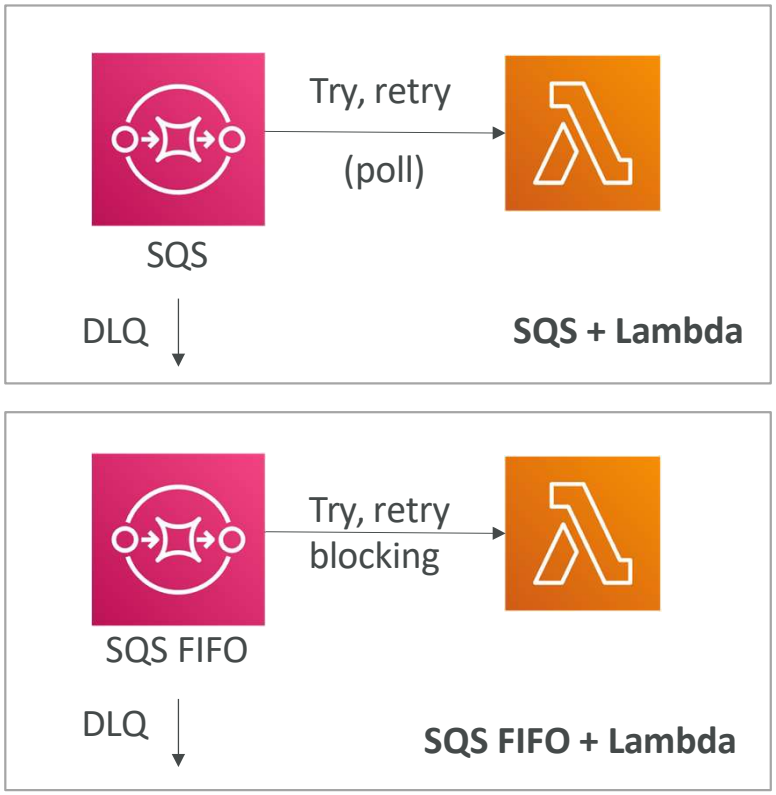
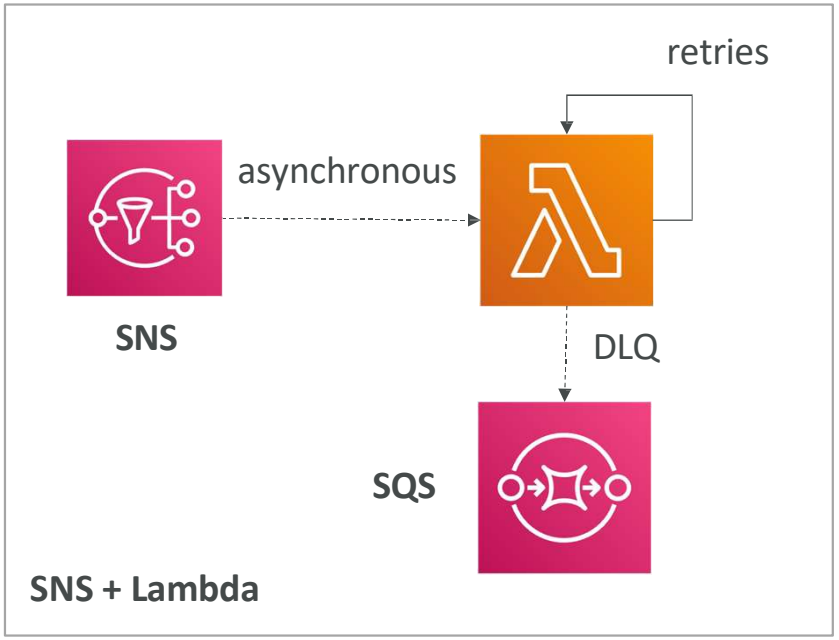
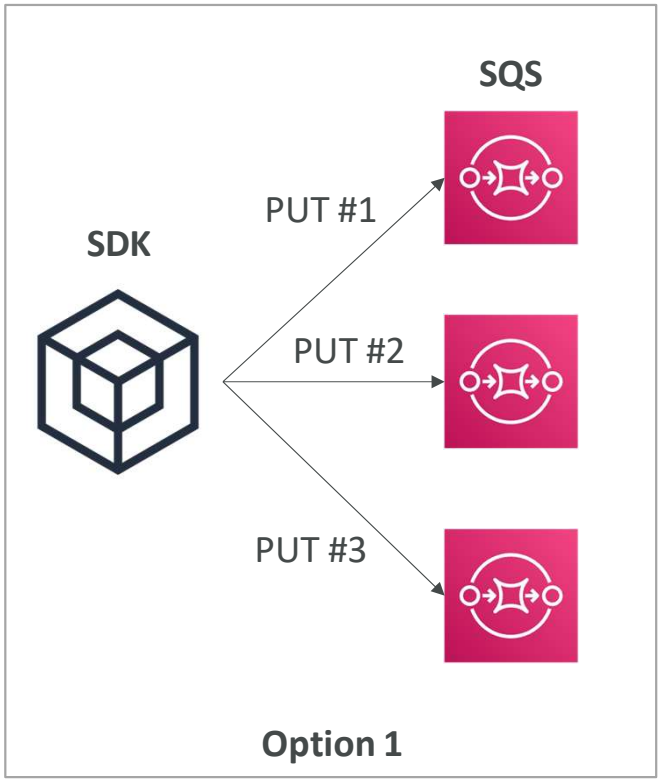
More Solutions Architecture

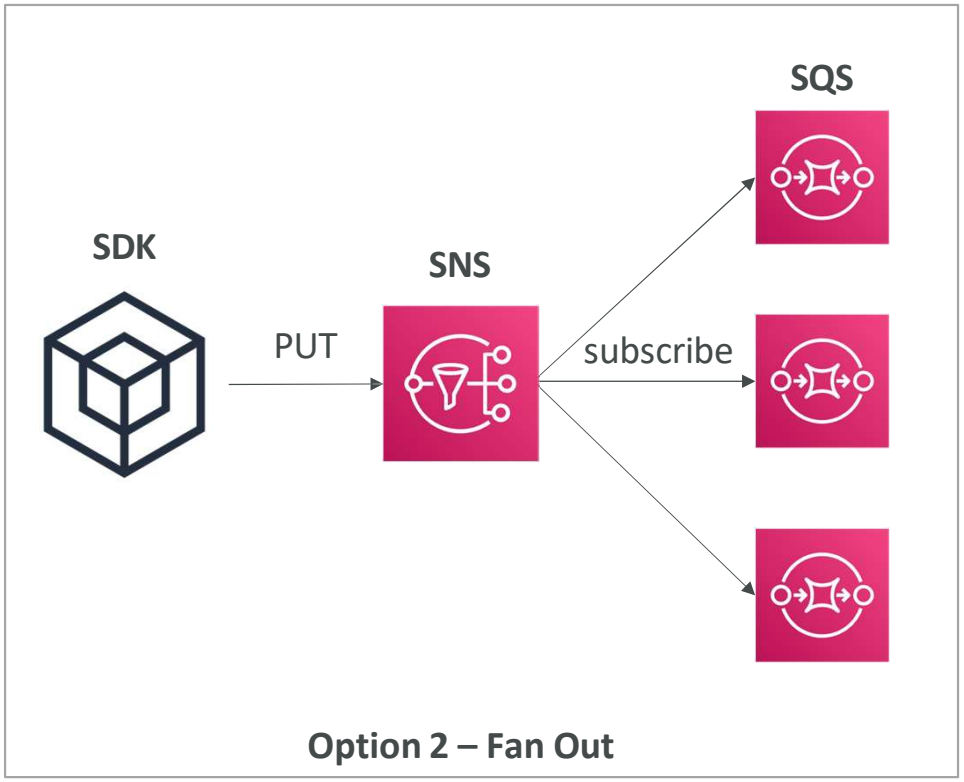
Lambda, SNS & SQS





Fan Out Pattern: deliver to multiple SQS

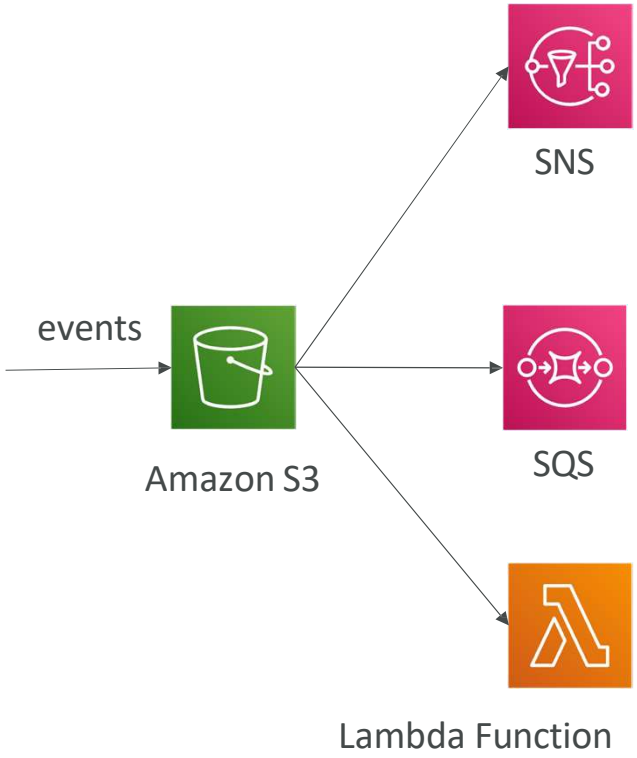




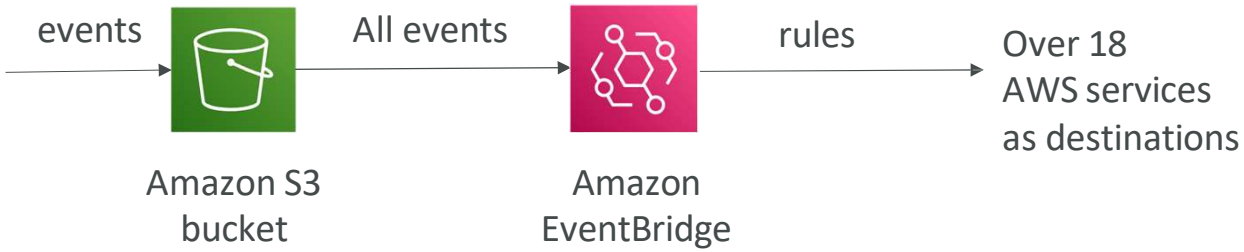
S3 Event Notifications

- S3:ObjectCreated, S3:ObjectRemoved, S3:ObjectRestore, S3:Replication...
- Object name filtering possible (*.jpg)
- Use case: generate thumbnails of images uploaded to S3
- Can create as many "S3 events" as desired

