

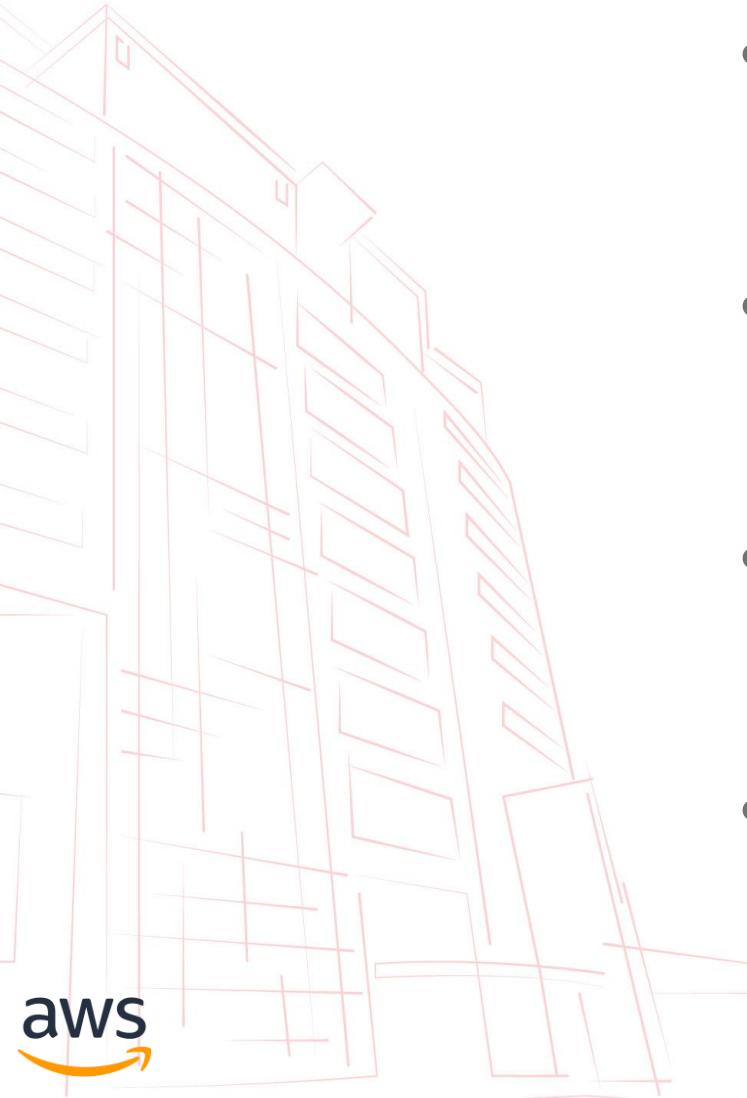
True IDC Cloud Professional Service

AWS On Boarding Part 2



Agenda

- Storage Service
- Database Service
- Monitoring Service
- Lab: S3 Security Best Practice

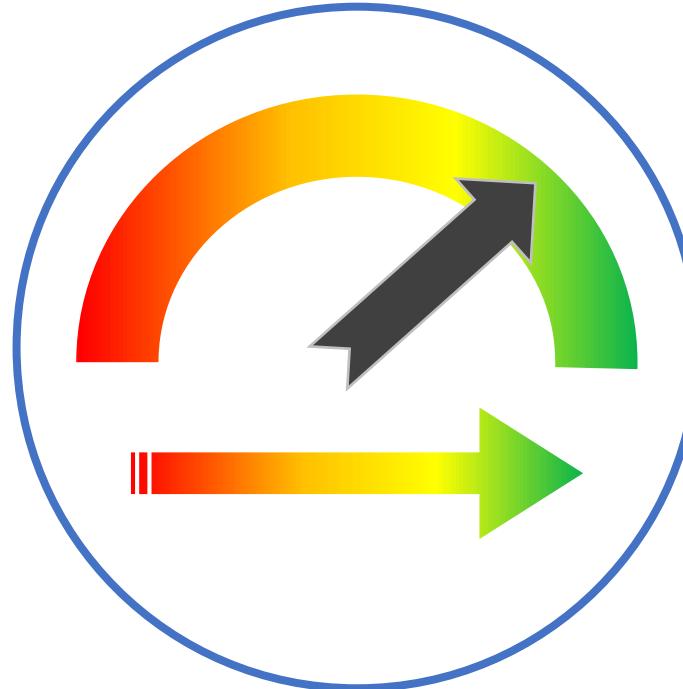


AWS Storage Service

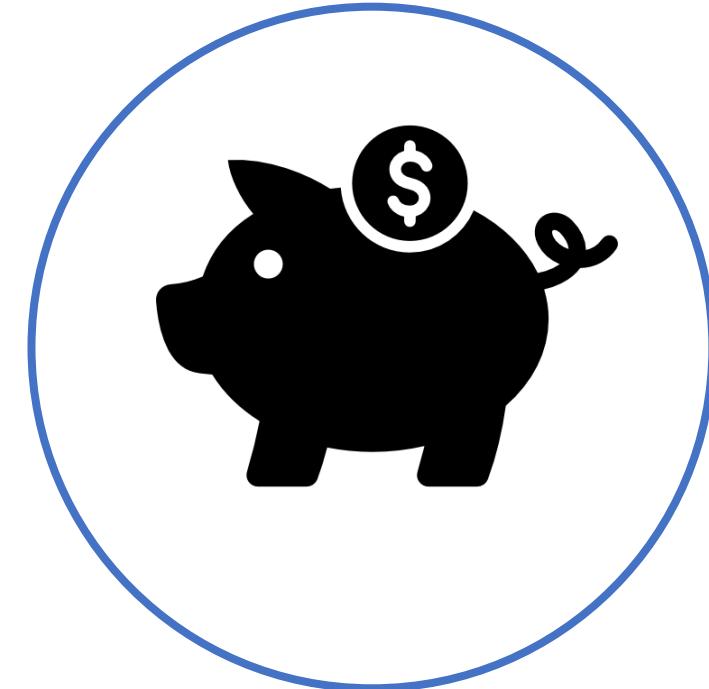
What do you think about when choosing a storage solution ?



