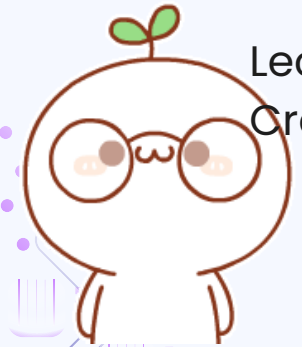
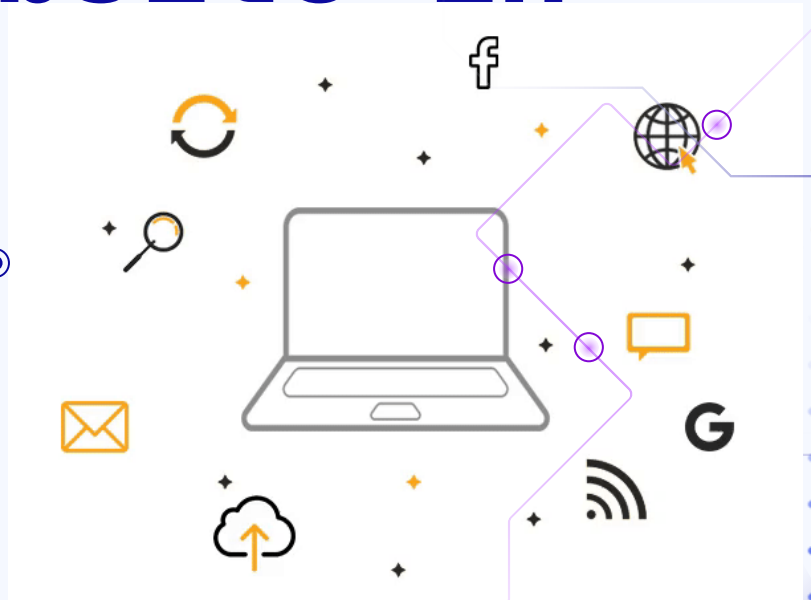
Deploying E-Commerce Website in AWS



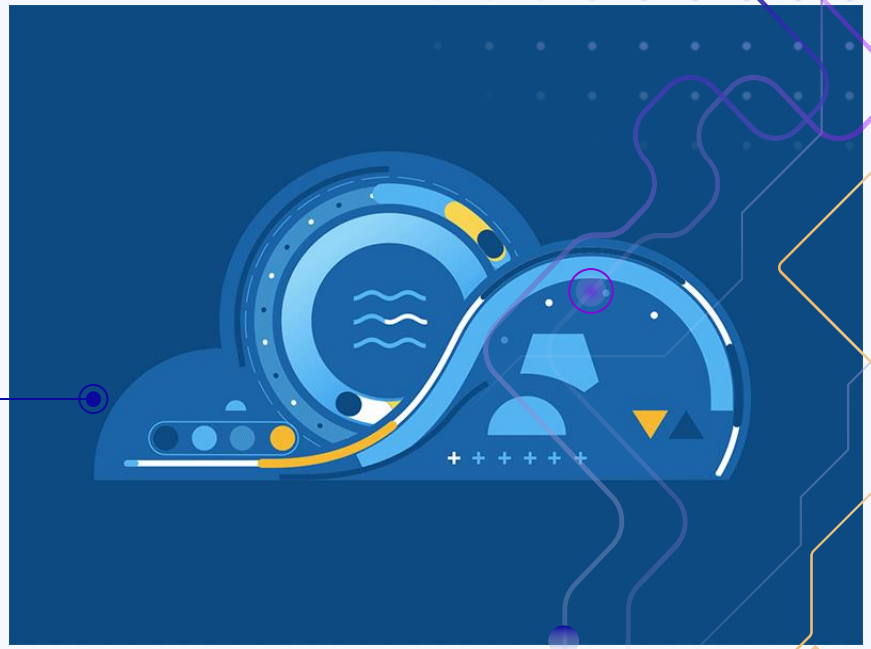


Lecturer: Dr.Phan Xuân Thiện
Created by Group 2

Table of contents

01

Introduction



Brief introduction of AWS and its relevance for e-commerce

AWS defines

AWS is a cloud service provided by Amazon that allows organizations to build and manage online applications operationally and efficiently.

AWS is the largest and most popular cloud platform in the world, with a wide range of services and resources available to support a wide range of applications.

Founding:

AWS was officially launched in 2006 and has since grown rapidly.

Service Career Diversity:

The platform includes high-value services, from servers to storage and artificial intelligence.

Why is AWS Important for E-Commerce?

Flexible

AWS offers a range of customizable services to meet the specific needs of e-commerce businesses.

Extend

Based on cloud infrastructure, e-commerce can scale without having to invest in hardware.

Security and Trust

Business-level security

AWS provides industry-leading security standards and tools to protect customer data and transactions.

Reliability and Performance

AWS cloud services help ensure high availability and stable performance for web e-commerce.

Special Service For E-Commerce

Amazon EC2 and S3:

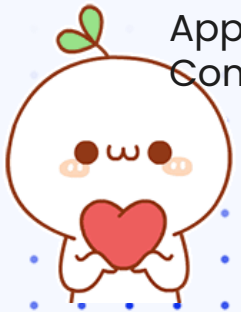
Use EC2 for Virtual servers and S3 for data storage, providing a powerful platform for e-commerce websites.

AWS Lambda and API Gateway:

Use Lambda and API Gateway to build fast-acting and responsive systems for your e-commerce applications.

02 Using AWS Services

Apply AWS Services for E-Commerce Website



Infrastructure Analysis

A. Amazon EC2 (Elastic Compute Cloud)

Describe:

Use EC2 to deploy virtual servers that are flexible, scalable, and optimized for performance.

Advantage:

Provides a scalable compute environment that responds well to traffic fluctuations.

Infrastructure Analysis

B. Amazon S3 (Simple Storage Service)
Describe:

Use S3 to store and manage data, images, and documents.

Advantage:

Unlimited storage, fault tolerance, and easy integration with other services.

Security and Account Management

A. AWS Identity and Access Management (IAM)
Describe:

Use IAM to manage user access and identity.

Advantage:

Securely control and automate availability and rights management processes.

Security and Account Management

B. AWS Virtual Private Cloud (VPC)
Describe:

Provides control over a virtual networking environment, including selection of IP address range, creation of subnets, and configuration of route tables and network gateways.

Advantage:

Leverage cloud-based applications full potential in terms of security, flexibility, and integration capabilities

Security and Account Management

C. AWS CloudWatch

Describe:

Use CloudWatch to monitor and manage resources.

Advantage:

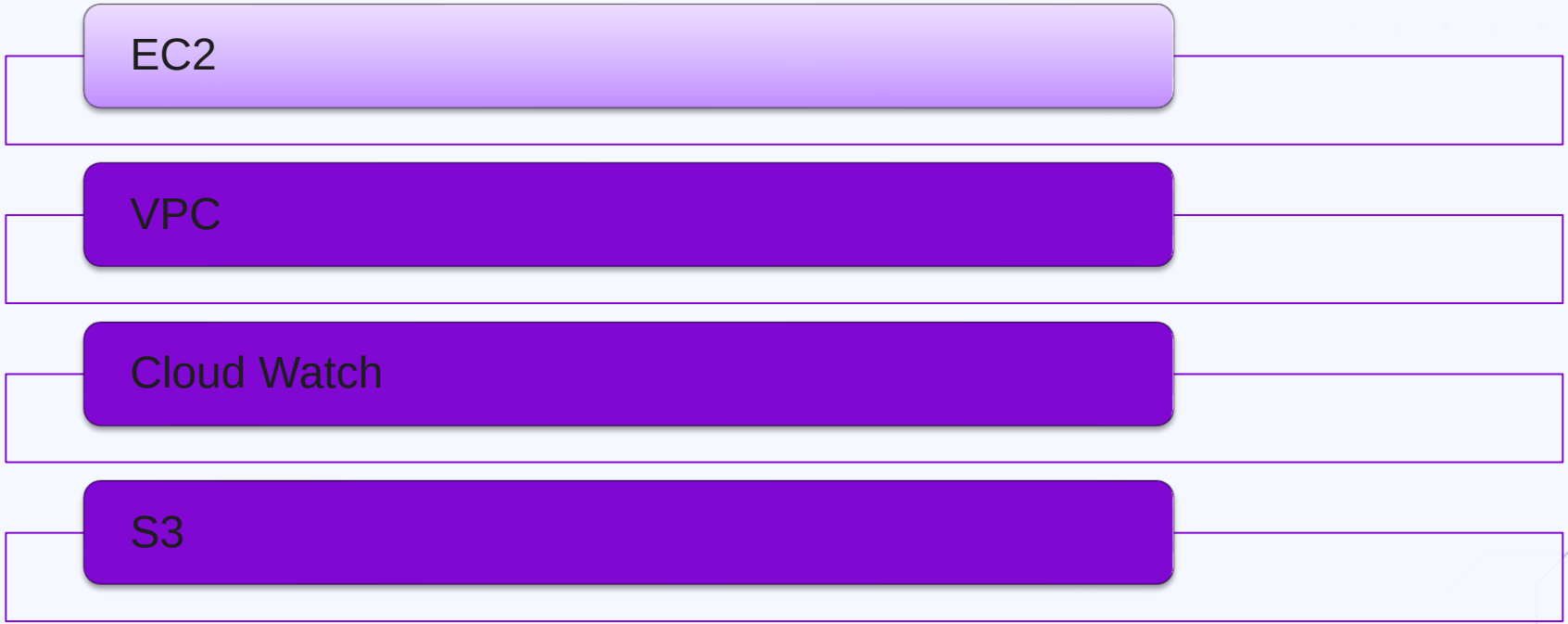
Monitor performance, store logs, and crash alerts to keep your website running smoothly.

03 Deployment Strategy

Step-by-step process for deploying E-Commerce Web to AWS

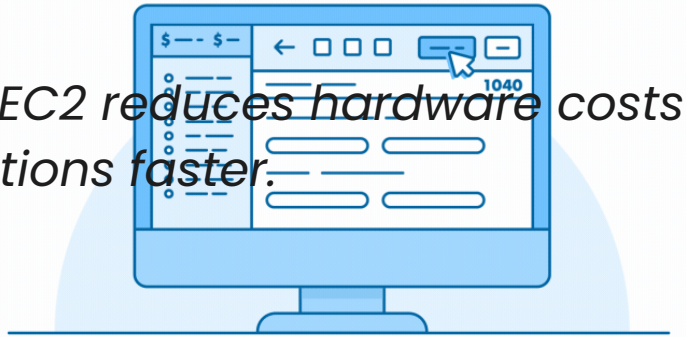
Flowchart of E-Commerce Website

Flowchart of E-Commerce Website



Amazon Elastic Compute Cloud (Amazon EC2)

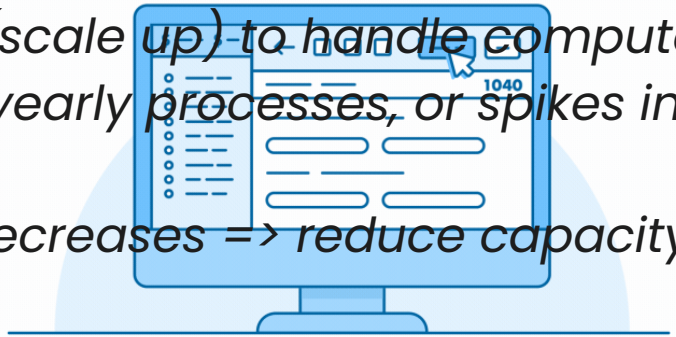
- *Amazon Elastic Compute Cloud (Amazon EC2) provides on-demand, scalable computing capacity in the Amazon Web Services (AWS) Cloud.*

