# Monitoring & Autoscaling

DE HOGESCHOOL MET HET NETWERK

Elfde-Liniestraat 24, 3500 Hasselt, www.pxl.be

# Quick recap

Dictionary

Search for a word

monitor
/ˈmɒnɪtə/

See definitions in:

All | Intelligence | Broadcasting | Electronics

*verb*

gerund or present participle: **monitoring**

observe and check the progress or quality of (something) over a period of time; keep under systematic review.
"equipment was installed to monitor air quality"

Similar: observe | watch | keep an eye on | keep track of | track

- maintain regular surveillance over.
  "he was a man of routine and it was easy for an enemy to monitor his movements"
- listen to and report on (a foreign radio broadcast or a phone conversation).
  "listening devices were used to monitor conversations"

Definitions from Oxford Languages *Feedback*

Translations and more definitions

Dictionary

Search for a word

metric[1]
/ˈmetrɪk/

See definitions in:

All | Commerce | Mathematics | Physics | Prosody

*noun*

plural noun: **metrics**

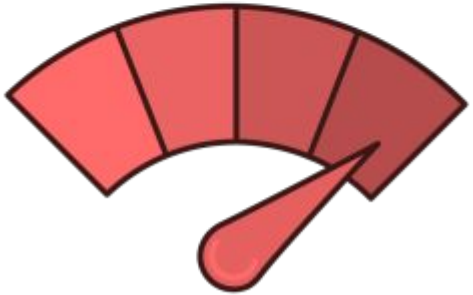
1. TECHNICAL
   a system or standard of measurement.
   "the levels of branching are arbitrary and no precise metric is applied to distance between the
2. INFORMAL
   the metric system.
   "it's easier to work in metric"

Definitions from Oxford Languages *Fe*

Translations and more definitions

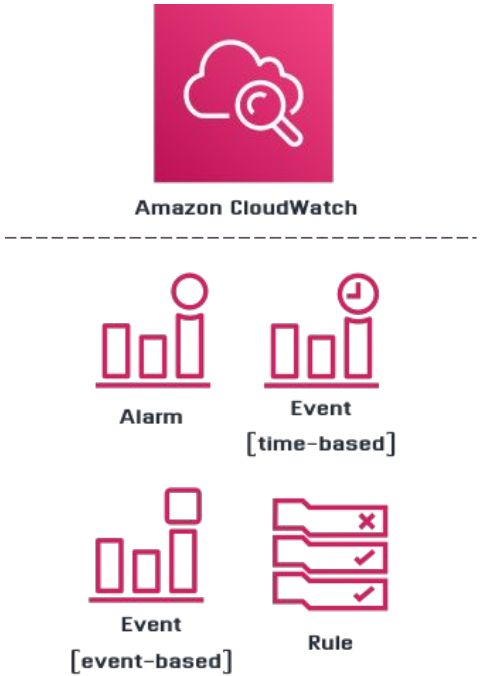
# “Basic” Monitoring in AWS

**Amazon CloudWatch**



- **Monitors**
  - AWS resources
  - Applications that run on AWS
- **Collects and tracks**
  - Standard metrics
  - Custom metrics
- **Alarms**
  - Send notifications to an Amazon SNS topic
  - Perform Amazon EC2 Auto Scaling or Amazon EC2 actions
- **Events**
  - Define rules to match changes in AWS environment and route these events to one or more target functions or streams for processing

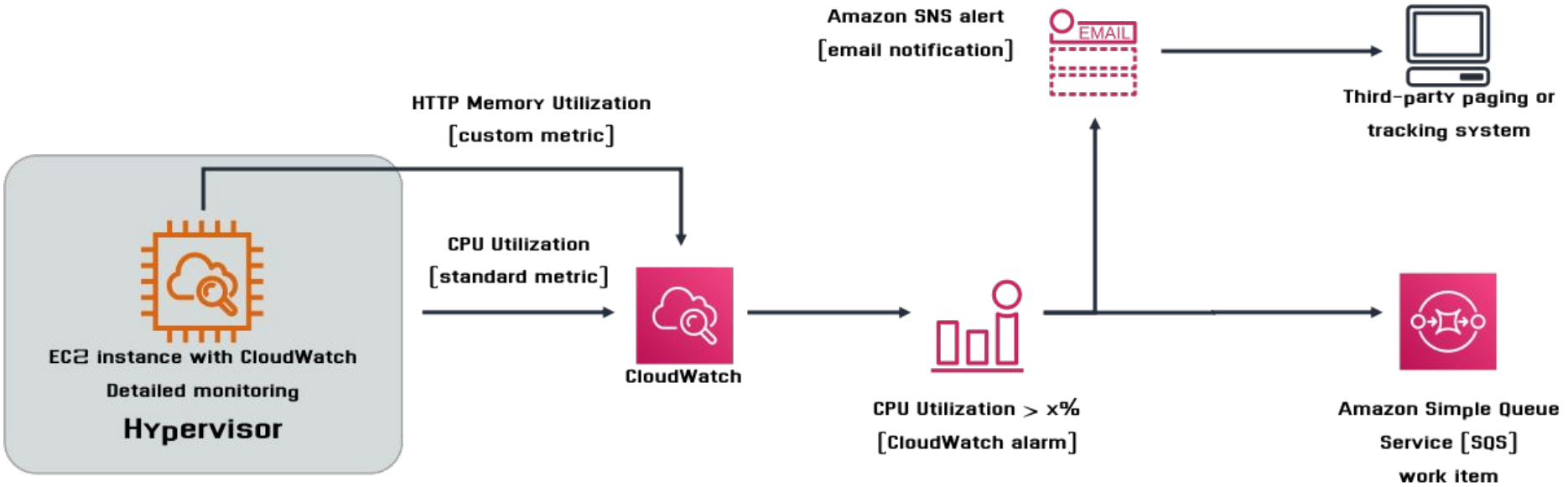
# Monitoring metrics




**Amazon CloudWatch**

- Monitors the state and utilization of most of the resources that you are managing under AWS
- Key concepts:
  - Standard metrics
  - Custom metrics
  - Alarms
  - Notifications
- **CloudWatch Agent** to collect system-level metrics:
  - Amazon EC2 instances
  - On-premises servers
- **Tiers**
  - Basic monitoring (free tier) provides metrics every 5 minutes
  - Detailed monitoring provides metrics every minute

