

AWS Cloud Security Foundations– AWS-CSF

Dr. Ibrahim Gomaa

Lecture 5 – Automatic Scaling, Logging and Monitoring



Course Outline

Lecture 5: Automatic Scaling, Logging and Monitoring

Topics

- Elastic Load Balancing
- Amazon CloudWatch
- Amazon EC2 Auto Scaling
- Importance of logging and monitoring
- Capture and collect
- AWS services with built-in logs
- Monitor and report

Activities

- Elastic Load Balancing activity
- Amazon CloudWatch

Lab

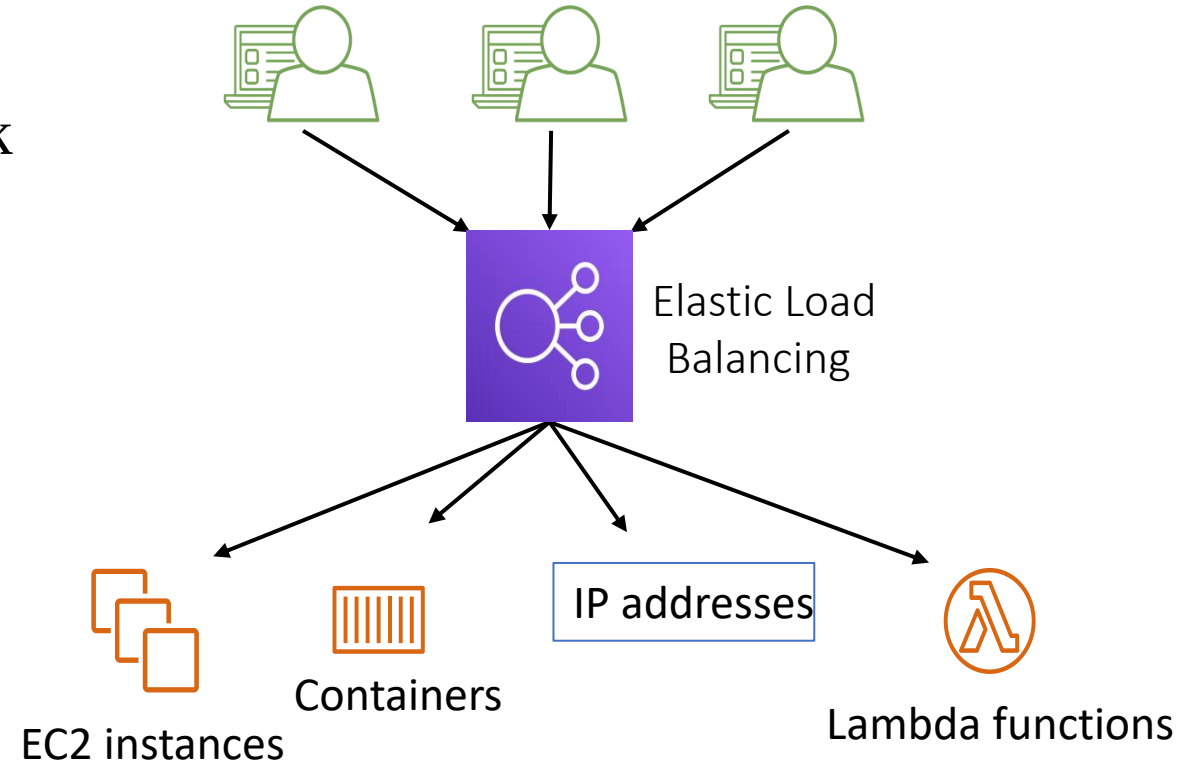
- Scale and Load Balance Your Architecture
- Monitoring and Alerting with CloudTrail and CloudWatch

Elastic Load Balancing



Elastic Load Balancing (ELB)

- Distributes incoming application or network traffic across multiple targets in a single Availability Zone or across multiple Availability Zones.
- Scales your load balancer as traffic to your application changes over time.