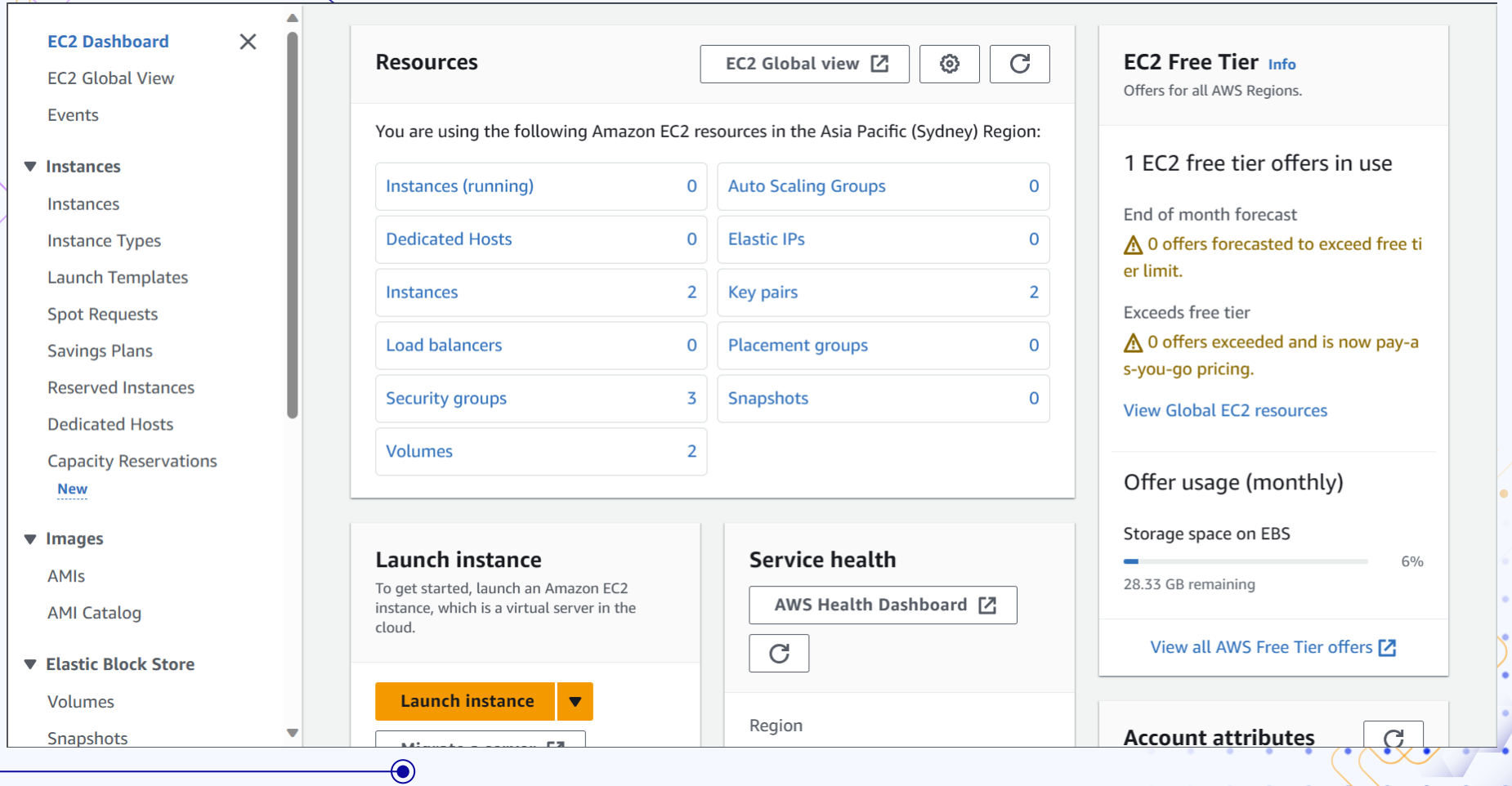


- *Using Amazon EC2 reduces hardware costs =>can develop and deploy applications faster.*

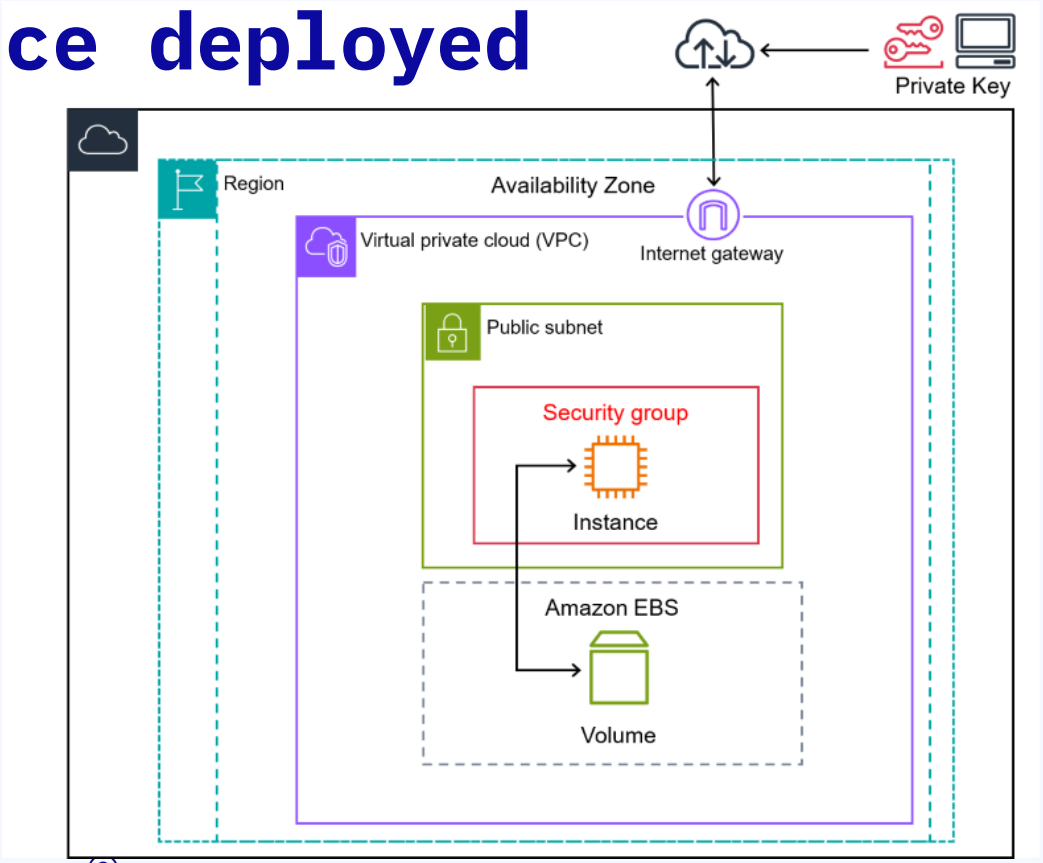
Amazon Elastic Compute Cloud (Amazon EC2)

- *Use Amazon EC2 to launch as many or as few virtual servers, configure security and networking, and manage storage.*
- *Add capacity (scale up) to handle compute-heavy tasks, such as monthly or yearly processes, or spikes in website traffic.*
- *When usage decreases => reduce capacity (scale down) again.*

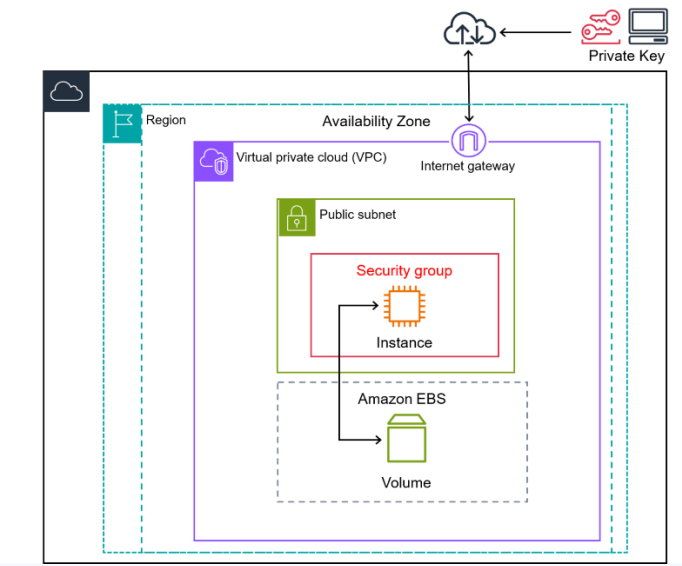



EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
New
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Resources
EC2 Global view
You are using the following Amazon EC2 resources in the Asia Pacific (Sydney) Region:
Instances (running) 0
Auto Scaling Groups 0
Dedicated Hosts 0
Elastic IPs 0
Instances 2
Key pairs 2
Load balancers 0
Placement groups 0
Security groups 3
Snapshots 0
Volumes 2
Launch instance
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
Launch instance
Service health
AWS Health Dashboard
Region
EC2 Free Tier Info
Offers for all AWS Regions.
1 EC2 free tier offers in use
End of month forecast
0 offers forecasted to exceed free tier limit.
Exceeds free tier
0 offers exceeded and is now pay-as-you-go pricing.
View Global EC2 resources
Offer usage (monthly)
Storage space on EBS
6%
28.33 GB remaining
View all AWS Free Tier offers
Account attributes

Basic architecture of an Amazon EC2 instance deployed

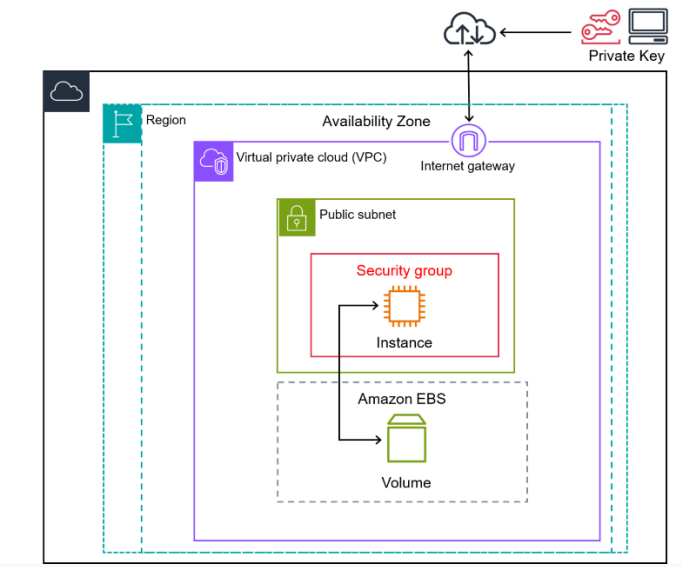


Basic architecture of an Amazon EC2 instance deployed



- The following diagram shows a basic architecture of an Amazon EC2 instance deployed within an Amazon Virtual Private Cloud (VPC).
- In this example, the EC2 instance is within an Availability Zone in the Region.
- The EC2 instance is secured with a security group, which is a virtual firewall that controls incoming and outgoing traffic.
- A private key is stored on the local computer and a public key is stored on the instance.

Basic architecture of an Amazon EC2 instance deployed



- Both keys are specified as a key pair to prove the identity of the user.
- In this scenario, the instance is backed by an Amazon EBS volume.
- The VPC communicates with the internet using an internet gateway
- Amazon EC2 supports the processing, storage, and transmission of credit card data by a merchant or service provider, and has been validated as being compliant with Payment Card Industry (PCI) Data Security Standard (DSS).

Network settings Info

Edit

Network Info

vpc-0ad35e8f259717228

Subnet Info

No preference (Default subnet in any availability zone)

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

- (•) Create security group
- ( ) Select existing security group

We'll create a new security group called '**launch-wizard-3**' with the following rules:

- [x] Allow SSH traffic from
  Helps you connect to your instance
  Anywhere
  0.0.0.0/0
- [ ] Allow HTTPS traffic from the internet
  To set up an endpoint, for example when creating a web server
- [ ] Allow HTTP traffic from the internet
  To set up an endpoint, for example when creating a web server

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Features of Amazon EC2

Instances	• Virtual servers.
Amazon Machine Images (AMIs)	• Preconfigured templates for your instances that package the components you need for your server (including the operating system and additional software).
Instance types	• Various configurations of CPU, memory, storage, networking capacity, and graphics hardware for your instances.
Key pairs	• Secure login information for your instances. AWS stores the public key and you store the private key in a secure place.

Features of Amazon EC2

Instance store volumes	• Storage volumes for temporary data that is deleted when you stop, hibernate, or terminate your instance.
Amazon EBS volumes	• Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS).
Regions, Availability Zones, Local Zones, AWS Outposts, and Wavelength Zones	• Multiple physical locations for your resources, such as instances and Amazon EBS volumes.

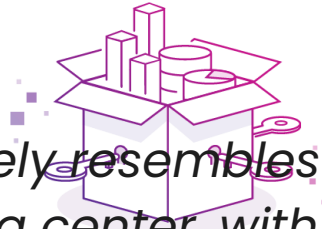
Features of Amazon EC2

Security groups	• A virtual firewall that allows you to specify the protocols, ports, and source IP ranges that can reach your instances, and the destination IP ranges to which your instances can connect.
Elastic IP addresses	• Static IPv4 addresses for dynamic cloud computing.
Tags	• Metadata that you can create and assign to your Amazon EC2 resources.
Virtual private clouds (VPCs)	• Virtual networks you can create that are logically isolated from the rest of the AWS Cloud. You can optionally connect these virtual networks to your own network.

