



Solutions Architect Professional

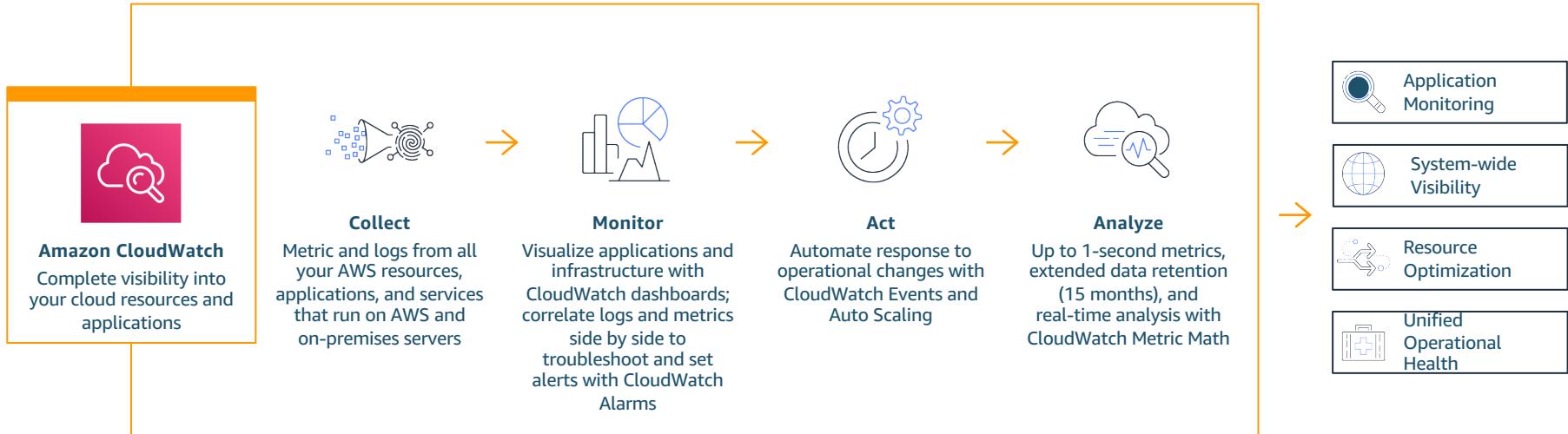
Deployment and Operations



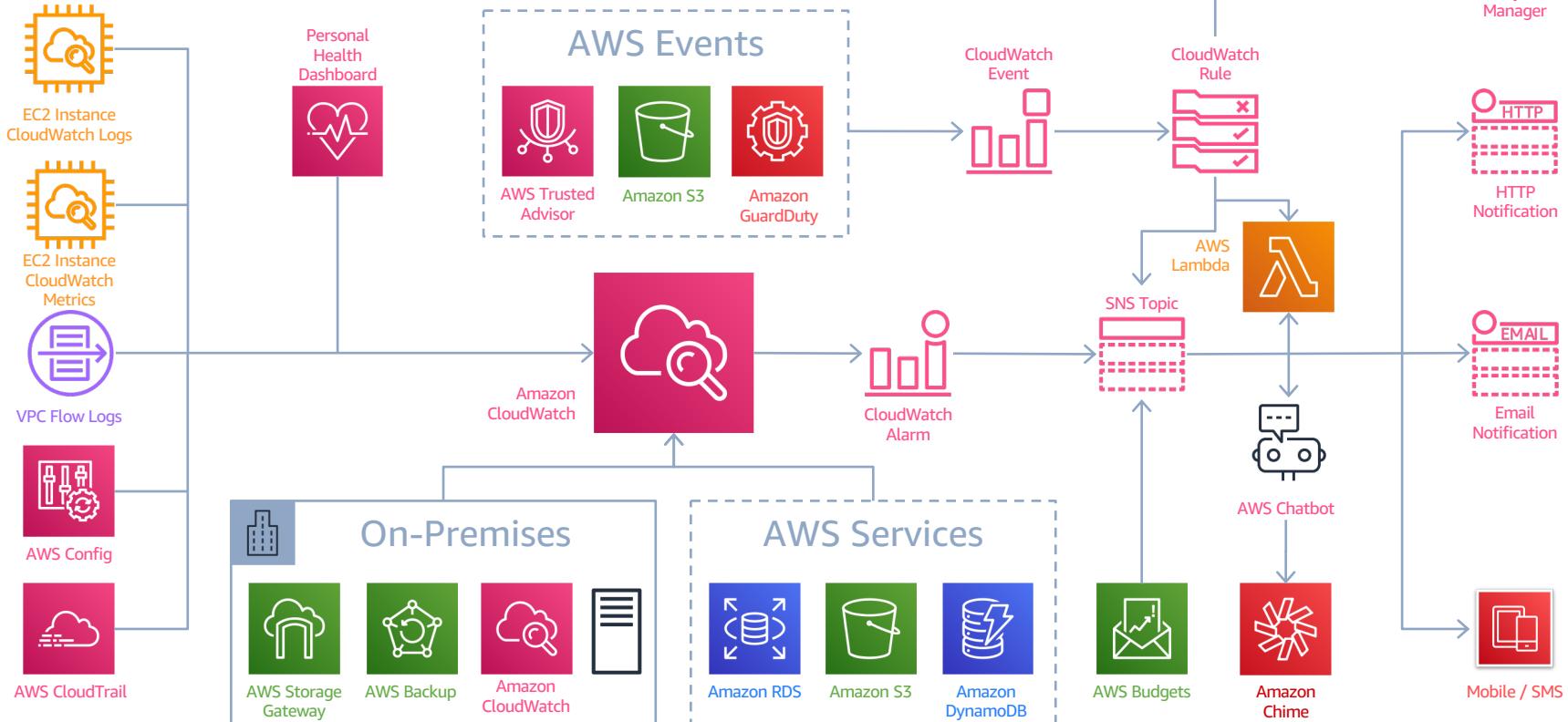
CloudWatch



How it works



Integration



Collect



Easily collect and store logs

The Amazon CloudWatch Logs service allows you to collect and store logs from your resources, applications, and services in near real-time.

Collect logs from:

- Amazon EC2 instances
- On-premises servers
- VPC Flow Logs
- AWS CloudTrail
- AWS Lambda
- Other AWS Services

Log data can be stored and accessed indefinitely in highly durable, low-cost storage so you don't have to worry about filling up hard drives.

The screenshot shows the AWS CloudWatch Logs console interface. At the top, there's a header with 'CloudWatch' and 'CloudWatch Logs' sections, followed by 'Log groups' and a search bar. Below the header, the specific log group 'application.log' is selected, indicated by a blue border. The main area is divided into two main sections: 'Log group details' and 'Log streams'.

Log group details:

| Retention | Creation time | Stored bytes | ARN |
|--------------|----------------|--|---|
| Never expire | 5 months ago | 14.67 MB | arn:aws:logs:eu-west-1:012345678910:log-group:application.log:* |
| KMS key ID | Metric filters | Subscriptions | Contributor Insights rules |
| - | 1 | LambdaStream_centralized-logging-LogStreamer-1A2RQLP14N1TW | - |

Log streams:

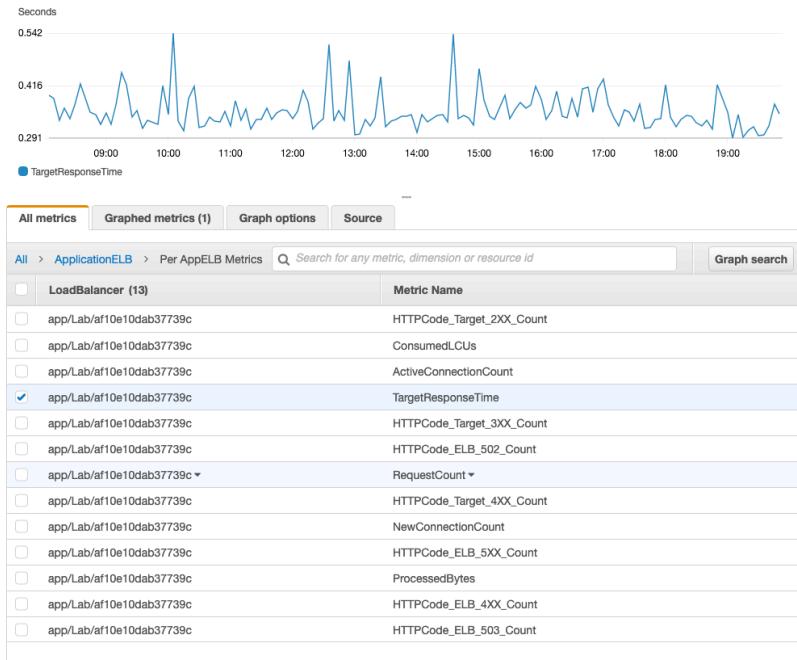
| Log stream | Last event time |
|---------------------|------------------------|
| I-077f7e49ee1c0112c | 1/10/2020, 8:00:49 PM |
| I-03343584efd07d2a6 | 11/29/2019, 8:03:35 PM |
| I-09bd407810ebfa83f | 11/29/2019, 8:00:52 PM |
| I-0bf3c984cda70e7c0 | 9/19/2019, 9:00:35 PM |
| I-0d6468fa547a61f14 | 9/19/2019, 9:00:35 PM |

Built-in metrics

Collecting metrics is time consuming. Amazon CloudWatch allows you to collect default metrics from more than 70 AWS services, such as:

- Amazon EC2
- Amazon DynamoDB
- Amazon S3
- Amazon ECS
- AWS Lambda
- Amazon API Gateway

No action is required on your part. For example, EC2 instances automatically publish CPU utilization, data transfer, and disk usage metrics to help you understand changes in state.



