Designing Well Architected Framework- Week 2

Performance Efficiency, Operational Excellence, and Security

Rohit Bhardwaj

Hands-on Director of Architecture, Salesforce

Founder: ProductiveCloudInnovation.com

Twitter: rbhardwaj1

LinkedIn: www.linkedin.com/in/rohit-bhardwaj-cloud

tinyurl.com/DesigningWellArchitected

https://www.productivecloudinnovation.com/lessons

Design Resilient Architectures

Design Cost-Optimized Architectures

Sustainability Architectures

Design Performant Architectures

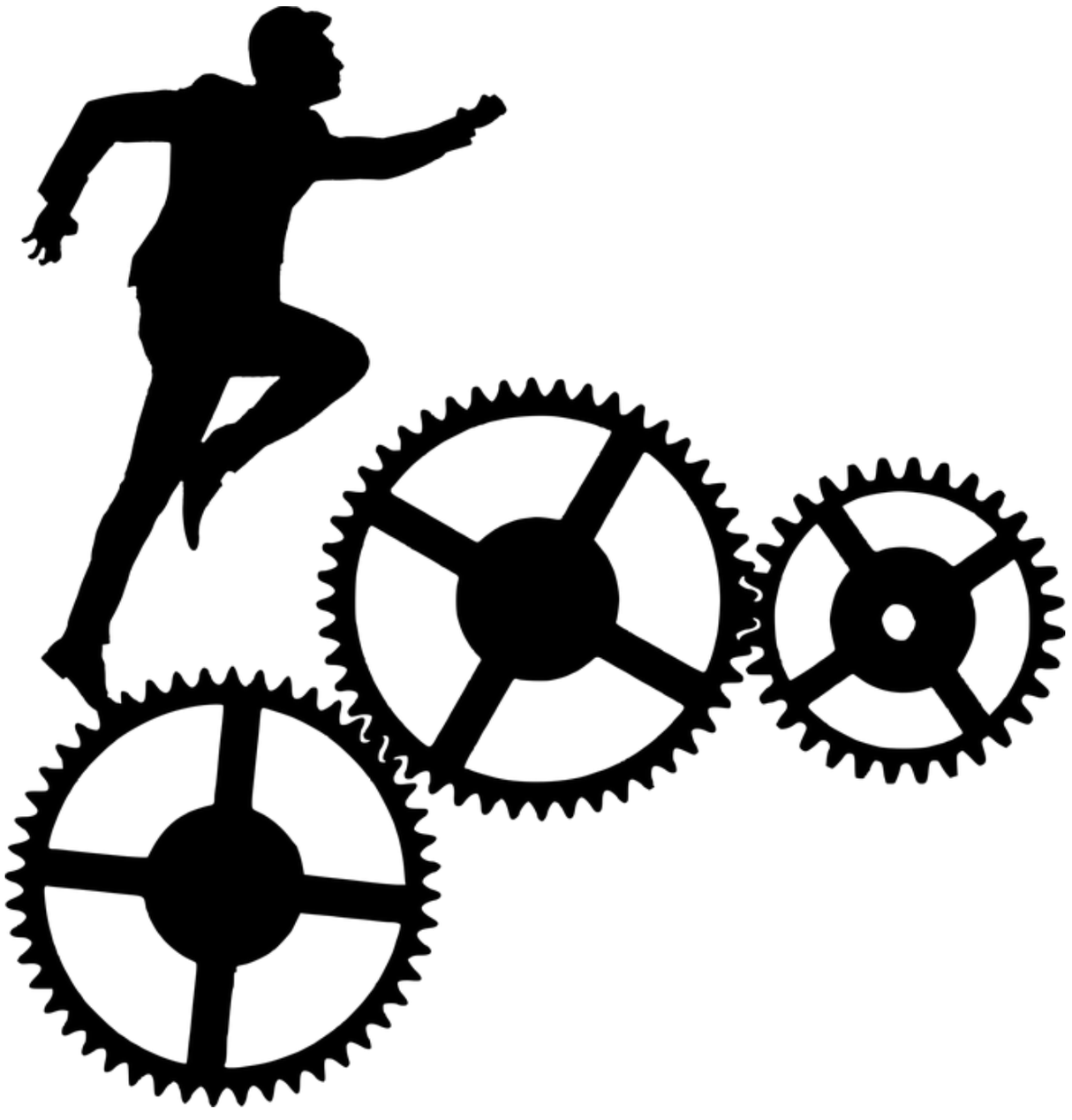
Operationally Excellent Architectures

Specify Secure Applications

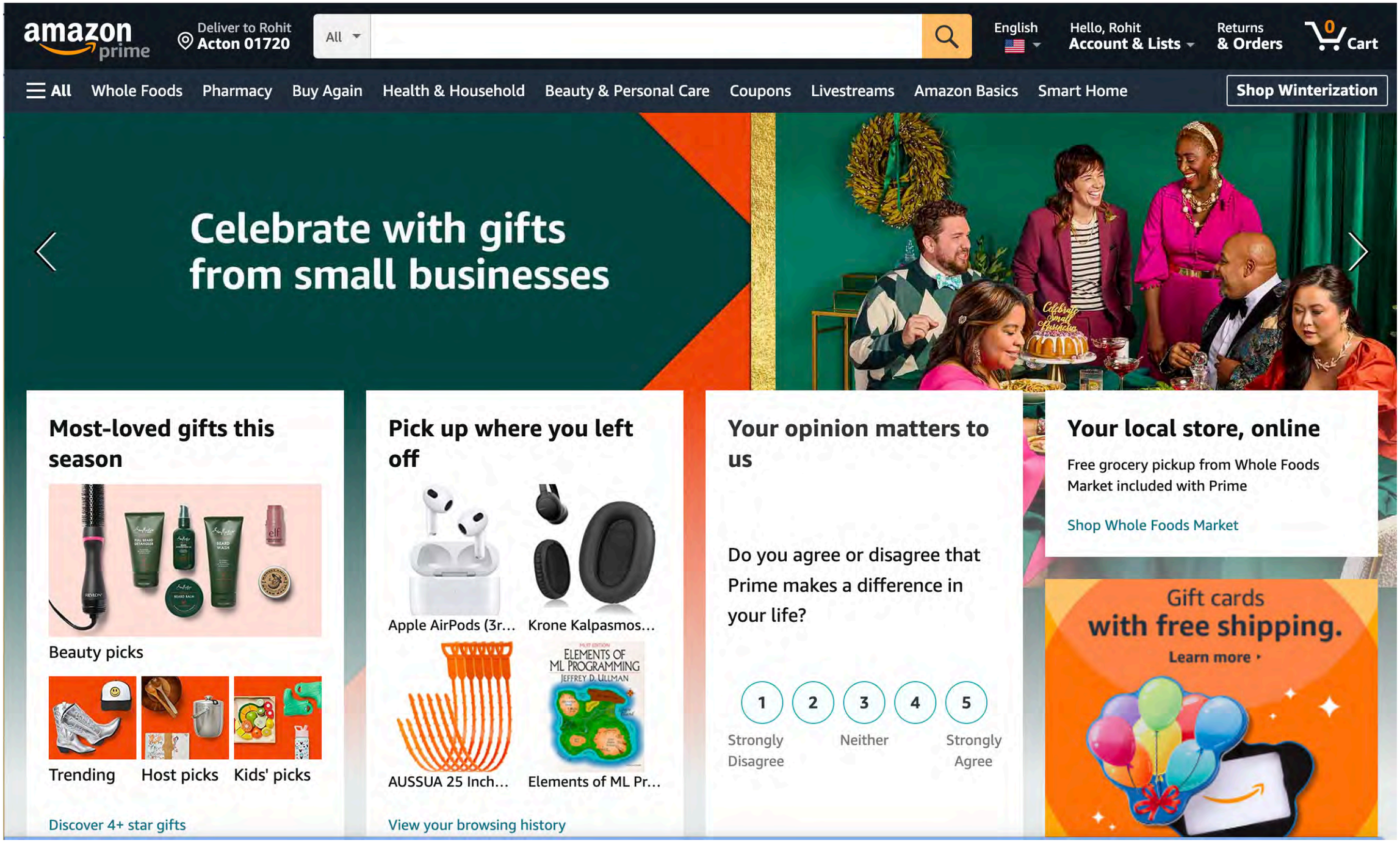
Well Architected Framework

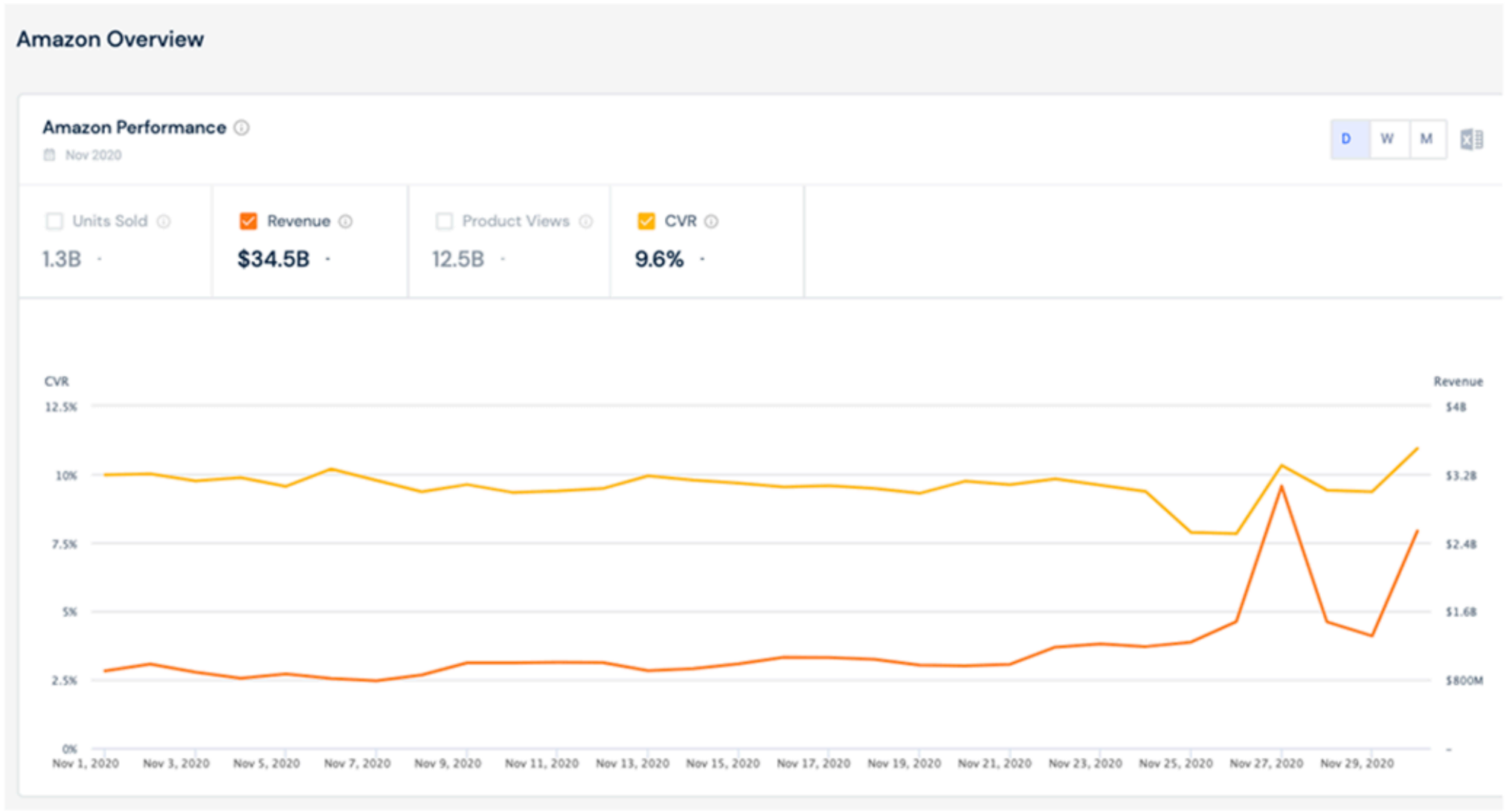
tinyurl.com/DesigningWellArchitected

Performance Efficient Architectures



How does Amazon/Ebay design for performance?





similarweb

$6.3 million per minute online, at an average of $27.50 per person.