Storage Type



Features and
Performance



Economics

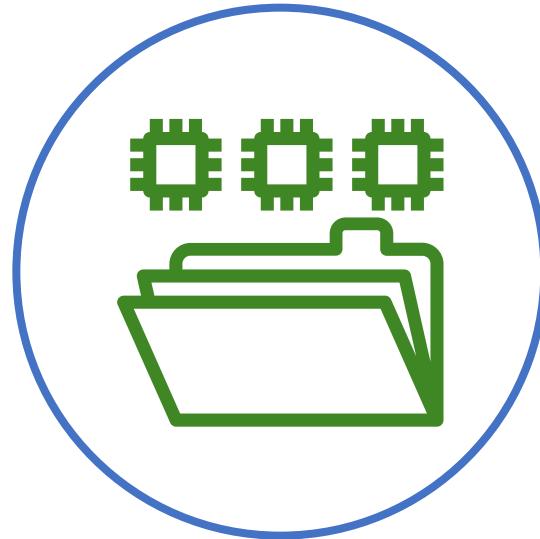
Storage Type



Block

Data stored as blocks on a disk or disks

Locally attached



File

Data stored as files in a directory hierarchy

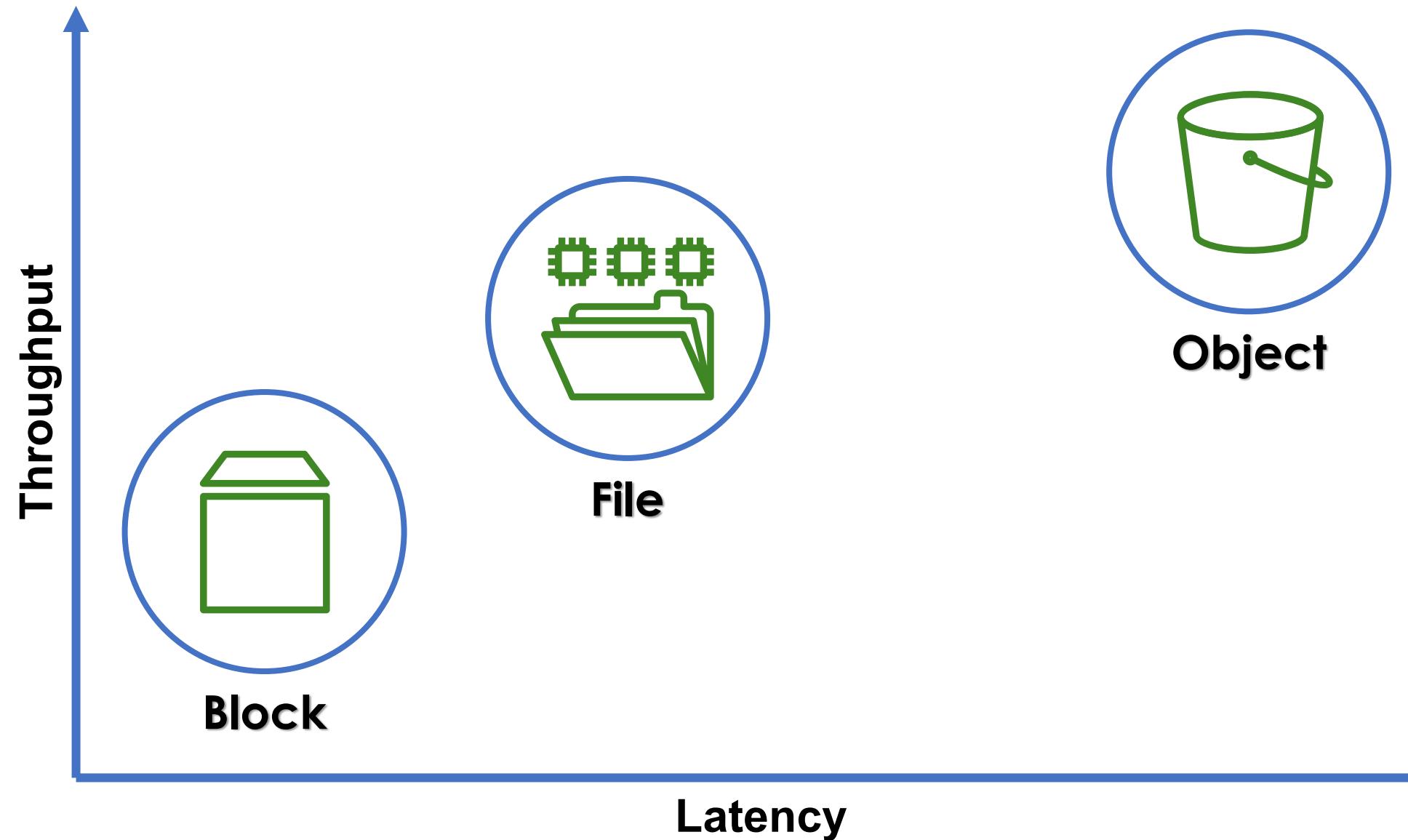
Shared over a network

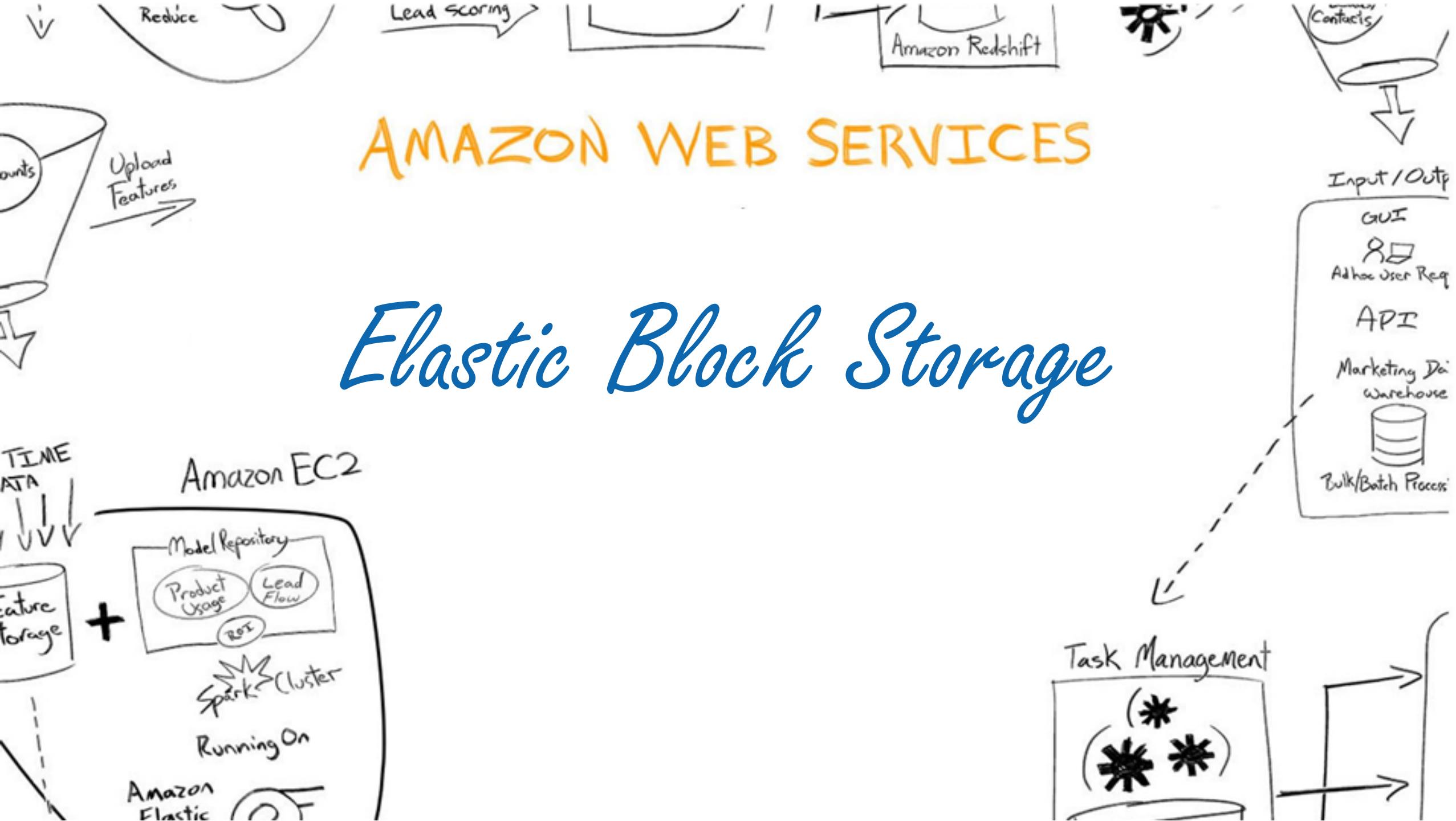


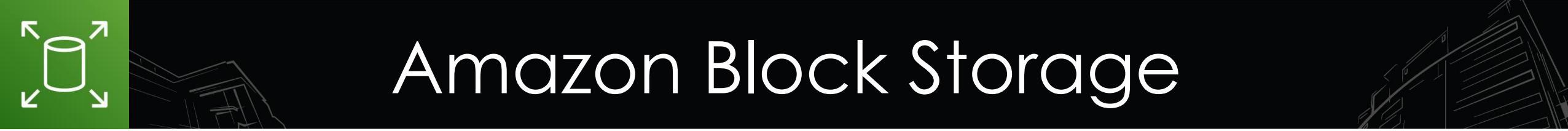
Object

Data is stored as an object that's identified by a key in a flat space
Simple API to get and put data based on key

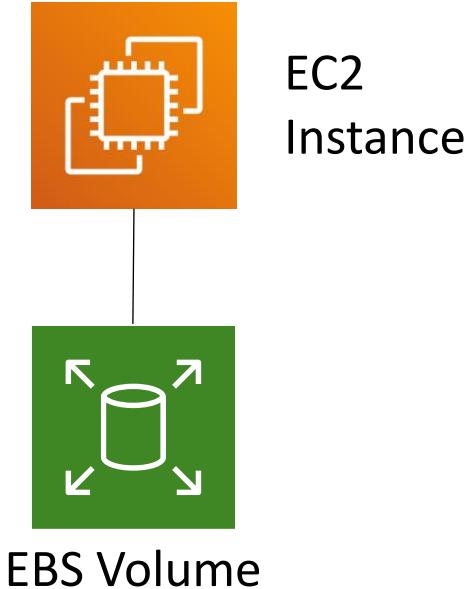
How does performance compare ?



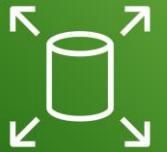




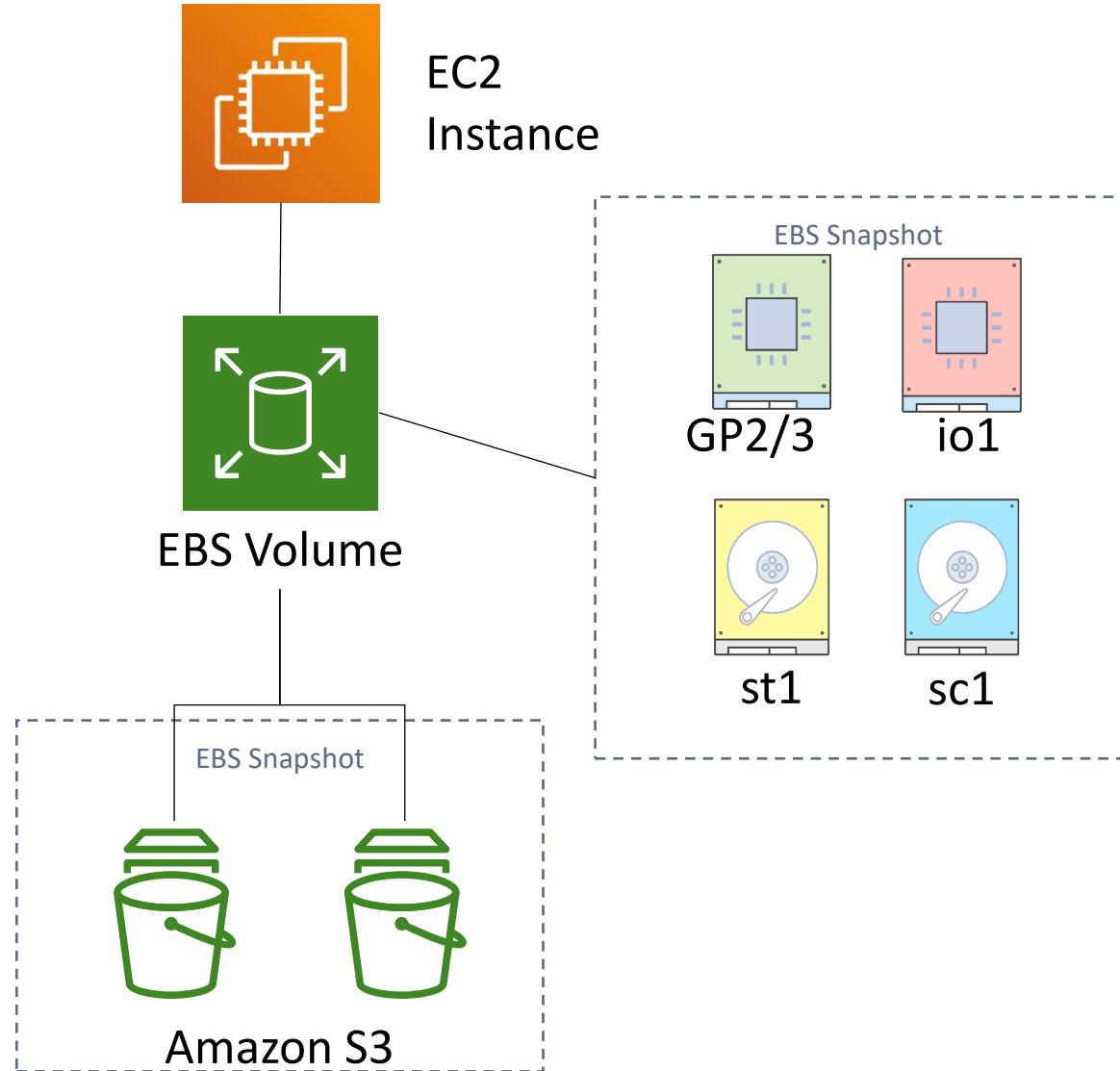
Amazon Block Storage



- Block storage as a service
- Create, attach, modify through an API
- Select Storage and compute based on your workload
- Detach and attach between instances



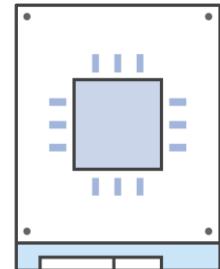
Amazon Block Storage



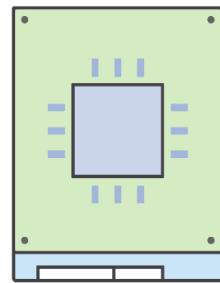
- Block storage as a service
- Create, attach, modify through an API
- Select Storage and compute based on your workload
- Detach and attach between instances
- Choice of magnetic and SSD-based volume types
- Supports snapshots: Point-in-time backup of modified volume blocks



Amazon Block Storage



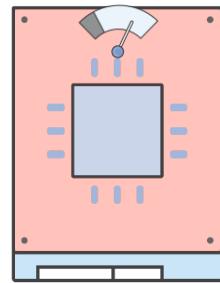
SSD



GP2/3

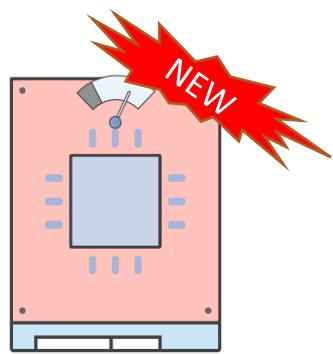
General Purpose
SSD

Boot volumes,
low-latency
interactive
applications,
dev, test.