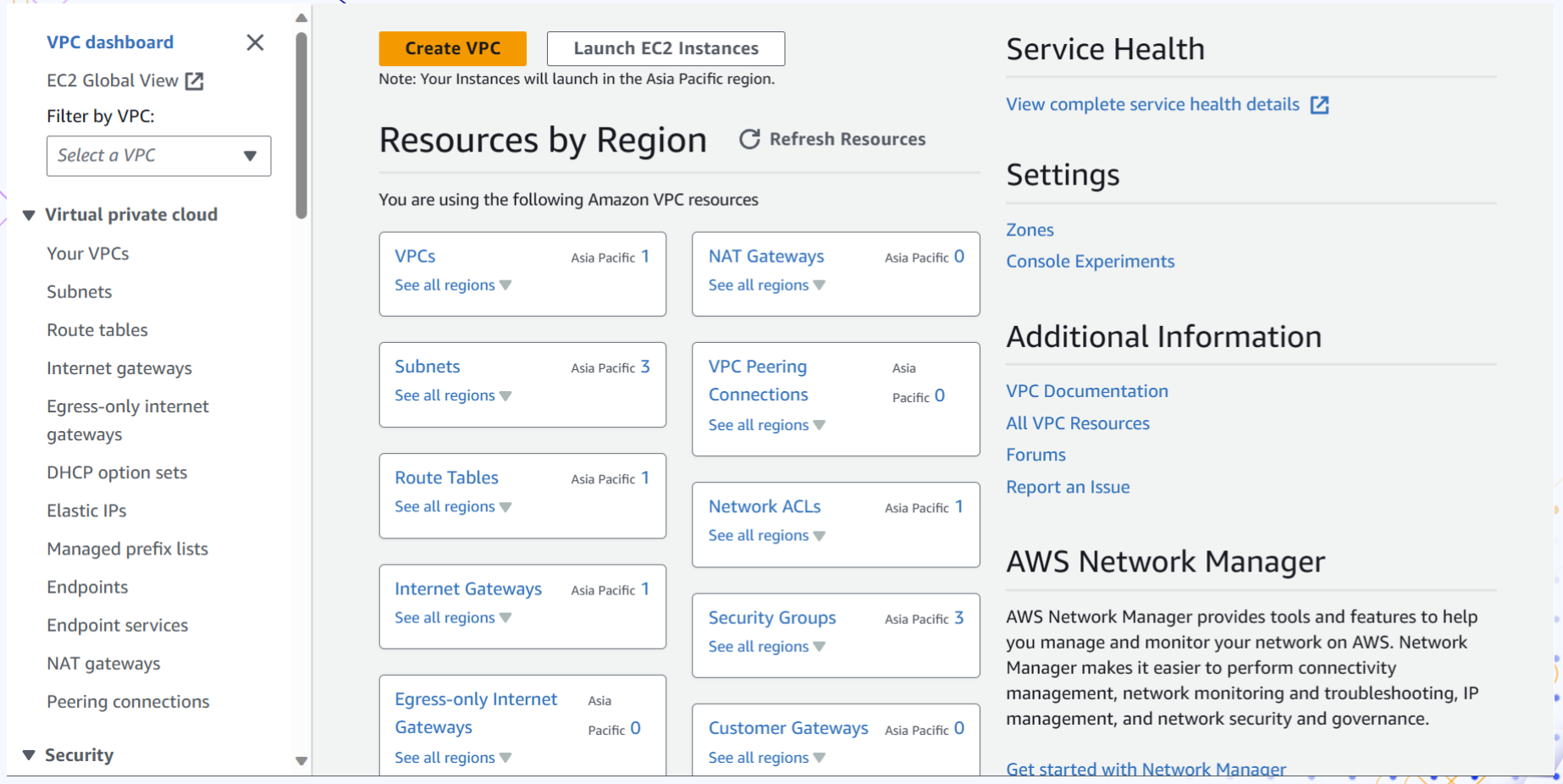
Flowchart of E-Commerce Website

Amazon VPC?

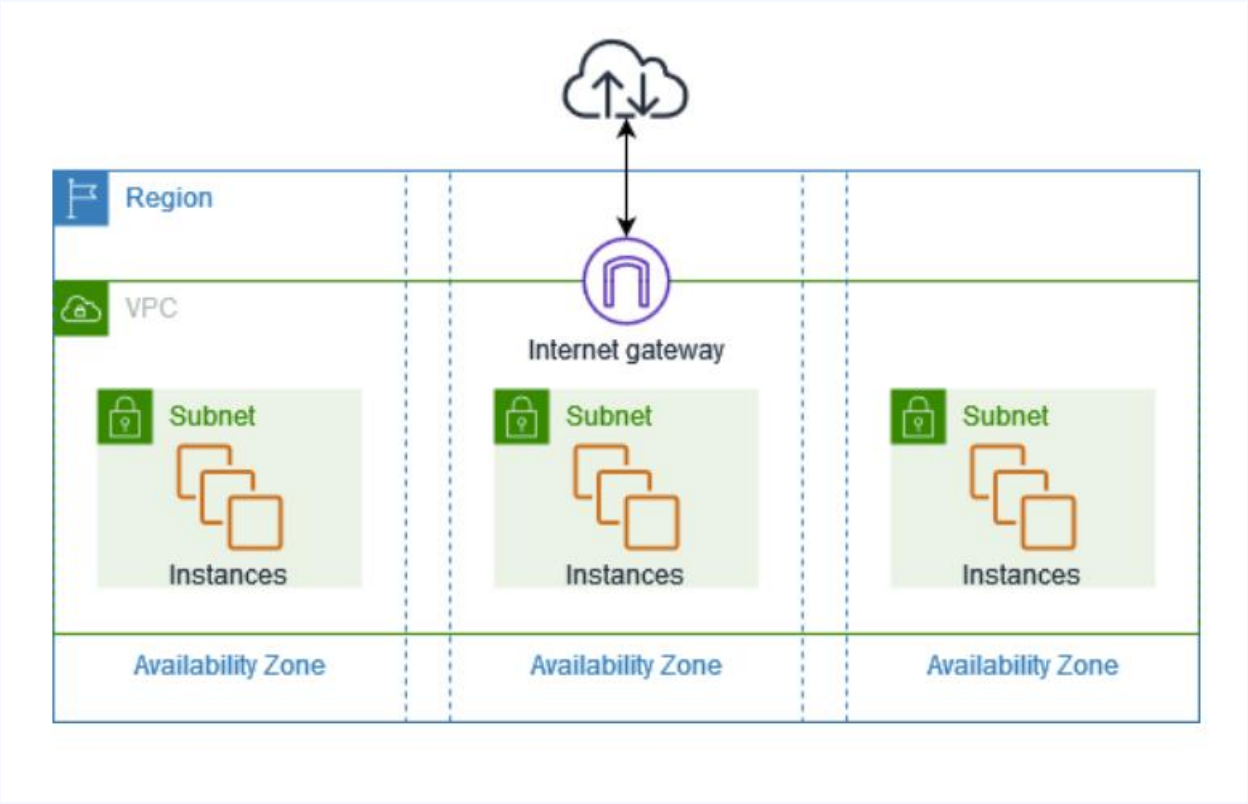
- *With Amazon Virtual Private Cloud (Amazon VPC), => launch AWS resources in a logically isolated virtual network that you've defined.*



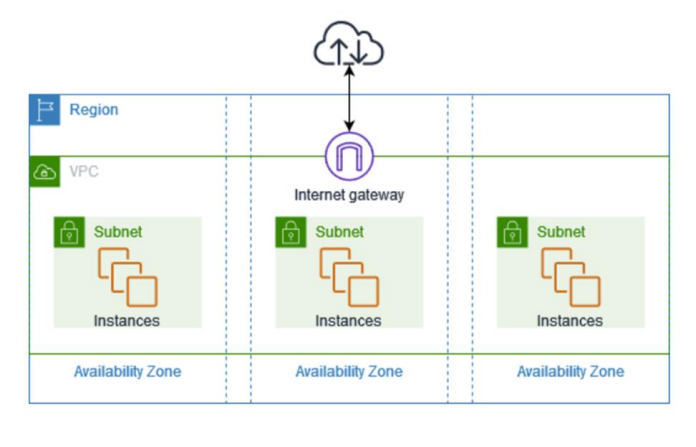
- *This virtual network closely resembles a traditional network => operate in your own data center, with the benefits of using the scalable infrastructure of AWS.*


VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Create VPC
Launch EC2 Instances
Note: Your Instances will launch in the Asia Pacific region.
Resources by Region
Refresh Resources
You are using the following Amazon VPC resources
VPCs Asia Pacific 1
See all regions
NAT Gateways Asia Pacific 0
See all regions
Subnets Asia Pacific 3
See all regions
VPC Peering Connections Asia Pacific 0
See all regions
Route Tables Asia Pacific 1
See all regions
Network ACLs Asia Pacific 1
See all regions
Internet Gateways Asia Pacific 1
See all regions
Security Groups Asia Pacific 3
See all regions
Egress-only Internet Gateways Asia Pacific 0
See all regions
Customer Gateways Asia Pacific 0
See all regions
Service Health
View complete service health details
Settings
Zones
Console Experiments
Additional Information
VPC Documentation
All VPC Resources
Forums
Report an Issue
AWS Network Manager
AWS Network Manager provides tools and features to help you manage and monitor your network on AWS. Network Manager makes it easier to perform connectivity management, network monitoring and troubleshooting, IP management, and network security and governance.
Get started with Network Manager

Architecture VPC With EC2

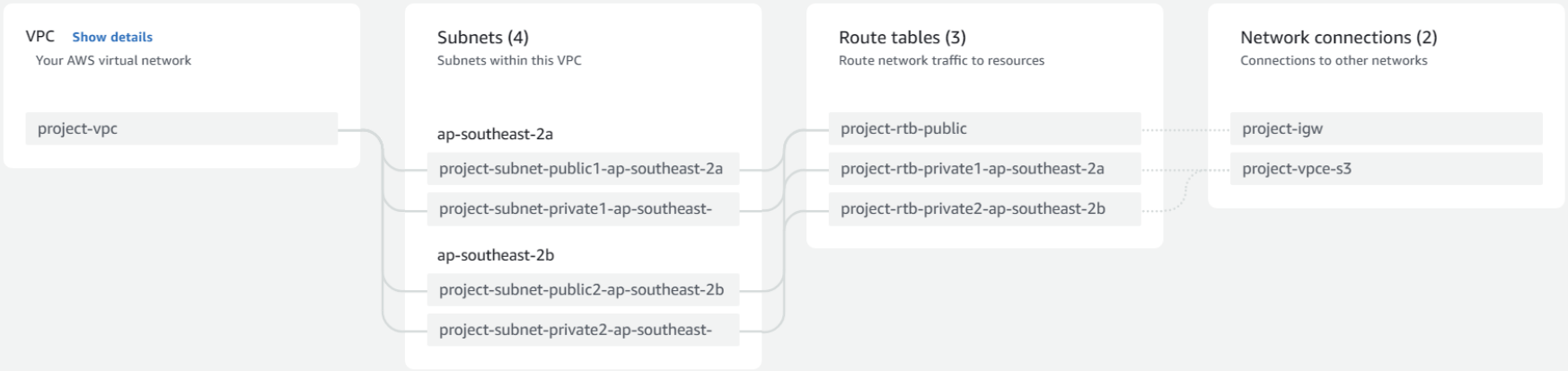


Basic architecture of an Amazon EC2 instance deployed



- The VPC has one subnet in each of the Availability Zones in the Region, EC2 instances in each subnet, and an internet gateway to allow communication between the resources in your VPC and the internet.

Preview


VPC
Show details
Your AWS virtual network
project-vpc
Subnets (4)
Subnets within this VPC
ap-southeast-2a
project-subnet-public1-ap-southeast-2a
project-subnet-private1-ap-southeast-
ap-southeast-2b
project-subnet-public2-ap-southeast-2b
project-subnet-private2-ap-southeast-
Route tables (3)
Route network traffic to resources
project-rtb-public
project-rtb-private1-ap-southeast-2a
project-rtb-private2-ap-southeast-2b
Network connections (2)
Connections to other networks
project-igw
project-vpce-s3

Features of Amazon VPC

Virtual private clouds (VPC)	• A VPC is a virtual network that closely resembles a traditional network that you'd operate in your own data center. After you create a VPC, you can add subnets.
Subnets	• A subnet is a range of IP addresses in your VPC. A subnet must reside in a single Availability Zone. After you add subnets, you can deploy AWS resources in your VPC.
IP addressing	• You can assign IP addresses, both IPv4 and IPv6, to your VPCs and subnets. You can also bring your public IPv4 and IPv6 GUA addresses to AWS and allocate them to resources in your VPC, such as EC2 instances, NAT gateways, and Network Load Balancers.
Routing	• Use route tables to determine where network traffic from your subnet or gateway is directed.

Features of Amazon VPC

Gateways and endpoints

- A gateway connects your VPC to another network. For example, use an internet gateway to connect your VPC to the internet. Use a VPC endpoint to connect to AWS services privately, without the use of an internet gateway or NAT device.

Peering connections

- Use a VPC peering connection to route traffic between the resources in two VPCs.

Traffic Mirroring

- Copy network traffic from network interfaces and send it to security and monitoring appliances for deep packet inspection.

Features of Amazon VPC

Transit gateways

- Use a transit gateway, which acts as a central hub, to route traffic between your VPCs, VPN connections, and AWS Direct Connect connections.

VPC Flow Logs

- A flow log captures information about the IP traffic going to and from network interfaces in your VPC.

VPN connections

- Connect your VPCs to your on-premises networks using AWS Virtual Private Network (AWS VPN).