Black Friday 2020 was the second-highest online spending day in U.S. history, bringing in a total of $9 billion

Keep your ride running smoothly

Shop transmissions, differentials, and clutch components.

Get the parts →

The Andy Warhol Collection

Shop original sketches, prints and posters

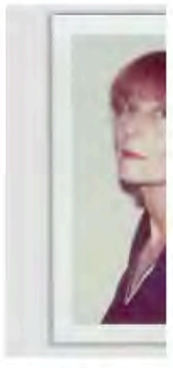
Shop Now →

$4,000.00

$4,000.00

$7,000.00

$10,000.00



$5,000.00

What are the issues in Performance?

Think about Availability

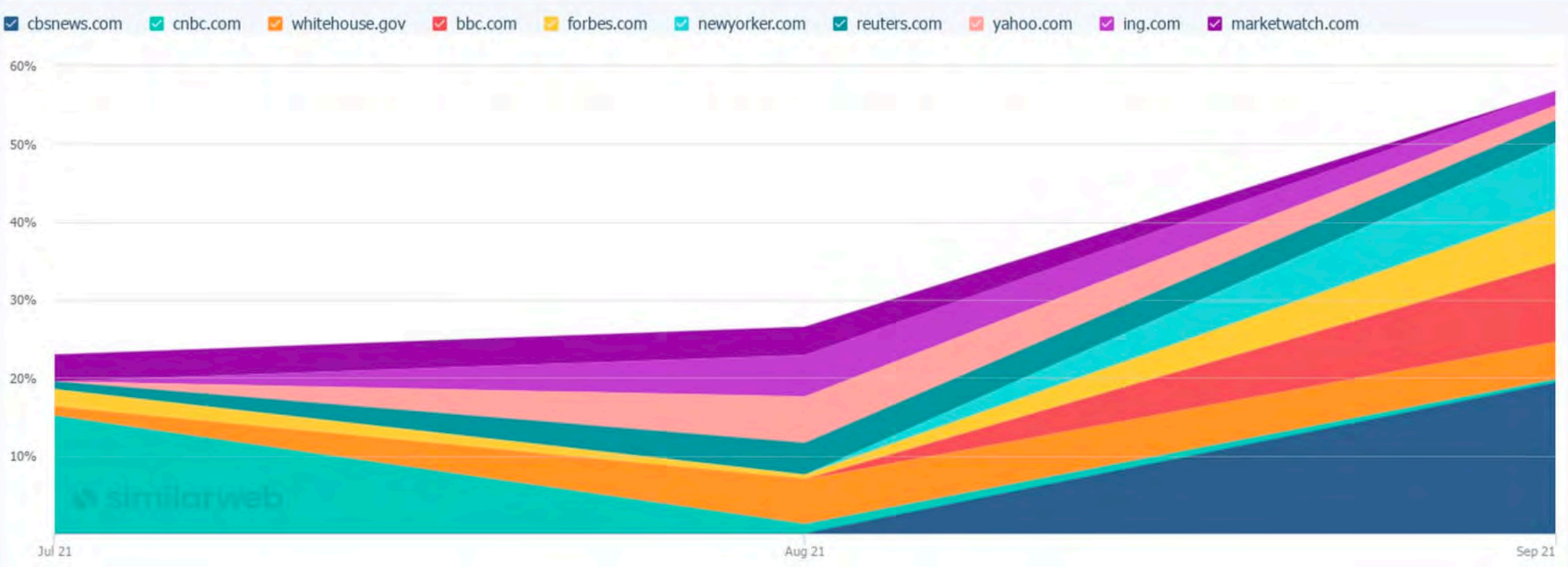
Think about Response time

Think about Data

Think about Distributed Data

Traffic distribution

Jul 2021 - Sep 2021 | Worldwide | Organic Only | Keyword 'supply chain issues'

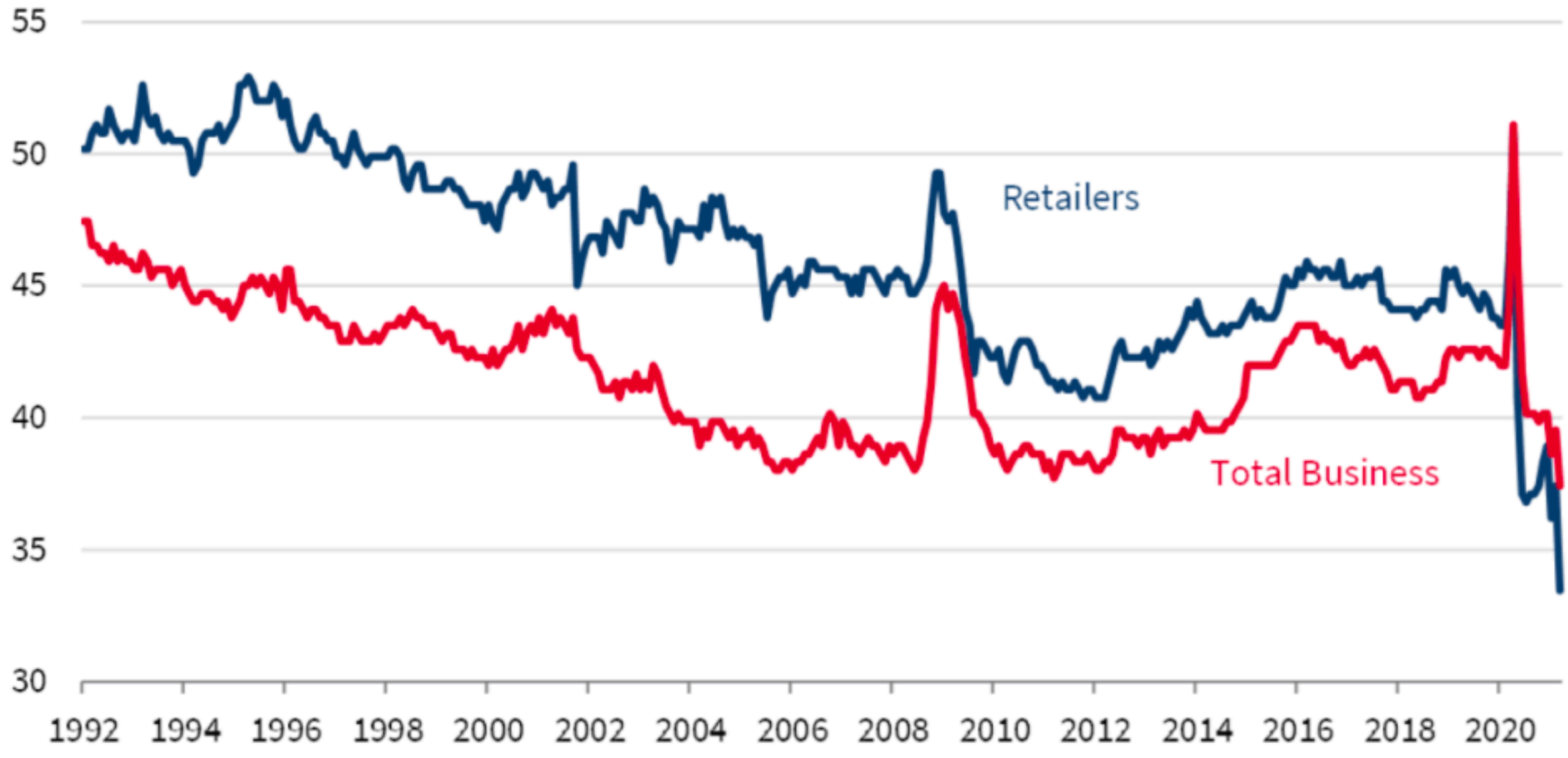


similarweb

https://www.similarweb.com/corp/blog/ecommerce/amazon-insights/global-supply-chain/

