a list of EC2 instances. The Prometheus ports of these instances have to be open to the server where the CloudWatch agent runs. The IAM role for the EC2 instance where the CloudWatch agent runs must include the `ec2:DescribeInstances` permission. For example, you could attach the managed policy `AmazonEC2ReadOnlyAccess` to the instance running the CloudWatch agent.

```yaml
PS C:\ProgramData\Amazon\AmazonCloudWatchAgent> cat prometheus.yaml
global:
  scrape_interval: 1m
  scrape_timeout: 10s
scrape_configs:
  - job_name: MY_JOB
    sample_limit: 10000
    ec2_sd_configs:
      - region: us-east-1
        port: 9404
        filters:
          - name: instance-id
            values:
              - i-98765432109876543
              - i-12345678901234567
```

This example contains the following parameters:

• **region**— The AWS Region where the target EC2 instance is. If you leave this blank, the Region from the instance metadata is used.
• **port**— The port to scrape metrics from.
• **filters**— Optional filters to use to filter the instance list. This example filters based on EC2 instance IDs. For more criteria that you can filter on, see [DescribeInstances](#).
CloudWatch agent configuration for Prometheus

The CloudWatch agent configuration file includes prometheus sections under both logs and metrics_collected. It includes the following parameters.

- **cluster_name**— specifies the cluster name to be added as a label in the log event. This field is optional.
- **log_group_name**— specifies the log group name for the scraped Prometheus metrics.
- **prometheus_config_path**— specifies the Prometheus scrape configuration file path.
- **emf_processor**— specifies the embedded metric format processor configuration. For more information about embedded metric format, see Ingesting high-cardinality logs and generating metrics with CloudWatch embedded metric format (p. 668).

The emf_processor section can contain the following parameters:

- **metric_declaration_dedup**— It set to true, the de-duplication function for the embedded metric format metrics is enabled.
- **metric_namespace**— Specifies the metric namespace for the emitted CloudWatch metrics.
- **metric_unit**— Specifies the metric name:metric unit map. For information about supported metrit units, see MetricDatum.
- **metric_declaration**— are sections that specify the array of logs with embedded metric format to be generated. There are metric_declaration sections for each Prometheus source that the CloudWatch agent imports from by default. These sections each include the following fields:
  - **source_labels** specifies the value of the labels that are checked by the label_matcher line.
  - **label_matcher** is a regular expression that checks the value of the labels listed in source_labels. The metrics that match are enabled for inclusion in the embedded metric format sent to CloudWatch.
  - **metric_selectors** is a regular expression that specifies the metrics to be collected and sent to CloudWatch.
  - **dimensions** is the list of labels to be used as CloudWatch dimensions for each selected metric.

The following is an example CloudWatch agent configuration for Prometheus.

```json
{
  "logs":{
    "metrics_collected":{
      "prometheus":{
        "cluster_name":"prometheus-cluster",
        "log_group_name":"Prometheus",
        "prometheus_config_path":"C:\ProgramData\Amazon\AmazonCloudWatchAgent\prometheus.yaml",
        "emf_processor":{
          "metric_declaration_dedup":true,
          "metric_namespace":"CWAgent-Prometheus",
          "metric_unit":{
            "jvm_threads_current": "Count",
            "jvm_gc_collection_seconds_sum": "Milliseconds"
          },
          "metric_declaration":{
            "source_labels":[
              "job", "key2"
            ],
            "label_matcher":"MY_JOB;^value2",
            "dimensions":[
              ["key1", "key2"
            ],
```
Manually create or edit the CloudWatch agent configuration file

The previous example configures an embedded metric format section to be sent as a log event if the following conditions are met:

- The value of the label `job` is `MY_JOB`
- The value of the label `key2` is `value2`
- The Prometheus metrics `jvm_threads_current` and `jvm_gc_collection_seconds_sum` contain both `job` and `key2` labels.

The log event that is sent includes the following highlighted section.

```json
{
    "CloudWatchMetrics": [
        {
            "Metrics": [
                {
                    "Name": "jvm_threads_current",
                    "Unit": "Count"
                },
                {
                    "Name": "jvm_gc_collection_seconds_sum",
                    "Unit": "Milliseconds"
                }
            ],
            "Dimensions": [
                ["key1", "key2"],
                ["key2"]
            ],
            "Namespace": "CWAgent-Prometheus"
        }
    ],
    "ClusterName": "prometheus-cluster",
    "InstanceId": "i-0e45bd06f196096c8",
    "Timestamp": "1607966368109",
    "Version": "0",
    "host": "EC2AMAZ-PDDOIUM",
    "instance": "127.0.0.1:9404",
    "jvm_threads_current": 2,
    "jvm_gc_collection_seconds_sum": 0.006000000000000002,
    "prom_metric_type": "gauge",
    ...
}
```
Example: Set up Java/JMX sample workloads for Prometheus metric testing

JMX Exporter is an official Prometheus exporter that can scrape and expose JMX mBeans as Prometheus metrics. For more information, see prometheus/jmx_exporter.

The CloudWatch agent can collect predefined Prometheus metrics from Java Virtual Machine (JVM), Hjava, and Tomcat (Catalina), from a JMX exporter on EC2 instances.

Step 1: Install the CloudWatch agent

The first step is to install the CloudWatch agent on the EC2 instance. For instructions, see Installing the CloudWatch agent (p. 429).

Step 2: Start the Java/JMX workload

The next step is to start the Java/JMX workload.

First, download the latest JMX exporter jar file from the following location: prometheus/jmx_exporter.

Use the jar for your sample application

The example commands in the following sections use SampleJavaApplication-1.0-SNAPSHOT.jar as the jar file. Replace these parts of the commands with the jar for your application.

Prepare the JMX exporter configuration

The config.yaml file is the JMX exporter configuration file. For more information, see Configuration in the JMX exporter documentation.

Here is a sample configuration for Java and Tomcat.

```yaml
---
lowercaseOutputName: true
lowercaseOutputLabelNames: true

rules:
- pattern: 'java.lang\langle type=OperatingSystem\rangle\{(FreePhysicalMemorySize|TotalPhysicalMemorySize|FreeSwapSpaceSize|TotalSwapSpaceSize|SystemCpuLoad|ProcessCpuLoad|OpenFileDescriptorCount|AvailableProcessors)\}'
  name: java_lang_OperatingSystem_$1
  type: GAUGE

- pattern: 'java.lang\langle type=Threading\rangle\{(TotalStartedThreadCount|ThreadCount)\}'
  name: java_lang_threading_$1
  type: GAUGE

- pattern: 'Catalina\langle type=GlobalRequestProcessor, name="(\w+-\w+)-\d+\"\rangle\{(\w+)\}'
  name: catalina_globalrequestprocessor_$3_total
  labels:
    port: "$2"
    protocol: "$1"
    help: Catalina global $3
  type: COUNTER

- pattern: 'Catalina\langle j2eeType=Servlet, WebModule=/(\-[a-zA-Z0-9-]+&@=\%=\-\/[a-zA-Z0-9-]+&@=\%=\-\/]\)\{requestCount|maxTime|processingTime|errorCount\}'
  name: catalina_servlet_$3_total
  labels:
    module: "$1"
    servlet: "$2"
    help: Catalina servlet $3 total
  type: COUNTER
```
- pattern: 'Catalina<type=ThreadPool, name="(\w+-\w+)-(\d+)">\<\(currentThreadCount|currentThreadsBusy|keepAliveCount|pollerThreadCount|connectionCount\)\>'
  name: catalina_threadpool_\$3
  labels:
    port: "\$2"
    protocol: "\$1"
  help: Catalina threadpool \$3
  type: GAUGE

- pattern: 'Catalina<type=Manager, host=([-a-zA-Z0-9+@#/%?=~_|!:.,;]*[-a-zA-Z0-9+@#/%=~_|]), context=([-a-zA-Z0-9+/%_\-|!\.|\s]*\$2)>\<\(processingTime|sessionCounter|rejectedSessions|expiredSessions\)\>'
  name: catalina_session_\$3_total
  labels:
    context: "\$2"
    host: "\$1"
  help: Catalina session \$3 total
  type: COUNTER

Start the Java application with the Prometheus exporter

Start the sample application. This will emit Prometheus metrics to port 9404. Be sure to replace the entry point `com.gubupt.sample.app.App` with the correct information for your sample Java application.

On Linux, enter the following command.

```
$ nohup java -javaagent:./jmx_prometheus_javaagent-0.14.0.jar=9404:./config.yaml -cp ./SampleJavaApplication-1.0-SNAPSHOT.jar com.gubupt.sample.app.App &
```

On Windows, enter the following command.

```
PS C:\> java -javaagent:./jmx_prometheus_javaagent-0.14.0.jar=9404:./config.yaml -cp ./SampleJavaApplication-1.0-SNAPSHOT.jar com.gubupt.sample.app.App
```

Verify the Prometheus metrics emission

Verify that Prometheus metrics are being emitted.

On Linux, enter the following command.

```
$ curl localhost:9404
```

On Windows, enter the following command.

```
PS C:\> curl http://localhost:9404
```

Sample output on Linux:

```bash
StatusCode : 200
StatusDescription : OK
Content : # HELP jvm_classes_loaded The number of classes that are currently loaded in the JVM
          # TYPE jvm_classes_loaded gauge
          jvm_classes_loaded 2526.0
          # HELP jvm_classes_loaded_total The total number of class...
```
Step 3: Configure the CloudWatch agent to scrape Prometheus metrics

Next, set up the Prometheus scrape configuration in the CloudWatch agent configuration file.

To set up the Prometheus scrape configuration for the Java/JMX example

1. Set up the configuration for `file_sd_config` and `static_config`.

On Linux, enter the following command.

```
$ cat /opt/aws/amazon-cloudwatch-agent/var/prometheus.yaml
```

```
---
# HELP jvm_classes_loaded The number of classes that are currently loaded.

# réglage globale
scrape_interval: 1m
scrape_timeout: 10s
scrape_configs:
  - job_name: jmx
    sample_limit: 10000
    file_sd_configs:
      - files: [ "/opt/aws/amazon-cloudwatch-agent/var/prometheus_file_sd.yaml" ]
```

On Windows, enter the following command.

```
PS C:\ProgramData\Amazon\AmazonCloudWatchAgent> cat prometheus.yaml
```

```
---
# HELP jvm_classes_loaded The number of classes that are currently loaded.

# réglage globale
scrape_interval: 1m
scrape_timeout: 10s
scrape_configs:
  - job_name: jmx
    sample_limit: 10000
    file_sd_configs:
      - files: [ "C:\ProgramData\Amazon\AmazonCloudWatchAgent\prometheus_file_sd.yaml" ]
```

2. Set up the scrape targets configuration.

On Linux, enter the following command.

```
$ cat /opt/aws/amazon-cloudwatch-agent/var/prometheus_file_sd.yaml
```

```
---
targets:
  - 127.0.0.1:9404
labels:
  application: sample_java_app
  os: linux
```

On Windows, enter the following command.

```
PS C:\ProgramData\Amazon\AmazonCloudWatchAgent> cat prometheus_file_sd.yaml
```

```
---
targets:
  - 127.0.0.1:9404
labels:
  application: sample_java_app
  os: linux
```
Manually create or edit the CloudWatch agent configuration file

3. Set up the Prometheus scrape configuration by `ec2_sc_config`. Replace `your-ec2-instance-id` with the correct EC2 instance ID.

On Linux, enter the following command.

```bash
$ cat .prometheus.yaml
```

```
global:
sample_interval: 1m
scrape_timeout: 10s
scrape_configs:
  - job_name: jmx
    sample_limit: 10000
    ec2_sd_configs:
      - region: us-east-1
        port: 9404
        filters:
          - name: instance-id
        values:
          - your-ec2-instance-id
```

On Windows, enter the following command.

```bash
PS C:\ProgramData\Amazon\AmazonCloudWatchAgent> cat prometheus_file_sd.yaml
```

```
- targets:
  - 127.0.0.1:9404
labels:
  application: sample_java_app
  os: windows
```

4. Set up the CloudWatch agent configuration. First, navigate to the correct directory. On Linux, it is `/opt/aws/amazon-cloudwatch-agent/var/cwagent-config.json`. On Windows, it is `C:\ProgramData\Amazon\AmazonCloudWatchAgent\cwagent-config.json`.

The following is a sample configuration with Java/JHX Prometheus metrics defined. Be sure to replace `path-to-Prometheus-Scrape-Configuration-file` with the correct path.

```json
{
  "agent": {
    "region": "us-east-1"
  },
  "logs": {
    "metrics_collected": {
      "prometheus": {
        "cluster_name": "my-cluster",
        "log_group_name": "prometheus-test",
        "prometheus_config_path": "path-to-Prometheus-Scrape-Configuration-file",
        "emf_processor": {
          "metric_declaration_dedup": true,
          "metric_namespace": "PrometheusTest",
          "metric_unit": {
            "jvm_threads_current": "Count",
            "jvm_classes_loaded": "Count",
            "java_lang_operatingsystem_freephysicalmemorysize": "Bytes",
            "catalina_manager_activesessions": "Count",
```

514
5. Restart the CloudWatch agent by entering one of the following commands.

On Linux, enter the following command.

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/var/cwagent-config.json
```

On Windows, enter the following command.

```
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -m ec2 -s -c file:C:\ProgramData\Amazon\AmazonCloudWatchAgent\cwagent-config.json
```

Viewing the Prometheus metrics and logs

You can now view the Java/JMX metrics being collected.
To view the metrics for your sample Java/JMX workload

2. In the Region where your cluster is running, choose Metrics in the left navigation pane. Find the PrometheusTest namespace to see the metrics.
3. To see the CloudWatch Logs events, choose Log groups in the navigation pane. The events are in the log group prometheus-test.

Metrics collected by the CloudWatch agent

You can collect metrics from servers by installing the CloudWatch agent on the server. You can install the agent on both Amazon EC2 instances and on-premises servers, and on computers running either Linux, Windows Server, or macOS. If you install the agent on an Amazon EC2 instance, the metrics it collects are in addition to the metrics enabled by default on Amazon EC2 instances.

For information about installing the CloudWatch agent on an instance, see Collecting metrics and logs from Amazon EC2 instances and on-premises servers with the CloudWatch agent (p. 428).

All metrics discussed in this section are collected directly by the CloudWatch agent.

Metrics collected by the CloudWatch agent on Windows Server instances

On a server running Windows Server, installing the CloudWatch agent enables you to collect the metrics associated with the counters in Windows Performance Monitor. The CloudWatch metric names for these counters are created by putting a space between the object name and the counter name. For example, the % Interrupt Time counter of the Processor object is given the metric name Processor % Interrupt Time in CloudWatch. For more information about Windows Performance Monitor counters, see the Microsoft Windows Server documentation.

The default namespace for metrics collected by the CloudWatch agent is CWAgent, although you can specify a different namespace when you configure the agent.

Advanced network metrics with the Elastic Network Adapter (ENA)

On Windows servers that have the Elastic Network Adapter (ENA) enabled, the CloudWatch agent also collects the following advanced network metrics.

For more information about using the ENA on Windows instances, see Enabling enhanced networking with the Elastic Network Adapter (ENA) on Windows instances.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregate inbound BW allowance exceeded</td>
<td>The number of packets queued and/or dropped because the inbound aggregate bandwidth exceeded the maximum for the instance. This metric is collected only if you have listed it in the ethtool subsection of the metrics_collected section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492)</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Aggregate outbound BW allowance exceeded</td>
<td>The number of packets queued and/or dropped because the outbound aggregate bandwidth exceeded the maximum for the instance..</td>
</tr>
<tr>
<td></td>
<td>This metric is collected only if you have listed it in the ethtool subsection of the metrics_collected section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492)</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td>Connection tracking allowance exceeded</td>
<td>The number of packets dropped because connection tracking exceeded the maximum for the instance and new connections could not be established. This can result in packet loss for traffic to or from the instance.</td>
</tr>
<tr>
<td></td>
<td>This metric is collected only if you have listed it in the ethtool subsection of the metrics_collected section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492)</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td>Link local packet rate allowance exceeded</td>
<td>The number of packets dropped because the PPS of the traffic to local proxy services exceeded the maximum for the network interface. This impacts traffic to the DNS service, the Instance Metadata Service, and the Amazon Time Sync Service.</td>
</tr>
<tr>
<td></td>
<td>This metric is collected only if you have listed it in the ethtool subsection of the metrics_collected section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492)</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td>PPS allowance exceeded</td>
<td>The number of packets queued and/or dropped because the bidirectional PPS exceeded the maximum for the instance.</td>
</tr>
<tr>
<td></td>
<td>This metric is collected only if you have listed it in the ethtool subsection of the metrics_collected section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492)</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
</tbody>
</table>
## Metrics collected by the CloudWatch agent on Linux and macOS instances

The following table lists the metrics that you can collect with the CloudWatch agent on Linux servers and macOS computers.

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>cpu_time_active</code></td>
<td>The amount of time that the CPU is active in any capacity. This metric is measured in hundredths of a second.</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td><code>cpu_time_guest</code></td>
<td>The amount of time that the CPU is running a virtual CPU for a guest operating system. This metric is measured in hundredths of a second.</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td><code>cpu_time_guest_nice</code></td>
<td>The amount of time that the CPU is running a virtual CPU for a guest operating system, which is low-priority and can be interrupted by other processes. This metric is measured in hundredths of a second.</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td><code>cpu_time_idle</code></td>
<td>The amount of time that the CPU is idle. This metric is measured in hundredths of a second.</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td><code>cpu_time_iowait</code></td>
<td>The amount of time that the CPU is waiting for I/O operations to complete. This metric is measured in hundredths of a second.</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td><code>cpu_time_irq</code></td>
<td>The amount of time that the CPU is servicing interrupts. This metric is measured in hundredths of a second.</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td><code>cpu_time_nice</code></td>
<td>The amount of time that the CPU is in user mode with low-priority processes, which can easily be interrupted by higher-priority processes. This metric is measured in hundredths of a second.</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td><code>cpu_time_softirq</code></td>
<td>The amount of time that the CPU is servicing software interrupts. This metric is measured in hundredths of a second.</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td><code>cpu_time_steal</code></td>
<td>The amount of time that the CPU is in stolen time, which is time spent in other operating systems in a small time quantum.</td>
</tr>
</tbody>
</table>
### Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>virtualized environment</td>
<td>This metric is measured in hundredths of a second.</td>
<td>None</td>
</tr>
<tr>
<td>cpu_time_system</td>
<td>The amount of time that the CPU is in system mode. This metric is measured in hundredths of a second.</td>
<td>None</td>
</tr>
<tr>
<td>cpu_time_user</td>
<td>The amount of time that the CPU is in user mode. This metric is measured in hundredths of a second.</td>
<td>None</td>
</tr>
<tr>
<td>cpu_usage_active</td>
<td>The percentage of time that the CPU is active in any capacity.</td>
<td>Percent</td>
</tr>
<tr>
<td>cpu_usage_guest</td>
<td>The percentage of time that the CPU is running a virtual CPU for a guest operating system.</td>
<td>Percent</td>
</tr>
<tr>
<td>cpu_usage_guest_nice</td>
<td>The percentage of time that the CPU is running a virtual CPU for a guest operating system, which is low-priority and can be interrupted by other processes.</td>
<td>Percent</td>
</tr>
<tr>
<td>cpu_usage_idle</td>
<td>The percentage of time that the CPU is idle.</td>
<td>Percent</td>
</tr>
<tr>
<td>cpu_usage_iowait</td>
<td>The percentage of time that the CPU is waiting for I/O operations to complete.</td>
<td>Percent</td>
</tr>
<tr>
<td>cpu_usage_irq</td>
<td>The percentage of time that the CPU is servicing interrupts.</td>
<td>Percent</td>
</tr>
<tr>
<td>cpu_usage_nice</td>
<td>The percentage of time that the CPU is in user mode with low-priority processes, which higher-priority processes can easily interrupt.</td>
<td>Percent</td>
</tr>
<tr>
<td>cpu_usage_softirq</td>
<td>The percentage of time that the CPU is servicing software interrupts.</td>
<td>Percent</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>cpu_usage_steal</td>
<td>The percentage of time that the CPU is in stolen time, or time spent in other operating systems in a virtualized environment. Unit: Percent</td>
<td></td>
</tr>
<tr>
<td>cpu_usage_system</td>
<td>The percentage of time that the CPU is in system mode. Unit: Percent</td>
<td></td>
</tr>
<tr>
<td>cpu_usage_user</td>
<td>The percentage of time that the CPU is in user mode. Unit: Percent</td>
<td></td>
</tr>
<tr>
<td>disk_free</td>
<td>Free space on the disks. Unit: Bytes</td>
<td></td>
</tr>
<tr>
<td>disk_inodes_free</td>
<td>The number of available index nodes on the disk. Unit: Count</td>
<td></td>
</tr>
<tr>
<td>disk_inodes_total</td>
<td>The total number of index nodes reserved on the disk. Unit: Count</td>
<td></td>
</tr>
<tr>
<td>disk_inodes_used</td>
<td>The number of used index nodes on the disk. Unit: Count</td>
<td></td>
</tr>
<tr>
<td>disk_total</td>
<td>Total space on the disks, including used and free. Unit: Bytes</td>
<td></td>
</tr>
<tr>
<td>disk_used</td>
<td>Used space on the disks. Unit: Bytes</td>
<td></td>
</tr>
<tr>
<td>disk_used_percent</td>
<td>The percentage of total disk space that is used. Unit: Percent</td>
<td></td>
</tr>
<tr>
<td>diskio_iops_in_progress</td>
<td>The number of I/O requests that have been issued to the device driver but have not yet completed. Unit: Count</td>
<td></td>
</tr>
<tr>
<td>diskio_io_time</td>
<td>The amount of time that the disk has had I/O requests queued. Unit: Milliseconds The only statistic that should be used for this metric is Sum. Do not use Average.</td>
<td></td>
</tr>
</tbody>
</table>
### Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>diskio_reads</code></td>
<td>The number of disk read operations.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td><code>diskio_read_bytes</code></td>
<td>The number of bytes read from the disks.</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td><code>diskio_read_time</code></td>
<td>The amount of time that read requests have waited on the disks. Multiple read requests waiting at the same time increase the number. For example, if 5 requests all wait for an average of 100 milliseconds, 500 is reported.</td>
</tr>
<tr>
<td></td>
<td>Unit: Milliseconds</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td><code>diskio_writes</code></td>
<td>The number disk write operations.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td><code>diskio_write_bytes</code></td>
<td>The number of bytes written to the disks.</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td><code>diskio_write_time</code></td>
<td>The amount of time that write requests have waited on the disks. Multiple write requests waiting at the same time increase the number. For example, if 8 requests all wait for an average of 1000 milliseconds, 8000 is reported.</td>
</tr>
<tr>
<td></td>
<td>Unit: Milliseconds</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>ethtool_bw_in_allowance_exceeded</code></td>
<td>The number of packets queued and/or dropped because the inbound aggregate bandwidth exceeded the maximum for the instance. This metric is collected only if you have listed it in the <code>ethtool</code> subsection of the <code>metrics_collected</code> section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492). Unit: None</td>
</tr>
<tr>
<td><code>ethtool_bw_out_allowance_exceeded</code></td>
<td>The number of packets queued and/or dropped because the outbound aggregate bandwidth exceeded the maximum for the instance. This metric is collected only if you have listed it in the <code>ethtool</code> subsection of the <code>metrics_collected</code> section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492). Unit: None</td>
</tr>
<tr>
<td><code>ethtool_conntrack_allowance_exceeded</code></td>
<td>The number of packets dropped because connection tracking exceeded the maximum for the instance and new connections could not be established. This can result in packet loss for traffic to or from the instance. This metric is collected only if you have listed it in the <code>ethtool</code> subsection of the <code>metrics_collected</code> section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492). Unit: None</td>
</tr>
<tr>
<td><code>ethtool_linklocal_allowance_exceeded</code></td>
<td>The number of packets dropped because the PPS of the traffic to local proxy services exceeded the maximum for the network interface. This impacts traffic to the DNS service, the Instance Metadata Service, and the Amazon Time Sync Service. This metric is collected only if you have listed it in the <code>ethtool</code> subsection of the <code>metrics_collected</code> section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492). Unit: None</td>
</tr>
<tr>
<td>Metric</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ethtool_pps_allowance_exceeded</td>
<td>The number of packets queued and/or dropped because the bidirectional PPS exceeded the maximum for the instance.</td>
</tr>
<tr>
<td></td>
<td>This metric is collected only if you have listed it in the ethtool subsection of the metrics_collected section of the CloudWatch agent configuration file. For more information, see Collect network performance metrics (p. 492).</td>
</tr>
<tr>
<td></td>
<td>Unit: None</td>
</tr>
<tr>
<td>mem_active</td>
<td>The amount of memory that has been used in some way during the last sample period.</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>mem_available</td>
<td>The amount of memory that is available and can be given instantly to processes.</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>mem_available_percent</td>
<td>The percentage of memory that is available and can be given instantly to processes.</td>
</tr>
<tr>
<td></td>
<td>Unit: Percent</td>
</tr>
<tr>
<td>mem_buffered</td>
<td>The amount of memory that is being used for buffers.</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>mem_cached</td>
<td>The amount of memory that is being used for file caches.</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>mem_free</td>
<td>The amount of memory that isn't being used.</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>mem_inactive</td>
<td>The amount of memory that hasn't been used in some way during the last sample period</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>mem_total</td>
<td>The total amount of memory.</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>mem_used</td>
<td>The amount of memory currently in use.</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td>mem_used_percent</td>
<td>The percentage of memory currently in use.</td>
</tr>
<tr>
<td></td>
<td>Unit: Percent</td>
</tr>
</tbody>
</table>
## Metrics collected by the CloudWatch agent on Linux and macOS instances

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>net_bytes_recv</td>
<td>The number of bytes received by the network interface.</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td>net_bytes_sent</td>
<td>The number of bytes sent by the network interface.</td>
</tr>
<tr>
<td></td>
<td>Unit: Bytes</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td>net_drop_in</td>
<td>The number of packets received by this network interface that were dropped.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td>net_drop_out</td>
<td>The number of packets transmitted by this network interface that were dropped.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td>net_err_in</td>
<td>The number of receive errors detected by this network interface.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td>net_err_out</td>
<td>The number of transmit errors detected by this network interface.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td>net_packets_sent</td>
<td>The number of packets sent by this network interface.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
</tbody>
</table>
### Metrics collected by the CloudWatch agent on Linux and macOS instances

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>net_packets_recv</td>
<td>The number of packets received by this network interface.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td></td>
<td>The only statistic that should be used for this metric is Sum. Do not use Average.</td>
</tr>
<tr>
<td>netstat_tcp_close</td>
<td>The number of TCP connections with no state.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>netstat_tcp_close_wait</td>
<td>The number of TCP connections waiting for a termination request from the client.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>netstat_tcp_closing</td>
<td>The number of TCP connections that are waiting for a termination request with acknowledgement from the client.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>netstat_tcp_established</td>
<td>The number of TCP connections established.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>netstat_tcp_fin_wait1</td>
<td>The number of TCP connections in the FIN_WAIT1 state during the process of closing a connection.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>netstat_tcp_fin_wait2</td>
<td>The number of TCP connections in the FIN_WAIT2 state during the process of closing a connection.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>netstat_tcp_last_ack</td>
<td>The number of TCP connections waiting for the client to send acknowledgement of the connection termination message. This is the last state right before the connection is closed down.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>netstat_tcp_listen</td>
<td>The number of TCP ports currently listening for a connection request.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>netstat_tcp_none</td>
<td>The number of TCP connections with inactive clients.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
<tr>
<td>netstat_tcp_syn_sent</td>
<td>The number of TCP connections waiting for a matching connection request after having sent a connection request.</td>
</tr>
<tr>
<td></td>
<td>Unit: Count</td>
</tr>
</tbody>
</table>
## Metrics collected by the CloudWatch agent on Linux and macOS instances

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
<th>Unit</th>
</tr>
</thead>
<tbody>
<tr>
<td>netstat_tcp_syn_recv</td>
<td>The number of TCP connections waiting for connection request acknowledgement after having sent and received a connection request.</td>
<td>Count</td>
</tr>
<tr>
<td>netstat_tcp_time_wait</td>
<td>The number of TCP connections currently waiting to ensure that the client received the acknowledgement of its connection termination request.</td>
<td>Count</td>
</tr>
<tr>
<td>netstat_udp_socket</td>
<td>The number of current UDP connections.</td>
<td>Count</td>
</tr>
<tr>
<td>processes_blocked</td>
<td>The number of processes that are blocked.</td>
<td>Count</td>
</tr>
<tr>
<td>processes_dead</td>
<td>The number of processes that are dead, indicated by the X state code on Linux.</td>
<td>Count</td>
</tr>
<tr>
<td></td>
<td>This metric is not collected on macOS computers.</td>
<td></td>
</tr>
<tr>
<td>processes_idle</td>
<td>The number of processes that are idle (sleeping for more than 20 seconds). Available only on FreeBSD instances.</td>
<td>Count</td>
</tr>
<tr>
<td>processes_paging</td>
<td>The number of processes that are paging, indicated by the W state code on Linux.</td>
<td>Count</td>
</tr>
<tr>
<td></td>
<td>This metric is not collected on macOS computers.</td>
<td></td>
</tr>
<tr>
<td>processes_running</td>
<td>The number of processes that are running, indicated by the R state code.</td>
<td>Count</td>
</tr>
<tr>
<td>processes_sleeping</td>
<td>The number of processes that are sleeping, indicated by the S state code.</td>
<td>Count</td>
</tr>
<tr>
<td>processes_stopped</td>
<td>The number of processes that are stopped, indicated by the T state code.</td>
<td>Count</td>
</tr>
<tr>
<td>processes_total</td>
<td>The total number of processes on the instance.</td>
<td>Count</td>
</tr>
</tbody>
</table>
### Metric Description

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>processes_total_threads</td>
<td>The total number of threads making up the processes. This metric is available only on Linux instances. This metric is not collected on macOS computers. Unit: Count</td>
</tr>
<tr>
<td>processes_wait</td>
<td>The number of processes that are paging, indicated by the W state code on FreeBSD instances. This metric is available only on FreeBSD instances, and is not available on Linux, Windows Server, or macOS instances. Unit: Count</td>
</tr>
<tr>
<td>processes_zombies</td>
<td>The number of zombie processes, indicated by the Z state code. Unit: Count</td>
</tr>
<tr>
<td>swap_free</td>
<td>The amount of swap space that isn’t being used. Unit: Bytes</td>
</tr>
<tr>
<td>swap_used</td>
<td>The amount of swap space currently in use. Unit: Bytes</td>
</tr>
<tr>
<td>swap_used_percent</td>
<td>The percentage of swap space currently in use. Unit: Percent</td>
</tr>
</tbody>
</table>

---

### OpenTelemetry support in the CloudWatch agent

Versions 1.247347.3 and later of the CloudWatch agent have an embedded AWS OpenTelemetry Collector. This enables the CloudWatch agent to integrate with AWS OpenTelemetry APIs and SDKs, and send application telemetry data from EC2 instances to CloudWatch and AWS X-Ray. This feature is intended for existing CloudWatch agent users who want to begin monitoring with OpenTelemetry without installing or configuring multiple agents. For more information about AWS OpenTelemetry, see [AWS Distro for OpenTelemetry](https://aws.amazon.com/distro-for-opentelemetry/).

By using the CloudWatch agent with the embedded AWS OpenTelemetry Collector, you don’t have to install a separate AWS OpenTelemetry Collector.
The CloudWatch agent with the embedded OpenTelemetry Collector can receive metrics and traces from the AWS OpenTelemetry SDK, and publish them to CloudWatch and X-Ray. The OpenTelemetry Collector that is embedded in the CloudWatch agent has the same behavior as the AWS OpenTelemetry Collector, and using it means that you don’t need to install the separate AWS OpenTelemetry Collector. But if you do install both on the same server, be aware that the embedded OpenTelemetry Collector in the CloudWatch agent and the AWS OpenTelemetry Collector are located in different directories, managed through different tools, and run as separate processes. For example, if you configure and run both processes in the same server, be sure that the local ports that they use to listen do not conflict with each other.

OpenTelemetry in the CloudWatch agent is supported for the CloudWatch agent running on EC2 instances, but not for the CloudWatch agent running in containers or on on-premises servers. Both x86-64 and ARM64 architectures are supported on Linux instances, and x86-64 is supported on Windows Server instances.

**IAM permissions**

To be able to publish OpenTelemetry metrics and traces, the CloudWatch agent needs extra IAM permissions in addition to those permissions listed in the `CloudWatchAgentServerPolicy` managed policy. On servers where you want to use the agent's OpenTelemetry support, grant the following policy to the CloudWatch agent's IAM role that is attached to the instance. If you used the default suggested name in the documentation, then this role is called `CloudWatchAgentServerRole`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "xray:PutTraceSegments",
        "xray:PutTelemetryRecords",
        "xray:GetSamplingRules",
        "xray:GetSamplingTargets",
        "xray:GetSamplingStatisticSummaries",
        "ssm:GetParameters"
      ],
      "Resource": "*"
    }
  ]
}
```
CloudWatch agent OpenTelemetry configuration

Amazon provides a default configuration file for the embedded OpenTelemetry Collector. This configuration enables collecting OpenTelemetry metrics and traces through a default port. If the default configuration works for you, you don't need to do any more configuration steps. To see the the contents of this default configuration files, see config.yaml on Github.

If you want to customize the configuration file, see the AWS Distro for OpenTelemetry documentation. If you do this, once you have made the custom configuration file, you can either upload it to Parameter Store or copy it to the file system of every server where you want to use it. For more information about uploading it to Parameter Store, see Uploading the CloudWatch agent configuration file to Systems Manager Parameter Store (p. 492).

Use the command line to manage the CloudWatch agent with OpenTelemetry support

The CloudWatch agent with embedded OpenTelemetry support runs as two processes: the CloudWatch agent process and the OpenTelemetry Collector process. When you start the CloudWatch agent, each process determines separately whether it can start successfully.

You can run the amazon-cloudwatch-agent-ctl script to managed the OpenTelemetry Collector process. To configure and start the embedded OpenTelemetry Collector, run one of the the following commands:

Linux:

```bash
sudo /usr/bin/amazon-cloudwatch-agent-ctl -a fetch-config -o configuration-file -s
```

Windows Server:

```powershell
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a fetch-config -o configuration-file -s
```

In this command, -a fetch-config loads the configuration for the OpenTelemetry Collector. The configuration can be the default configuration or a custom configuration from either Parameter Store or a local file. The -s parameter restarts the agent with this configuration.

The value of configuration-file can be default to use the default built-in configuration. To use a customized configuration in Parameter Store, you specify ssm:your-configuration-parameter-name. If you store the configuration in a local file instead, specify it as file:your-configuration-file.yaml.

For example, the following configures and starts the agent's OpenTelemetry process with the default built-in configuration for the OpenTelemetry Collector.

```bash
sudo /usr/bin/amazon-cloudwatch-agent-ctl -a fetch-config -o default -s
```

Important
Use the -o option to configure the agent's OpenTelemetry Collector process, and use the -c option when you are configuring the CloudWatch agent process. The following command is an example that starts both the embedded OpenTelemetry Collector and the CloudWatch agent in Linux with each's default built-in configuration:
Use the command line to manage the CloudWatch agent with OpenTelemetry support

```bash
sudo /usr/bin/amazon-cloudwatch-agent-ctl -a fetch-config -o default -c default -s
```

**Use the command line to stop and start the OpenTelemetry Collector in the CloudWatch agent**

**Stop only the OpenTelemetry Collector process**

To stop the OpenTelemetry process in the agent but let the CloudWatch agent process keep running, you use commands to tell the agent to remove the OpenTelemetry configuration, and then restart the agent with no configuration for the OpenTelemetry Collector.

In the following command, `-a remove-config -o` tells the CloudWatch agent to remove the configuration file for the OpenTelemetry Collector, and `-s` restarts the OpenTelemetry Collector without using any configuration, which effectively stops it.

**Linux:**

```bash
sudo /usr/bin/amazon-cloudwatch-agent-ctl -a remove-config -o configuration-file -s
```

**Windows Server:**

```bash
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a remove-config -o configuration-file -s
```

In this command, for `configuration-file` you can specify `all` to remove whatever configuration was currently applied. For example, the following command removes the configuration and stops the embedded OpenTelemetry Collector in Linux:

```bash
sudo /usr/bin/amazon-cloudwatch-agent-ctl -a remove-config -o all -s
```

**Stop both agent processes**

You can use the `-a stop` parameter to stop both the embedded OpenTelemetry Collector process and the CloudWatch agent process if they are running.

**Linux:**

```bash
sudo /usr/bin/amazon-cloudwatch-agent-ctl -a stop
```

**Windows Server:**

```bash
& "C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1" -a stop
```

**Start both agent processes**

You can use the `-a start` parameter to start both the embedded OpenTelemetry Collector process and the CloudWatch agent process if they have already been configured. If you have never configured the OpenTelemetry Collector, using this parameter will not start it. If you have never started the CloudWatch agent process before, this command will start it with the default configuration.

**Linux:**

```bash
sudo /usr/bin/amazon-cloudwatch-agent-ctl -a start
```
Use Systems Manager to manage the CloudWatch agent with the embedded OpenTelemetry Collector

You can also use Systems Manager to manage the CloudWatch agent with the OpenTelemetry Collector.

To configure and start the CloudWatch agent using Run Command

2. In the navigation pane, choose Run Command.
   -or-
   If the AWS Systems Manager home page opens, scroll down and choose Explore Run Command.
3. Choose Run command.
4. In the Command document list, choose AmazonCloudWatch-ManageAgent.
5. In the Targets area, choose the instance where you installed the CloudWatch agent.
6. In the Action list, choose configure.
7. In the Optional OpenTelemetry Configuration Source list, choose ssm if you want to use your custom configuration, or choose default to use the default configuration.
8. In the Optional OpenTelemetry Configuration Location box, enter the name of the OpenTelemetry configuration parameter that you created and saved to Systems Manager Parameter Store, as explained in the previous sections.
9. (Optional) If you want to configure and start the CloudWatch agent process at the same time, do the following:
   a. In the Optional Configuration Source list, choose ssm if you want to use your custom configuration, or choose default to use the default configuration.
   b. In the Optional Configuration Location box, enter the name of the CloudWatch agent configuration parameter that you created and saved to Systems Manager Parameter Store.
10. In the Optional Restart list, choose yes to start the agent after you have finished these steps.
12. Optionally, in the Targets and outputs areas, select the button next to an instance name and choose View output. Systems Manager should show that the agent was successfully started.

To remove the configuration and stop the OpenTelemetry Collector process

2. In the navigation pane, choose Run Command.
   -or-
   If the AWS Systems Manager home page opens, scroll down and choose Explore Run Command.
3. Choose Run command.
4. In the Command document list, choose AmazonCloudWatch-ManageAgent.
5. In the Targets area, choose the instance where you installed the CloudWatch agent.
6. In the Action list, choose configure (remove).
7. In the **Optional OpenTelemetry Configuration Source** list, choose **all**.
8. In the **Optional Restart** list, choose **yes** to start the agent after you have finished these steps.
9. Choose **Run**.
10. Optionally, in the **Targets and outputs** areas, select the button next to an instance name and choose **View output**. Systems Manager should show that the agent was successfully started.

### Generating OpenTelemetry metrics and traces

AWS provides OpenTelemetry SDKs and a Java auto instrumentation agent for your applications to use to generate OpenTelemetry metrics and traces and feed them to an OpenTelemetry Collector. For more information, see the following:

- Getting Started with the Java SDK on Traces and Metrics Instrumentation
- Tracing with the AWS Distro for OpenTelemetry Go SDK
- Getting Started with the Python SDK
- Getting Started with the JavaScript SDK on Traces and Metrics Instrumentation

### Common scenarios with the CloudWatch agent

The following sections outline how to complete some common configuration and customization tasks when using the CloudWatch agent.

**Topics**

- Running the CloudWatch agent as a different user (p. 532)
- Adding custom dimensions to metrics collected by the CloudWatch agent (p. 534)
- Multiple CloudWatch agent configuration files (p. 534)
- Aggregating or rolling up metrics collected by the CloudWatch agent (p. 536)
- Collecting high-resolution metrics with the CloudWatch agent (p. 537)
- Sending metrics and logs to a different account (p. 537)
- Timestamp differences between the unified CloudWatch agent and the earlier CloudWatch Logs agent (p. 539)

### Running the CloudWatch agent as a different user

On Linux servers, the CloudWatch runs as the root user by default. To have the agent run as a different user, use the `run_as_user` parameter in the `agent` section in the CloudWatch agent configuration file. This option is available only on Linux servers.

If you're already running the agent with the root user and want to change to using a different user, use one of the following procedures.

**To run the CloudWatch agent as a different user on an EC2 instance running Linux**

1. Download and install a new CloudWatch agent package. For more information, see [Download the CloudWatch agent package](p. 430).
2. Create a new Linux user or use the default user named `cwagent` that the RPM or DEB file created.
3. Provide credentials for this user in one of these ways:
• If the file `.aws/credentials` exists in the home directory of the root user, you must create a credentials file for the user you are going to use to run the CloudWatch agent. This credentials file will be `/home/username/.aws/credentials`. Then set the value of the `shared_credential_file` parameter in `common-config.toml` to the pathname of the credential file. For more information, see (Optional) Modify the common configuration for proxy or Region information (p. 441).

• If the file `.aws/credentials` does not exist in the home directory of the root user, you can do one of the following:
  • Create a credentials file for the user you are going to use to run the CloudWatch agent. This credentials file will be `/home/username/.aws/credentials`. Then set the value of the `shared_credential_file` parameter in `common-config.toml` to the pathname of the credential file. For more information, see (Optional) Modify the common configuration for proxy or Region information (p. 441).
  • Instead of creating a credentials file, attach an IAM role to the instance. The agent uses this role as the credential provider.

4. In the CloudWatch agent configuration file, add the following line in the `agent` section:

```
"run_as_user": "username"
```

Make other modifications to the configuration file as needed. For more information, see Create the CloudWatch agent configuration file (p. 466)

5. Give the user necessary permissions. The user must have Read (r) permissions for the log files to be collected, and must have Execute (x) permission on every directory in the log files' path.

6. Start the agent with the configuration file that you just modified.

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:configuration-file-path
```

---

To run the CloudWatch agent as a different user on an on-premises server running Linux

1. Download and install a new CloudWatch agent package. For more information, see Download the CloudWatch agent package (p. 430).

2. Create a new Linux user or use the default user named `cwagent` that the RPM or DEB file created.

3. Store the credentials of this user to a path that the user can access, such as `/home/username/.aws/credentials`.

4. Set the value of the `shared_credential_file` parameter in `common-config.toml` to the pathname of the credential file. For more information, see (Optional) Modify the common configuration for proxy or Region information (p. 441).

5. In the CloudWatch agent configuration file, add the following line in the `agent` section:

```
"run_as_user": "username"
```

Make other modifications to the configuration file as needed. For more information, see Create the CloudWatch agent configuration file (p. 466)

6. Give the user necessary permissions. The user must have Read (r) permissions for the log files to be collected, and must have Execute (x) permission on every directory in the log files' path.

7. Start the agent with the configuration file that you just modified.

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:configuration-file-path
```

---

533
Adding custom dimensions to metrics collected by the CloudWatch agent

To add custom dimensions such as tags to metrics collected by the agent, add the `append_dimensions` field to the section of the agent configuration file that lists those metrics.

For example, the following example section of the configuration file adds a custom dimension named `stackName` with a value of `Prod` to the `cpu` and `disk` metrics collected by the agent.

```json
"cpu":{
    "resources": ["*"],
    "measurement": [
        "cpu_usage_guest",
        "cpu_usage_nice",
        "cpu_usage_idle"
    ],
    "totalcpu":false,
    "append_dimensions": {
        "stackName": "Prod"
    }
},
"disk": {
    "resources": ["/", "/tmp"],
    "measurement": [
        "total",
        "used"
    ],
    "append_dimensions": {
        "stackName": "Prod"
    }
}
```

Remember that any time you change the agent configuration file, you must restart the agent to have the changes take effect.

**Multiple CloudWatch agent configuration files**

You can set up the CloudWatch agent to use multiple configuration files. For example, you can use a common configuration file that collects a set of metrics and logs that you always want to collect from all servers in your infrastructure. You can then use additional configuration files that collect metrics from certain applications or in certain situations.

To set this up, first create the configuration files that you want to use. Any configuration files that will be used together on the same server must have different file names. You can store the configuration files on servers or in Parameter Store.

Start the CloudWatch agent using the `fetch-config` option and specify the first configuration file. To append the second configuration file to the running agent, use the same command but with the `append-config` option. All metrics and logs listed in either configuration file are collected. The following example Linux commands illustrate this scenario using configurations stores as files. The first line starts the agent using the `infrastructure.json` configuration file, and the second line appends the `app.json` configuration file.
The following example configuration files illustrate a use for this feature. The first configuration file is used for all servers in the infrastructure, and the second collects only logs from a certain application and is appended to servers running that application.

**infrastructure.json**

```json
{
  "metrics": {
    "metrics_collected": {
      "cpu": {
        "resources": ["*"]
      },
      "measurement": ["usage_active"],
      "totalcpu": true
    },
    "mem": {
      "measurement": ["used_percent"]
    }
  },
  "logs": {
    "logs_collected": {
      "files": {
        "collect_list": [
        
          "log_group_name": "amazon-cloudwatch-agent.log"
        },
        
        {"file_path": "/var/log/messages",
          "log_group_name": "/var/log/messages"
        }
        
        ]
    }
  }
}
```

**app.json**

```json
{
  "logs": {
    "logs_collected": {
      "files": {
        "collect_list": [
        
        {"file_path": "*/app/app.log*", 
          "log_group_name": "/app/app.log"
        }
        
        ]
    }
  }
}
```
Any configuration files appended to the configuration must have different file names from each other and from the initial configuration file. If you use append-config with a configuration file with the same file name as a configuration file that the agent is already using, the append command overwrites the information from the first configuration file instead of appending to it. This is true even if the two configuration files with the same file name are on different file paths.

The preceding example shows the use of two configuration files, but there is no limit to the number of configuration files that you can append to the agent configuration. You can also mix the use of configuration files located on servers and configurations located in Parameter Store.

**Aggregating or rolling up metrics collected by the CloudWatch agent**

To aggregate or roll up metrics collected by the agent, add an aggregation_dimensions field to the section for that metric in the agent configuration file.

For example, the following configuration file snippet rolls up metrics on the AutoScalingGroupName dimension. The metrics from all instances in each Auto Scaling group are aggregated and can be viewed as a whole.

```
"metrics": {
    "cpu":{},
    "disk":{},
    "aggregation_dimensions": [["AutoScalingGroupName"]]
}
```

To roll up along the combination of each InstanceId and InstanceType dimensions in addition to rolling up on the Auto Scaling group name, add the following.

```
"metrics": {
    "cpu":{},
    "disk":{},
    "aggregation_dimensions": [["AutoScalingGroupName"], ["InstanceId", "InstanceType"]]
}
```

To roll up metrics into one collection instead, use [].

```
"metrics": {
    "cpu":{},
    "disk":{},
    "aggregation_dimensions": [[]]
}
```

Remember that any time you change the agent configuration file, you must restart the agent to have the changes take effect.
Collecting high-resolution metrics with the CloudWatch agent

The `metrics_collection_interval` field specifies the time interval for the metrics collected, in seconds. By specifying a value of less than 60 for this field, the metrics are collected as high-resolution metrics.

For example, if your metrics should all be high-resolution and collected every 10 seconds, specify 10 as the value for `metrics_collection_interval` under the `agent` section as a global metrics collection interval.

```
"agent": {
   "metrics_collection_interval": 10
}
```

Alternatively, the following example sets the `cpu` metrics to be collected every second, and all other metrics are collected every minute.

```
"agent":{
   "metrics_collection_interval": 60
},
"metrics":{
   "metrics_collected":{
      "cpu":{
         "resources":[
            "*
         ],
         "measurement":{
            "cpu_usage_guest",
            "totalcpu":false,
            "metrics_collection_interval": 1
         }
      },
      "disk":{
         "resources":[
            "/",
            "/tmp"
         ],
         "measurement":{
            "total",
            "used"
         }
      }
   }
}
```

Remember that any time you change the agent configuration file, you must restart the agent to have the changes take effect.

Sending metrics and logs to a different account

To have the CloudWatch agent send the metrics, logs, or both to a different account, specify a `role_arn` parameter in the agent configuration file on the sending server. The `role_arn` value specifies an IAM role in the target account that the agent uses when sending data to the target account. This role enables the sending account to assume a corresponding role in the target account when delivering the metrics or logs to the target account.

You can also specify two separate `role_arn` strings in the agent configuration file: one to use when sending metrics and another for sending logs.
The following example of part of the `agent` section of the configuration file sets the agent to use `CrossAccountAgentRole` when sending metrics and logs to a different account.

```
{
    "agent": {
        "credentials": {
            "role_arn": "arn:aws:iam::123456789012:role/CrossAccountAgentRole"
        }
    }
}
```

Alternatively, the following example sets different roles for the sending account to use for sending metrics and logs:

```
"metrics": {
    "credentials": {
        "role_arn": "RoleToSendMetrics"
    },
    "metrics_collected": {
        ...
    }
}
```

```
"logs": {
    "credentials": {
        "role_arn": "RoleToSendLogs"
    },
    ...
}
```

### Policies needed

When you specify a `role_arn` in the agent configuration file, you must also make sure the IAM roles of the sending and target accounts have certain policies. The roles in both the sending and target accounts should have `CloudWatchAgentServerPolicy`. For more information about assigning this policy to a role, see Create IAM roles to use with the CloudWatch agent on Amazon EC2 instances (p. 444).

The role in the sending account also must include the following policy. You add this policy on the Permissions tab in the IAM console when you edit the role.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["sts:AssumeRole"],
            "Resource": [
                "arn:aws:iam::target-account-ID:role/agent-role-in-target-account"
            ]
        }
    ]
}
```

The role in the target account must include the following policy so that it recognizes the IAM role used by the sending account. You add this policy on the Trust relationships tab in the IAM console when you edit the role. The role in the target account where you add this policy is the role you created in Create IAM roles and users for use with CloudWatch agent (p. 435). This role is the role specified in `agent-role-in-target-account` in the policy used by the sending account.
Timestamp differences between the unified CloudWatch agent and the earlier CloudWatch Logs agent

The CloudWatch agent supports a different set of symbols for timestamp formats, compared to the earlier CloudWatch Logs agent. These differences are shown in the following table.

<table>
<thead>
<tr>
<th>Symbols supported by both agents</th>
<th>Symbols supported only by unified CloudWatch agent</th>
<th>Symbols supported only by earlier CloudWatch Logs agent</th>
</tr>
</thead>
<tbody>
<tr>
<td>%A, %a, %b, %B, %d, %f, %H, %I, %m, %M, %p, %S, %y, %Y, %Z, %z</td>
<td>%-d, %-l, %-m, %-M, %-S</td>
<td>%c, %j, %U, %W, %w</td>
</tr>
</tbody>
</table>

For more information about the meanings of the symbols supported by the new CloudWatch agent, see CloudWatch Agent Configuration File: Logs Section in the Amazon CloudWatch User Guide. For information about symbols supported by the CloudWatch Logs agent, see Agent Configuration File in the Amazon CloudWatch Logs User Guide.

Troubleshooting the CloudWatch agent

Use the following information to help troubleshoot problems with the CloudWatch agent.

Topics
- CloudWatch agent command line parameters (p. 540)
- Installing the CloudWatch agent using Run Command fails (p. 540)
- The CloudWatch agent won’t start (p. 540)
- Verify that the CloudWatch agent is running (p. 540)
- The CloudWatch agent won’t start, and the error mentions an Amazon EC2 Region (p. 541)
- The CloudWatch agent won’t start on Windows Server (p. 541)
- Unable to find credentials on Windows Server (p. 542)
- Where are the metrics? (p. 542)
- I updated my agent configuration but don’t see the new metrics or logs in the CloudWatch console (p. 542)
CloudWatch agent command line parameters

To see the full list of parameters supported by the CloudWatch agent, enter the following at the command line at a computer where you have it installed:

```
amazon-cloudwatch-agent-ctl -help
```

Installing the CloudWatch agent using Run Command fails

To install the CloudWatch agent using Systems Manager Run Command, the SSM Agent on the target server must be version 2.2.93.0 or later. If your SSM Agent isn't the correct version, you might see errors that include the following messages:

```
no latest version found for package AmazonCloudWatchAgent on platform linux
```

```
failed to download installation package reliably
```

For information about updating your SSM Agent version, see Installing and Configuring SSM Agent in the AWS Systems Manager User Guide.

The CloudWatch agent won't start

If the CloudWatch agent fails to start, there might be an issue in your configuration. Configuration information is logged in the `configuration-validation.log` file. This file is located in `/opt/aws/amazon-cloudwatch-agent/logs/configuration-validation.log` on Linux servers and in `\%ProgramData\Amazon\AmazonCloudWatchAgent\Logs\configuration-validation.log` on servers running Windows Server.

Verify that the CloudWatch agent is running

You can query the CloudWatch agent to find whether it's running or stopped. You can use AWS Systems Manager to do this remotely. You can also use the command line, but only to check the local server.

To query the status of the CloudWatch agent using Run Command

2. In the navigation pane, choose Run Command.
   -or-

   If the AWS Systems Manager home page opens, scroll down and choose Explore Run Command.
3. Choose Run command.
4. In the Command document list, choose the button next to AmazonCloudWatch-ManageAgent.
5. In the **Action** list, choose **status**.
6. For **Optional Configuration Source** choose **default** and keep **Optional Configuration Location** blank.
7. In the **Target** area, choose the instance to check.
8. Choose **Run**.

If the agent is running, the output resembles the following.