- S3 event notifications typically deliver events in seconds but can sometimes take a minute or longer

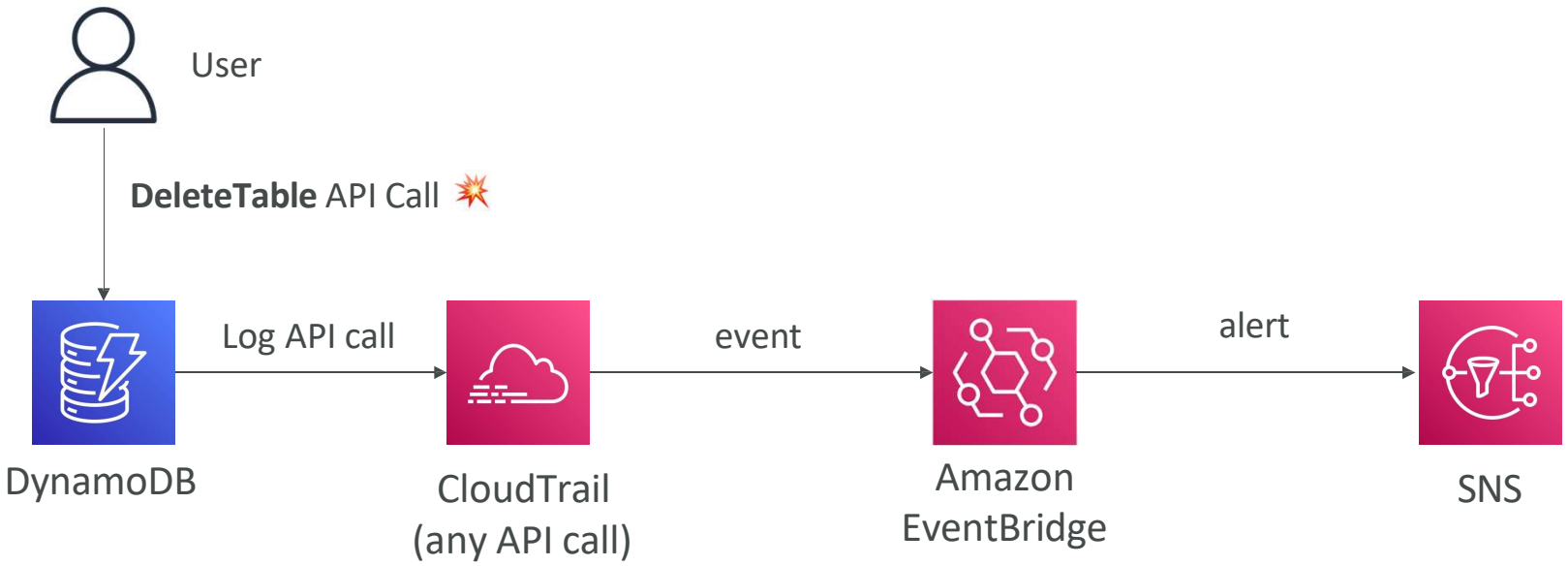


S3 Event Notifications with Amazon EventBridge

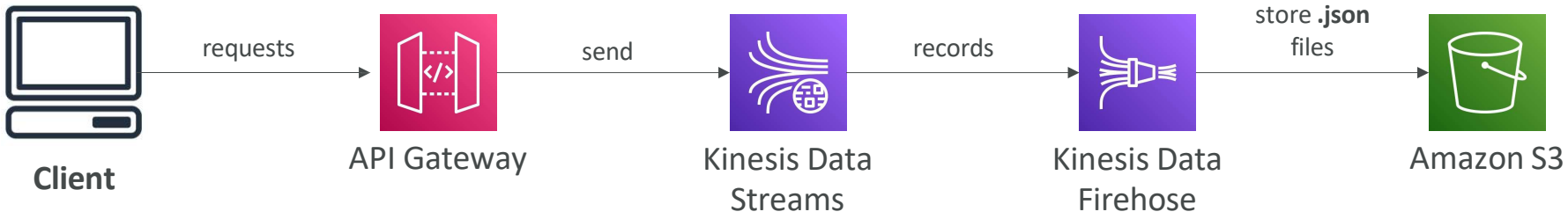


- Advanced filtering options with JSON rules (metadata, object size, name...)
- Multiple Destinations – ex Step Functions, Kinesis Streams / Firehose...
- EventBridge Capabilities – Archive, Replay Events, Reliable delivery

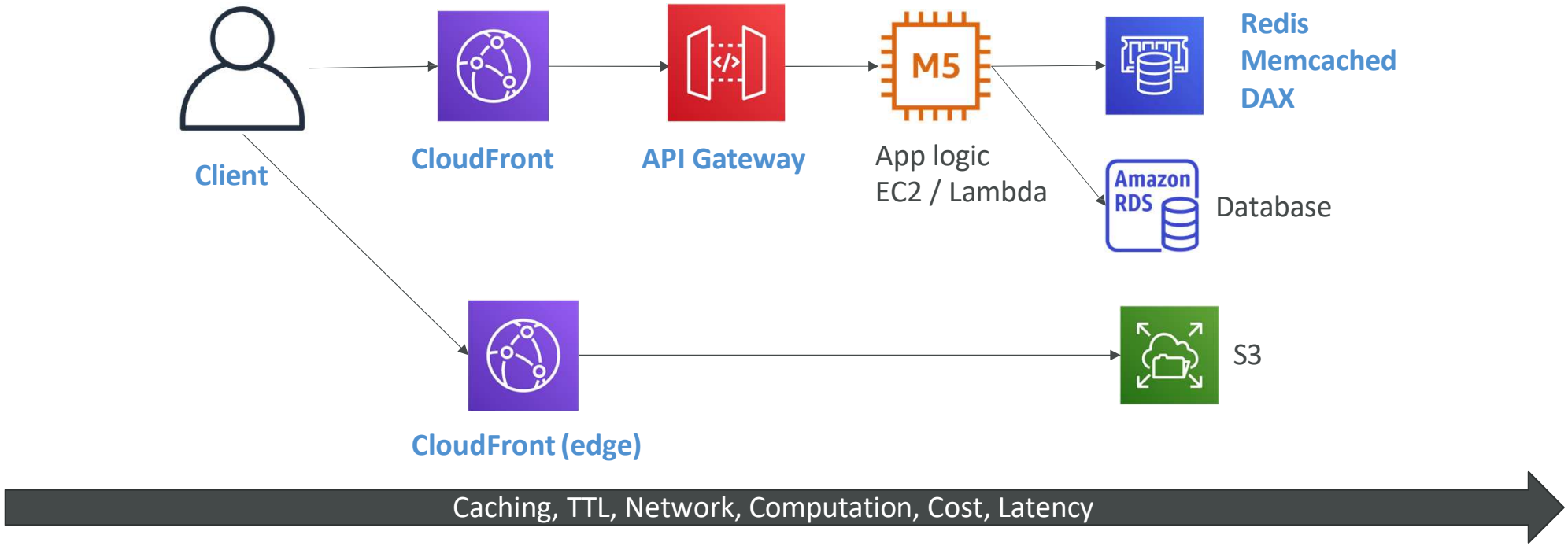
Amazon EventBridge - Intercept API Calls



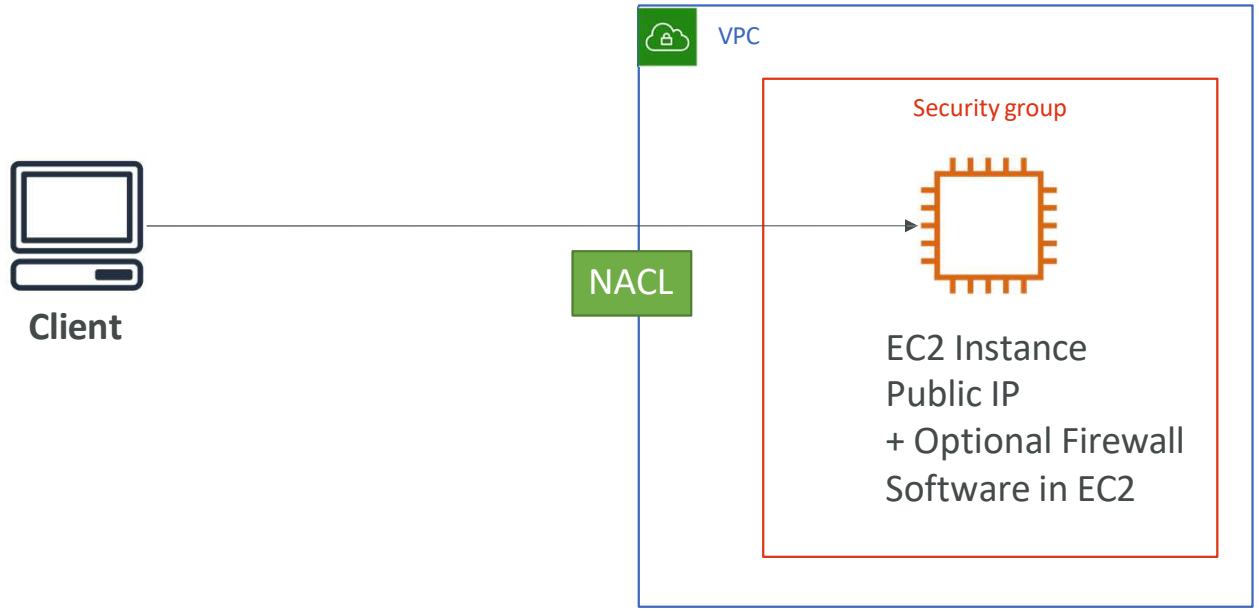
API Gateway – AWS Service Integration Kinesis Data Streams example