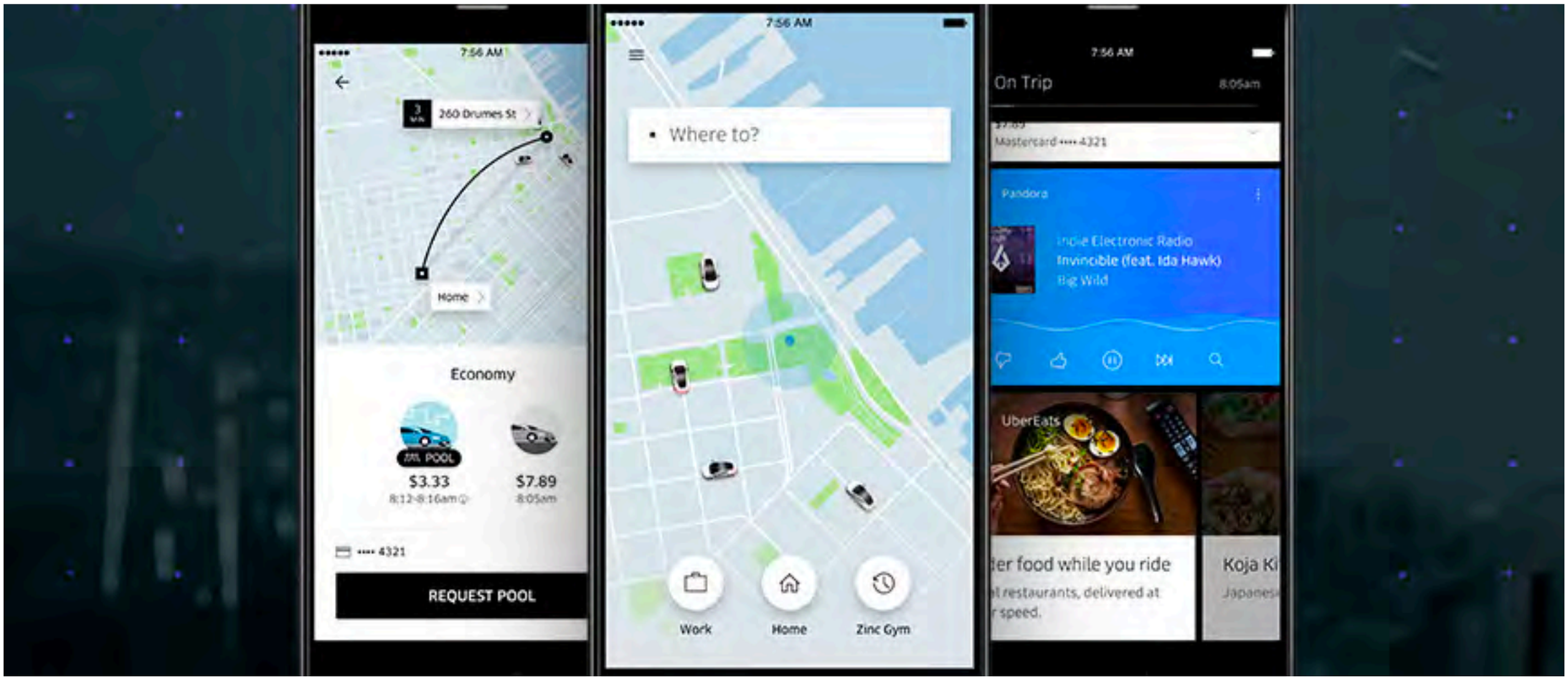
Figure 1. Businesses Have Little Inventory to Sell

Inventory-to-sales ratio (days of sales in inventory)



Sources: U.S. Census Bureau; CEA Calculations

Uber/Lyft design



https://www.uber.com/blog/new-rider-app-architecture/

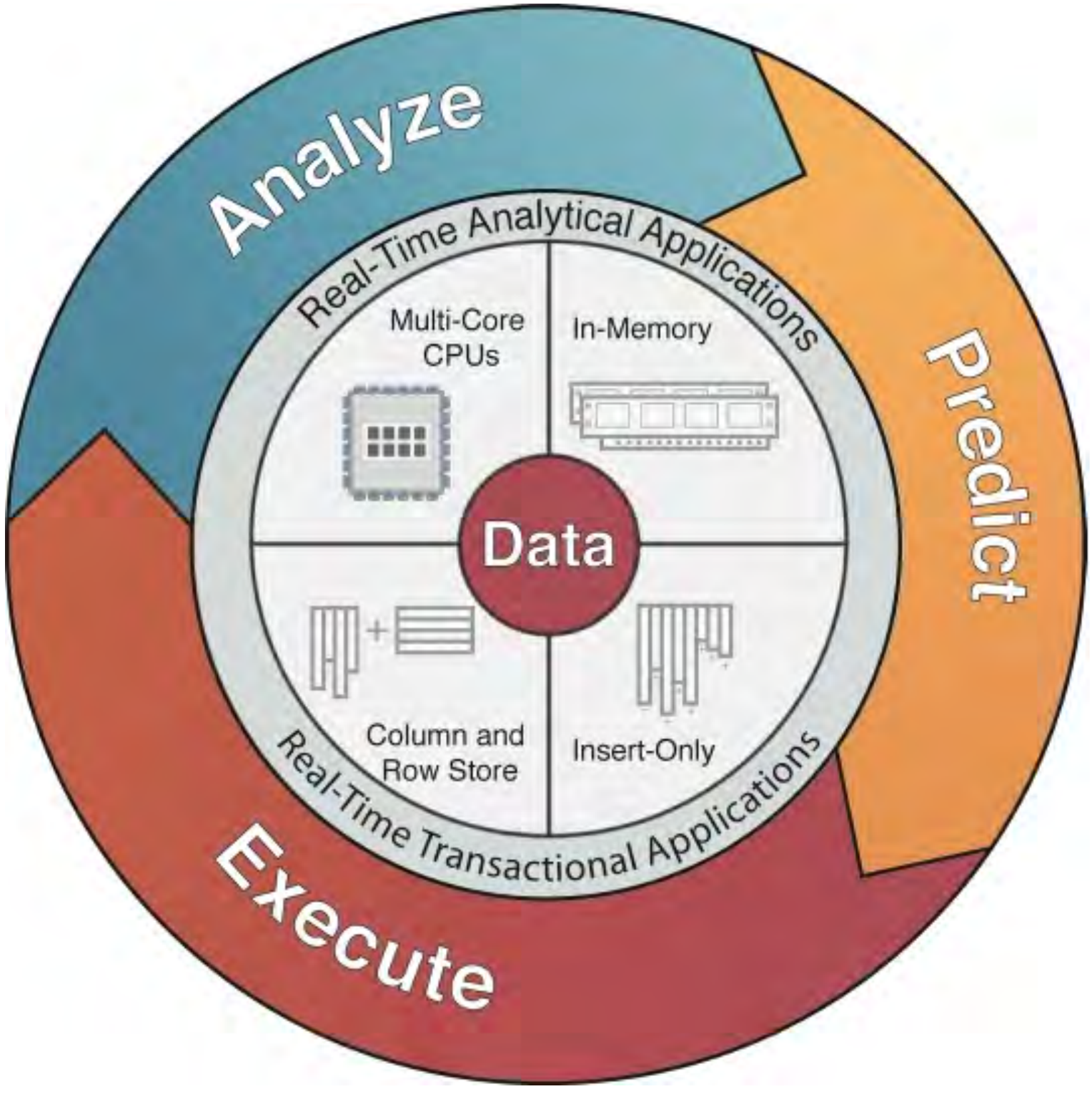
For Impatient Web Users,
an Eye Blink Is Just Too Long to Wait

250 ms is magic number

https://www.nytimes.com/2012/03/01/technology/impatient-web-users-flee-slow-loading-sites.html?pagewanted=all&_r=0

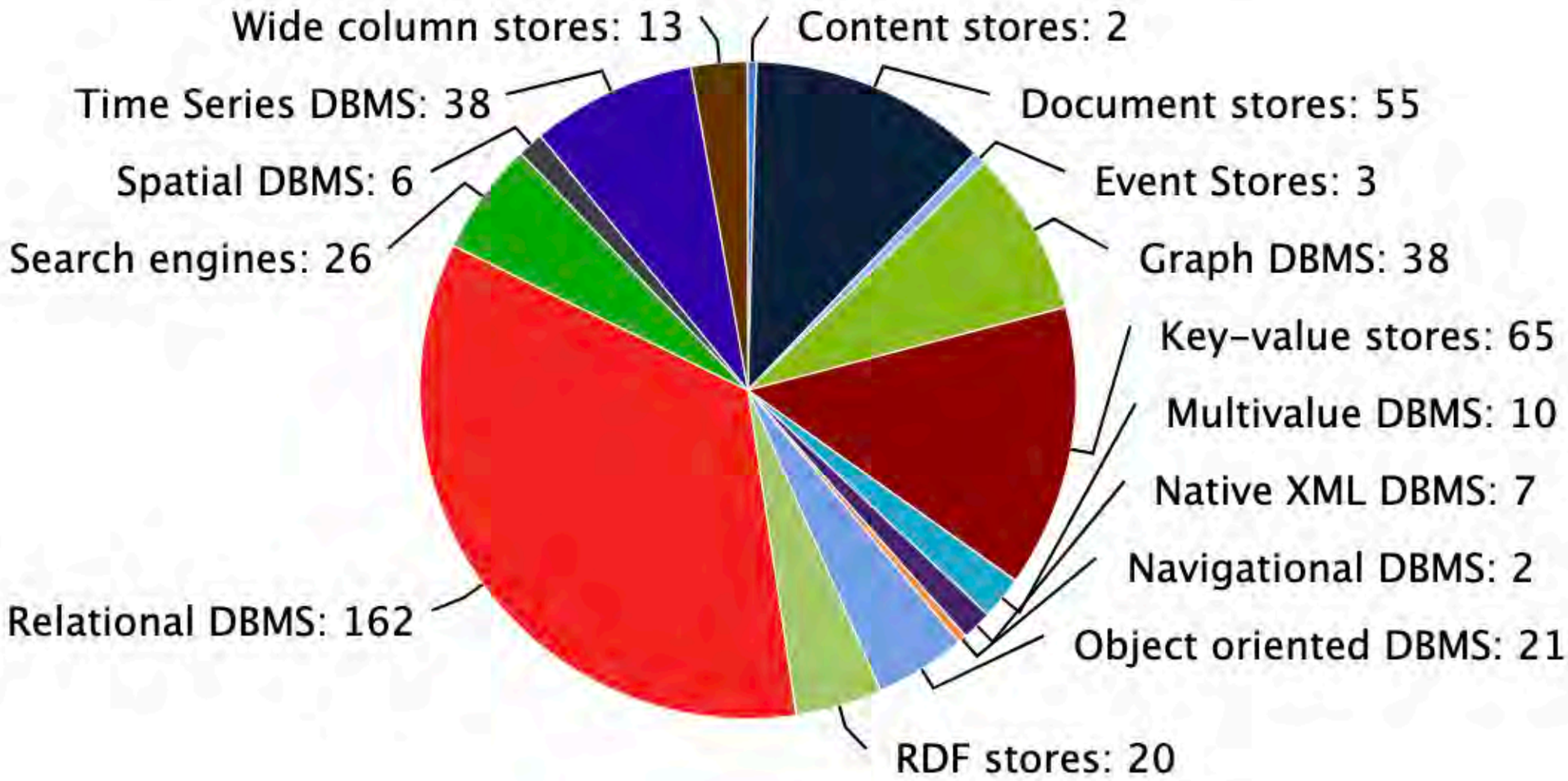
How do you select the best-performing architecture?