# Cloudwatch monitoring example



# Metric specifics

| | |
|---|---|
| Metric | Name and Value |
| Namespace | Group related metrics together |
| Dimensions | Name-value pairs that further categorize metrics |
| | Example: **InstanceId** a dimension of **CPUUtilization** |
| | Metric Name + Dimension = a new, unique metric |
| Period | Specified time (in seconds) over which metric was collected |

# Metric specifics

**Namespace:**

**Groups related metrics together**

```
{
   "Metrics": [
      {
         "Namespace": "AWS/S3",
         "Dimensions": [
            {
               "Name“: "StorageType",
               "Value": "GlacierStorage"
            },
            {
               "Name": "BucketName",
               "Value": "mybucket"
            }
         ],
         "MetricName": "BucketSizeBytes"
      }
   ]
}
```

# Standard & Custom Metrics

**Standard metrics:**

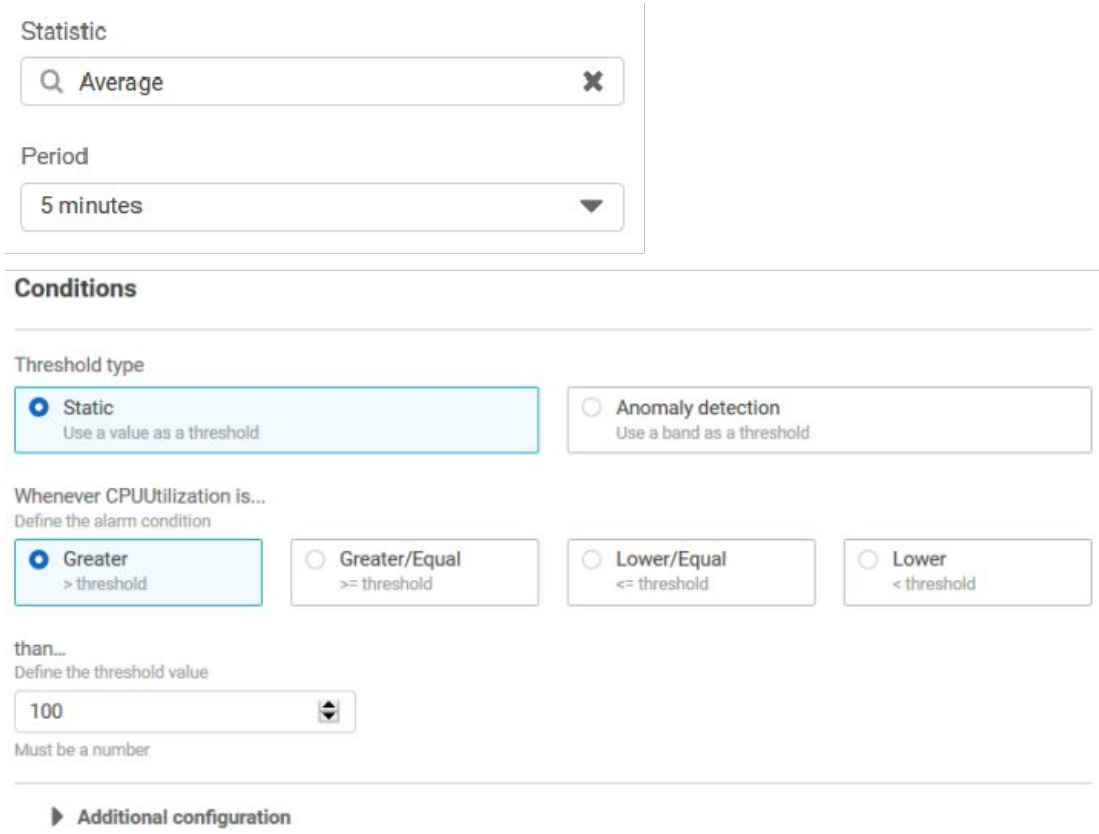
- Grouped by service name
- Display graphically so selected metrics can be compared
- Only appear if you have used the service within the past 15 months
- Reachable programmatically through AWS CLI or application programming interface (API)

**Custom metrics:**

- Grouped by user-defined namespace
- Publish to CloudWatch using AWS CLI, API, or CloudWatch Agent

# Cloudwatch Alarms

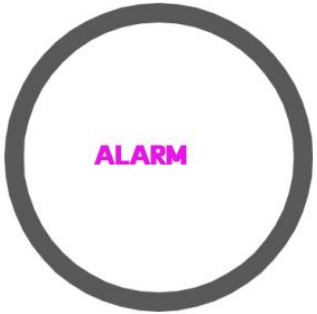
- **Create alarms based on**
  - Static threshold
  - Anomaly detection
  - Metric math expression
- **Specify**
  - Namespace
  - Metric
  - Statistic
  - Period
  - Conditions
  - Additional configuration
  - Actions