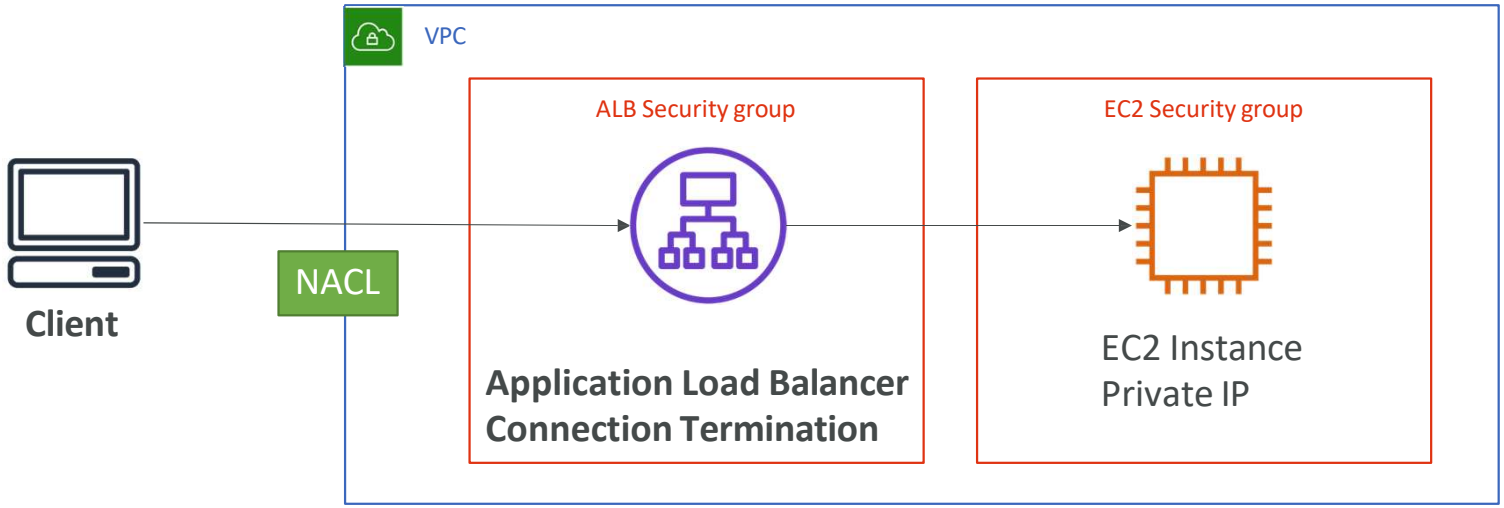
Caching Strategies



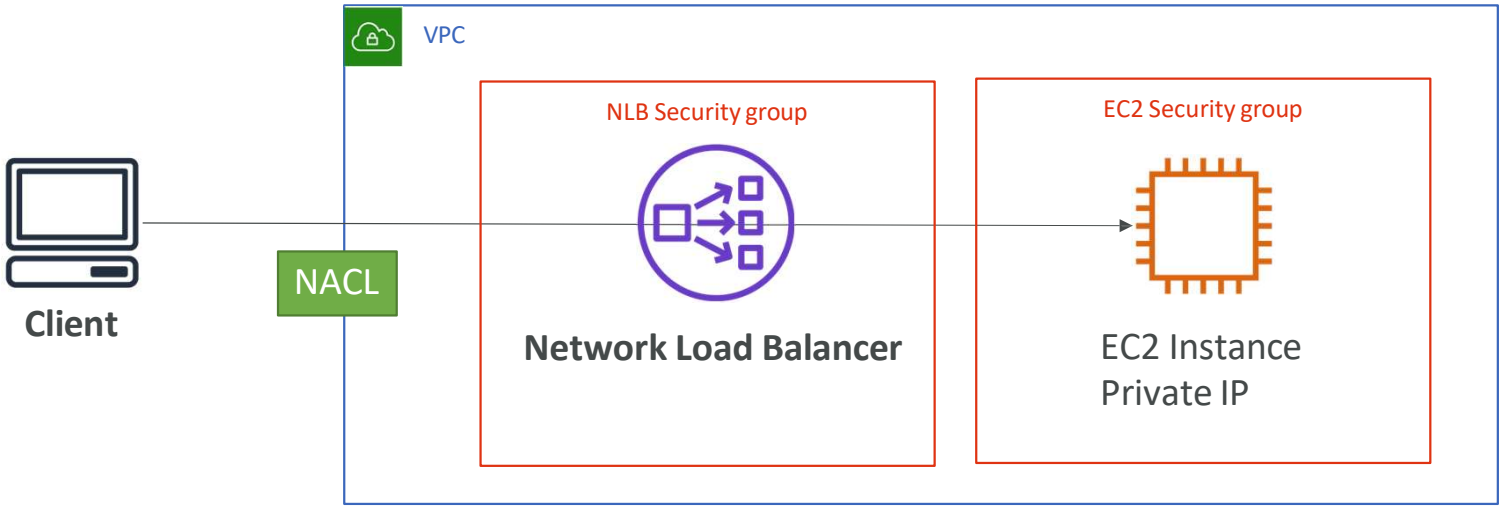
Blocking an IP address



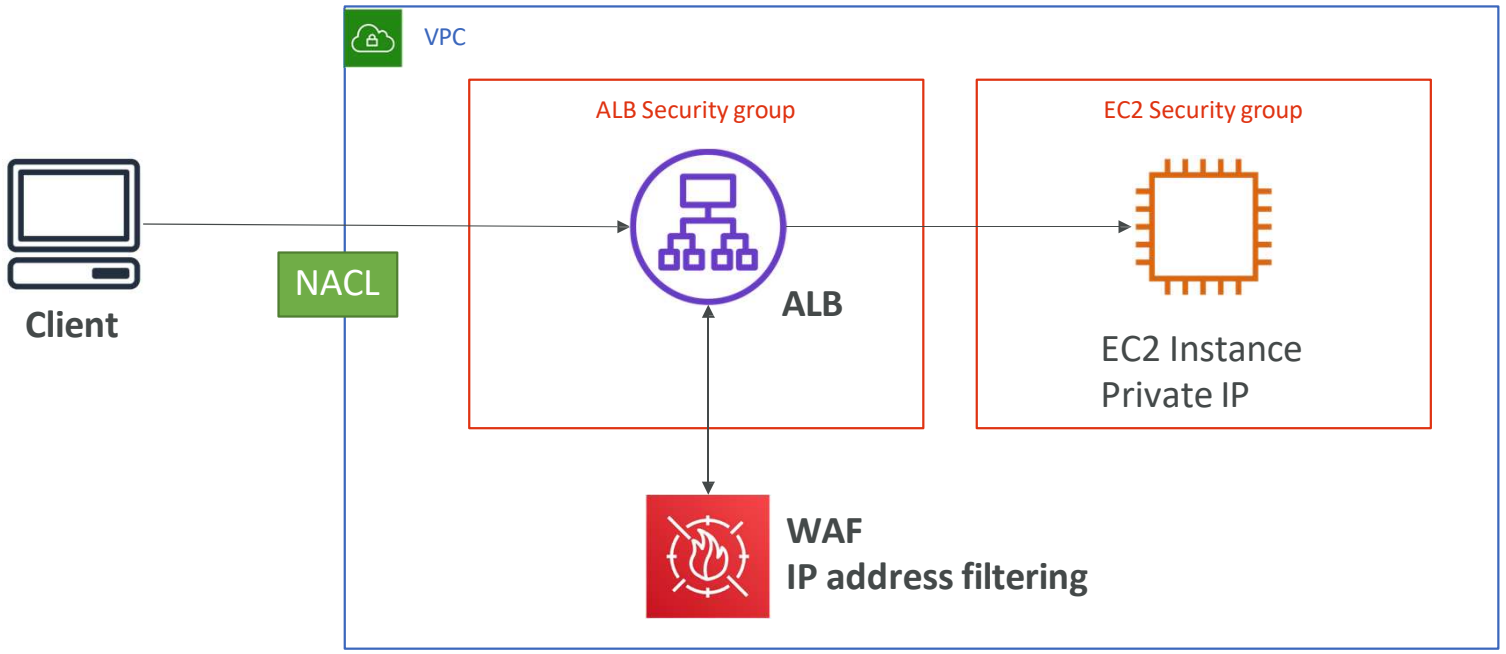
Blocking an IP address - with an ALB



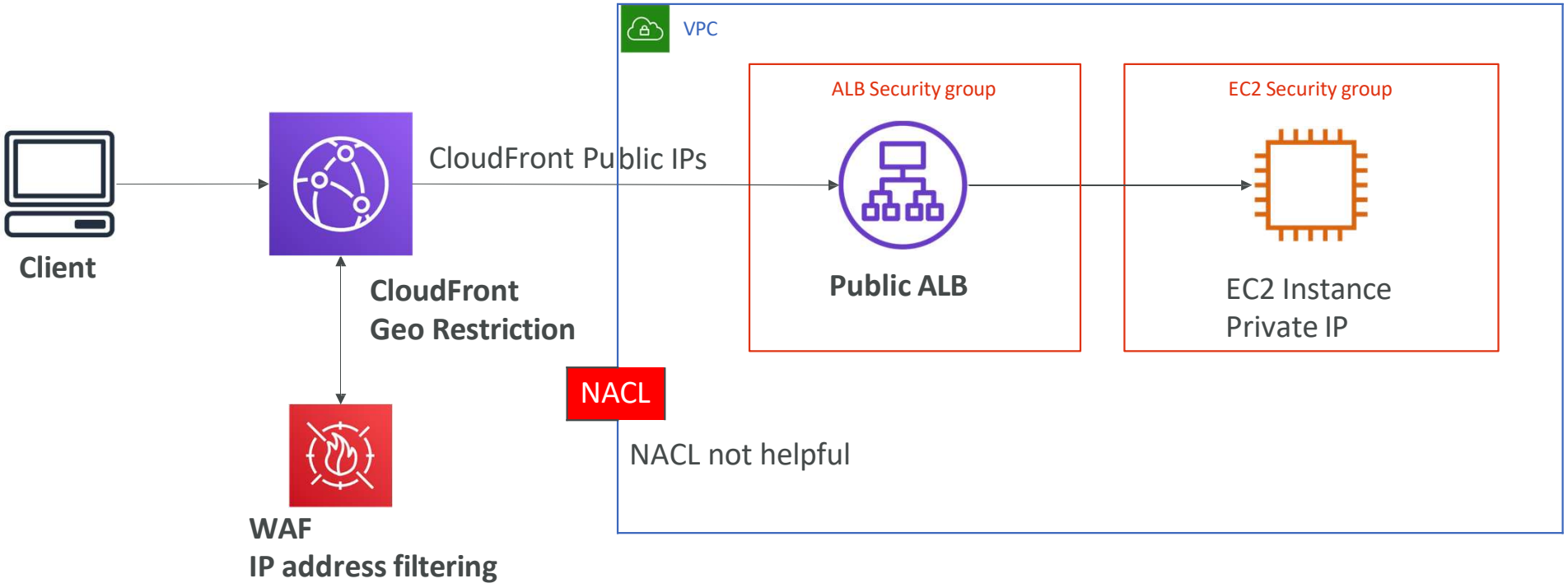
Blocking an IP address - with an NLB



Blocking an IP address - ALB + WAF



Blocking an IP address - ALB, CloudFront WAF



High Performance Computing (HPC)

- The cloud is the perfect place to perform HPC
- You can create a very high number of resources in no time
- You can speed up time to results by adding more resources
- You can pay only for the systems you have used

- Perform genomics, computational chemistry, financial risk modeling, weather prediction, machine learning, deep learning, autonomous driving

- Which services help perform HPC?