Flowchart of E-Commerce Website

Amazon CloudWatch

- *Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real time.*

- *Use CloudWatch to collect and track metrics, which are variables you can measure for your resources and applications.*

Amazon CloudWatch

- *The CloudWatch home page automatically displays metrics about every AWS service you use.*

- *Create custom dashboards to display metrics about your custom applications, and display custom collections of metrics that you choose.*

Amazon CloudWatch

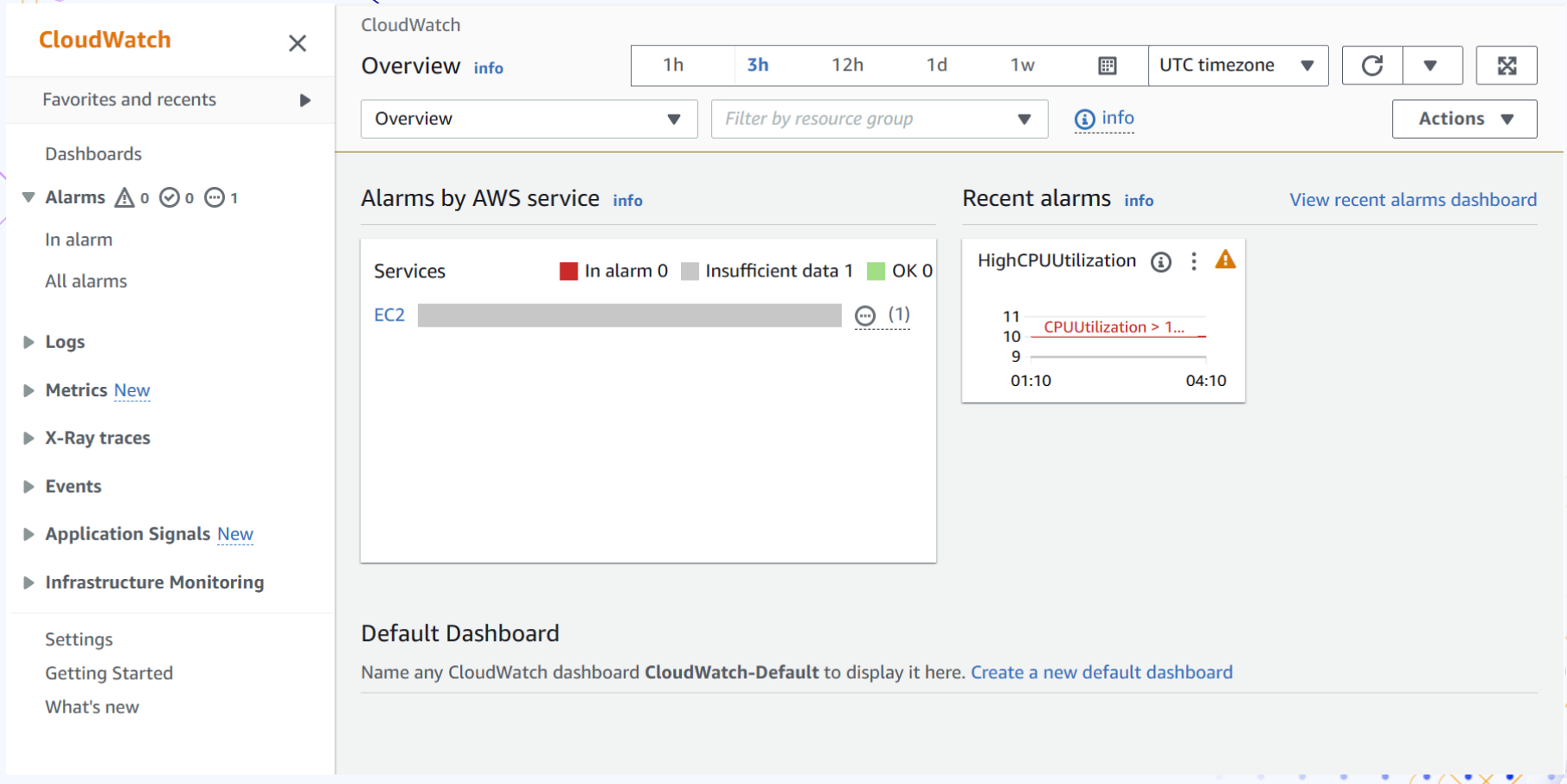
- You can create alarms that watch metrics and send notifications or automatically make changes to the resources you are monitoring when a threshold is breached.

- For example, you can monitor the CPU usage and disk reads and writes of your Amazon EC2 instances and then use that data to determine whether you should launch additional instances to handle increased load.

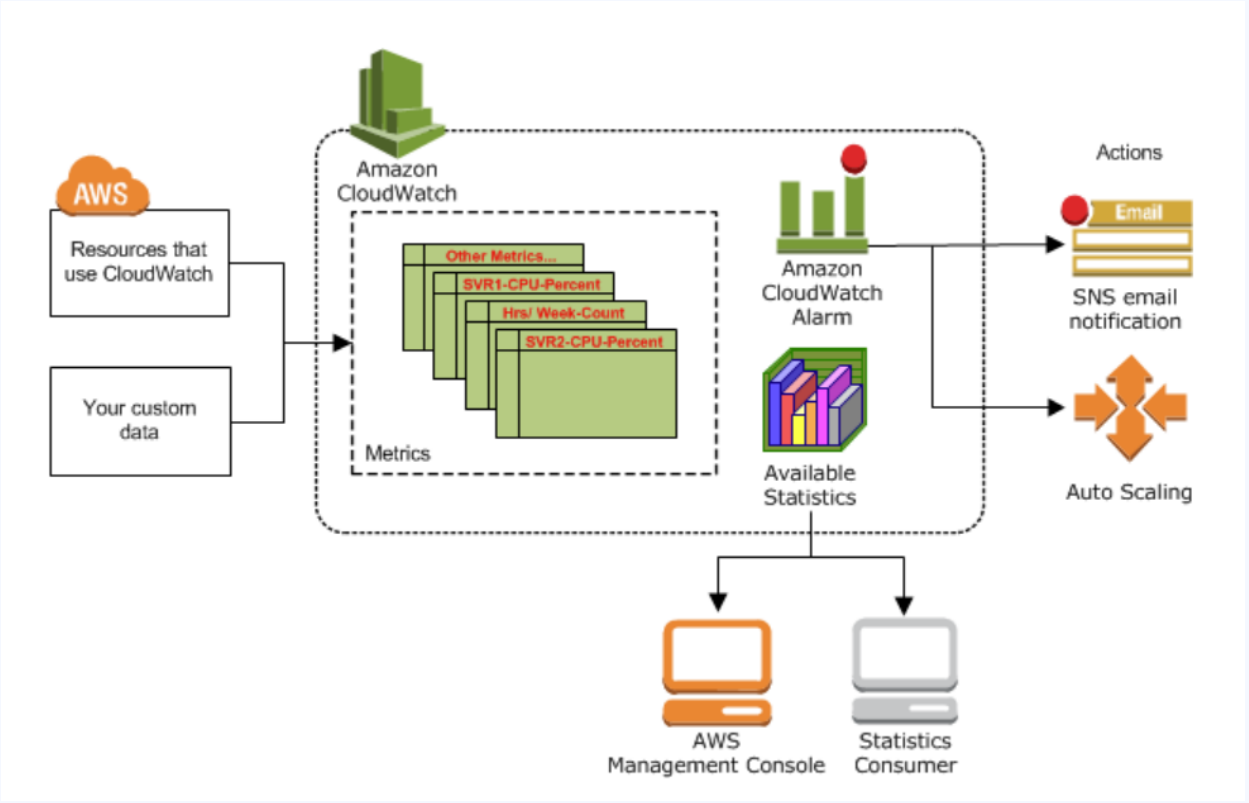
Amazon CloudWatch

- You can also use this data to stop under-used instances to save money.

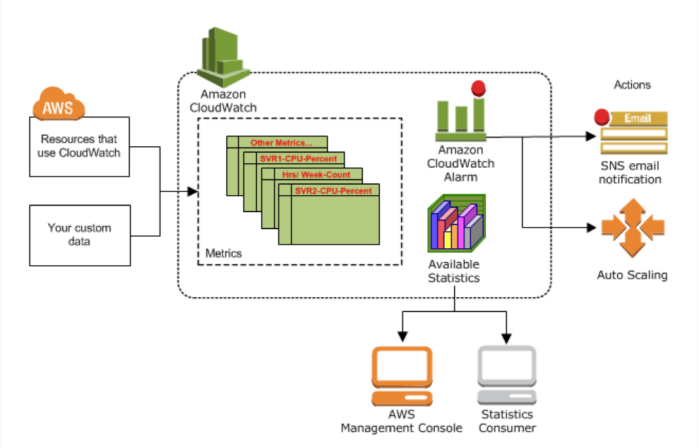
- With CloudWatch, you gain system-wide visibility into resource utilization, application performance, and operational health.


CloudWatch
Favorites and recents
Dashboards
Alarms 0 0 1
In alarm
All alarms
Logs
Metrics New
X-Ray traces
Events
Application Signals New
Infrastructure Monitoring
Settings
Getting Started
What's new
CloudWatch
Overview info
1h
3h
12h
1d
1w
UTC timezone
Overview
Filter by resource group
info
Actions
Alarms by AWS service info
Services
In alarm 0
Insufficient data 1
OK 0
EC2
(1)
Recent alarms info
View recent alarms dashboard
HighCPUUtilization
11
10
9
CPUUtilization > 1...
01:10
04:10
Default Dashboard
Name any CloudWatch dashboard CloudWatch-Default to display it here. Create a new default dashboard

How Amazon CloudWatch works



Basic architecture of an Amazon EC2 instance deployed



- 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.

Specify metric and conditions

Metric

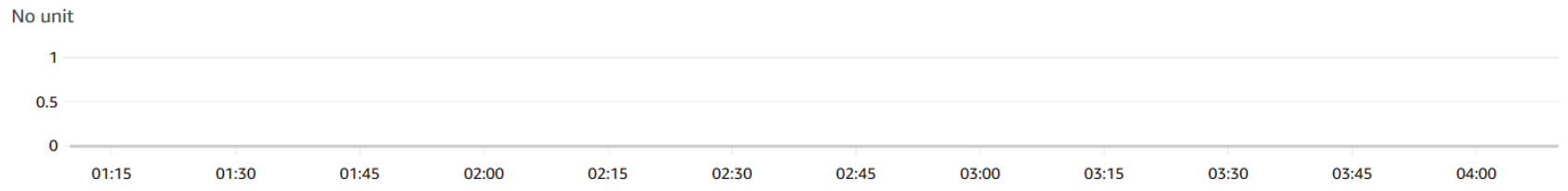
Graph

Preview of the metric or metric expression and the alarm threshold.

Select metric

Cancel Next

Select metric



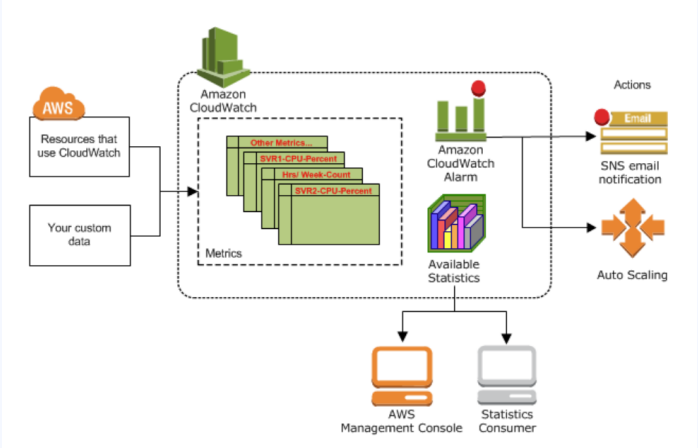
Browse | Multi source query - *new* | Graphed metrics (1) | Options | Source

Add math ▼ | Add query ▼

☐	i-0be11dde342ef1ced	DiskReadBytes ⓘ	No alarms
☐	i-0be11dde342ef1ced	NetworkOut ⓘ	No alarms
☑	i-0be11dde342ef1ced	CPUUtilization ⓘ	1 alarm(s)
☐	i-0be11dde342ef1ced	NetworkPacketsOut ⓘ	No alarms
☐	i-0be11dde342ef1ced	DiskWriteOps ⓘ	No alarms
☐	i-0be11dde342ef1ced	NetworkPacketsIn ⓘ	No alarms

Cancel | Select metric

Basic architecture of an Amazon EC2 instance deployed



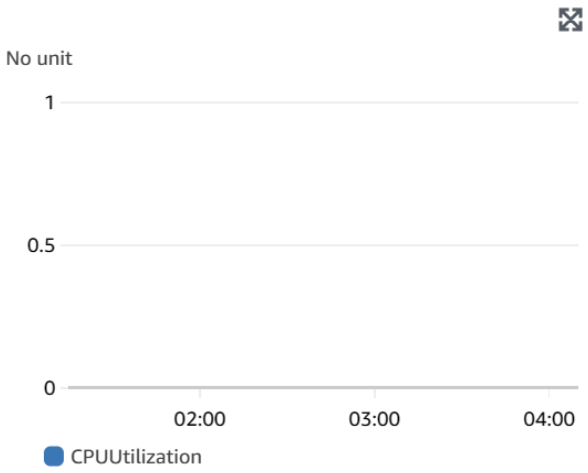
- You can use metrics to calculate statistics and then present the data graphically in the CloudWatch console

Metric

Edit

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.



Namespace
AWS/EC2

Metric name
CPUUtilization

InstanceId
i-0be11dde342ef1ced

Instance name
FoodWebDeploy

Statistic
Average

Period
5 minutes

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.