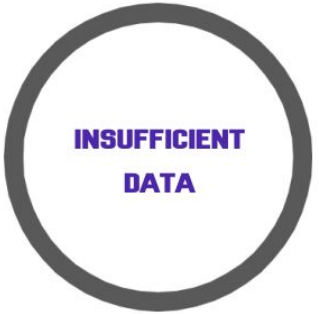
# Cloudwatch Alarms

**Alarms have three possible states:**


Threshold *not* exceeded



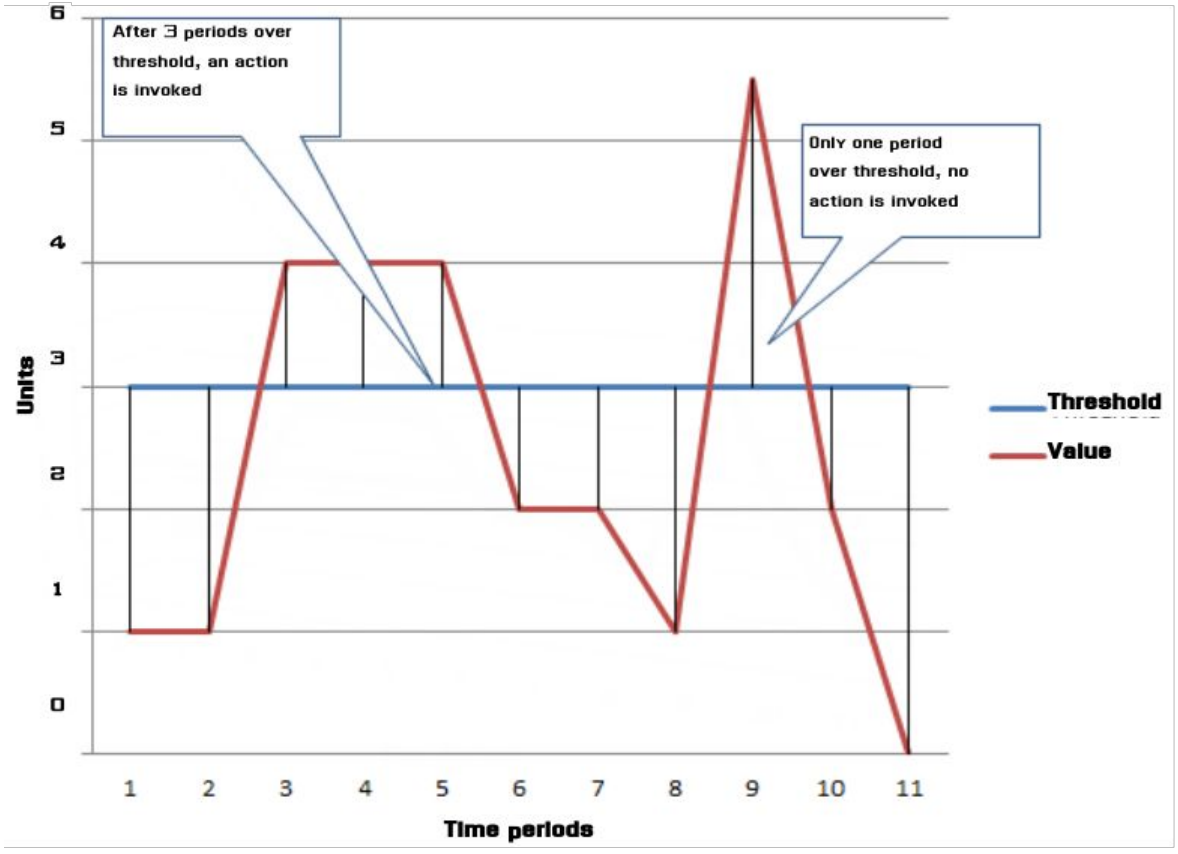

Threshold exceeded



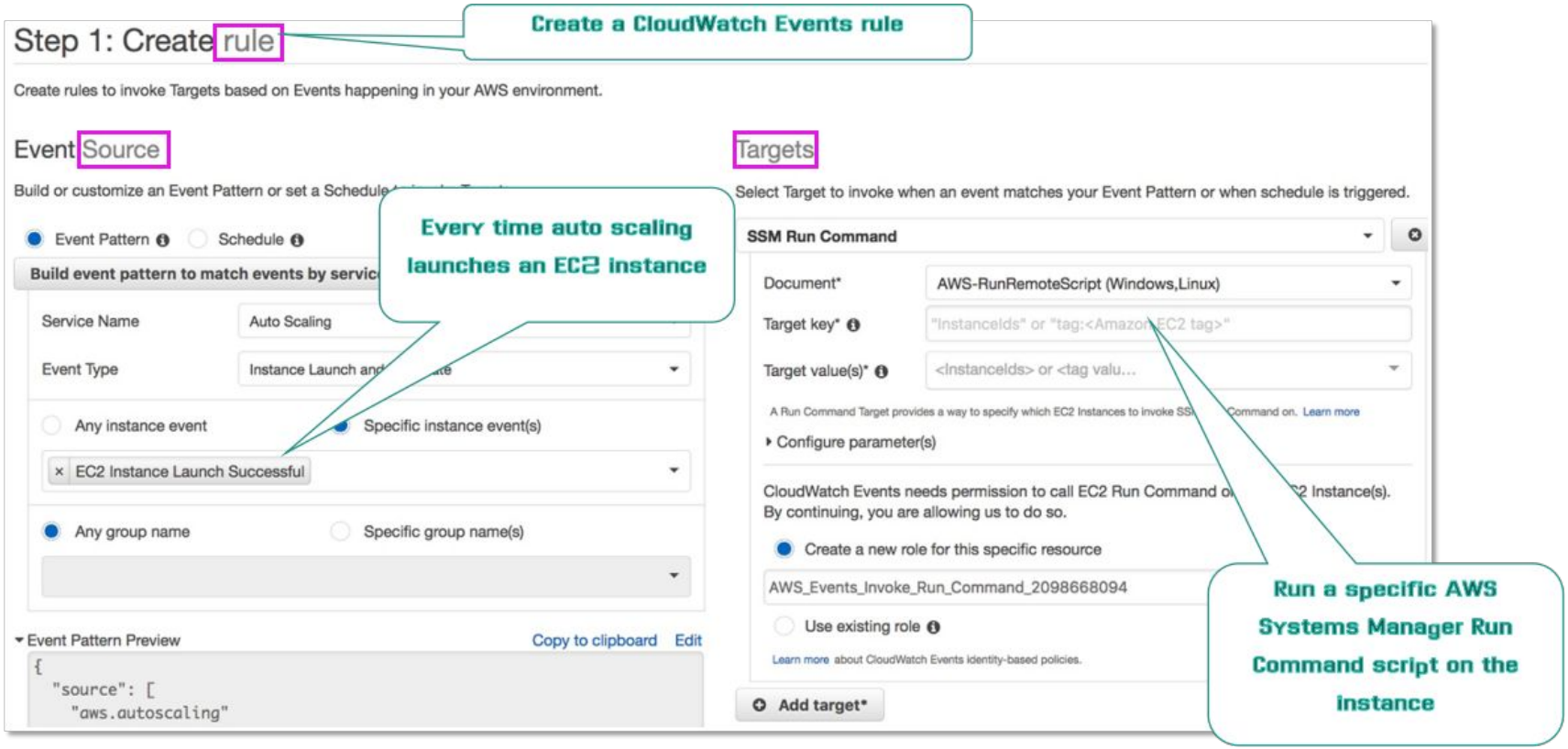

Alarm has just started, metric not available, or insufficient data

- Test a selected metric against a specific threshold [greater than or equal to, less than or equal to]
- The ALARM state is not necessarily an emergency condition