```json
{
  "status": "running",
  "starttime": "2017-12-12T18:41:18",
  "version": "1.73.4"
}
```

If the agent is stopped, the "status" field displays "stopped".

**To query the status of the CloudWatch agent locally using the command line**

- On a Linux server, enter the following:

  ```bash
  sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -m ec2 -a status
  ```

- On a server running Windows Server, enter the following in PowerShell as an administrator:

  ```powershell
  & $Env:ProgramFiles\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1 -m ec2 -a status
  ```

**The CloudWatch agent won't start, and the error mentions an Amazon EC2 Region**

If the agent doesn't start and the error message mentions an Amazon EC2 Region endpoint, you might have configured the agent to need access to the Amazon EC2 endpoint without granting that access.

For example, if you specify a value for the `append_dimensions` parameter in the agent configuration file that depends on Amazon EC2 metadata and you use proxies, you must make sure that the server can access the endpoint for Amazon EC2. For more information about these endpoints, see Amazon Elastic Compute Cloud (Amazon EC2) in the *Amazon Web Services General Reference*.

**The CloudWatch agent won't start on Windows Server**

On Windows Server, you might see the following error:

```
Start-Service : Service 'Amazon CloudWatch Agent (AmazonCloudWatchAgent)' cannot be started due to the following error: Cannot start service AmazonCloudWatchAgent on computer '.'.
At C:\Program Files\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1:113 char:12
  + $svc | Start-Service
  + ~~~~~~~~~~~~~
  + CategoryInfo : OpenError:
(System.ServiceProcess.ServiceController:ServiceController) [Start-Service],
```
Unable to find credentials on Windows Server

On Windows Server, if you have credentials in a location other than `$SystemDrive\Users\Administrator\.aws` on Windows Server 2012, or `$SystemDrive\Documents and Settings \Administrator\.aws` on Windows Server 2003, you can specify your own credential path by using the `shared_credential_file` option in `common.toml`.

If you don’t have a credential file, you must create one. For more information, see (Optional) Modify the common configuration for proxy or Region information (p. 441).

Where are the metrics?

If the CloudWatch agent has been running but you can’t find metrics collected by it in the AWS Management Console or the AWS CLI, confirm that you’re using the correct namespace. By default, the namespace for metrics collected by the agent is `CWAgent`. You can customize this namespace using the `namespace` field in the `metrics` section of the agent configuration file. If you don’t see the metrics that you expect, check the configuration file to confirm the namespace being used.

When you first download the CloudWatch agent package, the agent configuration file is `amazon-cloudwatch-agent.json`. This file is in the directory where you ran the configuration wizard, or you might have moved it to a different directory. If you use the configuration wizard, the agent configuration file output from the wizard is named `config.json`. For more information about the configuration file, including the `namespace` field, see CloudWatch agent configuration file: Metrics section (p. 473).

I updated my agent configuration but don’t see the new metrics or logs in the CloudWatch console

If you update your CloudWatch agent configuration file, the next time that you start the agent, you need to use the `fetch-config` option. For example, if you stored the updated file on the local computer, enter the following command:

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -s -m ec2 -c file:configuration-file-path
```

CloudWatch agent files and locations

The following table lists the files installed by and used with the CloudWatch agent, along with their locations on servers running Linux or Windows Server.
### Finding information about CloudWatch agent versions

To find the version number of the CloudWatch agent on a Linux server, enter the following command:

```bash
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a status
```

To find the version number of the CloudWatch agent on Windows Server, enter the following command:

```bash
$Env:ProgramFiles\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1
```

<table>
<thead>
<tr>
<th>File</th>
<th>Linux location</th>
<th>Windows Server location</th>
</tr>
</thead>
<tbody>
<tr>
<td>The control script that controls starting, stopping, and</td>
<td>/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl or /usr/bin/amazon-cloudwatch-agent-ctl</td>
<td>$Env:ProgramFiles\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1</td>
</tr>
<tr>
<td>restarting the agent.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The log file the agent writes to. You might need to attach this</td>
<td>/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log or /var/log/amazon/amazon-cloudwatch-agent/amazon-cloudwatch-agent.log</td>
<td>$Env:ProgramData\Amazon\AmazonCloudWatchAgent\Logs\amazon-cloudwatch-agent.log</td>
</tr>
<tr>
<td>when contacting AWS Support.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Agent configuration validation file.</td>
<td>/opt/aws/amazon-cloudwatch-agent/logs/configuration-validation.log or /var/log/amazon/amazon-cloudwatch-agent/configuration-validation.log</td>
<td>$Env:ProgramData\Amazon\AmazonCloudWatchAgent\Logs\configuration-validation.log</td>
</tr>
<tr>
<td>The JSON file used to configure the agent immediately after the</td>
<td>/opt/aws/amazon-cloudwatch-agent/bin/config.json</td>
<td>$Env:ProgramFiles\Amazon\AmazonCloudWatchAgent\config.json</td>
</tr>
<tr>
<td>wizard creates it. For more information, see Create the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CloudWatch agent configuration file (p. 466).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The JSON file used to configure the agent if this configuration file</td>
<td>/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json or /etc/amazon/amazon-cloudwatch-agent/amazon-cloudwatch-agent.json</td>
<td>$Env:ProgramData\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent.json</td>
</tr>
<tr>
<td>has been downloaded from Parameter Store.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TOML file used to specify Region and credential information to</td>
<td>/opt/aws/amazon-cloudwatch-agent/etc/common-config.toml or /etc/amazon/amazon-cloudwatch-agent/common-config.toml</td>
<td>$Env:ProgramData\Amazon\AmazonCloudWatchAgent\common-config.toml</td>
</tr>
<tr>
<td>be used by the agent, overriding system defaults.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Logs generated by the CloudWatch agent

The agent generates a log while it runs. This log includes troubleshooting information. This log is the `amazon-cloudwatch-agent.log` file. This file is located in `/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log` on Linux servers and in `$Env:ProgramData\Amazon\AmazonCloudWatchAgent\Logs\amazon-cloudwatch-agent.log` on servers running Windows Server.

You can configure the agent to log additional details in the `amazon-cloudwatch-agent.log` file. In the agent configuration file, in the `agent` section, set the `debug` field to `true`, then reconfigure and restart the CloudWatch agent. To disable the logging of this extra information, set the `debug` field to `false` reconfigure and restart the agent. For more information, see Manually create or edit the CloudWatch agent configuration file (p. 471).

Stopping and restarting the CloudWatch agent

You can manually stop the CloudWatch agent using either AWS Systems Manager or the command line.

To stop the CloudWatch agent using Run Command

2. In the navigation pane, choose Run Command.
   - or-
   If the AWS Systems Manager home page opens, scroll down and choose Explore Run Command.
3. Choose Run command.
4. In the Command document list, choose AmazonCloudWatch-ManageAgent.
5. In the Targets area, choose the instance where you installed the CloudWatch agent.
6. In the Action list, choose stop.
7. Keep Optional Configuration Source and Optional Configuration Location blank.

To stop the CloudWatch agent locally using the command line

- On a Linux server, enter the following:
Stopping and restarting the CloudWatch agent

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -m ec2 -a stop
```

On a server running Windows Server, enter the following in PowerShell as an administrator:

```
& $Env:ProgramFiles\Amazon\AmazonCloudWatchAgent\amazon-cloudwatch-agent-ctl.ps1 -m ec2 -a stop
```

To restart the agent, follow the instructions in Start the CloudWatch agent (p. 450).
Amazon CloudWatch Application Insights

Amazon CloudWatch Application Insights facilitates observability for your applications and underlying AWS resources. It helps you set up the best monitors for your application resources to continuously analyze data for signs of problems with your applications. Application Insights, which is powered by SageMaker and other AWS technologies, provides automated dashboards that show potential problems with monitored applications, which help you to quickly isolate ongoing issues with your applications and infrastructure. The enhanced visibility into the health of your applications that Application Insights provides helps reduce mean time to repair (MTTR) to troubleshoot your application issues.

When you add your applications to Amazon CloudWatch Application Insights, it scans the resources in the applications and recommends and configures metrics and logs on CloudWatch for application components. Example application components include SQL Server backend databases and Microsoft IIS/Web tiers. Application Insights analyzes metric patterns using historical data to detect anomalies, and continuously detects errors and exceptions from your application, operating system, and infrastructure logs. It correlates these observations using a combination of classification algorithms and built-in rules. Then, it automatically creates dashboards that show the relevant observations and problem severity information to help you prioritize your actions. For common problems in .NET and SQL application stacks, such as application latency, SQL Server failed backups, memory leaks, large HTTP requests, and canceled I/O operations, it provides additional insights that point to a possible root cause and steps for resolution. Built-in integration with AWS SSM OpsCenter allows you to resolve issues by running the relevant Systems Manager Automation document.

Sections
- What is Amazon CloudWatch Application Insights? (p. 546)
- How Amazon CloudWatch Application Insights works (p. 551)
- Get started with Amazon CloudWatch Application Insights (p. 555)
- Work with component configurations (p. 573)
- Create and configure CloudWatch Application Insights monitoring using CloudFormation templates (p. 599)
- Tutorial: Set up monitors for .NET applications using SQL Server (p. 608)
- View and troubleshoot problems detected by Amazon CloudWatch Application Insights (p. 613)
- Logs and metrics supported by Amazon CloudWatch Application Insights (p. 615)

What is Amazon CloudWatch Application Insights?

CloudWatch Application Insights helps you monitor your applications that use Amazon EC2 instances along with other application resources (p. 550). It identifies and sets up key metrics, logs, and alarms across your application resources and technology stack (for example, your Microsoft SQL Server database, web (IIS) and application servers, OS, load balancers, and queues). It continuously monitors metrics and logs to detect and correlate anomalies and errors. When errors and anomalies are detected, Application Insights generates CloudWatch Events that you can use to set up notifications or take actions. To assist with troubleshooting, it creates automated dashboards for detected problems, which include correlated metric anomalies and log errors, along with additional insights to point you to a potential root cause. The automated dashboards help you to take remedial actions to keep your
applications healthy and to prevent impact to the end-users of your application. It also creates OpsItems so that you can resolve problems using AWS SSM OpsCenter.

You can configure important counters, such as Mirrored Write Transaction/sec, Recovery Queue Length, and Transaction Delay, as well as Windows Event Logs on CloudWatch. When a failover event or problem occurs with your SQL HA workload, such as a restricted access to query a target database, CloudWatch Application Insights provides automated insights.

CloudWatch Application Insights integrates with AWS Launch Wizard to provide a one-click monitoring setup experience for deploying SQL Server HA workloads on AWS. When you select the option to set up monitoring and insights with Application Insights on the Launch Wizard console, CloudWatch Application Insights automatically sets up relevant metrics, logs, and alarms on CloudWatch, and starts monitoring newly deployed workloads. You can view automated insights and detected problems, along with the health of your SQL Server HA workloads, on the CloudWatch console.

Contents

• Features (p. 547)
• Concepts (p. 547)
• Pricing (p. 548)
• Related services (p. 548)
• Supported application components (p. 550)
• Supported technology stacks (p. 550)

Features

Application Insights provides the following features.

Automatic set up of monitors for application resources

CloudWatch Application Insights reduces the time it takes to set up monitoring for your applications. It does this by scanning your application resources, providing a customizable list of recommended metrics and logs, and setting them up on CloudWatch to provide necessary visibility into your application resources, such as Amazon EC2 and Elastic Load Balancers (ELB). It also sets up dynamic alarms on monitored metrics. The alarms are automatically updated based on anomalies detected in the previous two weeks.

Problem detection and notification

CloudWatch Application Insights detects signs of potential problems with your application, such as metric anomalies and log errors. It correlates these observations to surface potential problems with your application. It then generates CloudWatch Events, which can be configured to receive notifications or take actions (p. 572). This eliminates the need for you to create individual alarms on metrics or log errors.

Troubleshooting

CloudWatch Application Insights creates CloudWatch automatic dashboards for problems that are detected. The dashboards show details about the problem, including the associated metric anomalies and log errors to help you with troubleshooting. They also provide additional insights that point to potential root causes of the anomalies and errors.

Concepts

The following concepts are important for understanding how Application Insights monitors your application.
Component
An auto-grouped, standalone, or custom grouping of similar resources that make up an application. We recommend grouping similar resources into custom components for better monitoring.

Observation
An individual event (metric anomaly, log error, or exception) that is detected with an application or application resource.

Problem
Problems are detected by correlating, classifying, and grouping related observations.

For definitions of other key concepts for CloudWatch Application Insights, see Amazon CloudWatch Concepts.

Pricing
CloudWatch Application Insights sets up recommended metrics and logs for selected application resources using CloudWatch Metrics, Logs, and CloudWatch Events for notifications on detected problems. These features are charged to your AWS account according to CloudWatch pricing. For the detected problems, it creates CloudWatch Events and automatic dashboards. You are not charged for setup assistance, monitoring data analysis, or problem detection.

Related services
The following services are used along with CloudWatch Application Insights:

Related AWS services
- **Amazon CloudWatch** provides system-wide visibility into resource utilization, application performance, and operational health. It collects and tracks metrics, sends alarm notifications, automatically updates resources that you are monitoring based on the rules that you define, and allows you to monitor your own custom metrics. CloudWatch Application Insights is initiated through CloudWatch—specifically, within the CloudWatch default operational dashboards. For more information, see the Amazon CloudWatch User Guide.
- **Amazon DynamoDB** is a fully managed NoSQL database service that lets you offload the administrative burdens of operating and scaling a distributed database so that you don't have to worry about hardware provisioning, setup and configuration, replication, software patching, or cluster scaling. DynamoDB also offers encryption at rest, which eliminates the operational burden and complexity involved in protecting sensitive data.
- **Amazon EC2** provides scalable computing capacity in the AWS Cloud. You can use Amazon EC2 to launch as many or as few virtual servers as you need, to configure security and networking, and to manage storage. You can scale up or down to handle changes in requirements or spikes in popularity, which reduces your need to forecast traffic. For more information, see the Amazon EC2 User Guide for Linux Instances or Amazon EC2 Guide for Windows Instances.
- **Amazon Elastic Block Store (Amazon EBS)** provides block-level storage volumes for use with Amazon EC2 instances. Amazon EBS volumes behave like raw, unformatted block devices. You can mount these volumes as devices on your instances. Amazon EBS volumes that are attached to an instance are exposed as storage volumes that persist independently from the life of the instance. You can create a file system on top of these volumes, or use them in any way you would use a block device (such as a hard drive). You can dynamically change the configuration of a volume attached to an instance. For more information, see the Amazon EBS User Guide.
- **Amazon EC2 Auto Scaling** helps ensure that you have the correct number of EC2 instances available to handle the load for your application. For more information, see the Amazon EC2 Auto Scaling User Guide.
• **Elastic Load Balancing** distributes incoming applications or network traffic across multiple targets, such as EC2 instances, containers, and IP addresses, in multiple Availability Zones. For more information, see the Elastic Load Balancing User Guide.

• IAM is a web service that helps you to securely control access to AWS resources for your users. Use IAM to control who can use your AWS resources (authentication), and to control the resources they can use and how they can use them (authorization). For more information, see Authentication and Access Control for Amazon CloudWatch.

• AWS Lambda lets you build serverless applications composed of functions that are triggered by events and automatically deploy them using CodePipeline and AWS CodeBuild. For more information, see AWS Lambda Applications.

• **AWS Launch Wizard for SQL Server** reduces the time it takes to deploy SQL Server high availability solution to the cloud. You input your application requirements, including performance, number of nodes, and connectivity on the service console, and AWS Launch Wizard identifies the right AWS resources to deploy and run your SQL Server Always On application.

• **AWS Resource Groups** help you to organize the resources that make up your application. With Resource Groups, you can manage and automate tasks on a large number of resources at one time. Only one Resource Group can be registered for a single application. For more information, see the AWS Resource Groups User Guide.

• **Amazon SQS** offers a secure, durable, and available hosted queue that allows you to integrate and decouple distributed software systems and components. For more information, see the Amazon SQS User Guide.

• **AWS Step Functions** is a serverless function composer that allows you to sequence a variety of AWS services and resources, including AWS Lambda functions, into structured, visual workflows. For more information, see the AWS Step Functions User Guide.

• **AWS SSM OpsCenter** aggregates and standardizes OpsItems across services while providing contextual investigation data about each OpsItem, related OpsItems, and related resources. OpsCenter also provides Systems Manager Automation documents (runbooks) that you can use to quickly resolve issues. You can specify searchable, custom data for each OpsItem. You can also view automatically-generated summary reports about OpsItems by status and source. For more information, see the AWS Systems Manager User Guide.

• **Amazon API Gateway** is an AWS service for creating, publishing, maintaining, monitoring, and securing REST, HTTP, and WebSocket APIs at any scale. API developers can create APIs that access AWS or other web services, as well as data stored in the AWS Cloud. For more information, see the Amazon API Gateway User Guide.

**Note**

Application Insights supports only REST API protocols (v1 of the API Gateway service).

• **Amazon Elastic Container Service (Amazon ECS)** is a fully managed container orchestration service. You can use Amazon ECS to run your most sensitive and mission-critical applications. For more information, see the Amazon Elastic Container Service Developer Guide.

• **Amazon Elastic Kubernetes Service (Amazon EKS)** is a managed service that you can use to run Kubernetes on AWS without having to install, operate, and maintain your own Kubernetes control plane or nodes. Kubernetes is an open-source system for automating the deployment, scaling, and management of containerized applications. For more information, see the Amazon EKS User Guide.

• **Kubernetes on Amazon EC2**. Kubernetes is open-source software that helps you deploy and manage containerized applications at scale. Kubernetes manages clusters of Amazon EC2 compute instances and runs containers on those instances with processes for deployment, maintenance, and scaling. With Kubernetes you can run any type of containerized application with the same toolset on-premises and in the cloud. For more information, see Running Kubernetes on AWS EC2.

**Related third-party services**

- For some workloads and applications monitored in Application Insights, Prometheus JMX exporter is installed using AWS Systems Manager Distributor so that CloudWatch Application Insights can
retrieve Java-specific metrics. When you choose to monitor a Java application, Application Insights automatically installs the Prometheus JMX exporter for you.

**Supported application components**

CloudWatch Application Insights scans your resource group to identify application components. Components can be standalone, auto-grouped (such as instances in an Auto Scaling group or behind a load balancer), or custom (by grouping together individual EC2 instances).

The following components are supported by CloudWatch Application Insights:

**AWS components**

- Amazon EC2
- Amazon EBS
- Amazon RDS
- Elastic Load Balancing: Application Load Balancer and Classic Load Balancer (all target instances of these load balancers are identified and configured).
- Amazon EC2 Auto Scaling groups: AWS Auto Scaling (Auto Scaling groups are dynamically configured for all target instances; if your application scales up, CloudWatch Application Insights automatically configure the new instances). Auto Scaling groups are not supported for CloudFormation-based Resource Groups.
- AWS Lambda
- Amazon Simple Queue Service (Amazon SQS)
- Amazon DynamoDB table
- Amazon S3 bucket metrics
- AWS Step Functions
- Amazon API Gateway REST API stages
- Amazon Elastic Container Service (Amazon ECS): cluster, service, and task
- Amazon Elastic Kubernetes Service (Amazon EKS): cluster
- Kubernetes on Amazon EC2: Kubernetes cluster running on EC2

Any other component type resources are not currently tracked by CloudWatch Application Insights. If a component type that is supported does not appear in your Application Insights application, the component may already be registered and managed by another application you own that is monitored by Application Insights.

**Supported technology stacks**

You can use CloudWatch Application Insights to monitor your applications running on Windows Server and Linux operating systems by selecting the application tier dropdown menu option for one of the following technologies:

- Front-end: Microsoft Internet Information Services (IIS) Web Server
- Worker-tier:
  - .NET Framework
  - .NET Core
- Applications: Java
- Databases:
How Application Insights works

This section contains information about how CloudWatch Application Insights works, including:

- How Application Insights monitors applications (p. 551)
- Data retention (p. 552)
- Quotas (p. 552)
- AWS Systems Manager (SSM) packages used by CloudWatch Application Insights (p. 552)

How Application Insights monitors applications

Application Insights monitors applications as follows.

Application discovery and configuration

The first time an application is added to CloudWatch Application Insights it scans the application components to recommend key metrics, logs, and other data sources to monitor for your application. You can then configure your application based on these recommendations.

Data preprocessing

CloudWatch Application Insights continuously analyzes the data sources being monitored across the application resources to discover metric anomalies and log errors (observations).

Intelligent problem detection

The CloudWatch Application Insights engine detects problems in your application by correlating observations using classification algorithms and built-in rules. To assist in troubleshooting, it creates automated CloudWatch dashboards, which include contextual information about the problems.

Alert and action

When CloudWatch Application Insights detects a problem with your application, it generates CloudWatch Events to notify you of the problem. See Application Insights CloudWatch Events and notifications for detected problems (p. 572) for more information about how to set up these Events.

Example scenario

You have an ASP.NET application that is backed by a SQL Server database. Suddenly, your database begins to malfunction because of high memory pressure. This leads to application performance degradation and possibly HTTP 500 errors in your web servers and load balancer.
With CloudWatch Application Insights and its intelligent analytics, you can identify the application layer that is causing the problem by checking the dynamically created dashboard that shows the related metrics and log file snippets. In this case, the problem might be at the SQL database layer.

**Data retention**

CloudWatch Application Insights retains problems for 55 days and observations for 60 days.

**Quotas**

For default quotas for CloudWatch Application Insights, see Amazon CloudWatch Application Insights endpoints and quotas. Unless otherwise noted, each quota is per AWS Region. Contact AWS Support to request an increase in your service quota. Many services contain quotas that cannot be changed. For more information about the quotas for a specific service, see the documentation for that service.

**AWS Systems Manager (SSM) packages used by CloudWatch Application Insights**

The packages listed in this section are used by Application Insights and can be independently managed and deployed with AWS Systems Manager Distributor. For more information about SSM Distributor, see AWS Systems Manager Distributor in the AWS Systems Manager User Guide.

**Packages:**

- AWSObservabilityExporter-JMXExporterInstallAndConfigure (p. 552)

**AWSObservabilityExporter-JMXExporterInstallAndConfigure**

You can retrieve workload-specific Java metrics from Prometheus JMX exporter for Application Insights to configure and monitor alarms. In the Application Insights console, on the Manage monitoring page, select JAVA application from the Application tier dropdown. Then under JAVA Prometheus exporter configuration, select your Collection method and JMX port number.

To use AWS Systems Manager Distributor to package, install, and configure the AWS-provided Prometheus JMX exporter package independently of Application Insights, complete the following steps.

**Prerequisites for using the Prometheus JMX exporter SSM package**

- SSM agent version 2.3.1550.0 or later installed
- The JAVA_HOME environment variable is set

**Install and configure the AWSObservabilityExporter-JMXExporterInstallAndConfigure package**

The AWSObservabilityExporter-JMXExporterInstallAndConfigure package is an SSM Distributor package that you can use to install and configure Prometheus JMX Exporter. When Java metrics are sent by the Prometheus JMX exporter, the CloudWatch agent can be configured to retrieve the metrics for the CloudWatch service.

1. Based on your preferences, prepare the Prometheus JMX exporter YAML configuration file located in the Prometheus GitHub repository using the example configuration and option descriptions to guide you.
2. Copy the Prometheus JMX exporter YAML configuration file encoded as Base64 to a new SSM parameter in SSM Parameter Store.

3. Navigate to the SSM Distributor console and open the Third party tab. Select AWSObservabilityExporter-JMXExporterInstallAndConfigure and choose Install one time.

4. Update the SSM parameter you created in the first step by replacing "Additional Arguments" with the following:

```
{
  "SSM_EXPORTER_CONFIGURATION": "{{ssm:<SSM_PARAMETER_STORE_NAME>}}",
  "SSM_EXPOSITION_PORT": "9404"
}
```

**Note**

Port 9404 is the default port used to send Prometheus JMX metrics; however, you can update it.

**Example: Configure CloudWatch agent to retrieve Java metrics**

1. Install the Prometheus JMX exporter as described in the previous procedure and verify that it is correctly installed on your instance by checking the port status.

   **Successful installation on Windows instance example**

   ```
   PS C:\> curl http://localhost:9404 (http://localhost:9404/)
   StatusCode : 200
   StatusDescription : OK
   Content : # HELP jvm_info JVM version info
   ```

   **Successful installation on Linux instance example**

   ```
   # curl localhost:9404
   # HELP jmx_config_reload_failure_total Number of times configuration have failed to be reloaded.
   # TYPE jmx_config_reload_failure_total counter
   jmx_config_reload_failure_total 0.0
   ```

2. Create the Prometheus service discovery YAML file. The following example service discovery file performs the following:

   * Specifies the Prometheus JMX exporter host port as localhost: 9404.
   * Attaches labels (Application, ComponentName, and InstanceId) to the metrics, which can be set as CloudWatch metric dimensions.

   ```
   # cat prometheus_sd_jmx.yaml
   - targets:
     - 127.0.0.1:9404
   labels:
     Application: myApp
     ComponentName: arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/sample-App1-MMZ8E3GH4H2/aac36d7feal6e5b
     InstanceId: i-12345678901234567
   ```

3. Create the Prometheus JMX exporter configuration YAML file. The following example configuration file specifies the following:

   * The metrics retrieval job interval and timeout period.
• The metrics retrieval (also known as "scraping") jobs (jmx and sap), which include the job name, maximum time series returned at a time, and service discovery file path.

```yaml
$ cat prometheus.yaml
global:
  scrape_interval: 1m
  scrape_timeout: 10s
scrape_configs:
  - job_name: jmx
    sample_limit: 10000
    file_sd_configs:
      - files: ["/tmp/prometheus_sd_jmx.yaml"]
  - job_name: sap
    sample_limit: 10000
    file_sd_configs:
      - files: ["/tmp/prometheus_sd_sap.yaml"]
```

4. Verify that the CloudWatch agent is installed on your Amazon EC2 instance and that the version is 1.247346.1b249759 or later. To install the CloudWatch agent on your EC2 instance, see Installing the CloudWatch Agent. To verify the version, see Finding information about CloudWatch agent versions.

5. Configure the CloudWatch agent. For more information about how to configure the CloudWatch agent configuration file, see Manually create or edit the CloudWatch agent configuration file. The following example CloudWatch agent configuration file performs the following:

• Specifies the Prometheus JMX exporter configuration file path.
• Specifies the target log group to which to publish EMF metric logs.
• Specifies two sets of dimensions for each metric name.
• Sends 8 (4 metric names * 2 sets of dimensions per metric name) CloudWatch metrics.

```json
{
  "logs":{
    "logs_collected":{
      ...
    },
    "metrics_collected":{
      "prometheus":{
        "cluster_name":"prometheus-test-cluster",
        "log_group_name":"prometheus-test",
        "prometheus_config_path":"/tmp/prometheus.yaml",
        "emf_processor":{
          "metric_declaration_dedup":true,
          "metric_namespace":"CWAgent",
          "metric_unit":{
            "jvm_threads_current":"Count",
            "jvm_gc_collection_seconds_sum":"Second",
            "jvm_memory_bytes_used":"Bytes"
          },
          "metric_declaration":[
            {
              "source_labels":[
                "job"
              ],
              "label_matcher":"^jmx$",
              "dimensions":[
                ["InstanceId",
                "ComponentName"
              ],
```
Get started with Amazon CloudWatch Application Insights

To get started on CloudWatch Application Insights, verify that you have met the prerequisites outlined below and have created an IAM policy. Then, you can get started using the console link to enable CloudWatch Application Insights. To configure your application resources, follow the steps under Set up, configure, and manage your application for monitoring (p. 557).

Contents

- Access CloudWatch Application Insights (p. 555)
- Prerequisites (p. 555)
- IAM policy (p. 556)
- Set up, configure, and manage your application for monitoring (p. 557)

Access CloudWatch Application Insights

If you have access to CloudWatch Application Insights, you can manage it through one of the following interfaces:

- **CloudWatch console**: To add monitors for your application, choose Application Insights under Insights in the left navigation pane of the CloudWatch console. After your application is configured, you can use the CloudWatch console to view and analyze problems that are detected.

- **AWS Command Line Interface (AWS CLI)**: You can use the AWS CLI to access AWS API operations. For more information, see Installing the AWS Command Line Interface in the AWS Command Line Interface User Guide. For the API reference, see the Amazon CloudWatch Application Insights API Reference.

Prerequisites

You must complete the following prerequisites to configure an application with CloudWatch Application Insights:

- **AWS SSM enablement**: You must install Systems Manager Agent (SSM Agent), and your instances must be SSM enabled. For steps on how to install the SSM Agent, see Setting Up AWS SSM.
IAM policy

To use CloudWatch Application Insights, you must create an Identity and Access Management (IAM) policy and attach it to your IAM user identity. The IAM policy defines the user permissions.

To create an IAM policy using the console

To create an IAM policy using the IAM console, follow these steps.

1. Go to the IAM console. In the left navigation pane, select Policies.
2. At the top of the page, select Create policy.
3. Select the JSON tab.
4. Copy and paste the following JSON document under the JSON tab.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "applicationinsights:*",
                "iam:CreateServiceLinkedRole",
                "iam:ListRoles"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

5. Select Review Policy.
6. Enter a Name for the policy, for example, “AppInsightsPolicy.” Optionally, enter a Description.
7. Select **Create Policy**.
8. Select **Users** from the left navigation pane.
9. Select the **User name** of the user to which you would like to attach the policy.
10. Select **Add permissions**.
11. Select **Attach existing policies directly**.
12. Search for the policy that you just created, and select the check box to the left of the policy name.
13. Select **Next: Review**.
14. Make sure that the correct policy is listed, and select **Add permissions**.
15. Make sure that you log in with the user associated with the policy that you just created when you use CloudWatch Application Insights.

**To create an IAM policy using the AWS CLI**

To create an IAM policy using the AWS CLI, run the `create-policy` operation from the command line using the JSON document above as a file in your current folder.

**To create an IAM policy using AWS Tools for Windows PowerShell**

To create an IAM policy using the AWS Tools for Windows PowerShell, run the `New-IAMPolicy` cmdlet using the JSON document above as a file in your current folder.

**Set up, configure, and manage your application for monitoring**

This section provides steps for setting up, configuring, and managing your CloudWatch Application Insights application using the console, the AWS CLI, and AWS Tools for Windows PowerShell.

**Topics**

- Set up, configure, and manage your application for monitoring from the CloudWatch console (p. 557)
- Set up, configure, and manage your application for monitoring using the command line (p. 560)
- Application Insights CloudWatch Events and notifications for detected problems (p. 572)

**Set up, configure, and manage your application for monitoring from the CloudWatch console**

This section provides steps for setting up, configuring, and managing your application for monitoring from the CloudWatch console.

**Console procedures**

- **Add and configure an application** (p. 557)
- Disable an application (p. 559)
- Disable monitoring for an application component (p. 560)
- Delete an application (p. 560)

**Add and configure an application**

Add and configure an application from the CloudWatch console
To get started with CloudWatch Application Insights from the CloudWatch console, follow these steps.

1. **Start.** Open the CloudWatch console landing page. From the left navigation pane, choose Application Insights under Insights.

2. **Add an application.** To set up monitoring for your .NET and SQL Server application, on the CloudWatch Application Insights page, select Add an application. This page shows the list of applications that are monitored with CloudWatch Application Insights, along with their monitoring status. After you select Add an application, you will be taken to the Add an application page.

3. **Select resource group.** On the Add an application page, to add an application to CloudWatch Application Insights, choose an AWS Resource Group from the dropdown list that contains your application resources. These resources include front-end servers, load balancers, auto scaling groups, and database servers.

   An ARN will be generated for the application in the following format:

   \[
   \text{arn:partition:applicationinsights:region:account-id:application/resource-group/resource-group-name}
   \]

   For example:

   \[
   \text{arn:aws:applicationinsights:us-east-1:123456789012:application/resource-group/my-resource-group}
   \]

   CloudWatch Application Insights supports both tag-based and CloudFormation-based Resource Groups (with the exception of Auto Scaling groups). For more information, see Working with Tag Editor.

   If you have not created a Resource Group for your .NET application, you can create one. For more information, see the AWS Resource Groups User Guide.

4. **Add monitoring details.** After you add an application, you are taken to the Monitoring Details page, which lists the application components, resources in those components, and their monitoring status. Components are auto-grouped, standalone, or custom groupings of similar resources that make up an application. By default, CloudWatch Application Insights groups instances that are in Auto Scaling groups, and instances that are behind your Elastic Load Balancers. On this page, you can configure custom components and can manage monitoring for each application component. For supported components, see Supported application components (p. 550).

5. **Configure components.** After selecting a Resource Group, you are prompted to configure components. We recommend grouping similar resources, such as .NET web server instances, into custom components for easier onboarding and better monitoring and insights. By default, CloudWatch Application Insights groups instances that are in Auto Scaling groups, and instances that are behind your Elastic Load Balancers. For supported components, see Supported application components (p. 550).

   Under Application components, for each component for which you want to set up monitors, select the component and select Manage Monitoring.

6. **Enable monitors.** To set up monitoring for an application component, select the components that you want to monitor and then choose Manage Monitoring. Select the Enable Monitoring check box. When you select the check box, the dropdown populates with the relevant application tiers. Choose the application tier for the selected component. The tiers indicate the part of the application stack running on the selected resources. If you select a custom tier, Application Insights recommends monitors based on the operating system. You can customize the list of metrics and logs, and add custom application logs and log patterns to detect.

   Based on your tier selection, CloudWatch Application Insights makes recommendations for logs to monitor for the selected component. This recommendation can be customized according to your needs.
For application-specific logs, including for Microsoft SQL Server Error logs and IIS logs, verify the default log path (if any) or enter the correct log location in your EC2 instance.

You can also choose to add Windows Event Logs, including Windows Logs and Applications and Services Logs. To do this, enter the types of events you want to store and analyze. Then, specify all of the event levels (critical, error, warning, informational, or verbose) that you want to store in your CloudWatch account.

You can add a log group for storing and grouping each of these logs on your CloudWatch account, which also facilitates searches.

CloudWatch Application Insights also sets up relevant metrics for your application resources. They are monitored for approximately two weeks to identify the appropriate metrics thresholds.

If you have created the metrics in the past, CloudWatch Application Insights pulls historical data for the last two weeks to identify the thresholds and to set the alarms accordingly. For newly created metrics, it may take up to three days before alarms are created. You can also monitor your application resources using the CloudWatch alarms you created in your account.

7. **Save monitors.** When you are finished selecting and customizing logs and metrics, select **Save** to set up monitors for the selected component. When you select **Save**, Application Insights sets up the CloudWatch Agent configuration files for all of the instances in your application based on the recommended metrics and your selection of logs. It can take up to an hour for this process to complete.

CloudWatch Application Insights also sets up CloudWatch alarms for selected metrics in the component. The alarms are dynamically updated by monitoring historical metric patterns from the past two weeks.

When you select **Cancel**, Application Insights only deletes your current selections.

When you create a new application with CloudWatch Application Insights, the service-linked role is created for you. To delete the service-linked role, you must first delete all of your applications on CloudWatch Application Insights and then manually delete the role. For more information, see Using service-linked roles for CloudWatch Application Insights (p. 722).

CloudWatch Application Insights is now set to monitor metrics and logs for your application. It may take up to two weeks for the system to generate meaningful insights.

*If your Resource Group is already configured and you want to save your configuration but don’t want CloudWatch Application Insights to monitor your application, you can disable CloudWatch Application Insights. You can also delete your configuration.

8. **Add AWS SSM OpsCenter integration.** To view and get notified when problems are detected for selected applications, select the **Integrate with AWS OpsCenter** check box on the **Monitoring Details** page. To track the operations that are taken to resolve operational work items (OpsItems) that are related to your AWS resources, provide the SNS topic ARN.

9. **View monitoring (optional).** After your application has been set up for monitoring, you can view and troubleshoot detected problems and insights in the default overview page of the CloudWatch console. You can view detected problems, alarms, and dashboards by selecting **View Insights** from the Application Insights landing page, or on the CloudWatch landing page.

**Disable an application**

To disable an application, from the CloudWatch dashboard, on the left navigation pane, choose **Application Insights** under **Insights**. Select the application that you want to disable. Under **Actions**, choose **Disable**. When you disable an application, monitoring is disabled, but Application Insights stores the saved monitors for application components.
Disable monitoring for an application component

To disable monitoring for an application component, from the Application Details page select the component for which you want to disable monitoring. Choose Manage Monitors, and then clear the Enable Monitoring check box.

Delete an application

To delete an application, from the CloudWatch dashboard, on the left navigation pane, choose Application Insights under Insights. Select the application that you want to delete. Under Actions, choose Delete. This deletes monitoring and deletes all of the saved monitors for application components. The application resources are not deleted.

Set up, configure, and manage your application for monitoring using the command line

This section provides steps for setting up, configuring, and managing your application for monitoring using the AWS CLI and AAWS Tools for Windows PowerShell.

Command line procedures

- Add and manage an application  (p. 560)
- Manage and update monitoring (p. 563)
- Configure monitoring for SQL Always On Availability Groups (p. 566)
- Configure monitoring for MySQL RDS (p. 569)
- Configure monitoring for MySQL EC2 (p. 569)
- Configure monitoring for PostgreSQL RDS (p. 570)
- Configure monitoring for PostgreSQL EC2 (p. 570)
- Configure monitoring for Oracle RDS (p. 571)
- Configure monitoring for Oracle EC2 (p. 571)

Add and manage an application

You can add, get information about, manage, and configure your Application Insights application using the command line.

Topics

- Add an application (p. 560)
- Describe an application (p. 561)
- List components in an application (p. 561)
- Describe a component (p. 561)
- Group similar resources into a custom component (p. 562)
- Ungroup a custom component (p. 562)
- Update an application (p. 563)
- Update a custom component (p. 563)

Add an application using the AWS CLI

To use the AWS CLI to add an application for your resource group called my-resource-group, with OpsCenter enabled to deliver the created opsItem to the SNS topic ARN arn:aws:sns:us-east-1:123456789012:MyTopic, use the following command.
Add an application using AWS Tools for Windows PowerShell

To use AWS Tools for Windows PowerShell to add an application for your resource group called `my-resource-group` with OpsCenter enabled to deliver the created opsItem to the SNS topic ARN `arn:aws:sns:us-east-1:123456789012:MyTopic`, use the following command.

```
New-CWAIApplication -ResourceGroupName my-resource-group -OpsCenterEnabled true - OpsItemSNSTopicArn arn:aws:sns:us-east-1:123456789012:MyTopic
```

Describe an application

Describe an application using the AWS CLI

To use the AWS CLI to describe an application created on a resource group called `my-resource-group`, use the following command.

```
aws application-insights describe-application --resource-group-name my-resource-group
```

Describe an application using AWS Tools for Windows PowerShell

To use the AWS Tools for Windows PowerShell to describe an application created on a resource group called `my-resource-group`, use the following command.

```
Get-CWAIApplication -ResourceGroupName my-resource-group
```

List components in an application

List components in an application using the AWS CLI

To use the AWS CLI to list the components created on a resource group called `my-resource-group`, use the following command.

```
aws application-insights list-components --resource-group-name my-resource-group
```

List components in an application using AWS Tools for Windows PowerShell

To use the AWS Tools for Windows PowerShell to list the components created on a resource group called `my-resource-group`, use the following command.

```
Get-CWAIComponentList -ResourceGroupName my-resource-group
```

Describe a component

Describe a component using the AWS CLI

You can use the following AWS CLI command to describe a component called `my-component` that belongs to an application created on a resource group called `my-resource-group`.

```
aws application-insights describe-component --resource-group-name my-resource-group --component-name my-component
```
Describe a component using AWS Tools for Windows PowerShell

You can use the following AWS Tools for Windows PowerShell command to describe a component called `my-component` that belongs to an application created on a resource group called `my-resource-group`.

```bash
Get-CWAIComponent -ComponentName my-component -ResourceGroupName my-resource-group
```

Group similar resources into a custom component

We recommend grouping similar resources, such as .NET web server instances, into custom components for easier onboarding and better monitoring and insights. Currently, CloudWatch Application Insights supports custom groups for EC2 instances.

To group resources into a custom component using the AWS CLI

To use the AWS CLI to group three instances (arn:aws:ec2:us-east-1:123456789012:instance/i-11111, arn:aws:ec2:us-east-1:123456789012:instance/i-22222, and arn:aws:ec2:us-east-1:123456789012:instance/i-33333) together into a custom component called `my-component` for an application created for the resource group called `my-resource-group`, use the following command.

```bash
```

To group resources into a custom component using AWS Tools for Windows PowerShell

To use AWS Tools for Windows PowerShell to group three instances (arn:aws:ec2:us-east-1:123456789012:instance/i-11111, arn:aws:ec2:us-east-1:123456789012:instance/i-22222, and arn:aws:ec2:us-east-1:123456789012:instance/i-33333) together into a custom component called `my-component`, for an application created for the resource group called `my-resource-group`, use the following command.

```bash
```

Ungroup a custom component

To ungroup a custom component using the AWS CLI

To use the AWS CLI to ungroup a custom component named `my-component` in an application created on the resource group, `my-resource-group`, use the following command.

```bash
aws application-insights delete-component --resource-group-name my-resource-group --component-name my-new-component
```

To ungroup a custom component using AWS Tools for Windows PowerShell

To use the AWS Tools for Windows PowerShell to ungroup a custom component named `my-component` in an application created on the resource group, `my-resource-group`, use the following command.

```bash
Remove-CWAIComponent -ComponentName my-component -ResourceGroupName my-resource-group
```
Update an application

Update an application using the AWS CLI

You can use the AWS CLI to update an application to generate AWS Systems Manager OpsCenter OpsItems for problems detected with the application, and to associate the created OpsItems to the SNS topic arn:aws:sns:us-east-1:123456789012:MyTopic, using the following command.

```
aws application-insights update-application --resource-group-name my-resource-group --ops-center-enabled --ops-item-sns-topic-arn arn:aws:sns:us-east-1:123456789012:MyTopic
```

Update an application using AWS Tools for Windows PowerShell

You can use the AWS Tools for Windows PowerShell to update an application to generate AWS SSM OpsCenter OpsItems for problems detected with the application, and to associate the created OpsItems to the SNS topic arn:aws:sns:us-east-1:123456789012:MyTopic, using the following command.

```
Update-CWAIAPIApplication -ResourceGroupName my-resource-group -OpsCenterEnabled true -OpsItemSNSTopicArn arn:aws:sns:us-east-1:123456789012:MyTopic
```

Update a custom component

Update a custom component using the AWS CLI

You can use the AWS CLI to update a custom component called my-component with a new component name, my-new-component, and an updated group of instances, by using the following command.

```
```

Update a custom component using AWS Tools for Windows PowerShell

You can use the AWS Tools for Windows PowerShell to update a custom component called my-component with a new component name, my-new-component, and an updated group of instances, by using the following command.

```
```

Manage and update monitoring

You can manage and update monitoring for your Application Insights application using the command line.

Topics

- List problems with your application (p. 564)
- Describe an application problem (p. 564)
- Describe the anomalies or errors associated with a problem (p. 564)
- Describe an anomaly or error with the application (p. 564)
- Describe the monitoring configurations of a component (p. 565)
- Describe the recommended monitoring configuration of a component (p. 565)
- Update the monitoring configurations for a component (p. 566)
- Remove a specified resource group from Application Insights monitoring (p. 566)
List problems with your application

List problems with your application using the AWS CLI

To use the AWS CLI to list problems with your application detected between 1,000 and 10,000 milliseconds since Unix Epoch for an application created on a resource group called `my-resource-group`, use the following command.

```bash
aws application-insights list-problems --resource-group-name my-resource-group --start-time 1000 --end-time 10000
```

List problems with your application using AWS Tools for Windows PowerShell

To use the AWS Tools for Windows PowerShell to list problems with your application detected between 1,000 and 10,000 milliseconds since Unix Epoch for an application created on a resource group called `my-resource-group`, use the following command.

```powershell
$startDate = "8/6/2019 3:33:00"
$endDate = "8/6/2019 3:34:00"
Get-CWAIProblemList -ResourceGroupName my-resource-group -StartTime $startDate -EndTime $endDate
```

Describe an application problem

Describe an application problem using the AWS CLI

To use the AWS CLI to describe a problem with problem id `p-1234567890`, use the following command.

```bash
aws application-insights describe-problem --problem-id p-1234567890
```

Describe an application problem using AWS Tools for Windows PowerShell

To use the AWS Tools for Windows PowerShell to describe a problem with problem id `p-1234567890`, use the following command.

```powershell
Get-CWAIProblem -ProblemId p-1234567890
```

Describe the anomalies or errors associated with a problem

Describe the anomalies or errors associated with a problem using the AWS CLI

To use the AWS CLI to describe the anomalies or errors associated with a problem with problem id `p-1234567890`, use the following command.

```bash
aws application-insights describe-problem-observations --problem-id p-1234567890
```

Describe the anomalies or errors associated with a problem using AWS Tools for Windows PowerShell

To use the AWS Tools for Windows PowerShell to describe the anomalies or errors associated with a problem with problem id `p-1234567890`, use the following command.

```powershell
Get-CWAIProblemObservation -ProblemId p-1234567890
```

Describe an anomaly or error with the application

Describe an anomaly or error with the application using the AWS CLI
To use the AWS CLI to describe an anomaly or error with the application with the observation id `o-1234567890`, use the following command.

```bash
aws application-insights describe-observation --observation-id o-1234567890
```

**Describe an anomaly or error with the application using AWS Tools for Windows PowerShell**

To use the AWS Tools for Windows PowerShell to describe an anomaly or error with the application with the observation id `o-1234567890`, use the following command.

```powershell
Get-CWAIObservation -ObservationId o-1234567890
```

**Describe the monitoring configurations of a component**

**Describe the monitoring configurations of a component using the AWS CLI**

To use the AWS CLI to describe the monitoring configuration of a component called `my-component` in an application created on the resource group `my-resource-group`, use the following command.

```bash
aws application-insights describe-component-configuration --resource-group-name my-resource-group --component-name my-component
```

**Describe the monitoring configurations of a component using AWS Tools for Windows PowerShell**

To use the AWS Tools for Windows PowerShell to describe the monitoring configuration of a component called `my-component`, in an application created on the resource group `my-resource-group`, use the following command.

```powershell
Get-CWAIComponentConfiguration -ComponentName my-component -ResourceGroupName my-resource-group
```

For more information about component configuration and for example JSON files, see Work with component configurations (p. 573).

**Describe the recommended monitoring configuration of a component**

**Describe the recommended monitoring configuration of a component using the AWS CLI**

When the component is part of a .NET Worker application, you can use the AWS CLI to describe the recommended monitoring configuration of a component called `my-component` in an application created on the resource group `my-resource-group`, by using the following command.

```bash
aws application-insights describe-component-configuration-recommendation --resource-group-name my-resource-group --component-name my-component --tier DOT_NET_WORKER
```

**Describe the recommended monitoring configuration of a component using AWS Tools for Windows PowerShell**

When the component is part of a .NET Worker application, you can use the AWS Tools for Windows PowerShell to describe the recommended monitoring configuration of a component called `my-component` in an application created on the resource group `my-resource-group`, by using the following command.

```powershell
Get-CWAIComponentConfigurationRecommendation -ComponentName my-component -ResourceGroupName my-resource-group -Tier DOT_NET_WORKER
```

For more information about component configuration and for example JSON files, see Work with component configurations (p. 573).
Update the monitoring configurations for a component

Update the monitoring configurations for a component using the AWS CLI

To use the AWS CLI to update the component called my-component in an application created on the resource group called my-resource-group, use the following command. The command includes these actions:

1. Enable monitoring for the component.
2. Set the tier of the component to .NET Worker.
3. Update the JSON configuration of the component to read from the local file configuration.txt.

```bash
aws application-insights update-component-configuration --resource-group-name my-resource-group --component-name my-component --tier DOT_NET_WORKER --monitor --component-configuration "file://configuration.txt"
```

Update the monitoring configurations for a component using the AWS Tools for Windows PowerShell

To use the AWS Tools for Windows PowerShell to update the component called my-component in an application created on the resource group called my-resource-group, use the following command. The command includes these actions:

1. Enable monitoring for the component.
2. Set the tier of the component to .NET Worker.
3. Update the JSON configuration of the component to read from the local file configuration.txt.

```powershell
[string]$config = Get-Content -Path configuration.txt
Update-CWAICComponentConfiguration -ComponentName my-component -ResourceGroupName my-resource-group -Tier DOT_NET_WORKER -Monitor 1 -ComponentConfiguration $config
```

For more information about component configuration and for example JSON files, see Work with component configurations (p. 573).

Remove a specified resource group from Application Insights monitoring

Remove a specified resource group from Application Insights monitoring using the AWS CLI

To use the AWS CLI to remove an application created on the resource group called my-resource-group from monitoring, use the following command.

```bash
aws application-insights delete-application --resource-group-name my-resource-group
```

Remove a specified resource group from Application Insights monitoring using the AWS Tools for Windows PowerShell

To use the AWS Tools for Windows PowerShell to remove an application created on the resource group called my-resource-group from monitoring, use the following command.

```powershell
Remove-CWAIAplication -ResourceGroupName my-resource-group
```

Configure monitoring for SQL Always On Availability Groups

1. Create an application for the resource group with the SQL HA EC2 instances.
2. Define the EC2 instances that represent the SQL HA cluster by creating a new application component.

```

3. Configure the SQL HA component.