How No-SQL helps with performance

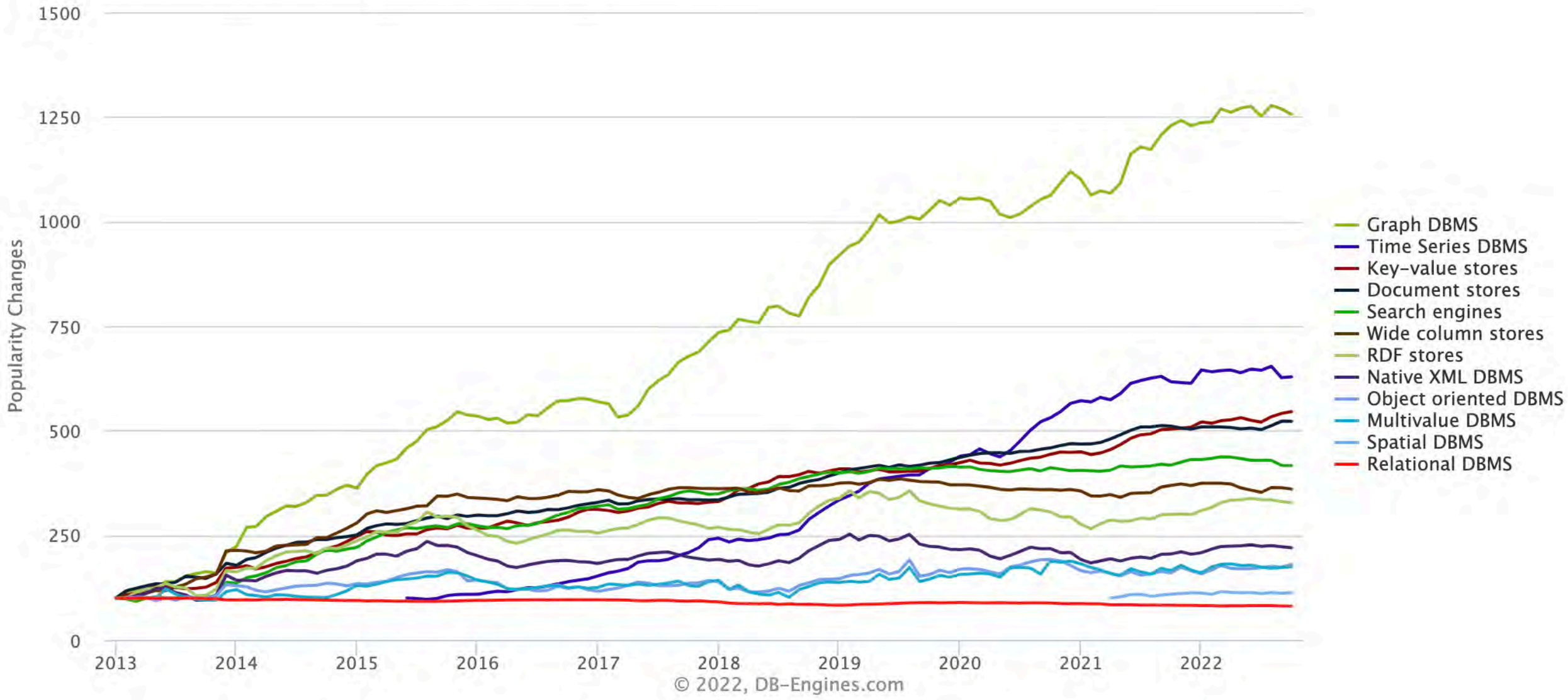


Big Data

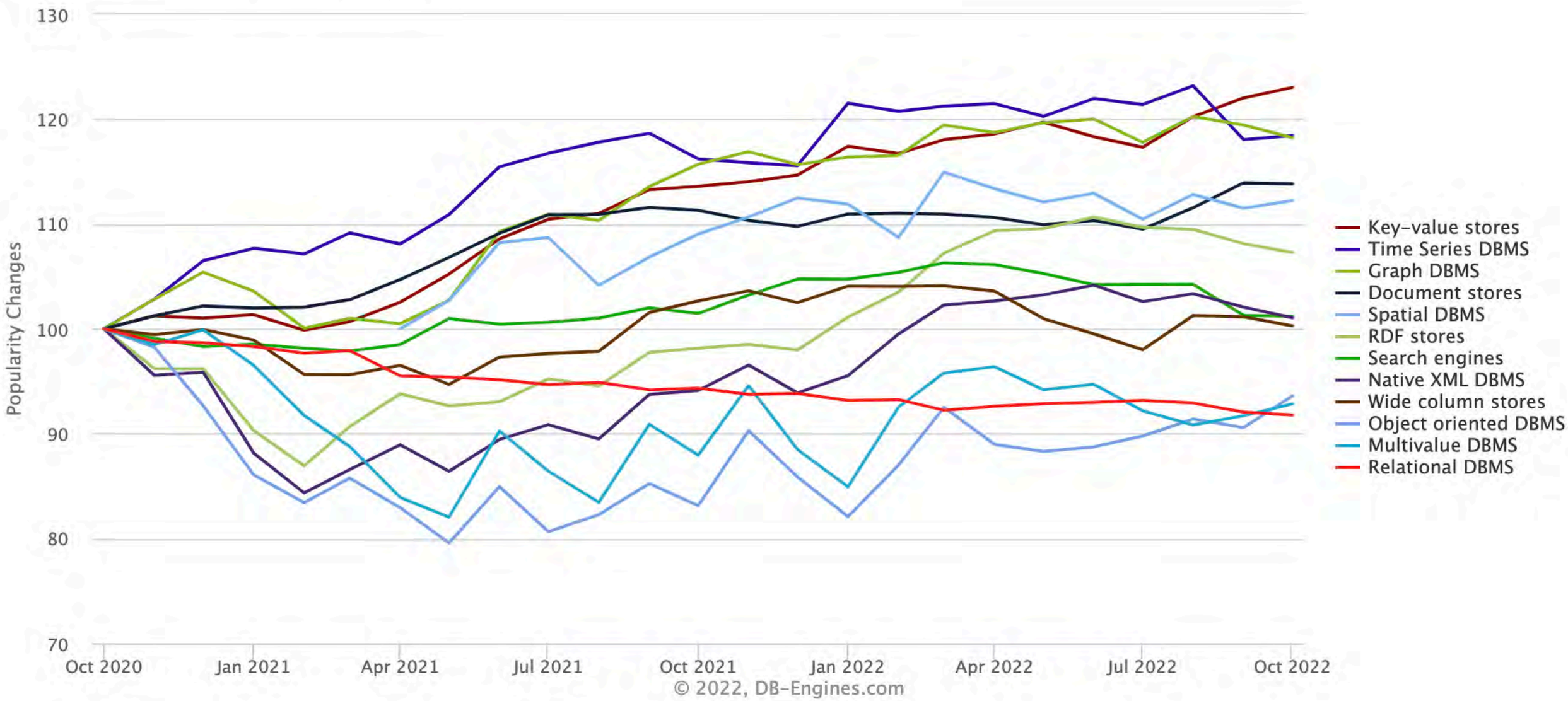
Number of systems per category, October 2022

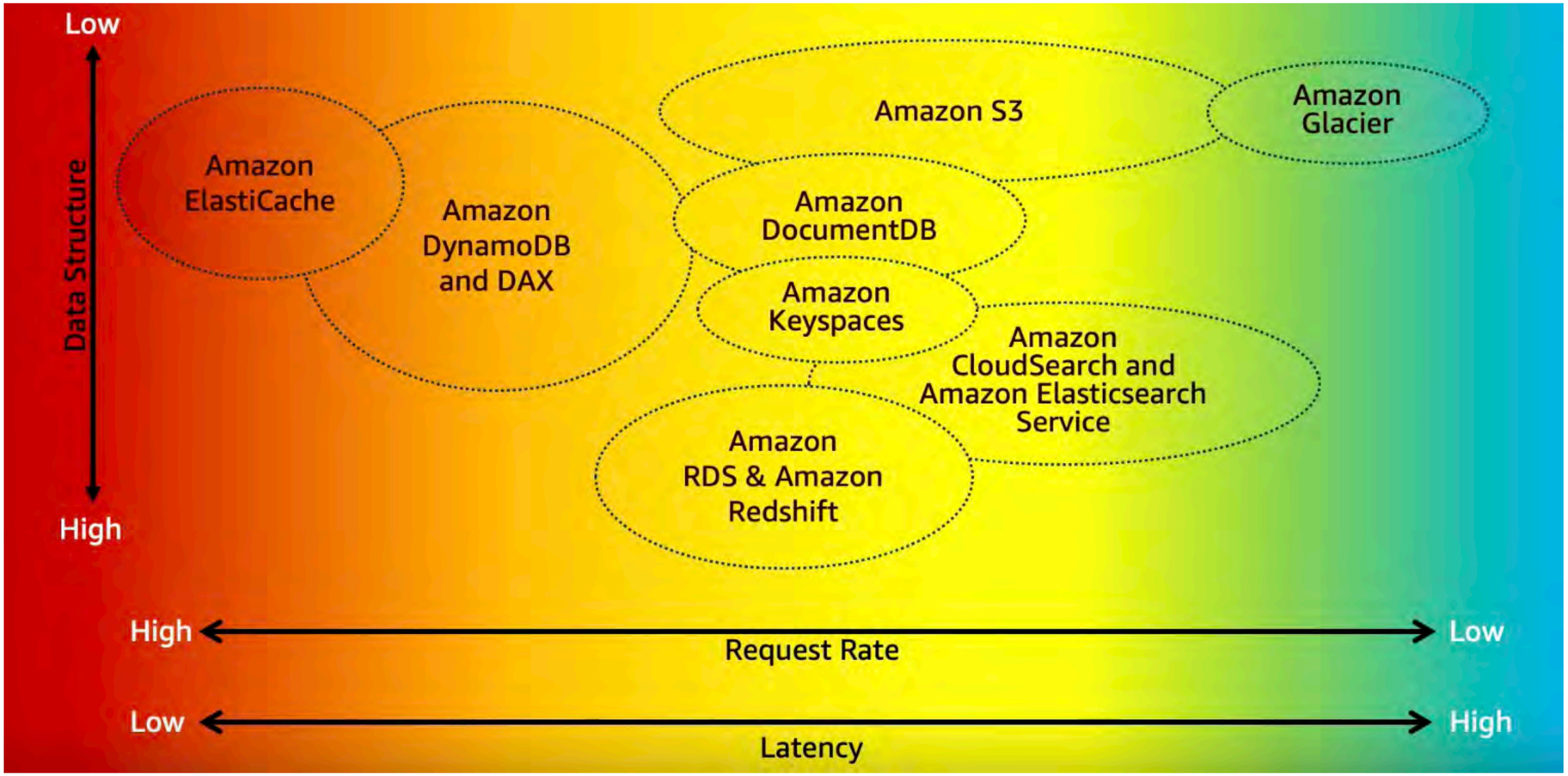


Complete trend, starting with January 2013



Trend of the last 24 months




Low
Data Structure
High
Amazon ElastiCache
Amazon DynamoDB and DAX
Amazon S3
Amazon Glacier
Amazon DocumentDB
Amazon Keyspaces
Amazon CloudSearch and Amazon Elasticsearch Service
Amazon RDS & Amazon Redshift
High
Request Rate
Low
Low
Latency
High

Application Enterprise Architecture Diagram

Gateways

- Portal
- B2B Gateway

Sales and Marketing

- Channel Management
- Leads Management
- Sales Force Management
- Campaign Management
- Quoting