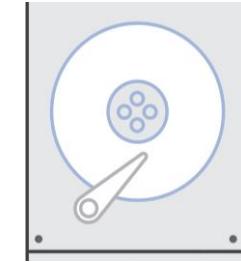
io1

Provisioned
IOPS
SSD
I/O intensive
NoSQL and
relational
databases.

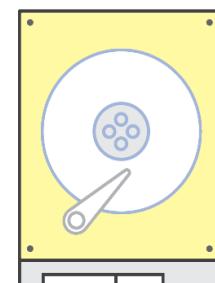


io2

Provisioned
IOPS
SSD
Better than io1
with same price



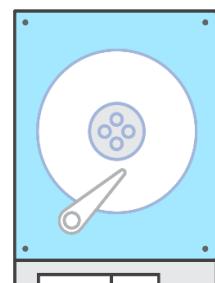
HDD



st1

Throughput Optimized
HDD

Big data, data
warehouses, log
processing.



sc1

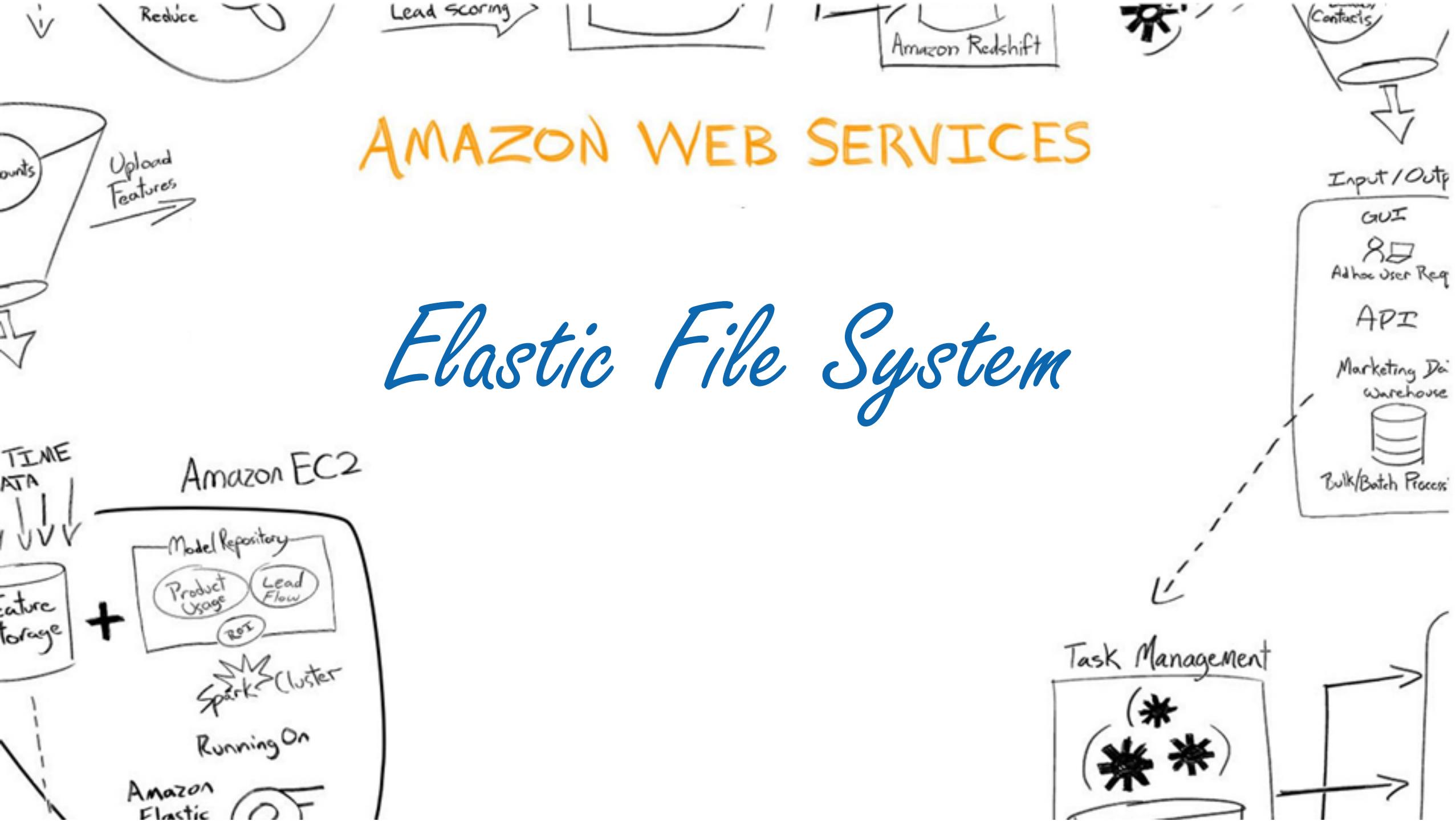
Cold
HDD

Colder data
requiring fewer
scans per day.



Amazon Block Storage

FEATURES	SSD Solid State Drive	HDD Hard Disk Drive
Best for workloads with:	<i>small, random</i> I/O operations	<i>large, sequential</i> I/O operations
Can be used as a bootable volume?	Yes	No
Suitable Use Cases	<ul style="list-style-type: none">- Best for transactional workloads- Critical business applications that require sustained IOPS performance- Large database workloads such as MongoDB, Oracle, Microsoft SQL Server and many others...	<ul style="list-style-type: none">- Best for large streaming workloads requiring consistent, fast throughput at a low price- Big data, Data warehouses, Log processing- Throughput-oriented storage for large volumes of data that is infrequently accessed
Cost	moderate / high 	low 
Dominant Performance Attribute	IOPS	Throughput (MiB/s)

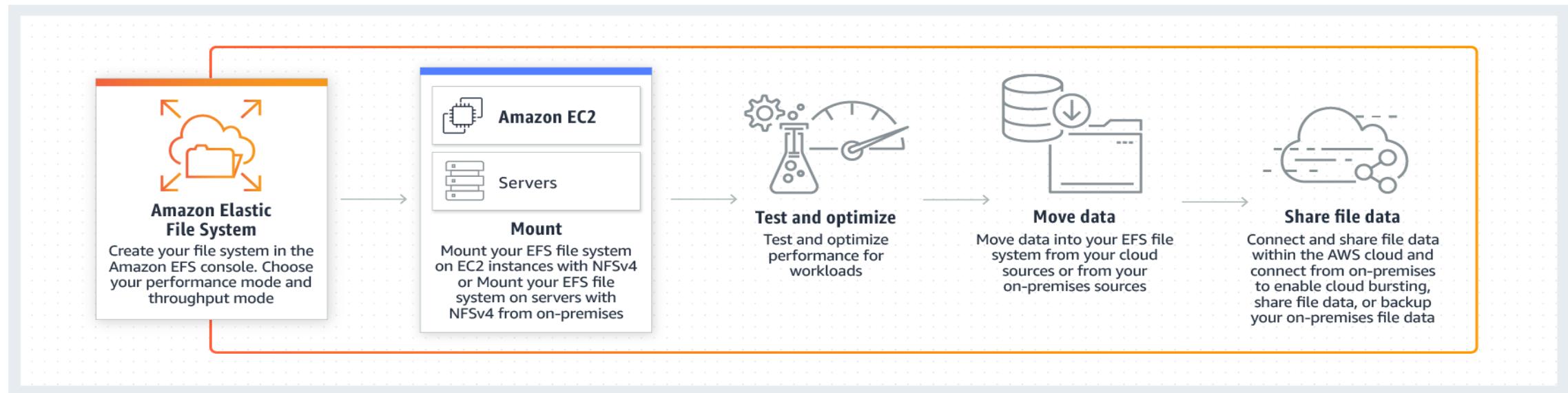




Amazon Elastic File System

a fully-managed service that makes it easy to set up, scale, and cost-optimize file storage in the Amazon Cloud.

- **Standard** – used to store frequently accessed files.
- **Infrequent Access(IA)** – lower-cost storage class, storing long-lived, infrequently accessed files cost-effectively.



Amazon FSx file System

provides fully managed third-party file systems with feature sets for workloads such as Windows-based storage, high-performance computing (HPC), machine learning, and electronic design automation (EDA).



for Windows File Server provides a fully managed native Microsoft Windows file system.



for Lustre is a fully managed file system that is optimized for compute-intensive workloads.