```bash/aws application-insights update-component-configuration --resource-group-name "<RESOURCE_GROUP_NAME>" --region <REGION> --component-name "SQL_HA_CLUSTER" --monitor #-tier SQL_SERVER_ALWAYSON_AVAILABILITY_GROUP --monitor #--component-configuration '{
  "subComponents": [
    {
      "subComponentType": "AWS::EC2::Instance",
      "alarmMetrics": [
        {
          "alarmMetricName": "CPUUtilization",
          "monitor": true
        },
        {
          "alarmMetricName": "StatusCheckFailed",
          "monitor": true
        },
        {
          "alarmMetricName": "Processor % Processor Time",
          "monitor": true
        },
        {
          "alarmMetricName": "Memory % Committed Bytes In Use",
          "monitor": true
        },
        {
          "alarmMetricName": "Memory Available Mbytes",
          "monitor": true
        },
        {
          "alarmMetricName": "Paging File % Usage",
          "monitor": true
        },
        {
          "alarmMetricName": "System Processor Queue Length",
          "monitor": true
        },
        {
          "alarmMetricName": "Network Interface Bytes Total/sec",
          "monitor": true
        },
        {
          "alarmMetricName": "PhysicalDisk % Disk Time",
          "monitor": true
        },
        {
          "alarmMetricName": "SQLServer:Buffer Manager Buffer cache hit ratio",
          "monitor": true
        },
        {
          "alarmMetricName": "SQLServer:Buffer Manager Page life expectancy",
          "monitor": true
        },
        {
          "alarmMetricName": "SQLServer:General Statistics Processes blocked",
          "monitor": true
        },
        {
          "alarmMetricName": "SQLServer:General Statistics User Connections",
          "monitor": true
        },
        {
          "alarmMetricName": "SQLServer:Locks Number of Deadlocks/sec",
          "monitor": true
        },
        {
          "alarmMetricName": "SQLServer:SQL Statistics Batch Requests/sec",
          "monitor": true
        }
    ]
  }
}'
```
Amazon CloudWatch User Guide
Set up, configure, and manage your application

```
{ "alarmMetricName" : "SQLServer:Database Replica File Bytes Received/sec",
  "monitor" : true
},
{ "alarmMetricName" : "SQLServer:Database Replica Log Bytes Received/sec",
  "monitor" : true
},
{ "alarmMetricName" : "SQLServer:Database Replica Log remaining for undo",
  "monitor" : true
},
{ "alarmMetricName" : "SQLServer:Database Replica Log Send Queue",
  "monitor" : true
},
{ "alarmMetricName" : "SQLServer:Database Replica Mirrored Write Transaction/sec",
  "monitor" : true
},
{ "alarmMetricName" : "SQLServer:Database Replica Recovery Queue",
  "monitor" : true
},
{ "alarmMetricName" : "SQLServer:Database Replica Redo Bytes Remaining",
  "monitor" : true
},
{ "alarmMetricName" : "SQLServer:Database Replica Redone Bytes/sec",
  "monitor" : true
},
{ "alarmMetricName" : "SQLServer:Database Replica Total Log requiring undo",
  "monitor" : true
},
{ "alarmMetricName" : "SQLServer:Database Replica Transaction Delay",
  "monitor" : true
}],
"windowsEvents" : [
  { "logGroupName" : "WINDOWS_EVENTS-Application-<RESOURCE_GROUP_NAME>",
    "eventName" : "Application",
    "eventLevels" : [ "WARNING", "ERROR", "CRITICAL", "INFORMATION" ],
    "monitor" : true
  },
  { "logGroupName" : "WINDOWS_EVENTS-System-<RESOURCE_GROUP_NAME>",
    "eventName" : "System",
    "eventLevels" : [ "WARNING", "ERROR", "CRITICAL" ],
    "monitor" : true
  },
  { "logGroupName" : "WINDOWS_EVENTS-Security-<RESOURCE_GROUP_NAME>",
    "eventName" : "Security",
    "eventLevels" : [ "WARNING", "ERROR", "CRITICAL" ],
    "monitor" : true
  }]
},
"logs" : [
  { "logGroupName" : "SQL_SERVER ALWAYSON_AVAILABILITY_GROUP-<RESOURCE_GROUP_NAME>",
    "logPath" : "C:\Program Files\Microsoft SQL Server\MSSQL**.MSSQLSERVER\MSSQL\Log\ERRORLOG",
    "logType" : "SQL_SERVER",
    "monitor" : true,
    "encoding" : "utf-8"
  }
],
{ "subComponentType" : "AWS::EC2::Volume",
  "alarmMetrics" : [
    { "alarmMetricName" : "VolumeReadBytes",
      "monitor" : true
    },
    { "alarmMetricName" : "VolumeWriteBytes",
      "monitor" : true
    },
    { "alarmMetricName" : "VolumeReadOps",
      "monitor" : true
    }
  ]
```
"alarmMetricName" : "VolumeWriteOps",
    "monitor" : true
  },
  {
    "alarmMetricName" : "VolumeQueueLength",
    "monitor" : true
  },
  {
    "alarmMetricName" : "VolumeThroughputPercentage",
    "monitor" : true
  },
  {
    "alarmMetricName" : "BurstBalance",
    "monitor" : true
  }
]}
}'

Note
Application Insights must ingest Application Event logs (information level) to detect cluster activities such as failover.

Configure monitoring for MySQL RDS

1. Create an application for the resource group with the RDS MySQL database instance.

```bash
aws application-insights create-application #--region <REGION> #--resource-group-name <RESOURCE_GROUP_NAME>
```

2. The error log is enabled by default. The slow query log can be enabled using data parameter groups. For more information, see Accessing the MySQL Slow Query and General Logs.
   
   • set slow_query_log = 1
   • set log_output = FILE

3. Export the logs to be monitored to CloudWatch logs. For more information, see Publishing MySQL Logs to CloudWatch Logs.

4. Configure the MySQL RDS component.

```bash
aws application-insights update-component-configuration #--resource-group-name "<RESOURCE_GROUP_NAME>" #--region <REGION> #--component-name "<DB_COMPONENT_NAME>" #--monitor DEFAULT #--tier DEFAULT #--component-configuration "{"alarmMetrics": [{"alarmMetricName": "CPUUtilization","monitor":true},{"alarmMetricName": "MYSQL","monitor":true},{"alarmMetricName": "MYSQL_SLOW_QUERY","monitor":false}]"
```

Configure monitoring for MySQL EC2

1. Create an application for the resource group with the SQL HA EC2 instances.

```bash
aws application-insights create-application #--region <REGION> #--resource-group-name <RESOURCE_GROUP_NAME>
```

2. The error log is enabled by default. The slow query log can be enabled using data parameter groups. For more information, see Accessing the MySQL Slow Query and General Logs.
   
   • set slow_query_log = 1
   • set log_output = FILE

3. Configure the MySQL EC2 component.

```bash
aws application-insights update-component-configuration #--resource-group-name "<RESOURCE_GROUP_NAME>" #--region <REGION> #--component-name "<DB_COMPONENT_NAME>"
```
Configure monitoring for PostgreSQL RDS

1. Create an application for the resource group with the PostgreSQL RDS database instance.

   ```bash
   aws application-insights create-application --region <REGION> --resource-group-name <RESOURCE_GROUP_NAME>
   ```

2. Publishing PostgreSQL logs to CloudWatch is not enabled by default. To enable monitoring, open the RDS console and select the database to monitor. Choose Modify in the upper right corner, and select the checkbox labeled PostgreSQL log. Choose Continue to save this setting.

3. Your PostgreSQL logs are exported to CloudWatch.

4. Configure the PostgreSQL RDS component.

   ```bash
   aws application-insights update-component-configuration --region <REGION> --resource-group-name <RESOURCE_GROUP_NAME> --component-name <DB_COMPONENT_NAME> --monitor --tier DEFAULT --component-configuration "{
   "alarmMetrics": [
   "{ "alarmMetricName": "CPUUtilization", "monitor": true },
   ],
   "logs": [
   { "logType": "POSTGRESQL", "monitor": true }
   ]
   }"
   ```

Configure monitoring for PostgreSQL EC2

1. Create an application for the resource group with the PostgreSQL EC2 instance.

   ```bash
   aws application-insights create-application --region <REGION> --resource-group-name <RESOURCE_GROUP_NAME>
   ```

2. Configure the PostgreSQL EC2 component.

   ```bash
   aws application-insights update-component-configuration --region <REGION> --resource-group-name <RESOURCE_GROUP_NAME> --component-name <DB_COMPONENT_NAME> --monitor --tier POSTGRESQL --component-configuration "{
   "alarmMetrics": [
   { "alarmMetricName": "CPUUtilization", "monitor": true }
   ]
   }"
   ```
Configure monitoring for Oracle RDS

1. Create an application for the resource group with the Oracle RDS database instance.

   ```bash
   aws application-insights create-application --region <REGION> --resource-group-name <RESOURCE_GROUP_NAME>
   ```

2. Publishing Oracle logs to CloudWatch is not enabled by default. To enable monitoring, open the RDS console and select the database to monitor. Choose Modify in the upper right corner, and select the checkboxes labeled Alert log and Listener log. Choose Continue to save this setting.

3. Your Oracle logs are exported to CloudWatch.

4. Configure the Oracle RDS component.

   ```bash
   aws application-insights update-component-configuration --region <REGION> --resource-group-name <RESOURCE_GROUP_NAME> --component-name <DB_COMPONENT_NAME> --monitor --tier DEFAULT --component-configuration "{
     "alarmMetrics": [
       {
         "alarmMetricName": "CPUUtilization",
         "monitor": true
       }
     ],
     "logs": [
       {
         "logType": "ORACLE_ALERT",
         "monitor": true
       },
       {
         "logType": "ORACLE_LISTENER",
         "monitor": true
       }
     ]
   }
   ```

Configure monitoring for Oracle EC2

1. Create an application for the resource group with the Oracle EC2 instance.

   ```bash
   aws application-insights create-application --region <REGION> --resource-group-name <RESOURCE_GROUP_NAME>
   ```

2. Configure the Oracle EC2 component.

   ```bash
   aws application-insights update-component-configuration --region <REGION> --resource-group-name <RESOURCE_GROUP_NAME> --component-name <DB_COMPONENT_NAME> --monitor --tier ORACLE --component-configuration "{
     "alarmMetrics": [
   ```
Application Insights CloudWatch Events and notifications for detected problems

For each application that is added to CloudWatch Application Insights, a CloudWatch event is published for the following events on a best effort basis:

- **Problem creation.** Emitted when CloudWatch Application Insights detects a new problem.
  - Detail Type: "Application Insights Problem Detected"
  - Detail:
    - problemId: The detected problem ID.
    - region: The AWS Region where the problem was created.
    - resourceGroupName: The Resource Group for the registered application for which the problem was detected.
    - status: The status of the problem.
    - severity: The severity of the problem.
    - problemUrl: The console URL for the problem.

- **Problem update.** Emitted when the problem is updated with a new observation or when an existing observation is updated and the problem is subsequently updated; updates include a resolution or closure of the problem.
  - Detail Type: "Application Insights Problem Updated"
  - Detail:
    - problemId: The created problem ID.
    - region: The AWS Region where the problem was created.
    - resourceGroupName: The Resource Group for the registered application for which the problem was detected.
    - status: The status of the problem.
    - severity: The severity of the problem.
    - problemUrl: The console URL for the problem.
From the CloudWatch console, select Rules under Events in the left navigation pane. From the Rules page, select Create rule. Choose Amazon CloudWatch Application Insights from the Service Name dropdown list and choose the Event Type. Then, choose Add target and select the target and parameters, for example, an SNS topic or Lambda function.

**Actions through AWS Systems Manager.** CloudWatch Application Insights provides built-in integration with Systems Manager OpsCenter. If you choose to use this integration for your application, an OpsItem is created on the OpsCenter console for every problem detected with the application. From the OpsCenter console, you can view summarized information about the problem detected by CloudWatch Application Insights and pick a Systems Manager Automation runbook to take remedial actions or further identify Windows processes that are causing resource issues in your application.

---

**Work with component configurations**

A component configuration is a text file in JSON format that describes the configuration settings of the component. This section provides an example template fragment, descriptions of component configuration sections, and example component configurations.

**Topics**

- Component configuration template fragment (p. 573)
- Component configuration sections (p. 574)
- Component configuration examples (p. 578)

**Component configuration template fragment**

The following example shows a template fragment in JSON format.

```json
{
    "alarmMetrics" : [
        list of alarm metrics
    ],
    "logs" : [
        list of logs
    ],
    "windowsEvents" : [
        list of windows events channels configurations
    ],
    "alarms" : [
        list of CloudWatch alarms
    ],
    "JMXPrometheusExporter": {
        JMX Prometheus Exporter configuration
    }
    "subComponents" : [
        {
            "subComponentType" : "AWS::EC2::Instance" ...
            component nested instances configuration
        },
        {
            "subComponentType" : "AWS::EC2::Volume" ...
            component nested volumes configuration
        }
    ]
}
```
Component configuration sections

A component configuration includes several major sections. Sections in a component configuration can be listed in any order.

- **alarmMetrics (optional)**
  A list of metrics (p. 575) to monitor for the component. All component types can have an alarmMetrics section.

- **logs (optional)**
  A list of logs (p. 575) to monitor for the component. Only EC2 instances can have a logs section.

- **subComponents (optional)**
  Nested instance and volume subComponent configuration for the component. The following types of components can have nested instances and a subComponents section: ELB, ASG, custom-grouped EC2 instances, and EC2 instances.

- **alarms (optional)**
  A list of alarms (p. 577) to monitor for the component. All component types can have an alarm section.

- **windowsEvents (optional)**
  A list of windows events (p. 577) to monitor for the component. Only Windows on EC2 instances have a windowsEvents section.

- **JMXPrometheusExporter (optional)**
  JMXPrometheus Exporter configuration.

The following example shows the syntax for the subComponents section fragment in JSON format.

```json
[
  {
    "subComponentType" : "AWS::EC2::Instance",
    "alarmMetrics" : [
      "list of alarm metrics"
    ],
    "logs" : [
      "list of logs"
    ],
    "windowsEvents" : [
      "list of windows events channels configurations"
    ]
  },
  {
    "subComponentType" : "AWS::EC2::Volume",
    "alarmMetrics" : [
      "list of alarm metrics"
    ]
  }
]
```

Component configuration section properties

This section describes the properties of each component configuration section.

Sections
Metric

Defines a metric to be monitored for the component.

**JSON**

```json
{
    "alarmMetricName": "monitoredMetricName",
    "monitor": true/false
}
```

**Properties**

- **alarmMetricName (required)**
  
The name of the metric to be monitored for the component. For metrics supported by Application Insights, see Logs and metrics supported by Amazon CloudWatch Application Insights (p. 615).

- **monitor (optional)**
  
  Boolean to indicate whether to monitor the metric. The default value is `true`.

Log

Defines a log to be monitored for the component.

**JSON**

```json
{
    "logGroupName": "logGroupName",
    "logPath": "logPath",
    "logType": "logType",
    "encoding": "encodingType",
    "monitor": true/false
}
```

**Properties**

- **logGroupName (required)**
  
The CloudWatch log group name to be associated to the monitored log. For the log group name constraints, see `CreateLogGroup`.

- **logPath (required for EC2 instance components; not required for components that do not use CloudWatch Agent, such as AWS Lambda)**
  
The path of the logs to be monitored. The log path must be an absolute Windows system file path. For more information, see `CloudWatch Agent Configuration File: Logs Section`.

- **logType (required)**
The log type decides the log patterns against which Application Insights analyzes the log. The log type is selected from the following:

- SQL_SERVER
- SQL_SERVER_ALWAYSON_AVAILABILITY_GROUP
- MYSQL
- MYSQL_SLOW_QUERY
- POSTGRESQL
- WINDOWS_EVENTS
- STEP_FUNCTION
- IIS
- APPLICATION
- DEFAULT
- CUSTOM
- ORACLE_ALERT
- ORACLE_LISTENER

- encoding (optional)

The type of encoding of the logs to be monitored. The specified encoding should be included in the list of CloudWatch agent supported encodings. If not provided, CloudWatch Application Insights uses the default encoding type for the log type:

- For MYSQL/POSTGRESQL/WINDOWS_EVENTS/SQL_SERVER_ALWAYSON_AVAILABILITY_GROUP/APLICATION/DEFAULT: utf-8 encoding
- For SQL_SERVER: utf-16 encoding
- For IIS: ascii encoding

- monitor (optional)

Boolean that indicates whether to monitor the logs. The default value is true.

### JMX Prometheus Exporter

Defines the JMX Prometheus Exporter settings.

**JSON**

```
"jmxPrometheusExporter": {
   "jmxURL" : "JMX URL",
   "hostPort" : "The host and port",
   "prometheusPort" : "Target port to emit Prometheus metrics"
}
```

**Properties**

- jmxURL (optional)

  A complete JMX URL to connect to.

- hostPort (optional)

  The host and port to connect to through remote JMX. Only one of jmxURL and hostPort can be specified.

- prometheusPort (optional)
The target port to send Prometheus metrics to. If not specified, the default port 9404 is used.

Windows Events

Defines Windows Events to log.

JSON

```
{
    "logGroupName" : "logGroupName",
    "eventName" : "eventName",
    "eventLevels" : ["ERROR","WARNING","CRITICAL","INFORMATION","VERBOSE"],
    "monitor" : true/false
}
```

Properties

- **logGroupName (required)**
  The CloudWatch log group name to be associated to the monitored log. For the log group name constraints, see CreateLogGroup.

- **eventName (required)**
  The type of Windows Events to log. It is equivalent to the Windows Event log channel name. For example, System, Security, CustomEventName, etc. This field is required for each type of Windows event to log.

- **eventLevels (required)**
  The levels of event to log. You must specify each level to log. Possible values include INFORMATION, WARNING, ERROR, CRITICAL, and VERBOSE. This field is required for each type of Windows Event to log.

- **monitor (optional)**
  Boolean that indicates whether to monitor the logs. The default value is true.

Alarm

Defines a CloudWatch alarm to be monitored for the component.

JSON

```
{
    "alarmName" : "monitoredAlarmName",
    "severity" : HIGH/MEDIUM/LOW
}
```

Properties

- **alarmName (required)**
  The name of the CloudWatch alarm to be monitored for the component.

- **severity (optional)**
  Indicates the degree of outage when the alarm goes off.
Component configuration examples

The following examples show component configurations in JSON format for relevant services.

Example component configurations

- Amazon Elastic Compute Cloud (EC2) instance (p. 578)
- Amazon Relational Database Service instance (p. 579)
- Amazon Relational Database Service (RDS) Aurora MySQL (p. 580)
- Elastic Load Balancing (ELB) (p. 580)
- Application Elastic Load Balancing (p. 581)
- Amazon EC2 Auto Scaling (ASG) (p. 582)
- Amazon Simple Queue Service (SQS) (p. 583)
- Customer grouped EC2 instances (p. 583)
- AWS Lambda Function (p. 584)
- Amazon DynamoDB table (p. 584)
- SQL Always On Availability Group (p. 585)
- RDS MySQL (p. 587)
- RDS PostgreSQL (p. 587)
- Amazon S3 bucket (p. 587)
- AWS Step Functions (p. 588)
- API Gateway REST API stages (p. 588)
- Java (p. 588)
- RDS Oracle (p. 589)
- Amazon Elastic Container Service (Amazon ECS) (p. 589)
- Amazon ECS service (p. 592)
- Amazon ECS task (p. 594)
- Amazon EKS cluster (p. 595)
- Kubernetes on Amazon EC2 (p. 597)

Amazon Elastic Compute Cloud (EC2) instance

```json
{
    "alarmMetrics" : [
        {
            "alarmMetricName" : "CPUUtilization",
            "monitor" : true
        },
        {
            "alarmMetricName" : "StatusCheckFailed"
        }
    ],
    "logs" : [
        {
            "logGroupName" : "my_log_group",
            "logPath" : "C:\\LogFolder\\**",
            "logType" : "APPLICATION",
            "monitor" : true
        },
        {
            "logGroupName" : "my_log_group_2",
```
Example configurations for relevant services

Amazon CloudWatch User Guide

```
{
    "logPath" : "C:\\LogFolder2\\*",
    "logType" : "IIS",
    "encoding" : "utf-8"
}
},
"windowsEvents" : [
{
    "logGroupName" : "my_log_group_3",
    "eventName" : "Application",
    "eventLevels" : [ "ERROR", "WARNING", "CRITICAL" ],
    "monitor" : true
},
    "logGroupName" : "my_log_group_4",
    "eventName" : "System",
    "eventLevels" : [ "ERROR", "WARNING", "CRITICAL" ],
    "monitor" : true
],
"alarms" : [
{
    "alarmName" : "my_instance_alarm_1",
    "severity" : "HIGH"
},
   { "alarmName" : "my_instance_alarm_2",
    "severity" : "LOW"
}]
"subComponents" : [
{
    "subComponentType" : "AWS::EC2::Volume",
    "alarmMetrics" : [
        { "alarmMetricName" : "VolumeQueueLength",
            "monitor" : "true"
        },
        { "alarmMetricName" : "VolumeThroughputPercentage",
            "monitor" : "true"
        },
        { "alarmMetricName" : "BurstBalance",
            "monitor" : "true"
        }
    ]
}]
}
```

Amazon Relational Database Service instance

```
{
    "alarmMetrics" : [
        { "alarmMetricName" : "BurstBalance",
            "monitor" : true
        },
        { "alarmMetricName" : "WriteThroughput",
            "monitor" : false
        }
    ],
    "alarms" : [
        { "alarmName" : "my_rds_instance_alarm",
            "severity" : "MEDIUM"
        }
    ]
}]
```
Amazon Relational Database Service (RDS) Aurora MySQL

```json
{
  "alarmMetrics": [
    {
      "alarmMetricName": "CPUUtilization",
      "monitor": true
    },
    {
      "alarmMetricName": "CommitLatency",
      "monitor": true
    }
  ],
  "logs": [
    {
      "logType": "MYSQL",
      "monitor": true,
    },
    {
      "logType": "MYSQL_SLOW_QUERY",
      "monitor": false
    }
  ]
}
```

Elastic Load Balancing (ELB)

```json
{
  "alarmMetrics": [
    {
      "alarmMetricName" : "EstimatedALBActiveConnectionCount",
      },
    {
      "alarmMetricName" : "HTTPCode_Backend_5XX"
    }
  ],
  "subComponents": [
    {
      "subComponentType" : "AWS::EC2::Instance",
      "alarmMetrics" : [
        {
          "alarmMetricName" : "CPUUtilization",
        },
        {
          "alarmMetricName" : "StatusCheckFailed"
        }
      ],
      "logs" : [
        {
          "logGroupName" : "my_log_group",
          "logPath" : "C:\\LogFolder\*",
          "logType" : "APPLICATION",
        }
      ],
      "windowsEvents" : [
        {
          "logGroupName" : "my_log_group_2",
          "eventName" : "Application",
          "eventLevels" : [ "ERROR", "WARNING", "CRITICAL" ],
          "monitor" : true
        }
      ]
    }
  ]
}
```
Example configurations for relevant services

Application Elastic Load Balancing

```json
{
    "alarmMetrics": [
        {
            "alarmMetricName": "ActiveConnectionCount",
            "alarmMetrics": [
                {
                    "alarmMetricName": "CPUUtilization",
                    "alarmMetricName": "TargetResponseTime"
                }
            ],
            "logs": [
                {
                    "logGroupName": "my_log_group",
                    "logPath": "C:\\LogFolder\*",
                    "logType": "APPLICATION"
                }
            ],
            "windowsEvents": [
                {
                    "logGroupName": "my_log_group_2",
                    "eventName": "Application",
                    "eventLevels": ["ERROR", "WARNING", "CRITICAL"]
                }
            ]
    }
}
```

581
Amazon EC2 Auto Scaling (ASG)

{
  "alarmMetrics" : [
    { "alarmMetricName" : "CPUCreditBalance" },
    { "alarmMetricName" : "EBSIOBalance%" }
  ],
  "subComponents" : [
    { "subComponentType" : "AWS::EC2::Instance",
      "alarmMetrics" : [
        { "alarmMetricName" : "CPUUtilization" },
        { "alarmMetricName" : "StatusCheckFailed" }
      ],
      "logs" : [
        { "logGroupName" : "my_log_group",
          "logPath" : "C:\LogFolder\*",
          "logType" : "APPLICATION"
        }
      ],
      "windowsEvents" : [
        { "logGroupName" : "my_log_group_2",
          "eventName" : "Application",
          "eventLevels" : [ "ERROR", "WARNING", "CRITICAL" ]
        }
      ]
    },
    { "subComponentType" : "AWS::EC2::Volume",
      "alarmMetrics" : [
        { "alarmMetricName" : "VolumeQueueLength" },
        { "alarmMetricName" : "BurstBalance" }
      ]
    }
  ],
  "alarms" : [
    { "alarmName" : "my_asg_alarm",
      "severity" : "LOW" }
  ]
}
Amazon Simple Queue Service (SQS)

```json
{
  "alarmMetrics": [
    {
      "alarmMetricName": "ApproximateAgeOfOldestMessage"
    },
    {
      "alarmMetricName": "NumberOfEmptyReceives"
    }
  ],
  "alarms": [
    {
      "alarmName": "my_sqs_alarm",
      "severity": "MEDIUM"
    }
  ]
}
```

Customer grouped EC2 instances

```json
{
  "subComponents": [
    {
      "subComponentType": "AWS::EC2::Instance",
      "alarmMetrics": [
        {
          "alarmMetricName": "CPUUtilization",
        },
        {
          "alarmMetricName": "StatusCheckFailed"
        }
      ],
      "logs": [
        {
          "logGroupName": "my_log_group",
          "logPath": "C:\LogFolder\*",
          "logType": "APPLICATION"
        }
      ],
      "windowsEvents": [
        {
          "logGroupName": "my_log_group_2",
          "eventName": "Application",
          "eventLevels": ["ERROR", "WARNING", "CRITICAL"]
        }
      ]
    },
    {
      "subComponentType": "AWS::EC2::Volume",
      "alarmMetrics": [
        {
          "alarmMetricName": "VolumeQueueLength"
        },
        {
          "alarmMetricName": "BurstBalance"
        }
      ]
    }
  ],
  "alarms": [
    {
      "alarmName": "my_alarm",
      "severity": "MEDIUM"
    }
  ]
}
```
AWS Lambda Function

```json
{
  "alarmMetrics": [
    {
      "alarmMetricName": "Errors",
      "monitor": true
    },
    {
      "alarmMetricName": "Throttles",
      "monitor": true
    },
    {
      "alarmMetricName": "IteratorAge",
      "monitor": true
    },
    {
      "alarmMetricName": "Duration",
      "monitor": true
    }
  ],
  "logs": [
    {
      "logType": "DEFAULT",
      "monitor": true
    }
  ]
}
```

Amazon DynamoDB table

```json
{
  "alarmMetrics": [
    {
      "alarmMetricName": "SystemErrors",
      "monitor": false
    },
    {
      "alarmMetricName": "UserErrors",
      "monitor": false
    },
    {
      "alarmMetricName": "ConsumedReadCapacityUnits",
      "monitor": false
    },
    {
      "alarmMetricName": "ConsumedWriteCapacityUnits",
      "monitor": false
    },
    {
      "alarmMetricName": "ReadThrottleEvents",
      "monitor": false
    },
    {
      "alarmMetricName": "WriteThrottleEvents",
      "monitor": false
    },
    {
      "alarmMetricName": "ConditionalCheckFailedRequests",
      "monitor": false
    }
  ]
}
```
Example configurations for relevant services

SQL Always On Availability Group

```json
{
    "subComponents" : [ {
        "subComponentType" : "AWS::EC2::Instance",
        "alarmMetrics" : [ {
            "alarmMetricName" : "CPUUtilization",
            "monitor" : true
        }, {
            "alarmMetricName" : "StatusCheckFailed",
            "monitor" : true
        }, {
            "alarmMetricName" : "Processor % Processor Time",
            "monitor" : true
        }, {
            "alarmMetricName" : "Memory % Committed Bytes In Use",
            "monitor" : true
        }, {
            "alarmMetricName" : "Memory Available Mbytes",
            "monitor" : true
        }, {
            "alarmMetricName" : "Paging File % Usage",
            "monitor" : true
        }, {
            "alarmMetricName" : "System Processor Queue Length",
            "monitor" : true
        }, {
            "alarmMetricName" : "Network Interface Bytes Total/sec",
            "monitor" : true
        }, {
            "alarmMetricName" : "PhysicalDisk % Disk Time",
            "monitor" : true
        }, {
            "alarmMetricName" : "SQLServer:Buffer Manager Buffer cache hit ratio",
            "monitor" : true
        }, {
            "alarmMetricName" : "SQLServer:Buffer Manager Page life expectancy",
            "monitor" : true
        }, {
            "alarmMetricName" : "SQLServer:General Statistics Processes blocked",
            "monitor" : true
        }, {
            "alarmMetricName" : "SQLServer:General Statistics User Connections",
            "monitor" : true
        }, {
            "alarmMetricName" : "SQLServer:Locks Number of Deadlocks/sec",
            "monitor" : true
        }, {
            "alarmMetricName" : "SQLServer:SQL Statistics Batch Requests/sec",
            "monitor" : true
        }, {
            "alarmMetricName" : "SQLServer:Database Replica File Bytes Received/sec",
            "monitor" : true
        }, {
            "alarmMetricName" : "SQLServer:Database Replica Log Bytes Received/sec",
            "monitor" : true
        }
    ]
}
```
Example configurations for relevant services

```
"monitor": true,
"alarmMetricName": "SQLServer:Database Replica Log remaining for undo",
"monitor": true,
"alarmMetricName": "SQLServer:Database Replica Log Send Queue",
"monitor": true,
"alarmMetricName": "SQLServer:Database Replica Mirrored Write Transaction/sec",
"monitor": true,
"alarmMetricName": "SQLServer:Database Replica Recovery Queue",
"monitor": true,
"alarmMetricName": "SQLServer:Database Replica Redo Bytes Remaining",
"monitor": true,
"alarmMetricName": "SQLServer:Database Replica Redone Bytes/sec",
"monitor": true,
"alarmMetricName": "SQLServer:Database Replica Total Log requiring undo",
"monitor": true,
"alarmMetricName": "SQLServer:Database Replica Transaction Delay",
"monitor": true
],
"windowsEvents": [
{ "logGroupName": "WINDOWS_EVENTS-Application-<RESOURCE_GROUP_NAME>",
"eventName": "Application",
"eventLevels": ["WARNING", "ERROR", "CRITICAL", "INFORMATION" ],
"monitor": true
},
{ "logGroupName": "WINDOWS_EVENTS-System-<RESOURCE_GROUP_NAME>",
"eventName": "System",
"eventLevels": ["WARNING", "ERROR", "CRITICAL" ],
"monitor": true
},
{ "logGroupName": "WINDOWS_EVENTS-Security-<RESOURCE_GROUP_NAME>",
"eventName": "Security",
"eventLevels": ["WARNING", "ERROR", "CRITICAL" ],
"monitor": true
}],
"logs": [
{ "logGroupName": "SQL_SERVER_ALWAYSON_AVAILABILITY_GROUP-<RESOURCE_GROUP_NAME>",
"logPath": "C:\Program Files\Microsoft SQL Server\MSSQL*.MSSQLSERVER\MSSQL\Log \ERRORLOG",
"logType": "SQL_SERVER",
"monitor": true,
"encoding": "utf-8"
}]
},
{ "subComponentType": "AWS::EC2::Volume",
"alarmMetrics": [
 { "alarmMetricName": "VolumeReadBytes",
"monitor": true
},
 { "alarmMetricName": "VolumeWriteBytes",
"monitor": true
},
 { "alarmMetricName": "VolumeReadOps",
"monitor": true
},
 { "alarmMetricName": "VolumeWriteOps",
"monitor": true
},
 { "alarmMetricName": "VolumeQueueLength",
"monitor": true
}]
```
Example configurations for relevant services

```json

RDS MySQL

{
    "alarmMetrics": [
        {
            "alarmMetricName": "CPUUtilization",
            "monitor": true
        }
    ],
    "logs": [
        {
            "logType": "MYSQL",
            "monitor": true
        },
        {
            "logType": "MYSQL_SLOW_QUERY",
            "monitor": false
        }
    ]
}

RDS PostgreSQL

{
    "alarmMetrics": [
        {
            "alarmMetricName": "CPUUtilization",
            "monitor": true
        }
    ],
    "logs": [
        {
            "logType": "POSTGRESQL",
            "monitor": true
        }
    ]
}

Amazon S3 bucket

{
    "alarmMetrics": [
        {
            "alarmMetricName": "ReplicationLatency",
            "monitor": true
        },
        {
            "alarmMetricName": "5xxErrors",
            "monitor": true
        },
        {
            "alarmMetricName": "VolumeThroughputPercentage",
            "monitor": true
        },
        {
            "alarmMetricName": "BurstBalance",
            "monitor": true
        }
    ]
}
```
Example configurations for relevant services

```
    "alarmMetricName" : "BytesDownloaded",
    "monitor" : true
  }
}

AWS Step Functions

```

{  
  "alarmMetrics": [  
    {  
      "alarmMetricName": "ExecutionsFailed",
      "monitor": true  
    },  
    {  
      "alarmMetricName": "LambdaFunctionsFailed",
      "monitor": true  
    },  
    {  
      "alarmMetricName": "ProvisionedRefillRate",
      "monitor": true  
    }  
  ],  
  "logs": [  
    {  
      "logGroupName": "/aws/states/HelloWorld-Logs",
      "logType": "STEP_FUNCTION",
      "monitor": true,  
    }  
  ]
}

API Gateway REST API stages

```

{  
  "alarmMetrics" : [  
    {  
      "alarmMetricName" : "4XXError",
      "monitor" : true  
    },  
    {  
      "alarmMetricName" : "5XXError",
      "monitor" : true  
    }  
  ],  
  "logs" : [  
    {  
      "logType" : "API_GATEWAY_EXECUTION",
      "monitor" : true  
    },  
    {  
      "logType" : "API_GATEWAY_ACCESS",
      "monitor" : true  
    }  
  ]
}

Java

```

{  

```
"alarmMetrics": [ {
    "alarmMetricName": "java_lang_threading_threadcount",
    "monitor": true
  },
  {
    "alarmMetricName": "java_lang_memory_heapmemoryusage_used",
    "monitor": true
  },
  {
    "alarmMetricName": "java_lang_memory_heapmemoryusage_committed",
    "monitor": true
  }],
"logs": [ ],
"JMXPrometheusExporter": { 
  "hostPort":"8686",
  "prometheusPort":"9404" 
}

**Note**
Application Insights does not support configuring authentication for Prometheus JMX exporter. For information about how to set up authentication, see the Prometheus JMX exporter example configuration.

**RDS Oracle**

```json
{
  "alarmMetrics": [ 
    { 
      "alarmMetricName": "CPUUtilization",
      "monitor": true
    }],
  "logs": [ 
    { 
      "logType": "ORACLE_ALERT",
      "monitor": true,
    },
    { 
      "logType": "ORACLE_LISTENER",
      "monitor": false
    }
  ]
}
```

**Amazon Elastic Container Service (Amazon ECS)**

```json
{
  "alarmMetrics": [ 
    { 
      "alarmMetricName": "CpuUtilized",
      "monitor": true
    },
    { 
      "alarmMetricName": "MemoryUtilized",
      "monitor": true
    },
    { 
      "alarmMetricName": "NetworkRxBytes",
      "monitor": true
    }
  ]
}
```
Example configurations for relevant services

```json
{
  "alarmMetricName": "NetworkTxBytes",
  "monitor": true
},
{
  "alarmMetricName": "RunningTaskCount",
  "monitor": true
},
{
  "alarmMetricName": "PendingTaskCount",
  "monitor": true
},
{
  "alarmMetricName": "StorageReadBytes",
  "monitor": true
},
{
  "alarmMetricName": "StorageWriteBytes",
  "monitor": true
},
"logs": [
{
  "logGroupName": "/ecs/my-task-definition",
  "logType": "APPLICATION",
  "monitor": true
}
],
"subComponents": [
{
  "subComponentType": "AWS::ElasticLoadBalancing::LoadBalancer",
  "alarmMetrics": [
    {
      "alarmMetricName": "HTTPCode_Backend_4XX",
      "monitor": true
    },
    {
      "alarmMetricName": "HTTPCode_Backend_5XX",
      "monitor": true
    },
    {
      "alarmMetricName": "Latency",
      "monitor": true
    },
    {
      "alarmMetricName": "SurgeQueueLength",
      "monitor": true
    },
    {
      "alarmMetricName": "UnHealthyHostCount",
      "monitor": true
    }
  ]
},
{
  "subComponentType": "AWS::ElasticLoadBalancingV2::LoadBalancer",
  "alarmMetrics": [
    {
      "alarmMetricName": "HTTPCode_Target_4XX_Count",
      "monitor": true
    },
    {
      "alarmMetricName": "HTTPCode_Target_5XX_Count",
      "monitor": true
    },
    {
      "alarmMetricName": "HTTPCode_Target_5xx_Count",
      "monitor": true
    }
  ]
}
]}
```
Example configurations for relevant services

```json
{
  "subComponentType": "AWS::EC2::Instance",
  "alarmMetrics": [
    {
      "alarmMetricName": "CPUUtilization",
      "monitor": true
    },
    {
      "alarmMetricName": "StatusCheckFailed",
      "monitor": true
    },
    {
      "alarmMetricName": "disk_used_percent",
      "monitor": true
    },
    {
      "alarmMetricName": "mem_used_percent",
      "monitor": true
    }
  ],
  "logs": [
    {
      "logGroupName": "my_log_group",
      "logPath": "mylog/path",
      "logType": "APPLICATION",
      "monitor": true
    }
  ],
  "windowsEvents": [
    {
      "logGroupName": "my_log_group_2",
      "eventName": "Application",
      "eventLevels": [
        "ERROR",
        "WARNING",
        "CRITICAL"
      ],
      "monitor": true
    }
  ]
}

{
  "subComponentType": "AWS::EC2::Volume",
  "alarmMetrics": [
    {
      "alarmMetricName": "VolumeQueueLength",
      "monitor": "true"
    },
    {
      "alarmMetricName": "VolumeThroughputPercentage",
      "monitor": "true"
    },
    {
      "alarmMetricName": "BurstBalance",
      "monitor": "true"
    }
  ]
}
```
Example configurations for relevant services

**Note**

- The `subComponents` section of `AWS::EC2::Instance` and `AWS::EC2::Volume` applies only to Amazon ECS clusters with ECS service or ECS task running on the EC2 launch type.
- The `windowsEvents` section of `AWS::EC2::Instance` in `subComponents` applies only to Windows running on Amazon EC2 instances.

**Amazon ECS service**

```json
{
  "alarmMetrics": [  
    {  
      "alarmMetricName": "CPUUtilization",
      "monitor": true
    },
    {  
      "alarmMetricName": "MemoryUtilization",
      "monitor": true
    },
    {  
      "alarmMetricName": "CpuUtilized",
      "monitor": true
    },
    {  
      "alarmMetricName": "MemoryUtilized",
      "monitor": true
    },
    {  
      "alarmMetricName": "NetworkRxBytes",
      "monitor": true
    },
    {  
      "alarmMetricName": "NetworkTxBytes",
      "monitor": true
    },
    {  
      "alarmMetricName": "RunningTaskCount",
      "monitor": true
    },
    {  
      "alarmMetricName": "PendingTaskCount",
      "monitor": true
    },
    {  
      "alarmMetricName": "StorageReadBytes",
      "monitor": true
    },
    {  
      "alarmMetricName": "StorageWriteBytes",
      "monitor": true
    }  
  ],
  "logs": [  
    {  
      "logGroupName": "/ecs/my-task-definition",
      "logType": "APPLICATION",
      "monitor": true
    }
  ]
}```
Example configurations for relevant services

```
], "subComponents": [
  {
    "subComponentType": "AWS::ElasticLoadBalancing::LoadBalancer",
    "alarmMetrics": [
      { "alarmMetricName": "HTTPCode_Backend_4XX",
        "monitor": true },
      { "alarmMetricName": "HTTPCode_Backend_5XX",
        "monitor": true },
      { "alarmMetricName": "Latency",
        "monitor": true },
      { "alarmMetricName": "SurgeQueueLength",
        "monitor": true },
      { "alarmMetricName": "UnHealthyHostCount",
        "monitor": true }
    ]
  },
  {
    "subComponentType": "AWS::ElasticLoadBalancingV2::LoadBalancer",
    "alarmMetrics": [
      { "alarmMetricName": "HTTPCode_Target_4XX_Count",
        "monitor": true },
      { "alarmMetricName": "HTTPCode_Target_5XX_Count",
        "monitor": true },
      { "alarmMetricName": "TargetResponseTime",
        "monitor": true },
      { "alarmMetricName": "UnHealthyHostCount",
        "monitor": true }
    ]
  },
  {
    "subComponentType": "AWS::EC2::Instance",
    "alarmMetrics": [
      { "alarmMetricName": "CPUUtilization",
        "monitor": true },
      { "alarmMetricName": "StatusCheckFailed",
        "monitor": true },
      { "alarmMetricName": "disk_used_percent",
        "monitor": true },
      { "alarmMetricName": "mem_used_percent",
        "monitor": true }
    ]
  }
],
```

Example configurations for relevant services

```json
{
  "logs": [
    {
      "logGroupName": "my_log_group",
      "logPath": "/mylog/path",
      "logType": "APPLICATION",
      "monitor": true
    }
  ],
  "windowsEvents": [
    {
      "logGroupName": "my_log_group_2",
      "eventName": "Application",
      "eventLevels": [
        "ERROR",
        "WARNING",
        "CRITICAL"
      ],
      "monitor": true
    }
  ],
  "subComponentType": "AWS::EC2::Volume",
  "alarmMetrics": [
    {
      "alarmMetricName": "VolumeQueueLength",
      "monitor": true
    },
    {
      "alarmMetricName": "VolumeThroughputPercentage",
      "monitor": true
    },
    {
      "alarmMetricName": "BurstBalance",
      "monitor": true
    }
  ]
}
```

**Note**

- The `subComponents` section of `AWS::EC2::Instance` and `AWS::EC2::Volume` applies only to Amazon ECS running on the EC2 launch type.
- The `windowsEvents` section of `AWS::EC2::Instance` in `subComponents` applies only to Windows running on Amazon EC2 instances.

**Amazon ECS task**

```json
{
  "logs": [
    {
      "logGroupName": "/ecs/my-task-definition",
      "logType": "APPLICATION",
      "monitor": true
    }
  ]
}
```
Amazon EKS cluster

```json
{
    "alarmMetrics": [
        {
            "alarmMetricName": "cluster_failed_node_count",
            "monitor": true
        },
        {
            "alarmMetricName": "node_cpu_reserved_capacity",
            "monitor": true
        },
        {
            "alarmMetricName": "node_cpu_utilization",
            "monitor": true
        },
        {
            "alarmMetricName": "node_filesystem_utilization",
            "monitor": true
        },
        {
            "alarmMetricName": "node_memory_reserved_capacity",
            "monitor": true
        },
        {
            "alarmMetricName": "node_memory_utilization",
            "monitor": true
        },
        {
            "alarmMetricName": "node_network_total_bytes",
            "monitor": true
        },
        {
            "alarmMetricName": "pod_cpu_reserved_capacity",
            "monitor": true
        },
        {
            "alarmMetricName": "pod_cpu_utilization",
            "monitor": true
        },
        {
            "alarmMetricName": "pod_cpu_utilization_over_pod_limit",
            "monitor": true
        },
        {
            "alarmMetricName": "pod_memory_reserved_capacity",
            "monitor": true
        },
        {
            "alarmMetricName": "pod_memory_utilization",
            "monitor": true
        },
        {
            "alarmMetricName": "pod_memory_utilization_over_pod_limit",
            "monitor": true
        },
        {
            "alarmMetricName": "pod_network_rx_bytes",
            "monitor": true
        },
        {
            "alarmMetricName": "pod_network_tx_bytes",
            "monitor": true
        }
    ]
}```
Example configurations for relevant services

```
{
  "logs": [
    {
      "logGroupName": "/aws/containerinsights/kubernetes/application",
      "logType": "APPLICATION",
      "monitor": true,
      "encoding": "utf-8"
    }
  ],
  "subComponents": [
    {
      "subComponentType": "AWS::EC2::Instance",
      "alarmMetrics": [
        {
          "alarmMetricName": "CPUUtilization",
          "monitor": true
        },
        {
          "alarmMetricName": "StatusCheckFailed",
          "monitor": true
        },
        {
          "alarmMetricName": "disk_used_percent",
          "monitor": true
        },
        {
          "alarmMetricName": "mem_used_percent",
          "monitor": true
        }
      ],
      "logs": [
        {
          "logGroupName": "APPLICATION-KubernetesClusterOnEC2-IAD",
          "logPath": "",
          "logType": "APPLICATION",
          "monitor": true,
          "encoding": "utf-8"
        }
      ],
      "windowsEvents": [
        {
          "logGroupName": "my_log_group_2",
          "eventName": "Application",
          "eventLevels": [
            "ERROR",
            "WARNING",
            "CRITICAL"
          ],
          "monitor": true
        }
      ]
    },
    {
      "subComponentType": "AWS::AutoScaling::AutoScalingGroup",
      "alarmMetrics": [
        {
          "alarmMetricName": "CPUCreditBalance",
          "monitor": true
        },
        {
          "alarmMetricName": "EBSIOBalance%",
          "monitor": true
        }
      ]
    }
  ]
}
```
Amazon CloudWatch User Guide
Example configurations for relevant services

```
"subComponentType":"AWS::EC2::Volume",
"alarmMetrics":[
  {
    "alarmMetricName":"VolumeReadBytes",
    "monitor":true
  },
  {
    "alarmMetricName":"VolumeWriteBytes",
    "monitor":true
  },
  {
    "alarmMetricName":"VolumeReadOps",
    "monitor":true
  },
  {
    "alarmMetricName":"VolumeWriteOps",
    "monitor":true
  },
  {
    "alarmMetricName":"VolumeQueueLength",
    "monitor":true
  },
  {
    "alarmMetricName":"BurstBalance",
    "monitor":true
  }
]
```

Note

- The `subComponents` section of `AWS::EC2::Instance`, `AWS::EC2::Volume`, and `AWS::AutoScaling::AutoScalingGroup` applies only to Amazon EKS cluster running on the EC2 launch type.
- The `windowsEvents` section of `AWS::EC2::Instance` in `subComponents` applies only to Windows running on Amazon EC2 instances.

Kubernetes on Amazon EC2

```
{ "alarmMetrics":[
  {
    "alarmMetricName":"cluster_failed_node_count",
    "monitor":true
  },
  {
    "alarmMetricName":"node_cpu_reserved_capacity",
    "monitor":true
  },
  {
    "alarmMetricName":"node_cpu_utilization",
    "monitor":true
  },
  {
    "alarmMetricName":"node_filesystem_utilization",
    "monitor":true
  },
  {
    "alarmMetricName":"node_memory_reserved_capacity",
    "monitor":true
  }
]}
```
Example configurations for relevant services

},
{  "alarmMetricName":"node_memory_utilization",
   "monitor":true
},
{  "alarmMetricName":"node_network_total_bytes",
   "monitor":true
},
{  "alarmMetricName":"pod_cpu_reserved_capacity",
   "monitor":true
},
{  "alarmMetricName":"pod_cpu_utilization",
   "monitor":true
},
{  "alarmMetricName":"pod_cpu_utilization_over_pod_limit",
   "monitor":true
},
{  "alarmMetricName":"pod_memory_reserved_capacity",
   "monitor":true
},
{  "alarmMetricName":"pod_memory_utilization",
   "monitor":true
},
{  "alarmMetricName":"pod_memory_utilization_over_pod_limit",
   "monitor":true
},
{  "alarmMetricName":"pod_network_rx_bytes",
   "monitor":true
},
{  "alarmMetricName":"pod_network_tx_bytes",
   "monitor":true
}
],
"logs":[
{  "logGroupName":"/aws/containerinsights/kubernetes/application",
   "logType":"APPLICATION",
   "monitor":true,
   "encoding":"utf-8"
}
],
"subComponents":[
{  "subComponentType":"AWS::EC2::Instance",
   "alarmMetrics":[
   {  "alarmMetricName":"CPUUtilization",
      "monitor":true
   },
   {  "alarmMetricName":"StatusCheckFailed",
      "monitor":true
   },
   {  "alarmMetricName":"disk_used_percent",
      "monitor":true
   }
   ]
}
Create and configure CloudWatch Application Insights monitoring using CloudFormation templates

You can add Application Insights monitoring, including key metrics and telemetry, to your application, database, and web server, directly from AWS CloudFormation templates.

This section provides sample AWS CloudFormation templates in both JSON and YAML formats to help you create and configure Application Insights monitoring.

To view the Application Insights resource and property reference in the AWS CloudFormation User Guide, see ApplicationInsights resource type reference.
Sample templates
- Create an Application Insights application for the entire AWS CloudFormation stack (p. 600)
- Create an Application Insights application with detailed settings (p. 601)
- Create an Application Insights application with CUSTOM mode component configuration (p. 603)
- Create an Application Insights application with DEFAULT mode component configuration (p. 606)
- Create an Application Insights application with DEFAULT_WITH_OVERWRITE mode component configuration (p. 607)

Create an Application Insights application for the entire AWS CloudFormation stack

To apply the following template, you must create AWS resources and one or more resource groups from which to create Application Insights applications to monitor those resources. For more information, see Getting started with AWS Resource Groups.

The first two parts of the following template specify a resource and a resource group. The last part of the template creates an Application Insights application for the resource group, but does not configure the application or apply monitoring. For more information, see the CreateApplication command details in the Amazon CloudWatch Application Insights API Reference.

Template in JSON format

```json
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Test Resource Group stack",
  "Resources": {
    "EC2Instance": {
      "Type": "AWS::EC2::Instance",
      "Properties": {
        "ImageId" : "ami-abcd1234efgh5678",
        "SecurityGroupIds" : ["sg-abcd1234"]
      }
    },
    ...
    "ResourceGroup": {
      "Type": "AWS::ResourceGroups::Group",
      "Properties": {
        "Name": "my_resource_group"
      }
    },
    "AppInsightsApp": {
      "Type": "AWS::ApplicationInsights::Application",
      "Properties": {
        "ResourceGroupName": "my_resource_group"
      },
      "DependsOn" : "ResourceGroup"
    }
  }
}
```

Template in YAML format

```yaml
---
AWSTemplateFormatVersion: '2010-09-09'
Description: Test Resource Group stack
Resources:
  EC2Instance:
    Type: AWS::EC2::Instance
```

600
Create an Application Insights application with detailed settings

Properties:
ImageId: ami-abcd1234efgh5678i
SecurityGroupIds:
  - sg-abcd1234

ResourceGroup:
  Type: AWS::ResourceGroups::Group
  Properties:
    Name: my_resource_group

AppInsightsApp:
  Type: AWS::ApplicationInsights::Application
  Properties:
    ResourceGroupName: my_resource_group
    DependsOn: ResourceGroup

The following template section applies the default monitoring configuration to the Application Insights application. For more information, see the CreateApplication command details in the Amazon CloudWatch Application Insights API Reference.

When AutoConfigurationEnabled is set to true, all components of the application are configured with the recommended monitoring settings for the DEFAULT application tier. For more information about these settings and tiers, see DescribeComponentConfigurationRecommendation and UpdateComponentConfiguration in the Amazon CloudWatch Application Insights API Reference.

Template in JSON format

```json
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description": "Test Application Insights Application stack",
  "Resources": {
    "AppInsightsApp": {
      "Type": "AWS::ApplicationInsights::Application",
      "Properties": {
        "ResourceGroupName": "my_resource_group",
        "AutoConfigurationEnabled": true
      }
    }
  }
}
```

Template in YAML format

```yaml
---
AWSTemplateFormatVersion: '2010-09-09'
Description: Test Application Insights Application stack
Resources:
  AppInsightsApp:
    Type: AWS::ApplicationInsights::Application
    Properties:
      ResourceGroupName: my_resource_group
      AutoConfigurationEnabled: true
```

Create an Application Insights application with detailed settings

The following template performs these actions:

- Creates an Application Insights application with CloudWatch Events notification and OpsCenter enabled. For more information, see the CreateApplication command details in the Amazon CloudWatch Application Insights API Reference.
• Tags the application with two tags, one of which has no tag values. For more information, see `TagResource` in the *Amazon CloudWatch Application Insights API Reference*.

• Creates two custom instance group components. For more information, see `CreateComponent` in the *Amazon CloudWatch Application Insights API Reference*.

• Creates two log pattern sets. For more information, see `CreateLogPattern` in the *Amazon CloudWatch Application Insights API Reference*.

• Sets `AutoConfigurationEnabled` to `true`, which configures all components of the application with the recommended monitoring settings for the `DEFAULT` tier. For more information, see `DescribeComponentConfigurationRecommendation` in the *Amazon CloudWatch Application Insights API Reference*.

**Template in JSON format**

```json
{
    "Type": "AWS::ApplicationInsights::Application",
    "Properties": {
        "ResourceGroupName": "my_resource_group",
        "CWEMonitorEnabled": true,
        "OpsCenterEnabled": true,
        "OpsItemSNSTopicArn": "arn:aws:sns:us-east-1:123456789012:my_topic",
        "AutoConfigurationEnabled": true,
        "Tags": [
            {
                "Key": "key1",
                "Value": "value1"
            },
            {
                "Key": "key2",
                "Value": ""
            }
        ],
        "CustomComponents": [
            {
                "ComponentName": "test_component_1",
                "ResourceList": [
                    "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1234efgh5678i"
                ]
            },
            {
                "ComponentName": "test_component_2",
                "ResourceList": [
                    "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1234efgh5678i",
                    "arn:aws:ec2:us-east-1:123456789012:instance/i-abcd1234efgh5678i"
                ]
            }
        ],
        "LogPatternSets": [
            {
                "PatternSetName": "pattern_set_1",
                "LogPatterns": [
                    {
                        "PatternName": "deadlock_pattern",
                        "Pattern": ".*\sDeadlocked\sSchedules\(\^[\x85]\s\)\$\)",
                        "Rank": 1
                    }
                ]
            },
            {
                "PatternSetName": "pattern_set_2",
                "LogPatterns": [
                    {
                        "PatternName": "error_pattern",
                        "Pattern": "\sDeadlocked\sSchedules\(\^[\x85]\s\)\$\)",
                        "Rank": 1
                    }
                ]
            }
        ]
    }
}
```
Create an Application Insights application with CUSTOM mode component configuration

The following template performs these actions:

- Creates an Application Insights application. For more information, see CreateApplication in the Amazon CloudWatch Application Insights API Reference.
- Component my_component sets ComponentConfigurationMode to CUSTOM, which causes this component to be configured with the configuration specified in CustomComponentConfiguration.
Create an Application Insights application with CUSTOM mode component configuration

For more information, see UpdateComponentConfiguration in the Amazon CloudWatch Application Insights API Reference.