Built-in metrics

| Service | Namespace | Service | Namespace | Service | Namespace |
|----------------------------------|-----------------------|---|----------------------|--|--------------------|
| Amazon API Gateway | AWS/ApiGateway | Amazon ElastiCache for Memcached | AWS/ElastiCache | Amazon Neptune | AWS/Neptune |
| AppStream 2.0 | AWS/AppStream | Amazon ElastiCache for Redis | AWS/ElasticCache | AWS OpsWorks | AWS/OpsWorks |
| AWS AppSync | AWS/AppSync | Amazon Elasticsearch Service | AWS/ES | Amazon Polly | AWS/Polly |
| Amazon Athena | AWS/Athena | Amazon EMR | AWS/ElasticMapReduce | Amazon QLDB | AWS/QLDB |
| AWS Billing and Cost Management | AWS/Billing | AWS Elemental MediaConnect | AWS/MediaConnect | Amazon Redshift | AWS/Redshift |
| ACM Private CA | AWS/ACMPublicCA | AWS Elemental MediaConvert | AWS/MediaConvert | Amazon Relational Database Service | AWS/RDS |
| AWS Chatbot | AWS/Chatbot | AWS Elemental MediaPackage | AWS/MediaPackage | AWS RoboMaker | AWS/Robomaker |
| Amazon CloudFront | AWS/CloudFront | AWS Elemental MediaStore | AWS/MediaStore | Amazon Route 53 | AWS/Route53 |
| AWS CloudHSM | AWS/CloudHSM | AWS Elemental MediaTailor | AWS/MediaTailor | Amazon SageMaker | AWS/SageMaker |
| Amazon CloudSearch | AWS/CloudSearch | Amazon EventBridge | AWS/Events | AWS SDK Metrics for Enterprise Support | AWS/SDKMetrics |
| Amazon CloudWatch Logs | AWS/Logs | Amazon FSx for Lustre | AWS/FSx | AWS Service Catalog | AWS/ServiceCatalog |
| AWS CodeBuild | AWS/CodeBuild | Amazon FSx for Windows File Server | AWS/FSx | AWS Shield Advanced | AWS/DDoSProtection |
| Amazon Cognito | AWS/Cognito | Amazon GameLift | AWS/GameLift | Amazon Simple Email Service | AWS/SES |
| Amazon Connect | AWS/Connect | AWS Glue | AWS/Glue | Amazon Simple Notification Service | AWS/SNS |
| AWS DataSync | AWS/DataSync | AWS Ground Station | AWS/GroundStation | Amazon Simple Queue Service | AWS/SQS |
| AWS Database Migration Service | AWS/DMS | Amazon Inspector | AWS/Inspector | Amazon Simple Storage Service | AWS/S3 |
| AWS Direct Connect | AWS/DX | AWS IoT | AWS/IoT | Amazon Simple Workflow Service | AWS/SWF |
| Amazon DocumentDB | AWS/DocDB | AWS IoT Analytics | AWS/IoTAnalytics | AWS Step Functions | AWS/States |
| Amazon DynamoDB | AWS/DynamoDB | AWS IoT SiteWise | AWS/IoTSiteWise | AWS Storage Gateway | AWS/StorageGateway |
| Amazon EC2 | AWS/EC2 | AWS IoT Things Graph | AWS/ThingsGraph | AWS Systems Manager Run Command | AWS/SSM-RunCommand |
| Amazon EC2 Spot Fleet | AWS/EC2Spot | AWS Key Management Service | AWS/KMS | Amazon Textract | AWS/Textract |
| Amazon EC2 Auto Scaling | AWS/AutoScaling | Amazon Keyspaces (for Apache Cassandra) | AWS/Cassandra | AWS Transfer for SFTP | AWS/Transfer |
| AWS Elastic Beanstalk | AWS/ElasticBeanstalk | Amazon Kinesis Data Analytics | AWS/KinesisAnalytics | Amazon Translate | AWS/Translate |
| Amazon Elastic Block Store | AWS/EBS | Amazon Kinesis Data Firehose | AWS/Firehose | AWS Trusted Advisor | AWS/TrustedAdvisor |
| Amazon Elastic Container Service | AWS/ECS | Amazon Kinesis Data Streams | AWS/Kinesis | Amazon VPC | AWS/NATGateway |
| Amazon Elastic File System | AWS/EFS | Amazon Kinesis Video Streams | AWS/KinesisVideo | Amazon VPC | AWS/TransitGateway |
| Amazon Elastic Inference | AWS/ElasticInference | AWS Lambda | AWS/Lambda | Amazon VPC | AWS/VPN |
| Elastic Load Balancing | AWS/ApplicationELB | Amazon Lex | AWS/Lex | AWS WAF | WAF |
| Elastic Load Balancing | AWS/ELB | Amazon Machine Learning | AWS/ML | Amazon WorkMail | AWS/WorkMail |
| Elastic Load Balancing | AWS/NetworkELB | Amazon Managed Streaming for Apache Kafka | AWS/Kafka | Amazon WorkSpaces | AWS/WorkSpaces |
| Amazon Elastic Transcoder | AWS/ElasticTranscoder | Amazon MQ | AWS/AmazonMQ | | |

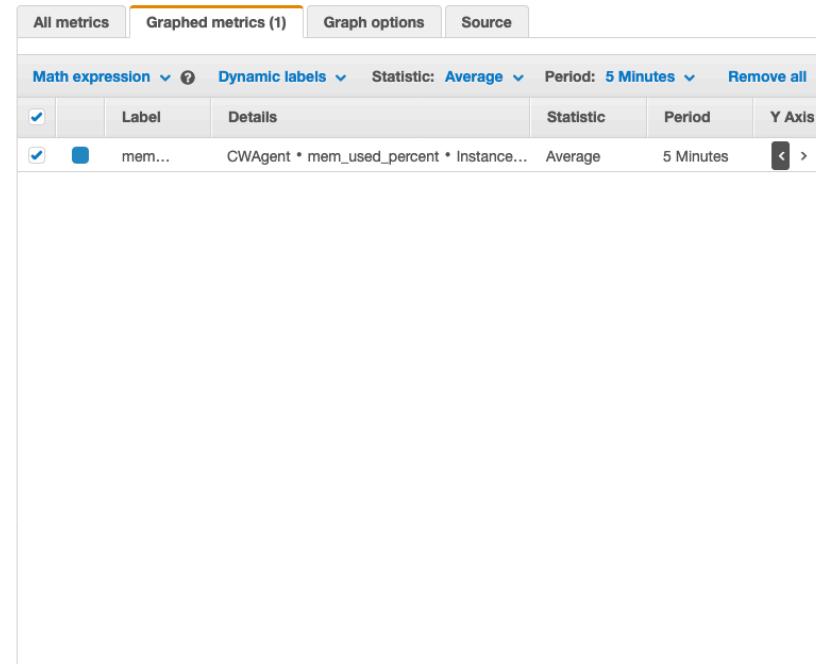
AWS Services That Publish CloudWatch Metrics:

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/aws-services-cloudwatch-metrics.html>

Custom metrics

Collect custom metrics from your own applications to monitor operational performance, troubleshoot issues, and spot trends. User activity is an example of a custom metric you can collect and monitor over a period of time.

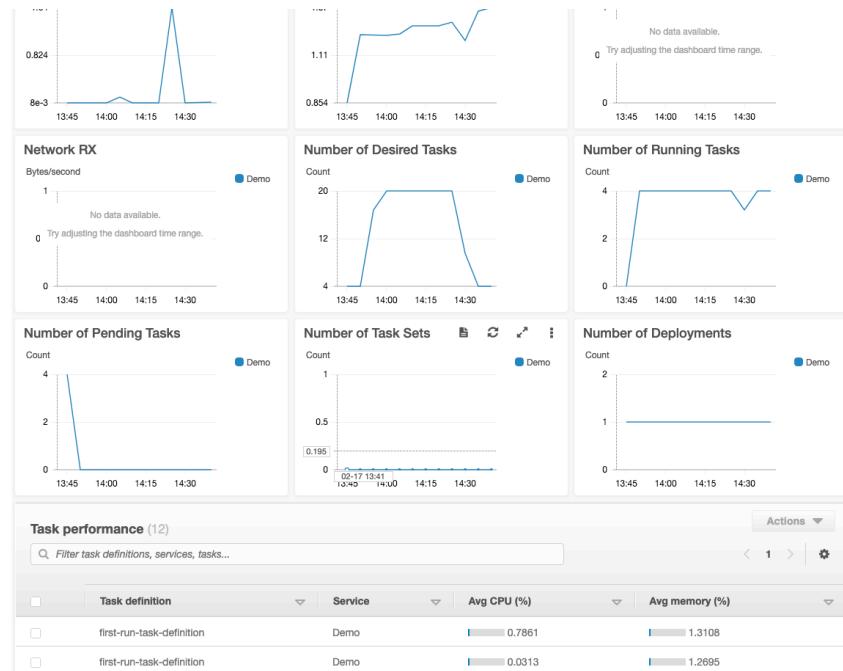
- Publish metrics using the AWS CLI or an API
- Standard resolution, with a one-minute granularity
- High resolution, with a granularity of one second
- Aggregate data before you publish to CloudWatch
- StatsD and collectd support via CloudWatch Agent



Collect and aggregate container metrics and logs

Use CloudWatch Container Insights to collect, aggregate, and summarize metrics and logs from your containerized applications and microservices.