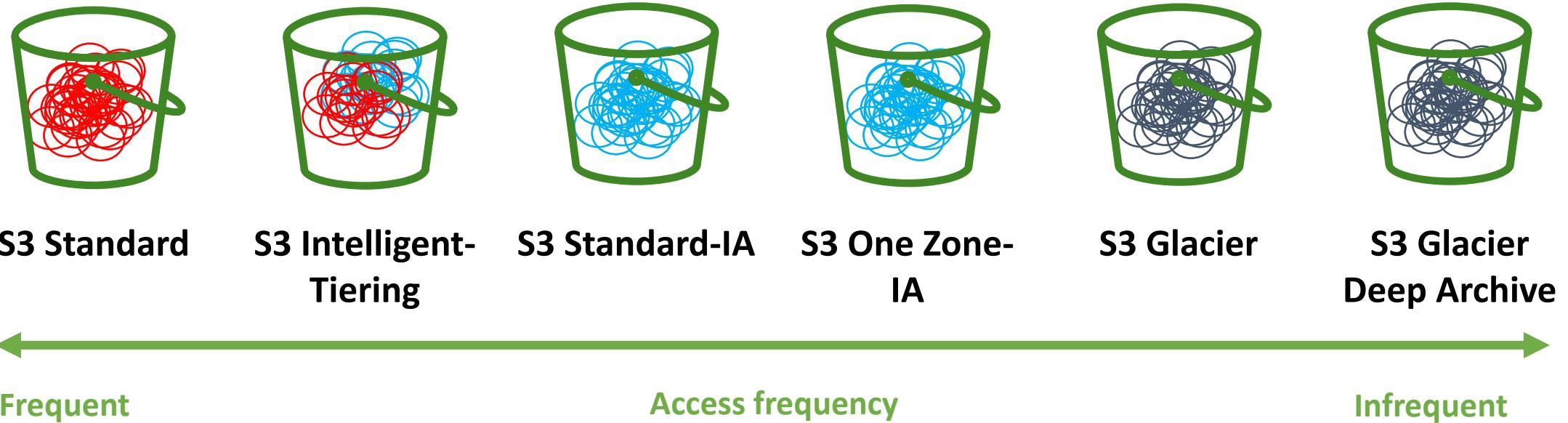
Amazon Simple Storage Service

Object storage built to store and retrieve any amount of data from anywhere on the internet

- Organize the Amazon S3 namespace at the highest level
- Identify the account responsible for storage and data transfer charges
- Play a role in access control
- Serve as the unit of aggregation for usage reporting
- Have globally unique bucket names, regardless of AWS region in which they were created



Amazon Simple Storage Service



- | | | | | | |
|------------------------------------|--------------------------------------|------------------------------|------------------------------------|------------------------|------------------------|
| • Active, frequently accessed data | • Data with changing access patterns | • Infrequently accessed data | • Re-creatable, less accessed data | • Archive data | • Archive data |
| • \$0.025 per GB | • \$0.02 to 0.025 per GB | • \$0.02 per GB | • \$0.016 per GB | • \$0.005 per GB | • \$0.002 per GB |
| | • Monitoring fee per object | • Retrieval fee per GB | • Retrieval fee per GB | • Retrieval fee per GB | • Retrieval fee per GB |



Amazon Simple Storage Service

	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)					
Designed for availability	99.99%	99.99%	99.99%	99.99%	99.99%	99.99%
Availability SLA	99.9%	99.9%	99.9%	99.9%	99.9%	99.9%
Availability Zones	≥3	≥3	≥3	≥3	≥3	≥3
Minimum storage duration charge	N/A	30 days				
Retrieval fee	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved

SLA percentage	Downtime per week	Downtime per month	Downtime per year
99	1.68 hours	7.2 hours	3.65 days
99.9	10.1 min	43.2 min	8.76 hours
99.95	5 min	21.6 min	4.38 hours
99.99	1.01 min	4.32 min	52.56 min
99.999	6 sec	25.9 sec	5.26 min



Amazon Simple Storage Service

SLA percentage	Downtime per week	Downtime per month	Downtime per year
99	1.68 hours	7.2 hours	3.65 days
99.9	10.1 min	43.2 min	8.76 hours
99.95	5 min	21.6 min	4.38 hours
99.99	1.01 min	4.32 min	52.56 min
99.999	6 sec	25.9 sec	5.26 min

AWS Database Service

SQL and NoSQL Database

	SQL	NoSQL
Data Storage	Rows and Columns	Key-Value
Schemas	Fixed	Dynamic
Querying	Using SQL	Focused on a collection of documents
Scalability	Vertical	Horizontal

SQL

CaseID	Topic	Submitter	Category
84713852	How to create EC2	TIDC-admin	Compute
84713853	Lambda is not working	TIDC-developer	Compute

NoSQL

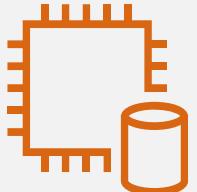
```
{  
    CaseID: 84713852,  
    Topic: "How to create EC2",  
    Submitter: "TIDC-admin",  
    Category: "Compute"  
}
```

Database Consideration

- No one size fits all
- Analyze your data requirements by considering:
 - Data formats
 - Data size
 - Query frequency
 - Data access speed
 - Data retention period

Database Options

Customer Managed



Database Server on Amazon EC2

Your choice of database running on Amazon EC2.

Bring Your Own License (BYOL)

AWS Managed



Amazon RDS

Microsoft SQL Server, Oracle, MySQL, PostgreSQL, or MariaDB as a managed service.

Flexible licensing BYOL or license included.



Amazon DynamoDB

Managed NoSQL database service using SSD storage.

Seamless scalability. Zero Administration.



Amazon Redshift

Massively Parallel, peta-byte scale, data warehouse service.

Fast, powerful and easy to scale.



Amazon Aurora

MySQL and PostgreSQL-compatible relational database built for the cloud

5x MySQL & 3x PostgreSQL faster



Relational Database Service

ORACLE



Amazon Aurora



PostgreSQL



Feature	Details
Platform support	MySQL, SQL Server, Oracle and PostgreSQL, MariaDB RDBMS
Preconfigured	Get started instantly with sensible default settings
Automated patching	Keep your database platform up to date automatically
Backups	Automatic backups and point in time recovery and full DB backups
Provisioned IOPS	Specify IO throughput depending on requirements
Failover	Automated failover to standby hosts in event of a failure with multi-az
Replication	Easily create read-replicas of your data and seamlessly replicate data across availability zones



How Amazon RDS Backup Work

Backup

Backup retention period
The number of days for which automated backups are retained. Setting this parameter to a positive number enables backups. Setting this parameter to 0 disables automated backups.

7 days

Backup window
The daily time range (in UTC) during which automated backups are created if automated backups are enabled.

Start Time: 20 : 38 UTC Duration: 0.5 hours

Copy tags to snapshots

RDS > Databases > Take snapshot

Take DB Snapshot

This feature is currently supported for InnoDB storage engine only. If you are using MyISAM, refer to details [here](#).

Settings
To take a snapshot of this DB instance you must provide a name for the snapshot.

DB instance
The unique key that identifies a DB instance. This parameter isn't case-sensitive.
database-1

Snapshot name
The Identifier for the DB Snapshot.

Cancel **Take Snapshot**

Automatic Backups

- Restore your database to a point in time
- Enabled by default
- Let you choose a retention period up to 35 days

Manual Snapshot

- Let you build a new database instance from a snapshot
- Initiated by user
- Persist until the user deletes.
- Stored in Amazon S3



RDS > Snapshots > Copy snapshot

Make Copy of DB Snapshot?

Settings

Source DB Snapshot

DB Snapshot Identifier for the snapshot being copied.

rds:database-1-2020-08-26-04-38

Destination Region [Info](#)

US East (Ohio)

US East (N. Virginia)

US East (Ohio)

US West (N. California)

US West (Oregon)

EU (Ireland)

EU (London)

EU (Paris)

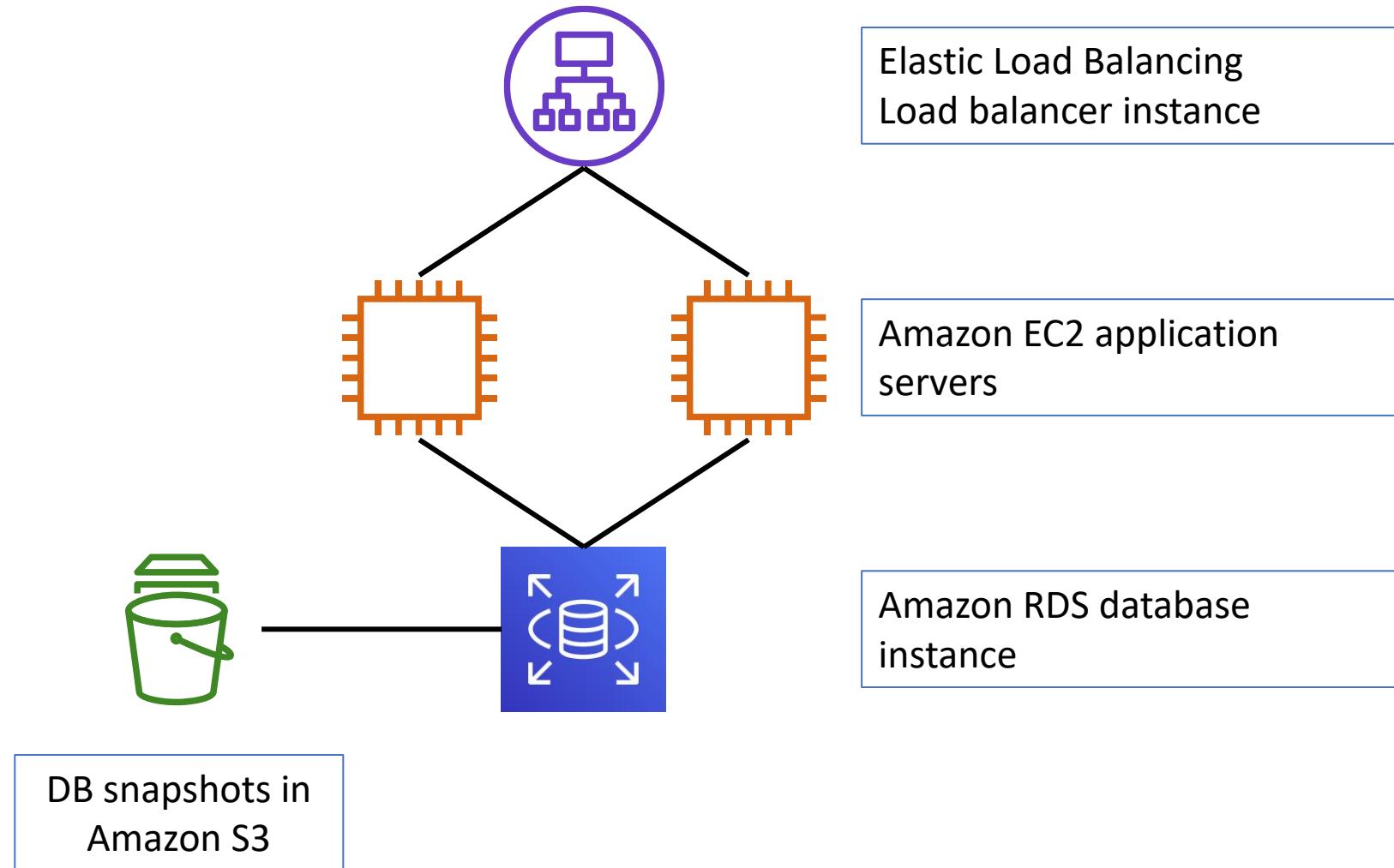
EU (Stockholm)

Asia Pacific (Tokyo)