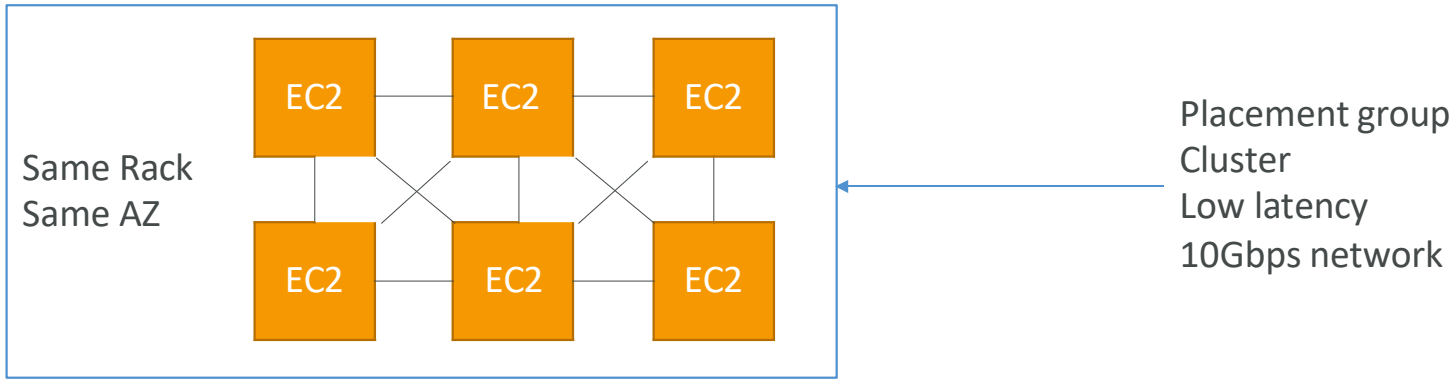
Data Management & Transfer

- AWS Direct Connect:
  - Move GB/s of data to the cloud, over a private secure network
- Snowball & Snowmobile
  - Move PB of data to the cloud
- AWS DataSync
  - Move large amount of data between on-premises and S3, EFS, FSx for Windows

Compute and Networking

- EC2 Instances:
  - CPU optimized, GPU optimized
  - Spot Instances / Spot Fleets for cost savings + Auto Scaling

- EC2 Placement Groups: Cluster for good network performance



Compute and Networking

- EC2 Enhanced Networking (SR-IOV)
  - Higher bandwidth, higher PPS (packet per second), lower latency
  - Option 1: Elastic Network Adapter (ENA) up to 100 Gbps
  - Option 2: Intel 82599 VF up to 10 Gbps – LEGACY

- Elastic Fabric Adapter (EFA)
  - Improved ENA for HPC, only works for Linux
  - Great for inter-node communications, tightly coupled workloads
  - Leverages Message Passing Interface (MPI) standard
  - Bypasses the underlying Linux OS to provide low-latency, reliable transport

Storage

- Instance-attached storage:
  - EBS: scale up to 256,000 IOPS with io2 Block Express
  - Instance Store: scale to millions of IOPS, linked to EC2 instance, low latency

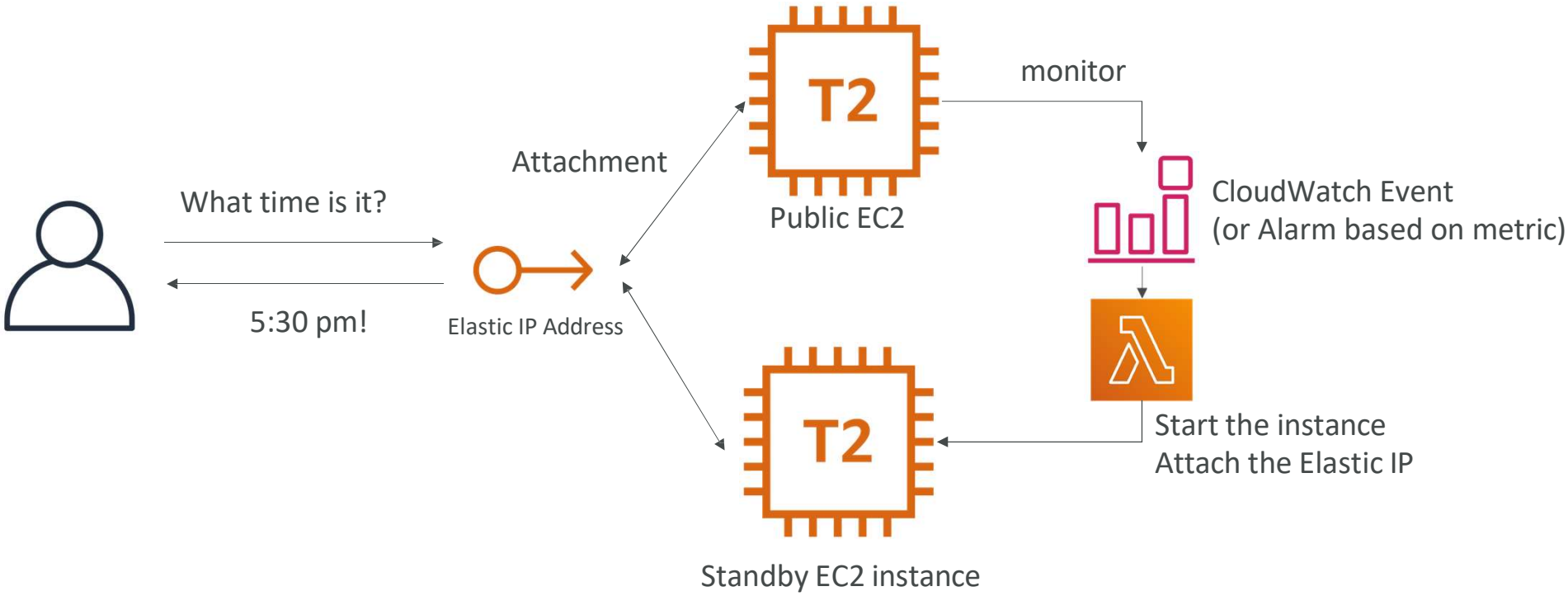
- Network storage:
  - Amazon S3: large blob, not a file system
  - Amazon EFS: scale IOPS based on total size, or use provisioned IOPS
  - Amazon FSx for Lustre:
    - HPC optimized distributed file system, millions of IOPS
    - Backed by S3

Automation and Orchestration

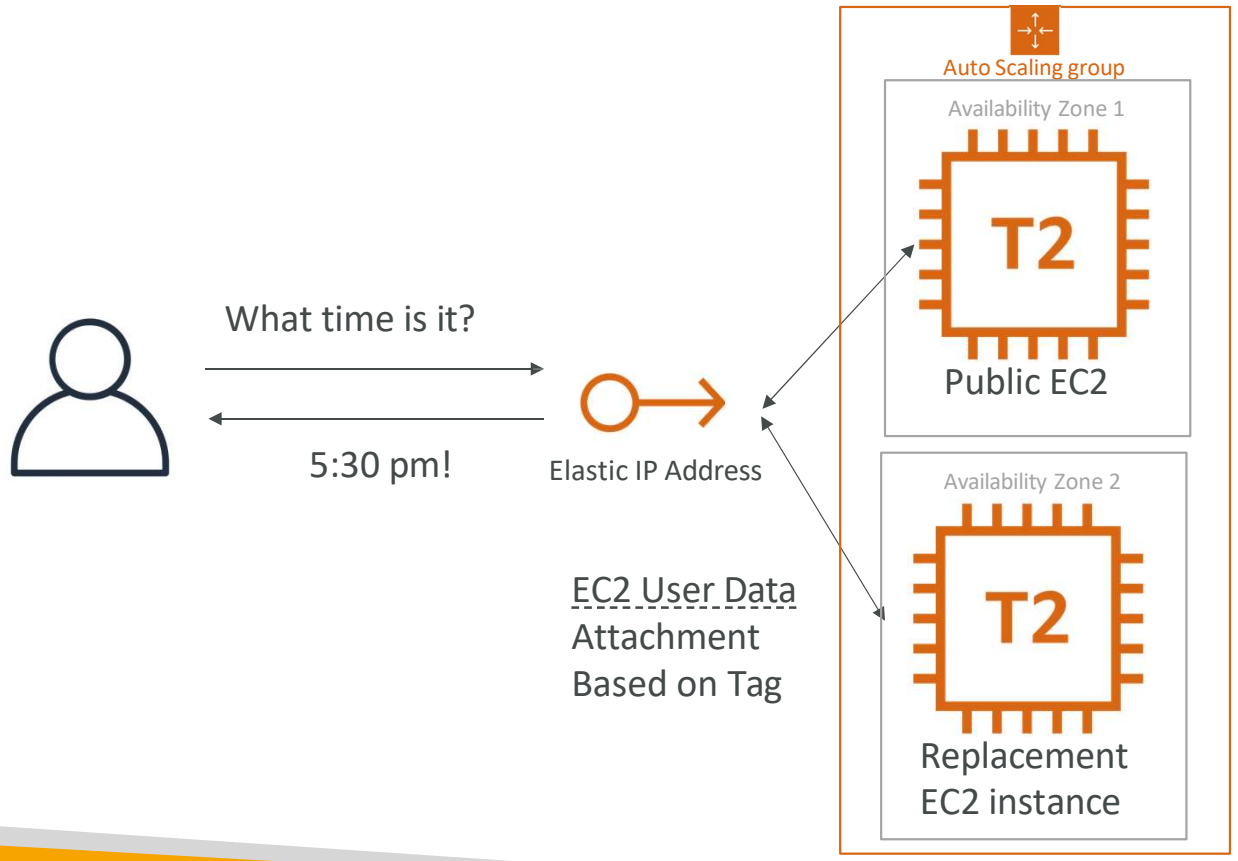
- AWS Batch
  - AWS Batch supports multi-node parallel jobs, which enables you to run single jobs that span multiple EC2 instances.
  - Easily schedule jobs and launch EC2 instances accordingly