- Collects metrics from each container
 - CPU
 - Memory
 - Disk
 - Network
- Automatically generated dashboards
- Set alarms on metrics



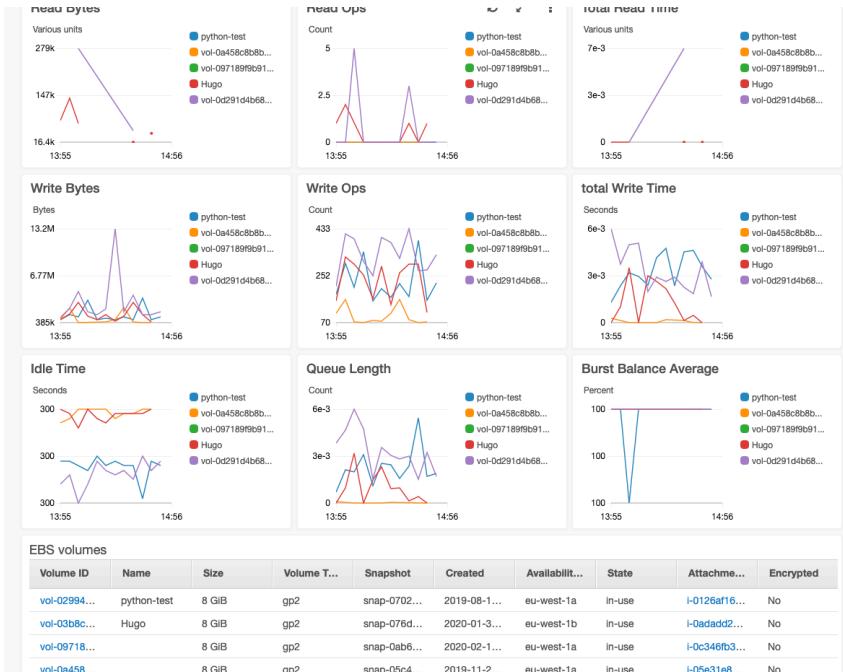
Monitor



Unified operational view with dashboards

Amazon CloudWatch dashboards enable you to create re-usable graphs and visualize your cloud resources and applications in a unified view.

- A single view for selected metrics and alarms
- Multiple AWS accounts and multiple Regions.
- An operational playbook
- A common view of critical resource and application measurements that can be shared



High resolution alarms

Amazon CloudWatch alarms allow you to set a threshold on metrics and trigger an action.

- Watch a single metric or the result of a math expression
- Perform actions based on the value of metrics
 - Send a notification to an SNS topic
 - Auto Scaling action
 - EC2 Action (Stop, Terminate, Reboot or Recover)
- Add alarms to dashboards to visualize them

| # | Name | Status | Condition | Actions |
|----|--|---|--|---------|
| 1 | ImageErrorAlarm | ⚠ In alarm | ImageError > 0 for 1 datapoints within 10 seconds | - |
| 2 | centralized-logging-StatusYellowAlarm-L8VNTMW93IP8 | 🟢 OK | ClusterStatus.yellow >= 1 for 1 datapoints within 1 minute | - |
| 3 | centralized-logging-MasterNotReachableFromNodeAlarm-12NUZCERB15HI | 🟢 OK | MasterReachableFromNode < 1 for 1 datapoints within 1 minute | - |
| 4 | centralized-logging-IndexWritesBlockedTooHighAlarm-SJ3CQWU5T2RS | 🟢 OK | ClusterIndexWritesBlocked >= 1 for 1 datapoints within 5 minutes | - |
| 5 | centralized-logging-JVMMemoryPressureToHighAlarm-145XR140EMJAP | 🟢 OK | JVMMemoryPressure >= 80 for 1 datapoints within 15 minutes | - |
| 6 | centralized-logging-MasterCPUUtilizationTooHighAlarm-VQQ5ZW5ZUVy9 | 🟢 OK | MasterCPUUtilization >= 50 for 3 datapoints within 45 minutes | - |
| 7 | centralized-logging-StatusRedAlarm-1C0JRPKQSi8GJ | 🟢 OK | ClusterStatus.red >= 1 for 1 datapoints within 1 minute | - |
| 8 | centralized-logging-MasterJVMMemoryPressureTooHighAlarm-1B2YB793W1A03 | 🟢 OK | MasterJVMMemoryPressure >= 50 for 1 datapoints within 15 minutes | - |
| 9 | centralized-logging-AutomatedSnapshotFailureTooHighAlarm-1IONHPWR16NX8 | 🟢 OK | AutomatedSnapshotFailure >= 1 for 1 datapoints within 1 minute | - |
| 10 | centralized-logging-FreeStorageSpaceToolLowAlarm-T60Q56YMGQI | 🟢 OK | FreeStorageSpace <= 2000 for 1 datapoints within 1 minute | - |

Logs and metrics correlation

Amazon CloudWatch also makes it easy to correlate metrics and logs.

- Manage logs and metrics in a single platform
- Use metric filters to convert logs to metrics

The screenshot shows the AWS CloudWatch Metrics Filter configuration interface. At the top, there's a navigation bar with 'CloudWatch' > 'CloudWatch Logs' > 'Log groups' > 'application.log'. To the right are buttons for 'Delete', 'Actions', 'Query log group', and 'View all log events'. A link 'Switch to the original interface.' is also present. Below the navigation is a section titled 'Log group details' with fields for Retention (Never expire), Creation time (5 months ago), Stored bytes (14.67 MB), and ARN (arn:aws:logs:eu-west-1:12345678910:log-group:application.log:*). There are also sections for KMS key ID, Metric filters (1), Subscriptions (LambdaStream_centralized-logging-LogStreamer-1A2RQLP14N1TW), and Contributor Insights rules. Below this, tabs for 'Log streams', 'Metric filters' (which is selected and highlighted in orange), and 'Contributor Insights' are shown. Under the 'Metric filters' tab, there's a sub-section titled 'Metric filters (1)' with a search bar 'Find metric filters'. A detailed view of the first filter is expanded, showing 'ActiveStorage-InvariableError' with a checkbox. It includes a 'Filter pattern' field containing 'ActiveStorage::InvariableError', a 'Metric' section with 'LogMetrics / ImageError', a 'Metric value' field set to '1', a 'Default value' field set to '...', and an 'Alarms' section with a link to 'ImageErrorAlarm'.

CloudWatch Metrics Example

The screenshot shows the AWS CloudWatch Log Stream interface. On the left, a sidebar menu is open under the 'Logs' section, showing various metrics and events. The main area displays a log stream titled 'SW_Log_Stream' with two entries. The first entry is a detailed JSON object representing a security alert. The second entry is a shorter JSON object representing a network notice. Both entries include fields like 'serial', 'timestamp', 'msgid', 'categoryname', 'priority', and 'message'. The interface includes a filter bar at the top and a text editor at the bottom.

CloudWatch Logs

CloudWatch > Log Groups > Sonicwall_Log_Group > SW_Log_Stream

Filter events

Message

2019-10-09 02:01:00

```
{ "serial": "C0EAE4CED0F8", "timestamp": 1570600860, "msgid": 608, "categoryname": "Security Services", "priority": "Alert", "sourceinterface": "X1", "destinationinterface": "X0", "sourceaddress": "8.8.8.8", "sourceport": 8, "destinationaddress": "192.168.171.54", "destinationport": 28162, "rxbytes": 0, "txbytes": 0, "firewallaction": "NA", "dpi": 0, "message": "IPS Detection Alert: ICMP Echo Reply, SID: 316, Priority: low" }
```

```
{ "serial": "C0EAE4CED0F8", "timestamp": 1570600882, "msgid": 36, "categoryname": "Network", "priority": "Notice", "sourceinterface": "X1", "destinationinterface": "X1", "sourceaddress": "71A 44 A 1B" }
```

CloudWatch Metrics Example

← → C console.aws.amazon.com/cloudwatch/home?region=us-east-1#metricFilterWizard:group=Sonicwall_Log_Group

aws Services Resource Groups ★

Step 1: Define Pattern

[Step 2: Assign Metric](#)

Define Logs Metric Filter

Editing Filter "message-Web-management-request-allowed-2" for Log Group "Sonicwall_Log_Group"

You can use metric filters to monitor events in a log group as they are sent to CloudWatch Logs. You can monitor and count specific terms or extract values from log events and associate the results with a metric. [Learn more about pattern syntax](#).