Template in JSON format

```
{
  "Type": "AWS::ApplicationInsights::Application",
  "Properties": {
    "ResourceGroupName": "my_resource_group",
    "ComponentMonitoringSettings": [
      {
        "ComponentARN": "my_component",
        "Tier": "SQL_SERVER",
        "ComponentConfigurationMode": "CUSTOM",
        "CustomComponentConfiguration": {
          "ConfigurationDetails": {
            "AlarmMetrics": [
              {
                "AlarmMetricName": "StatusCheckFailed"
              },
              ...
            ],
            "Logs": [
              {
                "LogGroupName": "my_log_group_1",
                "LogPath": "C:\\LogFolder_1\*",
                "LogType": "DOT_NET_CORE",
                "Encoding": "utf-8",
                "PatternSet": "my_pattern_set_1"
              },
              ...
            ],
            "WindowsEvents": [
              {
                "LogGroupName": "my_windows_event_log_group_1",
                "eventName": "Application",
                "EventLevels": [
                  "ERROR",
                  "WARNING",
                  ...
                ],
                "Encoding": "utf-8",
                "PatternSet": "my_pattern_set_2"
              },
              ...
            ],
            "Alarms": [
              {
                "AlarmName": "my_alarm_name",
                "Severity": "HIGH"
              },
              ...
            ]
          }
        },
        "SubComponentTypeConfigurations": [
          {
            "SubComponentType": "EC2_INSTANCE",
            "SubComponentConfigurationDetails": {
              "AlarmMetrics": [
                {
                  "AlarmMetricName": "DiskReadOps"
                },
                ...
              ]
            }
          }
        ]
      }
    ]
  }
}
```
Create an Application Insights application with CUSTOM mode component configuration

```
"Logs": [
  
  "LogGroupName": "my_log_group_2",
  "LogPath": "C:\LogFolder_2\*",
  "LogType": "IIS",
  "Encoding": "utf-8",
  "PatternSet": "my_pattern_set_3"
  
},
...
],
"WindowsEvents": [
  
  "LogGroupName": "my_windows_event_log_group_2",
  "EventName": "Application",
  "EventLevels": [
    "ERROR",
    "WARNING",
    ...  
  ],
  "Encoding": "utf-8",
  "PatternSet": "my_pattern_set_4"
},
...
]

Template in YAML format

```yaml
---
Type: AWS::ApplicationInsights::Application
Properties:
  ResourceGroupName: my_resource_group
  ComponentMonitoringSettings:
    
    - ComponentARN: my_component
      Tier: SQL_SERVER
      CustomComponentConfiguration:
        
        ConfigurationDetails:
          
          AlarmMetrics:
            - AlarmMetricName: StatusCheckFailed
            ...  
          Logs:
            - LogGroupName: my_log_group_1
              LogPath: C:\LogFolder_1\*
              LogType: DOT_NET_CORE
              Encoding: utf-8
              PatternSet: my_pattern_set_1
            ...  
          WindowsEvents:
            - LogGroupName: my_windows_event_log_group_1
              EventName: Application
              EventLevels:
                
                - ERROR
                - WARNING
                ...  
              Encoding: utf-8
              PatternSet: my_pattern_set_2
            ...  
```
Create an Application Insights application with DEFAULT mode component configuration

The following template performs these actions:

- Creates an Application Insights application. For more information, see CreateApplication in the Amazon CloudWatch Application Insights API Reference.

- Component my_component sets ComponentConfigurationMode to DEFAULT and Tier to SQL_SERVER, which causes this component to be configured with the configuration settings that Application Insights recommends for the SQL Server tier. For more information, see DescribeComponentConfiguration and UpdateComponentConfiguration in the Amazon CloudWatch Application Insights API Reference.

### Template in JSON format

```json
{
    "Type": "AWS::ApplicationInsights::Application",
    "Properties": {
        "ResourceGroupName": "my_resource_group",
        "ComponentMonitoringSettings": [
        {
            "ComponentARN": "my_component",
            "Tier": "SQL_SERVER",
            "ComponentConfigurationMode": "DEFAULT"
        }
        ]
    }
}
```

### Template in YAML format

```yaml
# (YAML format)
```
Create an Application Insights application with DEFAULT_WITH_OVERWRITE mode component configuration

The following template performs these actions:

- Creates an Application Insights application. For more information, see CreateApplication in the Amazon CloudWatch Application Insights API Reference.
- Component my_component sets ComponentConfigurationMode to DEFAULT_WITH_OVERWRITE and tier to DOT_NET_CORE, which causes this component to be configured with the configuration settings that Application Insights recommends for the DOT_NET_CORE tier. Overwritten configuration settings are specified in the DefaultOverwriteComponentConfiguration:
  - At the component level AlarmMetrics settings are overwritten.
  - At the sub-component level, for the EC2_Instance type sub-components, Logs settings are overwritten.

For more information, see UpdateComponentConfiguration in the Amazon CloudWatch Application Insights API Reference.

Template in JSON format

```
{
  "Type": "AWS::ApplicationInsights::Application",
  "Properties": {
    "ResourceGroupName": "my_resource_group",
    "ComponentMonitoringSettings": [
      {
        "ComponentName": "my_component",
        "Tier": "DOT_NET_CORE",
        "ComponentConfigurationMode": "DEFAULT_WITH_OVERWRITE",
        "DefaultOverwriteComponentConfiguration": {
          "ConfigurationDetails": {
            "AlarmMetrics": [
              {
                "AlarmMetricName": "StatusCheckFailed"
              }
            ]
          }
        },
        "SubComponentTypeConfigurations": [
          {
            "SubComponentType": "EC2_INSTANCE",
            "SubComponentConfigurationDetails": {
              "Logs": [
                {
                  "LogGroupName": "my_log_group",
                  "LogPath": "C:\LogFolder\*",
                  "LogType": "IIS",
                  "Encoding": "utf-8",
                }
              ]
            }
          }
        ]
      }
    ]
  }
}
```
Tutorial: Set up monitors for .NET applications using SQL Server

This tutorial demonstrates how to configure CloudWatch Application Insights to monitor an example solution and then simulate problem scenarios to test the solution. In this example, a load balanced web application using SQL Server on the backend is deployed. The web application and SQL Server are hosted on separate EC2 instances.

**Tutorial components**
- Use case scenario (p. 608)
- Prerequisites (p. 609)
- Deploy resources for example scenario (p. 609)
- Set up monitoring with Amazon CloudWatch Application Insights (p. 610)
- Simulate problem scenarios and view insights (p. 611)

**Use case scenario**

In this scenario, a .NET application using SQL Server on the backend runs on an Amazon EC2 instance. The deployment is configured with two load-balanced EC2 instances hosting the Barley Adventure Works
application. Both instances access SQL Server, which is hosted on a separate EC2 instance. Monitors are set up with CloudWatch Application Insights to quickly identify, isolate, and resolve application issues.

Prerequisites

To complete the steps in this tutorial, you must have an AWS account.

If you do not have an AWS account, complete the following steps to create one.

To sign up for an AWS account

2. Follow the online instructions.
   
   Part of the sign-up procedure involves receiving a phone call and entering a verification code on the phone keypad.

Deploy resources for example scenario

A CloudFormation template is provided to automate the deployment scenario for testing. The template deploys the following instances:

- An EC2 instance that hosts the Microsoft SQL Server database.
- Two load-balanced EC2 instances. Each load-balanced instance hosts the Barley Adventure Works web application.

The template deployment takes approximately 10 minutes to complete.

Steps to deploy the CloudFormation stack

1. Choose Create Stack>With new resources (standard) from the AWS CloudFormation landing page at https://console.aws.amazon.com/cloudformation to launch a CloudFormation stack in your account in the US East (N. Virginia) Region. This template is available only in the us-east-1 Region.
2. Select Template is ready on the Create Stack page.
3. Under Specify template, select Amazon S3 URL and enter the following S3 URL path: https://application-insights-demo-resources.s3.amazonaws.com/SampleApp.yml. Choose Next.
Note
This CloudFormation template can also be found in the aws-samples GitHub repo at the following location: https://github.com/aws-samples/application-insights-sample-application/blob/master/SampleApp.yml.

4. On the Specify stack details page, enter a name for the stack, such as ApplicationInsightsTest.
5. Review the default parameters under Parameters and modify the values to your preferences. Enter a password for SQLServer. Enter an existing EC2 key pair or create a new one in the EC2 console. Choose Next.
6. On the Configure stack options page, under Tags, optionally add tags to help you identify your stack. Select Next.
7. Review and confirm the settings on the Review page. Select the box acknowledging that the template may create AWS Identity and Access Management (IAM) resources.
8. Choose Create stack to deploy the stack.
9. Monitor the status of the stack deployment from the Events tab of the Cloud Formation stack page. When the stack is successfully deployed, continue to the next section.

Set up monitoring with Amazon CloudWatch Application Insights

This section demonstrates how to create a resource group from the resources deployed by the CloudFormation template, and how to add the resource group to CloudWatch Application Insights for monitoring.

Create resource group

1. Navigate to the AWS Resource Groups console and choose Create resource group.
2. On the Create query-based group page, under Group type, select CloudFormation stack based.
3. Under Grouping criteria, select the CloudFormation stack you created in the previous section (ApplicationInsightsTest) from the dropdown list. Keep resource types as All supported resource types.
4. Under Group details, enter a Group name, such as application-insights-resource-group, and an optional description of the resource group. Then, choose Create group.

Set up resource group monitoring on CloudWatch Application Insights

1. Navigate to the Amazon CloudWatch console and choose Application Insights under Insights on the left navigation pane.
2. Choose View applications next to Application Insights.
3. On the Applications monitored page, choose Add an application.
4. Under Resource Group selection, select the resource group you created in the previous procedure (application-insights-resource-group) and choose Add application.
5. On the Overview page, refresh your browser to display the application components in your resource group.
6. Select the Application Load Balancer group and choose Manage monitoring.
7. On the Manage monitoring page, select Enable monitoring.
8. Choose Save.
9. To enable monitoring for the SQL Server instance, select the SQL Server EC2 instance in the Application components section and repeat the previous steps for enabling monitoring from the Manage monitoring page.
The following metrics are monitored for the SQL Server instance:

- CPUUtilization
- StatusCheckFailed
- Memory % Committed Bytes in Use
- Memory Available Mbytes
- Network Interface Bytes Total/sec
- Paging File % Usage
- Physical Disk % Disk Time
- Processor % Processor Time
- SQLServer:Buffer Manager cache hit ratio
- SQLServer:Buffer Manager life expectancy
- SQLServer:General Statistics Processes blocked
- SQLServer:General Statistics User Connections
- SQLServer:Locks Number of Deadlocks/sec
- SQLServer:SQL Statistics Batch Requests/sec
- System Processor Queue Length

The following metrics are monitored for the volumes attached to the SQL Server instance:

- VolumeReadBytes
- VolumeWriteBytes
- VolumeReadOps
- VolumeWriteOps
- VolumeTotalReadTime
- VolumeTotalWriteTime
- VolumeIdleTime
- VolumeQueueLength
- VolumeThroughputPercentage
- VolumeConsumedReadWriteOps
- BurstBalance

10. When monitoring is enabled for both the load balancer and the SQL Server instance, the resource group to which they belong displays a status of Enabled on the resource group Overview page.

### Simulate problem scenarios and view insights

This section describes how to create a SQL login failure, a SQL memory pressure event, and an HTTP 500 error so that you can view the error details on the CloudWatch Application Insights dashboard.

#### Problems

- Simulate SQL login failure (p. 612)
- Simulate high memory pressure (p. 612)
- Simulate an HTTP 500 error (p. 612)
Simulate SQL login failure

To simulate a SQL login failure and view the problem from the CloudWatch dashboard, perform the following steps.

1. Log in to the EC2 instance provisioned for your SQL Server instance (M4 instance type) using the key pair you selected when you created the CloudFormation stack.
2. From the Start menu, launch SQL Management Studio.
3. Enter a username and an incorrect password and choose Connect. A message appears indicating that the login has failed. Repeat this step a few more times.
4. From the CloudWatch Application Insights Problems detected page (at the bottom of the CloudWatch console landing page), the error should appear under the problem summary as SQL: Login Failure. To see more details about the problem, select the problem link.

Simulate high memory pressure

To simulate a high memory pressure event, which can lead to application performance degradation and timeout errors on the web servers and load balancers, perform the following steps.

1. Launch SQL Management Studio from the SQL server instance and login using the Windows Administrator account.
2. Right-click on the database server, choose Properties, and select Memory.
3. Under the Server memory options, reduce the Maximum server memory to 256 KB.
4. In a new query window, run the following SQL query:

```sql
SELECT COUNT(*)
FROM [AdventureWorks2016].[Sales].[Customer]
```

A message appears indicating that there is insufficient memory to run the query.
5. From the CloudWatch Application Insights Problems detected page (at the bottom of the CloudWatch console landing page), the error should appear under the problem summary as SQL: Memory Pressure. To see more details about the problem, select the problem link.

Simulate an HTTP 500 error

HTTP requests for an unhandled HTTP request to a web application results in an HTTP 500 error. To simulate an HTTP 500 error, perform the following steps.

1. From the AWS Management Console, navigate to the AWS CloudFormation console.
2. Choose the Outputs tab of the AppInsightsTest CloudFormation stack that you previously launched.
3. Open the URL displayed under Value for the AdventureWorks application in a web browser.
4. Navigate to the customer details page of the Barley Adventure Works web application by suffixing the previously mentioned URL with barleyapp/SalesOrderDetails/edit/5.
5. Refresh the compiled URL request several times. Your URL should look something like this: http://<YourURL>.us-east-1.elb.amazonaws.com/barleyapp/SalesOrderDetails/edit/5.

An error message appears indicating that the file or directory cannot be found.
6. From the CloudWatch Application Insights Problems detected page (at the bottom of the CloudWatch console landing page), the error should appear under the problem summary as ALB: Backend 5XX errors. To see more details about the problem, select the problem link.
View and troubleshoot problems detected by Amazon CloudWatch Application Insights

An overview of problems impacting your .NET and SQL Server applications is listed under the CloudWatch Application Insights widget in the default overview page of the CloudWatch console. For more information, see Get started with Amazon CloudWatch Application Insights (p. 555).

The CloudWatch Application Insights widget displays the following:

- The severity of the problems detected
- A summary of the problem
- The possible root cause of the problem
- The time the problem started
- The resolution status of the problem
- The affected Resource Group

To drill down into details of a specific problem, under Problem Summary, select the description of the problem. A detailed dashboard displays insights into the problem and related metric anomalies and snippets of log errors. From here, you can provide feedback on the relevance of the insight by selecting whether it is useful.

If a new, unconfigured resource is detected, the problem summary description takes you to the Edit configuration wizard to configure your new resource. If needed, you can view or edit your Resource Group configuration by choosing View/edit configuration in the upper right-hand corner of the detailed dashboard.

To return to the overview, choose Back to overview, which is next to the CloudWatch Application Insights detailed dashboard header.

Information provided about detected problems

CloudWatch Application Insights provides the following information about detected problems:

- A short summary of the problem
- The start time and date of the problem
- The problem severity: High/Medium/Low
- The status of the detected problem: In-progress/Resolved
- Insights: Automatically generated insights on the detected problem and possible root cause
- Feedback on insights: Feedback you have provided about the usefulness of the insights generated by CloudWatch Application Insights
- Related observations: A detailed view of the metric anomalies and error snippets of relevant logs related to the problem across various application components

Feedback

You can provide feedback on the automatically generated insights on detected problems by designating them useful or not useful. Your feedback on the insights, along with your application diagnostics (metric anomalies and log exceptions), are used to improve the future detection of similar problems.

Configuration errors

CloudWatch Application Insights uses your configuration to create monitoring telemetries for the components. When Application Insights detects an issue with your account or your configuration,
information is provided in the **Remarks** field about how to resolve the configuration issue for your application.

The following table shows suggested resolutions for specific remarks.

<table>
<thead>
<tr>
<th>Remarks</th>
<th>Suggested resolution</th>
<th>Additional notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The quota for alarms has already been reached.</td>
<td>By default, each AWS account can have 5,000 CloudWatch alarms per AWS Region. See <a href="https://docs.aws.amazon.com/CloudWatch/latest/monitoring/cloudwatch-limits.html">CloudWatch Limits</a>. When throttled by this limit, CloudWatch Application Insights cannot create all of the required alarms to monitor your application. To resolve this, raise the account limit for CloudWatch alarms.</td>
<td>n/a</td>
</tr>
<tr>
<td>The quota for CloudFormation has already been reached.</td>
<td>Application Insights creates one CloudFormation stack for each application to manage CloudWatch agent installation and configuration for all application components. By default, each AWS account can have 200 stacks. See <a href="https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/cloudformation-limits.html">AWS CloudFormation Limits</a>. To resolve this, raise the limit for CloudFormation stacks.</td>
<td>n/a</td>
</tr>
<tr>
<td>No SSM instance role on the following instances.</td>
<td>For Application Insights to be able to install and configure CloudWatch agent on application instances, <a href="https://docs.aws.amazon.com/AmazonSSM/latest/SSM-Managed-Instance-SDK-Reference/latest/core-policy.html">AmazonSSMManagedInstanceCore</a> and <a href="https://docs.aws.amazon.com/AmazonSSM/latest/SSM-Managed-Instance-SDK-Reference/latest/server-policy.html">CloudWatchAgentServerPolicy</a> policies must be attached to the instance role.</td>
<td>Application Insights calls the SSM DescribeInstancesInformation API to get the list of instances with SSM permission. After the role is attached to the instance, it takes time for SSM to include the instance in the DescribeInstancesInformation result. Until SSM includes the instance in the result, NO_SSM_INSTANCE_ROLE error remains present for the application.</td>
</tr>
<tr>
<td>New components may need configuration.</td>
<td>Application Insights detects that there are new components in the application Resource Group. To resolve this, configure the new components accordingly.</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Logs and metrics supported by Amazon CloudWatch Application Insights

The following lists show the supported logs and metrics for Amazon CloudWatch Application Insights.

**CloudWatch Application Insights supports the following logs:**

- Microsoft Internet Information Services (IIS) logs
- Error log for SQL Server on EC2
- Custom .NET application logs, such as Log4Net
- Windows Event logs, including Windows logs (System, Application, and Security) and Applications and Services log
- Amazon CloudWatch Logs for AWS Lambda
- Error log and slow log for RDS MySQL, Aurora MySQL, and MySQL on EC2
- Postgresql log for PostgreSQL RDS and PostgreSQL on EC2
- Amazon CloudWatch Logs for AWS Step Functions
- Execution logs and access logs (JSON, CSV, and XML, but not CLF) for API Gateway REST API stages
- Prometheus JMX exporter logs (EMF)
- Alert logs and listener logs for Oracle on Amazon RDS and Oracle on Amazon EC2
- Container logs routing from Amazon ECS containers to CloudWatch using `awslogs log driver`
- Container logs routing from Amazon ECS containers to CloudWatch using `FireLens container log router`
- Container logs routing from Amazon EKS or Kubernetes running on Amazon EC2 to CloudWatch using `Fluent Bit or Fluentd log processor` with Container Insights

**CloudWatch Application Insights supports metrics for the following application components:**

- Amazon Elastic Compute Cloud (EC2) (p. 616)
  - CloudWatch built-in metrics (p. 616)
  - CloudWatch agent metrics (Windows server) (p. 617)
  - CloudWatch agent metrics (Linux server) (p. 620)
- Elastic Block Store (EBS) (p. 622)
- Elastic Load Balancer (ELB) (p. 622)
- Application ELB (p. 623)
- Amazon EC2 Auto Scaling groups (p. 623)
- Amazon Simple Queue Server (SQS) (p. 624)
- Amazon Relational Database Service (RDS) (p. 624)
  - RDS Database instances (p. 624)
  - RDS Database clusters (p. 625)
- AWS Lambda function (p. 626)
- Amazon DynamoDB table (p. 626)
- Amazon S3 bucket (p. 627)
- AWS Step Functions (p. 627)
  - Execution-level (p. 627)
  - Activity (p. 628)
  - Lambda function (p. 628)
  - Service integration (p. 628)
• Step Functions API (p. 628)
• API Gateway REST API stages (p. 629)
• Java (p. 629)
• Amazon Elastic Container Service (Amazon ECS) (p. 630)
  • CloudWatch built-in metrics (p. 630)
  • Container Insights metrics (p. 630)
  • Container Insights Prometheus metrics (p. 631)
• Kubernetes on AWS (p. 631)
  • Container Insights metrics (p. 631)
  • Container Insights Prometheus metrics (p. 632)
• Metrics with datapoints requirements (p. 633)
  • AWS/ApplicationELB (p. 633)
  • AWS/AutoScaling (p. 634)
  • AWS/EC2 (p. 634)
  • Elastic Block Store (EBS) (p. 635)
  • AWS/ELB (p. 635)
  • AWS/RDS (p. 635)
  • AWS/Lambda (p. 637)
  • AWS/SQS (p. 637)
  • AWS/CWAgent (p. 637)
  • AWS/DynamoDB (p. 638)
  • AWS/S3 (p. 639)
  • AWS/States (p. 639)
  • AWS/ApiGateway (p. 640)
• Recommended metrics (p. 640)
• Performance Counter metrics (p. 653)

Amazon Elastic Compute Cloud (EC2)

Metrics
• CloudWatch built-in metrics (p. 616)
• CloudWatch agent metrics (Windows server) (p. 617)
• CloudWatch agent metrics (Linux server) (p. 620)

CloudWatch built-in metrics

CPUCreditBalance
CPUCreditUsage
CPUSurplusCreditBalance
CPUSurplusCreditsCharged
CPUUtilization
DiskReadBytes
DiskReadOps
DiskWriteBytes
DiskWriteOps
EBSByteBalance%
EBSIOBalance%
EBSReadBytes
EBSReadOps
EBSWriteBytes
EBSWriteOps
NetworkIn
NetworkOut
NetworkPacketsIn
NetworkPacketsOut
StatusCheckFailed
StatusCheckFailed_Instance
StatusCheckFailed_System

CloudWatch agent metrics (Windows server)

.NET CLR Exceptions # of Exceps Thrown
.NET CLR Exceptions # of Exceps Thrown/Sec
.NET CLR Exceptions # of Filters/sec
.NET CLR Exceptions # of Finallys/sec
.NET CLR Exceptions Throw to Catch Depth/Sec
.NET CLR Interop # of CCWs
.NET CLR Interop # of Stubs
.NET CLR Interop # of TLB exports/sec
.NET CLR Interop # of TLB imports/sec
.NET CLR Interop # of marshaling
.NET CLR Jit % Time in Jit
.NET CLR Jit Standard Jit Failures
.NET CLR Loading % Time Loading
.NET CLR Loading Rate of Load Failures
.NET CLR LocksAndThreads Contention Rate/sec
.NET CLR LocksAndThreads Queue Length/sec
.NET CLR Memory # Total Committed Bytes
.NET CLR Memory % Time in GC
.NET CLR Networking 4.0.0.0 HttpWebRequest Average Queue Time
.NET CLR Networking 4.0.0.0 HttpWebRequests Aborted/sec
.NET CLR Networking 4.0.0.0 HttpWebRequests Failed/sec
.NET CLR Networking 4.0.0.0 HttpWebRequests Queued/sec
APP_POOL_WAS Total Worker Process Ping Failures
ASP.NET Application Restarts
ASP.NET Applications % Managed Processor Time (estimated)
ASP.NET Applications Errors Total/Sec
ASP.NET Applications Errors Unhandled During Execution/sec
ASP.NET Applications Requests in Application Queue
ASP.NET Applications Requests/Sec
ASP.NET Request Wait Time
ASP.NET Requests Queued
HTTP Service Request Queues CurrentQueueSize
LogicalDisk % Free Space
Memory % Committed Bytes In Use
Memory Available Mbytes
Memory Pages/sec
Network Interface Bytes Total/sec
Paging File % Usage
PhysicalDisk % Disk Time
PhysicalDisk Avg. Disk Queue Length
PhysicalDisk Avg. Disk sec/Read
PhysicalDisk Avg. Disk sec/Write
PhysicalDisk Disk Read Bytes/sec
PhysicalDisk Disk Reads/sec
PhysicalDisk Disk Write Bytes/sec
PhysicalDisk Disk Writes/sec
Processor % Idle Time
Processor % Interrupt Time
Processor % Processor Time
Processor % User Time
SQLServer:Access Methods Forwarded Records/sec
SQLServer:Access Methods Full Scans/sec
SQLServer:Access Methods Page Splits/sec
SQLServer:Buffer Manager Buffer cache hit ratio
SQLServer:Buffer Manager Page life expectancy
SQLServer:General Statistics Processes blocked
SQLServer:General Statistics User Connections
SQLServer:Latches Average Latch Wait Time (ms)
SQLServer:Locks Average Wait Time (ms)
SQLServer:Locks Lock Timeouts/sec
SQLServer:Locks Lock Waits/sec
SQLServer:Locks Number of Deadlocks/sec
SQLServer:Memory Manager Memory Grants Pending
SQLServer:SQL Statistics Batch Requests/sec
SQLServer:SQL Statistics SQL Compilations/sec
SQLServer:SQL Statistics SQL Re-Compilations/sec
System Processor Queue Length
TCPv4 Connections Established
TCPv6 Connections Established
W3SVC_W3WP File Cache Flushes
W3SVC_W3WP File Cache Misses
W3SVC_W3WP Requests/Sec
W3SVC_W3WP URI Cache Flushes
W3SVC_W3WP URI Cache Misses
Web Service Bytes Received/Sec
Web Service Bytes Sent/Sec
Web Service Connection attempts/sec
Web Service Current Connections
Web Service Get Requests/sec
Web Service Post Requests/sec
CloudWatch agent metrics (Linux server)

cpu_time_active
cpu_time_guest
cpu_time_guest_nice
cpu_time_idle
cpu_time_iowait
cpu_time_irq
cpu_time_nice
cpu_time_softirq
cpu_time_steal
cpu_time_system
cpu_time_user
cpu_usage_active
cpu_usage_guest
cpu_usage_guest_nice
cpu_usage_idle
cpu_usage_iowait
cpu_usage_irq
cpu_usage_nice
cpu_usage_softirq
cpu_usage_steal
cpu_usage_system
cpu_usage_user
disk_free
disk_inodes_free
disk_inodes_used
disk_used
disk_used_percent
diskio_io_time
diskio_iops_in_progress
diskio_read_bytes
diskio_read_time
<table>
<thead>
<tr>
<th>Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>diskio_reads</td>
</tr>
<tr>
<td>diskio_write_bytes</td>
</tr>
<tr>
<td>diskio_write_time</td>
</tr>
<tr>
<td>diskio_writes</td>
</tr>
<tr>
<td>mem_active</td>
</tr>
<tr>
<td>mem_available</td>
</tr>
<tr>
<td>mem_available_percent</td>
</tr>
<tr>
<td>mem_buffered</td>
</tr>
<tr>
<td>mem_cached</td>
</tr>
<tr>
<td>mem_free</td>
</tr>
<tr>
<td>mem_inactive</td>
</tr>
<tr>
<td>mem_used</td>
</tr>
<tr>
<td>mem_used_percent</td>
</tr>
<tr>
<td>net_bytes_recv</td>
</tr>
<tr>
<td>net_bytes_sent</td>
</tr>
<tr>
<td>net_drop_in</td>
</tr>
<tr>
<td>net_drop_out</td>
</tr>
<tr>
<td>net_err_in</td>
</tr>
<tr>
<td>net_err_out</td>
</tr>
<tr>
<td>net_packets_recv</td>
</tr>
<tr>
<td>net_packets_sent</td>
</tr>
<tr>
<td>netstat_tcp_close</td>
</tr>
<tr>
<td>netstat_tcp_close_wait</td>
</tr>
<tr>
<td>netstat_tcp_closing</td>
</tr>
<tr>
<td>netstat_tcp_established</td>
</tr>
<tr>
<td>netstat_tcp_fin_wait1</td>
</tr>
<tr>
<td>netstat_tcp_fin_wait2</td>
</tr>
<tr>
<td>netstat_tcp_last_ack</td>
</tr>
<tr>
<td>netstat_tcp_listen</td>
</tr>
<tr>
<td>netstat_tcp_none</td>
</tr>
<tr>
<td>netstat_tcp_syn_recv</td>
</tr>
<tr>
<td>netstat_tcp_syn_sent</td>
</tr>
</tbody>
</table>
Elastic Block Store (EBS)

VolumeReadBytes
VolumeWriteBytes
VolumeReadOps
VolumeWriteOps
VolumeTotalReadTime
VolumeTotalWriteTime
VolumeIdleTime
VolumeQueueLength
VolumeThroughputPercentage
VolumeConsumedReadWriteOps
BurstBalance

Elastic Load Balancer (ELB)

EstimatedALBActiveConnectionCount
EstimatedALBConsumedLCUs
EstimatedALBNewConnectionCount
EstimatedProcessedBytes
HTTPCode_Backend_4XX
HTTPCode_Backend_5XX
HealthyHostCount
RequestCount
UnHealthyHostCount

**Application ELB**

EstimatedALBActiveConnectionCount
EstimatedALBConsumedLCUs
EstimatedALBNewConnectionCount
EstimatedProcessedBytes
HTTPCode_Backend_4XX
HTTPCode_Backend_5XX
HealthyHostCount
Latency
RequestCount
SurgeQueueLength
UnHealthyHostCount

**Amazon EC2 Auto Scaling groups**

CPUCreditBalance
CPUCreditUsage
CPUSurplusCreditBalance
CPUSurplusCreditsCharged
CPUUtilization
DiskReadBytes
DiskReadOps
DiskWriteBytes
DiskWriteOps
EBSByteBalance%
EBSIOBalance%
EBSReadBytes
EBSReadOps
EBSWriteBytes
EBSWriteOps
NetworkIn
NetworkOut
NetworkPacketsIn
NetworkPacketsOut
StatusCheckFailed
StatusCheckFailed_Instance
StatusCheckFailed_System

**Amazon Simple Queue Server (SQS)**

ApproximateAgeOfOldestMessage
ApproximateNumberOfMessagesDelayed
ApproximateNumberOfMessagesNotVisible
ApproximateNumberOfMessagesVisible
NumberOfEmptyReceives
NumberOfMessagesDeleted
NumberOfMessagesReceived
NumberOfMessagesSent

**Amazon Relational Database Service (RDS)**

**RDS Database instances**

BurstBalance
CPUCreditBalance
CPUUtilization
DatabaseConnections
DiskQueueDepth
FailedSQLServerAgentJobsCount
FreeStorageSpace
FreeableMemory
NetworkReceiveThroughput
NetworkTransmitThroughput
ReadIOPS
ReadLatency
ReadThroughput
WriteIOPS
WriteLatency
WriteThroughput

**RDS Database clusters**

ActiveTransactions
AuroraBinlogReplicaLag
AuroraReplicaLag
BackupRetentionPeriodStorageUsed
BinLogDiskUsage
BlockedTransactions
BufferCacheHitRatio
CPUUtilization
CommitLatency
CommitThroughput
DDLLatency
DDLThroughput
DMLLatency
DMLThroughput
DatabaseConnections
Deadlocks
DeleteLatency
DeleteThroughput
EngineUptime
FreeLocalStorage
FreeableMemory
InsertLatency
InsertThroughput
LoginFailures
NetworkReceiveThroughput
NetworkThroughput
NetworkTransmitThroughput
Queries
ResultSetCacheHitRatio
SelectLatency
SelectThroughput
SnapshotStorageUsed
TotalBackupStorageBilled
UpdateLatency
UpdateThroughput
VolumeBytesUsed
VolumeReadIOPs
VolumeWriteIOPs

**AWS Lambda function**

Errors
DeadLetterErrors
Duration
Throttles
IteratorAge
ProvisionedConcurrencySpilloverInvocations

**Amazon DynamoDB table**

SystemErrors
UserErrors
ConsumedReadCapacityUnits
ConsumedWriteCapacityUnits
ReadThrottleEvents
WriteThrottleEvents
TimeToLiveDeletedItemCount
ConditionalCheckFailedRequests
TransactionConflict
ReturnedRecordsCount
PendingReplicationCount
ReplicationLatency

**Amazon S3 bucket**

ReplicationLatency
BytesPendingReplication
OperationsPendingReplication
4xxErrors
5xxErrors
AllRequests
GetRequests
PutRequests
DeleteRequests
HeadRequests
PostRequests
SelectRequests
ListRequests
SelectScannedBytes
SelectReturnedBytes
FirstByteLatency
TotalRequestLatency
BytesDownloaded
BytesUploaded

**AWS Step Functions**

**Execution-level**

ExecutionTime
ExecutionThrottled
ExecutionsFailed
ExecutionsTimedOut
ExecutionsAborted
ExecutionsSucceeded
ExecutionsStarted

**Activity**
- ActivityRunTime
- ActivityScheduleTime
- ActivityTime
- ActivitiesFailed
- ActivitiesHeartbeatTimedOut
- ActivitiesTimedOut
- ActivitiesScheduled
- ActivitiesSucceeded
- ActivitiesStarted

**Lambda function**
- LambdaFunctionRunTime
- LambdaFunctionScheduleTime
- LambdaFunctionTime
- LambdaFunctionsFailed
- LambdaFunctionsTimedOut
- LambdaFunctionsScheduled
- LambdaFunctionsSucceeded
- LambdaFunctionsStarted

**Service integration**
- ServiceIntegrationRunTime
- ServiceIntegrationScheduleTime
- ServiceIntegrationTime
- ServiceIntegrationsFailed
- ServiceIntegrationsTimedOut
- ServiceIntegrationsScheduled
- ServiceIntegrationsSucceeded
- ServiceIntegrationsStarted

**Step Functions API**
- ThrottledEvents
ProvisionedBucketSize
ProvisionedRefillRate
ConsumedCapacity

**API Gateway REST API stages**

4XXError
5XXError
IntegrationLatency
Latency
DataProcessed
CacheHitCount
CacheMissCount

**Java**