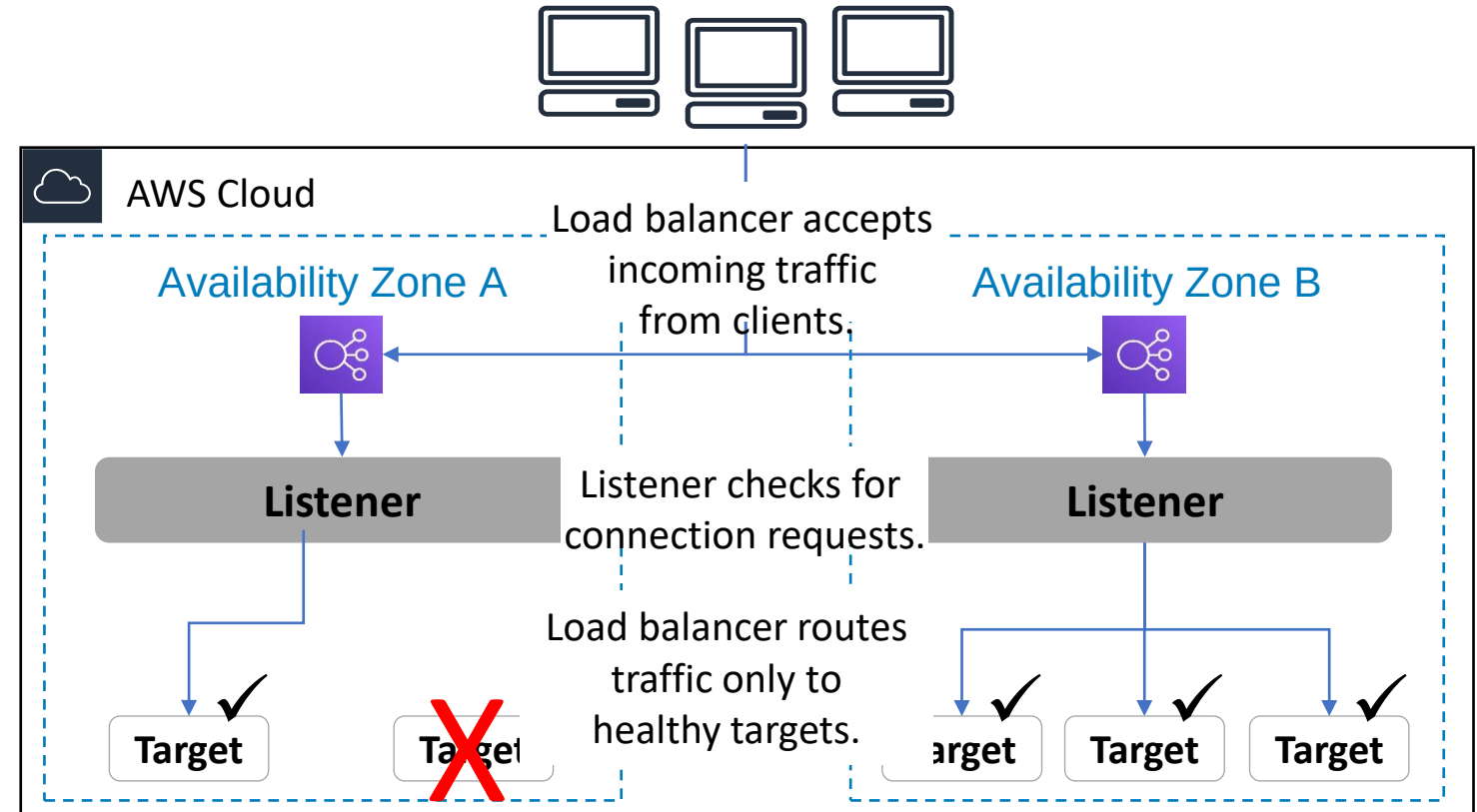
Types of load balancers

Application Load Balancer	Network Load Balancer	Classic Load Balancer (Previous Generation)
• Load balancing of HTTP and HTTPS traffic • Routes traffic to targets based on content of request • Provides advanced request routing targeted at the delivery of modern application architectures, including microservices and containers • Operates at the application layer (OSI model layer 7)	• Load balancing of TCP, UDP, and TLS traffic where extreme performance is required • Routes traffic to targets based on IP protocol data • Can handle millions of requests per second while maintaining ultra-low latencies • Is optimized to handle sudden and volatile traffic patterns • Operates at the transport layer (OSI model layer 4)	• Load balancing of HTTP, HTTPS, TCP, and SSL traffic • Load balancing across multiple EC2 instances • Operates at both the application and transport layers.

How Elastic Load Balancing works

- With Application Load Balancers and Network Load Balancers, you **register targets in target groups**, and route traffic to the target groups.
- With Classic Load Balancers, you **register instances with the load balancer**.

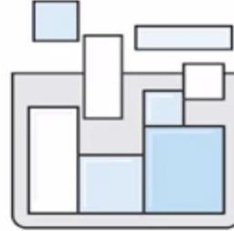
Load balancer performs health checks to monitor health of registered targets.



Elastic Load Balancing use cases



Highly available and
fault-tolerant
applications



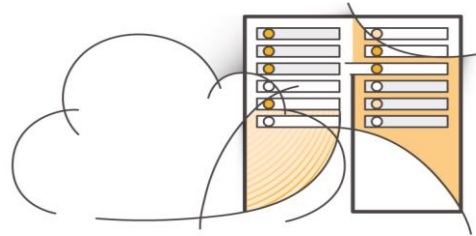
Containerized
applications



Elasticity
and scalability



Virtual private
cloud (VPC)



Hybrid environments



Invoke Lambda
functions over HTTP(S)

Activity: Elastic Load Balancing

You must support traffic to a containerized application.

Application Load Balancer

You have extremely spiky and unpredictable TCP traffic.

Network Load Balancer

You need simple load balancing with multiple protocols.

Classic Load Balancer

You need to support a static or Elastic IP address, or an IP target outside a VPC.

Network Load Balancer

You need a load balancer that can handle millions of requests per second while maintaining low latencies.