Customer Interaction

- Contact Management
- Customer Management
- Order Entry
- Trouble Tracking

Finance

- Customer Risk Management
- Revenue Assurance
- Billing
- Medication and Rating
- Accounting
- Vendor Billing Reconcillation

Business Intelligence

- Corporate Data Warehouse
- Decision Support Systems
- Reporting

Product Management

- Product Catalog

Service Delivery

- Order Management
- Inventory
- Service Image
- Assign and Design
- Workforce Management
- Vendor Order Management
- Capacity Planning
- Provisioning Interconnection

Service Assurance

- Activation Management
- Performance Management
- Trouble Management
- Testing and Diagnostics
- Service Level Management
- Usage Data Collection
- Fault Management
- Network / Element Management

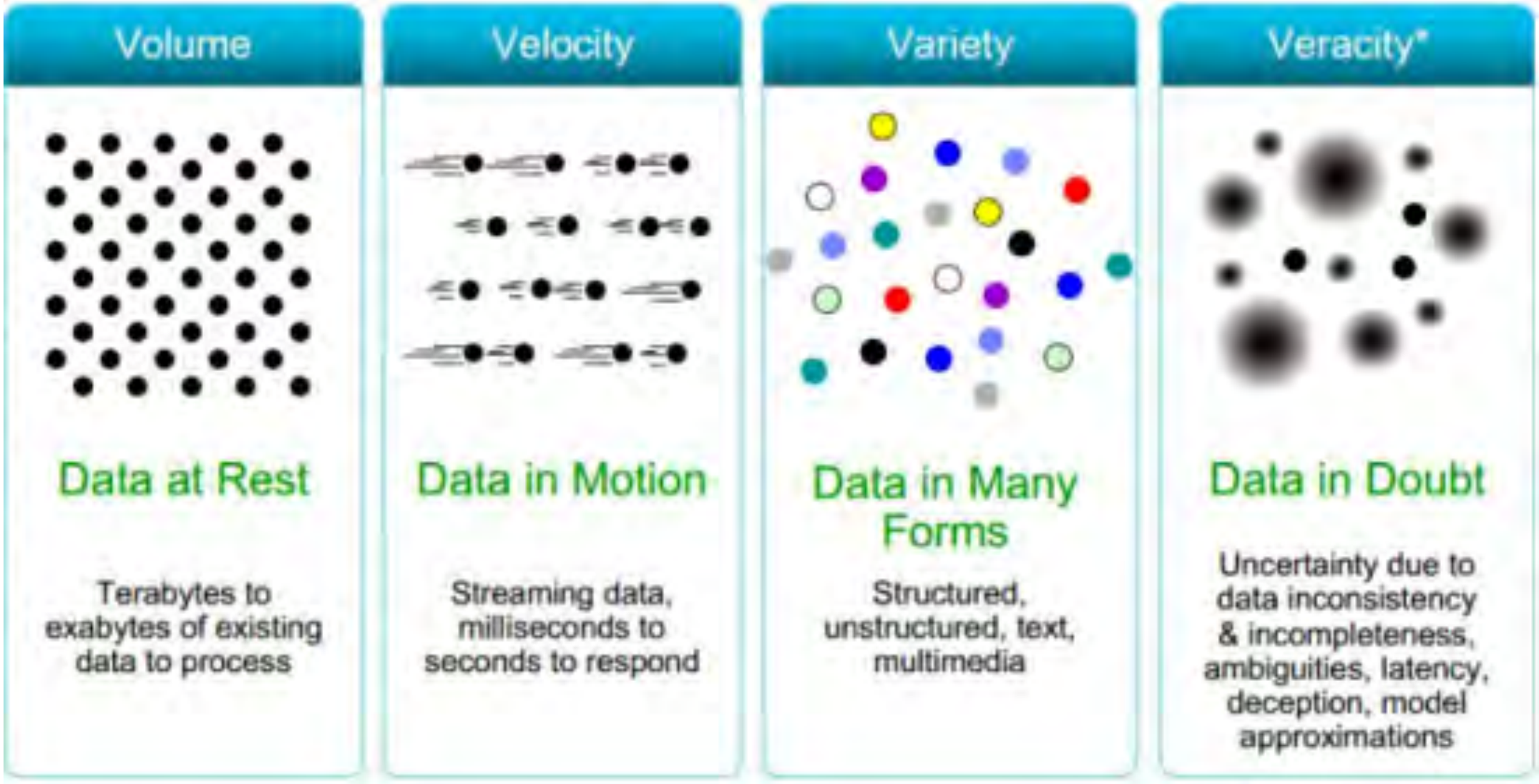
Corporate

- Assest Management
- Human Resources
- Tax and Regulatory
- Legal
- Corp Governance
- Document Managment

big data

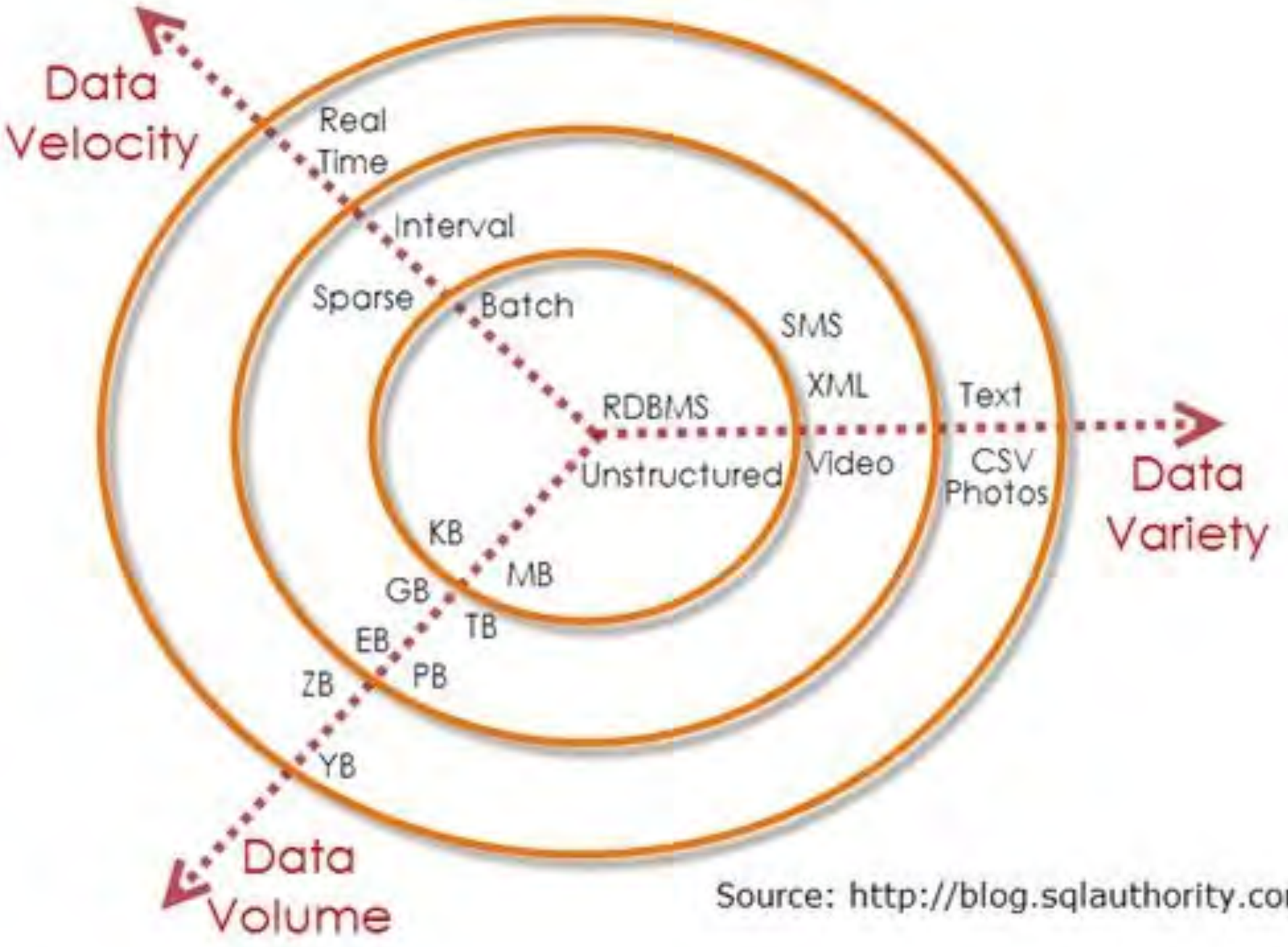
http://mattturck.com/wp-content/uploads/2016/03/Big-Data-Landscape-2016-v18-FINAL.png