# CloudWatch Alarms example



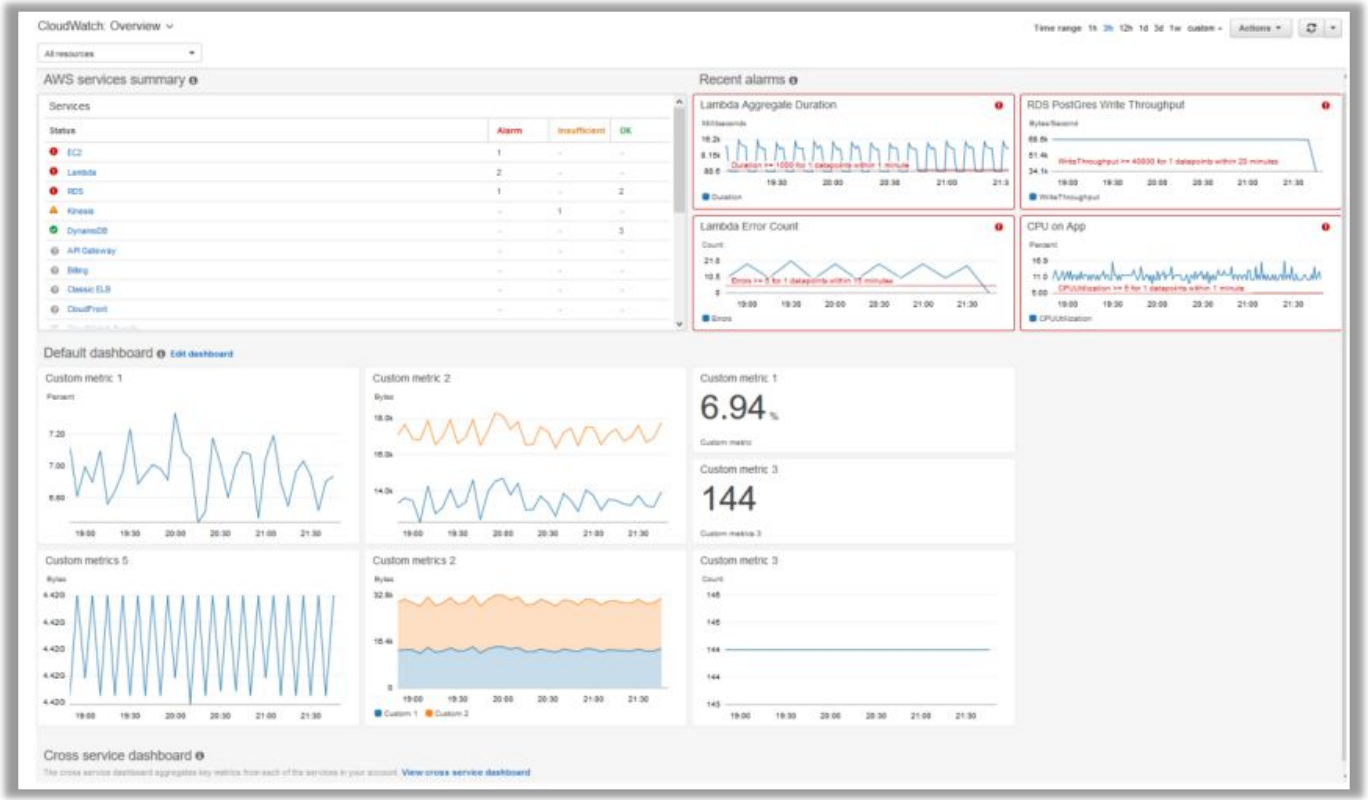
# Cloudwatch Events



# CloudWatch automatic dashboards

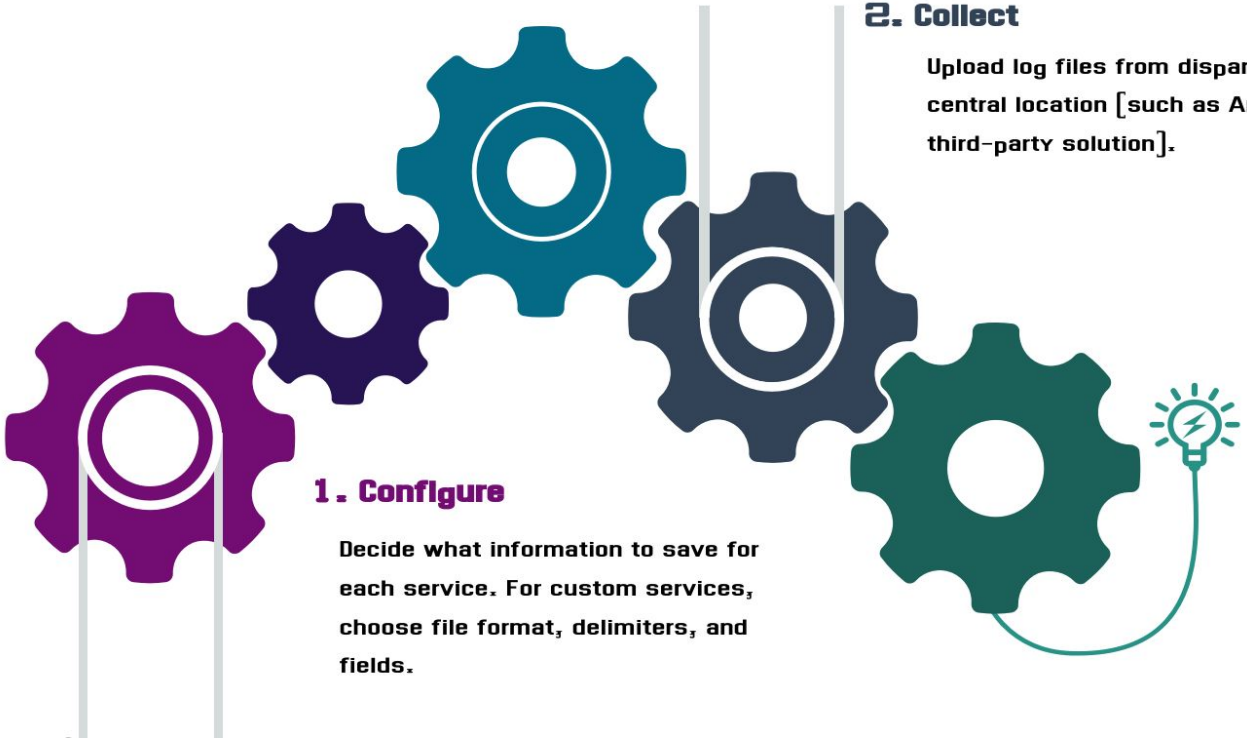
**Amazon CloudWatch dashboards:**

- Surface data about your running AWS ecosystem.
- Can be leveraged by existing monitoring tools.



# Amazon CloudWatch Logs

## Typical log analysis process



### 1. Configure

Decide what information to save for each service. For custom services, choose file format, delimiters, and fields.

### 2. Collect

Upload log files from disparate cloud resources into a central location (such as Amazon S3, Amazon EMR, or a third-party solution).

### 3. Analyze

Examine your data using analytics tools (like CloudWatch Log Insights) to report on errors, investigate problem reports, monitor new releases, and measure trends.

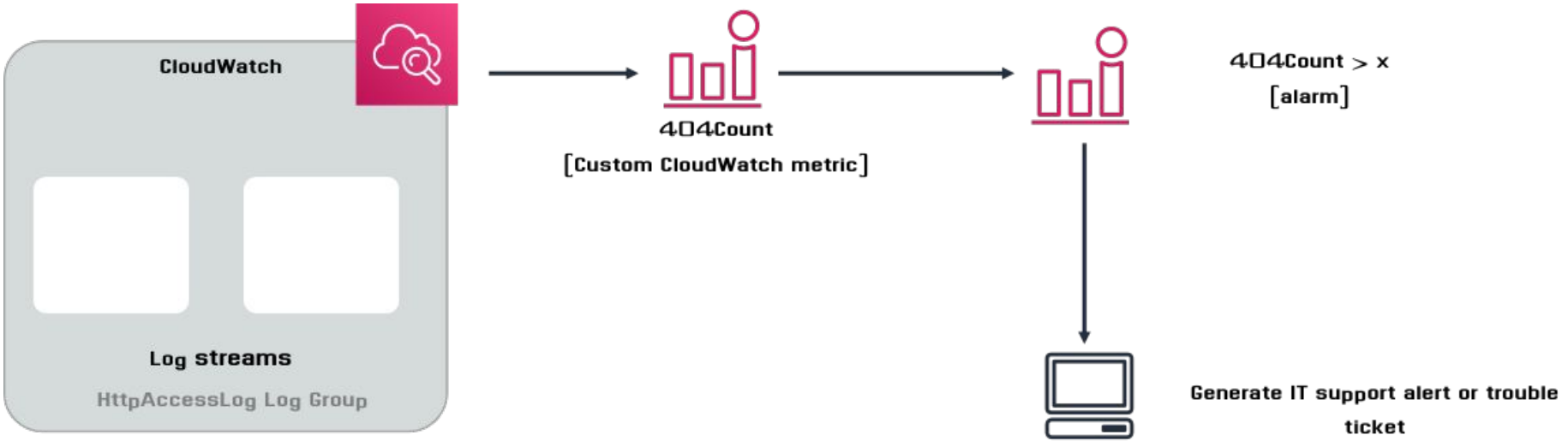
# Amazon CloudWatch Logs

PXL DIGITAL

**CloudWatch Logs** functionality includes:

- Automatically collecting logs (for example, from EC2 instances)
- Aggregating data into *log groups*
- Having the ability to configure *metric filters* on a log group:
  - Look for specific string patterns
  - Have each match increment a custom CloudWatch metric
  - Use the metric to create CloudWatch alarms or send notifications
- Querying logs and creating visualizations with **CloudWatch Logs Insights**

# Create CloudWatch alarms on log filter metrics



# Typical log formats

**Example:**

Apache httpd logs configured using a substitution string in httpd.conf

```
LogFormat "%h %l %u %t \“%r\" %>s %b" common
```

**Result:**

A space-delimited string containing information on each HTTP/HTTPS request

```
127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700] "GET /apache_pb.gif
HTTP/1.0" 200 2326
```

# Amazon CloudWatch filter patterns

**Filter patterns:**

- Case-sensitive
- Multiple terms allowed in a metrics filter pattern (however, all terms must appear in the log event to be a match)

**Example:**

Create a metric for all results with the string html anywhere in the request, and any HTTP 400-series (client) error

```
[ip, user, username, timestamp, request = *html*, status_code = 4*, bytes]
```