Network Load Balancer

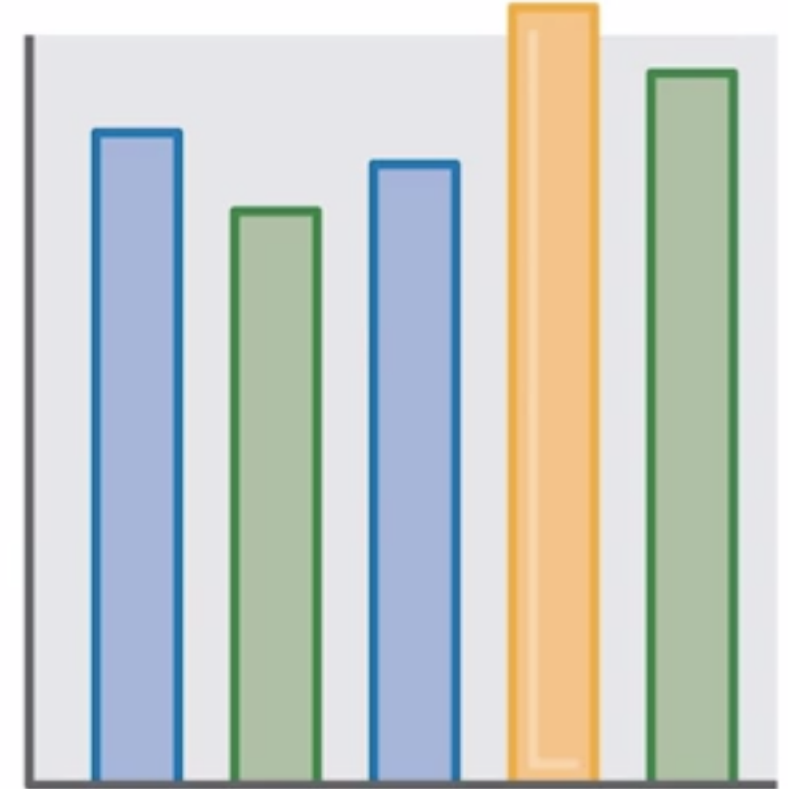
You must support HTTPS requests.

Application Load Balancer

Elastic Load Balancing

Load balancer monitoring

- **Amazon CloudWatch metrics** – Used to verify that the system is performing as expected and creates an alarm to initiate an action if a metric goes outside an acceptable range.
- **Access logs** – Capture detailed information about requests sent to your load balancer.
- **AWS CloudTrail logs** – Capture the who, what, when, and where of API interactions in AWS services.



Amazon CloudWatch



Monitoring AWS resources

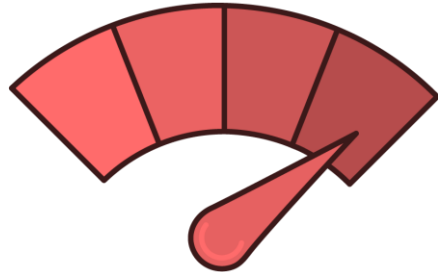
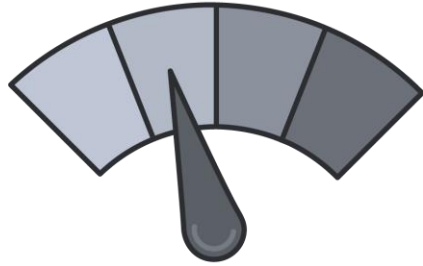
To use AWS efficiently, you need insight into your AWS resources:

- How do you know when you should **launch more Amazon EC2 instances**?
- Is your **application's performance or availability** being affected by a lack of sufficient capacity?
- How much of your infrastructure is actually **being used**?

Amazon CloudWatch



**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

CloudWatch alarms

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

Statistic

Period

Conditions

Threshold type

☒ Static

Use a value as a threshold

☐ Anomaly detection

Use a band as a threshold

Whenever CPUUtilization is...

Define the alarm condition

☒ Greater

> threshold

☐ Greater/Equal

>= threshold

☐ Lower/Equal

<= threshold

☐ Lower

< threshold

than...

Define the threshold value

Must be a number

[▶ Additional configuration](#)

CloudWatch alarms

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

Statistic

Period

Conditions

Threshold type

☒ Static

Use a value as a threshold

☐ Anomaly detection

Use a band as a threshold

Whenever CPUUtilization is...

Define the alarm condition

☒ Greater

> threshold

☐ Greater/Equal

>= threshold

☐ Lower/Equal

<= threshold

☐ Lower

< threshold

than...

Define the threshold value

Must be a number

[▶ Additional configuration](#)

Lecture
5

Automatic Scaling, Logging and Monitoring

Activity: Amazon CloudWatch



Amazon EC2

If average CPU utilization is $> 60\%$ for 5 minutes...

Correct!



Amazon RDS

If the number of simultaneous connections is > 10 for 1 minute...

Correct!



Amazon S3

If the maximum bucket size in bytes is around 3 for 1 day...

Incorrect. *Around* is not a threshold option. You must specify a threshold of $>$, $>=$, $<=$, or $<$.



Elastic Load Balancing

If the number of healthy hosts is < 5 for 10 minutes...

Correct!



Amazon Elastic Block Store

If the volume of read operations is $> 1,000$ for 10 seconds...

Incorrect. You must specify a statistic (for example, *average volume*).