```
java_lang_memory_heapmemoryusage_used
java_lang_memory_heapmemoryusage_committed
java_lang_operatingsystem_openfiledescriptorcount
java_lang_operatingsystem_maxfiledescriptorcount
java_lang_operatingsystem_ferephysicalmemorysize
java_lang_operatingsystem_freeswapspacesize
java_lang_threading_threadcount
java_lang_threading_daemonthreadcount
java_lang_classloading_loadedclasscount
java_lang_garbagecollector_collectiontime_copy
java_lang_garbagecollector_collectiontime_ps_scavenge
java_lang_garbagecollector_collectiontime_parnew
java_lang_garbagecollector_collectiontime_marksweepcompact
java_lang_garbagecollector_collectiontime_ps_marksweep
java_lang_garbagecollector_collectiontime_concurrentmarksweep
java_lang_garbagecollector_collectiontime_g1_young_generation
java_lang_garbagecollector_collectiontime_g1_old_generation
java_lang_garbagecollector_collectiontime_g1_mixed_generation
java_lang_operatingsystem_committedvirtualmemorysize
```
Amazon Elastic Container Service (Amazon ECS)

CloudWatch built-in metrics

CPUReservation
CPUUtilization
MemoryReservation
MemoryUtilization
GPUReservation

Container Insights metrics

ContainerInstanceCount
CpuUtilized
CpuReserved
DeploymentCount
DesiredTaskCount
MemoryUtilized
MemoryReserved
NetworkRxBytes
NetworkTxBytes
PendingTaskCount
RunningTaskCount
ServiceCount
StorageReadBytes
StorageWriteBytes
TaskCount
TaskSetCount
instance_cpu_limit
instance_cpu_reserved_capacity
instance_cpu_usage_total
instance_cpu_utilization
instance_filesystem_utilization
instance_memory_limit
instance_memory_reserved_capacity

630
instance_memory_utilization
instance_memory_working_set
instance_network_total_bytes
instance_number_of_running_tasks

**Container Insights Prometheus metrics**

**Java JMX metrics**

java_lang_memory_heapmemoryusage_used
java_lang_memory_heapmemoryusage_committed
java_lang_operatingsystem_openfiledescriptorcount
java_lang_operatingsystem_maxfiledescriptorcount
java_lang_operatingsystem_freephysicalmemorysize
java_lang_operatingsystem_freeswapspacesize
java_lang_threading_threadcount
java_lang_classloading_loadedclasscount
java_lang_threading_daemonthreadcount
java_lang_garbagecollector_collectiontime_copy
java_lang_garbagecollector_collectiontime_ps_scavenge
java_lang_garbagecollector_collectiontime_parnew
java_lang_garbagecollector_collectiontime_marksweepcompact
java_lang_garbagecollector_collectiontime_ps_marksweep
java_lang_garbagecollector_collectiontime_concurrentmarksweep
java_lang_garbagecollector_collectiontime_g1_young_generation
java_lang_garbagecollector_collectiontime_g1_old_generation
java_lang_garbagecollector_collectiontime_g1_mixed_generation
java_lang_operatingsystem_committedvirtualmemorysize

**Kubernetes on AWS**

**Container Insights metrics**

cluster_failed_node_count
cluster_node_count
namespace_number_of_running_pods
node_cpu_limit
node_cpu_reserved_capacity
node_cpu_usage_total
node_cpu_utilization
node_filesystem_utilization
node_memory_limit
node_memory_reserved_capacity
node_memory_utilization
node_memory_working_set
node_network_total_bytes
node_number_of_running_containers
node_number_of_running_pods
pod_cpu_reserved_capacity
pod_cpu_utilization
pod_cpu_utilization_over_pod_limit
pod_memory_reserved_capacity
pod_memory_utilization
pod_memory_utilization_over_pod_limit
pod_network_rx_bytes
pod_network_tx_bytes
service_number_of_running_pods

**Container Insights Prometheus metrics**

**Java JMX metrics**

java_lang_memory_heapmemoryusage_used
java_lang_memory_heapmemoryusage_committed
java_lang_operatingsystem_openfiledescriptorcount
java_lang_operatingsystem_maxfiledescriptorcount
java_lang_operatingsystem_freephysicalmemorysize
java_lang_operatingsystem_freeswapspacesize
java_lang_threading_threadcount
java_lang_classloading_loadedclasscount
java_lang_threading_daemonthreadcount
java_lang_garbagecollector_collectiontime_copy
java_lang_garbagecollector_collectiontime_ps_scavenge
java_lang_garbagecollector_collectiontime_parnew
java_lang_garbagecollector_collectiontime_marksweepcompact
java_lang_garbagecollector_collectiontime_ps_marksweep
java_lang_garbagecollector_collectiontime_concurrentmarksweep
java_lang_garbagecollector_collectiontime_g1_young_generation
java_lang_garbagecollector_collectiontime_g1_old_generation
java_lang_garbagecollector_collectiontime_g1_mixed_generation
java_lang_operatingsystem_committedvirtualmemorysize

Metrics with datapoints requirements

For metrics without an obvious default threshold to alarm on, Application Insights waits until the metric has enough data points to predict a reasonable threshold to alarm on. The metric datapoints requirement that CloudWatch Application Insights checks before an alarm is created are:

- The metric has at least 100 datapoints from the past 15 to the past 2 days.
- The metric has at least 100 datapoints from the last day.

The following metrics follow these datapoints requirements. Note that CloudWatch agent metrics require up to one hour to create alarms.

Metrics
- AWS/ApplicationELB (p. 633)
- AWS/AutoScaling (p. 634)
- AWS/EC2 (p. 634)
- Elastic Block Store (EBS) (p. 635)
- AWS/ELB (p. 635)
- AWS/RDS (p. 635)
- AWS/Lambda (p. 637)
- AWS/SQS (p. 637)
- AWS/CWAgent (p. 637)
- AWS/DynamoDB (p. 638)
- AWS/S3 (p. 639)
- AWS/States (p. 639)
- AWS/ApiGateway (p. 640)

AWS/ApplicationELB
ActiveConnectionCount
ConsumedLCUs
HTTPCode_ELB_4XX_Count
HTTPCode_Target_2XX_Count
HTTPCode_Target_3XX_Count
HTTPCode_Target_4XX_Count
HTTPCode_Target_5XX_Count
NewConnectionCount
ProcessedBytes
TargetResponseTime
UnHealthyHostCount

**AWS/AutoScaling**

GroupDesiredCapacity
GroupInServiceInstances
GroupMaxSize
GroupMinSize
GroupPendingInstances
GroupStandbyInstances
GroupTerminatingInstances
GroupTotalInstances

**AWS/EC2**

CPUCreditBalance
CPUCreditUsage
CPUSurplusCreditBalance
CPUSurplusCreditsCharged
CPUUtilization
DiskReadBytes
DiskReadOps
DiskWriteBytes
DiskWriteOps
EBSByteBalance%
EBSIOBalance%
EBSReadBytes
EBSReadOps
EBSWriteBytes
EBSWriteOps
NetworkIn
NetworkOut
NetworkPacketsIn
NetworkPacketsOut

**Elastic Block Store (EBS)**
- VolumeReadBytes
- VolumeWriteBytes
- VolumeReadOps
- VolumeWriteOps
- VolumeTotalReadTime
- VolumeTotalWriteTime
- VolumeIdleTime
- VolumeQueueLength
- VolumeThroughputPercentage
- VolumeConsumedReadWriteOps
- BurstBalance

**AWS/ELB**
- EstimatedALBActiveConnectionCount
- EstimatedALBConsumedLCUs
- EstimatedALBNewConnectionCount
- EstimatedProcessedBytes
- HTTPCode_Backend_4XX
- HTTPCode_Backend_5XX
- HealthyHostCount
- Latency
- RequestCount
- SurgeQueueLength
- UnHealthyHostCount

**AWS/RDS**
- ActiveTransactions
- AuroraBinlogReplicaLag
AuroraReplicaLag
BackupRetentionPeriodStorageUsed
BinLogDiskUsage
BlockedTransactions
CPUCreditBalance
CommitLatency
CommitThroughput
DDLLatency
DDLThroughput
DMLLatency
DMLThroughput
DatabaseConnections
Deadlocks
DeleteLatency
DeleteThroughput
DiskQueueDepth
EngineUptime
FreeLocalStorage
FreeStorageSpace
FreeableMemory
InsertLatency
InsertThroughput
LoginFailures
NetworkReceiveThroughput
NetworkThroughput
NetworkTransmitThroughput
Queries
ReadIOPS
ReadThroughput
SelectLatency
SelectThroughput
SnapshotStorageUsed
TotalBackupStorageBilled
UpdateLatency
UpdateThroughput
VolumeBytesUsed
VolumeReadIOPs
VolumeWriteIOPs
WriteIOPS
WriteThroughput

**AWS/Lambda**

Errors
DeadLetterErrors
Duration
Throttles
IteratorAge
ProvisionedConcurrencySpilloverInvocations

**AWS/SQS**

ApproximateAgeOfOldestMessage
ApproximateNumberOfMessagesDelayed
ApproximateNumberOfMessagesNotVisible
ApproximateNumberOfMessagesVisible
NumberOfEmptyReceives
NumberOfMessagesDeleted
NumberOfMessagesReceived
NumberOfMessagesSent

**AWS/CWAgent**

LogicalDisk % Free Space
Memory % Committed Bytes In Use
Memory Available Mbytes
Network Interface Bytes Total/sec
Paging File % Usage
PhysicalDisk % Disk Time
PhysicalDisk Avg. Disk sec/Read
PhysicalDisk Avg. Disk sec/Write
PhysicalDisk Disk Read Bytes/sec
PhysicalDisk Disk Reads/sec
PhysicalDisk Disk Write Bytes/sec
PhysicalDisk Disk Writes/sec
Processor % Idle Time
Processor % Interrupt Time
Processor % Processor Time
Processor % User Time
SQLServer:Access Methods Forwarded Records/sec
SQLServer:Access Methods Page Splits/sec
SQLServer:Buffer Manager Buffer cache hit ratio
SQLServer:Buffer Manager Page life expectancy
SQLServer:Database Replica File Bytes Received/sec
SQLServer:Database Replica Log Bytes Received/sec
SQLServer:Database Replica Log remaining for undo
SQLServer:Database Replica Log Send Queue
SQLServer:Database Replica Mirrored Write Transaction/sec
SQLServer:Database Replica Recovery Queue
SQLServer:Database Replica Redo Bytes Remaining
SQLServer:Database Replica Redone Bytes/sec
SQLServer:Database Replica Total Log requiring undo
SQLServer:Database Replica Transaction Delay
SQLServer:General Statistics Processes blocked
SQLServer:SQL Statistics Batch Requests/sec
SQLServer:SQL Statistics SQL Compilations/sec
SQLServer:SQL Statistics SQL Re-Compilations/sec
System Processor Queue Length
TCPv4 Connections Established
TCPv6 Connections Established

AWS/DynamoDB
ConsumedReadCapacityUnits
ConsumedWriteCapacityUnits
ReadThrottleEvents
WriteThrottleEvents
TimeToLiveDeletedItemCount
ConditionalCheckFailedRequests
TransactionConflict
ReturnedRecordsCount
PendingReplicationCount
ReplicationLatency

**AWS/S3**

ReplicationLatency
BytesPendingReplication
OperationsPendingReplication
4xxErrors
5xxErrors
AllRequests
GetRequests
PutRequests
DeleteRequests
HeadRequests
PostRequests
SelectRequests
ListRequests
SelectScannedBytes
SelectReturnedBytes
FirstByteLatency
TotalRequestLatency
BytesDownloaded
BytesUploaded

**AWS/States**

ActivitiesScheduled
ActivitiesStarted
ActivitiesSucceeded
ActivityScheduleTime
ActivityRuntime
ActivityTime
LambdaFunctionsScheduled
LambdaFunctionsStarted
LambdaFunctionsSucceeded
LambdaFunctionScheduleTime
LambdaFunctionRuntime
LambdaFunctionTime
ServiceIntegrationsScheduled
ServiceIntegrationsStarted
ServiceIntegrationsSucceeded
ServiceIntegrationScheduleTime
ServiceIntegrationRuntime
ServiceIntegrationTime
ProvisionedRefillRate
ProvisionedBucketSize
ConsumedCapacity
ThrottledEvents

**AWS/ApiGateway**

4XXError
IntegrationLatency
Latency
DataProcessed
CacheHitCount
CacheMissCount

**Recommended metrics**

The following table lists the recommended metrics for each component type.
<table>
<thead>
<tr>
<th>Component type</th>
<th>Workload type</th>
<th>Recommended metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC2 instance (Windows servers)</td>
<td>Java Application</td>
<td>CPUUtilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StatusCheckFailed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processor % Processor Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory % Committed Bytes In Use</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory Available Mbytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_threading_threadcount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_classloading_loadedclasscount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_memory_heapmemoryusage_used</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_memory_heapmemoryusage_committed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_operatingsystem_freephysicalmemory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_operatingsystem_freeswapspacesize</td>
</tr>
<tr>
<td>Microsoft IIS/.NET Web Front-End</td>
<td></td>
<td>CPUUtilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StatusCheckFailed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processor % Processor Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory % Committed Bytes In Use</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory Available Mbytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.NET CLR Exceptions # of Excep Thrown/Sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.NET CLR Memory # Total Committed Bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.NET CLR Memory % Time in GC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASP.NET Applications Requests in Application Queue</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASP.NET Requests Queued</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASP.NET Application Restarts</td>
</tr>
<tr>
<td>Microsoft SQL Server Database Tier</td>
<td></td>
<td>CPUUtilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StatusCheckFailed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processor % Processor Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory % Committed Bytes In Use</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory Available Mbytes</td>
</tr>
<tr>
<td>Component type</td>
<td>Workload type</td>
<td>Recommended metric</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------</td>
<td>------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Paging File % Usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>System Processor Queue Length</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Interface Bytes Total/Sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PhysicalDisk % Disk Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQLServer:Buffer Manager Buffer Cache Hit ratio</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQLServer:Buffer Manager Page Life Expectancy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQLServer:General Statistics Processes Blocked</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQLServer:General Statistics User Connections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQLServer:Locks Number of Deadlocks/Sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SQLServer:SQL Statistics Batch Requests/Sec</td>
</tr>
<tr>
<td>.NET workerpool/Mid-Tier</td>
<td>CPUUtilization</td>
<td>StatusCheckFailed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processor % Processor Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory % Committed Bytes In Use</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory Available Mbytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.NET CLR Exceptions # of Exceptions Thrown/Sec</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.NET CLR Memory # Total Committed Bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>.NET CLR Memory % Time in GC</td>
</tr>
<tr>
<td>.NET Core Tier</td>
<td>CPUUtilization</td>
<td>StatusCheckFailed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Processor % Processor Time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory % Committed Bytes In Use</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Memory Available Mbytes</td>
</tr>
<tr>
<td>Component type</td>
<td>Workload type</td>
<td>Recommended metric</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EC2 instance (Linux servers)</td>
<td>Java Application</td>
<td>CPUUtilization&lt;br&gt;StatusCheckFailed&lt;br&gt;disk_used_percent&lt;br&gt;mem_used_percent&lt;br&gt;java_lang_threading_threadcount&lt;br&gt;java_lang_classloading_loadedclasscount&lt;br&gt;java_lang_memory_heapmemoryusage_used&lt;br&gt;java_lang_memory_heapmemoryusage_committed&lt;br&gt;java_lang_operatingsystem_freephysicalmemorysize&lt;br&gt;java_lang_operatingsystem_freeswapspacesize</td>
</tr>
<tr>
<td>.NET Core Tier or SQL Server Database Tier</td>
<td>Any</td>
<td>CPUUtilization&lt;br&gt;StatusCheckFailed&lt;br&gt;disk_used_percent&lt;br&gt;mem_used_percent</td>
</tr>
<tr>
<td>EBS volume</td>
<td>Any</td>
<td>VolumeReadBytes&lt;br&gt;VolumeWriteBytes&lt;br&gt;VolumeReadOps&lt;br&gt;VolumeWriteOps&lt;br&gt;VolumeQueueLength&lt;br&gt;VolumeThroughputPercentage&lt;br&gt;VolumeConsumedReadWriteOps&lt;br&gt;BurstBalance</td>
</tr>
<tr>
<td>Classic ELB</td>
<td>Any</td>
<td>HTTPCode_Backend_4XX&lt;br&gt;HTTPCode_Backend_5XX&lt;br&gt;Latency&lt;br&gt;SurgeQueueLength&lt;br&gt;UnHealthyHostCount</td>
</tr>
<tr>
<td>Component type</td>
<td>Workload type</td>
<td>Recommended metric</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>Application ELB</td>
<td>Any</td>
<td>HTTPCode_Target_4XX_Count</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HTTPCode_Target_5XX_Count</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TargetResponseTime</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UnHealthyHostCount</td>
</tr>
<tr>
<td>RDS Database instance</td>
<td>Any</td>
<td>CPUUtilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReadLatency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>WriteLatency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BurstBalance</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FailedSQLServerAgentJobsCount</td>
</tr>
<tr>
<td>RDS Database cluster</td>
<td>Any</td>
<td>CPUUtilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CommitLatency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DatabaseConnections</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Deadlocks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FreeableMemory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkThroughput</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VolumeBytesUsed</td>
</tr>
<tr>
<td>Lambda Function</td>
<td>Any</td>
<td>Duration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Errors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IteratorAge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ProvisionedConcurrencySpilloverInvocations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Throttles</td>
</tr>
<tr>
<td>SQS Queue</td>
<td>Any</td>
<td>ApproximateAgeOfOldestMessage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ApproximateNumberOfMessagesVisible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NumberOfMessagesSent</td>
</tr>
<tr>
<td>Component type</td>
<td>Workload type</td>
<td>Recommended metric</td>
</tr>
<tr>
<td>-------------------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Amazon DynamoDB table</td>
<td>Any</td>
<td>SystemErrors, UserErrors, ConsumedReadCapacityUnits, ConsumedWriteCapacityUnits, ReadThrottleEvents, WriteThrottleEvents, ConditionalCheckFailedRequests, TransactionConflict</td>
</tr>
<tr>
<td>Amazon S3 bucket</td>
<td>Any</td>
<td>If replication configuration with Replication Time Control (RTC) is enabled: ReplicationLatency, BytesPendingReplication, OperationsPendingReplication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If request metrics are turned on: 5xxErrors, 4xxErrors, BytesDownloaded, BytesUploaded</td>
</tr>
<tr>
<td>Component type</td>
<td>Workload type</td>
<td>Recommended metric</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>AWS Step Functions</td>
<td>Any</td>
<td><strong>General</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ExecutionThrottled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ExecutionsAborted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ProvisionedBucketSize</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ProvisionedRefillRate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ConsumedCapacity</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>If state machine type is EXPRESS or log group level is OFF</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ExecutionsFailed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ExecutionsTimedOut</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>If state machine has Lambda functions</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• LambdaFunctionsFailed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• LambdaFunctionsTimedOut</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>If state machine has activities</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ActivitiesFailed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ActivitiesTimedOut</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ActivitiesHeartbeatTimedOut</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>If state machine has service integrations</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ServiceIntegrationsFailed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ServiceIntegrationsTimedOut</td>
</tr>
<tr>
<td>API Gateway REST API stage</td>
<td>Any</td>
<td>• 4XXErrors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 5XXErrors</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Latency</td>
</tr>
<tr>
<td>Component type</td>
<td>Workload type</td>
<td>Recommended metric</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>ECS Cluster</td>
<td>Any</td>
<td>CpuUtilized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MemoryUtilized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkRxBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkTxBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RunningTaskCount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PendingTaskCount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StorageReadBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StorageWriteBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CPUReservation (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CPUUtilization (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MemoryReservation (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MemoryUtilization (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GPUReservation (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>instance_cpu_utilization (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>instance_filesystem_utilization (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>instance_memory_utilization (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>instance_network_total_bytes (EC2 Launch Type only)</td>
</tr>
<tr>
<td>Component type</td>
<td>Workload type</td>
<td>Recommended metric</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Java Application</td>
<td></td>
<td>CpuUtilized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MemoryUtilized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkRxBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkTxBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RunningTaskCount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PendingTaskCount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StorageReadBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StorageWriteBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CPUReservation (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CPUUtilization (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MemoryReservation (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MemoryUtilization (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GPUReservation (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>instance_cpu_utilization (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>instance_filesystem_utilization (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>instance_memory_utilization (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>instance_network_total_bytes (EC2 Launch Type only)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_threading_threadcount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_classloading_loadedclasscount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_memory_heapmemoryusage_used</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_memory_heapmemoryusage_committed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_operatingsystem_freephysicalmemory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_operatingsystem_freeswapspacesize</td>
</tr>
<tr>
<td>Component type</td>
<td>Workload type</td>
<td>Recommended metric</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>ECS Service</td>
<td>Any</td>
<td>CPUUtilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MemoryUtilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CpuUtilized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MemoryUtilized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkRxBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkTxBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RunningTaskCount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PendingTaskCount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StorageReadBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StorageWriteBytes</td>
</tr>
<tr>
<td>Java Application</td>
<td></td>
<td>CPUUtilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MemoryUtilization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>CpuUtilized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MemoryUtilized</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkRxBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkTxBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>RunningTaskCount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PendingTaskCount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StorageReadBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StorageWriteBytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_threading_threadcount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_classloading_loadedclasscount</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_memory_heapmemoryusage_used</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_memory_heapmemoryusage_committed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_operatingsystem_freephysicalmemory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>java_lang_operatingsystem_freeswapspacesize</td>
</tr>
<tr>
<td>Component type</td>
<td>Workload type</td>
<td>Recommended metric</td>
</tr>
<tr>
<td>----------------</td>
<td>--------------</td>
<td>--------------------</td>
</tr>
</tbody>
</table>
| EKS Cluster    | Any          | cluster_failed_node_count  
                node_cpu_reserved_capacity  
                node_cpu_utilization  
                node_filesystem_utilization  
                node_memory_reserved_capacity  
                node_memory_utilization  
                node_network_total_bytes  
                pod_cpu_reserved_capacity  
                pod_cpu_utilization  
                pod_cpu_utilization_over_pod_limit  
                pod_memory_reserved_capacity  
                pod_memory_utilization  
                pod_memory_utilization_over_pod_limit  
                pod_network_rx_bytes  
                pod_network_tx_bytes |
<table>
<thead>
<tr>
<th>Component type</th>
<th>Workload type</th>
<th>Recommended metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java Application</td>
<td>cluster_failed_node_count</td>
<td></td>
</tr>
<tr>
<td></td>
<td>node_cpu_reserved_capacity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>node_cpu_utilization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>node_filesystem_utilization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>node_memory_reserved_capacity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>node_memory_utilization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>node_network_total_bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pod_cpu_reserved_capacity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pod_cpu_utilization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pod_cpu_utilization_over_pod_limit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pod_memory_reserved_capacity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pod_memory_utilization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pod_memory_utilization_over_pod_limit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pod_network_rx_bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>pod_network_tx_bytes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java_lang_threading_threadcount</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java_lang_classloading_loadedclasscount</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java_lang_memory_heapmemoryusage_used</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java_lang_memory_heapmemoryusage_committed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java_lang_operatingsystem_freetotalmemory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java_lang_operatingsystem_freevirtualmemory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>java_lang_operatingsystem_freeswapspacesize</td>
<td></td>
</tr>
<tr>
<td>Component type</td>
<td>Workload type</td>
<td>Recommended metric</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Kubernetes Cluster on EC2</td>
<td>Any</td>
<td>cluster_failed_node_count, node_cpu_reserved_capacity, node_cpu_utilization, node_filesystem_utilization, node_memory_reserved_capacity, node_memory_utilization, node_network_total_bytes, pod_cpu_reserved_capacity, pod_cpu_utilization, pod_cpu_utilization_over_pod_limit, pod_memory_reserved_capacity, pod_memory_utilization, pod_memory_utilization_over_pod_limit, pod_network_rx_bytes, pod_network_tx_bytes</td>
</tr>
</tbody>
</table>
### Performance Counter metrics

Performance Counter metrics are recommended for instances only when the corresponding Performance Counter sets are installed on the Windows instances.

<table>
<thead>
<tr>
<th>Performance Counter metric name</th>
<th>Performance Counter set name</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET CLR Exceptions # of Exceps Thrown</td>
<td>.NET CLR Exceptions</td>
</tr>
<tr>
<td>.NET CLR Exceptions # of Exceps Thrown/Sec</td>
<td>.NET CLR Exceptions</td>
</tr>
<tr>
<td>.NET CLR Exceptions # of Filters/Sec</td>
<td>.NET CLR Exceptions</td>
</tr>
<tr>
<td>.NET CLR Exceptions # of Finallys/Sec</td>
<td>.NET CLR Exceptions</td>
</tr>
<tr>
<td>Performance Counter metric name</td>
<td>Performance Counter set name</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>.NET CLR Exceptions Throw to Catch Depth/Sec</td>
<td>.NET CLR Exceptions</td>
</tr>
<tr>
<td>.NET CLR Interop # of CCWs</td>
<td>.NET CLR Interop</td>
</tr>
<tr>
<td>.NET CLR Interop # of Stubs</td>
<td>.NET CLR Interop</td>
</tr>
<tr>
<td>.NET CLR Interop # of TLB exports/Sec</td>
<td>.NET CLR Interop</td>
</tr>
<tr>
<td>.NET CLR Interop # of TLB imports/Sec</td>
<td>.NET CLR Interop</td>
</tr>
<tr>
<td>.NET CLR Interop # of Marshaling</td>
<td>.NET CLR Interop</td>
</tr>
<tr>
<td>.NET CLR Jit % Time in Jit</td>
<td>.NET CLR Jit</td>
</tr>
<tr>
<td>.NET CLR Jit Standard Jit Failures</td>
<td>.NET CLR Jit</td>
</tr>
<tr>
<td>.NET CLR Loading % Time Loading</td>
<td>.NET CLR Loading</td>
</tr>
<tr>
<td>.NET CLR Loading Rate of Load Failures</td>
<td>.NET CLR Loading</td>
</tr>
<tr>
<td>.NET CLR LocksAndThreads Contention Rate/Sec</td>
<td>.NET CLR LocksAndThreads</td>
</tr>
<tr>
<td>.NET CLR LocksAndThreads Queue Length/Sec</td>
<td>.NET CLR LocksAndThreads</td>
</tr>
<tr>
<td>.NET CLR Memory # Total Committed Bytes</td>
<td>.NET CLR Memory</td>
</tr>
<tr>
<td>.NET CLR Memory % Time in GC</td>
<td>.NET CLR Memory</td>
</tr>
<tr>
<td>.NET CLR Networking 4.0.0.0 HttpWebRequest Average Queue Time</td>
<td>.NET CLR Networking 4.0.0.0</td>
</tr>
<tr>
<td>.NET CLR Networking 4.0.0.0 HttpWebRequests Aborted/Sec</td>
<td>.NET CLR Networking 4.0.0.0</td>
</tr>
<tr>
<td>.NET CLR Networking 4.0.0.0 HttpWebRequests Failed/Sec</td>
<td>.NET CLR Networking 4.0.0.0</td>
</tr>
<tr>
<td>.NET CLR Networking 4.0.0.0 HttpWebRequests Queued/Sec</td>
<td>.NET CLR Networking 4.0.0.0</td>
</tr>
<tr>
<td>APP_POOL_WAS Total Worker Process Ping Failures</td>
<td>APP_POOL_WAS</td>
</tr>
<tr>
<td>ASP.NET Application Restarts</td>
<td>ASP.NET</td>
</tr>
<tr>
<td>ASP.NET Applications % Managed Processor Time (estimated)</td>
<td>ASP.NET Applications</td>
</tr>
<tr>
<td>ASP.NET Applications Errors Total/Sec</td>
<td>ASP.NET Applications</td>
</tr>
<tr>
<td>ASP.NET Applications Errors Unhandled During Execution/Sec</td>
<td>ASP.NET Applications</td>
</tr>
<tr>
<td>ASP.NET Applications Requests in Application Queue</td>
<td>ASP.NET Applications</td>
</tr>
<tr>
<td>ASP.NET Applications Requests/Sec</td>
<td>ASP.NET Applications</td>
</tr>
<tr>
<td>ASP.NET Request Wait Time</td>
<td>ASP.NET</td>
</tr>
<tr>
<td>Performance Counter metric name</td>
<td>Performance Counter set name</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td>ASP.NET Requests Queued</td>
<td>ASP.NET</td>
</tr>
<tr>
<td>HTTP Service Request Queues CurrentQueueSize</td>
<td>HTTP Service Request Queues</td>
</tr>
<tr>
<td>LogicalDisk % Free Space</td>
<td>LogicalDisk</td>
</tr>
<tr>
<td>Memory % Committed Bytes In Use</td>
<td>Memory</td>
</tr>
<tr>
<td>Memory Available Mbytes</td>
<td>Memory</td>
</tr>
<tr>
<td>Memory Pages/Sec</td>
<td>Memory</td>
</tr>
<tr>
<td>Network Interface Bytes Total/Sec</td>
<td>Network Interface</td>
</tr>
<tr>
<td>Paging File % Usage</td>
<td>Paging File</td>
</tr>
<tr>
<td>PhysicalDisk % Disk Time</td>
<td>PhysicalDisk</td>
</tr>
<tr>
<td>PhysicalDisk Avg. Disk Queue Length</td>
<td>PhysicalDisk</td>
</tr>
<tr>
<td>PhysicalDisk Avg. Disk Sec/Read</td>
<td>PhysicalDisk</td>
</tr>
<tr>
<td>PhysicalDisk Avg. Disk Sec/Write</td>
<td>PhysicalDisk</td>
</tr>
<tr>
<td>PhysicalDisk Disk Read Bytes/Sec</td>
<td>PhysicalDisk</td>
</tr>
<tr>
<td>PhysicalDisk Disk Reads/Sec</td>
<td>PhysicalDisk</td>
</tr>
<tr>
<td>PhysicalDisk Disk Write Bytes/Sec</td>
<td>PhysicalDisk</td>
</tr>
<tr>
<td>PhysicalDisk Disk Writes/Sec</td>
<td>PhysicalDisk</td>
</tr>
<tr>
<td>Processor % Idle Time</td>
<td>Processor</td>
</tr>
<tr>
<td>Processor % Interrupt Time</td>
<td>Processor</td>
</tr>
<tr>
<td>Processor % Processor Time</td>
<td>Processor</td>
</tr>
<tr>
<td>Processor % User Time</td>
<td>Processor</td>
</tr>
<tr>
<td>SQLServer:Access Methods Forwarded Records/Sec</td>
<td>SQLServer:Access Methods</td>
</tr>
<tr>
<td>SQLServer:Access Methods Full Scans/Sec</td>
<td>SQLServer:Access Methods</td>
</tr>
<tr>
<td>SQLServer:Access Methods Page Splits/Sec</td>
<td>SQLServer:Access Methods</td>
</tr>
<tr>
<td>SQLServer:Buffer Manager Buffer cache hit Ratio</td>
<td>SQLServer:Buffer Manager</td>
</tr>
<tr>
<td>SQLServer:Buffer Manager Page life Expectancy</td>
<td>SQLServer:Buffer Manager</td>
</tr>
<tr>
<td>SQLServer:Database Replica File Bytes Received/sec</td>
<td>SQLServer:Database Replica</td>
</tr>
<tr>
<td>SQLServer:Database Replica Log Bytes Received/sec</td>
<td>SQLServer:Database Replica</td>
</tr>
<tr>
<td>SQLServer:Database Replica Log remaining for undo</td>
<td>SQLServer:Database Replica</td>
</tr>
<tr>
<td>SQLServer:Database Replica Log Send Queue</td>
<td>SQLServer:Database Replica</td>
</tr>
<tr>
<td>Performance Counter metric name</td>
<td>Performance Counter set name</td>
</tr>
<tr>
<td>---------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>SQLServer:Database Replica Mirrored Write Transaction/sec</td>
<td>SQLServer:Database Replica</td>
</tr>
<tr>
<td>SQLServer:Database Replica Recovery Queue</td>
<td>SQLServer:Database Replica</td>
</tr>
<tr>
<td>SQLServer:Database Replica Redo Bytes Remaining</td>
<td>SQLServer:Database Replica</td>
</tr>
<tr>
<td>SQLServer:Database Replica Redone Bytes/sec</td>
<td>SQLServer:Database Replica</td>
</tr>
<tr>
<td>SQLServer:Database Replica Total Log requiring undo</td>
<td>SQLServer:Database Replica</td>
</tr>
<tr>
<td>SQLServer:Database Replica Transaction Delay</td>
<td>SQLServer:Database Replica</td>
</tr>
<tr>
<td>SQLServer:General Statistics Processes Blocked</td>
<td>SQLServer:General Statistics</td>
</tr>
<tr>
<td>SQLServer:General Statistics User Connections</td>
<td>SQLServer:General Statistics</td>
</tr>
<tr>
<td>SQLServer:Latches Average Latch Wait Time (ms)</td>
<td>SQLServer:Latches</td>
</tr>
<tr>
<td>SQLServer:Locks Average Wait Time (ms)</td>
<td>SQLServer:Locks</td>
</tr>
<tr>
<td>SQLServer:Locks Lock Timeouts/Sec</td>
<td>SQLServer:Locks</td>
</tr>
<tr>
<td>SQLServer:Locks Lock Waits/Sec</td>
<td>SQLServer:Locks</td>
</tr>
<tr>
<td>SQLServer:Locks Number of Deadlocks/Sec</td>
<td>SQLServer:Locks</td>
</tr>
<tr>
<td>SQLServer:Memory Manager Memory Grants Pending</td>
<td>SQLServer:Memory Manager</td>
</tr>
<tr>
<td>SQLServer:SQL Statistics Batch Requests/Sec</td>
<td>SQLServer:SQL Statistics</td>
</tr>
<tr>
<td>SQLServer:SQL Statistics SQL Compilations/Sec</td>
<td>SQLServer:SQL Statistics</td>
</tr>
<tr>
<td>SQLServer:SQL Statistics SQL Re-Compilations/Sec</td>
<td>SQLServer:SQL Statistics</td>
</tr>
<tr>
<td>System Processor Queue Length</td>
<td>System</td>
</tr>
<tr>
<td>TCPv4 Connections Established</td>
<td>TCPv4</td>
</tr>
<tr>
<td>TCPv6 Connections Established</td>
<td>TCPv6</td>
</tr>
<tr>
<td>W3SVC_W3WP File Cache Flushes</td>
<td>W3SVC_W3WP</td>
</tr>
<tr>
<td>W3SVC_W3WP File Cache Misses</td>
<td>W3SVC_W3WP</td>
</tr>
<tr>
<td>W3SVC_W3WP Requests/Sec</td>
<td>W3SVC_W3WP</td>
</tr>
<tr>
<td>W3SVC_W3WP URI Cache Flushes</td>
<td>W3SVC_W3WP</td>
</tr>
<tr>
<td>W3SVC_W3WP URI Cache Misses</td>
<td>W3SVC_W3WP</td>
</tr>
<tr>
<td>Web Service Bytes Received/Sec</td>
<td>Web Service</td>
</tr>
<tr>
<td>Web Service Bytes Sent/Sec</td>
<td>Web Service</td>
</tr>
<tr>
<td>Web Service Connection Attempts/Sec</td>
<td>Web Service</td>
</tr>
</tbody>
</table>

656
<table>
<thead>
<tr>
<th>Performance Counter metric name</th>
<th>Performance Counter set name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Service Current Connections</td>
<td>Web Service</td>
</tr>
<tr>
<td>Web Service Get Requests/Sec</td>
<td>Web Service</td>
</tr>
<tr>
<td>Web Service Post Requests/Sec</td>
<td>Web Service</td>
</tr>
</tbody>
</table>
## AWS services that publish CloudWatch metrics

The following AWS services publish metrics to CloudWatch. For information about the metrics and dimensions, see the specified documentation.

<table>
<thead>
<tr>
<th>Service</th>
<th>Namespace</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Amplify</td>
<td>AWS/AmplifyHosting</td>
<td>Monitoring</td>
</tr>
<tr>
<td>Amazon API Gateway</td>
<td>AWS/ApiGateway</td>
<td>Monitor API Execution with Amazon CloudWatch</td>
</tr>
<tr>
<td>AWS App Runner</td>
<td>AWS/AppRunner</td>
<td>Viewing App Runner service metrics reported to CloudWatch</td>
</tr>
<tr>
<td>AppStream 2.0</td>
<td>AWS/AppStream</td>
<td>Monitoring Amazon AppStream 2.0 Resources</td>
</tr>
<tr>
<td>AWS AppSync</td>
<td>AWS/AppSync</td>
<td>CloudWatch Metrics</td>
</tr>
<tr>
<td>Amazon Athena</td>
<td>AWS/Athena</td>
<td>Monitoring Athena Queries with CloudWatch Metrics</td>
</tr>
<tr>
<td>AWS Backup</td>
<td>Backup</td>
<td>Monitor Metrics with CloudWatch</td>
</tr>
<tr>
<td>AWS Billing and Cost Management</td>
<td>AWS/Billing</td>
<td>Monitoring Charges with Alerts and Notifications</td>
</tr>
<tr>
<td>AWS Certificate Manager</td>
<td>AWS/CertificateManager</td>
<td>Supported CloudWatch Metrics</td>
</tr>
<tr>
<td>ACM Private CA</td>
<td>AWS/ACMPrivateCA</td>
<td>Supported CloudWatch Metrics</td>
</tr>
<tr>
<td>AWS Chatbot</td>
<td>AWS/Chatbot</td>
<td>Monitoring AWS Chatbot with Amazon CloudWatch</td>
</tr>
<tr>
<td>AWS Client VPN</td>
<td>AWS/ClientVPN</td>
<td>Monitoring with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon CloudFront</td>
<td>AWS/CloudFront</td>
<td>Monitoring CloudFront Activity Using CloudWatch</td>
</tr>
<tr>
<td>AWS CloudHSM</td>
<td>AWS/CloudHSM</td>
<td>Getting CloudWatch Metrics</td>
</tr>
<tr>
<td>Amazon CloudSearch</td>
<td>AWS/CloudSearch</td>
<td>Monitoring an Amazon CloudSearch Domain with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon CloudWatch Logs</td>
<td>AWS/Logs</td>
<td>Monitoring Usage with CloudWatch Metrics</td>
</tr>
<tr>
<td>AWS CodeBuild</td>
<td>AWS/CodeBuild</td>
<td>Monitoring AWS CodeBuild</td>
</tr>
<tr>
<td>Amazon CodeGuru Profiler</td>
<td>AWS/CodeGuruProfiler</td>
<td>Monitoring Amazon CodeGuru Profiler with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon Cognito</td>
<td>AWS/Cognito</td>
<td>Monitoring Amazon Cognito</td>
</tr>
<tr>
<td>Amazon Connect</td>
<td>AWS/Connect</td>
<td>Monitoring Amazon Connect in Amazon CloudWatch Metrics</td>
</tr>
<tr>
<td>Service</td>
<td>Namespace</td>
<td>Documentation</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Amazon Data Lifecycle Manager</td>
<td>AWS/DataLifecycleManager</td>
<td>Monitor your policies using Amazon CloudWatch</td>
</tr>
<tr>
<td>AWS DataSync</td>
<td>AWS/DataSync</td>
<td>Monitoring Your Task</td>
</tr>
<tr>
<td>AWS Database Migration Service</td>
<td>AWS/DMS</td>
<td>Monitoring AWS DMS Tasks</td>
</tr>
<tr>
<td>AWS Direct Connect</td>
<td>AWS/DX</td>
<td>Monitoring with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon DocumentDB</td>
<td>AWS/DocDB</td>
<td>Amazon DocumentDB Metrics</td>
</tr>
<tr>
<td>Amazon DynamoDB</td>
<td>AWS/DynamoDB</td>
<td>DynamoDB Metrics and Dimensions</td>
</tr>
<tr>
<td>DynamoDB Accelerator (DAX)</td>
<td>AWS/DAX</td>
<td>Viewing DAX Metrics and Dimensions</td>
</tr>
<tr>
<td>Amazon EC2</td>
<td>AWS/EC2</td>
<td>Monitoring Your Instances Using CloudWatch</td>
</tr>
<tr>
<td>Amazon EC2 Elastic Graphics</td>
<td>AWS/ElasticGPUs</td>
<td>Using CloudWatch metrics to monitor Elastic Graphics</td>
</tr>
<tr>
<td>Amazon EC2 Spot Fleet</td>
<td>AWS/EC2Spot</td>
<td>CloudWatch Metrics for Spot Fleet</td>
</tr>
<tr>
<td>Amazon EC2 Auto Scaling</td>
<td>AWS/AutoScaling</td>
<td>Monitoring Your Auto Scaling Groups and Instances Using CloudWatch</td>
</tr>
<tr>
<td>AWS Elastic Beanstalk</td>
<td>AWS/ElasticBeanstalk</td>
<td>Publishing Amazon CloudWatch Custom Metrics for an Environment</td>
</tr>
<tr>
<td>Amazon Elastic Block Store</td>
<td>AWS/EBS</td>
<td>Amazon CloudWatch Metrics for Amazon EBS</td>
</tr>
<tr>
<td>Amazon Elastic Container Service</td>
<td>AWS/ECS</td>
<td>Amazon ECS CloudWatch Metrics</td>
</tr>
<tr>
<td>Amazon ECS Cluster auto scaling</td>
<td>AWS/ECS/ManagedScaling</td>
<td>Amazon ECS cluster auto scaling</td>
</tr>
<tr>
<td>Amazon Elastic File System</td>
<td>AWS/EFS</td>
<td>Monitoring with CloudWatch</td>
</tr>
<tr>
<td>Amazon Elastic Inference</td>
<td>AWS/ElasticInference</td>
<td>Using CloudWatch Metrics to Monitor Amazon EI</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>AWS/ApplicationELB</td>
<td>CloudWatch Metrics for your Application Load Balancer</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>AWS/NetworkELB</td>
<td>CloudWatch Metrics for your Network Load Balancer</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>AWS/GatewayELB</td>
<td>CloudWatch Metrics for your Gateway Load Balancer</td>
</tr>
<tr>
<td>Service</td>
<td>Namespace</td>
<td>Documentation</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------</td>
<td>-------------------------------------------------------------------</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>AWS/ELB</td>
<td>CloudWatch Metrics for your Classic Load Balancer</td>
</tr>
<tr>
<td>Amazon Elastic Transcoder</td>
<td>AWS/ElasticTranscoder</td>
<td>Monitoring with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon ElastiCache for Memcached</td>
<td>AWS/ElastiCache</td>
<td>Monitoring Use with CloudWatch Metrics</td>
</tr>
<tr>
<td>Amazon ElastiCache for Redis</td>
<td>AWS/ElastiCache</td>
<td>Monitoring Use with CloudWatch Metrics</td>
</tr>
<tr>
<td>Amazon Elasticsearch Service</td>
<td>AWS/ES</td>
<td>Monitoring Cluster Metrics with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon EMR</td>
<td>AWS/ElasticMapReduce</td>
<td>Monitor Metrics with CloudWatch</td>
</tr>
<tr>
<td>AWS Elemental MediaConnect</td>
<td>AWS/MediaConnect</td>
<td>Monitoring MediaConnect with Amazon CloudWatch</td>
</tr>
<tr>
<td>AWS Elemental MediaConvert</td>
<td>AWS/MediaConvert</td>
<td>Using CloudWatch Metrics to View Metrics for AWS Elemental MediaConvert Resources</td>
</tr>
<tr>
<td>AWS Elemental MediaLive</td>
<td>AWS/MediaLive</td>
<td>Monitoring activity using Amazon CloudWatch metrics</td>
</tr>
<tr>
<td>AWS Elemental MediaPackage</td>
<td>AWS/MediaPackage</td>
<td>Monitoring AWS Elemental MediaPackage with Amazon CloudWatch Metrics</td>
</tr>
<tr>
<td>AWS Elemental MediaStore</td>
<td>AWS/MediaStore</td>
<td>Monitoring AWS Elemental MediaStore with Amazon CloudWatch Metrics</td>
</tr>
<tr>
<td>AWS Elemental MediaTailor</td>
<td>AWS/MediaTailor</td>
<td>Monitoring AWS Elemental MediaTailor with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon EventBridge</td>
<td>AWS/Events</td>
<td>Monitoring Amazon EventBridge</td>
</tr>
<tr>
<td>Amazon FSx for Lustre</td>
<td>AWS/FSx</td>
<td>Monitoring Amazon FSx for Lustre</td>
</tr>
<tr>
<td>Amazon FSx for Windows File Server</td>
<td>AWS/FSx</td>
<td>Monitoring Amazon FSx for Windows File Server</td>
</tr>
<tr>
<td>Amazon GameLift</td>
<td>AWS/GameLift</td>
<td>Monitor Amazon GameLift with CloudWatch</td>
</tr>
<tr>
<td>AWS Global Accelerator</td>
<td>AWS/GlobalAccelerator</td>
<td>Using Amazon CloudWatch with AWS Global Accelerator</td>
</tr>
<tr>
<td>AWS Glue</td>
<td>Glue</td>
<td>Monitoring AWS Glue Using CloudWatch Metrics</td>
</tr>
<tr>
<td>Service</td>
<td>Namespace</td>
<td>Documentation</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AWS Ground Station</td>
<td>AWS/GroundStation</td>
<td>Metrics Using Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon HealthLake</td>
<td>AWS/HealthLake</td>
<td>Monitoring HealthLake with CloudWatch</td>
</tr>
<tr>
<td>Amazon Inspector</td>
<td>AWS/Inspector</td>
<td>Monitoring Amazon Inspector Using CloudWatch</td>
</tr>
<tr>
<td>Amazon Interactive Video Service (IVS)</td>
<td>AWS/IVS</td>
<td>Monitoring Amazon IVS with Amazon CloudWatch</td>
</tr>
<tr>
<td>AWS IoT</td>
<td>AWS/IoT</td>
<td>AWS IoT Metrics and Dimensions</td>
</tr>
<tr>
<td>AWS IoT Analytics</td>
<td>AWS/IoTAnalytics</td>
<td>Namespace, Metrics, and Dimensions</td>
</tr>
<tr>
<td>AWS IoT SiteWise</td>
<td>AWS/IoTSiteWise</td>
<td>Monitoring AWS IoT SiteWise with Amazon CloudWatch</td>
</tr>
<tr>
<td>AWS IoT Things Graph</td>
<td>AWS/ThingsGraph</td>
<td>Metrics</td>
</tr>
<tr>
<td>AWS Key Management Service</td>
<td>AWS/KMS</td>
<td>Monitoring with CloudWatch</td>
</tr>
<tr>
<td>Amazon Keyspaces (for Apache Cassandra)</td>
<td>AWS/Cassandra</td>
<td>Amazon Keyspaces Metrics and Dimensions</td>
</tr>
<tr>
<td>Amazon Kinesis Data Analytics</td>
<td>AWS/KinesisAnalytics</td>
<td><em>Kinesis Data Analytics for SQL Applications</em>: Monitoring with CloudWatch</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Kinesis Data Analytics for Apache Flink</em>: Viewing Amazon Kinesis Analytics</td>
</tr>
<tr>
<td>Amazon Kinesis Data Firehose</td>
<td>AWS/Firehose</td>
<td>Monitoring Kinesis Data Firehose Using CloudWatch Metrics</td>
</tr>
<tr>
<td>Amazon Kinesis Data Streams</td>
<td>AWS/Kinesis</td>
<td>Monitoring Amazon Kinesis Data Streams with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon Kinesis Video Streams</td>
<td>AWS/KinesisVideo</td>
<td>Monitoring Kinesis Video Streams Metrics with CloudWatch</td>
</tr>
<tr>
<td>AWS Lambda</td>
<td>AWS/Lambda</td>
<td>AWS Lambda Metrics</td>
</tr>
<tr>
<td>Amazon Lex</td>
<td>AWS/Lex</td>
<td>Monitoring Amazon Lex with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon Location Service</td>
<td>AWS/Location</td>
<td>Amazon Location Service metrics exported to Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon Lookout for Metrics</td>
<td>AWS/LookoutMetrics</td>
<td>Monitoring Lookout for Metrics with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon Machine Learning</td>
<td>AWS/ML</td>
<td>Monitoring Amazon ML with CloudWatch Metrics</td>
</tr>
<tr>
<td>Service</td>
<td>Namespace</td>
<td>Documentation</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Amazon Managed Streaming for Apache Kafka</td>
<td>AWS/Kafka</td>
<td>Monitoring Amazon MSK with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon MQ</td>
<td>AWS/AmazonMQ</td>
<td>Monitoring Amazon MQ Brokers Using Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon Neptune</td>
<td>AWS/Neptune</td>
<td>Monitoring Neptune with CloudWatch</td>
</tr>
<tr>
<td>AWS Network Firewall</td>
<td>AWS/NetworkFirewall</td>
<td>AWS Network Firewall metrics in Amazon CloudWatch</td>
</tr>
<tr>
<td>AWS OpsWorks</td>
<td>AWS/OpsWorks</td>
<td>Monitoring Stacks using Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon Polly</td>
<td>AWS/Polly</td>
<td>Integrating CloudWatch with Amazon Polly</td>
</tr>
<tr>
<td>Amazon QLDB</td>
<td>AWS/QLDB</td>
<td>Amazon QLDB Metrics and Dimensions</td>
</tr>
<tr>
<td>Amazon Redshift</td>
<td>AWS/Redshift</td>
<td>Amazon Redshift Performance Data</td>
</tr>
<tr>
<td>Amazon Relational Database Service</td>
<td>AWS/RDS</td>
<td>Monitoring with Amazon CloudWatch</td>
</tr>
<tr>
<td>AWS RoboMaker</td>
<td>AWS/Robomaker</td>
<td>Monitoring AWS RoboMaker with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon Route 53</td>
<td>AWS/Route53</td>
<td>Monitoring Amazon Route 53</td>
</tr>
<tr>
<td>Amazon SageMaker</td>
<td>AWS/SageMaker</td>
<td>Monitoring SageMaker with CloudWatch</td>
</tr>
<tr>
<td>AWS SDK Metrics for Enterprise Support</td>
<td>AWS/SDKMetrics</td>
<td>Metrics and Data Collected by AWS SDK Metrics for Enterprise Support</td>
</tr>
<tr>
<td>AWS Service Catalog</td>
<td>AWS/ServiceCatalog</td>
<td>AWS Service Catalog CloudWatch Metrics</td>
</tr>
<tr>
<td>AWS Shield Advanced</td>
<td>AWS/DDoSProtection</td>
<td>Monitoring with CloudWatch</td>
</tr>
<tr>
<td>Amazon Simple Email Service</td>
<td>AWS/SES</td>
<td>Retrieving Amazon SES Event Data from CloudWatch</td>
</tr>
<tr>
<td>Amazon Simple Notification Service</td>
<td>AWS/SNS</td>
<td>Monitoring Amazon SNS with CloudWatch</td>
</tr>
<tr>
<td>Amazon Simple Queue Service</td>
<td>AWS/SQS</td>
<td>Monitoring Amazon SQS Queues Using CloudWatch</td>
</tr>
<tr>
<td>Amazon Simple Storage Service</td>
<td>AWS/S3</td>
<td>Monitoring Metrics with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon Simple Workflow Service</td>
<td>AWS/SWF</td>
<td>Amazon SWF Metrics for CloudWatch</td>
</tr>
<tr>
<td>AWS Step Functions</td>
<td>AWS/States</td>
<td>Monitoring Step Functions Using CloudWatch</td>
</tr>
<tr>
<td>Service</td>
<td>Namespace</td>
<td>Documentation</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AWS Storage Gateway</td>
<td>AWS/StorageGateway</td>
<td>Monitoring Your Gateway and Resources</td>
</tr>
<tr>
<td>AWS Systems Manager Run Command</td>
<td>AWS/SSM-RunCommand</td>
<td>Monitoring Run Command Metrics Using CloudWatch</td>
</tr>
<tr>
<td>Amazon Textract</td>
<td>AWS/Textract</td>
<td>CloudWatch Metrics for Amazon Textract</td>
</tr>
<tr>
<td>Amazon Timestream</td>
<td>AWS/Timestream</td>
<td>Timestream Metrics and Dimensions</td>
</tr>
<tr>
<td>AWS Transfer for SFTP</td>
<td>AWS/Transfer</td>
<td>AWS SFTP CloudWatch Metrics</td>
</tr>
<tr>
<td>Amazon Translate</td>
<td>AWS/Translate</td>
<td>CloudWatch Metrics and Dimensions for Amazon Translate</td>
</tr>
<tr>
<td>AWS Trusted Advisor</td>
<td>AWS/TrustedAdvisor</td>
<td>Creating Trusted Advisor Alarms Using CloudWatch</td>
</tr>
<tr>
<td>Amazon VPC</td>
<td>AWS/NATGateway</td>
<td>Monitoring Your NAT Gateway with CloudWatch</td>
</tr>
<tr>
<td>Amazon VPC</td>
<td>AWS/TransitGateway</td>
<td>CloudWatch Metrics for Your Transit Gateways</td>
</tr>
<tr>
<td>Amazon VPC</td>
<td>AWS/VPN</td>
<td>Monitoring with CloudWatch</td>
</tr>
<tr>
<td>AWS WAF</td>
<td>AWS/WAFV2 for AWS WAF</td>
<td>Monitoring with CloudWatch</td>
</tr>
<tr>
<td></td>
<td>resources WAF for AWS WAF</td>
<td></td>
</tr>
<tr>
<td></td>
<td>classic resources</td>
<td></td>
</tr>
<tr>
<td>Amazon WorkMail</td>
<td>AWS/WorkMail</td>
<td>Monitoring Amazon WorkMail with Amazon CloudWatch</td>
</tr>
<tr>
<td>Amazon WorkSpaces</td>
<td>AWS/WorkSpaces</td>
<td>Monitor Your WorkSpaces Using CloudWatch Metrics</td>
</tr>
</tbody>
</table>
Alarm events and EventBridge

CloudWatch sends events to Amazon EventBridge whenever a CloudWatch alarm changes alarm state. You can use EventBridge and these events to write rules that take actions, such as notifying you, when an alarm changes state. For more information, see What is Amazon EventBridge?

CloudWatch guarantees the delivery of alarm state change events to EventBridge.

Sample events from CloudWatch

This section includes example events from CloudWatch.

State change for a single-metric alarm

```json
{
   "version": "0",
   "id": "c4c1c1c9-6542-e61b-6ef0-8c4d36933a92",
   "detail-type": "CloudWatch Alarm State Change",
   "source": "aws.cloudwatch",
   "account": "123456789012",
   "time": "2019-10-02T17:04:40Z",
   "region": "us-east-1",
   "resources": [
      "arn:aws:cloudwatch:us-east-1:123456789012:alarm:ServerCpuTooHigh"
   ],
   "detail": {
      "alarmName": "ServerCpuTooHigh",
      "configuration": {
         "description": "Goes into alarm when server CPU utilization is too high!",
         "metrics": [
            {
               "id": "30b6c6b2-a864-43a2-4877-c09a1afc3b87",
               "metricStat": {
                  "metric": {
                     "dimensions": {
                        "InstanceId": "i-12345678901234567"
                     },
                     "name": "CPUUtilization",
                     "namespace": "AWS/EC2"
                  },
                  "period": 300,
                  "stat": "Average"
               },
               "returnData": true
            }
         ],
         "previousState": {
            "reason": "Threshold Crossed: 1 out of the last 1 datapoints [0.0666851903306472 (01/10/19 13:46:00)] was not greater than the threshold (50.0) (minimum 1 datapoint for ALARM -> OK transition).",
            "reasonData": "\"\"\"\n            ",
            "timestamp": "2019-10-01T13:56:40.000+0000",
            "statistic": "Average",
            "period": 300,
            "recentDatapoints": [0.0666851903306472],
            "threshold": 50.00,
            "value": "OK"
         }
      }
   }
}
```
State change for a metric math alarm

```json
{
    "version": "0",
    "id": "2dde0eb1-528b-d2d5-9ca6-6d590caf2329",
    "detail-type": "CloudWatch Alarm State Change",
    "source": "aws.cloudwatch",
    "account": "123456789012",
    "time": "2019-10-02T17:20:48Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:cloudwatch:us-east-1:123456789012:alarm:TotalNetworkTrafficTooHigh"
    ],
    "detail": {
        "alarmName": "TotalNetworkTrafficTooHigh",
        "configuration": {
            "description": "Goes into alarm if total network traffic exceeds 10Kb",
            "metrics": [
                {
                    "expression": "SUM(METRICS())",
                    "id": "e1",
                    "label": "Total Network Traffic",
                    "returnData": true
                },
                {
                    "id": "m1",
                    "metricStat": {
                        "metric": {
                            "dimensions": {
                                "InstanceId": "i-12345678901234567"
                            },
                            "name": "NetworkIn",
                            "namespace": "AWS/EC2"
                        },
                        "period": 300,
                        "stat": "Maximum"
                    },
                    "returnData": false
                },
                {
                    "id": "m2",
                    "metricStat": {
                        "metric": {
                            "dimensions": {
                                "InstanceId": "i-12345678901234567"
                            },
                            "name": "NetworkOut",
                            "namespace": "AWS/EC2"
                        },
                        "period": 300,
                        "stat": "Maximum"
                    },
                    "returnData": false
                }
            ]
        }
    }
}
```
State change for an anomaly detection alarm

```json
{
  "version": "0",
  "id": "daaf9f1-bddd-c6c9-83af-74971fcfc4ef",
  "detail-type": "CloudWatch Alarm State Change",
  "source": "aws.cloudwatch",
  "account": "123456789012",
  "time": "2019-10-03T16:00:04Z",
  "region": "us-east-1",
  "resources": ["arn:aws:cloudwatch:us-east-1:123456789012:alarm:EC2 CPU Utilization Anomaly"],
  "detail": {
    "alarmName": "EC2 CPU Utilization Anomaly",
    "state": {
      "value": "ALARM",
      "reason": "Thresholds Crossed: 1 out of the last 1 datapoints [0.0 (03/10/19 15:58:00)] was less than the lower thresholds [0.020599447471798756] or greater than the upper thresholds [0.3006915352732461] (minimum 1 datapoint for OK -> ALARM transition).",
      "reasonData": "{\"version\":\"1.0\",\"queryDate\":\"2019-10-03T16:00:04.650+0000\",\"startDate\":\"2019-10-03T15:58:00.000+0000\",\"period\":60,\"recentDatapoints\":\[0.0\],\"recentLowerThresholds\":\[0.020599447471798756\],\"recentUpperThresholds\":\[0.3006915352732461\]}",
      "timestamp": "2019-10-03T16:00:04.653+0000"
    },
    "previousState": {
      "value": "OK",
      "reason": "Thresholds Crossed: 1 out of the last 1 datapoints [0.16666666664241] (03/10/19 15:57:00] was not less than the lower thresholds [0.0206719426210148] or not greater than the upper thresholds [0.3007687022143803] (minimum 1 datapoint for ALARM -> OK transition).",
      "reasonData": "{\"version\":\"1.0\",\"queryDate\":\"2019-10-03T15:59:04.670+0000\",\"startDate\":\"2019-10-03T15:57:00.000+0000\",\"period\":60,\"recentDatapoints\":\[0.166666666664241\],\"recentLowerThresholds\":\[0.0206719426210148\],\"recentUpperThresholds\":\[0.3007687022143803\]}",
      "timestamp": "2019-10-03T15:59:04.672+0000"
    },
    "configuration": {
      "description": "Goes into alarm if CPU Utilization is out of band",
      "metrics": [{
        "id": "m1",
```
"metricStat": {
    "metric": {
        "namespace": "AWS/EC2",
        "name": "CPUUtilization",
        "dimensions": {
            "InstanceId": "i-12345678901234567"
        }
    },
    "period": 60,
    "stat": "Average"
},
"returnData": true
},
{
    "id": "ad1",
    "expression": "ANOMALY_DETECTION_BAND(m1, 0.8)",
    "label": "CPUUtilization (expected)",
    "returnData": true
}
Ingesting high-cardinality logs and generating metrics with CloudWatch embedded metric format

The CloudWatch embedded metric format enables you to ingest complex high-cardinality application data in the form of logs and to generate actionable metrics from them. You can embed custom metrics alongside detailed log event data, and CloudWatch automatically extracts the custom metrics so that you can visualize and alarm on them, for real-time incident detection. Additionally, the detailed log events associated with the extracted metrics can be queried using CloudWatch Logs Insights to provide deep insights into the root causes of operational events.

Embedded metric format helps you to generate actionable custom metrics from ephemeral resources such as Lambda functions and containers. By using the embedded metric format to send logs from these ephemeral resources, you can now easily create custom metrics without having to instrument or maintain separate code, while gaining powerful analytical capabilities on your log data.

When using the embedded metric format, you can generate your logs using a client library— for more information, see Using the client libraries to generate embedded metric format logs (p. 669). Alternatively, you can manually construct the logs and submit them using the PutLogEvents API or the CloudWatch agent.

Charges are incurred for logs ingestion and archival, and custom metrics that are generated. For more information, see Amazon CloudWatch Pricing.

Note
Be careful when configuring your metric extraction as it impacts your custom metric usage and corresponding bill. If you unintentionally create metrics based on high-cardinality dimensions (such as requestId), the embedded metric format will by design create a custom metric corresponding to each unique dimension combination. For more information, see Dimensions.

Topics
- Generating logs using the embedded metric format (p. 668)
- Viewing your metrics and logs in the console (p. 681)

Generating logs using the embedded metric format

You can generate embedded metric format logs with the following methods:

- Generate and send the logs by using the open-sourced client libraries
- Manually generate the logs, and then use the CloudWatch agent or the PutLogEvents API to send the logs

If you use one of the manual methods, the logs must follow the defined JSON format.
Topics

- Using the client libraries to generate embedded metric format logs (p. 669)
- Using the embedded metric format with AWS Distro for OpenTelemetry (p. 669)
- Manually generating embedded metric format logs (p. 669)

Using the client libraries to generate embedded metric format logs

Amazon provides open-sourced client libraries, which you can use to create embedded metric format logs. Currently those libraries are available in Node.js, Python, and Java. Support for other languages is planned.

The libraries and the instructions for how to use them are located on Github. Use the links in the following list.

- Node.js
- Python
- Java
- C#

Using the embedded metric format with AWS Distro for OpenTelemetry

You can use the embedded metric format as a part of the OpenTelemetry project. OpenTelemetry is an open-source initiative that removes boundaries and restrictions between vendor-specific formats for tracing, logs, and metrics by offering a single set of specifications and APIs. For more information, see OpenTelemetry.

Using embedded metric format with OpenTelemetry requires two components: an OpenTelemetry-compliant data source, and the AWS Distro for OpenTelemetry Collector enabled for use with CloudWatch embedded metric format logs.

We have preconfigured redistributions of the OpenTelemetry components, maintained by AWS, to make onboarding as easy as possible. For more information about using OpenTelemetry with embedded metric format, in addition to other AWS services, see AWS Distro for OpenTelemetry.

For additional information regarding language support and usage, see AWS Observability on Github.

Manually generating embedded metric format logs

To send embedded metric format logs that you have manually created, you can use the PutLogEvents API or the CloudWatch agent.

If you use either of these methods, you must follow the embedded metric format specification.

Topics

- Specification: Embedded metric format (p. 670)
- Using the PutLogEvents API to send manually-created embedded metric format logs (p. 675)
- Using the CloudWatch agent to send embedded metric format logs (p. 677)
Specification: Embedded metric format

The CloudWatch embedded metric format is a JSON specification used to instruct CloudWatch Logs to automatically extract metric values embedded in structured log events. You can use CloudWatch to graph and create alarms on the extracted metric values.

Embedded metric format specification conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this format specification are to be interpreted as described in Key Words RFC2119.

The terms "JSON", "JSON text", "JSON value", "member", "element", "object", "array", "number", "string", "boolean", "true", "false", and "null" in this format specification are to be interpreted as defined in JavaScript Object Notation RFC8259.

Embedded metric format specification PutLogEvents request format

Clients MUST use the following log format header when sending an embedded metric format document using the CloudWatch Logs PutLogEvents API:

```
x-amzn-logs-format: json/emf
```

On Lambda, you do not need to set this header yourself. Writing JSON to standard out in the embedded metric format is sufficient. While Lambda may prepend log events with metadata such as timestamp and request id, a valid embedded metric format document after this metadata is considered valid.

Embedded metric format document structure

This section describes the structure of an embedded metric format document, which is identified by the log-format header `x-amzn-logs-format: json/emf`. Embedded metric format documents are defined in JavaScript Object Notation RFC8259.

Unless otherwise noted, objects defined by this specification MUST NOT contain any additional members. Members not recognized by this specification MUST be ignored. Members defined in this specification are case-sensitive.

The embedded metric format is subject to the same limits as standard CloudWatch Logs events and are limited to a maximum size of 256 KB.

Root node

The LogEvent message MUST be a valid JSON object with no additional data at the beginning or end of the LogEvent message string. For more information about the LogEvent structure, see InputLogEvent.

Embedded metric format documents MUST contain the following top-level member on the root node. This is a Metadata object (p. 671) object.

```
{
    "_aws": {  
        "CloudWatchMetrics": [ ... ]
    }
}
```

The root node MUST contain all ??? (p. 672) members defined by the references in the MetricDirective object (p. 671).
The root node MAY contain any other members that are not included in the above requirements. The values of these members MUST be valid JSON types.

**Metadata object**

The _aws member can be used to represent metadata about the payload that informs downstream services how they should process the LogEvent. The value MUST be an object and MUST contain the following members:

- **CloudWatchMetrics**— An array of MetricDirective object (p. 671) used to instruct CloudWatch to extract metrics from the root node of the LogEvent.

```
{  
"_aws": {  
  "CloudWatchMetrics": [ ... ]  
}
}
```

- **Timestamp**— A number representing the time stamp used for metrics extracted from the event. Values MUST be expressed as the number of milliseconds after Jan 1, 1970 00:00:00 UTC.

```
{  
"_aws": {  
  "Timestamp": 1559748430481  
}
}
```

**MetricDirective object**

The MetricDirective object instructs downstream services that the LogEvent contains metrics that will be extracted and published to CloudWatch. MetricDirectives MUST contain the following members:

- **Namespace**— A string representing the CloudWatch namespace for the metric.
- **Dimensions**— A DimensionSet array (p. 671).
- **Metrics**— An array of MetricDefinition (p. 672) objects. This array MUST NOT contain more than 100 MetricDefinition objects.

**DimensionSet array**

A DimensionSet is an array of strings containing the dimension keys that will be applied to all metrics in the document. The values within this array MUST also be members on the root-node—referred to as the Target members (p. 672).

A DimensionSet MUST NOT contain more than 9 dimension keys. A DimensionSet MAY be empty.

The target member MUST have a string value. The target member defines a dimension that will be published as part of the metric identity. Every DimensionSet used creates a new metric in CloudWatch. For more information about dimensions, see Dimension and Dimensions.

```
{  
"_aws": {  
  "CloudWatchMetrics": [  
  {  
    "Dimensions": [ [ "functionVersion" ] ],  
    "..."  
  }  
]  
}
```
Manually generating embedded metric format logs

Note
Be careful when configuring your metric extraction as it impacts your custom metric usage and corresponding bill. If you unintentionally create metrics based on high-cardinality dimensions (such as requestId), the embedded metric format will by design create a custom metric corresponding to each unique dimension combination. For more information, see Dimensions.

MetricDefinition object

A MetricDefinition is an object that MUST contain the following member:

- **Name**—A string Reference values (p. 672) to a metric Target members (p. 672). Metric targets MUST be either a numeric value or an array of numeric values.

A MetricDefinition object MAY contain the following member:

- **Unit**—An OPTIONAL string value representing the unit of measure for the corresponding metric. Values SHOULD be valid CloudWatch metric units. For information about valid units, see MetricDatum. If a value is not provided, then a default value of NONE is assumed.

```json
{
  "_aws": {
    "CloudWatchMetrics": [
      {
        "Metrics": [
          {
            "Name": "Time",
            "Unit": "Milliseconds"
          }
        ],
        ...
      }
    ],
    "Time": 1
  }
}
```

Reference values

Reference values are string values that reference Target members (p. 672) members on the root node. These references should NOT be confused with the JSON Pointers described in RFC6901. Target values cannot be nested.

Target members

Valid targets MUST be members on the root node and cannot be nested objects. For example, a _reference_ value of "A.a" MUST match the following member:

```json
{ "A.a" }
```

It MUST NOT match the nested member:

```json
{ "A": { "a" } }
```
Valid values of target members depend on what is referencing them. A metric target MUST be a numeric value or an array of numeric values. Numeric array metric targets MUST NOT have more than 100 members. A dimension target MUST have a string value.

Embedded metric format example and JSON schema

The following is a valid example of embedded metric format.

```json
{
    "_aws": {
        "Timestamp": 1574109732004,
        "CloudWatchMetrics": [
            {
                "Namespace": "lambda-function-metrics",
                "Dimensions": [["functionVersion"]],
                "Metrics": [
                    {
                        "Name": "time",
                        "Unit": "Milliseconds"
                    }
                ]
            }
        ],
        "functionVersion": "$LATEST",
        "time": 100,
        "requestId": "989ffbf8-9ace-4817-a57c-e4dd734019ee"
    }
}
```

You can use the following schema to validate embedded metric format documents.