- AWS ParallelCluster
  - Open-source cluster management tool to deploy HPC on AWS
  - Configure with text files
  - Automate creation of VPC, Subnet, cluster type and instance types
  - Ability to enable EFA on the cluster (improves network performance)

Creating a highly available EC2 instance



Creating a highly available EC2 instance With an Auto Scaling Group



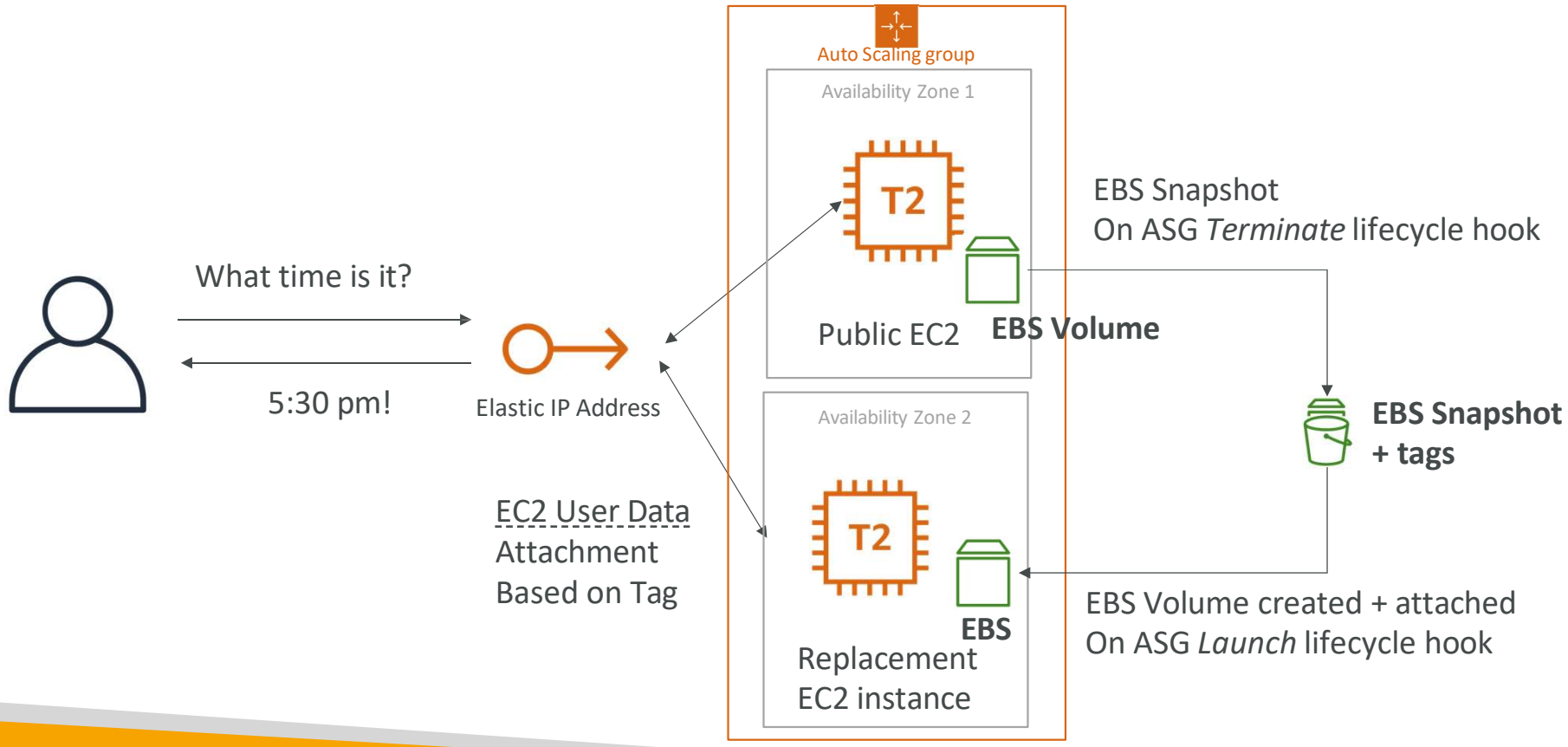
EC2 User Data
Attachment
Based on Tag

ASG Settings
1 min
1 max
1 desired
>= 2 AZ

EC2 user data to attach
The Elastic IP

EC2 instance role to
Allow API calls to attach
The Elastic IP

Creating a highly available EC2 instance With ASG + EBS



Other Services

Overview of Services that might come up in a few questions

What is CloudFormation

- CloudFormation is a declarative way of outlining your AWS Infrastructure, for any resources (most of them are supported).
- For example, within a CloudFormation template, you say:
  - I want a security group
  - I want two EC2 instances using this security group
  - I want an S3 bucket
  - I want a load balancer (ELB) in front of these machines
- Then CloudFormation creates those for you, in the right order, with the exact configuration that you specify

Benefits of AWS CloudFormation (1/2)

- Infrastructure as code
  - No resources are manually created, which is excellent for control
  - Changes to the infrastructure are reviewed through code

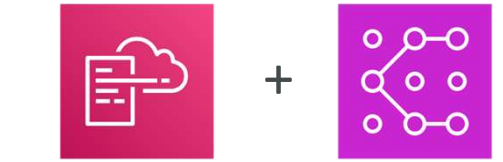
- Cost
  - Each resources within the stack is tagged with an identifier so you can easily see how much a stack costs you
  - You can estimate the costs of your resources using the CloudFormation template
  - Savings strategy: In Dev, you could automation deletion of templates at 5 PM and recreated at 8 AM, safely

Benefits of AWS CloudFormation (2/2)

- Productivity
  - Ability to destroy and re-create an infrastructure on the cloud on the fly
  - Automated generation of Diagram for your templates!
  - Declarative programming (no need to figure out ordering and orchestration)
- Don’t re-invent the wheel
  - Leverage existing templates on the web!
  - Leverage the documentation
- Supports (almost) all AWS resources:
  - Everything we’ll see in this course is supported
  - You can use “custom resources” for resources that are not supported

CloudFormation + Application Composer

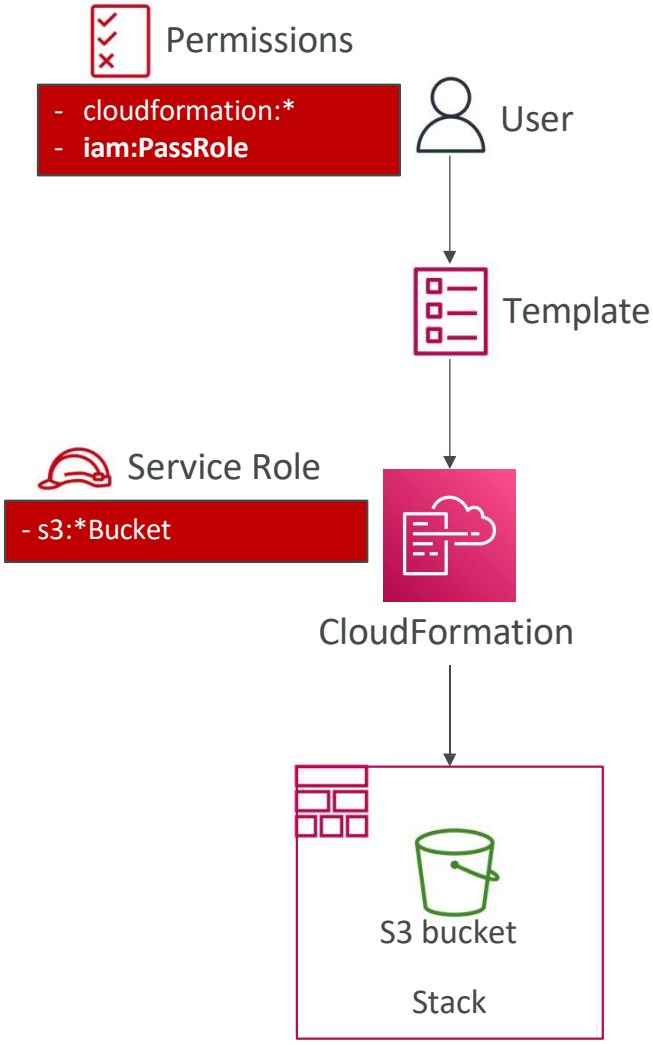
- Example: WordPress CloudFormation Stack



- We can see all the resources
- We can see the relations between the components

CloudFormation – Service Role

- IAM role that allows CloudFormation to create/update/delete stack resources on your behalf
- Give ability to users to create/update/delete the stack resources even if they don't have permissions to work with the resources in the stack
- Use cases:
  - You want to achieve the least privilege principle
  - But you don't want to give the user all the required permissions to create the stack resources
- User must have iam:PassRole permissions