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

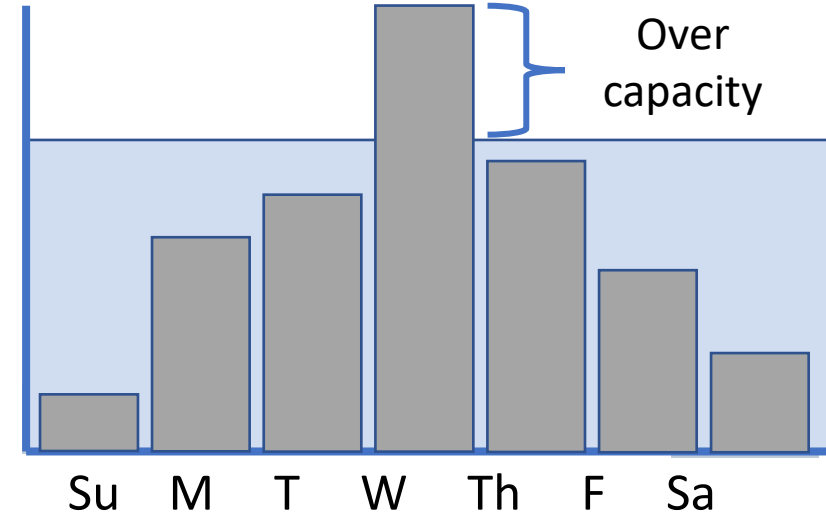
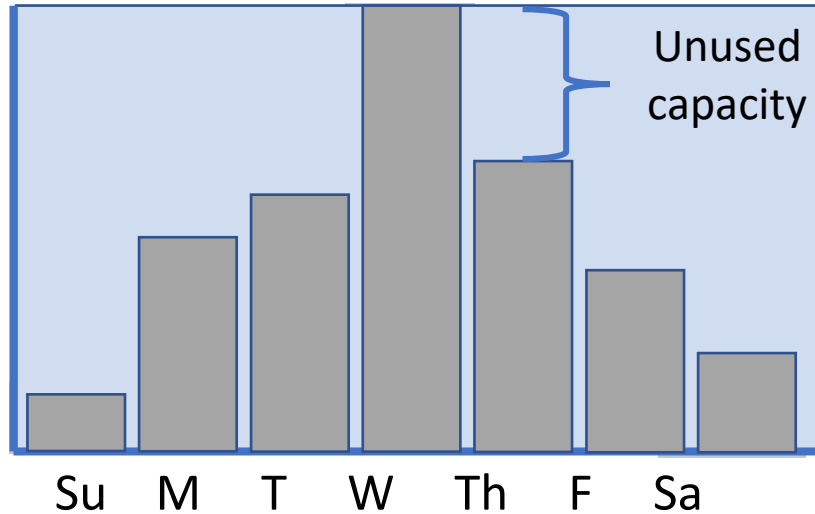
AWS Cloud Security Foundations– AWS-CSF

Amazon EC2 Auto Scaling



Amazon EC2 Auto Scaling

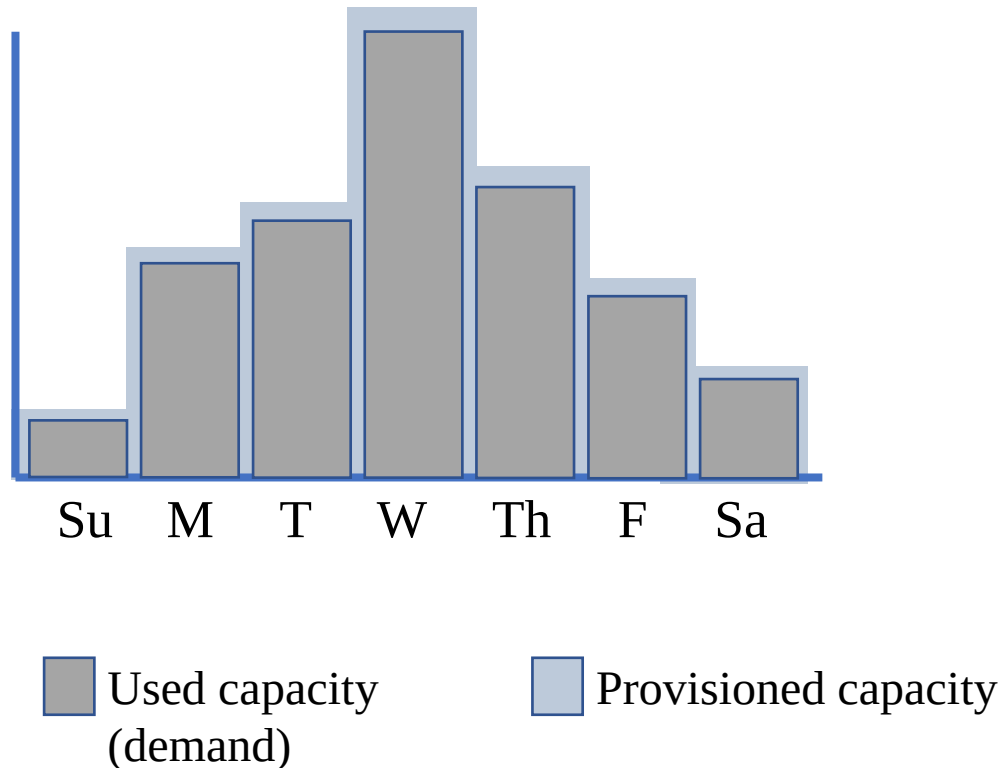
Why is scaling important?