Big data characteristics

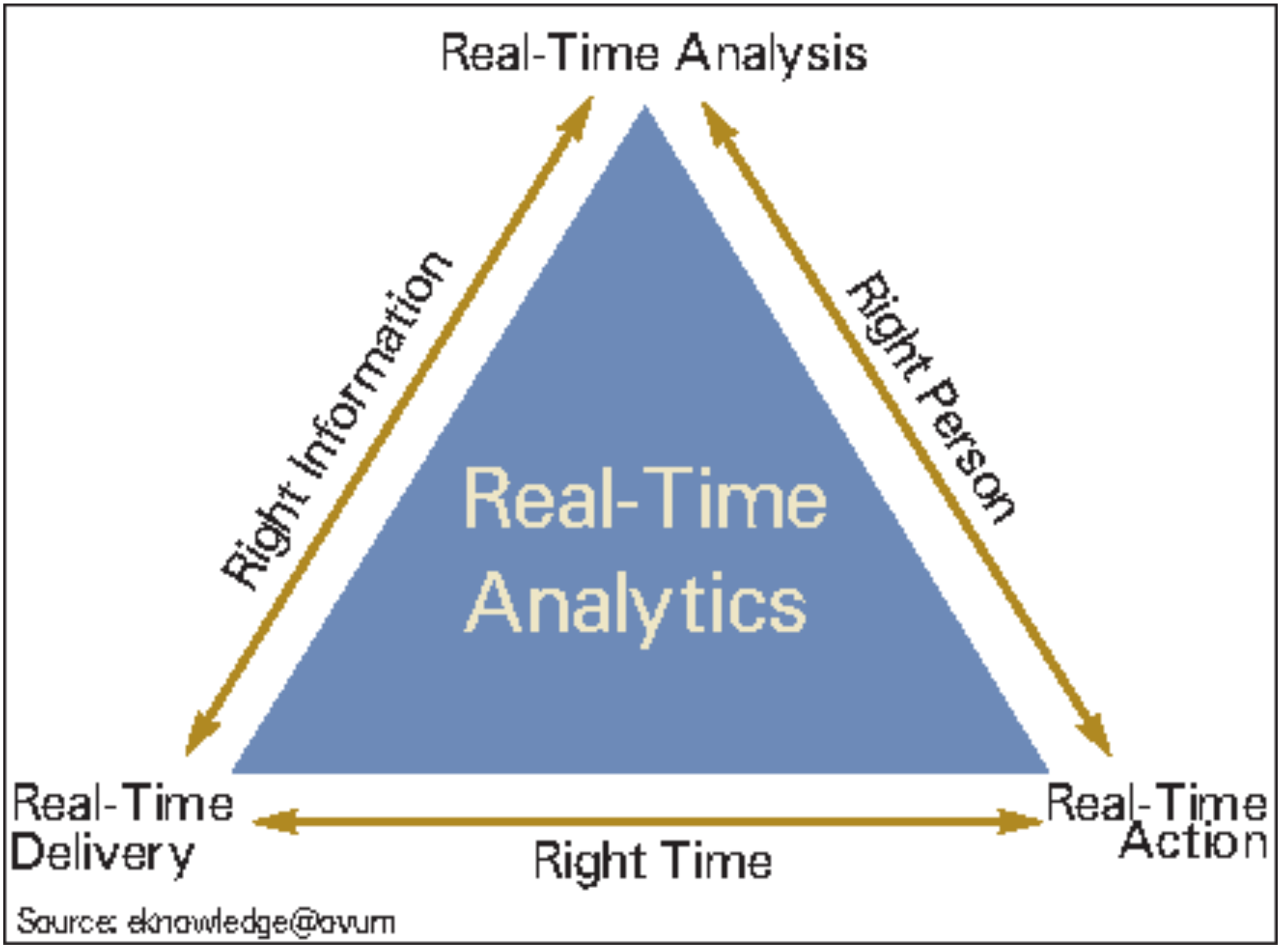


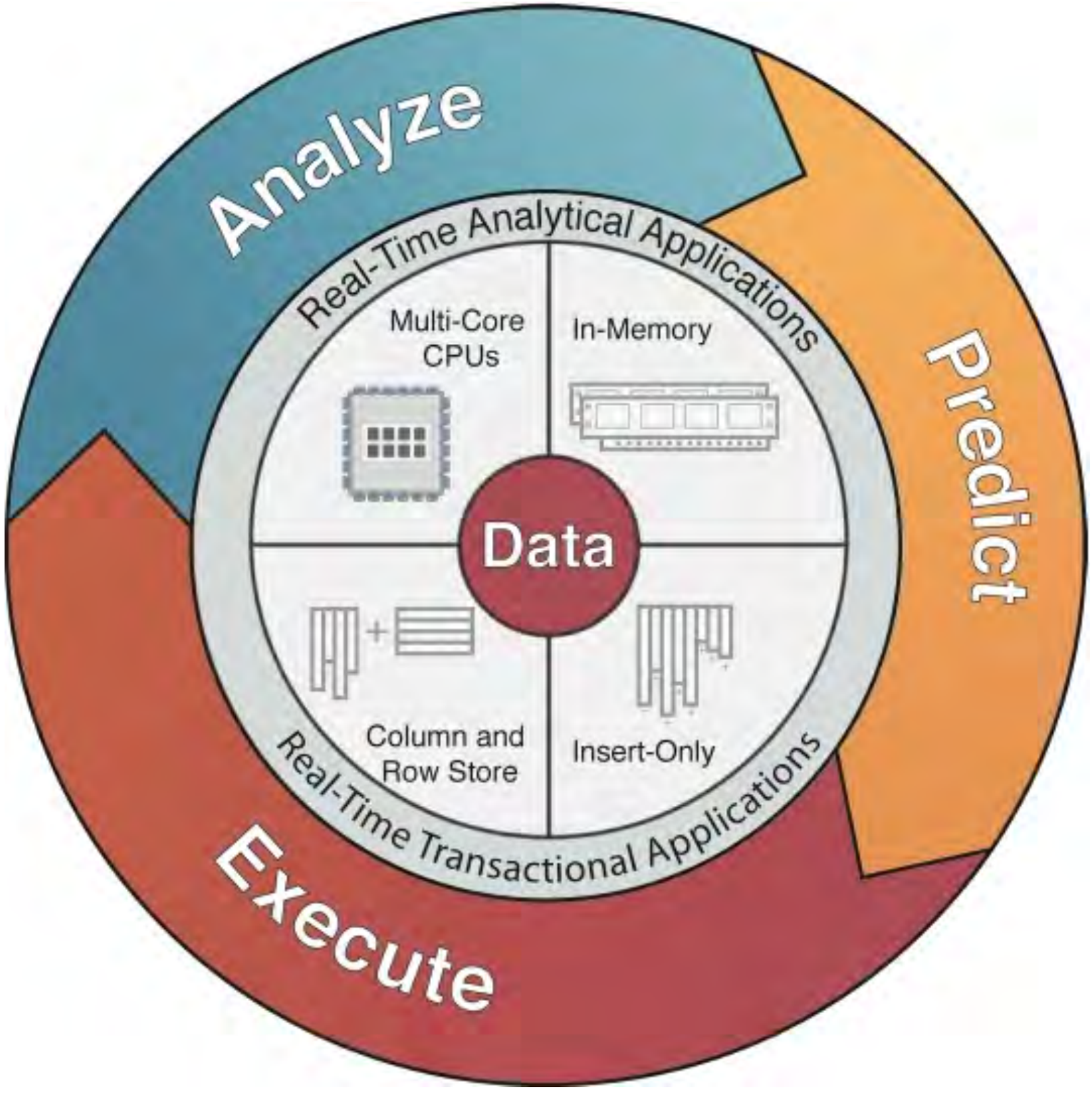
https://imasaikirangeek.files.wordpress.com/2014/05/defining-big-data1.png

3Vs of Big Data



Source: http://blog.sqlauthority.com


Real-Time Analysis
Right Information
Right Person
Real-Time Analytics
Real-Time Delivery
Right Time
Real-Time Action
Source: eknowledge@ovum



https://www.qubole.com/resources/solution/best-use-cases-for-big-data-analytics/

- Would ACID work with Bigdata ?

replication

```
SELECT COUNT(ArtifactID) FROM Document WHERE AccessControlListID_D IN (1,1000062) AND
(ArtifactID IN
 (SELECT ArtifactID FROM Document WHERE AccessControlListID_D IN (1,1000062)
  AND EXISTS
  (SELECT CodeArtifactID FROM CodeArtifact WHERE AssociatedArtifactID = Document.ArtifactID
   AND CodeArtifactID IN (17375543,17375544)
 ))
 OR ArtifactID IN
 (SELECT ArtifactID FROM Document WHERE AccessControlListID_D IN (1,1000062) AND
   (EXISTS
    (SELECT CodeArtifactID FROM CodeArtifact
     WHERE AssociatedArtifactID = Document.ArtifactID AND CodeArtifactID IN (13002091,13002080,17018689,13002017)
    )
    AND NOT EXISTS
    (SELECT CodeArtifactID FROM CodeArtifact WHERE AssociatedArtifactID = Document.ArtifactID
     AND CodeArtifactID IN (16851390,17018659)
   ))
))
```

db sharding

Key	Name	Description	Stock	Price	LastOrdered
ARC1	Arc welder	250 Amps	8	119.00	25-Nov-2013
BRK8	Bracket	250mm	46	5.66	18-Nov-2013
BRK9	Bracket	400mm	82	6.98	1-Jul-2013
HOS8	Hose	1/2"	27	27.50	18-Aug-2013
WGT4	Widget	Green	16	13.99	3-Feb-2013
WGT6	Widget	Purple	76	13.99	31-Mar-2013

Key	Name	Description	Stock	Price	LastOrdered
ARC1	Arc welder	250 Amps	8	119.00	25-Nov-2013
BRK8	Bracket	250mm	46	5.66	18-Nov-2013
BRK9	Bracket	400mm	82	6.98	1-Jul-2013

Key	Name	Description	Stock	Price	LastOrdered
HOS8	Hose	1/2"	27	27.50	18-Aug-2013
WGT4	Widget	Green	16	13.99	3-Feb-2013
WGT6	Widget	Purple	76	13.99	31-Mar-2013

BASE

- Basically Available – the system guarantees some level of availability to the data even in regards to node failures. The data may be stale, but will still give and accept responses.

- Soft State – the data is in a constant state of flux; so, while a response may be given, the freshness or consistency of the data is not guaranteed to be the most current.

- Eventual Consistency – the data will eventually be consistent through all nodes and in all databases, but not every transaction at every moment. It will reach some guaranteed state eventually.

ACID

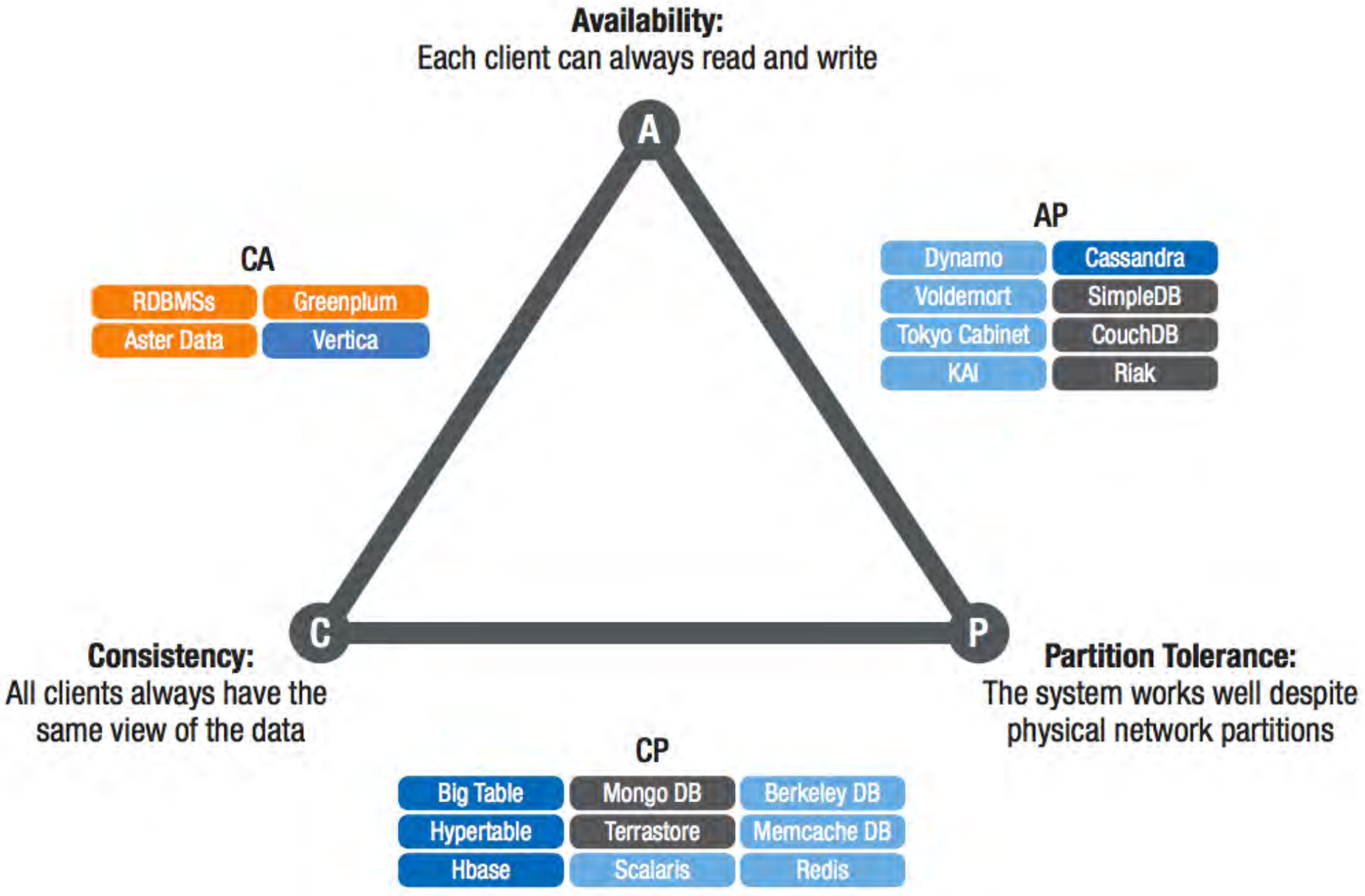
- Strong Consistency
- Isolation
- Focus on "commit"
- Nested transactions
- Availability?
- Conservative (pessimistic)
- Difficult evolution (e.g. schema)