Filter Pattern

```
($.message="Web management request allowed")
```

[Show examples](#)

Select Log Data to Test

SW_Log_Stream [Test Pattern](#)

[Clear](#)

```
{ "serial": "C0EAE4CED0F8", "timestamp": 1560278582, "msgid": 608, "categoryname": "Security" }  
{ "serial": "C0EAE4CED0F8", "timestamp": 1560278609, "msgid": 608, "categoryname": "Security" }  
{ "serial": "C0EAE4CED0F8", "timestamp": 1560278613, "msgid": 38, "categoryname": "Network" }  
{ "serial": "C0EAE4CED0F8", "timestamp": 1560278623, "msgid": 36, "categoryname": "Network" }  
{ "serial": "C0EAE4CED0F8", "timestamp": 1560278675, "msgid": 38, "categoryname": "Network" }  
{ "serial": "C0EAE4CED0F8", "timestamp": 1560278684, "msgid": 36, "categoryname": "Network" }
```

Results

Found 4 matches out of 50 event(s) in the sample log.

[Show test results](#)

[Cancel](#) [Assign Metric](#)

CloudWatch Metrics Example

The screenshot shows the AWS CloudWatch Metrics Filter creation interface. At the top, there's a navigation bar with the AWS logo, 'Services' dropdown, 'Resource Groups' dropdown, and a bell icon. On the left, a sidebar has two items: 'Step 1: Define Pattern' (disabled) and 'Step 2: Assign Metric' (selected). The main area is titled 'Create Metric Filter and Assign a Metric'. It shows a sub-section titled 'Editing Filter "message-Web-management-request-allowed-2" for Log Group "Sonicwall_Log_Group"' with a descriptive text about log events being recorded to a metric. Below this, there are input fields for 'Filter Name' (set to 'message-Web-management-request-allowed-2') and 'Filter Pattern' (set to '\${.message="Web management request allowed"}'). Under 'Metric Details', there are fields for 'Metric Namespace' (set to 'Sonicwall') and 'Metric Name' (set to 'Log in allowed'). A link 'Show advanced metric settings' is available. At the bottom, there are buttons for 'Cancel', 'Previous', and a prominent blue 'Save Filter' button.

Step 1: Define Pattern

Step 2: Assign Metric

Create Metric Filter and Assign a Metric

Editing Filter "message-Web-management-request-allowed-2" for Log Group "Sonicwall_Log_Group"

Log events that match the pattern you define are recorded to the metric that you specify. You can graph the metric and set alarms to notify you.

Filter Name: message-Web-management-request-allowed-2

Filter Pattern: \${.message="Web management request allowed"}

Metric Details

Metric Namespace: Sonicwall i Create new namespace

Metric Name: Log in allowed i

Show advanced metric settings

Cancel Previous Save Filter

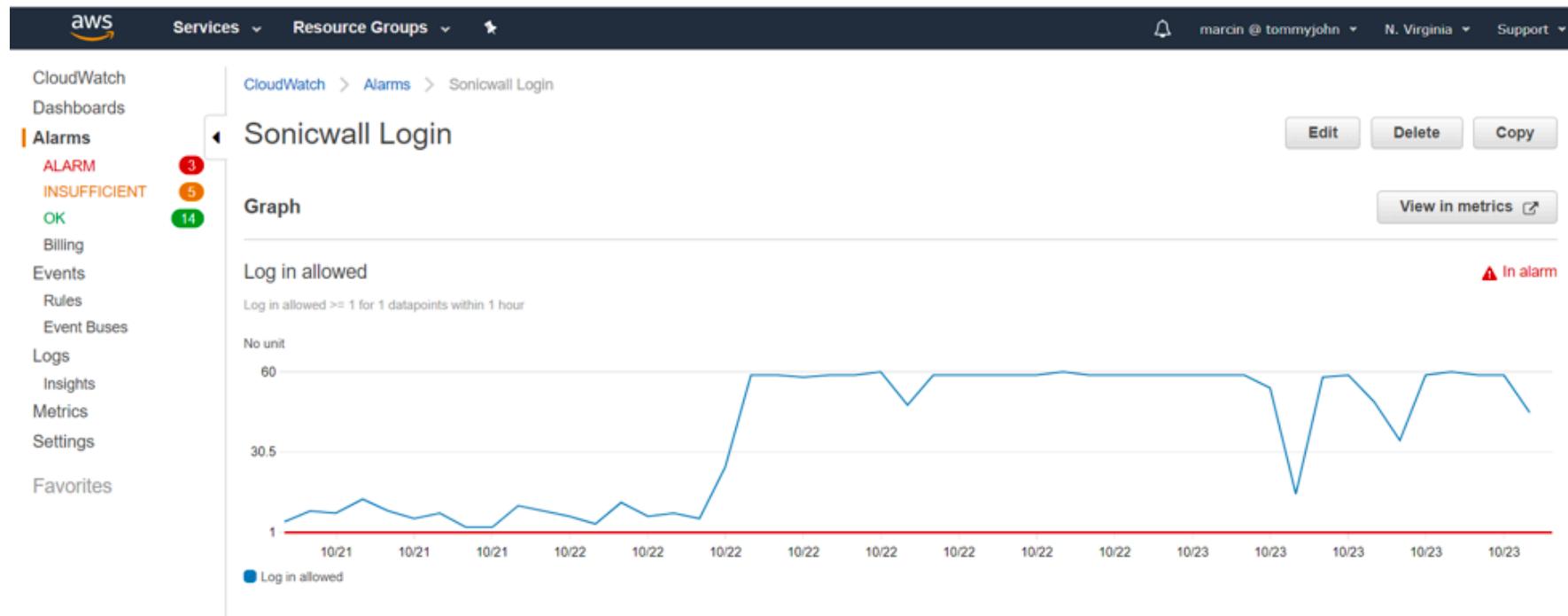
CloudWatch Metrics Example

The screenshot shows the AWS CloudWatch Metrics Filter interface. The left sidebar lists various services: CloudWatch (selected), Dashboards, Alarms, ALARM (2), INSUFFICIENT (5), OK (15), Billing, Events, Rules, Event Buses, Logs (selected), Insights, Metrics, Settings, and Favorites. The main area shows two filters under 'Filters for Sonicwall_Log_Group':

- Filter 1:** Filter Name: message-ICMP-packet-dropped-due-to-Policy. Filter Pattern: { \$.message = "ICMP packet dropped due to Policy" }. Metric: Sonicwall / Pocket Drop. Metric Value: 1. Default Value: none. Alarm: SonicWall Notifications.
- Filter 2:** Filter Name: message-Web-management-request-allowed-2. Filter Pattern: { \$.message = "Web management request allowed" }. Metric: Sonicwall / Log in allowed. Metric Value: 1. Default Value: none. Alarm: Sonicwall Login.

A red circle highlights the 'Create Alarm' button for the second filter's alarm, and a red arrow points from it towards the circled 'Create Alarm' button for the first filter's alarm.

CloudWatch Metrics Example



CloudWatch Metrics Example

ALARM: "Sonicwall Login" in US East (N. Virginia)

1 message

AWS Notifications <no-reply@sns.amazonaws.com>
To: marcin+alerts@tommyjohn.com

Wed, Oct 9, 2019 at 3:16 PM

You are receiving this email because your Amazon CloudWatch Alarm "Sonicwall Login" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [14.0 (09/10/19 18:16:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Wednesday 09 October, 2019 19:16:19 UTC".

View this alarm in the AWS Management Console:

<https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1&s=Alarms&alarm=Sonicwall%20Login>

Alarm Details:

- Name: Sonicwall Login
- Description: Someone login in to the sonicwall
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [14.0 (09/10/19 18:16:00)] was greater than or equal to the threshold (1.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Wednesday 09 October, 2019 19:16:19 UTC
- AWS Account: 353588062513

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 1.0 for 3600 seconds.

Monitored Metric:

- MetricNamespace: Sonicwall
- MetricName: Log in allowed
- Dimensions:
- Period: 3600 seconds
- Statistic: Sum
- Unit: not specified
- TreatMissingData: missing

State Change Actions:

- OK:
- ALARM: [arn:aws:sns:us-east-1:353588062513:Sonicwall-Alerts]

Application Insights for .NET and SQL Server applications

Easily monitor .NET and SQL Server applications, so you can get visibility into the health of such applications.

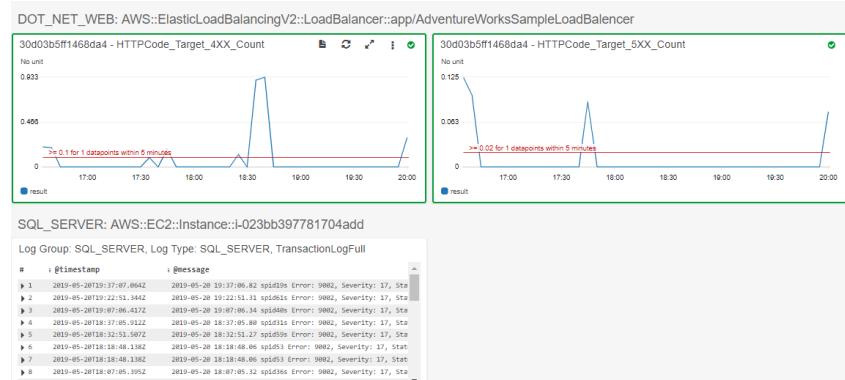
- Automatic Set Up of Monitors for Application Resources
- Problem Detection and Notification
- Automatic dashboards
- Insights that point to potential root causes

CloudWatch: Application Insights
Problem ID: p-2743c582-b59d-4364-bc76-4744aa0f3116 [Edit configuration](#)

| Severity | Problem summary | Source | Start / End time | Status | Resource group |
|----------|--------------------------|---------------------|----------------------|-------------|----------------|
| High | SQL Transaction Log Full | i-023bb397781704add | 2019-06-20T16:16:51Z | In progress | testapp2 |

Insight 0
SQL Server Engine issues a 9002 error when the transaction log is full. To make log space available, you may back up the log, free up disk space, move the log file to a disk drive with sufficient space, increase the size of the log file, or terminate a long-running transaction.