Used capacity
(demand)

Provisioned capacity

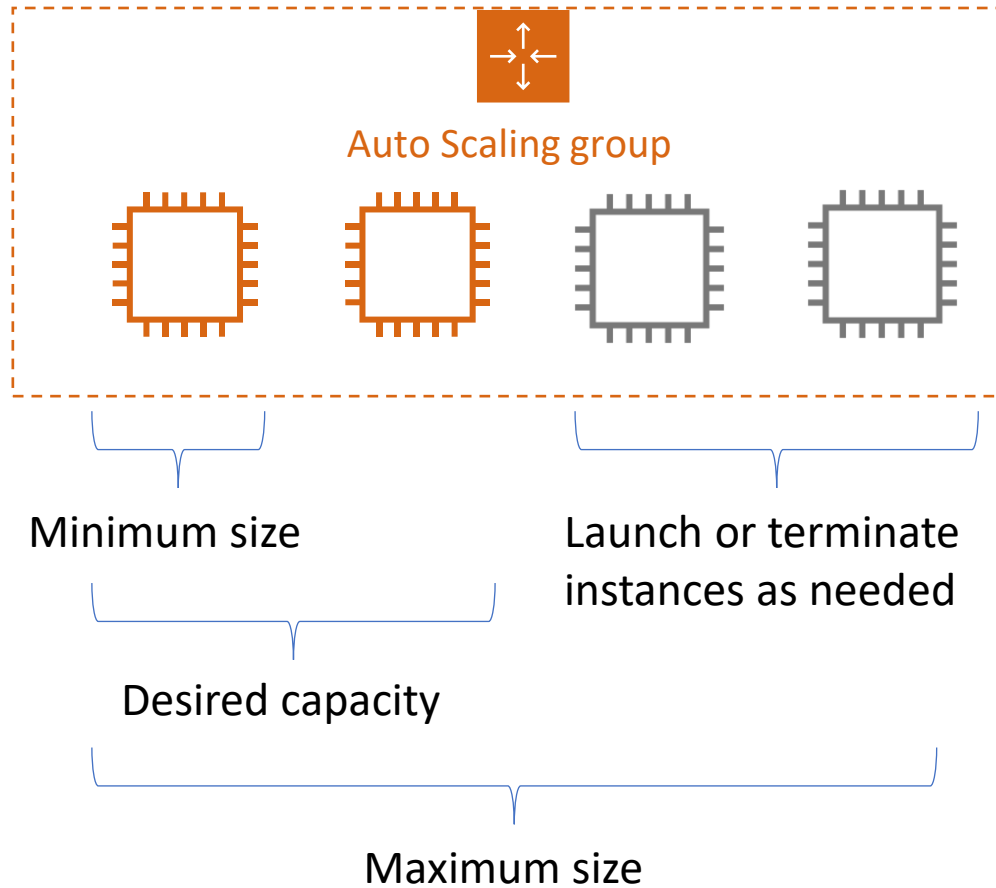
Amazon EC2 Auto Scaling



- 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

Amazon EC2 Auto Scaling

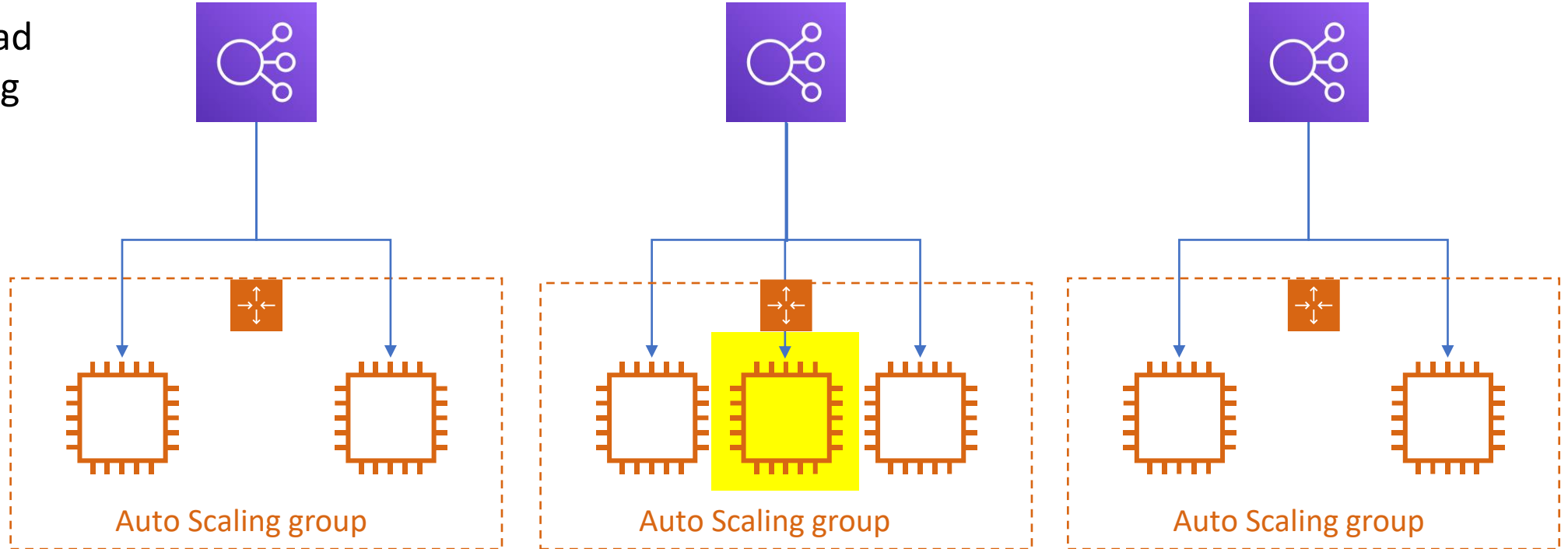
Auto Scaling groups



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.