- Copy of a database snapshot stored in a different AWS Region
- Provide a backup for disaster recovery
- Used as a base for migration to a different region

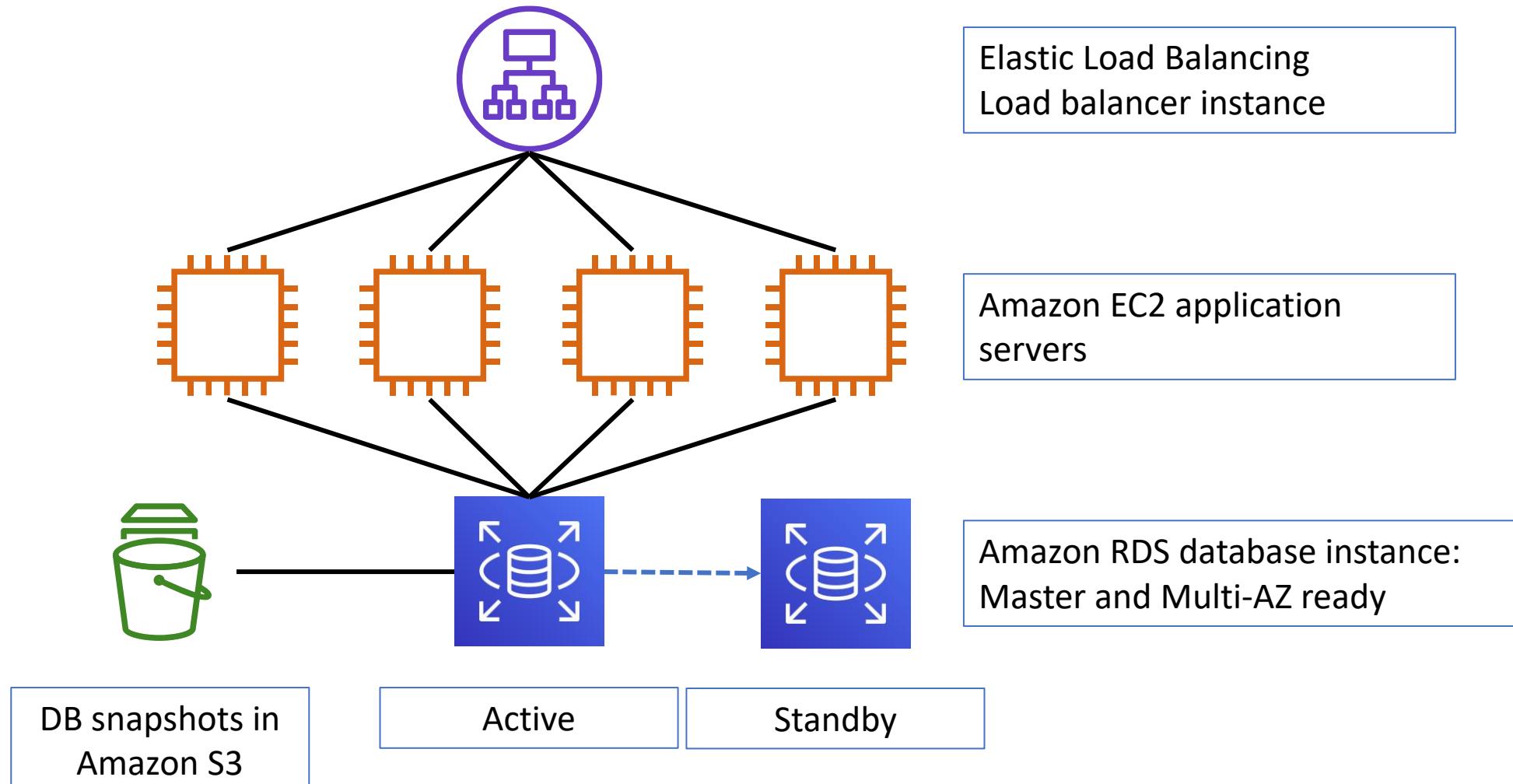


Relational Database Service





Multi-AZ RDS Deployment





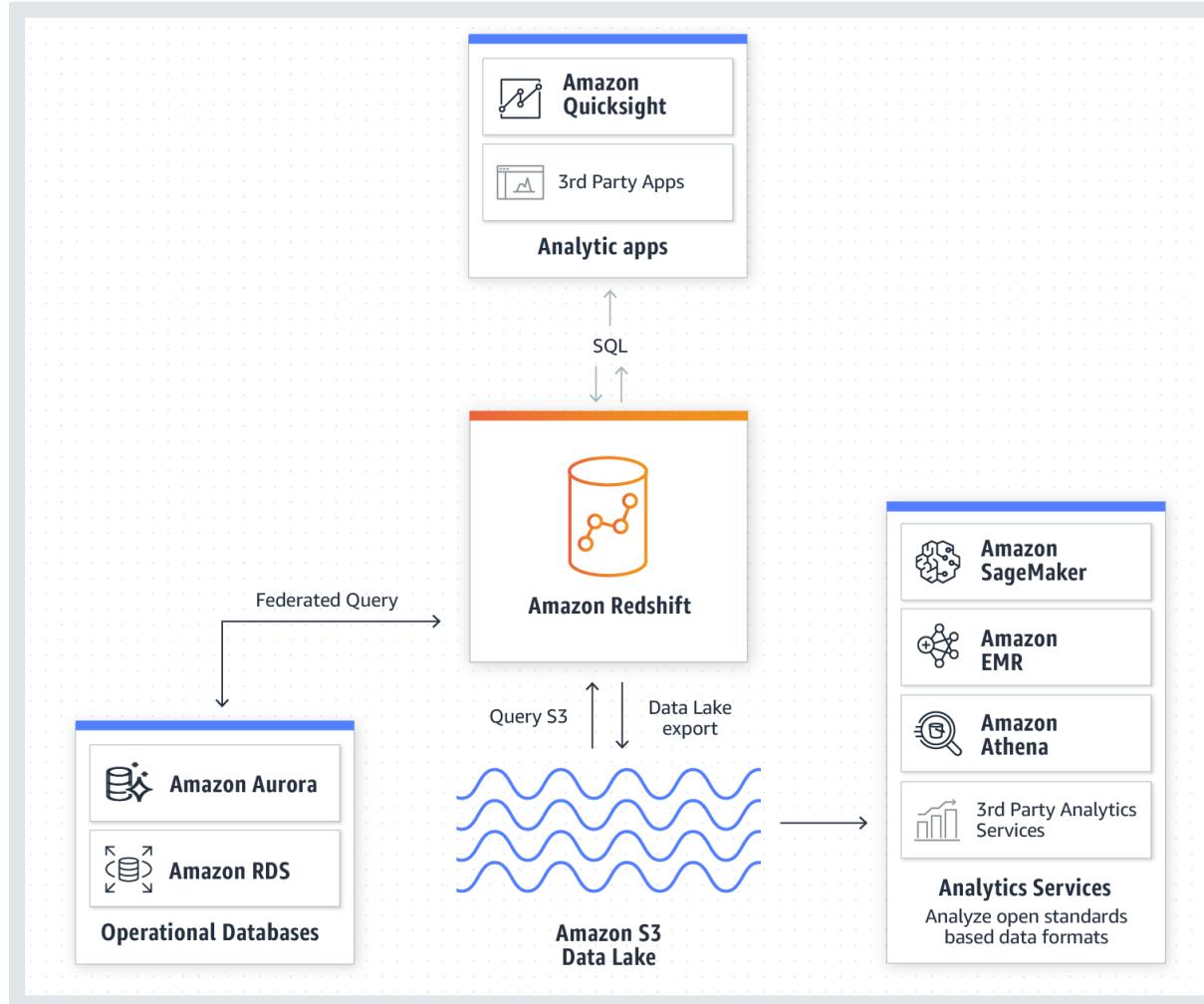
Amazon DynamoDB



Feature	Details
Provisioned throughput	Dial up or down provisioned read/write capacity
Predictable performance	Average single digit millisecond latencies from SSD backed infrastructure
Strong consistency	Be sure you are reading the most up to date values
Fault tolerant	Data replicated across availability zones
Monitoring	Integrated to Cloud Watch
Secure	Integrates with AWS Identity and Access Management (IAM)
Elastic MapReduce	Integrates with Elastic MapReduce for complex analytics on large datasets



Amazon Redshift



Amazon Redshift is a data warehouse product which forms part of the larger cloud-computing platform Amazon Web Services. High Performance, Low-Cost, Petabyte scale data warehouse. Fast, powerful and easy to scale.



Amazon ElastiCache



Feature	Details
Managed	Simplifies and offloads the management, monitoring, and operation of in-memory cache environments.
Compatible	Most client libraries will work with the respective engines they were built for - no additional changes or tweaking required.
Monitored	Detailed monitoring statistics for the engine nodes at no extra cost via Amazon CloudWatch
Memcached	ElastiCache is protocol compliant with Memcached, so popular tools that you use today with existing Memcached environments work seamlessly with the service.
Redis	Open-source in-memory key-value store that supports data structures such as sorted sets and lists. ElastiCache supports Master-Slave replication and Multi-AZ which can be used to achieve cross AZ redundancy.



ElastiCache for Memcached





ElastiCache for Redis

Amazon ElastiCache for Redis



Real-Time Apps



Sub-Millisecond Latency

AWS Monitoring Service

Business Goals

- WHY DO YOU NEED OBSERVABILITY?



Create new
revenue streams



Improve Operational
and Financial
efficiency



Lower
Business Risk

What is Observability?