```json
{
    "type": "object",
    "title": "Root Node",
    "required": ["_aws"],
    "properties": {
        "_aws": {
            "id": "#/properties/_aws",
            "type": "object",
            "title": "Metadata",
            "required": ["Timestamp", "CloudWatchMetrics"],
            "properties": {
                "Timestamp": {
                    "id": "#/properties/_aws/properties/Timestamp",
                    "type": "integer",
                    "title": "The Timestamp Schema",
                    "examples": [1565375354953]
                },
                "CloudWatchMetrics": {
                    "id": "#/properties/_aws/properties/CloudWatchMetrics",
                    "type": "array",
                    "title": "MetricDirectives",
                    "items": {
                        "id": "#/properties/_aws/properties/CloudWatchMetrics/items",
                        "type": "object",
                        "title": "MetricDirective",
                        "required": ["Name", "Unit"]
                    }
                }
            }
        }
    }
}
```
"Namespace",
"Dimensions",
"Metrics"
],
"properties": {
"Namespace": {
"$id": ",
"type": "string",
"title": "CloudWatch Metrics Namespace",
"examples": [
"MyApp"
],
"pattern": "^(.*)$",
"minLength": 1,
"maxLength": 255
},
"Dimensions": {
"$id": ",
"type": "array",
"title": "The Dimensions Schema",
"minItems": 1,
"items": {
"$id": ",
"type": "array",
"title": "DimensionSet",
"minItems": 0,
"maxItems": 9,
"items": {
"$id": "#/properties/_aws/properties/CloudWatchMetrics/items/properties/Dimensions/items/item",
"type": "string",
"title": "DimensionReference",
"examples": [
"Operation"
],
"pattern": "^(.*)$",
"minLength": 1,
"maxLength": 255
}
}
},
"Metrics": {
"$id": "#/
"type": "array",
"title": "MetricDefinitions",
"items": {
"$id": "#/properties/_aws/properties/CloudWatchMetrics/items/properties/Metrics/items/item",
"type": "object",
"title": "MetricDefinition",
"required": [
"Name"
],
"properties": {
"Name": {
"$id": "#/properties/_aws/properties/CloudWatchMetrics/items/properties/Metrics/items/item/properties/Name",
"type": "string",
"title": "MetricName",
"examples": [
"ProcessingLatency"
]}}
}
Using the PutLogEvents API to send manually-created embedded metric format logs

You can send embedded metric format logs to CloudWatch Logs using the CloudWatch Logs PutLogEvents API. When calling PutLogEvents, you need to include the following HTTP header to instruct CloudWatch Logs that the metrics should be extracted.

```
x-amzn-logs-format: json/emf
```

The following is a full example using the AWS SDK for Java 2.x:

```
package org.example.basicapp;

import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.cloudwatchlogs.CloudWatchLogsClient;
import software.amazon.awssdk.services.cloudwatchlogs.model.DescribeLogStreamsRequest;
import software.amazon.awssdk.services.cloudwatchlogs.model.DescribeLogStreamsResponse;
import software.amazon.awssdk.services.cloudwatchlogs.model.PutLogEventsRequest;
import java.util.Collections;

public class EmbeddedMetricsExample {
    public static void main(String[] args) {
        final String usage = "To run this example, supply a Region code (eg. us-east-1), log group, and stream name as command line arguments" + "Ex: PutLogEvents <region-id> <log-group-name> <stream-name>";

        if (args.length != 3) {
            System.out.println(usage);
            return;
        }

        // Additional code...
    }
}
```
System.exit(1);

String regionId = args[0];
String logGroupName = args[1];
String logStreamName = args[2];

CloudWatchLogsClient logsClient = CloudWatchLogsClient.builder().region(Region.of(regionId)).build();

// A sequence token is required to put a log event in an existing stream.
// Look up the stream to find its sequence token.
String sequenceToken = getNextSequenceToken(logsClient, logGroupName, logStreamName);

// Build a JSON log using the EmbeddedMetricFormat.
long timestamp = System.currentTimeMillis();
String message = "{" +
  "_aws": {" +
  "Timestamp": " + timestamp + "," +
  "CloudWatchMetrics": [" +
  "{ "Namespace": "MyApp" , " +
  "Dimensions": ["Operation"], ["Operation", "Cell"]}," +
  "Metrics": [{ "Name": "ProcessingLatency", " +
  "Unit": "Milliseconds" }]} +
  "," +
  "}" +
  "," +
  "}", +
  "}", +
  "Operation": \"Aggregator\"," +
  "Cell": \"001\"," +
  "ProcessingLatency": 100" +
  "}"};

InputLogEvent inputLogEvent = InputLogEvent.builder()
  .message(message)
  .timestamp(timestamp)
  .build();

// Specify the request parameters.
PutLogEventsRequest putLogEventsRequest = PutLogEventsRequest.builder()
  .overrideConfiguration(builder ->
    // provide the log-format header of json/emf
    builder.headers(Collections.singletonMap("x-amzn-logs-format", Collections.singletonMap("json/emf")))
  .logEvents(Collections.singletonList(inputLogEvent))
  .logGroupName(logGroupName)
  .logStreamName(logStreamName)
  .sequenceToken(sequenceToken)
  .build();

logsClient.putLogEvents(putLogEventsRequest);
System.out.println("Successfully put CloudWatch log event");

private static String getNextSequenceToken(CloudWatchLogsClient logsClient, String logGroupName, String logStreamName) {  
  DescribeLogStreamsRequest logStreamRequest = DescribeLogStreamsRequest.builder()
    .logGroupName(logGroupName)
    .logStreamNamePrefix(logStreamName)
    .build();

  DescribeLogStreamsResponse describeLogStreamsResponse = logsClient.describeLogStreams(logStreamRequest);  
}
// Assume that a single stream is returned since a specific stream name was
// specified in the previous request.
return
describeLogStreamsResponse.logStreams().get(0).uploadSequenceToken();
}

Using the CloudWatch agent to send embedded metric format logs

To use this method, first install the CloudWatch agent for the services you want to send embedded metric format logs from, and then you can begin sending the events.

The CloudWatch agent must be version 1.230621.0 or later.

Note
You do not need to install the CloudWatch agent to send logs from Lambda functions. Lambda function timeouts are not handled automatically. This means that if your function times out before the metrics get flushed, then the metrics for that invocation will not be captured.

Installing the CloudWatch agent

Install the CloudWatch agent for each service which is to send embedded metric format logs.

Installing the CloudWatch agent on EC2

First, install the CloudWatch agent on the instance. For more information, see Installing the CloudWatch agent (p. 429).

Once you have installed the agent, configure the agent to listen on a UDP or TCP port for the embedded metric format logs. The following is an example of this configuration that listens on the default socket tcp:25888. For more information about agent configuration, see Manually create or edit the CloudWatch agent configuration file (p. 471).

```
{
  "logs": {
    "metrics_collected": {
      "emf": {}  
    }
  }
}
```

Installing the CloudWatch agent on Amazon ECS

The easiest way to deploy the CloudWatch agent on Amazon ECS is to run it as a sidecar, defining it in the same task definition as your application.

Create agent configuration file

Create your CloudWatch agent configuration file locally. In this example, the relative file path will be amazon-cloudwatch-agent.json.

For more information about agent configuration, see Manually create or edit the CloudWatch agent configuration file (p. 471).

```
{
  "logs": {
```
Push configuration to SSM Parameter Store

Enter the following command to push the CloudWatch agent configuration file to the AWS Systems Manager (SSM) Parameter Store.

```
aws ssm put-parameter
   --name "cwagentconfig" \
   --type "String" \ 
   --value "\cat amazon-cloudwatch-agent.json" \ 
   --region "{{region}}"
```

Configure the task definition

Configure your task definition to use the CloudWatch Agent and expose the TCP or UDP port. The sample task definition that you should use depends on your networking mode.

Notice that the webapp specifies the AWS_EMF_AGENT_ENDPOINT environment variable. This is used by the library and should point to the endpoint that the agent is listening on. Additionally, the cwagent specifies the CW_CONFIG_CONTENT as a "valueFrom" parameter that points to the SSM configuration that you created in the previous step.

This section contains one example for bridge mode and one example for host or awsvpc mode. For more examples of how you can configure the CloudWatch agent on Amazon ECS, see the Github samples repository.

The following is an example for bridge mode. When bridge mode networking is enabled, the agent needs to be linked to your application using the links parameter and must be addressed using the container name.

```json
{
   "containerDefinitions": [
      {
         "name": "webapp",
         "links": [ "cwagent" ],
         "image": "my-org/web-app:latest",
         "memory": 256,
         "cpu": 256,
         "environment": [{
            "name": "AWS_EMF_AGENT_ENDPOINT",
            "value": "tcp://cwagent:25888"
         }],
      },
      {
         "name": "cwagent",
         "mountPoints": [],
         "image": "public.ecr.aws/cloudwatch-agent/cloudwatch-agent:latest",
         "memory": 256,
         "cpu": 256,
         "portMappings": [{
            "protocol": "tcp",
            "containerPort": 25888
         }],
         "environment": [{
            "name": "CW_CONFIG_CONTENT",
            "valueFrom": "cwagentconfig"
         }]
      }
   ]
}
```
The following is an example for host mode or awsvpc mode. When running on these network modes, the agent can be addressed over localhost.

```json
{
    "containerDefinitions": [  
    {
      "name": "webapp",
      "image": "my-org/web-app:latest",
      "memory": 256,
      "cpu": 256,
      "environment": [{
        "name": "AWS_EMF_AGENT_ENDPOINT",
        "value": "tcp://127.0.0.1:25888"
      }]
    },
    {
      "name": "cwagent",
      "mountPoints": [],
      "image": "public.ecr.aws/cloudwatch-agent/cloudwatch-agent:latest",
      "memory": 256,
      "cpu": 256,
      "portMappings": [{
        "protocol": "tcp",
        "containerPort": 25888
      }],
      "environment": [{
        "name": "CW_CONFIG_CONTENT",
        "valueFrom": "cwagentconfig"
      }]
    }
  ]
}
```

**Note**
In awsvpc mode, you must either give a public IP address to the VPC (Fargate only), set up a NAT gateway, or set up a CloudWatch Logs VPC endpoint. For more information about setting up a NAT, see [NAT Gateways](#). For more information about setting up a CloudWatch Logs VPC endpoint, see [Using CloudWatch Logs with Interface VPC Endpoints](#).

The following is an example of how to assign a public IP address to a task that uses the Fargate launch type.

```bash
aws ecs run-task \
  --cluster {{cluster-name}} \
  --task-definition cwagent-fargate \
  --region {{region}} \
  --launch-type FARGATE \
  --network-configuration \
  "awsvpcConfiguration={subnets=[{{subnetId}}],securityGroups=[{{sgId}}],assignPublicIp=ENABLED}"
```

**Ensure permissions**
Ensure the IAM role executing your tasks has permission to read from the SSM Parameter Store. You can add this permission by attaching the [AmazonSSMReadOnlyAccess](#) policy. To do so, enter the following command.

```bash
aws iam attach-role-policy --policy-arn arn:aws:iam::aws:policy/AmazonSSMReadOnlyAccess \
```


--role-name CWAgentECSExecutionRole

Installing the CloudWatch agent on Amazon EKS

Parts of this process can be skipped if you have already installed CloudWatch Container Insights on this cluster.

Permissions

If you have not already installed Container Insights, then first ensure that your Amazon EKS nodes have the appropriate IAM permissions. They should have the CloudWatchAgentServerPolicy attached. For more information, see Verify prerequisites (p. 275).

Create ConfigMap

Create a ConfigMap for the agent. The ConfigMap also tells the agent to listen on a TCP or UDP port. Use the following ConfigMap.

```yaml
# cwagent-emf-configmap.yaml
apiVersion: v1
data:
  # Any changes here must not break the JSON format
  cwagentconfig.json: |
  { "agent": {
    "omit_hostname": true
  },
  "logs": {
    "metrics_collected": {
      "emf": {}
    }
  }
}
kind: ConfigMap
metadata:
  name: cwagentemfconfig
  namespace: default
```

If you have already installed Container Insights, add the following "emf": { } line to your existing ConfigMap.

Apply the ConfigMap

Enter the following command to apply the ConfigMap.

```
kubectl apply -f cwagent-emf-configmap.yaml
```

Deploy the agent

To deploy the CloudWatch agent as a sidecar, add the agent to your pod definition, as in the following example.

```yaml
apiVersion: v1
kind: Pod
metadata:
  name: myapp
  namespace: default
spec:
  containers:
    # Your container definitions go here
```
Using the CloudWatch agent to send embedded metric format logs

When you have the CloudWatch agent installed and running, you can send the embedded metric format logs over TCP or UDP. There are two requirements when sending the logs over the agent:

- The logs must contain a `LogGroupName` key that tells the agent which log group to use.
- Each log event must be on a single line. In other words, a log event cannot contain the newline (\n) character.

The log events must also follow the embedded metric format specification. For more information, see Specification: Embedded metric format (p. 670).

The following is an example of sending log events manually from a Linux bash shell. You can instead use the UDP socket interfaces provided by your programming language of choice.

```
echo ’{
"_aws":{"Timestamp":1574109732004, "LogGroupName":"Foo", "CloudWatchMetrics":
[{{"Namespace":"MyApp", "Dimensions":[]}, "Metrics":
[{{"Name":"ProcessingLatency", "Unit":"Milliseconds"}}]}, "Operation":"Aggregator", "ProcessingLatency":100}]
}
’ > /dev/udp/0.0.0.0/25888
```

Viewing your metrics and logs in the console

After you generate embedded metric format logs that extract metrics, you can use the CloudWatch console to view the metrics. Embedded metrics have the dimensions that you specified when you generated the logs. Also, embedded metrics that you generated using the client libraries have the following default dimensions:

- `ServiceType`
- `ServiceName`
- `LogGroup`
To view metrics that were generated from embedded metric format logs

2. In the navigation pane, choose Metrics.
3. Select a namespace that you specified for your embedded metrics when you generated them. If you used the client libraries to generate the metrics and did not specify a namespace, then select aws-embedded-metrics. This is the default namespace for embedded metrics generated using the client libraries.
4. Select a metric dimension (for example, ServiceName).
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.

Querying logs using CloudWatch Logs Insights

You can query the detailed log events associated with the extracted metrics by using CloudWatch Logs Insights to provide deep insights into the root causes of operational events. One of the benefits of extracting metrics from your logs is that you can filter your logs later by the unique metric (metric name plus unique dimension set) and metric values, to get context on the events that contributed to the aggregated metric value.

For example, to get an impacted request id or x-ray trace id, you could run the following query in CloudWatch Logs Insights.

```plaintext
filter Latency > 1000 and Operation = "Aggregator"
| fields RequestId, TraceId
```

You can also perform query-time aggregation on high-cardinality keys, such as finding the customers impacted by an event. The following example illustrates this.

```plaintext
filter Latency > 1000 and Operation = "Aggregator"
| stats count() by CustomerId
```

For more information, see Analyzing Log Data with CloudWatch Logs Insights
AWS usage metrics

CloudWatch collects metrics that track the usage of some AWS resources and APIs. These metrics are published in the AWS/Usage namespace. Usage metrics in CloudWatch allow you to proactively manage usage by visualizing metrics in the CloudWatch console, creating custom dashboards, detecting changes in activity with CloudWatch anomaly detection, and configuring alarms that alert you when usage approaches a threshold.

Some AWS services integrate these usage metrics with Service Quotas. For these services, you can use CloudWatch to manage your account’s use of your service quotas. For more information, see Visualizing your service quotas and setting alarms (p. 683).

Topics
- Visualizing your service quotas and setting alarms (p. 683)
- AWS API usage metrics (p. 684)
- CloudWatch usage metrics (p. 688)

Visualizing your service quotas and setting alarms

For some AWS services, you can use the usage metrics to visualize your current service usage on CloudWatch graphs and dashboards. You can use a CloudWatch metric math function to display the service quotas for those resources on your graphs. You can also configure alarms that alert you when your usage approaches a service quota. For more information about service quotas, see What Is Service Quotas in the Service Quotas User Guide.

Currently, the following services integrate their usage metrics with Service Quotas:

- AWS CloudHSM
- Amazon CloudWatch
- Amazon DynamoDB
- Amazon EC2
- Amazon Elastic Container Registry
- AWS Fargate
- AWS Fault Injection Simulator
- AWS Interactive Video Service
- AWS Key Management Service
- Amazon Kinesis Data Firehose
- AWS Robomaker

To visualize a service quota and optionally set an alarm

2. In the navigation pane, choose Metrics.
3. On the All metrics tab, choose Usage, and then choose By AWS Resource.
   - The list of service quota usage metrics appears.
4. Select the check box next to one of the metrics.
   - The graph displays your current usage of that AWS resource.
5. To add your service quota to the graph, do the following:
a. Choose the **Graphed metrics** tab.

b. Choose **Math expression, Start with an empty expression**. In the new row, under **Details**, enter `SERVICE_QUOTA(m1)`.

   A new line is added to the graph, displaying the service quota for the resource represented in the metric.

6. To see your current usage as a percentage of the quota, add a new expression or change the current `SERVICE_QUOTA` expression. For the new expression, use `m1/SERVICE_QUOTA(m1)*100`.

7. (Optional) To set an alarm that notifies you if you approach the service quota, do the following:

   a. On the `m1/SERVICE_QUOTA(m1)*100` row, under **Actions**, choose the alarm icon. It looks like a bell.

      The alarm creation page appears.

   b. Under **Conditions**, ensure that **Threshold type** is **Static** and **Whenever Expression1 is** is set to **Greater**. Under **than**, enter **80**. This creates an alarm that goes into ALARM state when your usage exceeds 80 percent of the quota.

   c. Choose **Next**.

   d. On the next page, select an Amazon SNS topic or create a new one, and then choose **Next**. The topic you select is notified when the alarm goes to ALARM state.

   e. On the next page, enter a name and description for the alarm, and then choose **Next**.

   f. Choose **Create alarm**.

## AWS API usage metrics

Most APIs that support AWS CloudTrail logging also report usage metrics to CloudWatch. API usage metrics in CloudWatch allow you to proactively manage API usage by visualizing metrics in the CloudWatch console, creating custom dashboards, detecting changes in activity with CloudWatch Anomaly Detection, and configuring alarms that alert when usage approaches a threshold.

The following table lists the services that report API usage metrics to CloudWatch, and the value to use for the **Service** dimension to see the usage metrics from that service.

<table>
<thead>
<tr>
<th>Service</th>
<th>Value for the <strong>Service</strong> dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexa for Business</td>
<td>A4B</td>
</tr>
<tr>
<td>AWS AppConfig</td>
<td>AWS AppConfig</td>
</tr>
<tr>
<td>Amazon AppStream</td>
<td>AppStream</td>
</tr>
<tr>
<td>AppStream 2.0 Image Builder</td>
<td>Image Builder</td>
</tr>
<tr>
<td>AWS Audit Manager</td>
<td>Audit Manager</td>
</tr>
<tr>
<td>AWS Backup</td>
<td>Backup</td>
</tr>
<tr>
<td>AWS Batch</td>
<td>Batch</td>
</tr>
<tr>
<td>AWS Budgets</td>
<td>Budgets</td>
</tr>
<tr>
<td>AWS Certificate Manager</td>
<td>Certificate Manager</td>
</tr>
<tr>
<td>Amazon Cloud Directory</td>
<td>Cloud Directory</td>
</tr>
<tr>
<td>Service</td>
<td>Value for the Service dimension</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>AWS CloudHSM</td>
<td>CloudHSM</td>
</tr>
<tr>
<td>Amazon CloudSearch</td>
<td>CloudSearch</td>
</tr>
<tr>
<td>AWS CloudShell</td>
<td>CloudShell</td>
</tr>
<tr>
<td>Amazon CloudWatch</td>
<td>CloudWatch</td>
</tr>
<tr>
<td>Amazon CloudWatch Logs</td>
<td>Logs</td>
</tr>
<tr>
<td>Amazon CloudWatch Application Insights</td>
<td>CloudWatch Application Insights</td>
</tr>
<tr>
<td>AWS CodeBuild</td>
<td>CodeBuild</td>
</tr>
<tr>
<td>AWS CodeCommit</td>
<td>CodeCommit</td>
</tr>
<tr>
<td>Amazon CodeGuru Profiler</td>
<td>CodeGuru Profiler</td>
</tr>
<tr>
<td>AWS CodePipeline</td>
<td>CodePipeline</td>
</tr>
<tr>
<td>AWS CodeStar</td>
<td>CodeStar</td>
</tr>
<tr>
<td>AWS CodeStar Connections</td>
<td>CodeStar Connections</td>
</tr>
<tr>
<td>Amazon Cognito Identity pools</td>
<td>Cognito Identity Pools</td>
</tr>
<tr>
<td>Amazon Cognito Sync</td>
<td>Cognito Sync</td>
</tr>
<tr>
<td>Amazon Comprehend</td>
<td>Comprehend</td>
</tr>
<tr>
<td>Amazon Comprehend Medical</td>
<td>Comprehend Medical</td>
</tr>
<tr>
<td>AWS Compute Optimizer</td>
<td>ComputeOptimzier</td>
</tr>
<tr>
<td>Amazon Connect</td>
<td>Connect</td>
</tr>
<tr>
<td>AWS Cost and Usage Reports</td>
<td>Cost and Usage Report</td>
</tr>
<tr>
<td>AWS Cost Explorer</td>
<td>Cost Explorer</td>
</tr>
<tr>
<td>AWS Data Exchange</td>
<td>Data Exchange</td>
</tr>
<tr>
<td>AWS Data Lifecycle Manager</td>
<td>Data Lifecycle Manager</td>
</tr>
<tr>
<td>AWS DataSync</td>
<td>DataSync</td>
</tr>
<tr>
<td>AWS DeepLens</td>
<td>AWS DeepLens</td>
</tr>
<tr>
<td>Amazon Detective</td>
<td>Detective</td>
</tr>
<tr>
<td>Device Advisor</td>
<td>Device Advisor</td>
</tr>
<tr>
<td>Application Discovery Service</td>
<td>Application Discovery Service</td>
</tr>
<tr>
<td>DynamoDB Accelerator</td>
<td>DynamoDBAccelerator</td>
</tr>
<tr>
<td>Amazon Elastic Container Registry</td>
<td>ECR Public</td>
</tr>
<tr>
<td>Amazon Elastic Kubernetes Service</td>
<td>EKS</td>
</tr>
<tr>
<td>AWS Elastic Beanstalk</td>
<td>Elastic Beanstalk</td>
</tr>
<tr>
<td>Service</td>
<td>Value for the Service dimension</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Amazon Elastic Inference</td>
<td>Elastic Inference</td>
</tr>
<tr>
<td>Elastic Load Balancing</td>
<td>Elastic Load Balancing</td>
</tr>
<tr>
<td>Amazon EMR</td>
<td>EMR Containers</td>
</tr>
<tr>
<td>AWS Firewall Manager</td>
<td>Firewall Manager</td>
</tr>
<tr>
<td>Amazon FSx</td>
<td>FSx</td>
</tr>
<tr>
<td>Amazon GameLift</td>
<td>GameLift</td>
</tr>
<tr>
<td>AWS Glue DataBrew</td>
<td>DataBrew</td>
</tr>
<tr>
<td>AWS IoT Greengrass</td>
<td>Greengrass</td>
</tr>
<tr>
<td>AWS Ground Station</td>
<td>Ground Station</td>
</tr>
<tr>
<td>Amazon Interactive Video Service</td>
<td>IVS</td>
</tr>
<tr>
<td>AWS IoT Core</td>
<td>IoT</td>
</tr>
<tr>
<td>AWS IoT Events</td>
<td>IoT Events</td>
</tr>
<tr>
<td>AWS IoT SiteWise</td>
<td>IoT Sitewise</td>
</tr>
<tr>
<td>Amazon Keyspaces (for Apache Cassandra)</td>
<td>Keyspaces</td>
</tr>
<tr>
<td>Kinesis Video Streams</td>
<td>Kinesis Video Streams</td>
</tr>
<tr>
<td>AWS Key Management Service</td>
<td>KMS</td>
</tr>
<tr>
<td>AWS Launch Wizard</td>
<td>Launch Wizard</td>
</tr>
<tr>
<td>Amazon Lookout for Vision</td>
<td>Lookout for Vision</td>
</tr>
<tr>
<td>AWS Managed Services</td>
<td>AWS Managed Services</td>
</tr>
<tr>
<td>AWS Marketplace Commerce Analytics</td>
<td>Marketplace Analytics Service</td>
</tr>
<tr>
<td>AWS Elemental MediaConvert</td>
<td>MediaConvert</td>
</tr>
<tr>
<td>AWS Elemental MediaLive</td>
<td>MediaLive</td>
</tr>
<tr>
<td>AWS Elemental MediaTailor</td>
<td>MediaTailor</td>
</tr>
<tr>
<td>AWS OpsWorks</td>
<td>OpsWorks</td>
</tr>
<tr>
<td>AWS OpsWorks for Configuration Management</td>
<td>OpsWorks CM</td>
</tr>
<tr>
<td>AWS Outposts</td>
<td>Outposts</td>
</tr>
<tr>
<td>Amazon RDS Performance Insights</td>
<td>Performance Insights</td>
</tr>
<tr>
<td>AWS Certificate Manager Private Certificate Authority</td>
<td>Private Certificate Authority</td>
</tr>
<tr>
<td>AWS Proton</td>
<td>Proton</td>
</tr>
<tr>
<td>Amazon Quantum Ledger Database (Amazon QLDB)</td>
<td>QLDB</td>
</tr>
</tbody>
</table>

686
<table>
<thead>
<tr>
<th>Service</th>
<th>Value for the Service dimension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Redshift</td>
<td>Redshift Data API</td>
</tr>
<tr>
<td>Amazon Rekognition</td>
<td>Rekognition</td>
</tr>
<tr>
<td>AWS Resource Access Manager</td>
<td>Resource Access Manager</td>
</tr>
<tr>
<td>AWS Resource Groups</td>
<td>Resource Groups</td>
</tr>
<tr>
<td>AWS Resource Groups Tagging API</td>
<td>Resource Groups Tagging API</td>
</tr>
<tr>
<td>AWS RoboMaker</td>
<td>RoboMaker</td>
</tr>
<tr>
<td>Amazon Route 53 Domains</td>
<td>Route 53 Domains</td>
</tr>
<tr>
<td>Amazon S3 Glacier</td>
<td>Amazon S3 Glacier</td>
</tr>
<tr>
<td>Savings Plans</td>
<td>Savings Plans</td>
</tr>
<tr>
<td>AWS Secrets Manager</td>
<td>Secrets Manager</td>
</tr>
<tr>
<td>AWS Security Hub</td>
<td>Security Hub</td>
</tr>
<tr>
<td>Service Quotas</td>
<td>Service Quotas</td>
</tr>
<tr>
<td>AWS Signer</td>
<td>Signer</td>
</tr>
<tr>
<td>Amazon Simple Notification Service</td>
<td>SNS</td>
</tr>
<tr>
<td>Amazon Simple Queue Service</td>
<td>SQS</td>
</tr>
<tr>
<td>AWS SSO Identity Store</td>
<td>Identity Store</td>
</tr>
<tr>
<td>AWS Storage Gateway</td>
<td>Storage Gateway</td>
</tr>
<tr>
<td>AWS Support</td>
<td>Support</td>
</tr>
<tr>
<td>Amazon Simple Workflow Service</td>
<td>SWF</td>
</tr>
<tr>
<td>Amazon Textract</td>
<td>Textract</td>
</tr>
<tr>
<td>AWS IoT Things Graph</td>
<td>ThingsGraph</td>
</tr>
<tr>
<td>Amazon Transcribe</td>
<td>Transcribe</td>
</tr>
<tr>
<td>Amazon Transcribe streaming transcription</td>
<td>Transcribe Streaming</td>
</tr>
<tr>
<td>AWS WAF</td>
<td>WAF</td>
</tr>
<tr>
<td>Amazon WorkSpaces</td>
<td>Workspaces</td>
</tr>
<tr>
<td>AWS X-Ray</td>
<td>X-Ray</td>
</tr>
</tbody>
</table>

Some services report usage metrics for additional APIs as well. To see whether an API reports usage metrics to CloudWatch, use the CloudWatch console to see the metrics reported by that service in the AWS/Usage namespace.

**To see the list of a service's APIs that report usage metrics to CloudWatch**

2. In the navigation pane, choose **Metrics**.
3. On the **All metrics** tab, choose **Usage**, and then choose **By AWS Resource**.
4. In the search box near the list of metrics, enter the name of the service. The metrics are filtered by the service you entered.

## CloudWatch usage metrics

CloudWatch collects metrics that track the usage of some AWS resources. These metrics correspond to AWS service quotas. Tracking these metrics can help you proactively manage your quotas. For more information, see [Visualizing your service quotas and setting alarms](p. 683).

Service quota usage metrics are in the `AWS/Usage` namespace and are collected every minute.

Currently, the only metric name in this namespace that CloudWatch publishes is `CallCount`. This metric is published with the dimensions `Resource`, `Service`, and `Type`. The `Resource` dimension specifies the name of the API operation being tracked. For example, the `CallCount` metric with the dimensions "Service": "CloudWatch", "Type": "API" and "Resource": "PutMetricData" indicates the number of times the CloudWatch `PutMetricData` API operation has been called in your account.

The `CallCount` metric does not have a specified unit. The most useful statistic for the metric is `SUM`, which represents the total operation count for the 1-minute period.

### Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CallCount</td>
<td>The number of specified operations performed in your account.</td>
</tr>
</tbody>
</table>

### Dimensions

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>The name of the AWS service containing the resource. For CloudWatch usage metrics, the value for this dimension is <code>CloudWatch</code>.</td>
</tr>
<tr>
<td>Class</td>
<td>The class of resource being tracked. CloudWatch API usage metrics use this dimension with a value of <code>None</code>.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of resource being tracked. Currently, when the <code>Service</code> dimension is <code>CloudWatch</code>, the only valid value for <code>Type</code> is <code>API</code>.</td>
</tr>
<tr>
<td>Resource</td>
<td>The name of the API operation. Valid values include the following: <code>DeleteAlarms</code>, <code>DeleteDashboards</code>, <code>DescribeAlarmHistory</code>, <code>DescribeAlarms</code>, <code>GetDashboard</code>, <code>GetMetricData</code>, <code>GetMetricStatistics</code>, <code>ListMetrics</code>, <code>PutDashboard</code>, and <code>PutMetricData</code></td>
</tr>
</tbody>
</table>
CloudWatch tutorials

The following scenarios illustrate uses of Amazon CloudWatch. In the first scenario, you use the CloudWatch console to create a billing alarm that tracks your AWS usage and lets you know when you have exceeded a certain spending threshold. In the second, more advanced scenario, you use the AWS Command Line Interface (AWS CLI) to publish a single metric for a hypothetical application named GetStarted.

Scenarios

- Monitor your estimated charges (p. 689)
- Publish metrics (p. 691)

Scenario: Monitor your estimated charges using CloudWatch

In this scenario, you create an Amazon CloudWatch alarm to monitor your estimated charges. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data.

Billing metric data is stored in the US East (N. Virginia) Region and reflects worldwide charges. This data includes the estimated charges for every service in AWS that you use, as well as the estimated overall total of your AWS charges.

You can choose to receive alerts by email when charges have exceeded a certain threshold. These alerts are triggered by CloudWatch and messages are sent using Amazon Simple Notification Service (Amazon SNS).

Tasks

- Step 1: Enable billing alerts (p. 689)
- Step 2: Create a billing alarm (p. 690)
- Step 3: Check the alarm status (p. 691)
- Step 4: Edit a billing alarm (p. 691)
- Step 5: Delete a billing alarm (p. 691)

Step 1: Enable billing alerts

Before you can create an alarm for your estimated charges, you must enable billing alerts, so that you can monitor your estimated AWS charges and create an alarm using billing metric data. After you enable billing alerts, you cannot disable data collection, but you can delete any billing alarms that you created.

After you enable billing alerts for the first time, it takes about 15 minutes before you can view billing data and set billing alarms.

Requirements

- You must be signed in using account root user credentials or as an IAM user that has been given permission to view billing information.
• For consolidated billing accounts, billing data for each linked account can be found by logging in as the paying account. You can view billing data for total estimated charges and estimated charges by service for each linked account, in addition to the consolidated account.
• In a consolidated billing account, member linked account metrics are captured only if the payer account enables the Receive Billing Alerts preference. If you change which account is your master/payer account, you must enable the billing alerts in the new master/payer account.
• The account must not be part of the Amazon Partner Network (APN) because billing metrics are not published to CloudWatch for APN accounts. For more information, see AWS Partner Network.

To enable monitoring of your estimated charges
2. In the navigation pane, choose Preferences.
4. Choose Save preferences.

**Step 2: Create a billing alarm**

**Important**
Before you can create a billing alarm, you must enable billing alerts in your account, or in the master/payer account if you are using consolidated billing. For more information, see Enabling billing alerts (p. 130).

After you've enabled billing alerts, you can create a billing alarm. In this scenario, you create an alarm that sends an email message when your estimated charges for AWS exceed a specified threshold.

**Note**
This procedure uses the simple options. To use the advanced options, see Creating a billing alarm (p. 131) in Create a Billing Alarm to Monitor Your Estimated AWS Charges.

**To create a billing alarm**

2. If necessary, change the Region to US East (N. Virginia). Billing metric data is stored in this Region and reflects worldwide charges.
3. In the navigation pane, choose Alarms, Create Alarm.
4. Choose Select metric, Billing, Total Estimated Charge.
5. Select the checkbox next to EstimatedCharges and choose Select metric.
6. For Whenever my total AWS charges for the month exceed, specify the monetary amount (for example, 200) that must be exceeded to trigger the alarm and send an email notification. Then choose Next.

**Tip**
The graph shows a current estimate of your charges that you can use to set an appropriate amount.
7. For send a notification to, do one of the following:
   • Choose Select an existing SNS topic and then select the topic to notify under Send a notification to.
   • Choose Create a new topic and then type a name for the new SNS topic and enter the email addresses that are to receive the notifications. Separate the email names with commas.
8. Choose Create Alarm.
Step 3: Check the alarm status

Now, check the status of the billing alarm that you just created.

To check the alarm status

2. If necessary, change the Region to US East (N. Virginia). Billing metric data is stored in this Region and reflects worldwide charges.
3. In the navigation pane, choose Alarms.
4. Select the check box next to the alarm. Until the subscription is confirmed, it is shown as "Pending confirmation". After the subscription is confirmed, refresh the console to show the updated status.

Step 4: Edit a billing alarm

For example, you may want to increase the amount of money you spend with AWS each month from $200 to $400. You can edit your existing billing alarm and increase the monetary amount that must be exceeded before the alarm is triggered.

To edit a billing alarm

2. If necessary, change the Region to US East (N. Virginia). Billing metric data is stored in this Region and reflects worldwide charges.
3. In the navigation pane, choose Alarms.
4. Select the check box next to the alarm and choose Actions, Modify.
5. For Whenever my total AWS charges for the month exceed, specify the new amount that must be exceeded to trigger the alarm and send an email notification.
6. Choose Save Changes.

Step 5: Delete a billing alarm

If you no longer need your billing alarm, you can delete it.

To delete a billing alarm

2. If necessary, change the Region to US East (N. Virginia). Billing metric data is stored in this Region and reflects worldwide charges.
3. In the navigation pane, choose Alarms.
4. Select the check box next to the alarm and choose Actions, Delete.
5. When prompted for confirmation, choose Yes, Delete.

Scenario: Publish metrics to CloudWatch

In this scenario, you use the AWS Command Line Interface (AWS CLI) to publish a single metric for a hypothetical application named GetStarted. If you haven't already installed and configured the AWS CLI, see Getting Set Up with the AWS Command Line Interface in the AWS Command Line Interface User Guide.
Step 1: Define the data configuration

In this scenario, you publish data points that track the request latency for the application. Choose names for your metric and namespace that make sense to you. For this example, name the metric RequestLatency and place all of the data points into the GetStarted namespace.

You publish several data points that collectively represent three hours of latency data. The raw data comprises 15 request latency readings distributed over three hours. Each reading is in milliseconds:

- Hour one: 87, 51, 125, 235
- Hour two: 121, 113, 189, 65, 89
- Hour three: 100, 47, 133, 98, 100, 328

You can publish data to CloudWatch as single data points or as an aggregated set of data points called a statistic set. You can aggregate metrics to a granularity as low as one minute. You can publish the aggregated data points to CloudWatch as a set of statistics with four predefined keys: Sum, Minimum, Maximum, and SampleCount.

You publish the data points from hour one as single data points. For the data from hours two and three, you aggregate the data points and publish a statistic set for each hour. The key values are shown in the following table.

<table>
<thead>
<tr>
<th>Hour</th>
<th>Raw data</th>
<th>Sum</th>
<th>Minimum</th>
<th>Maximum</th>
<th>SampleCount</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>87</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>51</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>125</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>235</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>121, 113, 189, 65, 89</td>
<td>577</td>
<td>65</td>
<td>189</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>100, 47, 133, 98, 100, 328</td>
<td>806</td>
<td>47</td>
<td>328</td>
<td>6</td>
</tr>
</tbody>
</table>

Step 2: Add metrics to CloudWatch

After you have defined your data configuration, you are ready to add data.

To publish data points to CloudWatch

1. At a command prompt, run the following put-metric-data commands to add data for the first hour. Replace the example timestamp with a timestamp that is two hours in the past, in Universal Coordinated Time (UTC).

```bash
aws cloudwatch put-metric-data --metric-name RequestLatency --namespace GetStarted \
```
Step 3: Get statistics from CloudWatch

Now that you have published metrics to CloudWatch, you can retrieve statistics based on those metrics using the `get-metric-statistics` command as follows. Be sure to specify `--start-time` and `--end-time` far enough in the past to cover the earliest timestamp that you published.

```bash
aws cloudwatch get-metric-statistics --namespace GetStarted --metric-name RequestLatency --statistics Average --start-time 2016-10-14T00:00:00Z --end-time 2016-10-15T00:00:00Z --period 60
```

The following is example output:

```json
{
  "Datapoints": [],
  "Label": "Request:Latency"
}
```

Step 4: View graphs with the console

After you have published metrics to CloudWatch, you can use the CloudWatch console to view statistical graphs.

To view graphs of your statistics on the console

2. In the Navigation pane, choose Metrics.
3. On the All metrics tab, in the search box, type RequestLatency and press Enter.
4. Select the check box for the RequestLatency metric. A graph of the metric data is displayed in the upper pane.

For more information, see Graphing metrics (p. 66).
Tagging your Amazon CloudWatch resources

A tag is a custom attribute label that you or AWS assigns to an AWS resource. Each tag has two parts:

- A tag key (for example, CostCenter, Environment, or Project). Tag keys are case sensitive.
- An optional field known as a tag value (for example, 111122223333 or Production). Omitting the tag value is the same as using an empty string. Like tag keys, tag values are case sensitive.

Tags help you do the following:

- Identify and organize your AWS resources. Many AWS services support tagging, so you can assign the same tag to resources from different services to indicate that the resources are related. For example, you can assign the same tag to a CloudWatch rule that you assign to an EC2 instance.
- Track your AWS costs. You activate these tags on the AWS Billing and Cost Management dashboard. AWS uses the tags to categorize your costs and deliver a monthly cost allocation report to you. For more information, see Use Cost Allocation Tags in the AWS Billing and Cost Management User Guide.

The following sections provide more information about tags for CloudWatch.

Supported resources in CloudWatch

The following resources in CloudWatch support tagging:

- Alarms – You can tag alarms using the tag-resource AWS CLI command and the TagResource API.
- Canaries – You can tag canaries using the CloudWatch console. For more information, see Creating a canary (p. 138).
- Contributor Insights rules – You can tag Contributor Insights rules when you create them by using the put-insight-rule AWS CLI command and the PutInsightRule API. You can add tags to existing rules by using the tag-resource AWS CLI command and the TagResource API.
- Metric streams – You can tag metric streams when you create them by using the put-metric-stream AWS CLI command and the PutMetricStream API. You can add tags to existing metric streams by using the tag-resource AWS CLI command and the TagResource API.

For information about adding and managing tags, see Managing tags (p. 694).

Managing tags

Tags consist of the Key and Value properties on a resource. You can use the CloudWatch console, the AWS CLI, or the CloudWatch API to add, edit, or delete the values for these properties. For information about working with tags, see the following:

- TagResource, UntagResource, and ListTagsForResource in the Amazon CloudWatch API Reference
- tag-resource, untag-resource, and list-tags-for-resource in the Amazon CloudWatch CLI Reference
Tag naming and usage conventions

The following basic naming and usage conventions apply to using tags with CloudWatch resources:

- Each resource can have a maximum of 50 tags.
- For each resource, each tag key must be unique, and each tag key can have only one value.
- The maximum tag key length is 128 Unicode characters in UTF-8.
- The maximum tag value length is 256 Unicode characters in UTF-8.
- Allowed characters are letters, numbers, spaces representable in UTF-8, and the following characters: . : * = @ _ / - (hyphen).
- Tag keys and values are case sensitive. As a best practice, decide on a strategy for capitalizing tags and consistently implement that strategy across all resource types. For example, decide whether to use Costcenter, costcenter, or CostCenter and use the same convention for all tags. Avoid using similar tags with inconsistent case treatment.
- The aws: prefix is prohibited for tags because it's reserved for AWS use. You can't edit or delete tag keys or values with this prefix. Tags with this prefix don't count against your tags per resource limit.
Security in Amazon CloudWatch

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS Compliance Programs. To learn about the compliance programs that apply to WorkSpaces, see AWS Services in Scope by Compliance Program.

- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company’s requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon CloudWatch. It shows you how to configure Amazon CloudWatch to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your CloudWatch resources.

Contents

- Data protection in Amazon CloudWatch (p. 696)
- Identity and access management for Amazon CloudWatch (p. 697)
- Compliance validation for Amazon CloudWatch (p. 736)
- Resilience in Amazon CloudWatch (p. 736)
- Infrastructure security in Amazon CloudWatch (p. 737)
- Using CloudWatch and CloudWatch Synthetics with interface VPC endpoints (p. 737)
- Security considerations for Synthetics canaries (p. 741)

Data protection in Amazon CloudWatch

The AWS shared responsibility model applies to data protection in Amazon CloudWatch. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the AWS Security Blog.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.
• Set up API and user activity logging with AWS CloudTrail.
• Use AWS encryption solutions, along with all default security controls within AWS services.
• Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.
• If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers’ email addresses, into tags or free-form fields such as a Name field. This includes when you work with CloudWatch or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Encryption in transit
CloudWatch uses end-to-end encryption of data in transit.

Identity and access management for Amazon CloudWatch
Access to Amazon CloudWatch requires credentials. Those credentials must have permissions to access AWS resources, such as retrieving CloudWatch metric data about your cloud resources. The following sections provide details about how you can use AWS Identity and Access Management (IAM) and CloudWatch to help secure your resources by controlling who can access them:

• Authentication (p. 697)
• Access control (p. 698)

Authentication
You can access AWS as any of the following types of identities:

• AWS account root user – When you sign up for AWS, you provide an email address and password that is associated with your AWS account. These are your AWS account user credentials and they provide complete access to all of your AWS resources.

  Important
  For security reasons, we recommend that you use the AWS account user credentials only to create an administrator, which is an IAM user with full permissions to your account. Then, you can use this administrator to create other IAM users and roles with limited permissions. For more information, see IAM Best Practices and Creating an Admin User and Group in the IAM User Guide.

• IAM user – An IAM user is an identity within your AWS account that has specific custom permissions (for example, permissions to view metrics in CloudWatch). You can use an IAM user name and password to sign in to secure AWS webpages like the AWS Management Console, AWS Discussion Forums, or the AWS Support Center.
In addition to a user name and password, you can also generate access keys for each user. You can use these keys when you access AWS services programmatically, either through one of the several SDKs or by using the AWS Command Line Interface (CLI). The SDK and AWS CLI tools use the access keys to cryptographically sign your request. If you don’t use the AWS tools, you must sign the request yourself. CloudWatch supports Signature Version 4, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 Signing Process in the AWS General Reference.

- **IAM role** – An IAM role is another IAM identity you can create in your account that has specific permissions. It is similar to an IAM user, but it is not associated with a specific person. An IAM role enables you to obtain temporary access keys that can be used to access AWS services and resources. IAM roles with temporary credentials are useful in the following situations:

  - **Federated user access** – Instead of creating an IAM user, you can use preexisting identities from AWS Directory Service, your enterprise user directory, or a web identity provider (IdP). These are known as federated users. AWS assigns a role to a federated user when access is requested through an IdP. For more information, see Federated Users and Roles in the IAM User Guide.

  - **Cross-account access** – You can use an IAM role in your account to grant another AWS account permissions to access your account’s resources. For an example, see Tutorial: Delegate Access Across AWS Accounts Using IAM Roles in the IAM User Guide.

  - **AWS service access** – You can use an IAM role in your account to grant an AWS service the permissions needed to access your account’s resources. For example, you can create a role that allows Amazon Redshift to access an Amazon S3 bucket on your behalf and then load data stored in the bucket into an Amazon Redshift cluster. For more information, see Creating a Role to Delegate Permissions to an AWS Service in the IAM User Guide.

  - **Applications running on Amazon EC2** – Instead of storing access keys within the EC2 instance for use by applications running on the instance and making API requests, you can use an IAM role to manage temporary credentials for these applications. To assign an AWS role to an EC2 instance and make it available to all of its applications, you can create an instance profile that is attached to the instance. An instance profile contains the role and enables programs running on the EC2 instance to get temporary credentials. For more information, see Using Roles for Applications on Amazon EC2 in the IAM User Guide.

**Access control**

You can have valid credentials to authenticate your requests, but unless you have permissions you cannot create or access CloudWatch resources. For example, you must have permissions to create CloudWatch dashboard widgets, view metrics, and so on.

The following sections describe how to manage permissions for CloudWatch. We recommend that you read the overview first.

- Overview of managing access permissions to your CloudWatch resources (p. 699)
- Using identity-based policies (IAM policies) for CloudWatch (p. 702)
- Amazon CloudWatch permissions reference (p. 727)
CloudWatch dashboard permissions update

On May 1, 2018, AWS changed the permissions required to access CloudWatch dashboards. Dashboard access in the CloudWatch console now requires permissions that were introduced in 2017 to support dashboard API operations:

- `cloudwatch:GetDashboard`
- `cloudwatch:ListDashboards`
- `cloudwatch:PutDashboard`
- `cloudwatch:DeleteDashboards`

To access CloudWatch dashboards, you need one of the following:

- The [AdministratorAccess](https://docs.aws.amazon.com/iam/latest/userguide/permissions.html) policy.
- The [CloudWatchFullAccess](https://docs.aws.amazon.com/iam/latest/userguide/permissions.html) policy.
- A custom policy that includes one or more of these specific permissions:
  - `cloudwatch:GetDashboard` and `cloudwatch:ListDashboards` to be able to view dashboards
  - `cloudwatch:PutDashboard` to be able to create or modify dashboards
  - `cloudwatch:DeleteDashboards` to be able to delete dashboards

For more information for changing permissions for an IAM user using policies, see [Changing Permissions for an IAM User](https://docs.aws.amazon.com/iam/latest/userguide/permissions.html).

For more information about CloudWatch permissions, see [Amazon CloudWatch permissions reference](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/permissions.html) (p. 727).

For more information about dashboard API operations, see [PutDashboard](https://docs.aws.amazon.com/AmazonCloudWatch/latest/APIReference/API_PutDashboard.html) in the Amazon CloudWatch API Reference.

### Overview of managing access permissions to your CloudWatch resources

Every AWS resource is owned by an AWS account, and permissions to create or access a resource are governed by permissions policies. An account administrator can attach permissions policies to IAM identities (that is, users, groups, and roles), and some services (such as AWS Lambda) also support attaching permissions policies to resources.

**Note**

An [account administrator](https://docs.aws.amazon.com/IAM/latest/userguide/permissions.html) (or administrator IAM user) is a user with administrator privileges. For more information, see [IAM best practices](https://docs.aws.amazon.com/iam/latest/userguide/permissions.html) in the [IAM User Guide](https://docs.aws.amazon.com/iam/latest/userguide/permissions.html).

When granting permissions, you decide who is getting the permissions, the resources they get permissions for, and the specific actions that you want to allow on those resources.

**Topics**

- CloudWatch resources and operations (p. 700)
- Understanding resource ownership (p. 700)
- Managing access to resources (p. 701)
- Specifying policy elements: Actions, effects, and principals (p. 701)
- Specifying conditions in a policy (p. 702)
CloudWatch resources and operations

You can restrict access to specific alarms and dashboards by using their Amazon Resource Names (ARNs) in your policies. For more information, see Actions, Resources, and Condition Keys for Amazon CloudWatch in the IAM User Guide.

You use an * (asterisk) as the resource when writing a policy to control access to CloudWatch actions. For example:

```json
{
    "Version": "2012-10-17",
    "Statement": [{
        "Effect": "Allow",
        "Action": ["cloudwatch:GetMetricData", "cloudwatch:ListMetrics"],
        "Resource": "*",
        "Condition": {
            "Bool": {
                "aws:SecureTransport": "true"
            }
        }
    }]
}
```

For more information about ARNs, see ARNs in IAM User Guide. For information about CloudWatch Logs ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces in the Amazon Web Services General Reference. For an example of a policy that covers CloudWatch actions, see Using identity-based policies (IAM policies) for CloudWatch (p. 702).

<table>
<thead>
<tr>
<th>Action</th>
<th>ARN (with Region)</th>
<th>ARN (for use with IAM role)</th>
</tr>
</thead>
</table>

Understanding resource ownership

The AWS account owns the resources that are created in the account, regardless of who created the resources. Specifically, the resource owner is the AWS account of the principal entity (that is, the AWS account root user, an IAM user, or an IAM role) that authenticates the resource creation request. CloudWatch does not have any resources that you can own.
Managing access to resources

A permissions policy describes who has access to what. The following section explains the available options for creating permissions policies.

Note
This section discusses using IAM in the context of CloudWatch. It doesn't provide detailed information about the IAM service. For complete IAM documentation, see What is IAM? in the IAM User Guide. For information about IAM policy syntax and descriptions, see IAM policy reference in the IAM User Guide.

Policies attached to an IAM identity are referred to as identity-based policies (IAM policies) and policies attached to a resource are referred to as resource-based policies. CloudWatch supports only identity-based policies.

Topics
- Identity-based policies (IAM policies) (p. 701)
- Resource-based policies (IAM policies) (p. 701)

Identity-based policies (IAM policies)

You can attach policies to IAM identities. For example, you can do the following:

- **Attach a permissions policy to a user or a group in your account** – To grant a user permissions to create an Amazon CloudWatch resource, such as metrics, you can attach a permissions policy to a user or group that the user belongs to.

- **Attach a permissions policy to a role (grant cross-account permissions)** – You can attach an identity-based permissions policy to an IAM role to grant cross-account permissions. For example, the administrator in account A can create a role to grant cross-account permissions to another AWS account (for example, account B) or an AWS service as follows:
  1. Account A administrator creates an IAM role and attaches a permissions policy to the role that grants permissions on resources in account A.
  2. Account A administrator attaches a trust policy to the role identifying account B as the principal who can assume the role.
  3. Account B administrator can then delegate permissions to assume the role to any users in account B. Doing this allows users in account B to create or access resources in account A. The principal in the trust policy can also be an AWS service principal if you want to grant an AWS service permissions to assume the role.

For more information about using IAM to delegate permissions, see Access management in the IAM User Guide.

For more information about using identity-based policies with CloudWatch, see Using identity-based policies (IAM policies) for CloudWatch (p. 702). For more information about users, groups, roles, and permissions, see Identities (Users, Groups, and Roles) in the IAM User Guide.

Resource-based policies (IAM policies)

Other services, such as Amazon S3, also support resource-based permissions policies. For example, you can attach a policy to an Amazon S3 bucket to manage access permissions to that bucket. CloudWatch doesn't support resource-based policies.

Specifying policy elements: Actions, effects, and principals

For each CloudWatch resource, the service defines a set of API operations. To grant permissions for these API operations, CloudWatch defines a set of actions that you can specify in a policy. Some API operations
can require permissions for more than one action in order to perform the API operation. For more information about resources and API operations, see CloudWatch resources and operations (p. 700) and CloudWatch Actions.

The following are the basic policy elements:

- **Resource** – Use an Amazon Resource Name (ARN) to identify the resource that the policy applies to. CloudWatch does not have any resources for you to control using policies resources, so use the wildcard character (*) in IAM policies. For more information, see CloudWatch resources and operations (p. 700).

- **Action** – Use action keywords to identify resource operations that you want to allow or deny. For example, the `cloudwatch:ListMetrics` permission allows the user permissions to perform the ListMetrics operation.

- **Effect** – You specify the effect, either allow or deny, when the user requests the specific action. If you don't explicitly grant access to (allow) a resource, access is implicitly denied. You can also explicitly deny access to a resource, which you might do to make sure that a user cannot access it, even if a different policy grants access.

- **Principal** – In identity-based policies (IAM policies), the user that the policy is attached to is the implicit principal. For resource-based policies, you specify the user, account, service, or other entity that you want to receive permissions (applies to resource-based policies only). CloudWatch doesn't support resource-based policies.

To learn more about IAM policy syntax and descriptions, see AWS IAM JSON Policy Reference in the IAM User Guide.

For a table showing all of the CloudWatch API actions and the resources that they apply to, see Amazon CloudWatch permissions reference (p. 727).

**Specifying conditions in a policy**

When you grant permissions, you can use the access policy language to specify the conditions when a policy should take effect. For example, you might want a policy to be applied only after a specific date. For more information about specifying conditions in a policy language, see Condition in the IAM User Guide.

To express conditions, you use predefined condition keys. For a list of context keys supported by each AWS service and a list of AWS-wide policy keys, see Actions, resources, and condition keys for AWS services and Global and IAM Condition Context Keys in the IAM User Guide.

**Using identity-based policies (IAM policies) for CloudWatch**

This topic provides examples of identity-based policies that demonstrate how an account administrator can attach permissions policies to IAM identities (that is, users, groups, and roles) and thereby grant permissions to perform operations on CloudWatch resources.

**Important**

We recommend that you first review the introductory topics that explain the basic concepts and options available to manage access to your CloudWatch resources. For more information, see Access control (p. 698).

The sections in this topic cover the following:

- Permissions required to use the CloudWatch console (p. 703)
- AWS managed (predefined) policies for CloudWatch (p. 705)
- Customer managed policy examples (p. 711)
The following shows an example of a permissions policy.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["cloudwatch:GetMetricData", "cloudwatch:ListMetrics"],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "aws:SecureTransport": "true"
                }
            }
        }
    ]
}
```

This sample policy has one statement that grants permissions to a group for two CloudWatch actions (cloudwatch:GetMetricData, and cloudwatch:ListMetrics), but only if the group uses SSL with the request ("aws:SecureTransport": "true"). For more information about the elements within an IAM policy statement, see Specifying policy elements: Actions, effects, and principals (p. 701) and IAM Policy Elements Reference in IAM User Guide.