Scaling out versus scaling in

Elastic Load
Balancing



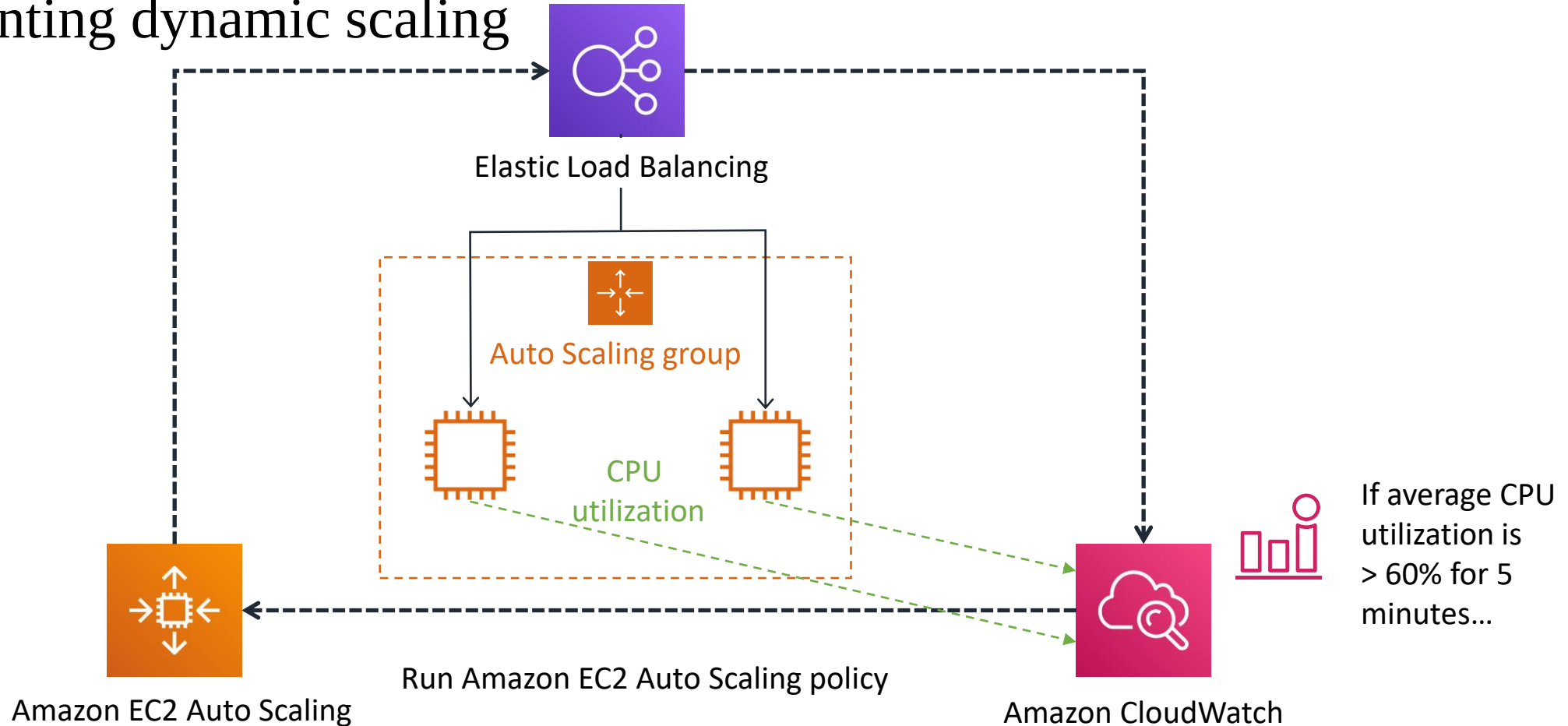
Base configuration

Scale out
(launch instances)

Scale in
(terminate instances)

AWS Cloud Security Foundations– AWS-CSF

Implementing dynamic scaling



AWS Auto Scaling



AWS Auto Scaling

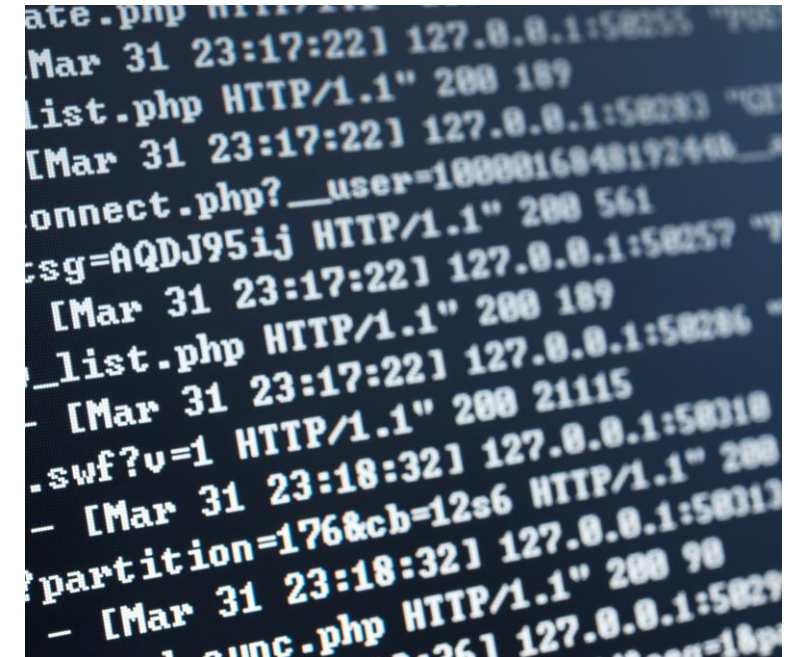
- Monitors your applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost
- Provides a simple, powerful user interface that enables you to build scaling plans for resources, including –
 - Amazon EC2 instances and Spot Fleets
 - Amazon Elastic Container Service (Amazon ECS) Tasks
 - Amazon DynamoDB tables and indexes
 - Amazon Aurora Replicas