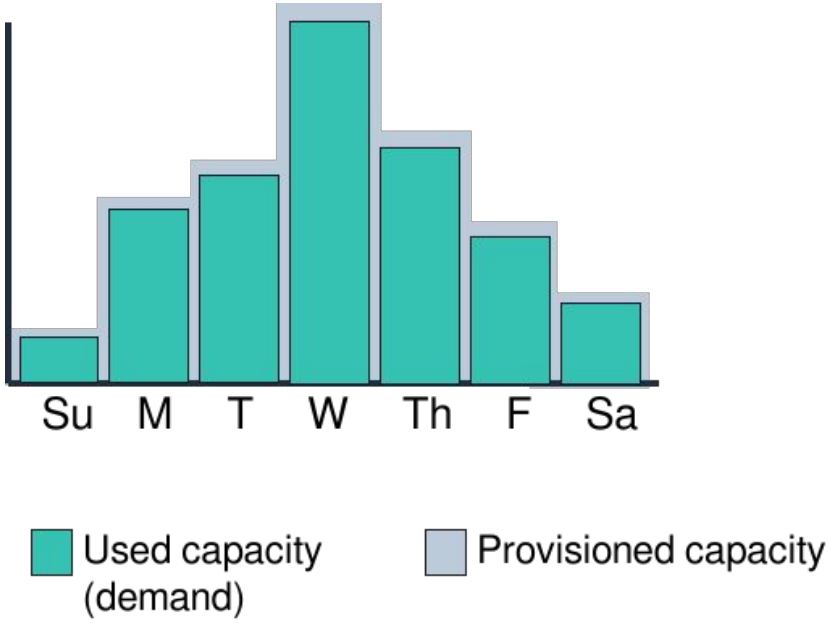
# AWS CloudTrail

**AWS CloudTrail**, a service that:

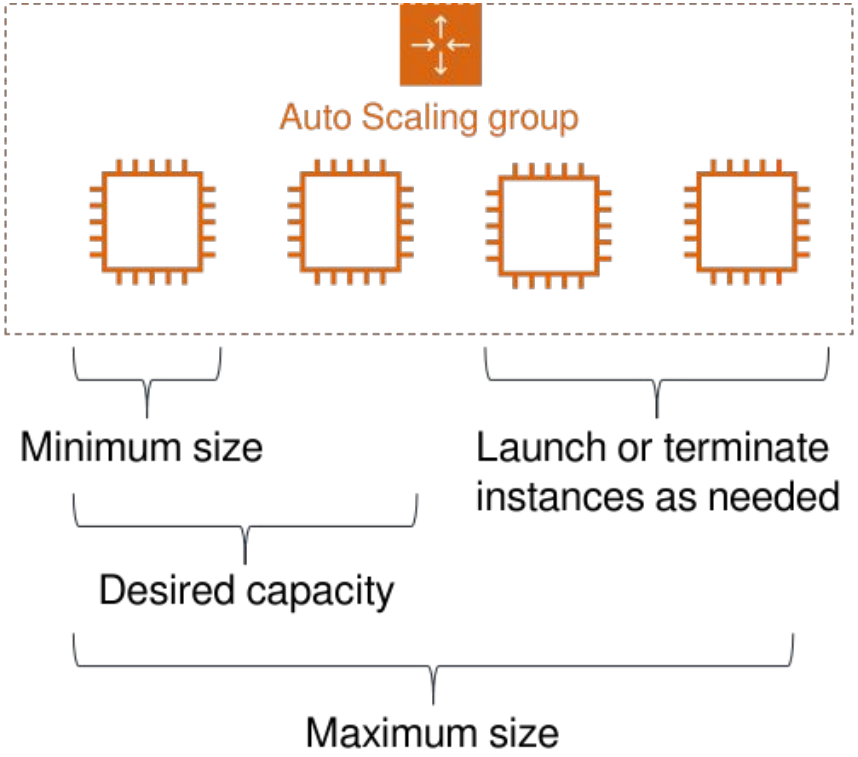
- Logs, continuously monitors, and retains account activity related to actions across your AWS infrastructure
- Records API calls for most AWS services
  - AWS Management Console and AWS CLI activity are also recorded
- Is supported for a growing number of AWS services
- Automatically pushes logs to Amazon S3 after it is configured
- Will not track events within an Amazon EC2 instance
  - **Example:** Manual shutdown of an instance

# Autoscaling

- Helps you maintain application availability
- Enables you to automatically add or remove EC2 instances according to conditions that you define
- Detects impaired EC2 instances and unhealthy applications, and replaces the instances without your intervention
- Provides several scaling options – Manual, scheduled, dynamic or on-demand, and predictive