Permissions required to use the CloudWatch console

For a user to work with the CloudWatch console, that user must have a minimum set of permissions that allow the user to describe other AWS resources in their account. The CloudWatch console requires permissions from the following services:

- Amazon EC2 Auto Scaling
- CloudTrail
- CloudWatch
- CloudWatch Events
- CloudWatch Logs
- Amazon EC2
- Amazon ES
- IAM
- Kinesis
- Lambda
- Amazon S3
- Amazon SNS
- Amazon SQS
- Amazon SWF
- X-Ray, if you are using the ServiceLens feature

If you create an IAM policy that is more restrictive than the minimum required permissions, the console won’t function as intended for users with that IAM policy. To ensure that those users can still use the CloudWatch console, also attach the CloudWatchReadOnlyAccess managed policy to the user, as described in AWS managed (predefined) policies for CloudWatch (p. 705).

You don’t need to allow minimum console permissions for users that are making calls only to the AWS CLI or the CloudWatch API.

The full set of permissions required to work with the CloudWatch console are listed below:
• application-autoscaling:DescribeScalingPolicies
• autoscaling:DescribeAutoScalingGroups
• autoscaling:DescribePolicies
• cloudtrail:DescribeTrails
• cloudwatch:DeleteAlarms
• cloudwatch:DescribeAlarmHistory
• cloudwatch:DescribeAlarms
• cloudwatch:GetMetricData
• cloudwatch:GetMetricStatistics
• cloudwatch:ListMetrics
• cloudwatch:PutMetricAlarm
• cloudwatch:PutMetricData
• ec2:DescribeInstances
• ec2:DescribeTags
• ec2:DescribeVolumes
• es:DescribeElasticsearchDomain
• es:ListDomainNames
• events:DeleteRule
• events:DescribeRule
• events:DisableRule
• events:EnableRule
• events:ListRules
• events:PutRule
• iam:AttachRolePolicy
• iam:CreateRole
• iam:GetPolicy
• iam:GetPolicyVersion
• iam:GetRole
• iam:ListAttachedRolePolicies
• iam:ListRoles
• kinesis:DescribeStream
• kinesis:ListStreams
• lambda:AddPermission
• lambda:CreateFunction
• lambda:GetFunctionConfiguration
• lambda:ListAliases
• lambda:ListFunctions
• lambda:ListVersionsByFunction
• lambda:RemovePermission
• logs:CancelExportTask
• logs:CreateExportTask
• logs:CreateLogGroup
• logs:CreateLogStream
• logs:DeleteLogGroup
• logs:DeleteLogStream
Using identity-based policies (IAM policies)

- logs:DeleteMetricFilter
- logs:DeleteRetentionPolicy
- logs:DeleteSubscriptionFilter
- logs:DescribeExportTasks
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:DescribeMetricFilters
- logs:DescribeQueries
- logs:DescribeSubscriptionFilters
- logs:FilterLogEvents
- logs:GetLogGroupFields
- logs:GetLogRecord
- logs:GetLogEvents
- logs:GetQueryResults
- logs:PutMetricFilter
- logs:PutRetentionPolicy
- logs:PutSubscriptionFilter
- logs:StartQuery
- logs:StopQuery
- logs:TestMetricFilter
- s3:CreateBucket
- s3:ListBucket
- sns:CreateTopic
- sns:GetTopicAttributes
- sns:ListSubscriptions
- sns:ListTopics
- sns:SetTopicAttributes
- sns:Subscribe
- sns:Unsubscribe
- sqs:GetQueueAttributes
- sqs:GetQueueUrl
- sqs:ListQueues
- sqs:SetQueueAttributes
- swf:CreateAction
- swf:DescribeAction
- swf:ListActionTemplates
- swf:RegisterAction
- swf:RegisterDomain
- swf:UpdateAction

Additionally, to view the service map in ServiceLens, you need AWSXrayReadOnlyAccess

AWS managed (predefined) policies for CloudWatch

AWS addresses many common use cases by providing standalone IAM policies that are created and administered by AWS. These AWS managed policies grant necessary permissions for common use cases...
so that you can avoid having to investigate what permissions are needed. For more information, see AWS managed policies in the IAM User Guide.

The following AWS managed policies, which you can attach to users in your account, are specific to CloudWatch.

**Note**
You can review these permissions policies by signing in to the IAM console and searching for specific policies there.

You can also create your own custom IAM policies to allow permissions for CloudWatch actions and resources. You can attach these custom policies to the IAM users or groups that require those permissions.

**Topics**
- CloudWatchFullAccess (p. 706)
- CloudWatchActionsEC2Access (p. 707)
- CloudWatchReadOnlyAccess (p. 707)
- CloudWatchAutomaticDashboardsAccess (p. 707)
- AWS managed (predefined) policies for CloudWatch Synthetics (p. 708)
- AWS managed policy for AWS Systems Manager Incident Manager (p. 708)

---

**CloudWatchFullAccess**

The CloudWatchFullAccess policy grants full access to all CloudWatch actions and resources. Its contents are as follows:

```json
{
"Version": "2012-10-17",
"Statement": [

{
"Effect": "Allow",
"Action": [
"autoscaling:Describe*",
"cloudwatch:*",
"logs:*",
"ssm-incidents:ListResponsePlans",
"sns:*",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRole"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": "iam:CreateServiceLinkedRole",
"Resource": "*",
"Condition": {
"StringLike": {
"iam:AWSServiceName": [
"events.amazonaws.com",
"ssm.alarms.cloudwatch.amazonaws.com",
"ssm-incidents.alarms.cloudwatch.amazonaws.com"
],
"ssm-alarms.cloudwatch.amazonaws.com"
}
}
}
}
```
CloudWatchActionsEC2Access

The **CloudWatchActionsEC2Access** policy grants read-only access to CloudWatch alarms and metrics in addition to Amazon EC2 metadata. It also grants access to the Stop, Terminate, and Reboot API actions for EC2 instances.

CloudWatchReadOnlyAccess

The **CloudWatchReadOnlyAccess** policy grants read-only access to CloudWatch.

CloudWatchAutomaticDashboardsAccess

The **CloudWatch-CrossAccountAccess** managed policy is used by the **CloudWatch-CrossAccountSharingRole** IAM role. This role and policy enable users of cross-account dashboards to view automatic dashboards in each account that is sharing dashboards.

The following is the content of **CloudWatchAutomaticDashboardsAccess**:

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Action": [
            "autoscaling:DescribeAutoScalingGroups",
            "cloudfront:GetDistribution",
            "cloudfront:ListDistributions",
            "dynamodb:DescribeTable",
            "dynamodb:ListTables",
            "ec2:DescribeInstances",
            "ec2:DescribeVolumes",
            "ecs:DescribeClusters",
            "ecs:DescribeContainerInstances",
            "ecs:ListClusters",
            "ecs:ListContainerInstances",
            "ecs:ListServices",
            "elasticache:DescribeCacheClusters",
            "elasticbeanstalk:DescribeEnvironments",
            "elasticfilesystem:DescribeFileSystems",
            "elasticloadbalancing:DescribeLoadBalancers",
            "kinesis:DescribeStream",
            "kinesis:ListStreams",
            "lambda:GetFunction",
            "lambda:ListFunctions",
            "rds:DescribeDBClusters",
            "rds:DescribeDBInstances",
            "resource-groups:ListGroupResources",
            "resource-groups:ListGroupResources",
            "route53:GetHealthCheck",
            "route53:ListHealthChecks",
            "s3:ListAllMyBuckets",
            "s3:ListBucket",
            "sns:ListTopics",
            "sqs:GetQueueAttributes",
            "sqs:GetQueueUrl",
            "sqs:ListQueues",
            "synthetics:DescribeCanariesLastRun",
            "tag:GetResources"
         ],
         "Effect": "Allow",
         "Resource": "*
      },
      {
         "Action": [
            "apigateway:GET"
```
Note
You can review these permissions policies by signing in to the IAM console and searching for specific policies there.

You can also create your own custom IAM policies to allow permissions for CloudWatch actions and resources. You can attach these custom policies to the IAM users or groups that require those permissions.

AWS managed (predefined) policies for CloudWatch Synthetics

The CloudWatchSyntheticsFullAccess and CloudWatchSyntheticsReadOnlyAccess AWS managed policies are available for you to assign to users who will manage or use CloudWatch Synthetics. The following additional policies are also relevant:

- AmazonS3ReadOnlyAccess and CloudWatchReadOnlyAccess – These are necessary to be able to read all Synthetics data in the CloudWatch console.
- AWSLambdaReadOnlyAccess – To be able to view the source code used by canaries.
- CloudWatchSyntheticsFullAccess enables you to create canaries, Additionally, to create a canary that will have a new IAM role created for it, you also need the following inline policy statement:

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["iam:CreateRole", "iam:CreatePolicy", "iam:AttachRolePolicy"],
        }
    ]
}
```

Important
Granting a user the iam:CreateRole, iam:CreatePolicy, and iam:AttachRolePolicy permissions gives that user full administrative access to your AWS account. For example, a user with these permissions can create a policy that has full permissions for all resources, and attach that policy to any role. Be very careful about who you grant these permissions to.

For information about attaching policies and granting permissions to users, see Changing Permissions for an IAM User and To embed an inline policy for a user or role.

AWS managed policy for AWS Systems Manager Incident Manager

The AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy policy is attached to a service-linked role that allows CloudWatch to start incidents in AWS Systems Manager Incident Manager on
your behalf. For more information, see Service-linked role permissions for CloudWatch alarms Systems Manager Incident Manager actions (p. 718).

The policy has the following permission:

- ssm-incidents:StartIncident

**CloudWatchSyntheticsFullAccess**

The following is the content of the CloudWatchSyntheticsFullAccess policy.

```json
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "ssm-incidents:*"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "ssm:CreateBucket",
            "ssm:PutEncryptionConfiguration"
         ],
         "Resource": [
            "arn:aws:ssm:*
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "iam:ListRoles",
            "s3:ListAllMyBuckets",
            "s3:GetBucketLocation",
            "xray:GetTraceSummaries",
            "xray:BatchGetTraces",
            "apigateway:GET"
         ],
         "Resource": "*"
      },
      {
         "Effect": "Allow",
         "Action": [
            "s3:GetObject",
            "s3:ListBucket"
         ],
         "Resource": "arn:aws:s3:*
      },
      {
         "Effect": "Allow",
         "Action": [
            "iam:PassRole"
         ],
         "Resource": [
            "arn:aws:iam:*
         ]
      }
   ]
}
```
"arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole"
],
"Condition": {
  "StringEquals": {
    "iam:PassedToService": [
      "lambda.amazonaws.com",
      "synthetics.amazonaws.com"
    ]
  }
}
},
{
  "Effect": "Allow",
  "Action": [
    "iam:GetRole"
  ],
  "Resource": [
    "arn:aws:iam::*:role/service-role/CloudWatchSyntheticsRole"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "cloudwatch:GetMetricData",
    "cloudwatch:GetMetricStatistics"
  ],
  "Resource": "*
},
{
  "Effect": "Allow",
  "Action": [
    "cloudwatch:PutMetricAlarm",
    "cloudwatch:DeleteAlarms"
  ],
  "Resource": [
    "arn:aws:cloudwatch::*:alarm:Synthetics-*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "cloudwatch:DescribeAlarms"
  ],
  "Resource": [
    "arn:aws:cloudwatch::*:alarm:*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "lambda:CreateFunction",
    "lambda:AddPermission",
    "lambda:PublishVersion",
    "lambda:UpdateFunctionCode",
    "lambda:UpdateFunctionConfiguration",
    "lambda:GetFunctionConfiguration"
  ],
  "Resource": [
    "arn:aws:lambda::*:function:cwsyn-*"
  ]
},
{
  "Effect": "Allow",
  "Action": [
    "lambda:GetLayerVersion",
    "lambda:PublishLayerVersion"
  ]
}
Using identity-based policies (IAM policies)

```
],
"Resource": [
    "arn:aws:lambda:*:*:layer:cwsyn-*",
    "arn:aws:lambda:*:*:layer:Synthetics:*"
]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "sns:ListTopics"
    ],
    "Resource": [
        "*
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "sns:CreateTopic",
        "sns:Subscribe",
        "sns:ListSubscriptionsByTopic"
    ],
    "Resource": [
        "arn:*:sns:*:Synthetics-*"
    ]
}
```

**CloudWatchSyntheticsReadOnlyAccess**

The following is the content of the **CloudWatchSyntheticsReadOnlyAccess** policy.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "synthetics:Describe*",
                "synthetics:Get*",
                "synthetics:List*"
            ],
            "Resource": "*
        }
    ]
}
```

**Customer managed policy examples**

In this section, you can find example user policies that grant permissions for various CloudWatch actions. These policies work when you are using the CloudWatch API, AWS SDKs, or the AWS CLI.
Examples

• Example 1: Allow user full access to CloudWatch (p. 712)
• Example 2: Allow read-only access to CloudWatch (p. 712)
• Example 3: Stop or terminate an Amazon EC2 instance (p. 712)

Example 1: Allow user full access to CloudWatch

To grant a user full access to CloudWatch, you can use grant them the CloudWatchFullAccess managed policy instead of creating a customer-managed policy. The contents of the CloudWatchFullAccess are listed in CloudWatchFullAccess (p. 706).

Example 2: Allow read-only access to CloudWatch

The following policy allows a user read-only access to CloudWatch and view Amazon EC2 Auto Scaling actions, CloudWatch metrics, CloudWatch Logs data, and alarm-related Amazon SNS data.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "autoscaling:Describe*",
        "cloudwatch:Describe*",
        "cloudwatch:Get*",
        "cloudwatch:List*",
        "logs:Get*",
        "logs:Describe*",
        "sns:Get*",
        "sns:List*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Example 3: Stop or terminate an Amazon EC2 instance

The following policy allows an CloudWatch alarm action to stop or terminate an EC2 instance. In the sample below, the GetMetricData, ListMetrics, and DescribeAlarms actions are optional. It is recommended that you include these actions to ensure that you have correctly stopped or terminated the instance.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "cloudwatch:PutMetricAlarm",
        "cloudwatch:GetMetricData",
        "cloudwatch:ListMetrics",
        "cloudwatch:DescribeAlarms"
      ],
      "Sid": "00000000000000",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```
CloudWatch updates to AWS managed policies

View details about updates to AWS managed policies for CloudWatch since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the CloudWatch Document history page.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudWatchSyntheticsFullAccess (p. 709)</td>
<td>– Update to an existing policy CloudWatch Synthetics added a permission to CloudWatchSyntheticsFullAccess. The lambda:UpdateFunctionCode permission was added so that users with this policy can change the runtime version of canaries.</td>
<td>July 20, 2021</td>
</tr>
<tr>
<td>AWSCloudWatchAlarms_ActionSSMIncidentsServiceRolePolicy (p. 708)</td>
<td>– New managed policy CloudWatch added a new managed IAM policy to allow CloudWatch to create incidents in AWS Systems Manager Incident Manager.</td>
<td>May 10, 2021</td>
</tr>
</tbody>
</table>
| CloudWatchFullAccess (p. 706) | – Update to an existing policy CloudWatch changed the CloudWatchFullAccess managed policy. The following changes were made:  
  - The ssm-incidents:ListResponsePlans permission was added to this policy to enable the customer to retrieve their SSM Incident response plans.  
  - The Resource allowed for the iam:CreateServiceLinkedRole permission was changed to * to enable CloudWatch to create multiple service- | May 10, 2021 |
### Using condition keys to limit access to CloudWatch namespaces

Use IAM condition keys to limit users to publishing metrics only in the CloudWatch namespaces that you specify.

#### Allowing publishing in one namespace only

The following policy limits the user to publishing metrics only in the namespace named `MyCustomNamespace`.

```json
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Allow",
        "Resource": "*",
        "Action": "cloudwatch:PutMetricData",
        "Condition": {
            "StringEquals": {
                "cloudwatch:namespace": "MyCustomNamespace"
            }
        }
    }
}
```
Using condition keys to limit Contributor Insights users' access to log groups

To create a rule in Contributor Insights and see its results, a user must have the `cloudwatch:PutInsightRule` permission. By default, a user with this permission can create a Contributor Insights rule that evaluates any log group in CloudWatch Logs and then see the results. The results can contain contributor data for those log groups.

You can create IAM policies with condition keys to grant users the permission to write Contributor Insights rules for some log groups while preventing them from writing rules for and seeing this data from other log groups.

For more information about the `Condition` element in IAM policies, see IAM JSON policy elements: `Condition`.

Allow access to write rules and view results for only certain log groups

The following policy allows the user access to write rules and view results for the log group named `AllowedLogGroup` and all log groups that have names that start with `AllowedWildcard*`. It does not grant access to write rules or view rule results for any other log groups.

```json
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowCertainLogGroups",
            "Effect": "Allow",
            "Action": "cloudwatch:PutInsightRule",
            "Resource": "arn:aws:cloudwatch:*:*:insight-rule/*",
            "Condition": {
                "ForAllValues:StringEqualsIgnoreCase": {
                    "cloudwatch:requestInsightRuleLogGroups": [
                        "AllowedLogGroup",
                        "AllowedWildcard*"
                    ]
                }
            }
        }
    ]
}
```
Deny writing rules for specific log groups but allow writing rules for all other log groups

The following policy explicitly denies the user access to write rules and view rule results for the log group named `ExplicitlyDeniedLogGroup`, but allows writing rules and viewing rule results for all other log groups.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowInsightRulesOnLogGroupsByDefault",
      "Effect": "Allow",
      "Action": "cloudwatch:PutInsightRule",
      "Resource": "arn:aws:cloudwatch:*:*:insight-rule/*"
    },
    {
      "Sid": "ExplicitDenySomeLogGroups",
      "Effect": "Deny",
      "Action": "cloudwatch:PutInsightRule",
      "Resource": "arn:aws:cloudwatch:*:*:insight-rule/*",
      "Condition": {
        "ForAllValues:StringEqualsIgnoreCase": {
          "cloudwatch:requestInsightRuleLogGroups": [ "/test/alpine/ExplicitlyDeniedLogGroup"
        ]
      }
    }
  ]
}
```

Using condition keys to limit alarm actions

When CloudWatch alarms change state, they can perform different actions such as stopping and terminating EC2 instances and performing Systems Manager actions. These actions can be initiated when the alarm changes to any state, including ALARM, OK, or INSUFFICIENT_DATA.

Use the `cloudwatch:AlarmActions` condition key to allow a user to create alarms that can only perform the actions you specify when the alarm state changes. For example, you can allow a user to create alarms that can only perform actions which are not EC2 actions.

**Allow a user to create alarms that can only send Amazon SNS notifications or perform Systems Manager actions**

The following policy limits the user to creating alarms that can only send Amazon SNS notifications and perform Systems Manager actions. The user can't create alarms that perform EC2 actions.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Create alarms that can perform only SNS and SSM actions",
      "Effect": "Allow",
      "Action": "cloudwatch:PutAlarmNotificationConfiguration",
      "Resource": "arn:aws:cloudwatch:*:*:alarm/*",
      "Condition": {
        "ForAllValues:StringEqualsIgnoreCase": {
          "cloudwatch:NotificationConfigurations": [ "/test/alpine/CreateSNSAndSSMAlarms"
        ]
      }
    }
  ]
}
```
Using service-linked roles for CloudWatch

Amazon CloudWatch uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to CloudWatch. Service-linked roles are predefined by CloudWatch and include all the permissions that the service requires to call other AWS services on your behalf.

One service-linked role in CloudWatch makes setting up CloudWatch alarms that can terminate, stop, or reboot an Amazon EC2 instance without requiring you to manually add the necessary permissions. Another service-linked role enables a monitoring account to access CloudWatch data from other accounts that you specify, to build cross-account cross-Region dashboards.

CloudWatch defines the permissions of these service-linked roles, and unless defined otherwise, only CloudWatch can assume the role. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete the roles only after first deleting their related resources. This restriction protects your CloudWatch resources because you can't inadvertently remove permissions to access the resources.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have Yes in the Service-Linked Role column. Choose a Yes with a link to view the service-linked role documentation for that service.

Service-linked role permissions for CloudWatch alarms EC2 actions

CloudWatch uses the service-linked role named AWSServiceRoleForCloudWatchEvents – CloudWatch uses this service-linked role to perform Amazon EC2 alarm actions.

The AWSServiceRoleForCloudWatchEvents service-linked role trusts the CloudWatch Events service to assume the role. CloudWatch Events invokes the terminate, stop, or reboot instance actions when called upon by the alarm.

The AWSServiceRoleForCloudWatchEvents service-linked role permissions policy allows CloudWatch Events to complete the following actions on Amazon EC2 instances:

- ec2:StopInstances
- ec2:TerminateInstances
- ec2:RecoverInstances
- ec2:DescribeInstanceRecoveryAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
The **AWSServiceRoleForCloudWatchCrossAccount** service-linked role permissions policy allows CloudWatch to complete the following actions:

- `sts:AssumeRole`

### Service-linked role permissions for CloudWatch alarms Systems Manager OpsCenter actions

CloudWatch uses the service-linked role named **AWSServiceRoleForCloudWatchAlarms_ActionSSM** – CloudWatch uses this service-linked role to perform Systems Manager OpsCenter actions when a CloudWatch alarm goes into ALARM state.

The **AWSServiceRoleForCloudWatchAlarms_ActionSSM** service-linked role trusts the CloudWatch service to assume the role. CloudWatch alarms invoke the Systems Manager OpsCenter actions when called upon by the alarm.

The **AWSServiceRoleForCloudWatchAlarms_ActionSSM** service-linked role permissions policy allows Systems Manager to complete the following actions:

- `ssm:CreateOpsItem`

### Service-linked role permissions for CloudWatch alarms Systems Manager Incident Manager actions

CloudWatch uses the service-linked role named **AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents** – CloudWatch uses this service-linked role to start Incident Manager incidents when a CloudWatch alarm goes into ALARM state.

The **AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents** service-linked role trusts the CloudWatch service to assume the role. CloudWatch alarms invoke the Systems Manager Incident Manager action when called upon by the alarm.

The **AWSServiceRoleForCloudWatchAlarms_ActionSSMIncidents** service-linked role permissions policy allows Systems Manager to complete the following actions:

- `ssm-incidents:StartIncident`

### Service-linked role permissions for CloudWatch cross-account cross-Region

CloudWatch uses the service-linked role named **AWSServiceRoleForCloudWatchCrossAccount** – CloudWatch uses this role to access CloudWatch data in other AWS accounts that you specify. The SLR only provides the assume role permission to allow the CloudWatch service to assume the role in the sharing account. It is the sharing role that provides access to data.

The **AWSServiceRoleForCloudWatchCrossAccount** service-linked role permissions policy allows CloudWatch to complete the following actions:

- `sts:AssumeRole`

The **AWSServiceRoleForCloudWatchCrossAccount** service-linked role trusts the CloudWatch service to assume the role.
Creating a service-linked role for CloudWatch

You do not need to manually create any of these service-linked roles. The first time you create an alarm in the AWS Management Console, the IAM CLI, or the IAM API, CloudWatch creates AWSServiceRoleForCloudWatchEvents and AWSServiceRoleForCloudWatchAlarms_ActionSSM for you. The first time you enable an account to be a monitoring account for cross-account cross-Region functionality, CloudWatch creates AWSServiceRoleForCloudWatchCrossAccount for you.

For more information, see Creating a Service-Linked Role in the IAM User Guide.

Editing a service-linked role for CloudWatch

CloudWatch does not allow you to edit the AWSServiceRoleForCloudWatchEvents, AWSServiceRoleForCloudWatchAlarms_ActionSSM or AWSServiceRoleForCloudWatchCrossAccount roles. After you create these roles, you cannot change their names because various entities might reference these roles. However, you can edit the description of these roles using IAM.

Editing a service-linked role description (IAM console)

You can use the IAM console to edit the description of a service-linked role.

To edit the description of a service-linked role (console)

1. In the navigation pane of the IAM console, choose Roles.
2. Choose the name of the role to modify.
3. To the far right of Role description, choose Edit.
4. Type a new description in the box, and choose Save.

Editing a service-linked role description (AWS CLI)

You can use IAM commands from the AWS Command Line Interface to edit the description of a service-linked role.

To change the description of a service-linked role (AWS CLI)

1. (Optional) To view the current description for a role, use the following commands:

```
$ aws iam get-role --role-name role-name
```

Use the role name, not the ARN, to refer to roles with the AWS CLI commands. For example, if a role has the following ARN: arn:aws:iam::123456789012:role/myrole, you refer to the role as myrole.

2. To update a service-linked role's description, use the following command:

```
$ aws iam update-role-description --role-name role-name --description description
```

Editing a service-linked role description (IAM API)

You can use the IAM API to edit the description of a service-linked role.

To change the description of a service-linked role (API)

1. (Optional) To view the current description for a role, use the following command:
GetRole
2. To update a role's description, use the following command:

UpdateRoleDescription

Deleting a service-linked role for CloudWatch

If you no longer have alarms that automatically stop, terminate, or reboot EC2 instances, we recommend that you delete the AWSServiceRoleForCloudWatchEvents role.

If you no longer have alarms that perform Systems Manager OpsCenter actions, we recommend that you delete the AWSServiceRoleForCloudWatchAlarms_ActionSSM role.

That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up your service-linked role before you can delete it.

Cleaning up a service-linked role

Before you can use IAM to delete a service-linked role, you must first confirm that the role has no active sessions and remove any resources used by the role.

To check whether the service-linked role has an active session in the IAM console
1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Roles. Choose the name (not the check box) of the AWSServiceRoleForCloudWatchEvents role.
3. On the Summary page for the selected role, choose Access Advisor and review the recent activity for the service-linked role.

   **Note**
   If you are unsure whether CloudWatch is using the AWSServiceRoleForCloudWatchEvents role, try to delete the role. If the service is using the role, then the deletion fails and you can view the Regions where the role is being used. If the role is being used, then you must wait for the session to end before you can delete the role. You cannot revoke the session for a service-linked role.

Deleting a service-linked role (IAM console)

You can use the IAM console to delete a service-linked role.

To delete a service-linked role (console)
1. Open the IAM console at https://console.aws.amazon.com/iam/.
2. In the navigation pane, choose Roles. Select the check box next to the name of the role you want to delete, not the name or row itself.
3. For Role actions, choose Delete role.
4. In the confirmation dialog box, review the service last accessed data, which shows when each of the selected roles last accessed an AWS service. This helps you to confirm whether the role is currently active. To proceed, choose Yes, Delete.
5. Watch the IAM console notifications to monitor the progress of the service-linked role deletion. Because the IAM service-linked role deletion is asynchronous, the deletion task can succeed or fail after you submit the role for deletion. If the task fails, choose View details or View Resources from the notifications to learn why the deletion failed. If the deletion fails because there are resources in the service that are being used by the role, then the reason for the failure includes a list of resources.
Deleting a service-linked role (AWS CLI)

You can use IAM commands from the AWS Command Line Interface to delete a service-linked role.

To delete a service-linked role (AWS CLI)

1. Because a service-linked role cannot be deleted if it is being used or has associated resources, you must submit a deletion request. That request can be denied if these conditions are not met. You must capture the deletion-task-id from the response to check the status of the deletion task. Type the following command to submit a service-linked role deletion request:

   ```bash
   $ aws iam delete-service-linked-role --role-name service-linked-role-name
   ```

2. Type the following command to check the status of the deletion task:

   ```bash
   $ aws iam get-service-linked-role-deletion-status --deletion-task-id deletion-task-id
   ```

   The status of the deletion task can be NOT_STARTED, IN_PROGRESS, SUCCEEDED, or FAILED. If the deletion fails, the call returns the reason that it failed so that you can troubleshoot.

Deleting a service-linked role (IAM API)

You can use the IAM API to delete a service-linked role.

To delete a service-linked role (API)

1. To submit a deletion request for a service-linked role, call DeleteServiceLinkedRole. In the request, specify the role name that you want to delete.

   ```json
   {
   "DeleteServiceLinkedRoleRequest": {
   "RoleName": "service-linked-role-name"
   }
   }
   ```

   Because a service-linked role cannot be deleted if it is being used or has associated resources, you must submit a deletion request. That request can be denied if these conditions are not met. You must capture the DeletionTaskId from the response to check the status of the deletion task.

2. To check the status of the deletion, call GetServiceLinkedRoleDeletionStatus. In the request, specify the DeletionTaskId.

   ```json
   {
   "GetServiceLinkedRoleDeletionStatusRequest": {
   "DeletionTaskId": "deletion-task-id"
   }
   }
   ```

   The status of the deletion task can be NOT_STARTED, IN_PROGRESS, SUCCEEDED, or FAILED. If the deletion fails, the call returns the reason that it failed so that you can troubleshoot.

CloudWatch updates to AWS service-linked roles

View details about updates to AWS managed policies for CloudWatch since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the CloudWatch Document history page.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWSServiceRoleForCloudWatchAlarms</td>
<td>CloudWatch added a new service-linked role to allow CloudWatch to create incidents in AWS Systems Manager Incident Manager.</td>
<td>April 26, 2021</td>
</tr>
</tbody>
</table>
Using service-linked roles for CloudWatch Application Insights

CloudWatch Application Insights uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to CloudWatch Application Insights. Service-linked roles are predefined by CloudWatch Application Insights and include all of the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up CloudWatch Application Insights easier because you don’t have to manually add the necessary permissions. CloudWatch Application Insights defines the permissions of its service-linked roles, and unless defined otherwise, only CloudWatch Application Insights can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

For information about other services that support service-linked roles, see AWS Services That Work with IAM and look for the services that have Yes in the Service-Linked Role column. Choose a Yes link to view the service-linked role documentation for that service.

Service-linked role permissions for CloudWatch Application Insights

CloudWatch Application Insights uses the service-linked role named AWSServiceRoleForApplicationInsights. Application Insights uses this role to perform operations such as analyzing the resource groups of the customer, creating CloudFormation stacks to create alarms on metrics, and configuring the CloudWatch Agent on EC2 instances. This service-linked role is attached to the following managed policy: CloudwatchApplicationInsightsServiceLinkedRolePolicy. For updates to this policy, see Application Insights updates to AWS managed policies (p. 727).

The role permissions policy allows CloudWatch Application Insights to complete the following actions on all resources:

- cloudwatch:DescribeAlarmHistory
- cloudwatch:DescribeAlarms
- cloudwatch:GetMetricData
- cloudwatch:ListMetrics
- cloudwatch:PutMetricAlarm
- cloudwatch:DeleteAlarms
- cloudwatch:PutAnomalyDetector
- cloudwatch:DeleteAnomalyDetector
- cloudwatch:DescribeAnomalyDetectors
- logs:FilterLogEvents
- logs:GetLogEvents
- logs:DescribeLogStreams
- logs:DescribeLogGroups
- events:DescribeRule
Amazon CloudWatch User Guide
Using service-linked roles for Application Insights

- cloudFormation:DescribeStacks
- cloudFormation:ListStackResources
- tag:GetResources
- resource-groups:ListGroupResources
- resource-groups:GetGroupQuery
- resource-groups:GetGroup
- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeTargetGroups
- elasticloadbalancing:DescribeTargetHealth
- autoscaling:DescribeAutoScalingGroups
- ssm:GetOpsItem
- ssm:CreateOpsItem
- ssm:DescribeOpsItems
- ssm:UpdateOpsItem
- ssm:DescribeInstanceInformation
- ssm:ListCommandInvocations
- ec2:DescribeInstances
- ec2:DescribeVolumes
- ec2:DescribeVolumeStatus
- rds:DescribeDBInstances
- rds:DescribeDBClusters
- lambda:GetFunctionConfiguration
- lambda:ListEventSourceMappings
- xray:GetServiceGraph
- xray:GetTraceSummaries
- xray:GetTimeSeriesServiceStatistics
- xray:GetTraceGraph
- dynamodb:DescribeTable
- dynamodb:DescribeContributorInsights
- dynamodb:DescribeTimeToLive
- application-autoscaling:DescribeScalableTargets
- s3:GetMetricsConfiguration
- s3:GetReplicationConfiguration
- states:DescribeExecution
- states:DescribeStateMachine
- states:GetExecutionHistory
- ecs:DescribeClusters
- ecs:DescribeContainerInstances
- ecs:DescribeServices
- ecs:DescribeTaskDefinition
- ecs:DescribeTasks
- ecs:DescribeTaskSets
- ecs:ListClusters
- ecs:ListContainerInstances
- ecs:ListServices
Using service-linked roles for Application Insights

Amazon CloudWatch User Guide

- `ecs:ListTasks`
- `eks:DescribeCluster`
- `eks:DescribeFargateProfile`
- `eks:DescribeNodegroup`
- `eks:ListClusters`
- `eks:ListFargateProfiles`
- `eks:ListNodegroups`

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see Service-Linked Role Permissions in the IAM User Guide.

Creating a service-linked role for CloudWatch Application Insights

You don't need to manually create a service-linked role. When you create a new Application Insights application in the AWS Management Console, CloudWatch Application Insights creates the service-linked role for you.

If you delete this service-linked role, and then want to create it again, you can use the same process to recreate the role in your account. When you create a new Application Insights application, CloudWatch Application Insights creates the service-linked role for you again.

Editing a service-linked role for CloudWatch Application Insights

CloudWatch Application Insights does not allow you to edit the AWSServiceRoleForApplicationInsights service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a Service-Linked Role in the IAM User Guide.

Deleting a service-linked role for CloudWatch Application Insights

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you avoid having an unused entity that is not actively monitored or maintained. However, you must delete all applications in Application Insights before you can manually delete the role.

**Note**

If the CloudWatch Application Insights service is using the role when you try to delete the resources, the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To delete CloudWatch Application Insights resources used by the AWSServiceRoleForApplicationInsights

- Delete all of your CloudWatch Application Insights applications. For more information, see "Deleting Your Application(s)" in the CloudWatch Application Insights User Guide.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the AWSServiceRoleForApplicationInsights service-linked role. For more information, see Deleting a Service-Linked Role in the IAM User Guide.
Supported Regions for CloudWatch Application Insights service-linked roles

CloudWatch Application Insights supports using service-linked roles in all of the AWS Regions where the service is available. For more information, see CloudWatch Application Insights Regions and Endpoints.

AWS managed policies for Amazon CloudWatch Application Insights

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the IAM User Guide.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the ReadOnlyAccess AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the IAM User Guide.

AWS managed policy: CloudWatchApplicationInsightsFullAccess

You can attach the CloudWatchApplicationInsightsFullAccess policy to your IAM identities.

This policy grants administrative permissions that allow full access to Application Insights functionality.

Permissions details

This policy includes the following permissions.

- applicationinsights – Allows full access to Application Insights functionality.
- iam – Allows Application Insights to create the service-linked role, AWSServiceRoleForApplicationInsights. This is required so that Application Insights can perform operations such as analyze the resource groups of a customer, create CloudFormation stacks to create alarms on metrics, and configure the CloudWatch Agent on EC2 instances. For more information, see Using service-linked roles for CloudWatch Application Insights (p. 722).
AWS managed policy:
CloudWatchApplicationInsightsReadOnlyAccess

You can attach the CloudWatchApplicationInsightsReadOnlyAccess policy to your IAM identities.

This policy grants administrative permissions that allow read-only access to all Application Insights functionality.

Permissions details
This policy includes the following permissions.

• applicationinsights – Allows read-only access to Application Insights functionality.
AWS managed policy: 
CloudwatchApplicationInsightsServiceLinkedRolePolicy

You can't attach CloudwatchApplicationInsightsServiceLinkedRolePolicy to your IAM entities. This policy is attached to a service-linked role that allows Application Insights to monitor customer resources. For more information, see Using service-linked roles for CloudWatch Application Insights (p. 722).

Application Insights updates to AWS managed policies

View details about updates to AWS managed policies for Application Insights since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Application Insights Document history (p. 754) page.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudwatchApplicationInsightsServiceLinkedRolePolicy</td>
<td>Application Insights added new permissions to describe and list ECS and EKS service resources. This permission is required for Amazon CloudWatch Application Insights to read customer container resources configuration, and to help customers automatically set up best practice container monitoring with CloudWatch.</td>
<td>May 18, 2021</td>
</tr>
<tr>
<td>CloudwatchApplicationInsightsServiceLinkedRolePolicy</td>
<td>Application Insights added new permissions to allow OpsCenter to tag OpsItems using the ssm:AddTagsToResource action on resources with the opsitem resource type. This permission is required by OpsCenter. Amazon CloudWatch Application Insights creates OpsItems so that the customer can resolve problems using AWS SSM OpsCenter.</td>
<td>April 13, 2021</td>
</tr>
<tr>
<td>Application Insights started tracking changes</td>
<td>Application Insights started tracking changes for its AWS managed policies.</td>
<td>April 13, 2021</td>
</tr>
</tbody>
</table>

Amazon CloudWatch permissions reference

When you are setting up Access control (p. 698) and writing permissions policies that you can attach to an IAM identity (identity-based policies), you can use the following table as a reference. The table
lists each CloudWatch API operation and the corresponding actions for which you can grant permissions to perform the action. You specify the actions in the policy's Action field, and you specify a wildcard character (*) as the resource value in the policy's Resource field.

You can use AWS-wide condition keys in your CloudWatch policies to express conditions. For a complete list of AWS-wide keys, see AWS Global and IAM Condition Context Keys in the IAM User Guide.

Note
To specify an action, use the cloudwatch: prefix followed by the API operation name. For example: cloudwatch:GetMetricData, cloudwatch:ListMetrics, or cloudwatch:* (for all CloudWatch actions).

Topics
- CloudWatch API operations and required permissions for actions (p. 728)
- CloudWatch Contributor Insights API operations and required permissions for actions (p. 730)
- CloudWatch Events API operations and required permissions for actions (p. 731)
- CloudWatch Logs API operations and required permissions for actions (p. 732)
- Amazon EC2 API operations and required permissions for actions (p. 735)
- Amazon EC2 Auto Scaling API operations and required permissions for actions (p. 736)

CloudWatch API operations and required permissions for actions

<table>
<thead>
<tr>
<th>CloudWatch API operations</th>
<th>Required permissions (API actions)</th>
</tr>
</thead>
</table>
| DeleteAlarms                   | cloudwatch:DeleteAlarms  
Required to delete an alarm. |
| DeleteDashboards               | cloudwatch:DeleteDashboards  
Required to delete a dashboard. |
| DeleteMetricStream             | cloudwatch:DeleteMetricStream  
Required to delete a metric stream. |
| DescribeAlarmHistory           | cloudwatch:DescribeAlarmHistory  
Required to view alarm history. |
| DescribeAlarms                 | cloudwatch:DescribeAlarms  
Required to retrieve information about alarms.  
To retrieve information about composite alarms, your cloudwatch:DescribeAlarms permission must have a * scope. You can't return information about composite alarms if your cloudwatch:DescribeAlarms permission has a narrower scope. |
| DescribeAlarmsForMetric        | cloudwatch:DescribeAlarmsForMetric  
Required to view alarms for a metric. |
| DisableAlarmActions            | cloudwatch:DisableAlarmActions |

728
<table>
<thead>
<tr>
<th>CloudWatch API operations</th>
<th>Required permissions (API actions)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Required to disable an alarm action.</td>
</tr>
<tr>
<td>EnableAlarmActions</td>
<td>cloudwatch:EnableAlarmActions</td>
</tr>
<tr>
<td></td>
<td>Required to enable an alarm action.</td>
</tr>
<tr>
<td>GetDashboard</td>
<td>cloudwatch:GetDashboard</td>
</tr>
<tr>
<td></td>
<td>Required to display data about existing dashboards.</td>
</tr>
<tr>
<td>GetMetricData</td>
<td>cloudwatch:GetMetricData</td>
</tr>
<tr>
<td></td>
<td>Required to graph metric data in the CloudWatch console, to retrieve large batches of metric data,</td>
</tr>
<tr>
<td></td>
<td>and perform metric math on that data.</td>
</tr>
<tr>
<td>GetMetricStatistics</td>
<td>cloudwatch:GetMetricStatistics</td>
</tr>
<tr>
<td></td>
<td>Required to view graphs in other parts of the CloudWatch console and in dashboard widgets.</td>
</tr>
<tr>
<td>GetMetricStream</td>
<td>cloudwatch:GetMetricStream</td>
</tr>
<tr>
<td></td>
<td>Required to view information about a metric stream.</td>
</tr>
<tr>
<td>GetMetricWidgetImage</td>
<td>cloudwatch:GetMetricWidgetImage</td>
</tr>
<tr>
<td></td>
<td>Required to retrieve a snapshot graph of one or more CloudWatch metrics as a bitmap image.</td>
</tr>
<tr>
<td>ListDashboards</td>
<td>cloudwatch:ListDashboards</td>
</tr>
<tr>
<td></td>
<td>Required to view the list of CloudWatch dashboards in your account.</td>
</tr>
<tr>
<td>ListMetrics</td>
<td>cloudwatch:ListMetrics</td>
</tr>
<tr>
<td></td>
<td>Required to view or search metric names within the CloudWatch console and in the CLI. Required to</td>
</tr>
<tr>
<td></td>
<td>select metrics on dashboard widgets.</td>
</tr>
<tr>
<td>ListMetricStreams</td>
<td>cloudwatch:ListMetricStreams</td>
</tr>
<tr>
<td></td>
<td>Required to view or search the list of metric streams in the account.</td>
</tr>
<tr>
<td>PutDashboard</td>
<td>cloudwatch:PutDashboard</td>
</tr>
<tr>
<td></td>
<td>Required to create a dashboard or update an existing dashboard.</td>
</tr>
<tr>
<td>PutMetricAlarm</td>
<td>cloudwatch:PutMetricAlarm</td>
</tr>
<tr>
<td></td>
<td>Required to create or update an alarm.</td>
</tr>
<tr>
<td>CloudWatch API operations</td>
<td>Required permissions (API actions)</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PutMetricData</td>
<td>cloudwatch:PutMetricData</td>
</tr>
<tr>
<td></td>
<td>Required to create metrics.</td>
</tr>
<tr>
<td>PutMetricStream</td>
<td>cloudwatch:PutMetricStream</td>
</tr>
<tr>
<td></td>
<td>Required to create a metric stream.</td>
</tr>
<tr>
<td>SetAlarmState</td>
<td>cloudwatch:SetAlarmState</td>
</tr>
<tr>
<td></td>
<td>Required to manually set an alarm's state.</td>
</tr>
<tr>
<td>StartMetricStreams</td>
<td>cloudwatch:StartMetricStreams</td>
</tr>
<tr>
<td></td>
<td>Required to start the flow of metrics in a metric stream.</td>
</tr>
<tr>
<td>StopMetricStreams</td>
<td>cloudwatch:StopMetricStreams</td>
</tr>
<tr>
<td></td>
<td>Required to temporarily stop the flow of metrics in a metric stream.</td>
</tr>
<tr>
<td>TagResource</td>
<td>cloudwatch:TagResource</td>
</tr>
<tr>
<td></td>
<td>Required to add or update tags on CloudWatch resources such as alarms and Contributor Insights rules.</td>
</tr>
<tr>
<td>UntagResource</td>
<td>cloudwatch:UntagResource</td>
</tr>
<tr>
<td></td>
<td>Required to remove tags from CloudWatch resources.</td>
</tr>
</tbody>
</table>

### CloudWatch Contributor Insights API operations and required permissions for actions

**Important**

When you grant a user the `cloudwatch:PutInsightRule` permission, by default that user can create a rule that evaluates any log group in CloudWatch Logs. You can add IAM policy conditions that limit these permissions for a user to include and exclude specific log groups. For more information, see Using condition keys to limit Contributor Insights users' access to log groups (p. 715).

<table>
<thead>
<tr>
<th>CloudWatch Contributor Insights API operations</th>
<th>Required permissions (API actions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeleteInsightRules</td>
<td>cloudwatch:DeleteInsightRules</td>
</tr>
<tr>
<td></td>
<td>Required to delete Contributor Insights rules.</td>
</tr>
<tr>
<td>DescribeInsightRules</td>
<td>cloudwatch:DescribeInsightRules</td>
</tr>
<tr>
<td></td>
<td>Required to view the Contributor Insights rules in your account.</td>
</tr>
<tr>
<td>EnableInsightRules</td>
<td>cloudwatch:EnableInsightRules</td>
</tr>
</tbody>
</table>
### CloudWatch Contributor Insights API operations and required permissions

<table>
<thead>
<tr>
<th>CloudWatch Contributor Insights API operations</th>
<th>Required permissions (API actions)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Required to retrieve time series data and other statistics collected by Contributor Insights rules.</td>
</tr>
<tr>
<td>PutInsightRule</td>
<td>cloudwatch:PutInsightRule</td>
</tr>
<tr>
<td></td>
<td>Required to create Contributor Insights rules. See the Important note at the beginning of this table.</td>
</tr>
</tbody>
</table>

### CloudWatch Events API operations and required permissions for actions

<table>
<thead>
<tr>
<th>CloudWatch Events API operations</th>
<th>Required permissions (API actions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeleteRule</td>
<td>events:DeleteRule</td>
</tr>
<tr>
<td></td>
<td>Required to delete a rule.</td>
</tr>
<tr>
<td>DescribeRule</td>
<td>events:DescribeRule</td>
</tr>
<tr>
<td></td>
<td>Required to list the details about a rule.</td>
</tr>
<tr>
<td>DisableRule</td>
<td>events:DisableRule</td>
</tr>
<tr>
<td></td>
<td>Required to disable a rule.</td>
</tr>
<tr>
<td>EnableRule</td>
<td>events:EnableRule</td>
</tr>
<tr>
<td></td>
<td>Required to enable a rule.</td>
</tr>
<tr>
<td>ListRuleNamesByTarget</td>
<td>events:ListRuleNamesByTarget</td>
</tr>
<tr>
<td></td>
<td>Required to list rules associated with a target.</td>
</tr>
<tr>
<td>ListRules</td>
<td>events:ListRules</td>
</tr>
<tr>
<td></td>
<td>Required to list all rules in your account.</td>
</tr>
<tr>
<td>ListTargetsByRule</td>
<td>events:ListTargetsByRule</td>
</tr>
<tr>
<td></td>
<td>Required to list all targets associated with a rule.</td>
</tr>
<tr>
<td>PutEvents</td>
<td>events:PutEvents</td>
</tr>
<tr>
<td></td>
<td>Required to add custom events that can be matched to rules.</td>
</tr>
<tr>
<td>PutRule</td>
<td>events:PutRule</td>
</tr>
<tr>
<td></td>
<td>Required to create or update a rule.</td>
</tr>
<tr>
<td>PutTargets</td>
<td>events:PutTargets</td>
</tr>
<tr>
<td></td>
<td>Required to add targets to a rule.</td>
</tr>
</tbody>
</table>
### CloudWatch Events API operations and required permissions (API actions)

<table>
<thead>
<tr>
<th>CloudWatch Events API operations</th>
<th>Required permissions (API actions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>RemoveTargets</td>
<td>events:RemoveTargets</td>
</tr>
<tr>
<td></td>
<td>Required to remove a target from a rule.</td>
</tr>
<tr>
<td>TestEventPattern</td>
<td>events:TestEventPattern</td>
</tr>
<tr>
<td></td>
<td>Required to test an event pattern against a given event.</td>
</tr>
</tbody>
</table>

### CloudWatch Logs API operations and required permissions for actions

<table>
<thead>
<tr>
<th>CloudWatch Logs API operations</th>
<th>Required permissions (API actions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CancelExportTask</td>
<td>logs:CancelExportTask</td>
</tr>
<tr>
<td></td>
<td>Required to cancel a pending or running export task.</td>
</tr>
<tr>
<td>CreateExportTask</td>
<td>logs:CreateExportTask</td>
</tr>
<tr>
<td></td>
<td>Required to export data from a log group to an Amazon S3 bucket.</td>
</tr>
<tr>
<td>CreateLogGroup</td>
<td>logs:CreateLogGroup</td>
</tr>
<tr>
<td></td>
<td>Required to create a new log group.</td>
</tr>
<tr>
<td>CreateLogStream</td>
<td>logs:CreateLogStream</td>
</tr>
<tr>
<td></td>
<td>Required to create a new log stream in a log group.</td>
</tr>
<tr>
<td>DeleteDestination</td>
<td>logs:DeleteDestination</td>
</tr>
<tr>
<td></td>
<td>Required to delete a log destination and disables any subscription filters to it.</td>
</tr>
<tr>
<td>DeleteLogGroup</td>
<td>logs:DeleteLogGroup</td>
</tr>
<tr>
<td></td>
<td>Required to delete a log group and any associated archived log events.</td>
</tr>
<tr>
<td>DeleteLogStream</td>
<td>logs:DeleteLogStream</td>
</tr>
<tr>
<td></td>
<td>Required to delete a log stream and any associated archived log events.</td>
</tr>
<tr>
<td>DeleteMetricFilter</td>
<td>logs:DeleteMetricFilter</td>
</tr>
<tr>
<td></td>
<td>Required to delete a metric filter associated with a log group.</td>
</tr>
<tr>
<td>DeleteQueryDefinition</td>
<td>logs:DeleteQueryDefinition</td>
</tr>
<tr>
<td>CloudWatch Logs API operations</td>
<td>Required permissions (API actions)</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DeleteResourcePolicy</td>
<td><em>required to delete a saved query definition in CloudWatch Logs Insights.</em></td>
</tr>
<tr>
<td>DeleteRetentionPolicy</td>
<td><em>logs:DeleteRetentionPolicy</em></td>
</tr>
<tr>
<td>DeleteSubscriptionFilter</td>
<td><em>required to delete a CloudWatch Logs resource policy.</em></td>
</tr>
<tr>
<td>DescribeDestinations</td>
<td><em>logs:DescribeDestinations</em></td>
</tr>
<tr>
<td>DescribeExportTasks</td>
<td><em>required to view all destinations associated with the account.</em></td>
</tr>
<tr>
<td>DescribeLogGroups</td>
<td><em>logs:DescribeLogGroups</em></td>
</tr>
<tr>
<td>DescribeLogStreams</td>
<td><em>required to view all log groups associated with the account.</em></td>
</tr>
<tr>
<td>DescribeMetricFilters</td>
<td><em>logs:DescribeMetricFilters</em></td>
</tr>
<tr>
<td>DescribeQueryDefinitions</td>
<td><em>required to see the list of saved query definitions in CloudWatch Logs Insights.</em></td>
</tr>
<tr>
<td>DescribeQueries</td>
<td><em>logs:DescribeQueries</em></td>
</tr>
<tr>
<td>DescribeResourcePolicies</td>
<td><em>required to view a list of CloudWatch Logs resource policies.</em></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>CloudWatch Logs API operations</th>
<th>Required permissions (API actions)</th>
</tr>
</thead>
</table>
| DescribeSubscriptionFilters         | logs:DescribeSubscriptionFilters
Required to view all subscription filters associated with a log group. |
| FilterLogEvents                     | logs:FilterLogEvents
Required to sort log events by log group filter pattern.                                           |
| GetLogEvents                        | logs:GetLogEvents
Required to retrieve log events from a log stream.                                                  |
| GetLogGroupFields                   | logs:GetLogGroupFields
Required to retrieve the list of fields that are included in the log events in a log group.       |
| GetLogRecord                        | logs:GetLogRecord
Required to retrieve the details from a single log event.                                            |
| GetQueryResults                     | logs:GetQueryResults
Required to retrieve the results of CloudWatch Logs Insights queries.                               |
| ListTagsLogGroup                    | logs:ListTagsLogGroup
Required to list the tags associated with a log group.                                                |
| PutDestination                      | logs:PutDestination
Required to create or update a destination log stream (such as a Kinesis stream).                   |
| PutDestinationPolicy                | logs:PutDestinationPolicy
Required to create or update an access policy associated with an existing log destination.          |
| PutLogEvents                        | logs:PutLogEvents
Required to upload a batch of log events to a log stream.                                             |
| PutMetricFilter                     | logs:PutMetricFilter
Required to create or update a metric filter and associate it with a log group.                     |
| PutQueryDefinition                  | logs:PutQueryDefinition
Required to save a query in CloudWatch Logs Insights.                                                |
### CloudWatch Logs API operations

<table>
<thead>
<tr>
<th>CloudWatch Logs API operations</th>
<th>Required permissions (API actions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PutResourcePolicy</td>
<td>logs:PutResourcePolicy&lt;br&gt;Required to create a CloudWatch Logs resource policy.</td>
</tr>
<tr>
<td>PutRetentionPolicy</td>
<td>logs:PutRetentionPolicy&lt;br&gt;Required to set the number of days to keep log events (retention) in a log group.</td>
</tr>
<tr>
<td>PutSubscriptionFilter</td>
<td>logs:PutSubscriptionFilter&lt;br&gt;Required to create or update a subscription filter and associate it with a log group.</td>
</tr>
<tr>
<td>StartQuery</td>
<td>logs:StartQuery&lt;br&gt;Required to start CloudWatch Logs Insights queries.</td>
</tr>
<tr>
<td>StopQuery</td>
<td>logs:StopQuery&lt;br&gt;Required to stop a CloudWatch Logs Insights query that is in progress.</td>
</tr>
<tr>
<td>TagLogGroup</td>
<td>logs:TagLogGroup&lt;br&gt;Required to add or update log group tags.</td>
</tr>
<tr>
<td>TestMetricFilter</td>
<td>logs:TestMetricFilter&lt;br&gt;Required to test a filter pattern against a sampling of log event messages.</td>
</tr>
</tbody>
</table>

### Amazon EC2 API operations and required permissions for actions

<table>
<thead>
<tr>
<th>Amazon EC2 API operations</th>
<th>Required permissions (API actions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>DescribeInstanceStatus</td>
<td>ec2:DescribeInstanceStatus&lt;br&gt;Required to view EC2 instance status details.</td>
</tr>
<tr>
<td>DescribeInstances</td>
<td>ec2:DescribeInstances&lt;br&gt;Required to view EC2 instance details.</td>
</tr>
<tr>
<td>RebootInstances</td>
<td>ec2:RebootInstances&lt;br&gt;Required to reboot an EC2 instance.</td>
</tr>
<tr>
<td>StopInstances</td>
<td>ec2:StopInstances&lt;br&gt;Required to stop an EC2 instance.</td>
</tr>
<tr>
<td>TerminateInstances</td>
<td>ec2:TerminateInstances</td>
</tr>
</tbody>
</table>
Amazon EC2 Auto Scaling API operations and required permissions for actions

<table>
<thead>
<tr>
<th>Amazon EC2 Auto Scaling API operations</th>
<th>Required permissions (API actions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scaling</td>
<td>autoscaling:Scaling</td>
</tr>
<tr>
<td></td>
<td>Required to scale an Auto Scaling group.</td>
</tr>
<tr>
<td>Trigger</td>
<td>autoscaling:Trigger</td>
</tr>
<tr>
<td></td>
<td>Required to trigger an Auto Scaling action.</td>
</tr>
</tbody>
</table>

Compliance validation for Amazon CloudWatch

Third-party auditors assess the security and compliance of Amazon CloudWatch as part of multiple AWS compliance programs. These include SOC, PCI, FedRAMP, HIPAA, and others.

For a list of AWS services in scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using Amazon CloudWatch is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- **Security and Compliance Quick Start Guides** – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- **Architecting for HIPAA Security and Compliance Whitepaper** – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- **AWS Compliance Resources** – This collection of workbooks and guides might apply to your industry and location.
- **Evaluating Resources with Rules** in the AWS Config Developer Guide – AWS Config; assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- **AWS Security Hub** – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Resilience in Amazon CloudWatch

The AWS global infrastructure is built around AWS Regions and Availability Zones. Regions provide multiple physically separated and isolated Availability Zones, which are connected through low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate
Applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

Infrastructure security in Amazon CloudWatch

As a managed service, Amazon CloudWatch is protected by the AWS global network security procedures that are described in the Amazon Web Services: Overview of Security Processes whitepaper.

You use AWS published API calls to access Amazon CloudWatch through the network. Clients must support Transport Layer Security (TLS) 1.0 or later. We recommend TLS 1.2 or later. Clients must also support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

Network isolation

A virtual private cloud (VPC) is a virtual network in your own logically isolated area in the Amazon Web Services Cloud. A subnet is a range of IP addresses in a VPC. You can deploy a variety of AWS resources in the subnets of your VPCs. For example, you can deploy Amazon EC2 instances, EMR clusters, and DynamoDB tables in subnets. For more information, see the Amazon VPC User Guide.

To enable CloudWatch to communicate with resources in a VPC without going through the public internet, use AWS PrivateLink. For more information, see Using CloudWatch and CloudWatch Synthetics with interface VPC endpoints (p. 737).

A private subnet is a subnet with no default route to the public internet. Deploying an AWS resource in a private subnet does not prevent Amazon CloudWatch from collecting built-in metrics from the resource.

If you need to publish custom metrics from an AWS resource in a private subnet, you can do so using a proxy server. The proxy server forwards those HTTPS requests to the public API endpoints for CloudWatch.

Using CloudWatch and CloudWatch Synthetics with interface VPC endpoints

If you use Amazon Virtual Private Cloud (Amazon VPC) to host your AWS resources, you can establish a private connection between your VPC, CloudWatch, and CloudWatch Synthetics. You can use these connections to enable CloudWatch and CloudWatch Synthetics to communicate with your resources on your VPC without going through the public internet.

Amazon VPC is an AWS service that you can use to launch AWS resources in a virtual network that you define. With a VPC, you have control over your network settings, such the IP address range, subnets, route tables, and network gateways. To connect your VPC to CloudWatch or CloudWatch Synthetics, you define an interface VPC endpoint to connect your VPC to AWS services. The endpoint provides reliable, scalable connectivity to CloudWatch or CloudWatch Synthetics without requiring an internet gateway.
network address translation (NAT) instance, or VPN connection. For more information, see What Is Amazon VPC in the Amazon VPC User Guide.

Interface VPC endpoints are powered by AWS PrivateLink, an AWS technology that enables private communication between AWS services using an elastic network interface with private IP addresses. For more information, see the New – AWS PrivateLink for AWS Services blog post.

The following steps are for users of Amazon VPC. For more information, see Getting Started in the Amazon VPC User Guide.

CloudWatch VPC endpoint

CloudWatch currently supports VPC endpoints in the following AWS Regions:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Hong Kong)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- South America (São Paulo)
- AWS GovCloud (US-East)
- AWS GovCloud (US-West)

Creating a VPC endpoint for CloudWatch

To start using CloudWatch with your VPC, create an interface VPC endpoint for CloudWatch. The service name to choose is com.amazonaws.region.monitoring. For more information, see Creating an Interface Endpoint in the Amazon VPC User Guide.

You do not need to change the settings for CloudWatch. CloudWatch calls other AWS services using either public endpoints or private interface VPC endpoints, whichever are in use. For example, if you create an interface VPC endpoint for CloudWatch, and you already have metrics flowing to CloudWatch from resources located on your VPC, these metrics begin flowing through the interface VPC endpoint by default.

Controlling access to your CloudWatch VPC endpoint

A VPC endpoint policy is an IAM resource policy that you attach to an endpoint when you create or modify the endpoint. If you don't attach a policy when you create an endpoint, Amazon VPC attaches a default policy for you that allows full access to the service. An endpoint policy doesn't override or
replace IAM user policies or service-specific policies. It's a separate policy for controlling access from the endpoint to the specified service.

Endpoint policies must be written in JSON format.

For more information, see Controlling Access to Services with VPC Endpoints in the Amazon VPC User Guide.

The following is an example of an endpoint policy for CloudWatch. This policy allows users connecting to CloudWatch through the VPC to send metric data to CloudWatch and prevents them from performing other CloudWatch actions.