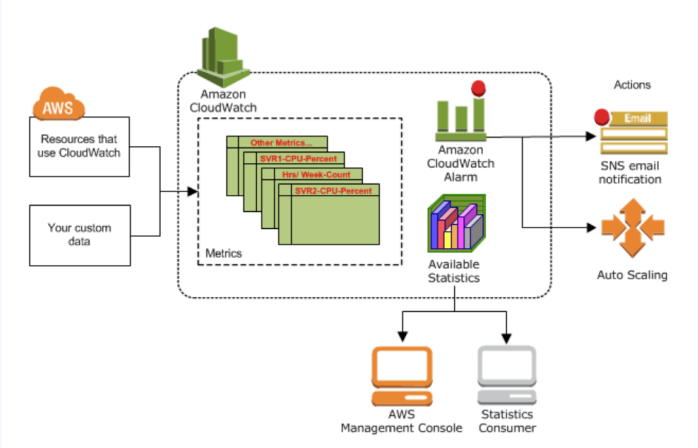
10

Must be a number

▶ Additional configuration

Cancel Next

Basic architecture of an Amazon EC2 instance deployed



- 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.

EC2 action

Alarm state trigger

Define the alarm state that will trigger this action.

Remove

- (●) **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.

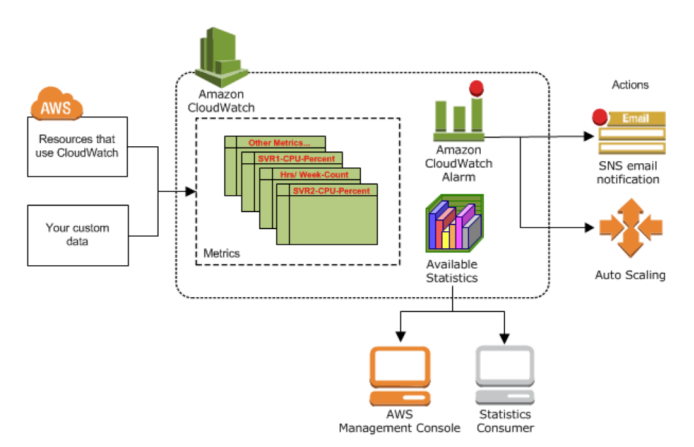
Take the following action...

Define what will happen to the EC2 instance with the Instance ID i-0be11dde342ef1ced when this alarm is triggered.

- ( ) Recover this instance
  You can only recover certain EC2 instance types. See documentation
- (●) Stop this instance
  You can only stop an instance if it is backed by an EBS volume. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. Show IAM policy document
- ( ) Terminate this instance
  You will not be able to terminate this instance if termination protection is enabled. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. Show IAM policy document
- ( ) Reboot this instance
  An instance reboot is equivalent to an operating system reboot. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. Show IAM policy document

Add EC2 action

Basic architecture of an Amazon EC2 instance deployed

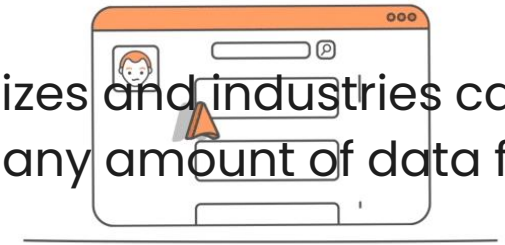


- AWS Cloud computing resources are housed in highly available data center facilities.
- To provide additional scalability and reliability, each data center facility is located in a specific geographical area, known as a Region.
- Each Region is designed to be completely isolated from the other Regions, 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.

Flowchart of E-Commerce Website

Amazon Simple Storage Service (S3)

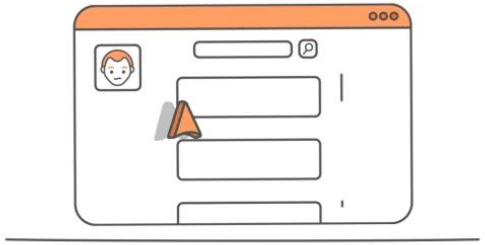
- Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance

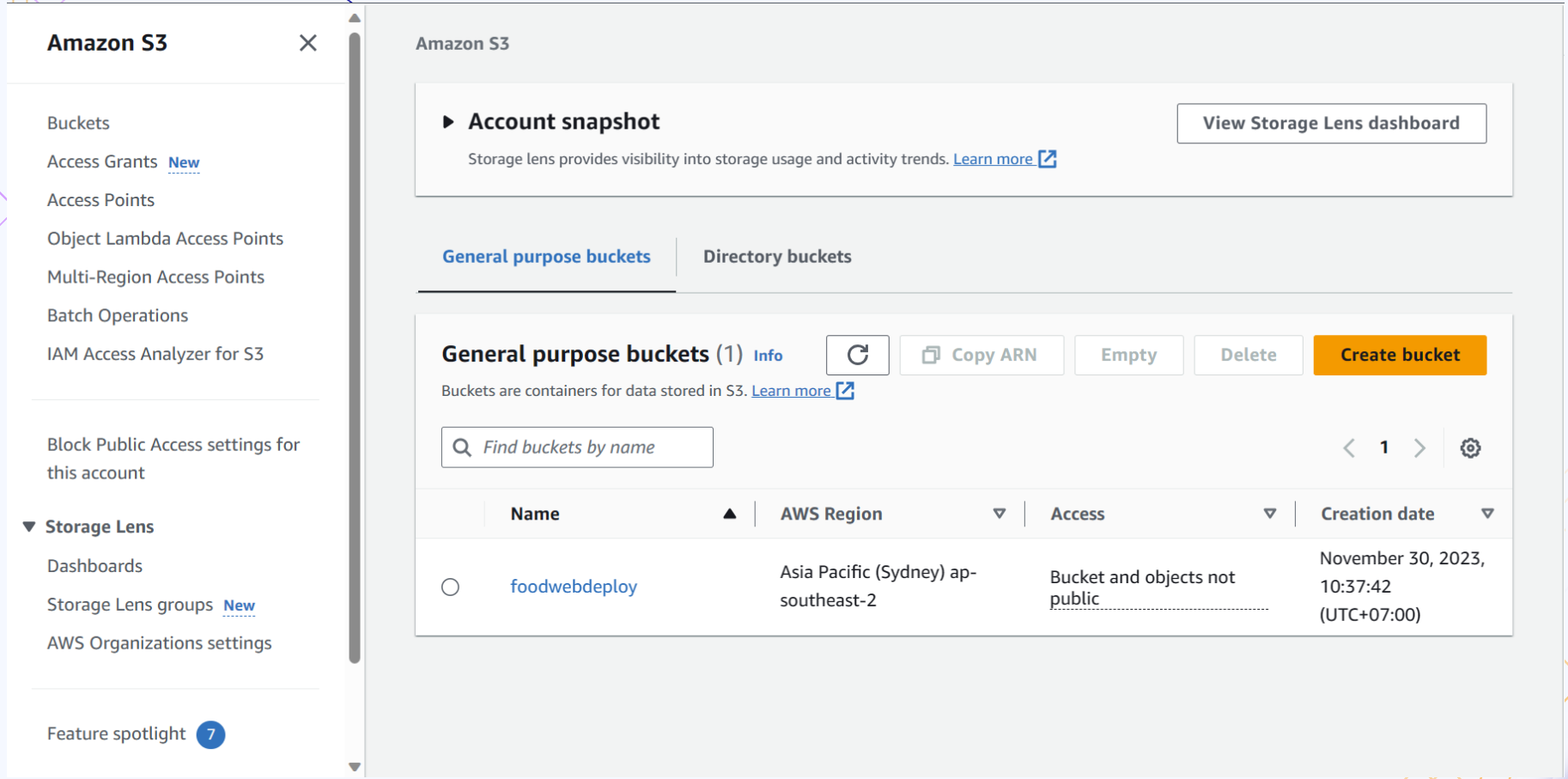


- Customers of all sizes and industries can use Amazon S3 to store and protect any amount of data for a range of use cases

Amazon Simple Storage Service (S3)

- Amazon S3 provides management features so that you can optimize, organize, and configure access to your data to meet your specific business, organizational, and compliance requirements.



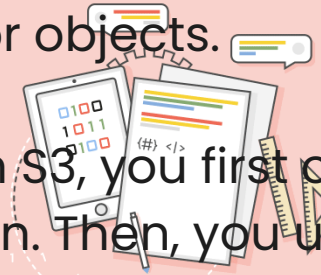

Amazon S3
Buckets
Access Grants New
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups New
AWS Organizations settings
Feature spotlight 7
Amazon S3
Account snapshot
Storage lens provides visibility into storage usage and activity trends. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
Copy ARN
Empty
Delete
Create bucket
Buckets are containers for data stored in S3. Learn more
Find buckets by name
1
Name
AWS Region
Access
Creation date
foodwebdeploy
Asia Pacific (Sydney) ap-southeast-2
Bucket and objects not public
November 30, 2023, 10:37:42 (UTC+07:00)

Features of Amazon S3

- Storage Classes
- Storage Management
- Access management and security
- Data Processing
- Storage logging and monitoring
- Analytics and insights
- Strong consistency

How AWS S3 Works?

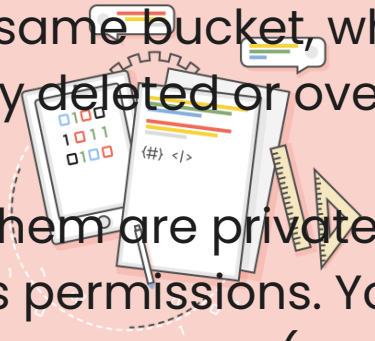
- Amazon S3 is an object storage service that stores data as objects within buckets. An object is a file and any metadata that describes the file. A bucket is a container for objects.



- To store your data in Amazon S3, you first create a bucket and specify a bucket name and AWS Region. Then, you upload your data to that bucket as objects in Amazon S3. Each object has a key (or key name), which is the unique identifier for the object within the bucket.

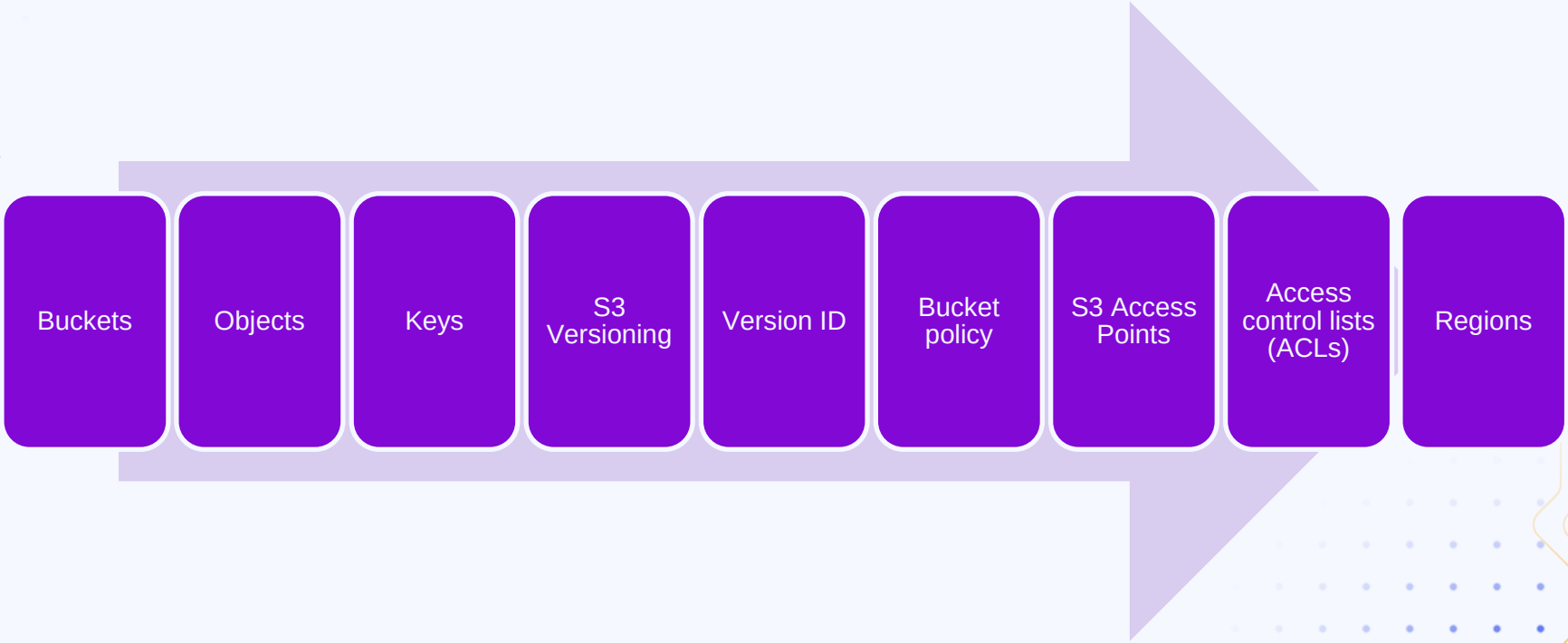
How AWS S3 Works?