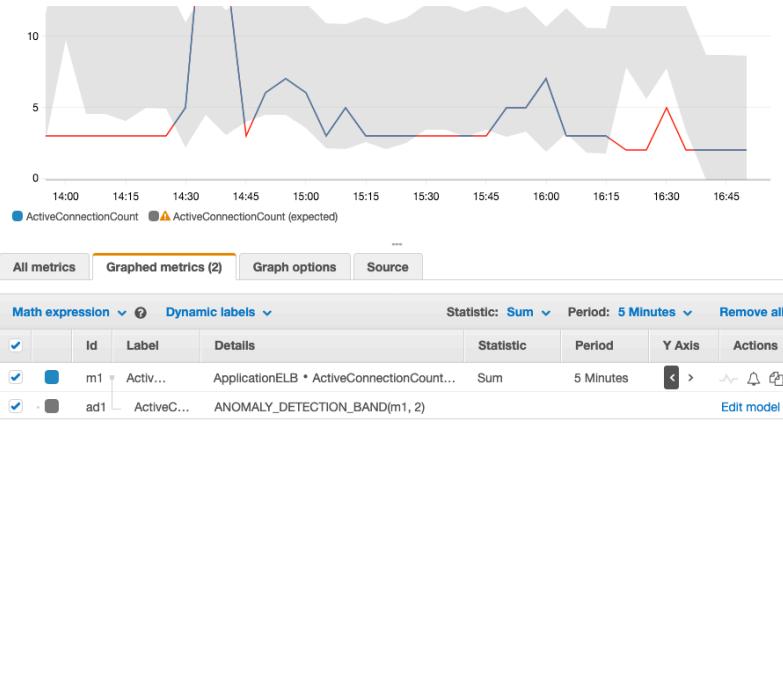
Help us improve our models: This insight is useful This insight is not useful [Submit feedback](#)



Anomaly Detection

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.

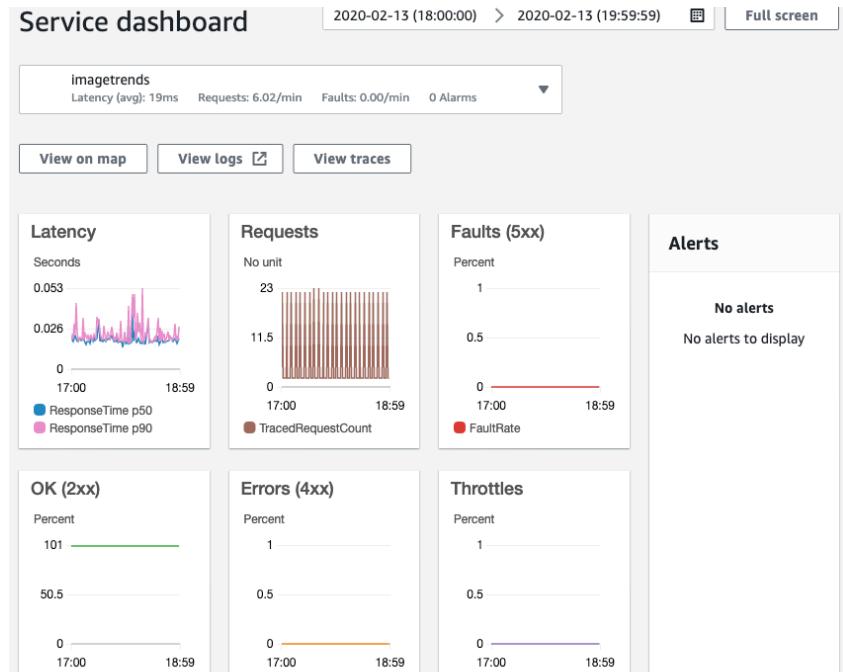
- Create alarms that auto-adjust thresholds based on natural metric patterns
- Alarm when the metric value is above or below the band, or both
- Visualize metrics with anomaly detection bands on dashboards



ServiceLens

You can use Amazon CloudWatch ServiceLens to visualize and analyze the health, performance, and availability of your applications in a single place.

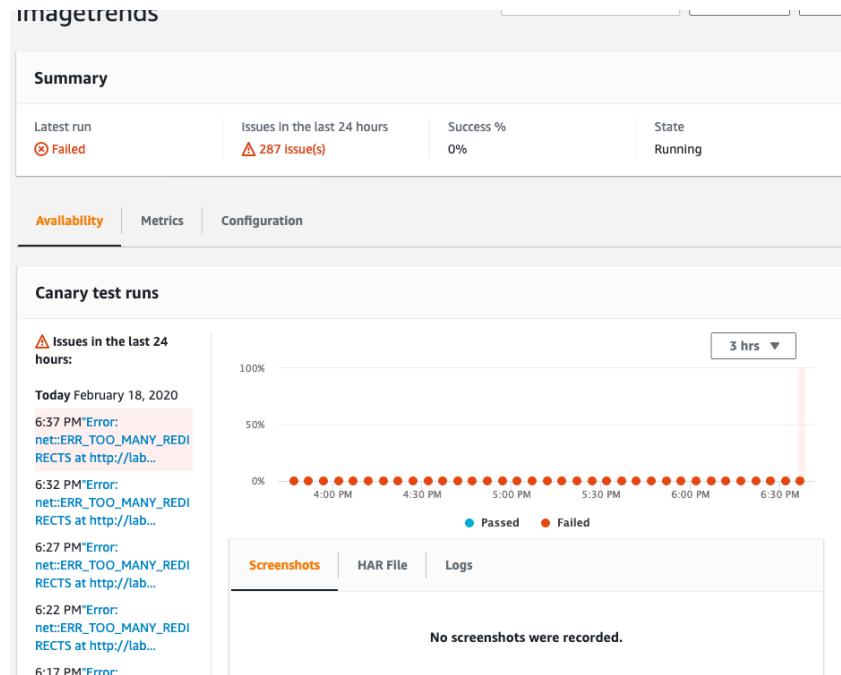
- Integrates CloudWatch with AWS X-Ray to provide an end-to-end view of your application
- A service map displays your service endpoints and resources as “nodes” and highlights the traffic, latency, and errors for each node and its connections
- You can choose a node to see detailed insights about the correlated metrics, logs, and traces associated with that part of the service



Synthetics

Run tests on your endpoints every minute, 24x7, and alerts you as soon as your application endpoints don't behave as expected.

- View of your customers' experiences
- Configurable scripts
- Run once
- Run on a schedule
- Check availability and latency
- Store load time data
- Store screenshots



Act



Auto Scaling

Auto Scaling helps you automate capacity and resource planning.

- Set a threshold to alarm on a key metric and trigger an automated Auto Scaling action
- For example, you could set up an Auto Scaling workflow based on queue depth
- Configure policies to scale in or scale out
- Allows you to set 1 scaling policy and trigger with multiple alarms

Auto Scaling action

Alarm state trigger
Define the alarm state that will trigger this action.

In alarm
The metric or expression is outside of the defined threshold.

OK
The metric or expression is within the defined threshold.

Insufficient data
The alarm has just started or not enough data is available.

Remove

Resource type
Select a resource type.

EC2 Auto Scaling group

ECS Service

Select a group

Lab-ASG-GK90F1O9AQP9-AppAutoScalingGro... ▾

Only Auto Scaling groups with a simple scaling or step scaling policy in this account are available.

Take the following action...

Test (Add 1 Instance) ▾

Only actions for the selected Auto Scaling group are available.

Add new Auto Scaling action

Automate response to changes with CloudWatch Events

CloudWatch Events provides a near real-time stream of system events that describe changes to your AWS resources.

- Respond quickly
- Take corrective action

Write rules to indicate which events are of interest to your application and what automated actions to take when a rule matches an event.

- Invoke a Lambda Function
- Notify an SNS Topic
- Create an Ops Item in Systems Manager

The screenshot shows the AWS CloudWatch Events Rule configuration interface. It includes sections for triggers, targets, and monitoring.