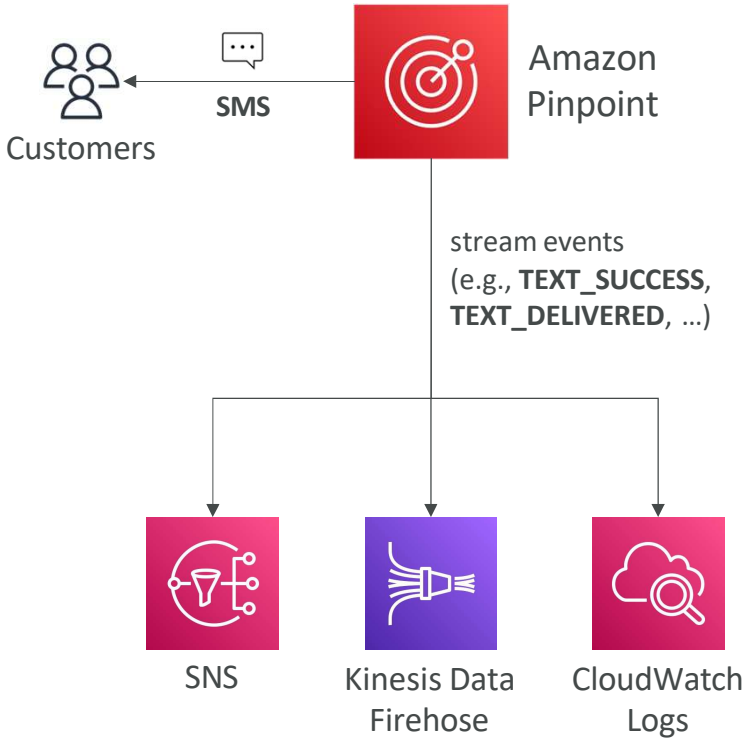
Amazon Simple Email Service (Amazon SES)

- Fully managed service to send emails securely, globally and at scale
- Allows inbound/outbound emails
- Reputation dashboard, performance insights, anti-spam feedback
- Provides statistics such as email deliveries, bounces, feedback loop results, email open
- Supports DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF)
- Flexible IP deployment: shared, dedicated, and customer-owned IPs
- Send emails using your application using AWS Console, APIs, or SMTP

- Use cases: transactional, marketing and bulk email communications

Amazon Pinpoint

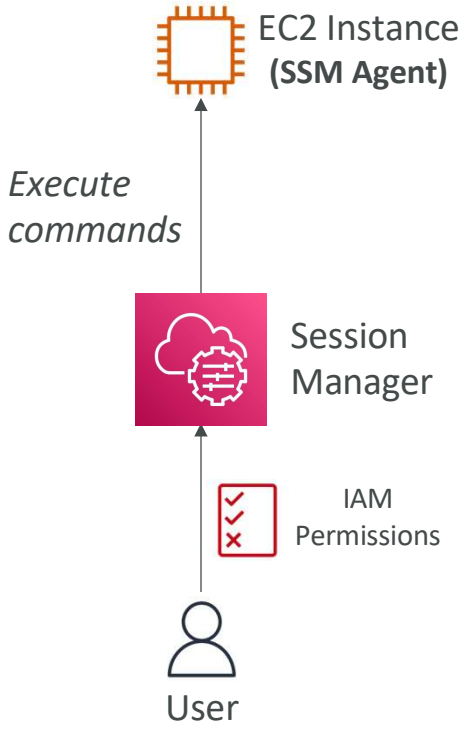
- Scalable 2-way (outbound/inbound) marketing communications service
- Supports email, SMS, push, voice, and in-app messaging
- Ability to segment and personalize messages with the right content to customers
- Possibility to receive replies
- Scales to billions of messages per day
- Use cases: run campaigns by sending marketing, bulk, transactional SMS messages
- Versus Amazon SNS or Amazon SES
  - In SNS & SES you managed each message's audience, content, and delivery schedule
  - In Amazon Pinpoint, you create message templates, delivery schedules, highly-targeted segments, and full campaigns



Systems Manager – SSM Session Manager

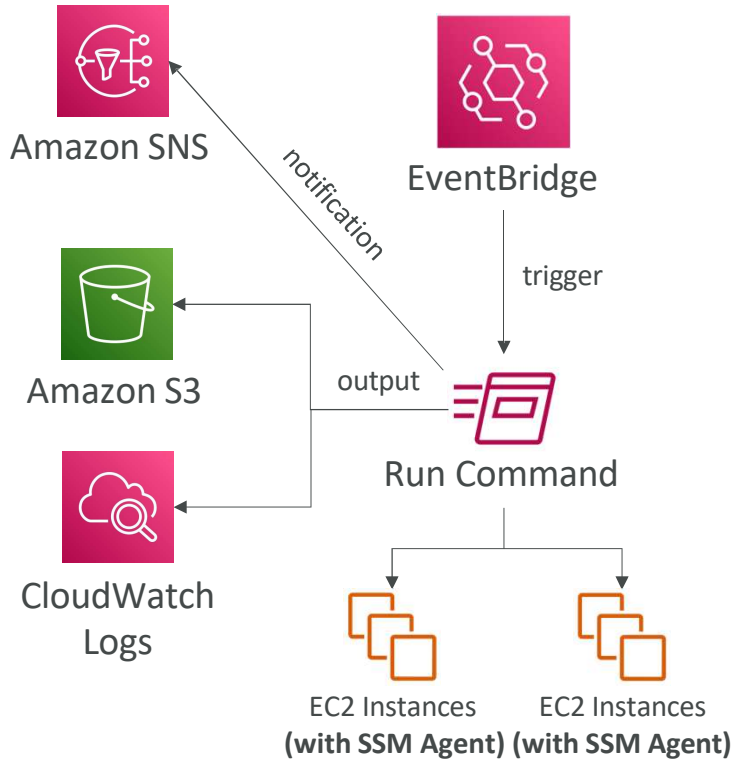
- Allows you to start a secure shell on your EC2 and on-premises servers

- No SSH access, bastion hosts, or SSH keys needed
- No port 22 needed (better security)
- Supports Linux, macOS, and Windows
- Send session log data to S3 or CloudWatch Logs



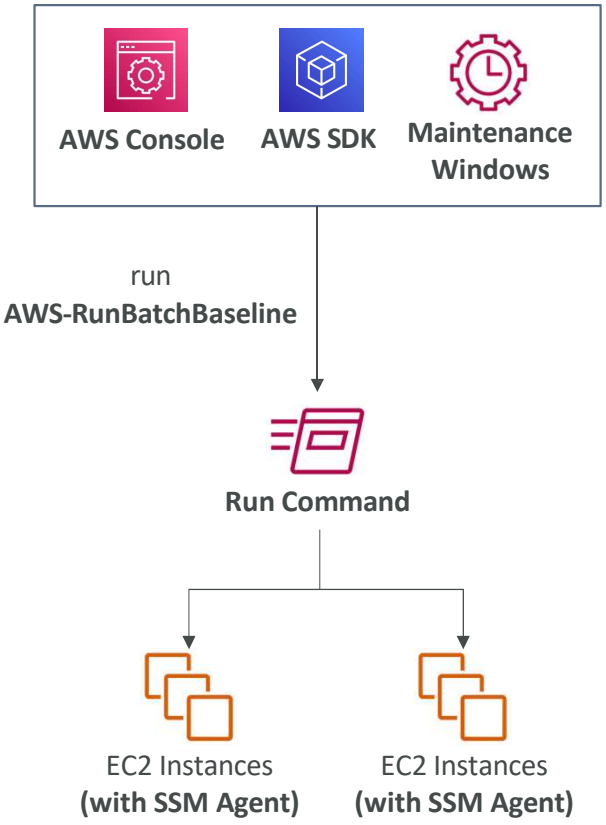
Systems Manager – Run Command

- Execute a document (= script) or just run a command
- Run command across multiple instances (using resource groups)
- No need for SSH
- Command Output can be shown in the AWS Console, sent to S3 bucket or CloudWatch Logs
- Send notifications to SNS about command status (In progress, Success, Failed, ...)
- Integrated with IAM & CloudTrail
- Can be invoked using EventBridge



Systems Manager – Patch Manager

- Automates the process of patching managed instances
- OS updates, applications updates, security updates
- Supports EC2 instances and on-premises servers
- Supports Linux, macOS, and Windows
- Patch on-demand or on a schedule using Maintenance Windows
- Scan instances and generate patch compliance report (missing patches)

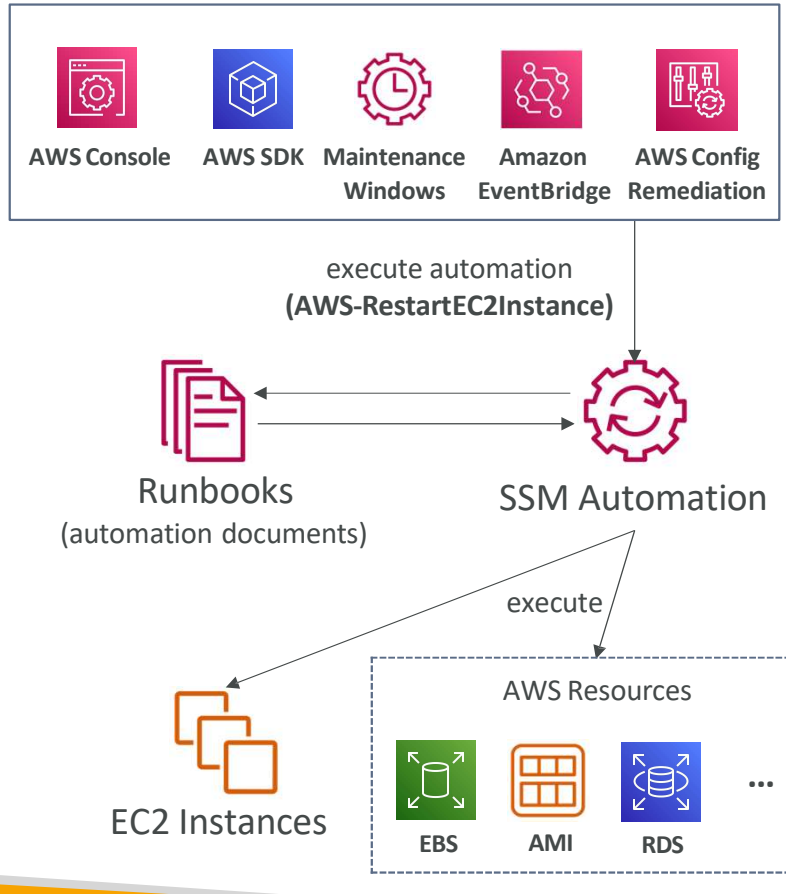


Systems Manager – Maintenance Windows

- Defines a schedule for when to perform actions on your instances
- Example: OS patching, updating drivers, installing software, ...
- Maintenance Window contains
  - Schedule
  - Duration
  - Set of registered instances
  - Set of registered tasks