- S3 provides features that you can configure to support your specific use case. For example, you can use S3 Versioning to keep multiple versions of an object in the same bucket, which allows you to restore objects that are accidentally deleted or overwritten.



- Buckets and the objects in them are private and can be accessed only if you explicitly grant access permissions. You can use bucket policies, AWS Identity and Access Management (IAM) policies, access control lists (ACLs), and S3 Access Points to manage access.

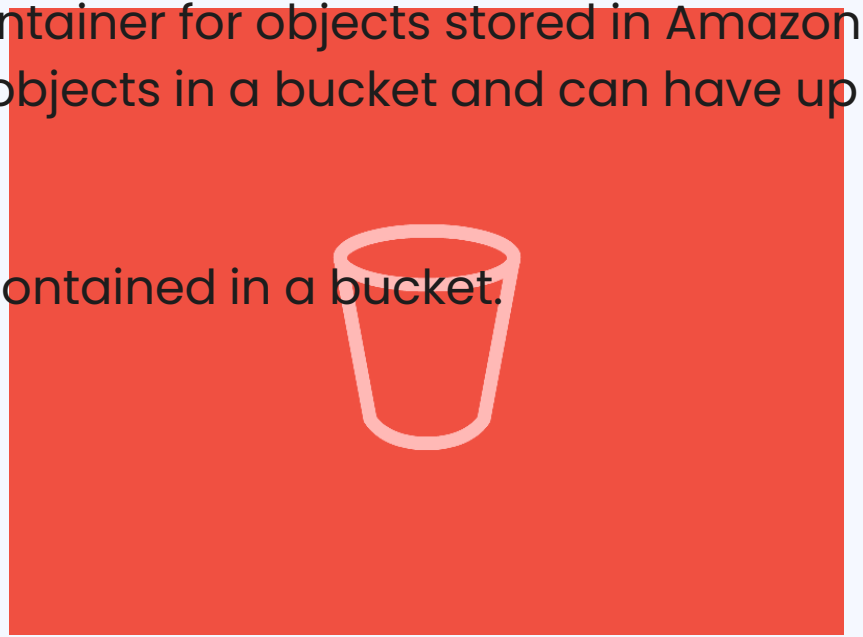
How AWS S3 Works?



Buckets

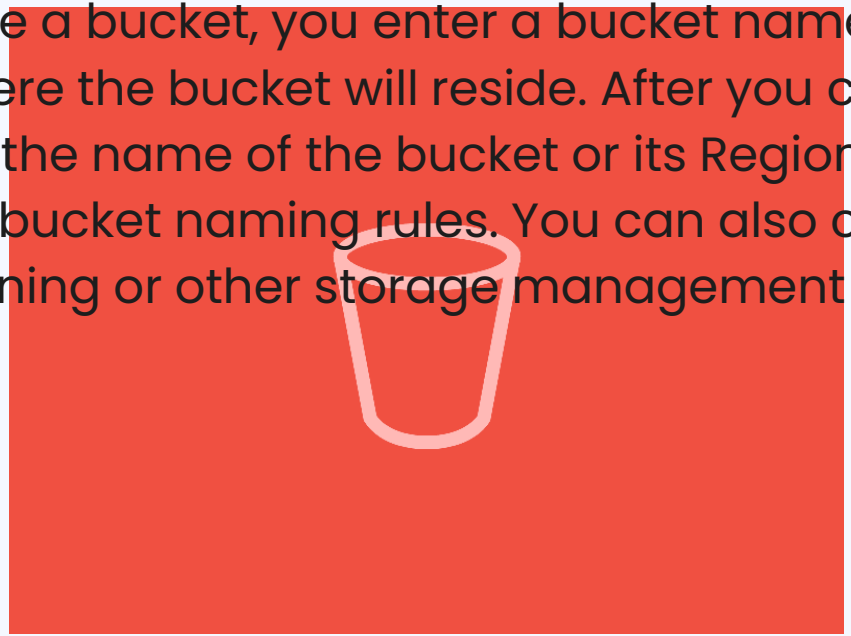
- A bucket is a container for objects stored in Amazon S3. You can store any number of objects in a bucket and can have up to 100 buckets in your account.

- Every object is contained in a bucket.



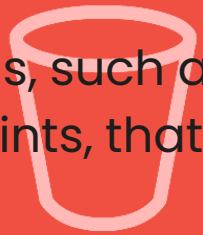
Buckets

- When you create a bucket, you enter a bucket name and choose the AWS Region where the bucket will reside. After you create a bucket, you cannot change the name of the bucket or its Region. Bucket names must follow the bucket naming rules. You can also configure a bucket to use S3 Versioning or other storage management features.



Buckets also

- Organize the Amazon S3 namespace at the highest level.
- Identify the account responsible for storage and data transfer charges.
- Provide access control options, such as bucket policies, access control lists (ACLs), and S3 Access Points, that you can use to manage access to your Amazon S3 resources.
- Serve as the unit of aggregation for usage reporting.



Account snapshot

Storage lens provides visibility into storage usage and activity trends. Learn more

View Storage Lens dashboard

General purpose buckets | Directory buckets

General purpose buckets (1) Info

Copy ARN | Empty | Delete | Create bucket

Buckets are containers for data stored in S3. Learn more

Find buckets by name

1

Name	AWS Region	Access	Creation date
foodwebdeploy	Asia Pacific (Sydney) ap-southeast-2	Bucket and objects not public	November 30, 2023, 10:37:42 (UTC+07:00)

Objects

- Objects are the fundamental entities stored in Amazon S3. Objects consist of object data and metadata.
- The metadata is a set of name-value pairs that describe the object.
- These pairs include some default metadata, such as the date last modified, and standard HTTP metadata, such as Content-Type. You can also specify custom metadata at the time that the object is stored.
- An object is uniquely identified within a bucket by a key (name) and a version ID (if S3 Versioning is enabled on the bucket).

foodwebdeploy Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Objects (1) Info

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

Copy S3 URI | Copy URL | Download | Open | Delete | Actions

Create folder | Upload

Find objects by prefix

1

Name	Type	Last modified	Size	Storage class
BackupFoodWeb/	Folder	-	-	-

Keys

- An object key (or key name) is the unique identifier for an object within a bucket. Every object in a bucket has exactly one key.
- The combination of a bucket, object key, and optionally, version ID (if S3 Versioning is enabled for the bucket) uniquely identify each object.

- you can think of Amazon S3 as a basic data map between "bucket + key + version" and the object itself.
- Every object in Amazon S3 can be So uniquely addressed through the combination of the web service endpoint, bucket name, key, and optionally, a version.

foodweb@@ Info

Delete

Summary

ARN
arn:aws:iam::614018551910:user/foodweb@@

Created
November 30, 2023, 14:20 (UTC+07:00)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
AKIAY55S3SBTNCMVS5OG - Active
Used today. Created today.

Access key 2
Create access key

Permissions | Groups | Tags (1) | Security credentials | Access Advisor

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Remove | Add permissions

Filter by Type

Search | All types

1

S3 Versioning

- You can use S3 Versioning to keep multiple variants of an object in the same bucket.
- With S3 Versioning, you can preserve, retrieve, and restore every version of every object stored in your buckets.
- You can easily recover from both unintended user actions and application failures.

foodwebdeploy Info

Objects | Properties | Permissions | Metrics | Management | Access Points

Bucket overview

AWS Region
Asia Pacific (Sydney) ap-southeast-2

Amazon Resource Name (ARN)
arn:aws:s3:::foodwebdeploy

Creation date
November 30, 2023, 10:37:42 (UTC+07:00)

Bucket Versioning

Edit

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

Disabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more

Disabled

Version ID

- When you enable S3 Versioning in a bucket, Amazon S3 generates a unique version ID for each object added to the bucket.
- Objects that already existed in the bucket at the time that you enable versioning have a version ID of null.
- If you modify these (or any other) objects with other operations, such as CopyObject and PutObject, the new objects get a unique version ID.

Edit Bucket Versioning Info

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

Bucket Versioning

- (•) Suspend
  This suspends the creation of object versions for all operations but preserves any existing object versions.
- ( ) Enable

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more

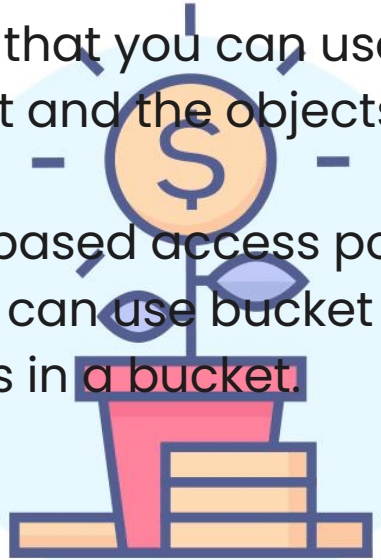
Disabled

Cancel Save changes

Bucket policy

- A bucket policy is a resource-based AWS Identity and Access Management (IAM) policy that you can use to grant access permissions to your bucket and the objects in it.

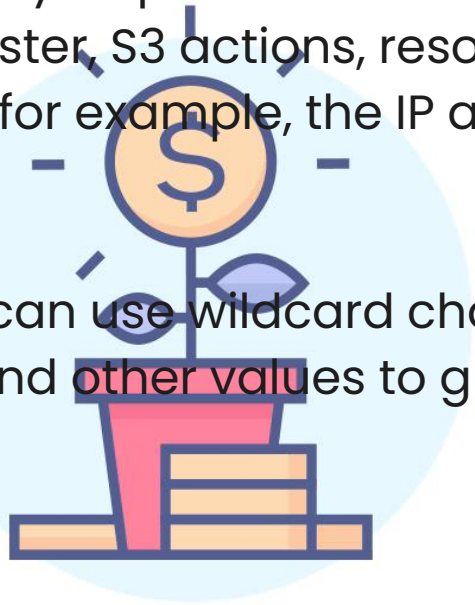
- Bucket policies use JSON-based access policy language that is standard across AWS. You can use bucket policies to add or deny permissions for the objects in a bucket.

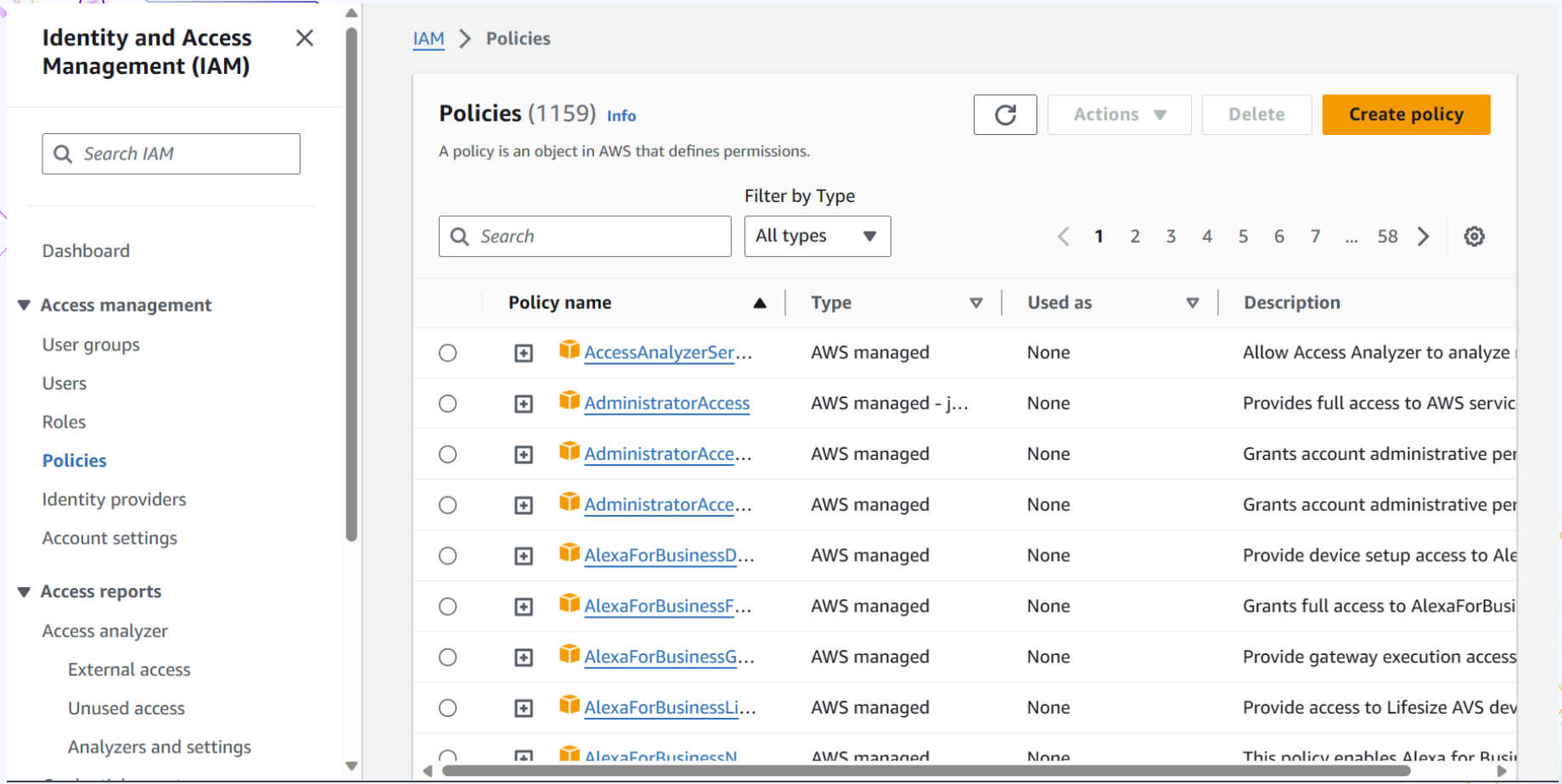


Bucket policy

- Bucket policies allow or deny requests based on the elements in the policy, including the requester, S3 actions, resources, and aspects or conditions of the request (for example, the IP address used to make the request).