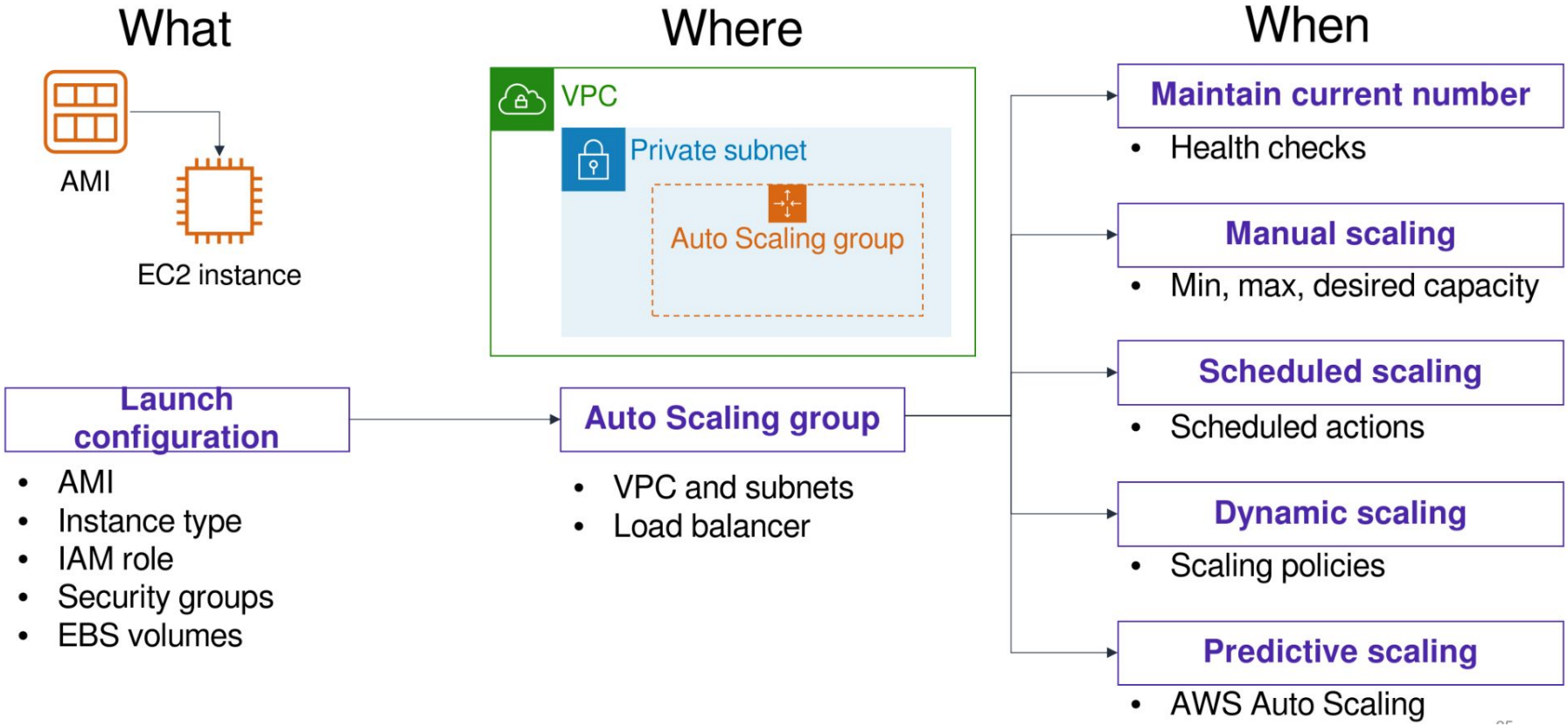


# Auto Scaling groups

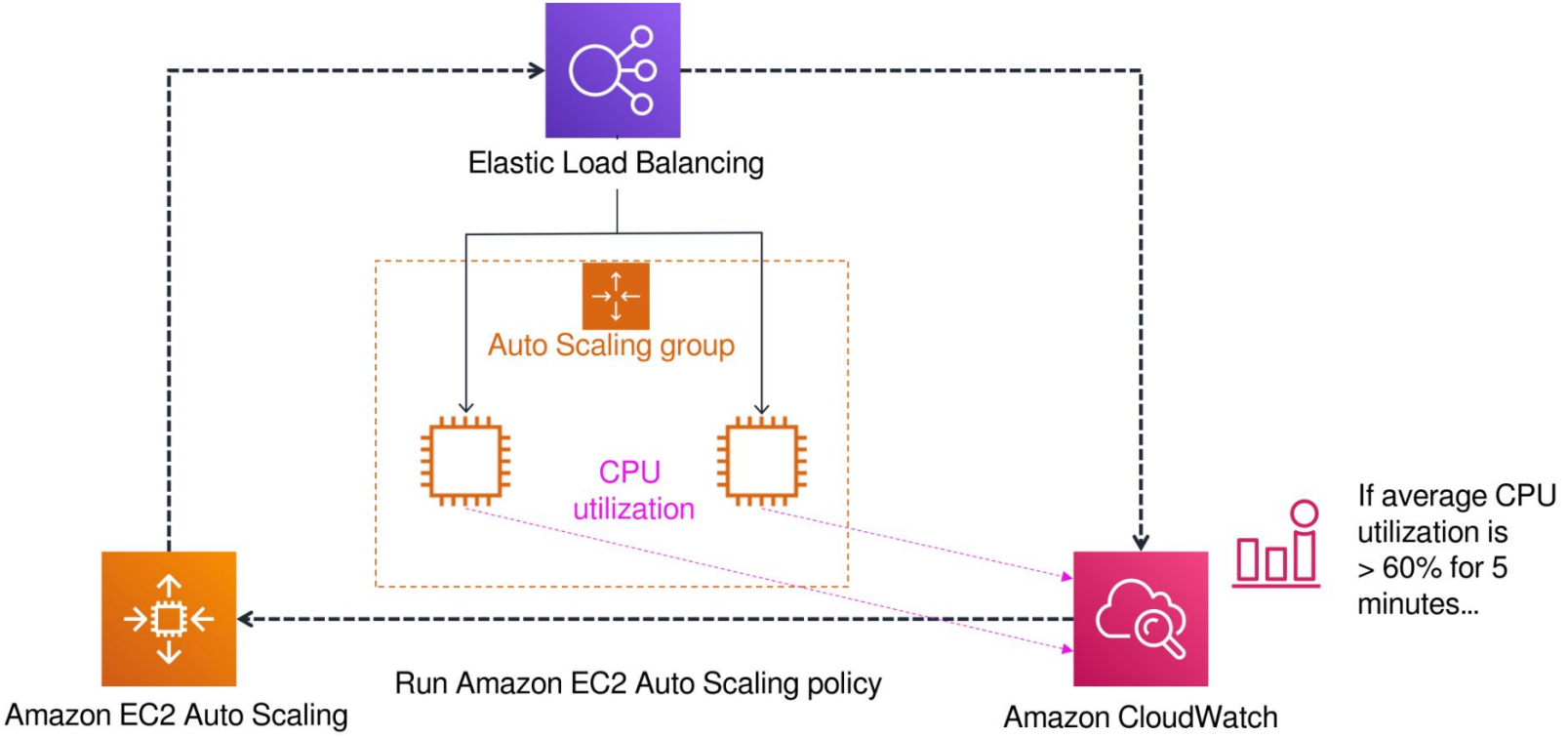



An Auto Scaling group is a collection of EC2 instances that are treated as a logical grouping for the purposes of automatic scaling and management.

# How Amazon EC2 Auto Scaling works



# Implementing dynamic scaling



# AWS Auto Scaling

- Monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost

- Provides a simple, powerful user interface that enables you to build scaling plans for resources, including –
  - Amazon EC2 instances
  - Amazon Elastic Container Service (Amazon ECS) Tasks
  - Amazon DynamoDB tables and indexes
  - Amazon Aurora Replicas

# Other monitoring tools


Purpose-built tools, not as deeply integrated but oftentimes better equipped for overall implementation.

**Datadog** is an observability service for cloud-scale applications, providing monitoring of servers, databases, tools, and services, through a SaaS-based data analytics platform.

(some already know this from Research Project).