Amazon CloudWatch

Amazon CloudWatch

- **OBSERVABILITY OF YOUR AWS RESOURCES AND APPLICATIONS**



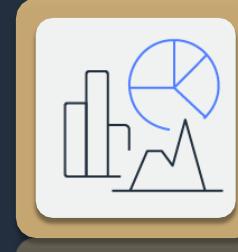
Observability
on a single
platform
across
applications
and
infrastructure



Easiest way to
collect metrics
in AWS and on-
premises



Improve
operational
performance
and resource
optimization



Get
operational
visibility and
insight



Derive
actionable
insights
from logs

Amazon CloudWatch Concepts

- Metrics
- Namespaces
- Dimensions
- Time Stamps
- Units
- Statistics
- Periods
- Aggregation
- Alarms
- Regions



CloudWatch Logs

- STORE LOGS IN NEAR REAL-TIME

Collect logs from:

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

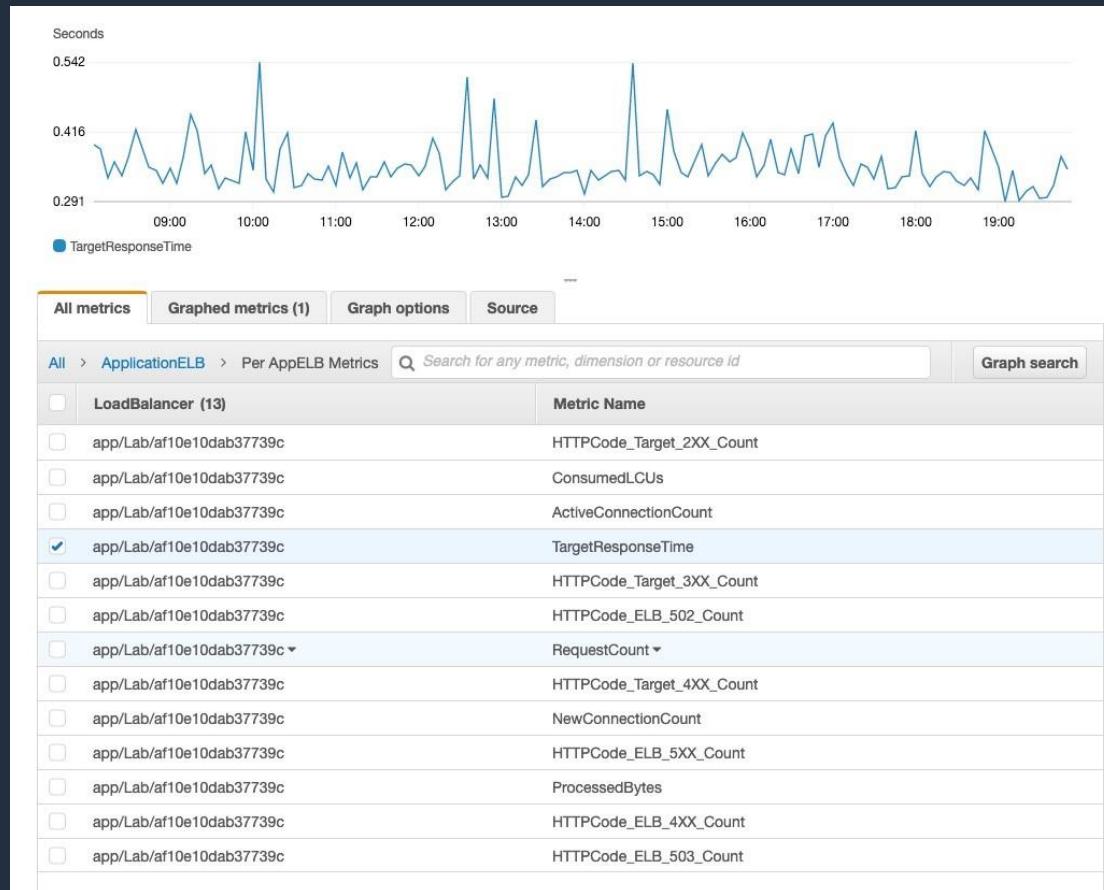
Log data can be stored and accessed indefinitely in highly durable, low-cost storage so you don't have to worry about filling up hard drives.

The screenshot shows the AWS CloudWatch Logs console. At the top, the navigation path is CloudWatch > CloudWatch Logs > Log groups > application.log. To the right are buttons for Delete, Actions, Query log group, and View all log events. The main area is titled "application.log" and contains "Log group details" with fields: Retention (Never expire), Creation time (5 months ago), Stored bytes (14.67 MB), KMS key ID (-), Metric filters (1), Subscriptions (LambdaStream_centralized-logging-LogStreamer-1A2RQLPI4N1TW), and ARN (arn:aws:logs:eu-west-1:012345678910:log-group:application.log:*) and Contributor Insights rules (-). Below this are tabs for Log streams, Metric filters, and Contributor Insights, with Log streams being the active tab. The Log streams section shows five entries with columns for Log stream (checkboxes) and Last event time. The entries are:

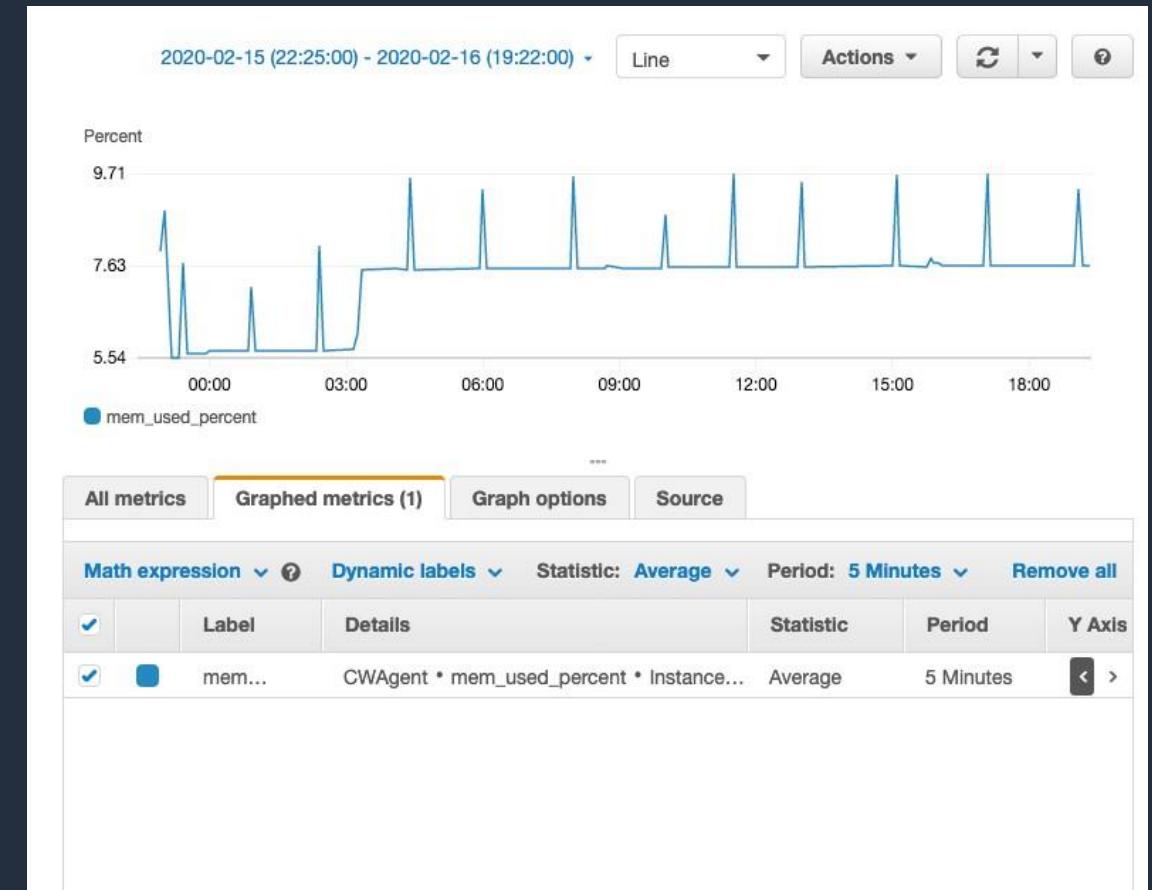
Log stream	Last event time
i-077f7e49ee1c0112c	1/10/2020, 8:00:49 PM
i-03343584efd07d2a6	11/29/2019, 8:03:35 PM
i-09bd407810ebfa83f	11/29/2019, 8:00:52 PM
i-0bf3c984cda70e7c0	9/19/2019, 9:00:35 PM

CloudWatch Metrics

Built-in metrics



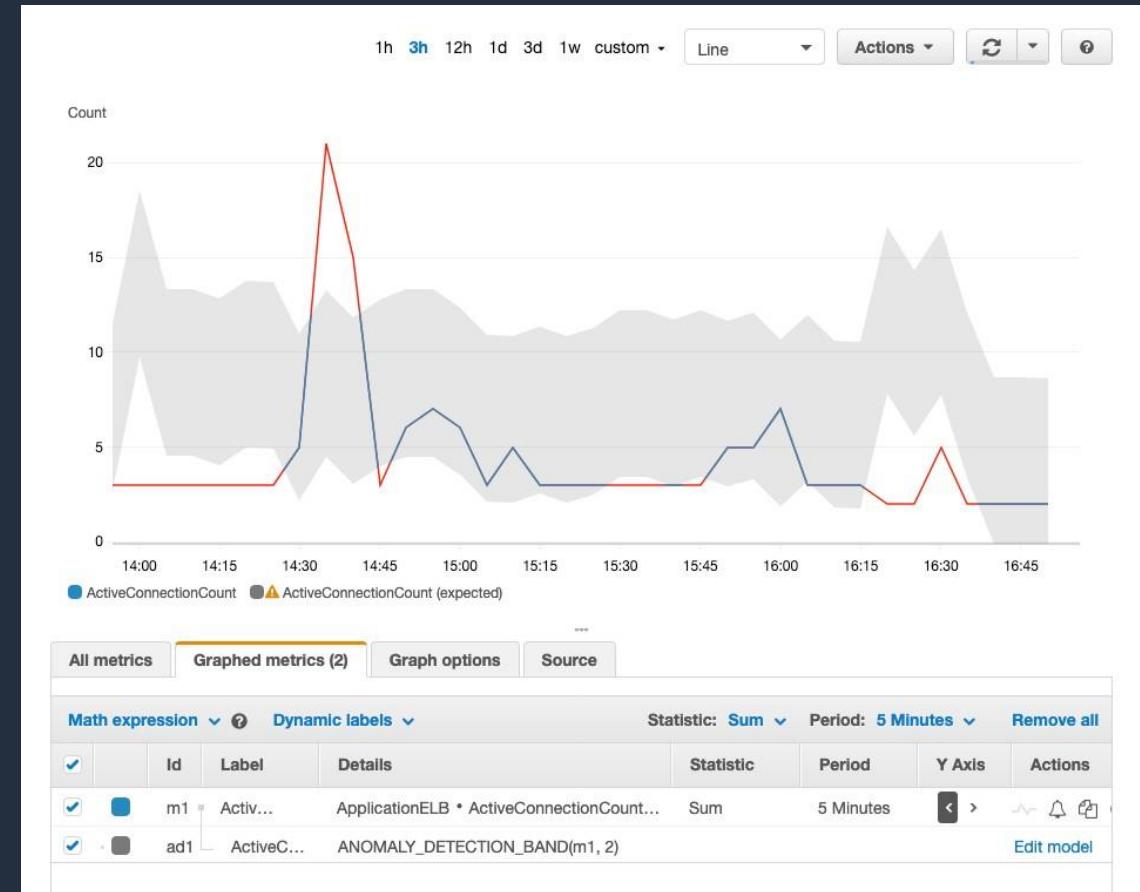
Custom metrics



Anomaly Detection

When you enable anomaly detection for a metric, CloudWatch applies machine learning algorithms to the metric's past data to create a model of the metric's expected values.