- In your bucket policy, you can use wildcard characters on Amazon Resource Names (ARNs) and other values to grant permissions to a subset of objects.




Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
External access
Unused access
Analyzers and settings
IAM > Policies
Policies (1159) Info
A policy is an object in AWS that defines permissions.
Actions
Delete
Create policy
Filter by Type
Search
All types
1 2 3 4 5 6 7 ... 58
Policy name
Type
Used as
Description
AccessAnalyzerSer...
AWS managed
None
Allow Access Analyzer to analyze
AdministratorAccess
AWS managed - j...
None
Provides full access to AWS servic
AdministratorAcce...
AWS managed
None
Grants account administrative per
AdministratorAcce...
AWS managed
None
Grants account administrative per
AlexaForBusinessD...
AWS managed
None
Provide device setup access to Ale
AlexaForBusinessF...
AWS managed
None
Grants full access to AlexaForBusi
AlexaForBusinessG...
AWS managed
None
Provide gateway execution access
AlexaForBusinessLi...
AWS managed
None
Provide access to Lifesize AVS dev

S3 Access Points

- Amazon S3 Access Points are named network endpoints with dedicated access policies that describe how data can be accessed using that endpoint.

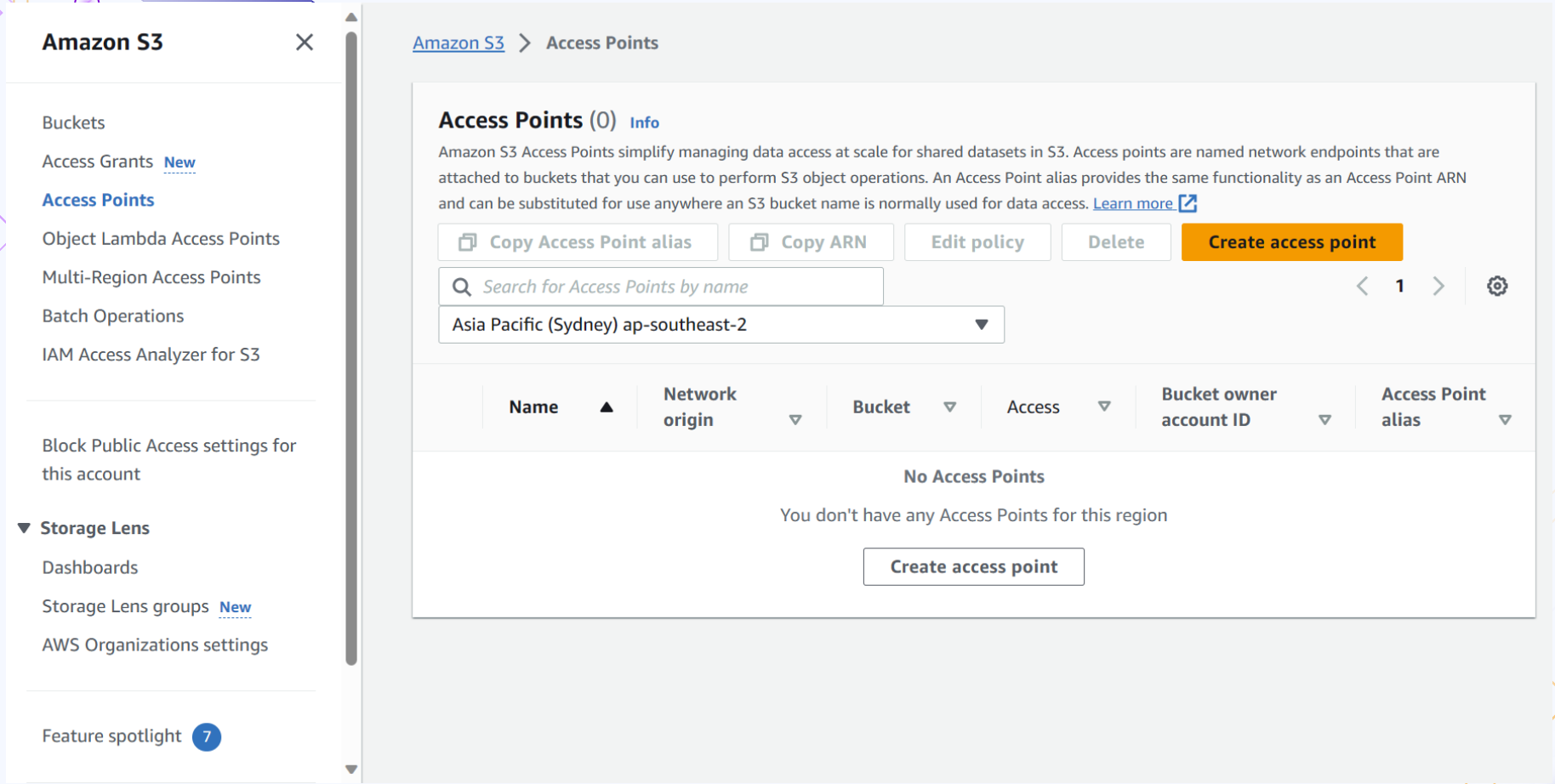
- Access Points are attached to buckets that you can use to perform S3 object operations, such as GetObject and PutObject.

S3 Access Points

- Points simplify managing data access at scale for shared datasets in Amazon S3.

- Each access point has its own access point policy. You can configure Block Public Access settings for each access point.

- To restrict Amazon S3 data access to a private network, you can also configure any access point to accept requests only from a virtual private cloud (VPC).


Amazon S3
Buckets
Access Grants New
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups New
AWS Organizations settings
Feature spotlight 7
Amazon S3 > Access Points
Access Points (0) Info
Amazon S3 Access Points simplify managing data access at scale for shared datasets in S3. Access points are named network endpoints that are attached to buckets that you can use to perform S3 object operations. An Access Point alias provides the same functionality as an Access Point ARN and can be substituted for use anywhere an S3 bucket name is normally used for data access. Learn more
Copy Access Point alias
Copy ARN
Edit policy
Delete
Create access point
Search for Access Points by name
1
Asia Pacific (Sydney) ap-southeast-2
Name
Network origin
Bucket
Access
Bucket owner account ID
Access Point alias
No Access Points
You don't have any Access Points for this region
Create access point

Access control lists (ACLs)

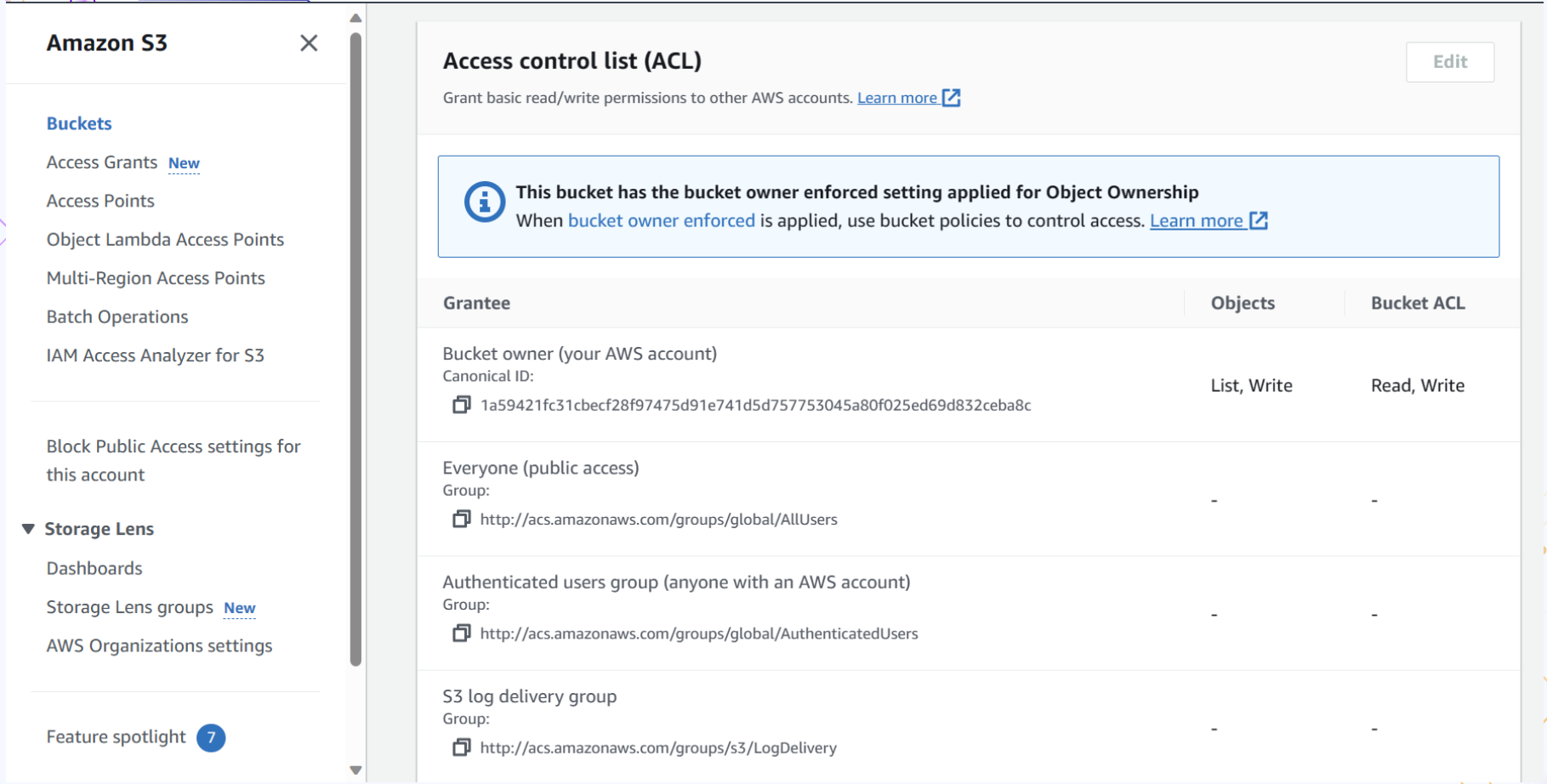
- You can use ACLs to grant read and write permissions to authorized users for individual buckets and objects. Each bucket and object has an ACL attached to it as a subresource.

- The ACL defines which AWS accounts or groups are granted access and the type of access. ACLs are an access control mechanism that predates IAM

Access control lists (ACLs)

- S3 Object Ownership is an Amazon S3 bucket-level setting that you can use to both control ownership of the objects that are uploaded to your bucket and to disable or enable ACLs..

- A majority of modern use cases in Amazon S3 no longer require the use of ACLs. With ACLs disabled, you can use policies to control access to all objects in your bucket, regardless of who uploaded the objects to your bucket.


Amazon S3
Buckets
Access Grants New
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups New
AWS Organizations settings
Feature spotlight 7
Access control list (ACL)
Edit
Grant basic read/write permissions to other AWS accounts. Learn more
This bucket has the bucket owner enforced setting applied for Object Ownership
When bucket owner enforced is applied, use bucket policies to control access. Learn more
Grantee
Objects
Bucket ACL
Bucket owner (your AWS account)
Canonical ID:
1a59421fc31cbecf28f97475d91e741d5d757753045a80f025ed69d832ceba8c
List, Write
Read, Write
Everyone (public access)
Group:
http://acs.amazonaws.com/groups/global/AllUsers
-
-
Authenticated users group (anyone with an AWS account)
Group:
http://acs.amazonaws.com/groups/global/AuthenticatedUsers
-
-
S3 log delivery group
Group:
http://acs.amazonaws.com/groups/s3/LogDelivery
-
-

Regions

- You can choose the geographical AWS Region where Amazon S3 stores the buckets that you create.
- You might choose a Region to optimize latency, minimize costs, or address regulatory requirements.
- Objects stored in an AWS Region never leave the Region unless you explicitly transfer or replicate them to another Region.
- For example, objects stored in the Europe (Ireland) Region never leave it.

Create bucket Info

Buckets are containers for data stored in S3. Learn more

General configuration

AWS Region

Asia Pacific (Sydney) ap-southeast-2

United States

US East (N. Virginia) us-east-1

US East (Ohio) us-east-2

US West (N. California) us-west-1

US West (Oregon) us-west-2

Africa

Africa (Cape Town) af-south-1
Disabled Region

ing rules. See rules for bucket naming

use of access control lists (ACLs). Object ownership determines who can specify access to objects.