Importance of logging and monitoring



What is logging?

- Logging is the collection and recording of activity and event data.
 - Provided by the service itself (Amazon VPC Flow Logs and Amazon S3 server access logs)
 - Provided by a secondary service (AWS CloudTrail)
- Information logged will vary based on the service conducting the logging.
 - Common log elements:
 - Date and time of event
 - Origin of event
 - Identity of resources accessed



Why is logging important?

- Logging provides a record of events, which is useful for the following:
 - Troubleshooting
 - Auditing
 - Recordkeeping
 - Incident response and remediation
- Logs are a requirement for demonstrating compliance with regulations, such as the following:
 - HIPAA (US Health Insurance Portability and Accountability Act)
 - GDPR (European Union General Data Protection Regulation)
 - LGPD (Brazil's General Data Protection Law)



What is monitoring?

- Monitoring is the continuous verification of the security and performance of your resources, applications, and data.
- AWS provides several services that give you the visibility to spot issues before they impact operations:
 - AWS CloudTrail
 - Amazon CloudWatch
 - Amazon EventBridge
 - AWS X-Ray

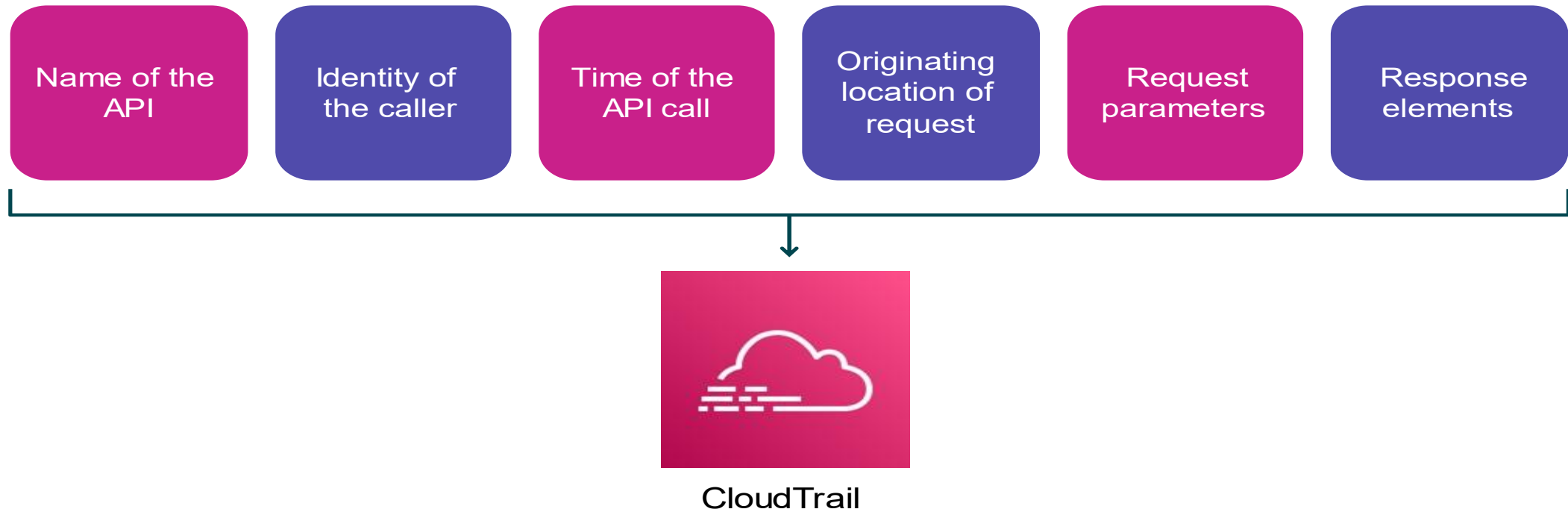


Capture and collect



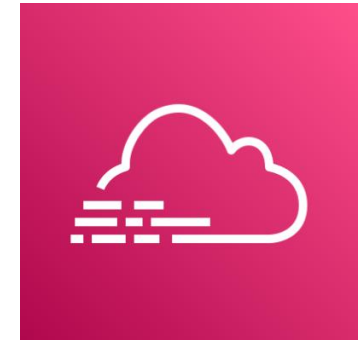
API security-relevant information

CloudTrail records important information about each API call, this information helps you to track changes made to your AWS resources, troubleshoot operational issues, and ensure compliance with internal policies and regulatory standards.