Systems Manager - Automation

- Simplifies common maintenance and deployment tasks of EC2 instances and other AWS resources
- Examples: restart instances, create an AMI, EBS snapshot
- Automation Runbook - SSM Documents to define actions preformed on your EC2 instances or AWS resources (pre-defined or custom)
- Can be triggered using:
  - Manually using AWS Console, AWS CLI or SDK
  - Amazon EventBridge
  - On a schedule using Maintenance Windows
  - By AWS Config for rules remediations



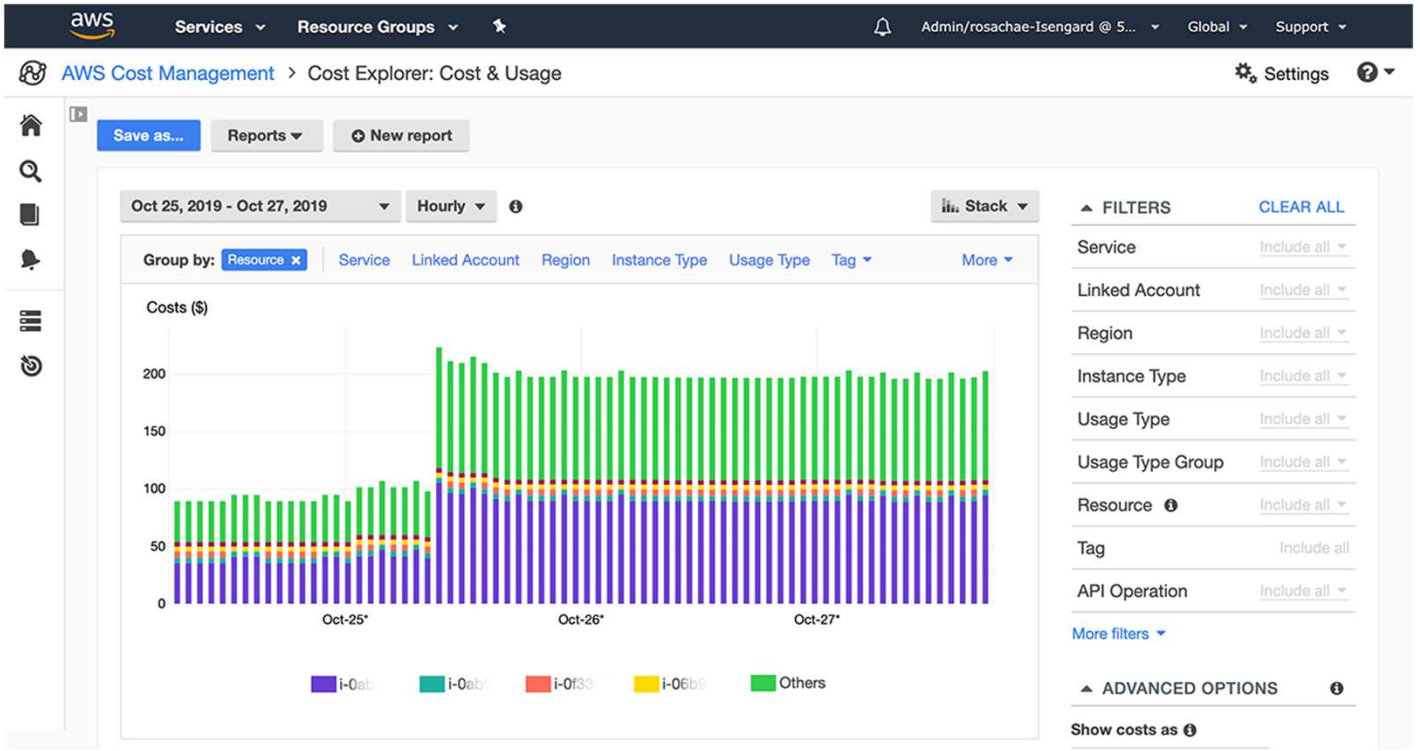
Cost Explorer

- Visualize, understand, and manage your AWS costs and usage over time
- Create custom reports that analyze cost and usage data.
- Analyze your data at a high level: total costs and usage across all accounts
- Or Monthly, hourly, resource level granularity
- Choose an optimal Savings Plan (to lower prices on your bill)
- Forecast usage up to 12 months based on previous usage

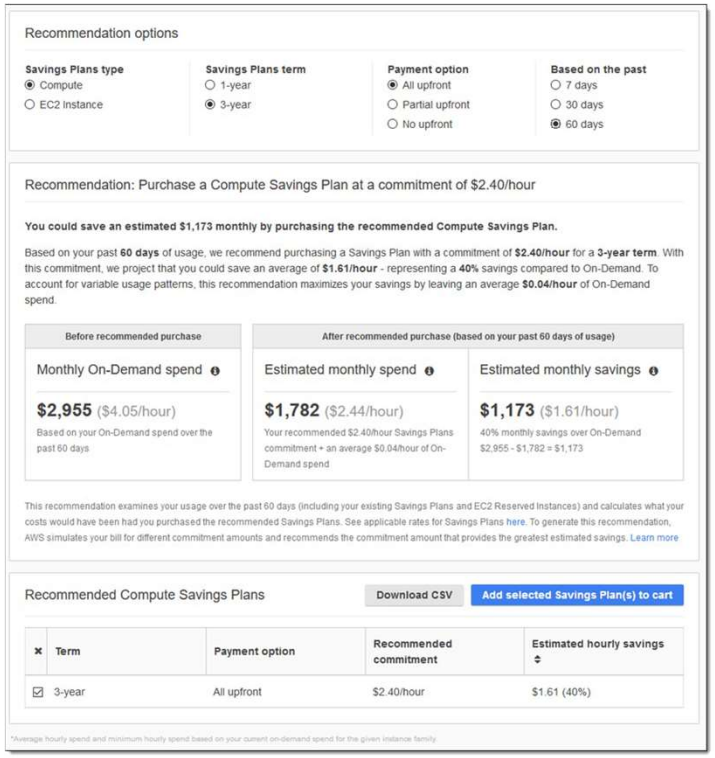
Cost Explorer - Monthly Cost by AWS Service

Instance Type	Oct 1, 2018	Nov 1, 2018	Dec 1, 2018	Jan 1, 2019
Total cost ($)	1,312.71	1,328.54	1,125.99	1,129.65
t2.micro ($)	486.75	475.89	405.63	409.27
c4.2xlarge ($)	296.11	286.56	296.11	296.11

Cost Explorer- Hourly & Resource Level



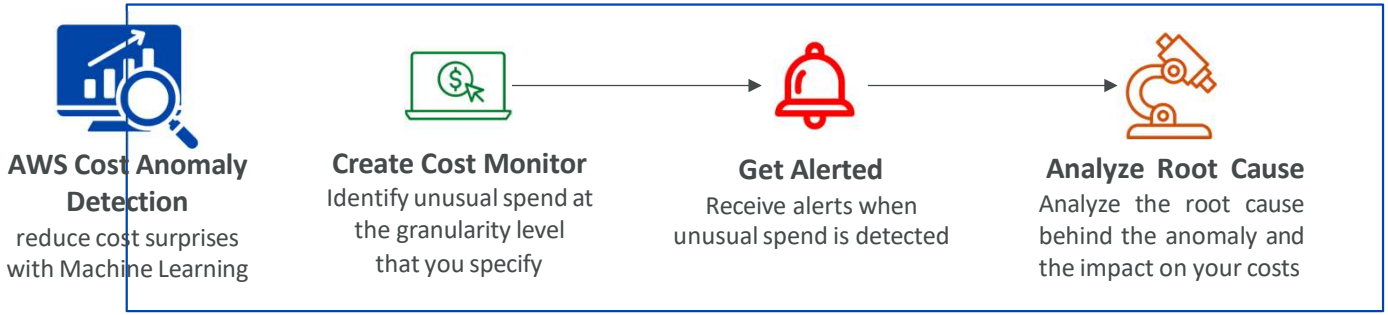
Cost Explorer - Savings Plan Alternative to Reserved Instances



Cost Explorer - Forecast Usage

AWS Cost Anomaly Detection

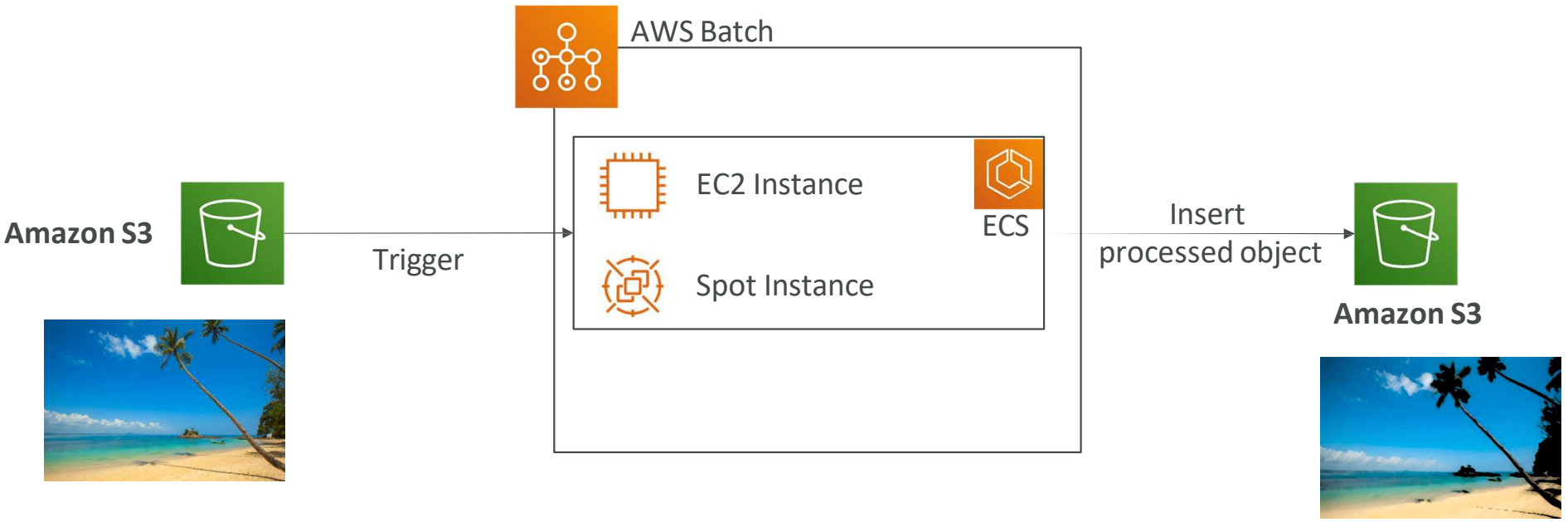
- Continuously monitor your cost and usage using ML to detect unusual spends
- It learns your unique, historic spend patterns to detect one-time cost spike and/or continuous cost increases (you don't need to define thresholds)
- Monitor AWS services, member accounts, cost allocation tags, or cost categories
- Sends you the anomaly detection report with root-cause analysis
- Get notified with individual alerts or daily/weekly summary (using SNS)