Amazon S3 data consistency model

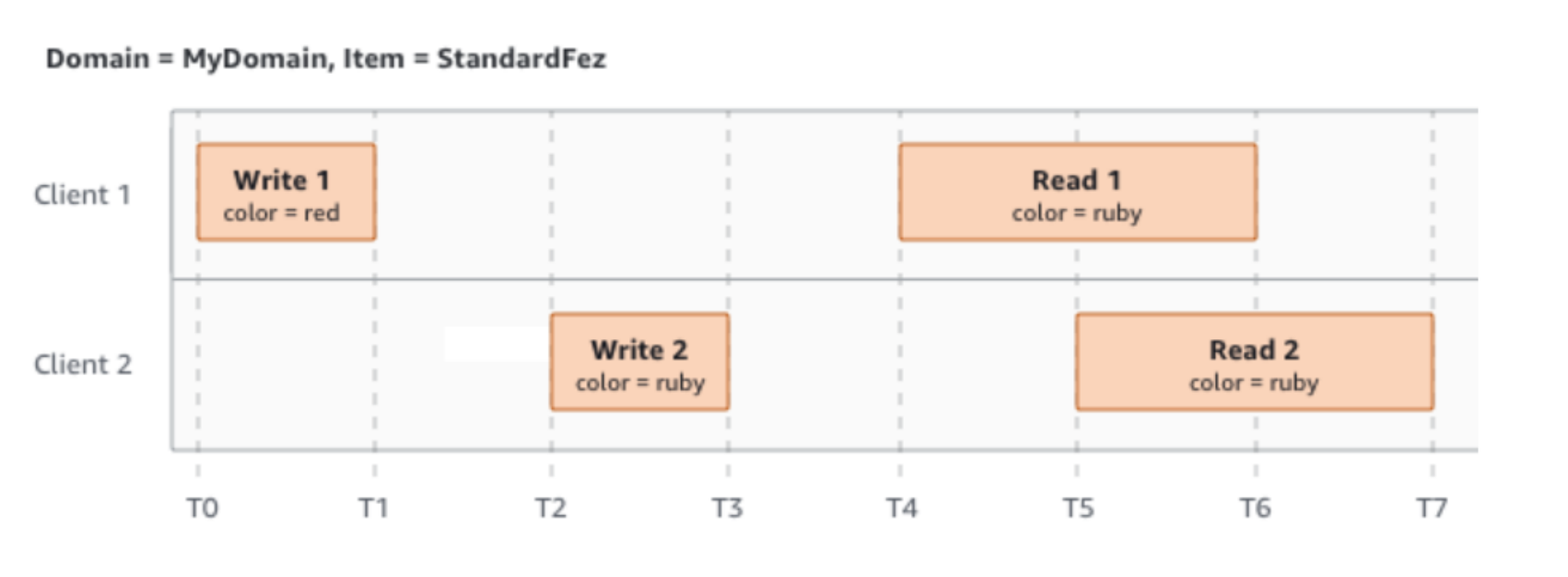
- Amazon S3 provides strong read-after-write consistency for PUT and DELETE requests of objects in your Amazon S3 bucket in all AWS Regions. This behavior applies to both writes to new objects as well as PUT requests that overwrite existing objects and DELETE requests.

- In addition, read operations on Amazon S3 Select, Amazon S3 access controls lists (ACLs), Amazon S3 Object Tags, and object metadata (for example, the HEAD object) are strongly consistent.

Amazon S3 data consistency model

- Updates to a single key are atomic. For example, if you make a PUT request to an existing key from one thread and perform a GET request on the same key from a second thread concurrently, you will get either the old data or the new data, but never partial or corrupt data.

Amazon S3 data consistency model - Concurrent applications – Example 1

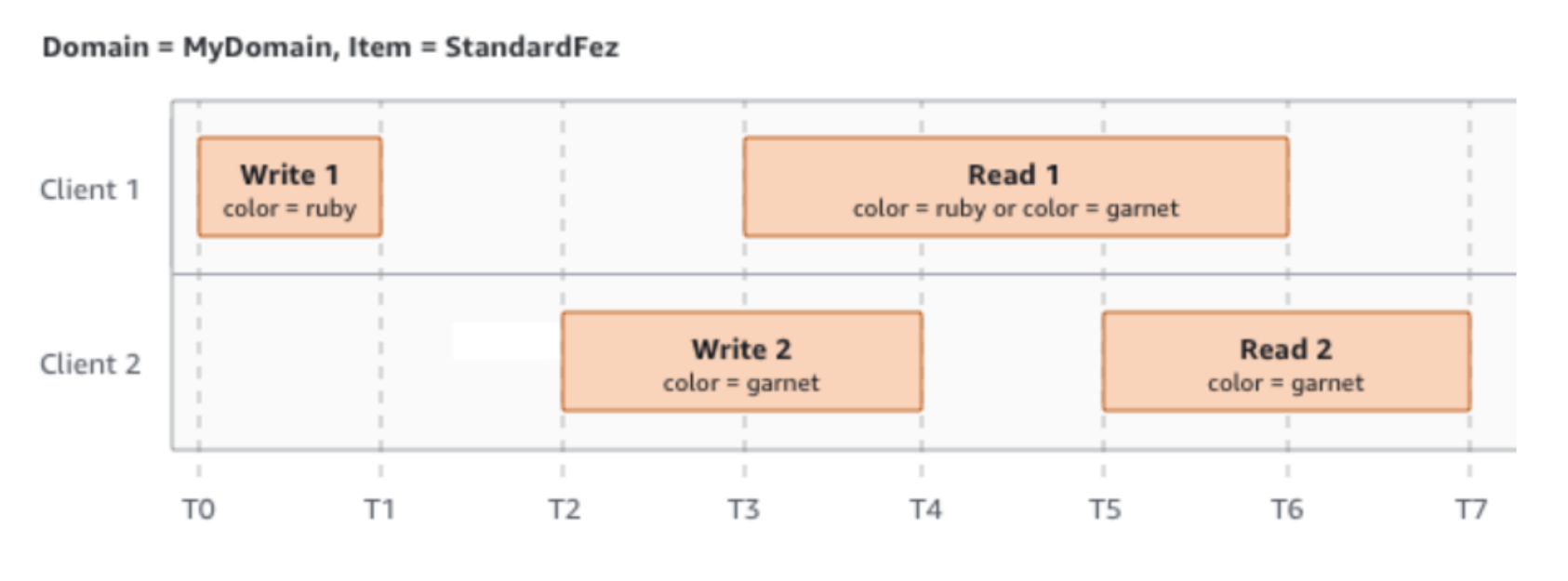


Amazon S3 data consistency model - Concurrent applications – Example 1

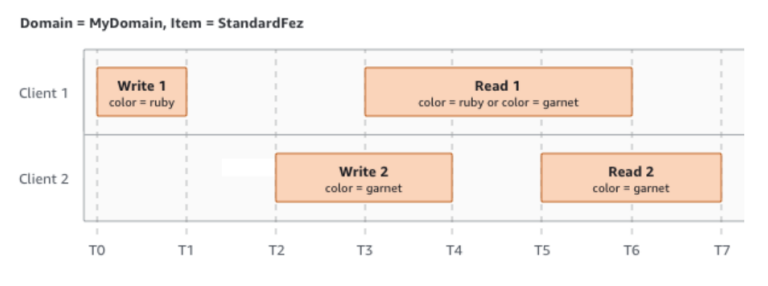
Examples of behavior to be expected from Amazon S3 when multiple clients are writing to the same items.

With example 1: Both W1 (write 1) and W2 (write 2) finish before the start of R1 (read 1) and R2 (read 2). Because S3 is strongly consistent, R1 and R2 both return color = ruby.

Amazon S3 data consistency model - Concurrent applications – Example 2



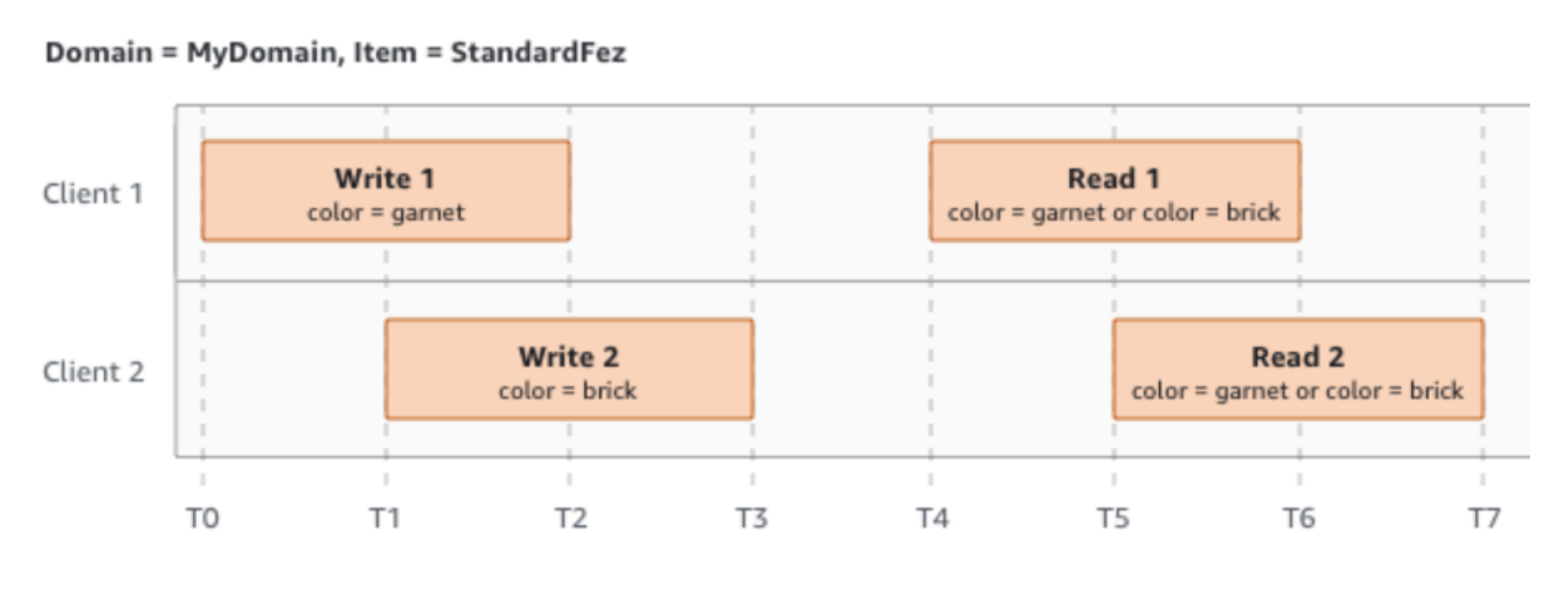
Amazon S3 data consistency model - Concurrent applications – Example 2



Examples of behavior to be expected from Amazon S3 when multiple clients are writing to the same items.

With example 2, W2 does not finish before the start of R1. Therefore, R1 might return color = ruby or color = garnet. However, because W1 and W2 finish before the start of R2, R2 returns color = garnet.

Amazon S3 data consistency model - Concurrent applications – Example 3



Amazon S3 data consistency model - Concurrent applications – Example 3

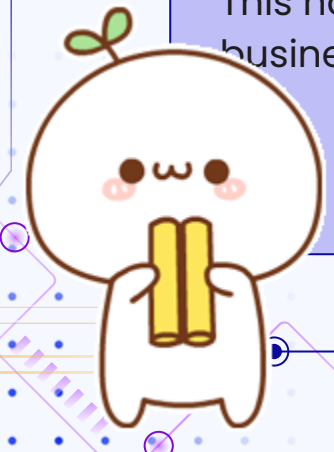
Examples of behavior to be expected from Amazon S3 when multiple clients are writing to the same items.

- With Example 3, W2 begins before W1 has received an acknowledgment. Therefore, these writes are considered concurrent. Amazon S3 internally uses last-writer-wins semantics to determine which write takes precedence.
- However, the order in which Amazon S3 receives the requests and the order in which applications receive acknowledgments cannot be predicted because of various factors, such as network latency.
- For example, W2 might be initiated by an Amazon EC2 instance in the same Region, while W1 might be initiated by a host that is farther away. The best way to determine the final value is to perform a read after both writes have been acknowledged.

04 Conclusion

Summary key point from report

In total, deploying an ecommerce site to AWS offers a range of performance, security, and cost benefits.
Using services like EC2, S3, and tools like IAM and CloudWatch created a flexible and powerful environment.
This not only provides a good user experience but also helps businesses maintain and grow online effectively.



Reference

[1] What is Amazon EC2? - Amazon Elastic Compute Cloud
[2] What is Amazon S3? - Amazon Simple Storage Service
[3] What is the AWS Command Line Interface? - AWS Command Line Interface (amazon.com)
[4] Use Amazon S3 with the AWS CLI - AWS Command Line Interface
[5] Use Amazon S3 with Amazon EC2 - Amazon Elastic Compute Cloud

Thank you for listening!!!

Do you have any question ?