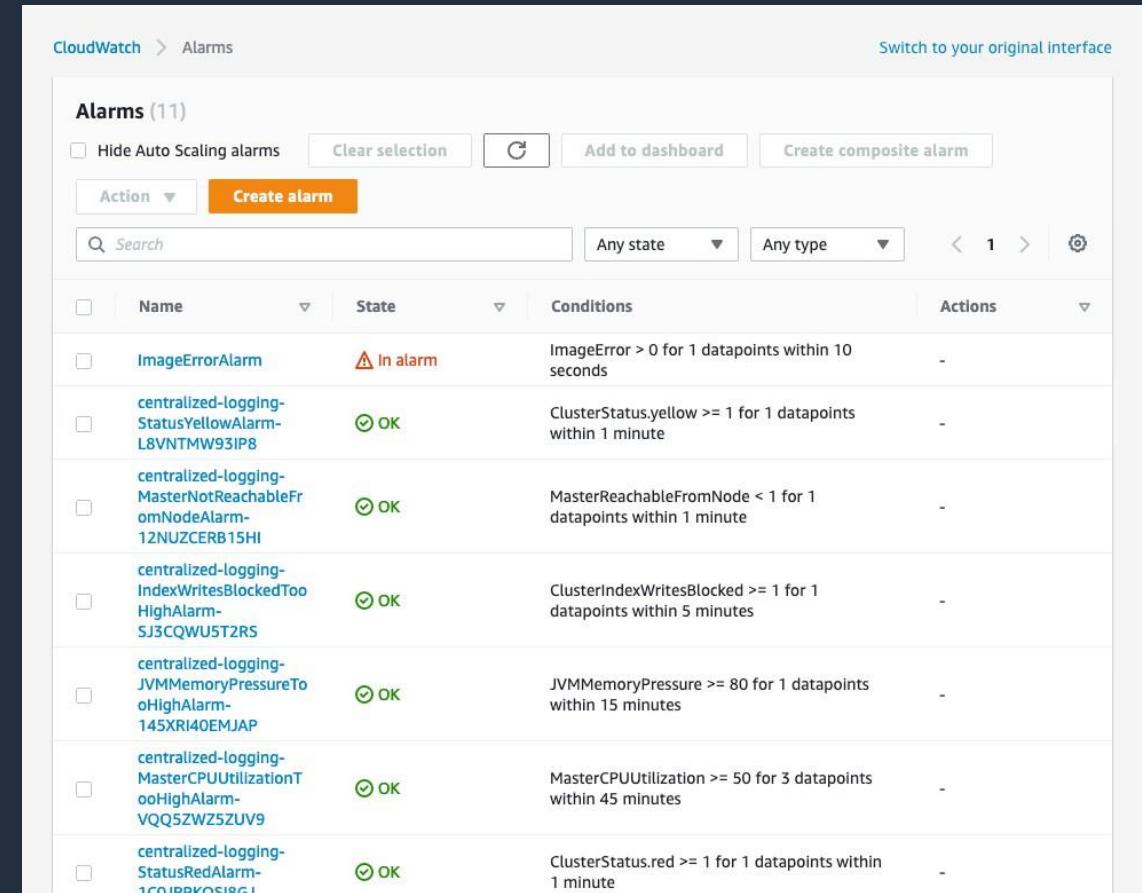
- Create alarms that auto-adjust thresholds based on natural metric patterns
- Alarm when the metric value is above or below the band, or both
- Visualize metrics with anomaly detection bands on dashboards



CloudWatch Alarms

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

- Watch a single metric or the result of a math expression
- Perform actions based on the value of metrics
 - Send a notification to an SNS topic
 - Auto Scaling action
 - EC2Action (Stop, Terminate, Reboot or Recover)
- Add alarms to dashboards to visualize them



The screenshot shows the AWS CloudWatch Alarms console interface. At the top, there's a header with 'CloudWatch' and 'Alarms'. Below the header, there are several buttons: 'Hide Auto Scaling alarms' (unchecked), 'Clear selection', a search bar, and three buttons labeled 'G', 'Add to dashboard', and 'Create composite alarm'. There are also filters for 'Any state' and 'Any type', and navigation controls like arrows and a refresh icon. The main area is titled 'Alarms (11)' and contains a table with the following data:

	Name	State	Conditions	Actions
<input type="checkbox"/>	ImageErrorAlarm	⚠ In alarm	ImageError > 0 for 1 datapoints within 10 seconds	-
<input type="checkbox"/>	centralized-logging-StatusYellowAlarm-L8VNTMW93IP8	🕒 OK	ClusterStatus.yellow >= 1 for 1 datapoints within 1 minute	-
<input type="checkbox"/>	centralized-logging-MasterNotReachableFromNodeAlarm-12NUZCERB15HI	🕒 OK	MasterReachableFromNode < 1 for 1 datapoints within 1 minute	-
<input type="checkbox"/>	centralized-logging-IndexWritesBlockedTooHighAlarm-SJ3CQWU5T2RS	🕒 OK	ClusterIndexWritesBlocked >= 1 for 1 datapoints within 5 minutes	-
<input type="checkbox"/>	centralized-logging-JVMMemoryPressureToohighAlarm-145XR140EMJAP	🕒 OK	JVMMemoryPressure >= 80 for 1 datapoints within 15 minutes	-
<input type="checkbox"/>	centralized-logging-MasterCPUUtilizationTooHighAlarm-VQQ5ZW5ZUV9	🕒 OK	MasterCPUUtilization >= 50 for 3 datapoints within 45 minutes	-
<input type="checkbox"/>	centralized-logging-StatusRedAlarm-1COURPKOSIRGI	🕒 OK	ClusterStatus.red >= 1 for 1 datapoints within 1 minute	-

CloudWatch Events

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

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

Rules > ChangelInstanceSize Actions ▾

Summary

ARN ⓘ arn:aws:events:eu-west-1:180304385487:rule/ChangelInstanceSize

Schedule Cron expression 0 6 ? * 6L *

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

Status Enabled

Description

Monitoring Show metrics for the rule

Targets

Filter:

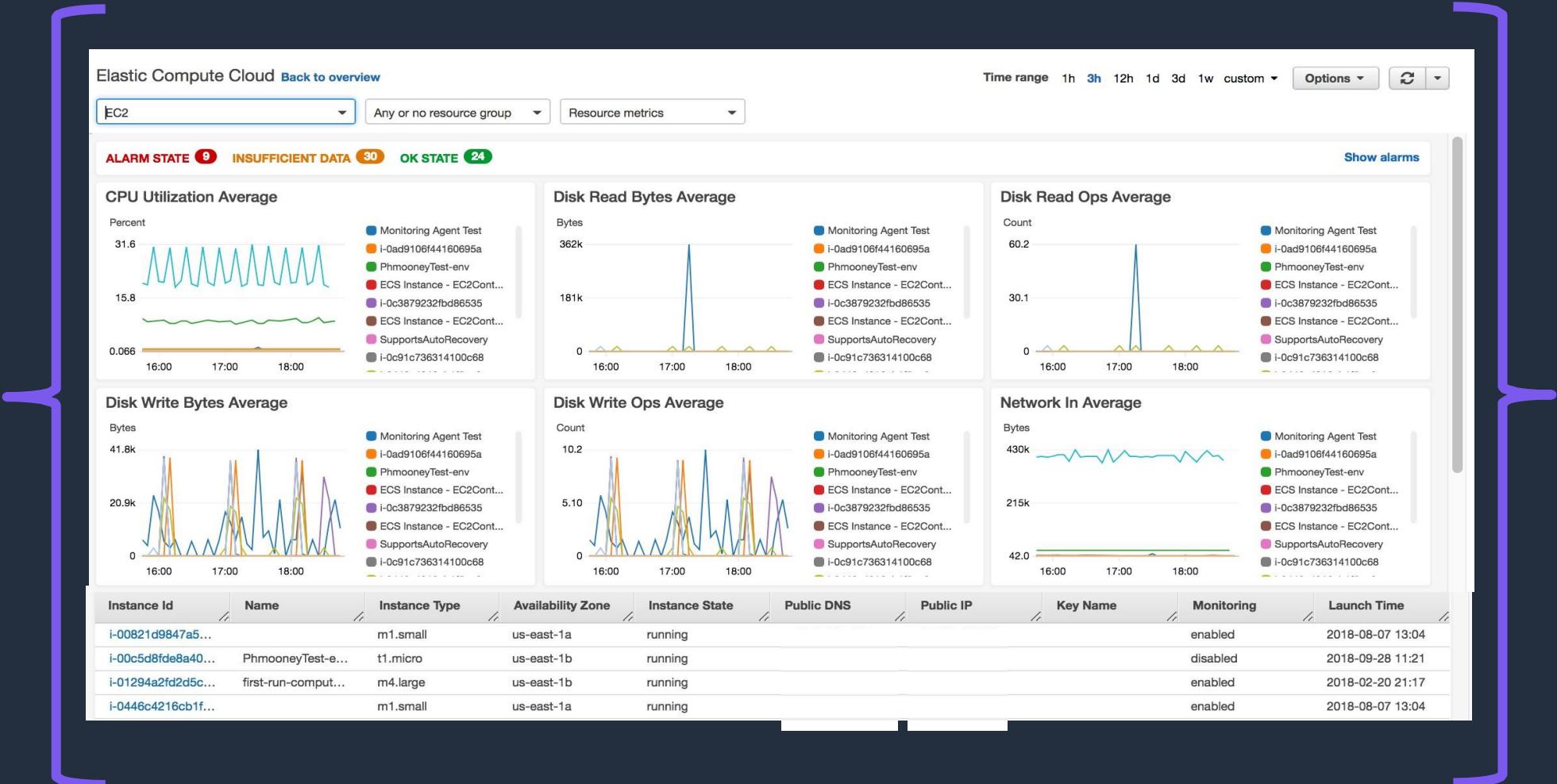
Type	Name	Input
SSM Automation	ChangelInstanceSize (version \$DEFAULT)	Constant: {"InstanceId": ["i-0cb0104ddf22a"]}



CloudWatch Automatic Dashboards

- CloudWatch simplifies infrastructure monitoring with a default, getting started experience.