Triggers:

- Next 10 trigger Date(s):
 - 1. Fri, 28 Feb 2020 06:00:00 GMT
 - 2. Fri, 27 Mar 2020 06:00:00 GMT
 - 3. Fri, 24 Apr 2020 06:00:00 GMT
 - 4. Fri, 29 May 2020 06:00:00 GMT
 - 5. Fri, 26 Jun 2020 06:00:00 GMT
 - 6. Fri, 31 Jul 2020 06:00:00 GMT
 - 7. Fri, 28 Aug 2020 06:00:00 GMT
 - 8. Fri, 25 Sep 2020 06:00:00 GMT
 - 9. Fri, 30 Oct 2020 06:00:00 GMT
 - 10. Fri, 27 Nov 2020 06:00:00 GMT
- Status: Enabled

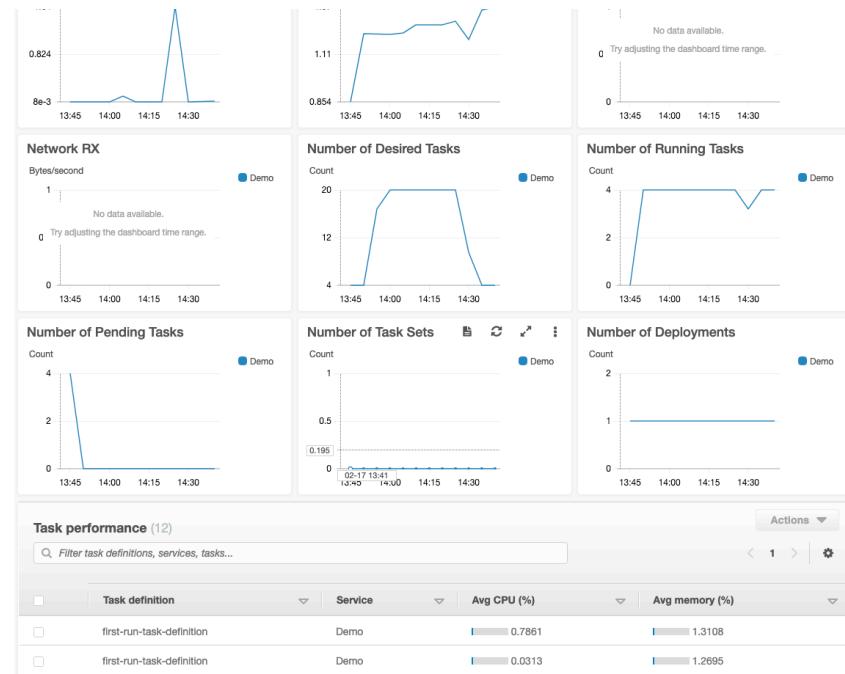
Description: Monitoring [Show metrics for the rule](#)

Targets:

| Type | Name | Input |
|----------------|---|--|
| SSM Automation | ChangeInstanceState (version \$DEFAULT) | Constant: {"InstanceId": ["i-0cb0104ddf22a..."]} |

Alarm and automate actions on EKS, ECS, and k8s clusters

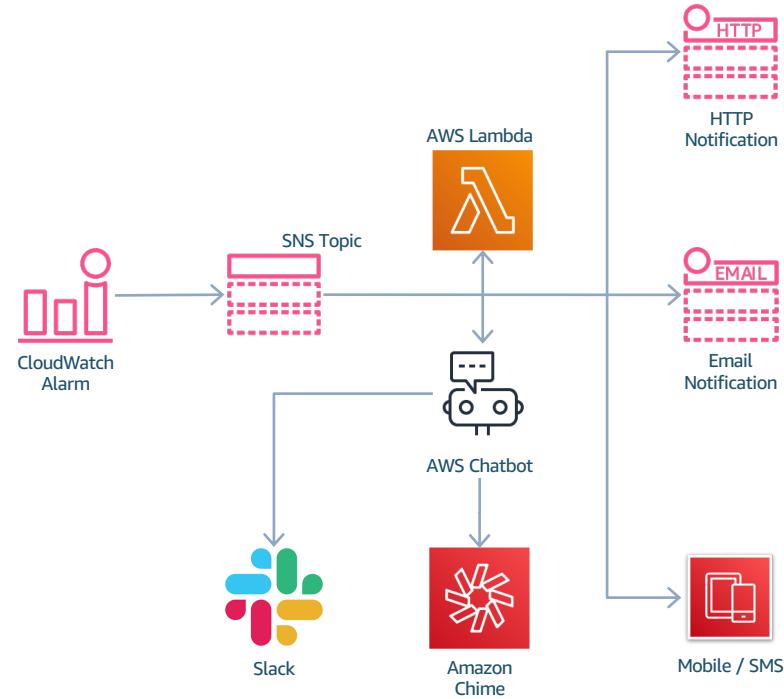
For Amazon EKS and k8s clusters, Container Insights allows you to alarm on compute metrics to trigger auto scaling policies on your Amazon EC2 Auto Scaling group and provides you the ability to stop, terminate, reboot, and recover any Amazon EC2 instance.



Automation

CloudWatch Alarms can send a notification to SNS, from there, you can trigger a Lambda function or push a message to Slack or Amazon Chime via AWS Chatbot. This allows you to do almost anything, including:

- Trigger a Systems Manager Automation
- Resize an instance
- Send a message to Chime or Slack
 - Respond with CLI commands
- Invoke disaster recovery
- Update security groups
- Automate deployments
- Instigate backups and snapshots
- Responding to security events



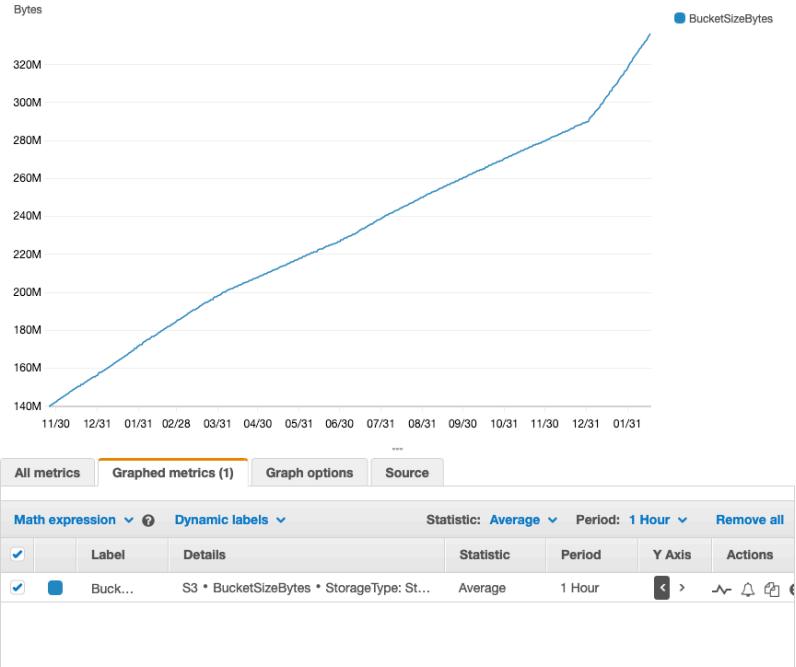
Analyze



Granular data and extended retention

Amazon CloudWatch allows you to monitor trends and seasonality with 15 months of metric data (storage and retention).

- Historical analysis to fine-tune resource utilization
- Collect metrics with a granularity of 1 second
- Granular real-time data enables better visualization
- Spot and monitor trends to optimize applications



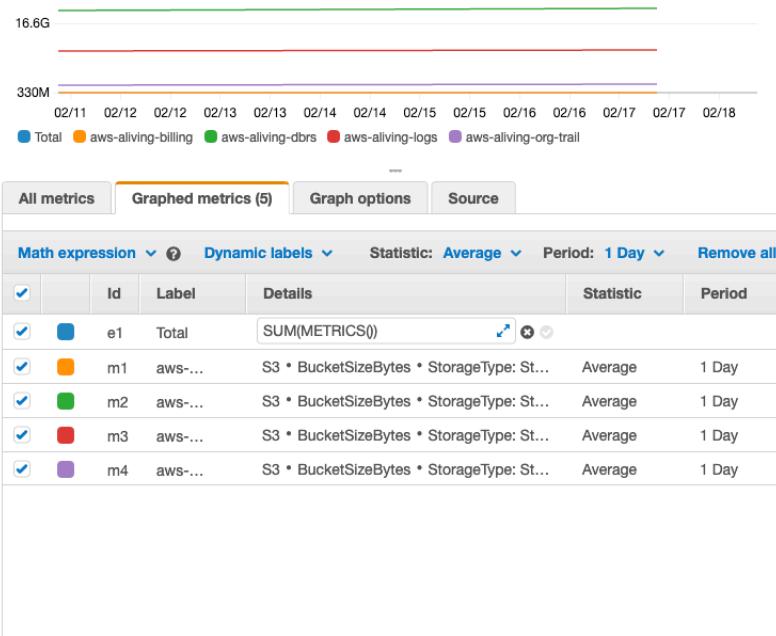
Custom operations on metrics

Metric Math enables you to perform calculations across multiple metrics for real-time analysis.

- Visualize computed metrics in the Console
- Add them to CloudWatch dashboards
- Retrieve them using the GetMetricData API action

Metric Math supports arithmetic operations such as +, -, /, *, and mathematical functions such as Sum, Average, Min, Max, and Standard Deviation.