Others include:

solarwinds

splunk>

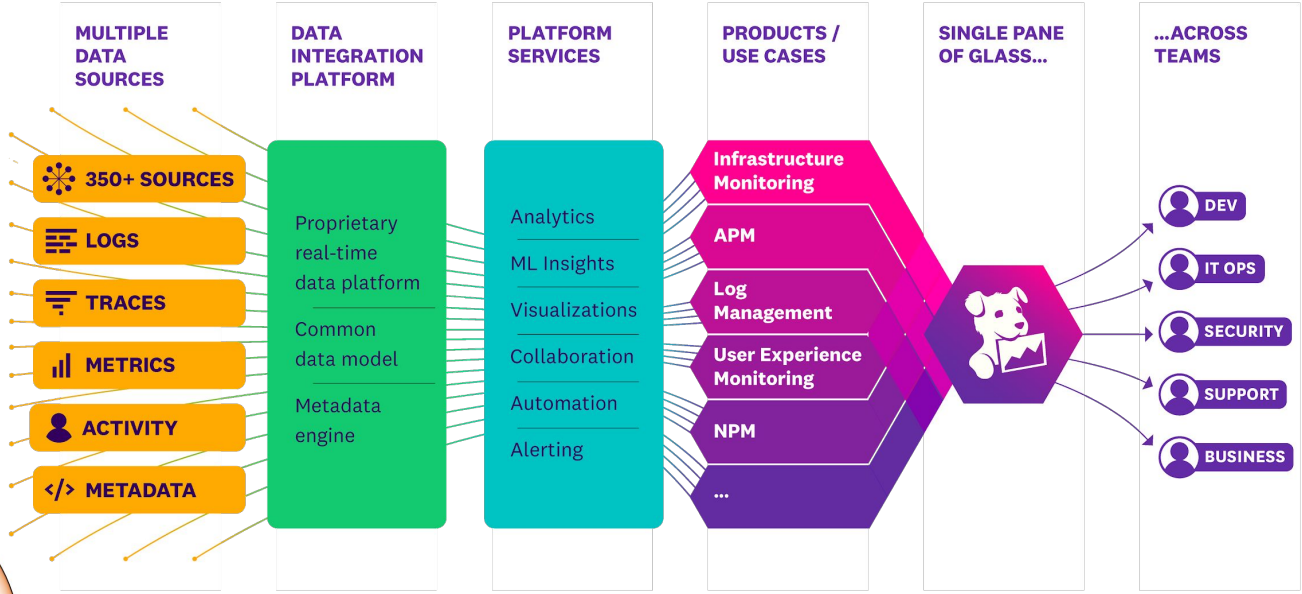
new relic

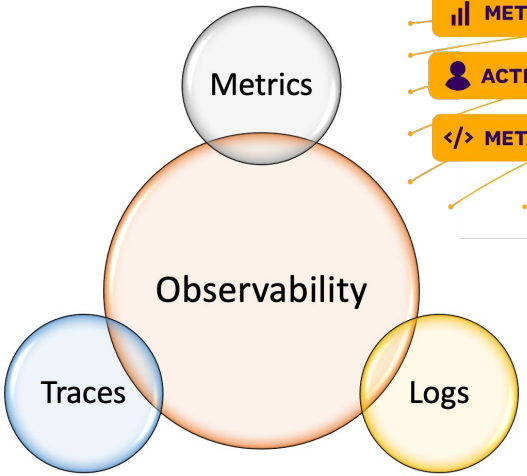
dynatrace

sumo logic

# Other monitoring tools

Remember this?

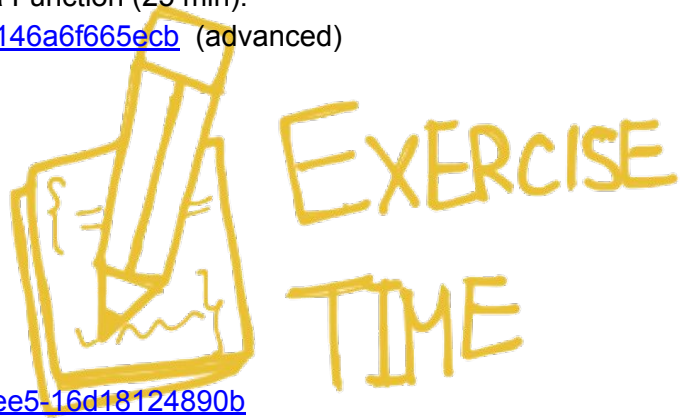



Next year…

# Cloudwatch labs

- Monitor Resources and Deployed Configurations Using AWS CloudWatch (60min):
  https://app.pluralsight.com/labs/detail/ace0abe1-0450-4d9a-adf7-2886f81373ba/
- Query and Analyze VPC Flow Logs in AWS CloudWatch Logs (35min):
  https://app.pluralsight.com/labs/detail/f65d4fc3-094e-48a3-8d98-bd80020f6179
- Monitor Amazon EC2 Application logs with Cloudwatch Logs Insights (35min):
  https://app.pluralsight.com/labs/detail/a2dc7685-49a7-444f-b40d-0147764386d2
- Implement a CloudWatch Events Rule That Calls an AWS Lambda Function (25 min):
  https://app.pluralsight.com/labs/detail/c62ca4b8-4b41-4068-8c82-146a6f665ecb (advanced)




**Optioneel:**

- GCP references:
  “Cloud Logging on Kubernetes Engine” (45min)
  “Fundamentals of Cloud Logging” (60min)

- Azure References:
  - Monitor Logs and Analytics in Azure Monitor (100min)
    https://app.pluralsight.com/labs/play/74d6bc30-a699-447f-bee5-16d18124890b
  - Monitor performance of virtual machines by using Azure Monitor for VMs (48min)
    https://docs.microsoft.com/en-us/learn/modules/monitor-performance-using-azure-monitor-for-vms/
  - Monitor the health of your Azure virtual machine by using Azure Metrics Explorer and metric alerts (43min)
    https://docs.microsoft.com/en-us/learn/modules/monitor-azure-vm-using-diagnostic-data/