```json
{
    "Statement": [
        {
            "Sid": "PutOnly",
            "Principal": "*",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

To edit the VPC endpoint policy for CloudWatch

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Endpoints.
3. If you have not already created the endpoint for CloudWatch, choose Create Endpoint. Select com.amazonaws.region.monitoring, and then choose Create endpoint.
4. Select the com.amazonaws.region.monitoring endpoint, and then choose the Policy tab.
5. Choose Edit Policy, and then make your changes.

CloudWatch Synthetics VPC endpoint

CloudWatch Synthetics currently supports VPC endpoints in the following AWS Regions:

- US East (Ohio)
- US East (N. Virginia)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Hong Kong)
- Asia Pacific (Mumbai)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
Creating a VPC endpoint for CloudWatch Synthetics

To start using CloudWatch Synthetics with your VPC, create an interface VPC endpoint for CloudWatch Synthetics. The service name to choose is `com.amazonaws.region.synthetics`. For more information, see Creating an Interface Endpoint in the Amazon VPC User Guide.

You do not need to change the settings for CloudWatch Synthetics. CloudWatch Synthetics communicates with other AWS services using either public endpoints or private interface VPC endpoints, whichever are in use. For example, if you create an interface VPC endpoint for CloudWatch Synthetics, and you already have an interface endpoint for Amazon S3, CloudWatch Synthetics begins communicating with Amazon S3 through the interface VPC endpoint by default.

Controlling access to your CloudWatch Synthetics VPC endpoint

A VPC endpoint policy is an IAM resource policy that you attach to an endpoint when you create or modify the endpoint. If you don't attach a policy when you create an endpoint, we attach a default policy for you that allows full access to the service. An endpoint policy doesn't override or replace IAM user policies or service-specific policies. It's a separate policy for controlling access from the endpoint to the specified service.

Endpoint policies affect canaries that are managed privately by VPC. They are not needed for canaries that run on private subnets.

Endpoint policies must be written in JSON format.

For more information, see Controlling Access to Services with VPC Endpoints in the Amazon VPC User Guide.

The following is an example of an endpoint policy for CloudWatch Synthetics. This policy enables users connecting to CloudWatch Synthetics through the VPC to view information about canaries and their runs, but not to create, modify, or delete canaries.

```json
{
    "Statement": [
        {
            "Action": [
                "synthetics:DescribeCanaries",
                "synthetics:GetCanaryRuns"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Principal": "*
        }
    ]
}
```

To edit the VPC endpoint policy for CloudWatch Synthetics

1. Open the Amazon VPC console at https://console.aws.amazon.com/vpc/.
2. In the navigation pane, choose Endpoints.
3. If you have not already created the endpoint for CloudWatch Synthetics, choose Create Endpoint. Select `com.amazonaws.region.synthetics` and then choose Create endpoint.
4. Select the `com.amazonaws.region.synthetics` endpoint and then choose the Policy tab.
5. Choose Edit Policy, and then make your changes.

- Europe (Paris)
- South America (São Paulo)
Security considerations for Synthetics canaries

The following sections explain security issues that you should consider when creating and running canaries in Synthetics.

Use secure connections

Because canary code and the results from canary test runs can contain sensitive information, do not have your canary connect to endpoints over unencrypted connections. Always use encrypted connections, such as those that begin with `https://`.

Canary naming considerations

The Amazon Resource Name (ARN) of a canary is included in the user-agent header as a part of outbound calls made from the Puppeteer-driven Chromium browser that is included as a part of the CloudWatch Synthetics wrapper library. This helps identify CloudWatch Synthetics canary traffic and relate it back to the canaries that are making calls.

The canary ARN includes the canary name. Choose canary names that do not reveal proprietary information.

Additionally, be sure to point your canaries only at websites and endpoints that you control.

Secrets in canary code

We recommend that you don’t include secrets, such as access keys or database credentials, in your canary source code. For more information about how to use AWS Secrets Manager to help keep your secrets safe, see What is AWS Secrets Manager?.

Permissions considerations

We recommend that you restrict access to resources that are created or used by CloudWatch Synthetics. Use tight permissions on the Amazon S3 buckets where canaries store test run results and other artifacts, such as logs and screenshots.

Similarly, keep tight permissions on the locations where your canary source code is stored, so that no user accidentally or maliciously deletes the Lambda layers or Lambda functions used for the canary.

To help make sure you run the canary code you intend, you can use object versioning on the Amazon S3 bucket where your canary code is stored. Then when you specify this code to run as a canary, you can include the object `versionId` as part of the path, as in the following examples.

```
https://bucket.s3.amazonaws.com/path/object.zip?versionId=version-id
https://s3.amazonaws.com/bucket/path/object.zip?versionId=version-id
https://bucket.s3-region.amazonaws.com/path/object.zip?versionId=version-id
```

Stack traces and exception messages

By default, CloudWatch Synthetics canaries capture any exception thrown by your canary script, no matter whether the script is custom or is from a blueprint. CloudWatch Synthetics logs both the exception message and the stack trace to three locations:

- Back into the CloudWatch Synthetics service to speed up debugging when you describe test runs
Scope your IAM roles narrowly

We recommend that you do not configure your canary to visit potentially malicious URLs or endpoints. Pointing your Canary to untrusted or unknown websites or endpoints could expose your Lambda function code to malicious user's scripts. Assuming a malicious website can break out of Chromium, it could have access to your Lambda code in a similar way to if you connected to it using an internet browser.

Run your Lambda function with an IAM execution role that has scoped-down permissions. This way, if your Lambda function is compromised by a malicious script, it is limited in the actions it can take when running as your canary's AWS account.

When you use the CloudWatch console to create a canary, it is created with a scoped-down IAM execution role.

Sensitive data redaction

CloudWatch Synthetics captures URLs, status code, failure reason (if any), and headers and bodies of requests and responses. This enables a canary user to understand, monitor, and debug canaries.

The configurations described in the following sections can be set at any point in canary execution. You can also choose to apply different configurations to different synthetics steps.

Request URLs

By default, CloudWatch Synthetics logs request URLs, status codes, and the status reason for each URL in canary logs. Request URLs can also appear in canary execution reports, HAR files, and so on. Your request URL might contain sensitive query parameters, such as access tokens or passwords. You can redact sensitive information from being logged by CloudWatch Synthetics.

To redact sensitive information, set the configuration property restrictedUrlParameters. For more information, see SyntheticsConfiguration class (p. 164). This causes CloudWatch Synthetics to redact URL parameters, including path and query parameter values, based on restrictedUrlParameters before logging. If you are logging URLs in your script, you can use ??? (p. 174) to redact URLs before logging. For more information, see SyntheticsLogHelper class (p. 173).

Headers

By default, CloudWatch Synthetics doesn't log request/response headers. For UI canaries, this is the default behavior for canaries using runtime version syn-nodejs-puppeteer-3.2 and later.

If your headers don't contain sensitive information, you can enable headers in HAR file and HTTP reports by setting the includeRequestHeaders and includeResponseHeaders properties to true. You can
enable all headers but choose to restrict values of sensitive header keys. For example, you can choose to only redact Authorization headers from artifacts produced by canaries.

## Request and response body

By default, CloudWatch Synthetics doesn't log the request/response body in canary logs or reports. This information is particularly useful for API canaries. Synthetics captures all HTTP requests and can show headers, request and response bodies. For more information, see `executeHttpStep(stepName, requestOptions, [callback], [stepConfig])` (p. 182). You can choose to enable request/response body by setting the `includeRequestBody` and `includeResponseBody` properties to `true`. 

743
Logging Amazon CloudWatch API calls with AWS CloudTrail

Amazon CloudWatch and CloudWatch Synthetics are integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service. CloudTrail captures API calls made by or on behalf of your AWS account. The captured calls include calls from the console and code calls to API operations.

If you create a trail, you can enable continuous delivery of CloudTrail events to an S3 bucket, including events for CloudWatch. If you don’t configure a trail, you can still view the most recent events in the CloudTrail console in Event history. Using the information collected by CloudTrail, you can determine the request that was made to CloudWatch, the IP address from which the request was made, who made the request, when it was made, and other details.

To learn more about CloudTrail, including how to configure and enable it, see the AWS CloudTrail User Guide.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element.

For an ongoing record of events in your AWS account, including events for CloudWatch and CloudWatch Synthetics, create a trail. A trail enables CloudTrail to deliver log files to an S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the S3 bucket that you specify. You can configure other AWS services to further analyze and act on the event data collected in CloudTrail logs. For more information, see the following:

- Overview for Creating a Trail
- CloudTrail Supported Services and Integrations
- Configuring Amazon SNS Notifications for CloudTrail
- Receiving CloudTrail Log Files from Multiple Regions and Receiving CloudTrail Log Files from Multiple Accounts

Topics

- CloudWatch information in CloudTrail (p. 744)
- CloudWatch Synthetics information in CloudTrail (p. 747)
Example: CloudWatch log file entries

The following example shows a CloudTrail log entry that demonstrates the PutMetricAlarm action.

```json
{
  "Records": [
    {
      "eventVersion": "1.01",
      "userIdentity": {
        "type": "Root",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "123456789012",
        "accessKeyId": "EXAMPLE_KEY_ID"
      },
      "eventTime": "2014-03-23T21:50:34Z",
      "eventSource": "monitoring.amazonaws.com",
      "eventName": "PutMetricAlarm",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "aws-sdk-ruby2/2.0.0.rc4 ruby/1.9.3 x86_64-linux Seahorse/0.1.0",
      "requestParameters": {
        "threshold": 50.0,
        "period": 60,
        "metricName": "CloudTrail Test",
        "evaluationPeriods": 3,
        "comparisonOperator": "GreaterThanThreshold",
        "namespace": "AWS/CloudWatch",
        "alarmName": "CloudTrail Test Alarm",
        "statistic": "Sum"
      },
      "responseElements": null,
      "requestID": "29184022-b2d5-11e3-a63d-9b463e6d0ff0",
      "eventID": "b096d5b7-dcf2-4399-998b-5a53eca76a27"
    },
    ..additional entries
  ]
}
```

The following log file entry shows that a user called the CloudWatch Events PutRule action.
The following log file entry shows that a user called the CloudWatch Logs `CreateExportTask` action.
CloudWatch Synthetics information in CloudTrail

CloudWatch Synthetics supports logging the following actions as events in CloudTrail log files:

- CreateCanary
- DeleteCanary
- DescribeCanaries
- DescribeCanariesLastRun
- DescribeRuntimeVersions
- GetCanary
- GetCanaryRuns
- ListTagsForResource
- StartCanary
- StopCanary
- TagResource
- UntagResource
- UpdateCanary

Example: CloudWatch Synthetics log file entries

The following example shows a CloudTrail Synthetics log entry that demonstrates the DescribeCanaries action.

```json
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:assumed-role/role_name",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EX_PRINCIPAL_ID",
                "arn": "arn:aws:iam::111222333444:role/Administrator",
                "accountId": "123456789012",
                "userName": "SAMPLE_NAME"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-04-08T21:43:34Z"
            }
        }
    }
}
```
The following example shows a CloudTrail Synthetics log entry that demonstrates the `UpdateCanary` action.

```json
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::123456789012:assumed-role/role_name",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EX_PRINCIPAL_ID",
                "arn": "arn:aws:iam::123456789012:role/Administrator",
                "accountId": "123456789012",
                "userName": "SAMPLE_NAME"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2020-04-08T21:43:24Z"
            }
        }
    },
    "eventTime": "2020-04-08T23:06:47Z",
    "eventSource": "synthetics.amazonaws.com",
    "eventName": "UpdateCanary",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "127.0.0.1",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.590 Linux/4.9.184-0.1.ac.235.83.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.212-b03 java/1.8.0_212 vendor/oracle_corporation",
    "requestParameters": {
        "Schedule": {
            "Expression": "rate(1 minute)"
        },
        "name": "sample_canary_name",
        "Code": {
            "Handler": "myOwnScript.handler",
            "ZipFile": "SAMPLE_ZIP_FILE"
        }
    },
    "responseElements": null
}
```
Example: CloudWatch Synthetics log file entries

```json
"requestID": "fe4759b0-0849-4e0e-be71-1234567890",
"eventID": "9dc60c83-c3c8-4fa5-bd02-1234567890",
"readOnly": false,
"eventType": "AwsApiCall",
"recipientAccountId": "111122223333"
}
```

The following example shows a CloudTrail Synthetics log entry that demonstrates the `GetCanaryRuns` action.

```json
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "EX_PRINCIPAL_ID",
    "arn": "arn:aws:iam::123456789012:assumed-role/role_name",
    "accountId": "123456789012",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EX_PRINCIPAL_ID",
        "arn": "arn:aws:iam::111222333444:role/Administrator",
        "accountId": "123456789012",
        "userName": "SAMPLE_NAME"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-04-08T21:43:24Z"
      }
    },
    "sourceIPAddress": "127.0.0.1",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.590 Linux/4.9.184-0.1.ac.235.83.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.212-b03 java/1.8.0_212 vendor/oracleCorporation",
    "requestParameters": {
      "Filter": "TIME_RANGE",
      "name": "sample_canary_name",
      "FilterValues": [
        "2020-04-08T23:00:00.000Z",
        "2020-04-08T23:10:00.000Z"
      ]
    },
    "responseElements": null,
  },
  "eventTime": "2020-04-08T23:06:30Z",
  "eventSource": "synthetics.amazonaws.com",
  "eventName": "GetCanaryRuns",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "127.0.0.1",
  "userAgent": "aws-internal/3 aws-sdk-java/1.11.590 Linux/4.9.184-0.1.ac.235.83.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.212-b03 java/1.8.0_212 vendor/oracleCorporation",
  "requestParameters": {
    "Filter": "TIME_RANGE",
    "name": "sample_canary_name",
    "FilterValues": [
      "2020-04-08T23:00:00.000Z",
      "2020-04-08T23:10:00.000Z"
    ]
  },
  "responseElements": null,
  "requestID": "2f56318c-cfbd-4b60-9d93-1234567890",
  "eventID": "52723fd9-4a54-478c-ac55-1234567890",
  "readOnly": true,
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}
```
Grafana integration

You can use Grafana version 6.5.0 and later to contextually advance through the CloudWatch console and query a dynamic list of metrics by using wildcards. This can help you monitor metrics for AWS resources, such as Amazon Elastic Compute Cloud instances or containers. When new instances are created as part of an Auto Scaling event, they appear in the graph automatically. You don't need to track the new instance IDs. Prebuilt dashboards help simplify the getting started experience for monitoring Amazon EC2, Amazon Elastic Block Store, and AWS Lambda resources.

You can use Grafana version 7.0 and later to perform CloudWatch Logs Insights queries on log groups in CloudWatch Logs. You can visualize your query results in bar, line, and stacked graphs and in a table format. For more information about CloudWatch Logs Insights, see Analyzing Log Data with CloudWatch Logs Insights.

For more information about how to get started, see Using AWS CloudWatch in Grafana in the Grafana Labs documentation.
CloudWatch has the following quotas for metrics, alarms, API requests, and alarm email notifications.

<table>
<thead>
<tr>
<th>Resource</th>
<th>Default quota</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm actions</td>
<td>5/alarm. This quota cannot be changed.</td>
</tr>
<tr>
<td>Alarms</td>
<td>10/month/customer for free. 5000 per Region, per account. You can request a quota increase. Alarms based on metric math expressions can have up to 10 metrics.</td>
</tr>
<tr>
<td>Anomaly detection models</td>
<td>500 per Region, per account.</td>
</tr>
<tr>
<td>API requests</td>
<td>1,000,000/month/customer for free.</td>
</tr>
<tr>
<td>Canaries</td>
<td>200 per Region per account in the following Regions: US East (N. Virginia), US East (Ohio), US West (Oregon), Europe (Ireland), and Asia Pacific (Tokyo). 100 per Region per account in all other Regions. You can request a quota increase.</td>
</tr>
<tr>
<td>Contributor Insights API requests</td>
<td>GetInsightRuleReport has a quota of 20 transactions per second (TPS), per Region. You can request a quota increase. The following APIs have a quota of 1 TPS per Region. This quota cannot be changed. • DeleteInsightRules • DescribeInsightRules • DisableInsightRules • EnableInsightRules • PutInsightRule</td>
</tr>
<tr>
<td>Contributor Insights rules</td>
<td>100 rules per Region per account. You can request a quota increase.</td>
</tr>
<tr>
<td>Custom metrics</td>
<td>No quota.</td>
</tr>
<tr>
<td>Dashboards</td>
<td>Up to 500 metrics per dashboard widget. Up to 2500 metrics per dashboard, across all widgets. These quotas include all metrics retrieved for use in metric math functions, even if those metrics are not displayed on the graph. These quotas cannot be changed.</td>
</tr>
<tr>
<td>Resource</td>
<td>Default quota</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>DescribeAlarms</strong></td>
<td>9 transactions per second (TPS) per Region. The maximum number of operation requests you can make per second without being throttled. You can request a quota increase.</td>
</tr>
<tr>
<td><strong>DeleteAlarms</strong> request</td>
<td>3 TPS per Region for each of these operations. The maximum number of operation requests you can make per second without being throttled. These quotas cannot be changed.</td>
</tr>
<tr>
<td><strong>DescribeAlarmHistory</strong> request</td>
<td>3 TPS per Region for each of these operations. The maximum number of operation requests you can make per second without being throttled. These quotas cannot be changed.</td>
</tr>
<tr>
<td><strong>DisableAlarmActions</strong> request</td>
<td>3 TPS per Region for each of these operations. The maximum number of operation requests you can make per second without being throttled. These quotas cannot be changed.</td>
</tr>
<tr>
<td><strong>EnableAlarmActions</strong> request</td>
<td>3 TPS per Region for each of these operations. The maximum number of operation requests you can make per second without being throttled. These quotas cannot be changed.</td>
</tr>
<tr>
<td><strong>SetAlarmState</strong> request</td>
<td>3 TPS per Region for each of these operations. The maximum number of operation requests you can make per second without being throttled. These quotas cannot be changed.</td>
</tr>
<tr>
<td><strong>DescribeAlarmsForMetric</strong> request</td>
<td>9 TPS per Region. The maximum number of operation requests you can make per second without being throttled. This quotas cannot be changed.</td>
</tr>
<tr>
<td><strong>DeleteDashboards</strong> request</td>
<td>10 TPS per Region for each of these operations. The maximum number of operation requests you can make per second without being throttled. These quotas cannot be changed.</td>
</tr>
<tr>
<td><strong>GetDashboard</strong> request</td>
<td>10 TPS per Region for each of these operations. The maximum number of operation requests you can make per second without being throttled. These quotas cannot be changed.</td>
</tr>
<tr>
<td><strong>ListDashboards</strong> request</td>
<td>10 TPS per Region for each of these operations. The maximum number of operation requests you can make per second without being throttled. These quotas cannot be changed.</td>
</tr>
<tr>
<td><strong>PutDashboard</strong> request</td>
<td>10 TPS per Region. The maximum number of operation requests you can make per second without being throttled.</td>
</tr>
<tr>
<td><strong>PutAnomalyDetector</strong></td>
<td>10 TPS per Region. The maximum number of operation requests you can make per second without being throttled.</td>
</tr>
<tr>
<td><strong>DescribeAnomalyDetectors</strong></td>
<td>5 TPS per Region. The maximum number of operation requests you can make per second without being throttled.</td>
</tr>
<tr>
<td><strong>DeleteAnomalyDetector</strong></td>
<td>5 TPS per Region. The maximum number of operation requests you can make per second without being throttled.</td>
</tr>
<tr>
<td><strong>Dimensions</strong></td>
<td>10/metric. This quota cannot be changed.</td>
</tr>
<tr>
<td><strong>GetMetricData</strong></td>
<td>50 TPS per Region. The maximum number of operation requests you can make per second without being throttled. You can request a quota increase.</td>
</tr>
<tr>
<td></td>
<td>180,000 Datapoints Per Second (DPS) if the StartTime used in the API request is less than or equal to three hours from current time. 396,000 DPS if the StartTime is more than three hours from current time. This is the maximum number of datapoints you can request per second using one or more API calls without being throttled. This quota cannot be changed.</td>
</tr>
<tr>
<td></td>
<td>The DPS is calculated based on estimated data points, not actual data points. The data point estimate is calculated using the requested time range, period, and retention period. This means that if the actual data points in the requested metrics are sparse or empty, throttling still occurs if the estimated data points exceed the quota. The DPS quota is per-Region.</td>
</tr>
<tr>
<td>Resource</td>
<td>Default quota</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GetMetricData</td>
<td>A single GetMetricData call can include as many as 500 MetricDataQuery structures. This quota cannot be changed.</td>
</tr>
<tr>
<td>GetMetricStatistics</td>
<td>400 TPS per Region. The maximum number of operation requests you can make per second without being throttled. You can request a quota increase.</td>
</tr>
<tr>
<td>GetMetricWidgetImage</td>
<td>Up to 500 metrics per image. This quota cannot be changed. 20 TPS per Region. The maximum number of operation requests you can make per second without being throttled. This quota cannot be changed.</td>
</tr>
<tr>
<td>ListMetrics</td>
<td>25 TPS per Region. The maximum number of operation requests you can make per second without being throttled. You can request a quota increase.</td>
</tr>
<tr>
<td>Metric data storage</td>
<td>15 months. This quota cannot be changed.</td>
</tr>
<tr>
<td>Metric data values</td>
<td>The value of a metric data point must be within the range of -2^360 to 2^360. Special values (for example, NaN, +Infinity, -Infinity) are not supported. This quota cannot be changed.</td>
</tr>
<tr>
<td>MetricDatum items</td>
<td>20/PutMetricData request. A MetricDatum object can contain a single value or a StatisticSet object representing many values. This quota cannot be changed.</td>
</tr>
<tr>
<td>Metrics</td>
<td>10/month/customer for free.</td>
</tr>
<tr>
<td>Period</td>
<td>Maximum value is one day (86,400 seconds). This quota cannot be changed.</td>
</tr>
<tr>
<td>PutMetricAlarm request</td>
<td>3 TPS per Region. The maximum number of operation requests you can make per second without being throttled. You can request a quota increase.</td>
</tr>
<tr>
<td>PutMetricData request</td>
<td>40 KB for HTTP POST requests. PutMetricData can handle 150 transactions per second (TPS), which is the maximum number of operation requests you can make per second without being throttled. You can request a quota increase.</td>
</tr>
<tr>
<td>Amazon SNS email notifications</td>
<td>1,000/month/customer for free.</td>
</tr>
</tbody>
</table>
# Document history

The following table describes important changes in each release of the *Amazon CloudWatch User Guide*, beginning in June 2018. For notification about updates to this documentation, you can subscribe to an RSS feed.

<table>
<thead>
<tr>
<th>update-history-change</th>
<th>update-history-description</th>
<th>update-history-date</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDK Metrics is no longer supported. (p. 754)</td>
<td>CloudWatch SDK Metrics is no longer supported.</td>
<td>August 25, 2021</td>
</tr>
<tr>
<td>Amazon CloudWatch Application Insights support for setting up container monitoring. (p. 546)</td>
<td>You can monitor containers using best practices with Amazon CloudWatch Application Insights.</td>
<td>May 18, 2021</td>
</tr>
<tr>
<td>Metric streams is generally available (p. 754)</td>
<td>You can use metric streams to continually stream CloudWatch metrics to a destination of your choice. For more information, see Metric streams in the <em>Amazon CloudWatch User Guide</em>.</td>
<td>March 31, 2021</td>
</tr>
<tr>
<td>Amazon CloudWatch Application Insights monitoring for Oracle databases on Amazon RDS and Amazon EC2. (p. 546)</td>
<td>You can monitor metrics and logs retrieved from Oracle with Amazon CloudWatch Application Insights.</td>
<td>January 16, 2021</td>
</tr>
<tr>
<td>Lambda Insights is generally available (p. 754)</td>
<td>CloudWatch Lambda Insights is a monitoring and troubleshooting solution for serverless applications running on AWS Lambda. For more information, see Using Lambda Insights in the <em>Amazon CloudWatch User Guide</em>.</td>
<td>December 3, 2020</td>
</tr>
<tr>
<td>Amazon CloudWatch Application Insights monitoring for Prometheus JMX exporter metrics. (p. 546)</td>
<td>You can monitor metrics retrieved from Prometheus JMX exporter with Amazon CloudWatch Application Insights.</td>
<td>November 20, 2020</td>
</tr>
<tr>
<td>CloudWatch Synthetics releases new runtime version (p. 754)</td>
<td>CloudWatch Synthetics has released a new runtime version. For more information, see Canary Runtime Versions in the <em>Amazon CloudWatch User Guide</em>.</td>
<td>September 11, 2020</td>
</tr>
<tr>
<td>Amazon CloudWatch Application Insights monitoring for PostgreSQL running on Amazon RDS and Amazon EC2. (p. 546)</td>
<td>You can monitor applications built with PostgreSQL running on Amazon RDS or Amazon EC2.</td>
<td>September 11, 2020</td>
</tr>
<tr>
<td>CloudWatch supports dashboard sharing (p. 754)</td>
<td>You can now share CloudWatch dashboards with people outside of your organization and AWS account. For more information,</td>
<td>September 10, 2020</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Set up monitors for .NET applications using SQL Server on the backend with CloudWatch Application Insights (p. 546)</td>
<td>You can use the documentation tutorial to help you to set up monitors for .NET applications using SQL Server on the backend with CloudWatch Application Insights.</td>
<td>August 19, 2020</td>
</tr>
<tr>
<td>AWS CloudFormation support for Amazon CloudWatch Application Insights applications. (p. 546)</td>
<td>You can add CloudWatch Application Insights monitoring, including key metrics and telemetry, to your application, database, and web server, directly from AWS CloudFormation templates.</td>
<td>July 30, 2020</td>
</tr>
<tr>
<td>Amazon CloudWatch Application Insights monitoring for Aurora for MySQL database clusters. (p. 546)</td>
<td>You can monitor Aurora for MySQL database clusters (RDS Aurora) with Amazon CloudWatch Application Insights.</td>
<td>July 2, 2020</td>
</tr>
<tr>
<td>CloudWatch Contributor Insights general availability (p. 754)</td>
<td>CloudWatch Contributor Insights is now generally available. It enables you to analyze log data and create time series that display contributor data. You can see metrics about the top-N contributors, the total number of unique contributors, and their usage. For more information, see Using Contributor Insights to Analyze High-Cardinality Data in the Amazon CloudWatch User Guide.</td>
<td>April 2, 2020</td>
</tr>
<tr>
<td>CloudWatch Synthetics public preview (p. 754)</td>
<td>CloudWatch Synthetics is now in public preview. It enables you to create canaries to monitor your endpoints and APIs. For more information, see Using Canaries in the Amazon CloudWatch User Guide.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td>CloudWatch Contributor Insights public preview (p. 754)</td>
<td>CloudWatch Contributor Insights is now in public preview. It enables you to analyze log data and create time series that display contributor data. You can see metrics about the top-N contributors, the total number of unique contributors, and their usage. For more information, see Using Contributor Insights to Analyze High-Cardinality Data in the Amazon CloudWatch User Guide.</td>
<td>November 25, 2019</td>
</tr>
<tr>
<td>CloudWatch launches ServiceLens feature (p. 754)</td>
<td>ServiceLens enhances the observability of your services and applications by enabling you to integrate traces, metrics, logs, and alarms into one place. ServiceLens integrates CloudWatch with AWS X-Ray to provide an end-to-end view of your application. For more information, see Using ServiceLens to Monitor the Health of Your Applications in the Amazon CloudWatch User Guide.</td>
<td>November 21, 2019</td>
</tr>
<tr>
<td>Use CloudWatch to proactively manage your AWS service quotas (p. 754)</td>
<td>You can use CloudWatch to proactively manage your AWS service quotas. CloudWatch usage metrics provide visibility into your account's usage of resources and API operations. For more information, see Service Quotas Integration and Usage Metrics in the Amazon CloudWatch User Guide.</td>
<td>November 19, 2019</td>
</tr>
<tr>
<td>CloudWatch sends events when alarms change state (p. 754)</td>
<td>CloudWatch now sends an event to Amazon EventBridge when any CloudWatch alarm changes state. For more information, see Alarm Events and EventBridge in the Amazon CloudWatch User Guide.</td>
<td>October 8, 2019</td>
</tr>
<tr>
<td><strong>Container Insights (p. 754)</strong></td>
<td>CloudWatch Container Insights is now generally available. It enables you to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices. For more information, see Using Container Insights in the Amazon CloudWatch User Guide.</td>
<td>August 30, 2019</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td><strong>Updates for Container Insights preview metrics on Amazon EKS and Kubernetes (p. 754)</strong></td>
<td>The Container Insights on Amazon EKS and Kubernetes public preview has been updated. InstanceId is now included as a dimension to the cluster EC2 instances. This allows alarms that have been created on these metrics to trigger the following EC2 actions: Stop, Terminate, Reboot, or Recover. Additionally, pod and service metrics are now reported by Kubernetes namespace to simplify the monitoring and alarming on metrics by namespace.</td>
<td>August 19, 2019</td>
</tr>
<tr>
<td><strong>Updates for AWS Systems Manager OpsCenter integration (p. 754)</strong></td>
<td>Updates on how CloudWatch Application Insights integrates with Systems Manager OpsCenter.</td>
<td>August 7, 2019</td>
</tr>
<tr>
<td><strong>CloudWatch usage metrics (p. 754)</strong></td>
<td>CloudWatch usage metrics help you track the usage of your CloudWatch resources and stay within your service limits. For more information, see <a href="https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Usage-Metrics.html">https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/CloudWatch-Usage-Metrics.html</a>.</td>
<td>August 6, 2019</td>
</tr>
<tr>
<td><strong>CloudWatch Container Insights public preview (p. 754)</strong></td>
<td>CloudWatch Container Insights is now in public preview. It enables you to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices. For more information, see Using Container Insights in the Amazon CloudWatch User Guide.</td>
<td>July 9, 2019</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td>Date</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------</td>
</tr>
<tr>
<td>CloudWatch Anomaly Detection public preview (p. 754)</td>
<td>CloudWatch anomaly detection is now in public preview. CloudWatch applies machine-learning algorithms to a metric's past data to create a model of the metric's expected values. You can use this model for visualization and for setting alarms. For more information, see Using CloudWatch Anomaly Detection in the Amazon CloudWatch User Guide.</td>
<td>July 9, 2019</td>
</tr>
<tr>
<td>CloudWatch Application Insights for .NET and SQL Server (p. 754)</td>
<td>CloudWatch Application Insights for .NET and SQL Server facilitates observability for .NET and SQL Server applications. It can help you set up the best monitors for your application resources to continuously analyze data for signs of problems with your applications.</td>
<td>June 21, 2019</td>
</tr>
<tr>
<td>CloudWatch agent section re-organized (p. 754)</td>
<td>The CloudWatch agent documentation has been rewritten to improve clarity, especially for customers using the command line to install and configure the agent. For more information, see Collecting Metrics and Logs from Amazon EC2 Instances and On-Premises Servers with the CloudWatch Agent in the Amazon CloudWatch User Guide.</td>
<td>March 28, 2019</td>
</tr>
<tr>
<td>SEARCH function added to metric math expressions (p. 754)</td>
<td>You can now use a SEARCH function in metric math expressions. This enables you to create dashboards that update automatically as new resources are created that match the search query. For more information, see Using Search Expressions in Graphs in the Amazon CloudWatch User Guide.</td>
<td>March 21, 2019</td>
</tr>
<tr>
<td>AWS SDK Metrics for Enterprise Support (p. 754)</td>
<td>SDK Metrics helps you assess the health of your AWS services and diagnose latency caused by reaching your account usage limits or by a service outage. For more information, see Monitor Applications Using AWS SDK Metrics in the Amazon CloudWatch User Guide.</td>
<td>December 11, 2018</td>
</tr>
</tbody>
</table>
The following table describes important changes to the Amazon CloudWatch User Guide before June 2018.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Release date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric math</td>
<td>You can now perform math expressions on CloudWatch metrics, producing new time series that you can add to graphs on your dashboard. For more information, see Using metric math (p. 77).</td>
<td>April 4, 2018</td>
</tr>
</tbody>
</table>

<p>| Alarms on math expressions (p. 754) | CloudWatch supports creating alarms based on metric math expressions. For more information, see Alarms on Math Expressions in the Amazon CloudWatch User Guide. | November 20, 2018 |
| New CloudWatch console homepage (p. 754) | Amazon has created a new home page in the CloudWatch console, which automatically displays key metrics and alarms for all the AWS services you are using. For more information, see Getting Started with Amazon CloudWatch in the Amazon CloudWatch User Guide. | November 19, 2018 |
| AWS CloudFormation templates for the CloudWatch Agent (p. 754) | Amazon has uploaded AWS CloudFormation templates that you can use to install and update the CloudWatch agent. For more information, see Install the CloudWatch Agent on New Instances Using AWS CloudFormation in the Amazon CloudWatch User Guide. | November 9, 2018 |
| Enhancements to the CloudWatch Agent (p. 754) | The CloudWatch agent has been updated to work with both the StatsD and collectd protocols. It also has improved cross-account support. For more information, see Retrieve Custom Metrics with StatsD, Retrieve Custom Metrics with collectd, and Sending Metrics and Logs to a Different AWS Account in the Amazon CloudWatch User Guide. | September 28, 2018 |
| Support for Amazon VPC endpoints (p. 754) | You can now establish a private connection between your VPC and CloudWatch. For more information, see Using CloudWatch with Interface VPC Endpoints in the Amazon CloudWatch User Guide. | June 28, 2018 |</p>
<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Release date</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;M out of N&quot; alarms</td>
<td>You can now configure an alarm to trigger based on &quot;M out of N&quot; datapoints in any alarm evaluation interval. For more information, see Evaluating an alarm (p. 103).</td>
<td>December 8, 2017</td>
</tr>
<tr>
<td>CloudWatch agent</td>
<td>A new unified CloudWatch agent was released. You can use the unified multi-platform agent to collect custom both system metrics and log files from Amazon EC2 instances and on-premises servers. The new agent supports both Windows and Linux and enables customization of metrics collected, including sub-resource metrics such as per-CPU core. For more information, see Collecting metrics and logs from Amazon EC2 instances and on-premises servers with the CloudWatch agent (p. 428).</td>
<td>September 7, 2017</td>
</tr>
<tr>
<td>NAT gateway metrics</td>
<td>Added metrics for Amazon VPC NAT gateway.</td>
<td>September 7, 2017</td>
</tr>
<tr>
<td>High-resolution metrics</td>
<td>You can now optionally set up custom metrics as high-resolution metrics, with a granularity of as low as one second. For more information, see High-resolution metrics (p. 74).</td>
<td>July 26, 2017</td>
</tr>
<tr>
<td>Dashboard APIs</td>
<td>You can now create, modify, and delete dashboards using APIs and the AWS CLI. For more information, see Creating a CloudWatch dashboard (p. 18).</td>
<td>July 6, 2017</td>
</tr>
<tr>
<td>AWS Direct Connect metrics</td>
<td>Added metrics for AWS Direct Connect.</td>
<td>June 29, 2017</td>
</tr>
<tr>
<td>Amazon VPC VPN metrics</td>
<td>Added metrics for Amazon VPC VPN.</td>
<td>May 15, 2017</td>
</tr>
<tr>
<td>AppStream 2.0 metrics</td>
<td>Added metrics for AppStream 2.0.</td>
<td>March 8, 2017</td>
</tr>
<tr>
<td>CloudWatch console color picker</td>
<td>You can now choose the color for each metric on your dashboard widgets. For more information, see Edit a graph on a CloudWatch dashboard (p. 25).</td>
<td>February 27, 2017</td>
</tr>
<tr>
<td>Alarms on dashboards</td>
<td>Alarms can now be added to dashboards. For more information, see Add an alarm widget to a CloudWatch dashboard (p. 28).</td>
<td>February 15, 2017</td>
</tr>
<tr>
<td>Added metrics for Amazon Polly</td>
<td>Added metrics for Amazon Polly.</td>
<td>December 1, 2016</td>
</tr>
<tr>
<td>Added metrics for Amazon Kinesis Data Analytics</td>
<td>Added metrics for Amazon Kinesis Data Analytics.</td>
<td>December 1, 2016</td>
</tr>
<tr>
<td>Added support for percentile statistics</td>
<td>You can specify any percentile, using up to two decimal places (for example, p95.45). For more information, see Percentiles (p. 7).</td>
<td>November 17, 2016</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Release date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Added metrics for Amazon Simple Email Service</td>
<td>Added metrics for Amazon Simple Email Service.</td>
<td>November 2, 2016</td>
</tr>
<tr>
<td>Updated metrics retention</td>
<td>Amazon CloudWatch now retains metrics data for 15 months instead of 14 days.</td>
<td>November 1, 2016</td>
</tr>
<tr>
<td>Updated metrics console interface</td>
<td>The CloudWatch console is updated with improvements to existing functionality and new functionality.</td>
<td>November 1, 2016</td>
</tr>
<tr>
<td>Added metrics for Amazon Elastic Transcoder</td>
<td>Added metrics for Amazon Elastic Transcoder.</td>
<td>September 20, 2016</td>
</tr>
<tr>
<td>Added metrics for Amazon API Gateway</td>
<td>Added metrics for Amazon API Gateway.</td>
<td>September 9, 2016</td>
</tr>
<tr>
<td>Added metrics for AWS Key Management Service</td>
<td>Added metrics for AWS Key Management Service.</td>
<td>September 9, 2016</td>
</tr>
<tr>
<td>Added metrics for the new Application Load Balancers supported by Elastic Load Balancing</td>
<td>Added metrics for Application Load Balancers.</td>
<td>August 11, 2016</td>
</tr>
<tr>
<td>Added new metrics for Amazon EC2 Spot fleet</td>
<td>Added new metrics for Amazon EC2 Spot fleet.</td>
<td>March 21, 2016</td>
</tr>
<tr>
<td>Added new CloudWatch Logs metrics</td>
<td>Added new CloudWatch Logs metrics.</td>
<td>March 10, 2016</td>
</tr>
<tr>
<td>Added Amazon Elasticsearch Service and AWS WAF metrics and dimensions</td>
<td>Added Amazon Elasticsearch Service and AWS WAF metrics and dimensions.</td>
<td>October 14, 2015</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Release date</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>Added support for CloudWatch dashboards</td>
<td>Dashboards are customizable home pages in the CloudWatch console that you can use to monitor your resources in a single view, even those that are spread out across different Regions. For more information, see Using Amazon CloudWatch dashboards (p. 17).</td>
<td>October 8, 2015</td>
</tr>
<tr>
<td>Added AWS Lambda metrics and dimensions</td>
<td>Added AWS Lambda metrics and dimensions.</td>
<td>September 4, 2015</td>
</tr>
<tr>
<td>Added Amazon Elastic Container Service metrics and dimensions</td>
<td>Added Amazon Elastic Container Service metrics and dimensions.</td>
<td>August 17, 2015</td>
</tr>
<tr>
<td>Added Amazon Simple Storage Service metrics and dimensions</td>
<td>Added Amazon Simple Storage Service metrics and dimensions.</td>
<td>July 26, 2015</td>
</tr>
<tr>
<td>New feature: Reboot alarm action</td>
<td>Added the reboot alarm action and new IAM role for use with alarm actions. For more information, see Create alarms to stop, terminate, reboot, or recover an EC2 instance (p. 125).</td>
<td>July 23, 2015</td>
</tr>
<tr>
<td>Added Amazon WorkSpaces metrics and dimensions</td>
<td>Added Amazon WorkSpaces metrics and dimensions.</td>
<td>April 30, 2015</td>
</tr>
<tr>
<td>Added Amazon Machine Learning metrics and dimensions</td>
<td>Added Amazon Machine Learning metrics and dimensions.</td>
<td>April 9, 2015</td>
</tr>
<tr>
<td>New feature: Amazon EC2 instance recovery alarm actions</td>
<td>Updated alarm actions to include new EC2 instance recovery action. For more information, see Create alarms to stop, terminate, reboot, or recover an EC2 instance (p. 125).</td>
<td>March 12, 2015</td>
</tr>
<tr>
<td>Added Amazon CloudFront and Amazon CloudSearch metrics and dimensions</td>
<td>Added Amazon CloudFront and Amazon CloudSearch metrics and dimensions.</td>
<td>March 6, 2015</td>
</tr>
<tr>
<td>Added Amazon Simple Workflow Service metrics and dimensions</td>
<td>Added Amazon Simple Workflow Service metrics and dimensions.</td>
<td>May 9, 2014</td>
</tr>
<tr>
<td>Updated guide to add support for AWS CloudTrail</td>
<td>Added a new topic to explain how you can use AWS CloudTrail to log activity in Amazon CloudWatch. For more information, see Logging Amazon CloudWatch API calls with AWS CloudTrail (p. 744).</td>
<td>April 30, 2014</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Release date</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
<td>--------------</td>
</tr>
<tr>
<td>Updated guide to use the new AWS Command Line Interface (AWS CLI)</td>
<td>The AWS CLI is a cross-service CLI with a simplified installation, unified configuration, and consistent command line syntax. The AWS CLI is supported on Linux/Unix, Windows, and Mac. The CLI examples in this guide have been updated to use the new AWS CLI. For information about how to install and configure the new AWS CLI, see Getting Set Up with the AWS CLI Interface in the AWS Command Line Interface User Guide.</td>
<td>February 21, 2014</td>
</tr>
<tr>
<td>Added Amazon Redshift and AWS OpsWorks metrics and dimensions</td>
<td>Added Amazon Redshift and AWS OpsWorks metrics and dimensions.</td>
<td>July 16, 2013</td>
</tr>
<tr>
<td>Added Amazon Route 53 metrics and dimensions</td>
<td>Added Amazon Route 53 metrics and dimensions.</td>
<td>June 26, 2013</td>
</tr>
<tr>
<td>New feature: Amazon CloudWatch Alarm Actions</td>
<td>Added a new section to document Amazon CloudWatch alarm actions, which you can use to stop or terminate an Amazon Elastic Compute Cloud instance. For more information, see Create alarms to stop, terminate, reboot, or recover an EC2 instance (p. 125).</td>
<td>January 8, 2013</td>
</tr>
<tr>
<td>Updated EBS metrics</td>
<td>Updated the EBS metrics to include two new metrics for Provisioned IOPS volumes.</td>
<td>November 20, 2012</td>
</tr>
<tr>
<td>New billing alerts</td>
<td>You can now monitor your AWS charges using Amazon CloudWatch metrics and create alarms to notify you when you have exceeded the specified threshold. For more information, see Creating a billing alarm to monitor your estimated AWS charges (p. 130).</td>
<td>May 10, 2012</td>
</tr>
<tr>
<td>New metrics</td>
<td>You can now access six new Elastic Load Balancing metrics that provide counts of various HTTP response codes.</td>
<td>October 19, 2011</td>
</tr>
<tr>
<td>New feature</td>
<td>You can now access metrics from Amazon EMR.</td>
<td>June 30, 2011</td>
</tr>
<tr>
<td>New feature</td>
<td>You can now access metrics from Amazon Simple Notification Service and Amazon Simple Queue Service.</td>
<td>July 14, 2011</td>
</tr>
<tr>
<td>New Feature</td>
<td>Added information about using the PutMetricData API to publish custom metrics. For more information, see Publishing custom metrics (p. 74).</td>
<td>May 10, 2011</td>
</tr>
<tr>
<td>Updated metrics retention</td>
<td>Amazon CloudWatch now retains the history of an alarm for two weeks rather than six weeks. With this change, the retention period for alarms matches the retention period for metrics data.</td>
<td>April 7, 2011</td>
</tr>
<tr>
<td>Change</td>
<td>Description</td>
<td>Release date</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>New feature</td>
<td>Added ability to send Amazon Simple Notification Service or Auto Scaling notifications when a metric has crossed a threshold. For more information, see Alarms (p. 8).</td>
<td>December 2, 2010</td>
</tr>
<tr>
<td>New feature</td>
<td>A number of CloudWatch actions now include the MaxRecords and NextToken parameters, which enable you to control pages of results to display.</td>
<td>December 2, 2010</td>
</tr>
<tr>
<td>New feature</td>
<td>This service now integrates with AWS Identity and Access Management (IAM).</td>
<td>December 2, 2010</td>
</tr>
</tbody>
</table>