BASE

- Weak Consistency – stale data OK
- Availability first
- Best effort
- Approximate answers OK
- Aggressive (optimistic)
- Simpler!
- Faster
- Easier evolution

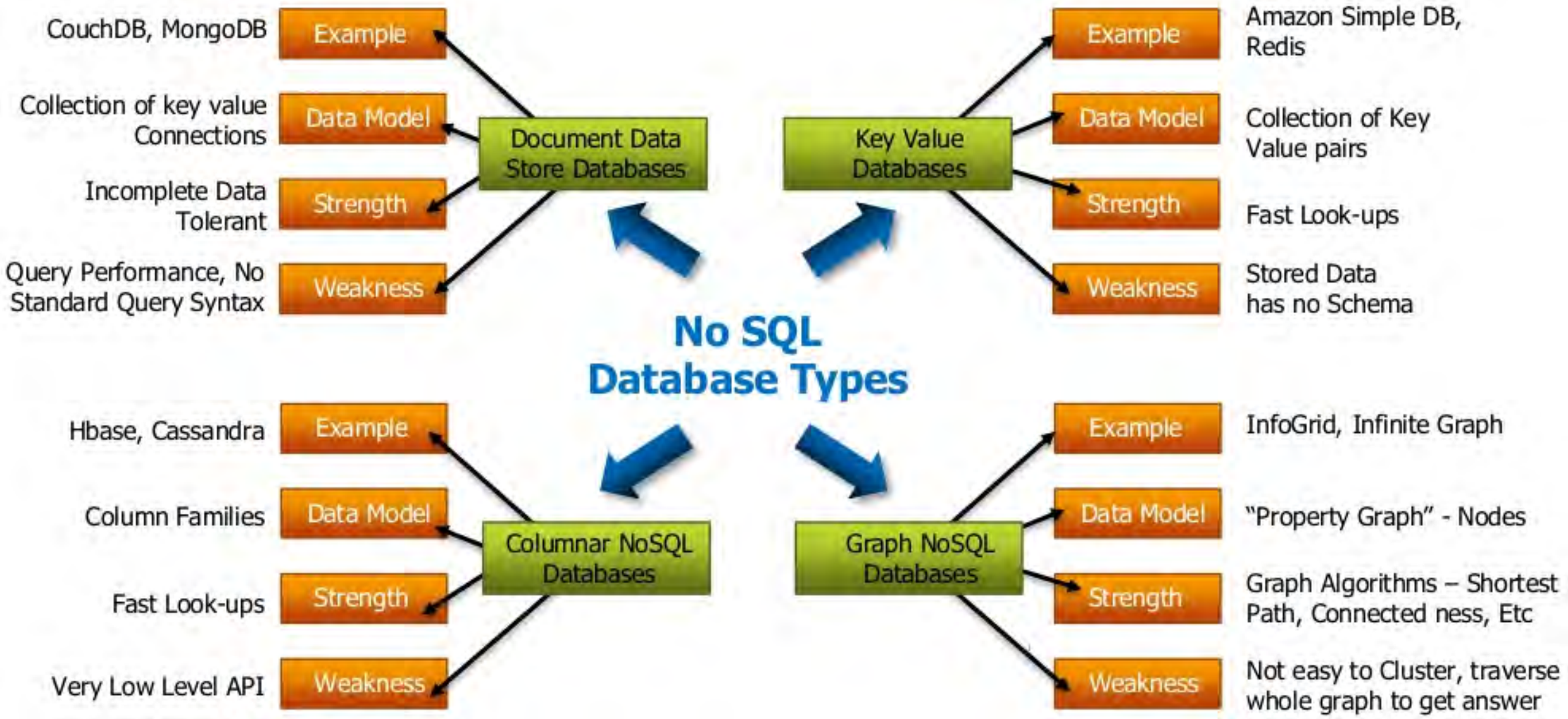
AVAILABILITY LEVEL[11]	ESTIMATED DOWNTIME PER YEAR
99.999%	5 minutes
99.99%	52 minutes
99.9%	8.5 hours
99%	3.5 days or about 87 hours

CAP Theorem



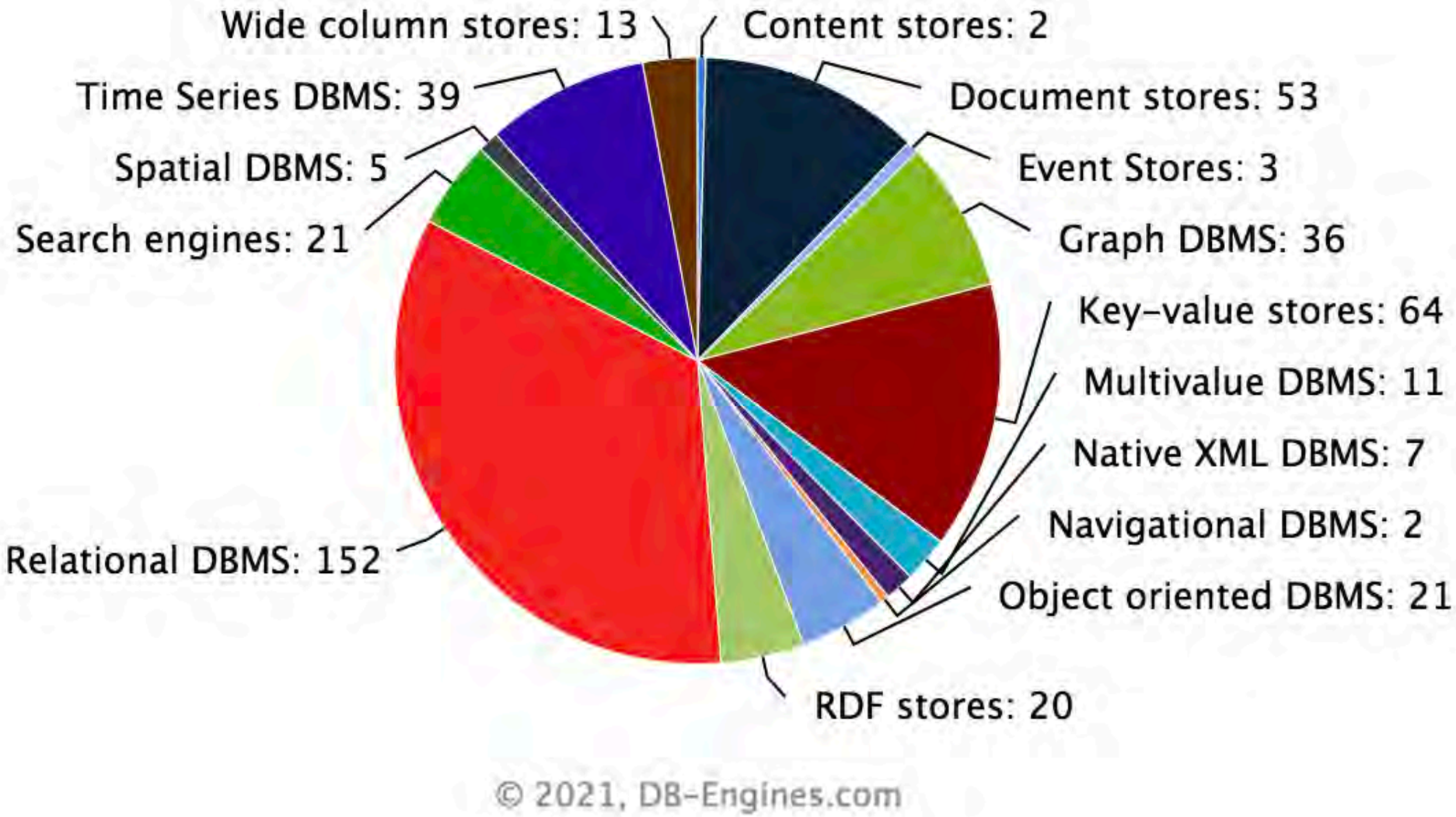
BASE (Basically Available, Soft-State, Eventual Consistency) data store