AWS CloudTrail

- Assists you to enable governance and compliance, as well as operational and risk auditing of your AWS account
- Records actions taken by a user, role, or AWS service as events
- Provides visibility of events in the CloudTrail console
- Can be used to view, search, download, archive, analyze, and respond to account activity across your AWS infrastructure



Activity: Reading a Log File

Reading a log: Identity of the caller

```
{  
  "Records": [{  
    "eventVersion": "1.0",  
    "userIdentity": {  
      "type": "IAMUser",  
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",  
      "arn": "arn:aws:iam::111122223333:user/Jane",  
      "accountId": "111122223333",  
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",  
      "userName": "Jane"  
    },  
  ],  
}
```



Activity: Reading a Log File

Reading a log: Time and origin of the request

```
"eventTime": "2021-07-06T21:01:59Z",  
"eventSource": "ec2.amazonaws.com",  
"eventName": "StopInstances",  
"awsRegion": "us-east-2",  
"sourceIPAddress": "203.0.113.176",  
"userAgent": "ec2-api-tools 1.6.12.2",
```

Activity: Reading a Log File

Reading a log: Request parameters and response elements

```
"requestParameters": {  
  "instancesSet": {  
    "items": [{  
      "instanceId": "i-ebeaf9e2" } ] },  
  "force": false },  
"responseElements": {  
  "instancesSet": {  
    "items": [{  
      "instanceId": "i-ebeaf9e2",  
      "currentState": {  
        "code": 64,  
        "name": "stopping" },  
      "previousState": {  
        "code": 16,  
        "name": "running" } } ] },
```

AWS Cloud Security Foundations– AWS-CSF



Activity: Reading a Log File

Reading a log: Answer

AWS Identity and Access Management (IAM) user named **Jane**. Jane used the **ec2-stop-instances** command in the **AWS CLI** to call the Amazon **EC2 StopInstances** action.



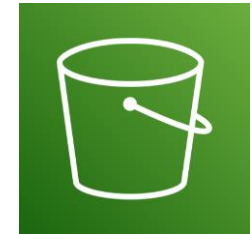
AWS services with built-in logs



Services with built-in logs: Amazon S3

Server access logging is a built-in feature of Amazon S3. Enable the feature for detailed records of requests that are made to an S3 bucket

- Amazon S3 provides detailed access request records through **Amazon S3 server access logging**.
- Server access logs provide useful information for security and access audits.
- Server access logs can provide insight into your customer base and assist you to understand your Amazon S3 bill.



Amazon Simple
Storage Service
(Amazon S3)

Services with built-in logs: Amazon VPC

- With **VPC Flow Logs**, you can capture information about inbound and outbound IP traffic from the following:
 - VPC
 - Subnets
 - Individual network interfaces
- Publish flow log data to CloudWatch or Amazon S3.
- Flow log data is collected outside of the path of your network traffic, with no impact on throughput or latency.



Amazon Virtual
Private Cloud
(Amazon VPC)

Services with built-in logs: ELB

- **ELB access logs** capture detailed information about requests sent to your load balancer.
- Use access logs to analyze traffic patterns and for troubleshooting.
- ELB captures, compresses, and stores logs in a specified S3 bucket.



Elastic Load Balancing
(ELB)

Monitor and Report



Amazon CloudWatch

- Is a monitoring and observability service
- Provides a unified view of the operational health of your AWS resources, applications, and services
- Collects metrics in the AWS Cloud and on premises
- Can be used for infrastructure monitoring and troubleshooting
- Provides the ability to customize logs and events



Amazon CloudWatch

Comparing CloudTrail and CloudWatch

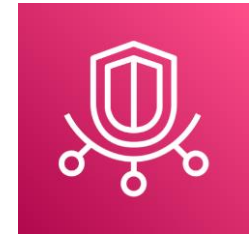
AWS CloudTrail	Amazon CloudWatch
Continuously monitors and logs user activities	Continuously monitors resource and application performance
Useful for compliance auditing, security analysis, and troubleshooting	Useful for detecting anomalous service behavior, setting alarms, and discovering insights
Helps you determine WHO performed WHAT unauthorized action and WHEN they did it	Alerts you that an issue has occurred due to an unauthorized action

When used together, you can create custom CloudWatch dashboards, alarms, and notifications for key metrics and specific CloudTrail events.



AWS Trusted Advisor

- Provides recommendations based on five categories of AWS best practices: cost optimization, security, fault tolerance, service limits, and performance improvement
- Evaluates your account to suggest improvements and optimizations for your resources
- Is accessible through the AWS Management Console and available to all support tiers



AWS Trusted Advisor

Amazon EventBridge

- Is a serverless event bus service that is used to connect your applications with data from a variety of sources
- Provides a stream of real-time data from applications and services to targets, such as AWS Lambda or event buses
- Was formerly called Amazon CloudWatch Events



Amazon EventBridge

AWS Security Hub

- Aggregates security alerts from various AWS services and partner products in a standardized format
- Collects data across accounts and checks cloud security posture against AWS security best practices
- Helps you to understand your overall security posture by using a consolidated security score across all of your AWS accounts



AWS Security Hub

AWS Config

- Helps to assess, audit, and evaluate the configurations of your AWS resources
- Continuously monitors and records AWS resource configurations
- Provides automated evaluation of recorded configurations against desired configurations



AWS Config

Thanks