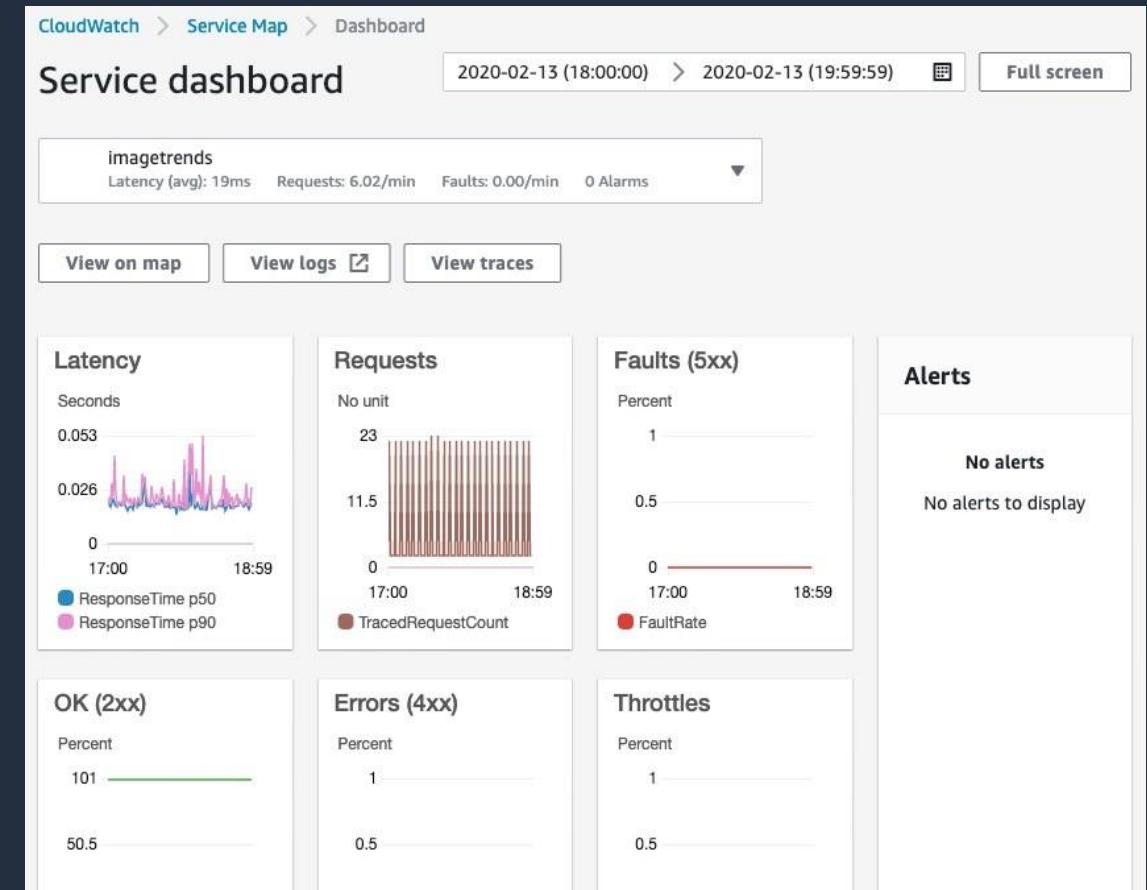
Dynamic, self-updating AWS infrastructure dashboards



CloudWatch ServiceLens

Visualize and analyze the health, performance, and availability of your applications in a single place.

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



AWS CloudTrail & CloudTrail Insights

AWS CloudTrail

- Track user and resource activity across your AWS infrastructure and resources for governance and auditing.
- Identify and respond to unusual usage based on automated analysis.



Capture

Record activity as CloudTrail events



Store

Retain events logs in secure S3 bucket



Act

Trigger actions when important events are detected



Review

Analyze findings or recent and historical activity

AWS CloudTrail Features



Compliance
Aid



Visibility
into Activity



Anomaly
Detection



Detect Data
Exfiltration



Automate
Security
Analysis



Analyze
Permissions

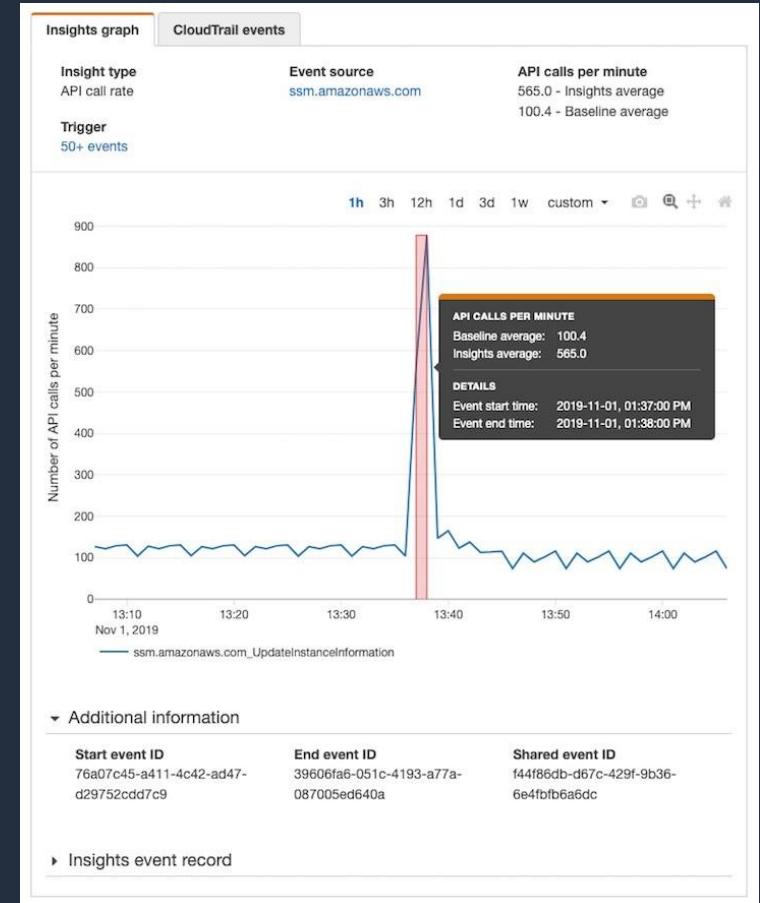


Detect Unusual
Activity

CloudTrail Insights



- Identify and respond to unusual operational activity
 - Unexpected spikes in resource provisioning
 - Bursts of IAM management actions
 - Gaps in periodic maintenance activity
- Automatic analysis of API calls and usage patterns
- Alerts when unusual activity is detected



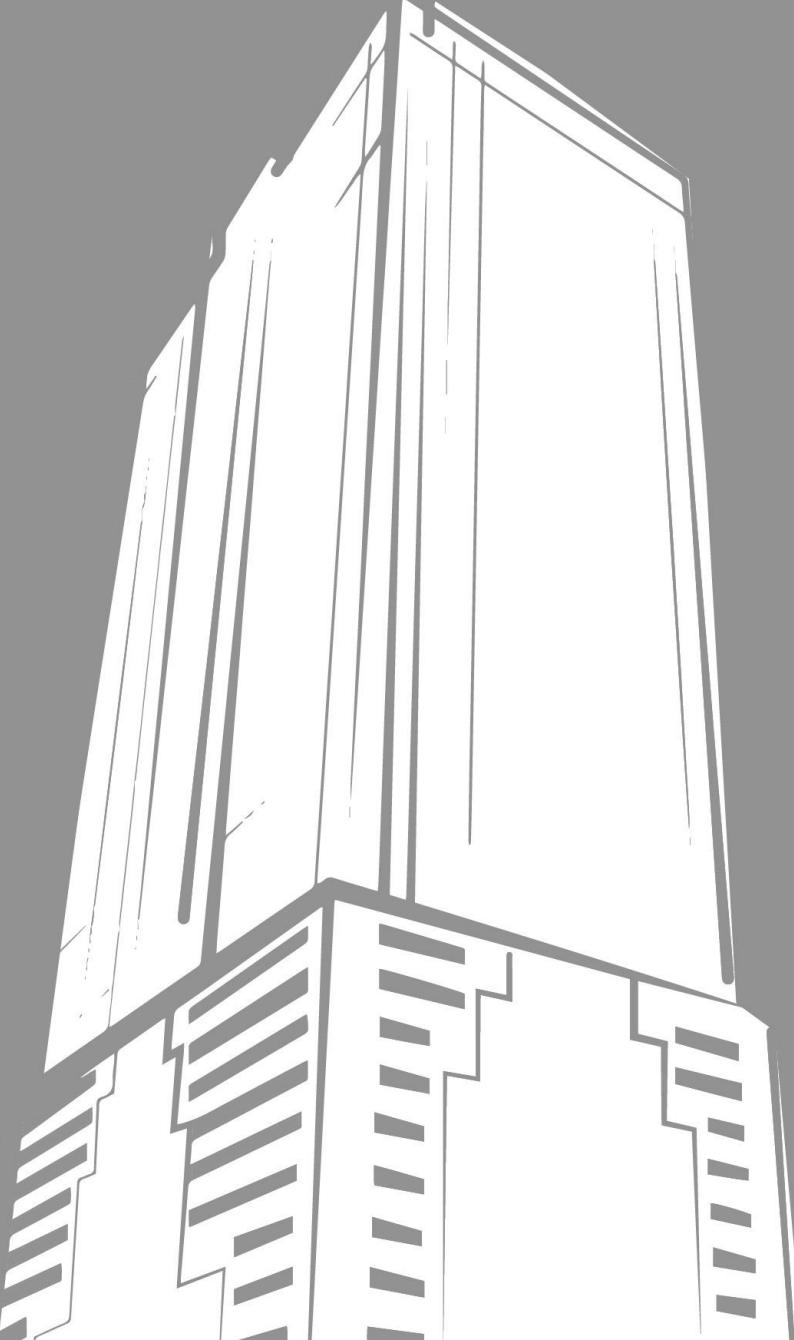
What you can do with CloudTrail today

- Identify users logged in during an incident, and all actions taken during that period
- Notify when admin privileges are granted or console logins occur
- Detect access from authorized networks or IP addresses
- Identify when a file or object has changes to public access, and who made the change
- Understand top user, role, or service callers of API calls or Lambda functions
- Get alerted when you misconfigure your autoscaling script
- Comply with internal and regulatory compliance requirements with the immutable history of all AWS activity

Lab Session - github



<https://github.com/TIDC-PS-Inter/AWS-Workshop>



THAILAND#1

CARRIER NEUTRAL DATA CENTER
AND CLOUD SERVICE PROVIDER