AWS Batch

- Fully managed batch processing at any scale
- Efficiently run 100,000s of computing batch jobs on AWS
- A “batch” job is a job with a start and an end (opposed to continuous)
- Batch will dynamically launch EC2 instances or Spot Instances
- AWS Batch provisions the right amount of compute / memory
- You submit or schedule batch jobs and AWS Batch does the rest!
- Batch jobs are defined as Docker images and run on ECS
- Helpful for cost optimizations and focusing less on the infrastructure

AWS Batch - Simplified Example

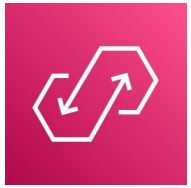


Batch vs Lambda

- Lambda:
  - Time limit
  - Limited runtimes
  - Limited temporary disk space
  - Serverless

- Batch:
  - No time limit
  - Any runtime as long as it's packaged as a Docker image
  - Rely on EBS / instance store for disk space
  - Relies on EC2 (can be managed by AWS)

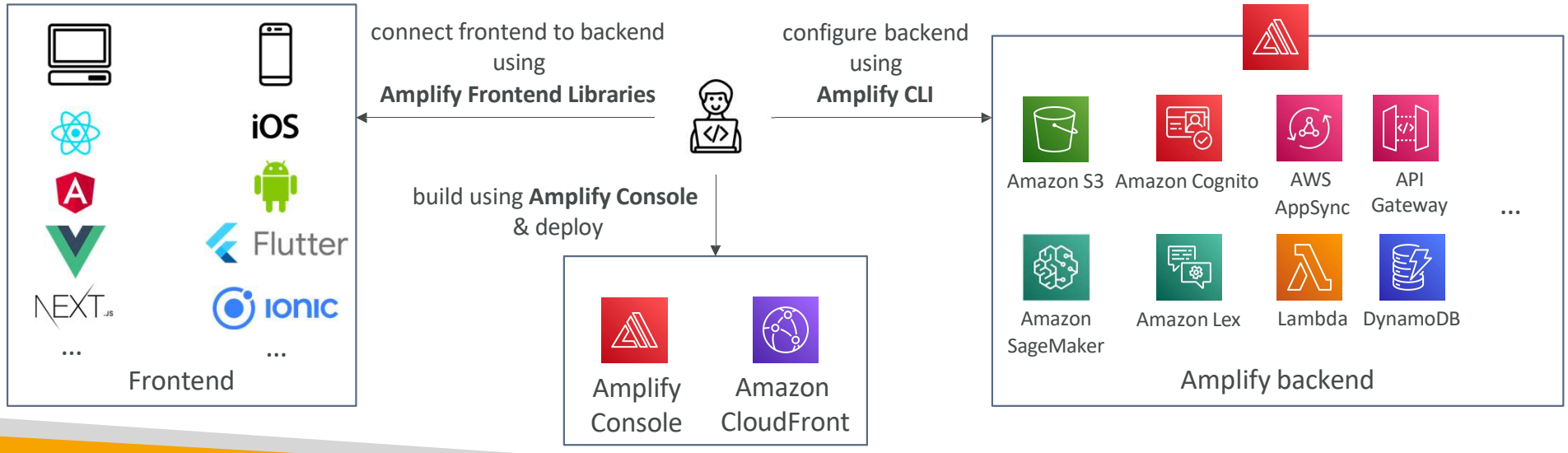
Amazon AppFlow



- Fully managed integration service that enables you to securely transfer data between Software-as-a-Service (SaaS) applications and AWS
- Sources: Salesforce, SAP, Zendesk, Slack, and ServiceNow
- Destinations: AWS services like Amazon S3, Amazon Redshift or non-AWS such as SnowFlake and Salesforce
- Frequency: on a schedule, in response to events, or on demand
- Data transformation capabilities like filtering and validation
- Encrypted over the public internet or privately over AWS PrivateLink
- Don't spend time writing the integrations and leverage APIs immediately

AWS Amplify - web and mobile applications

- A set of tools and services that helps you develop and deploy scalable full stack web and mobile applications
- Authentication, Storage, API (REST, GraphQL), CI/CD, PubSub, Analytics, AI/ML Predictions, Monitoring, ...
- Connect your source code from GitHub, AWS CodeCommit, Bitbucket, GitLab, or upload directly



White Papers & Architectures

Well Architected Framework, Disaster Recovery, etc...

Section Overview

- Well Architected Framework Whitepaper
- Well Architected Tool
- AWS Trusted Advisor
- Reference architectures resources (for real-world)
- Disaster Recovery on AWS Whitepaper

Well Architected Framework
General Guiding Principles

- https://aws.amazon.com/architecture/well-architected
- Stop guessing your capacity needs
- Test systems at production scale
- Automate to make architectural experimentation easier
- Allow for evolutionary architectures
  - Design based on changing requirements
- Drive architectures using data
- Improve through game days
  - Simulate applications for flash sale days

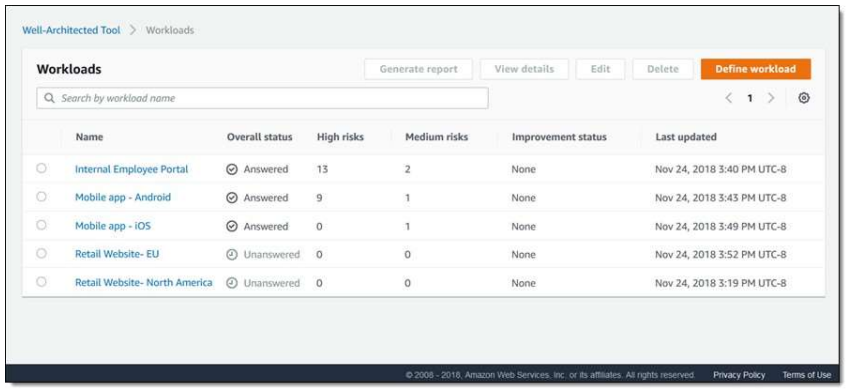
Well Architected Framework
6 Pillars

- 1) Operational Excellence
- 2) Security
- 3) Reliability
- 4) Performance Efficiency
- 5) Cost Optimization
- 6) Sustainability

- They are not something to balance, or trade-offs, they're a synergy

AWS Well-Architected Tool

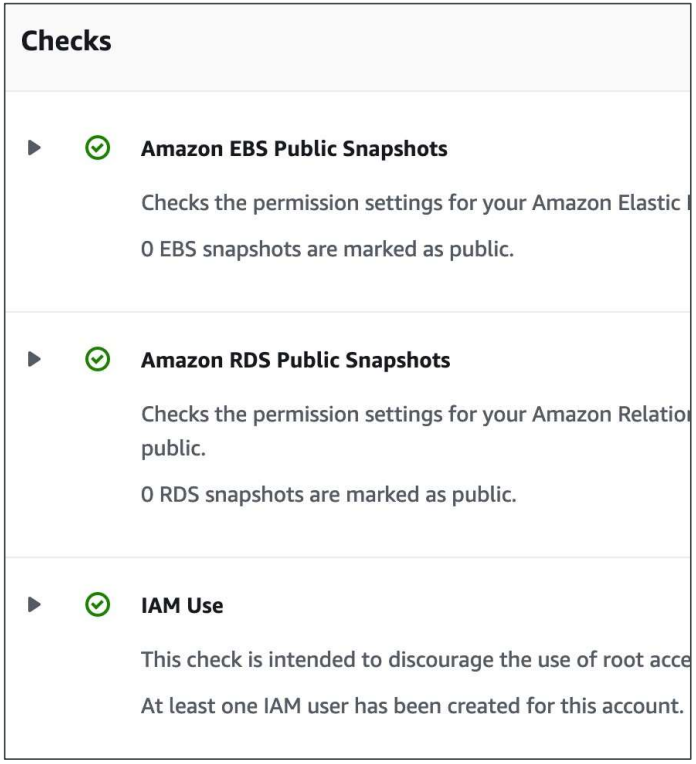
- Free tool to review your architectures against the 6 pillars Well-Architected Framework and adopt architectural best practices
- How does it work?
  - Select your workload and answer questions
  - Review your answers against the 6 pillars
  - Obtain advice: get videos and documentations, generate a report, see the results in a dashboard
- Let's have a look: https://console.aws.amazon.com/wellarchitected



https://aws.amazon.com/blogs/aws/new-aws-well-architected-tool-review-workloads-against-best-practices/

Trusted Advisor

- No need to install anything - high level AWS account assessment
- Analyze your AWS accounts and provides recommendation on 6 categories:
  - Cost optimization
  - Performance
  - Security
  - Fault tolerance
  - Service limits
  - Operational Excellence
- Business & Enterprise Support plan
  - Full Set of Checks
  - Programmatic Access using AWS Support API



More Architecture Examples

- We've explored the most important architectural patterns:
  - Classic: EC2, ELB, RDS, ElastiCache, etc...
  - Serverless: S3, Lambda, DynamoDB, CloudFront, API Gateway, etc...

- If you want to see more AWS architectures:
- https://aws.amazon.com/architecture/
- https://aws.amazon.com/solutions/