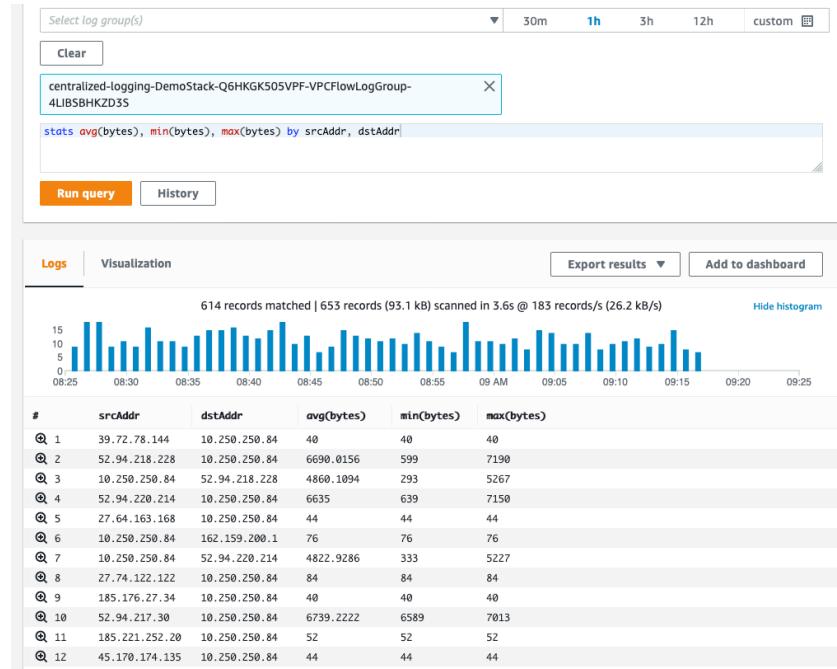
Using AWS Lambda metrics as an example, you could divide the Errors metric by the Invocations metric to get an error rate.



Log analytics

CloudWatch Logs Insights enables you to drive actionable intelligence from your logs to address operational issues without needing to provision servers or manage software.

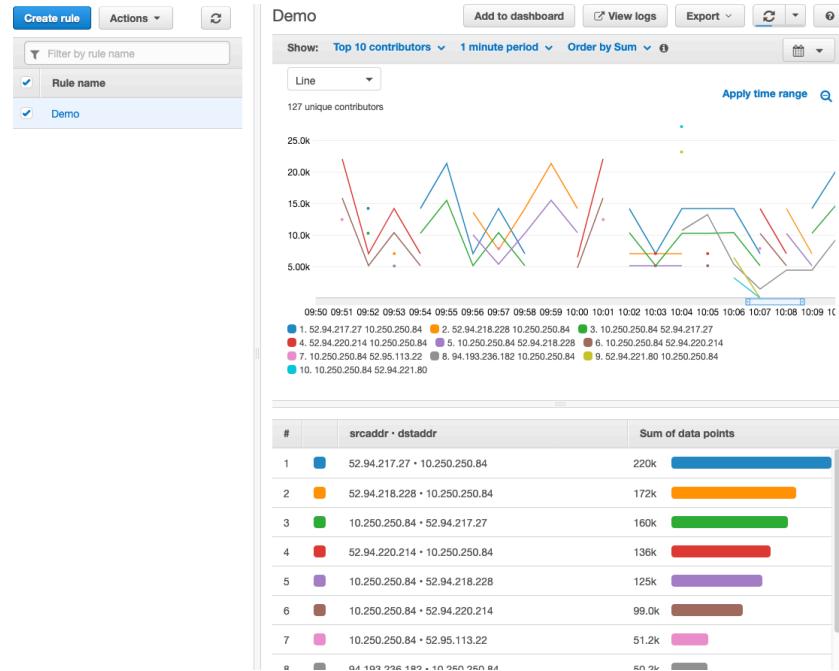
- You can instantly begin writing queries with aggregations, filters, and regular expressions
- In addition, you can:
 - Visualize timeseries data
 - Drill down into individual log events
 - Export query results to CloudWatch Dashboards
- You only pay for the queries you run



Contributor Insights

Analyzes time-series data to provide a view of the top contributors influencing system performance.

- Runs continuously without needing user intervention
- Understand who or what is impacting your system
- Evaluate patterns in structured log events
- Display on CloudWatch dashboards
- Add to CloudWatch alarms



CloudTrail



CloudTrail

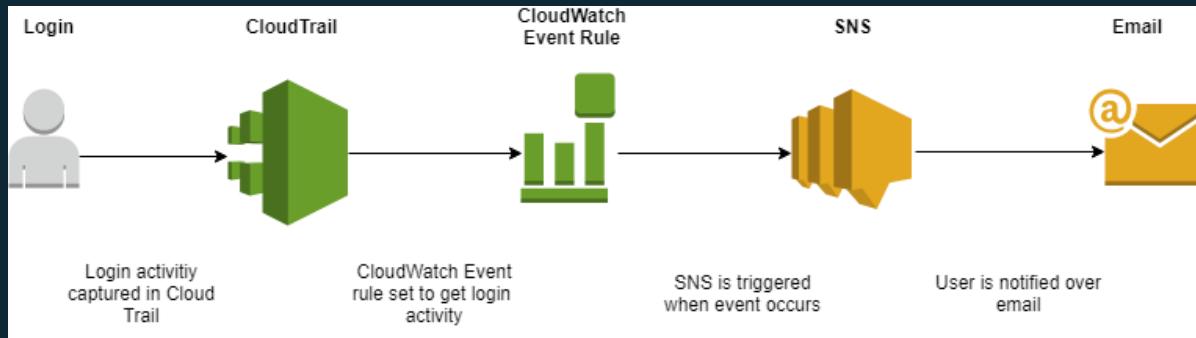
- By **default**, CloudTrail is configured to store 90 days of event history
- Logs API calls (ie. Console, CLI, API, SDK)
- You can view entries in the **Event History**
- A Trail is how you configure CloudTrail to deliver to S3
 - Can be for a single region or multiple regions

CloudTrail – Configuration options

- **Management Events** – Control plane events:
 - User login events
 - Configuring Security
 - Setting up logging
- **Data Events**
 - Object-level events in S3 (GetObject, PutObject)
 - Function-level events in Lambda (Invocation API functions)
- **Encryption**
 - Encrypted in S3 server-side by default, can be changed to KMS.
- **Organizations**
 - Can create Trail for an Organization
 - Inherits to sub-accounts

CloudTrail – CloudWatch Logs integration

- You can configure CloudTrail to deliver logs to CloudWatch Logs
- In an Organization, each account would have its own Log Stream
- You can create Metric Filters from CloudTrail Logs



Systems Manager

AWS Systems Manager Capabilities



Resource Groups



Patch Manager



State Manager



Run Command



Automation



Maintenance Window



Inventory



Parameter Store



Session Manager

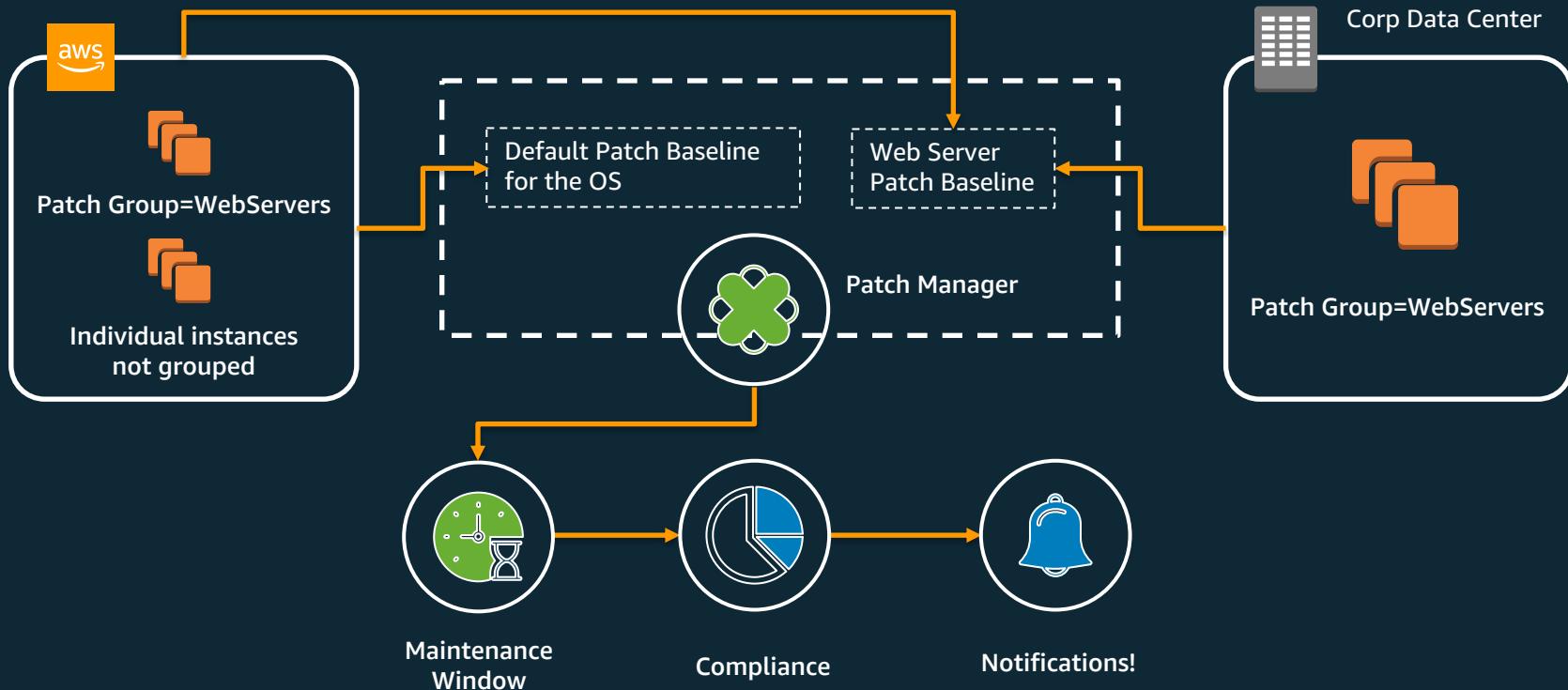


Distributor

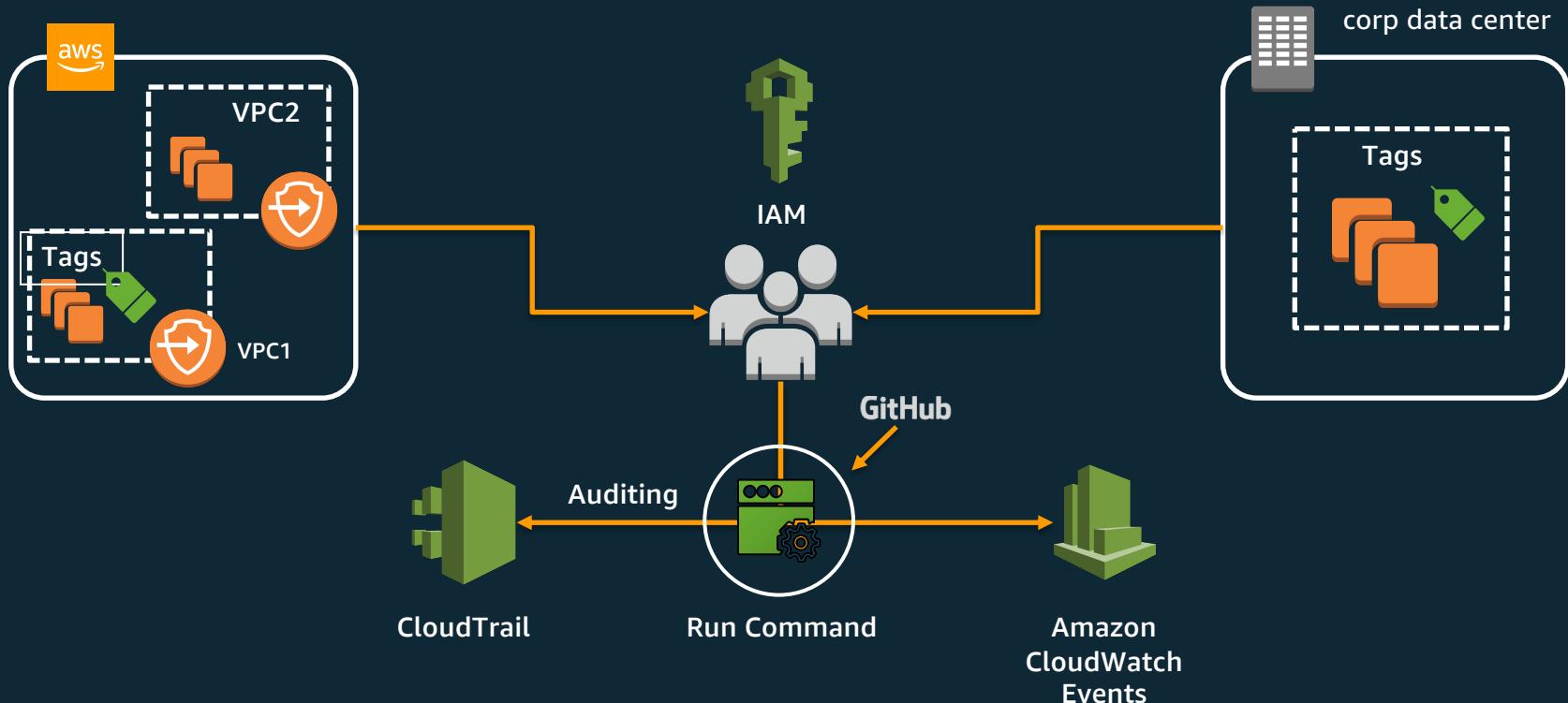


OpsCenter

Compliance with Patch Manager



Safe and Secure Operations



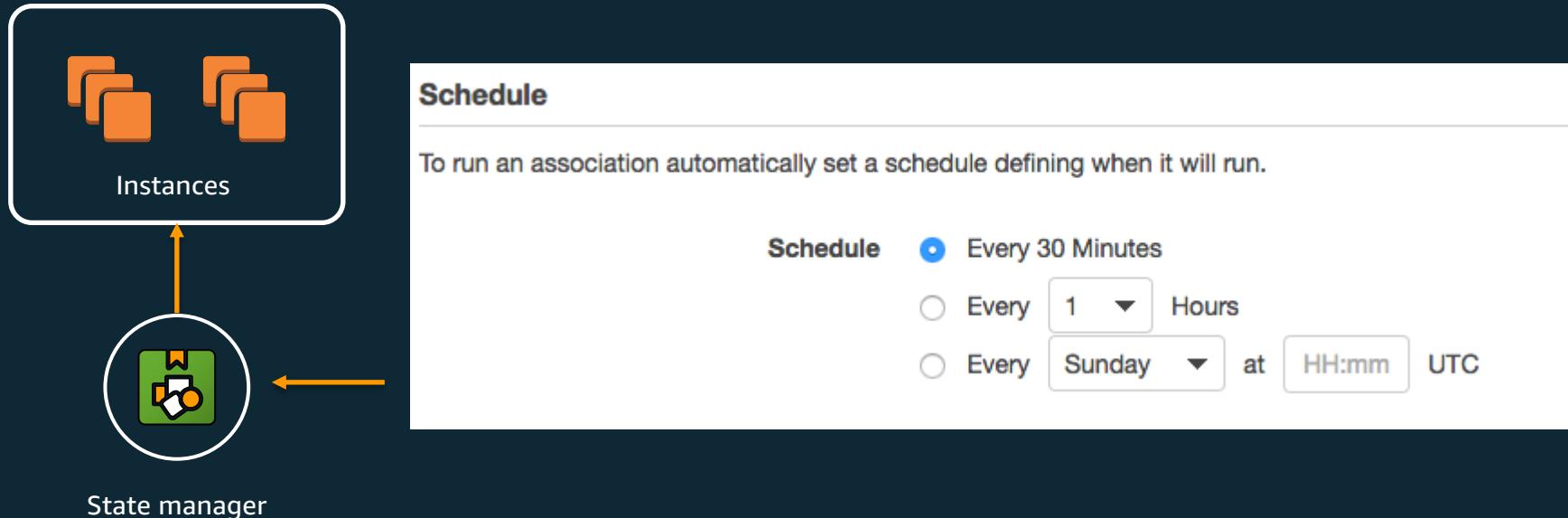
Systems Manager State Manager

Automates the process of keeping your Amazon EC2 and hybrid infrastructure in a state that you define.

One of the use case I found out of AWS System Manager State Manager is to run the command on a scheduled basis(eg: SnapShot Creation)

Manage Configuration Drift with State Manager

State Manager automates the process of keeping your Amazon EC2 and hybrid infrastructure in a state that you define.



Systems Manager Parameter Store

- Provides secure, hierarchical storage for configuration data management and secrets management. We can store data such as,
 - passwords
 - database strings
 - license codes
- Which we can then be programmatically accessed via the SSM API.
- Free

Creating a parameter from the Console

AWS Systems Manager > Parameter store > Create parameter

Parameter details

Name X

Description- *Optional*

Type
 String Any string value.
 StringList Separate strings using commas.
 SecureString Encrypt sensitive data using the KMS keys for your account.

Value Maximum length 4096 characters.

Tags

No tags associated with the resource

Add tag

Retrieving a parameter from the CLI

```
$ aws ssm get-parameters --names "testpass"
```

```
{  
  "InvalidParameters": [],  
  "Parameters": [  
    {  
      "Name": "testpass",  
      "LastModifiedDate": 1552923749.085,  
      "Value": "test123",  
      "Version": 1,  
      "Type": "String",  
      "ARN": "arn:aws:ssm:us-west-2:xxxxxxx:parameter/testpass"  
    }  
  ]  
}
```

Parameter Store SecureString

- Any sensitive data that needs to be stored and referenced in a secure manner. If you have data that you don't want users to alter or reference in plain text, such as passwords or license keys, create those parameters using the SecureString datatype.
- Recommend using SecureString parameters for the following scenarios.
 - You want to use data/parameters across AWS services **without exposing the values as plain text in commands, functions, agent logs, or AWS CloudTrail logs**.
 - You want to **control who has access** to sensitive data.
 - You want to be able to **audit** when sensitive data is accessed (AWS CloudTrail).
 - You want to **encrypt** your sensitive data and you want to **bring your own encryption keys** to manage access.

CloudFormation

CloudFormation

Expect questions about CloudFormation on the test

Understand:

- Stack Updates
- Stack Sets – create stacks in multiple accounts
- Nested Stack – stacks created by other stacks (reusable patterns, standardization)
- Drift Detection – detects whether a stack's actual configuration differs from the expected configuration.
- Custom Resources

CloudFormation for Disaster Recovery

CloudFormation (Infrastructure as code) can be used as part of a DR strategy to spin up resources quickly in the event of a disaster.

- Create infrastructure when needed
- Scale up pilot light resources

Homework – Scheduled your Exam!

- Work with your Training contact (Kala Srikanth) to request voucher
- Note that certifications are currently available in online-proctored mode.
 - Quite place, reliable device, webcam, reliable internet
- Be aware of ESL +30min accommodations
 - https://www.certmetrics.com/amazon/candidate/exam_scheduling.aspx