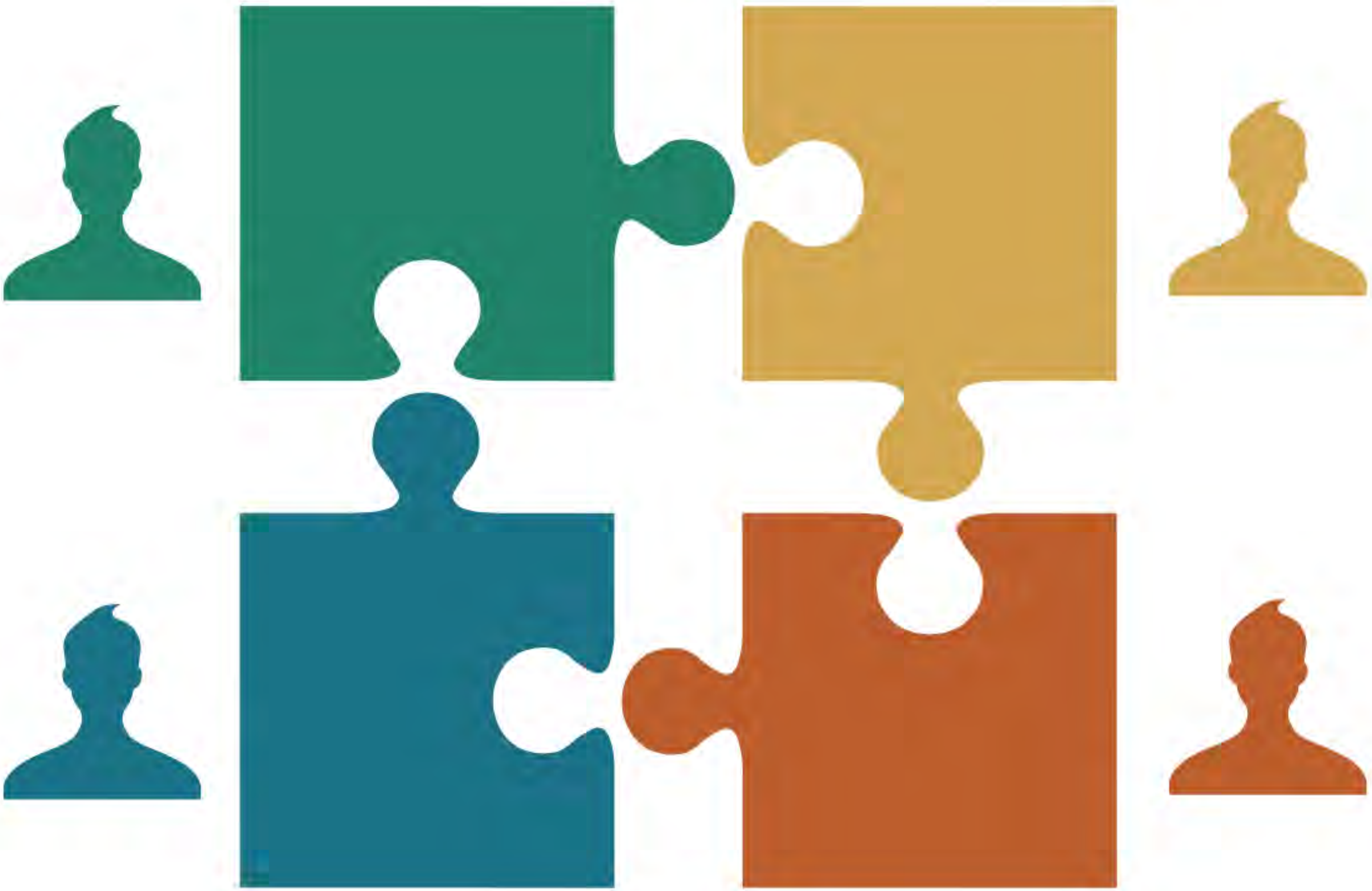
SELECTION	CHARACTERISTICS	EXAMPLES
C + A (No P)	2-phase commits Cache validation protocols	Single-site databases Cluster databases LDAP xFS file system
C + P (no A)	Pessimistic locking Make minority partitions unavailable	Distributed databases Distributed locking Majority protocols
A + P (no C)	Expirations/leases Conflict resolution Optimistic	Coda Web caching DNS



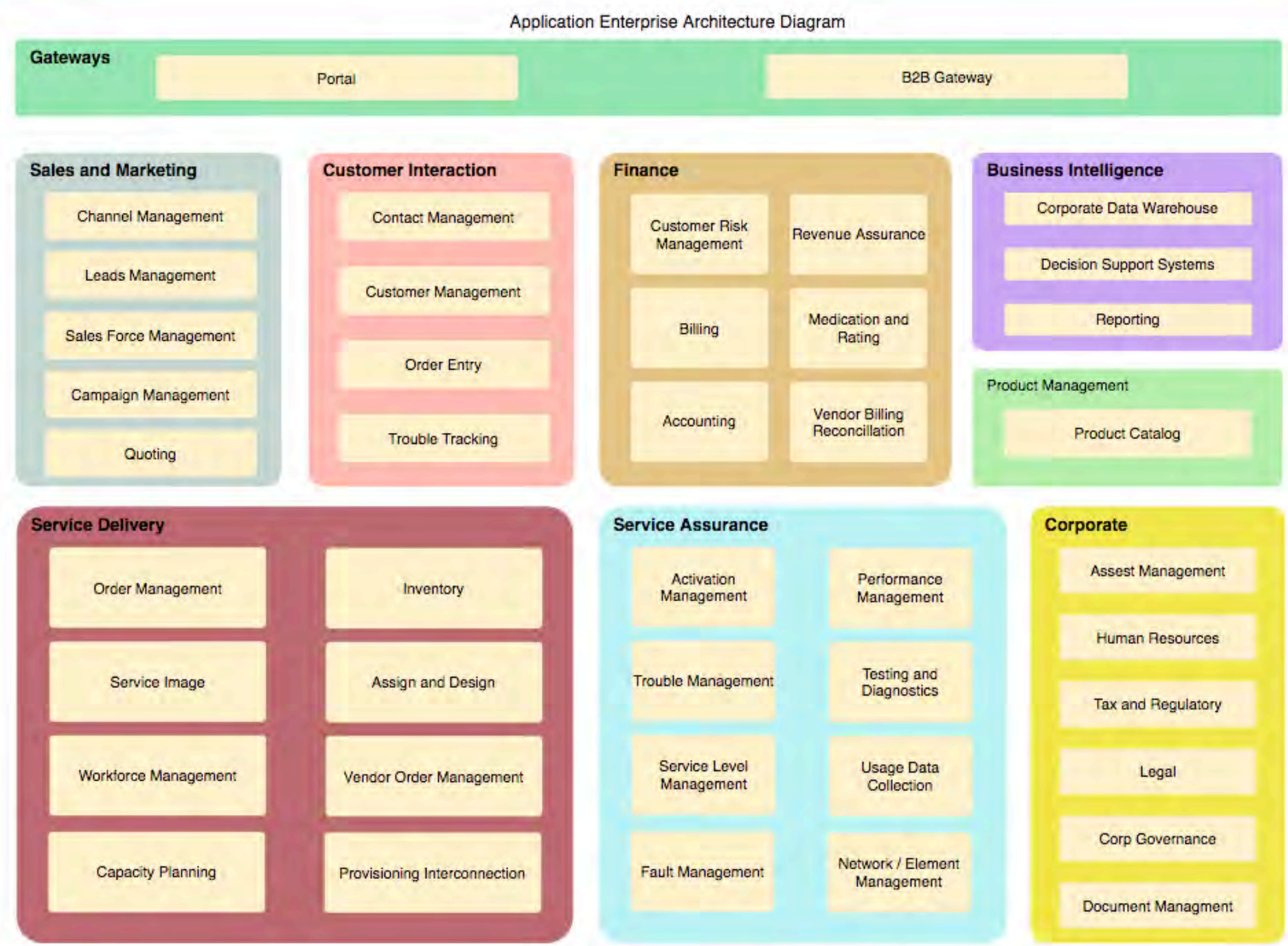
http://www.nosql-database.org

Number of systems per category, December 2021





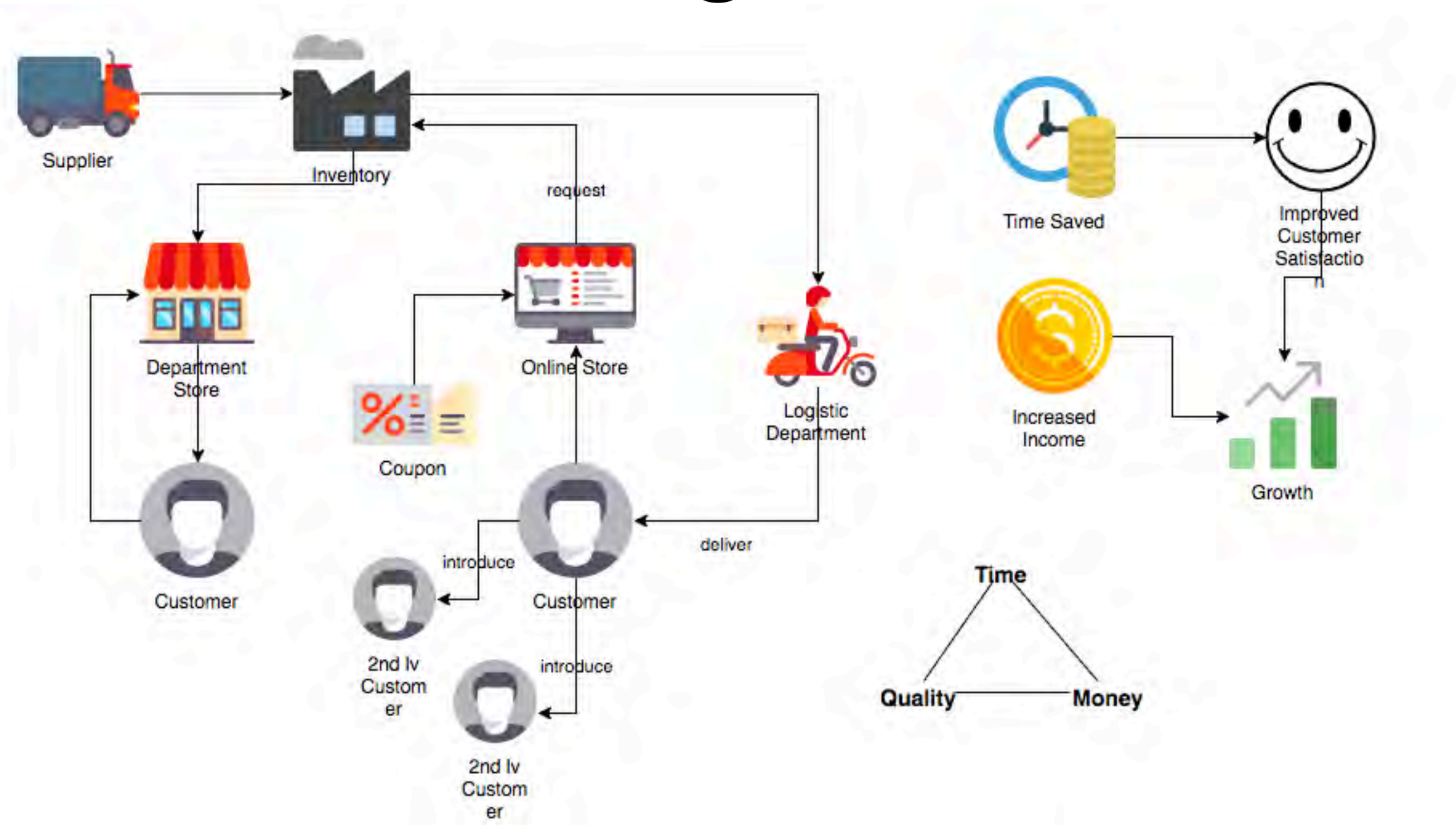
How to send requests to multiple systems?



abstraction

abstraction

Distributed Data Management



Modern application requirements

Requires more performance, scale, and availability

E-commerce

Media streaming

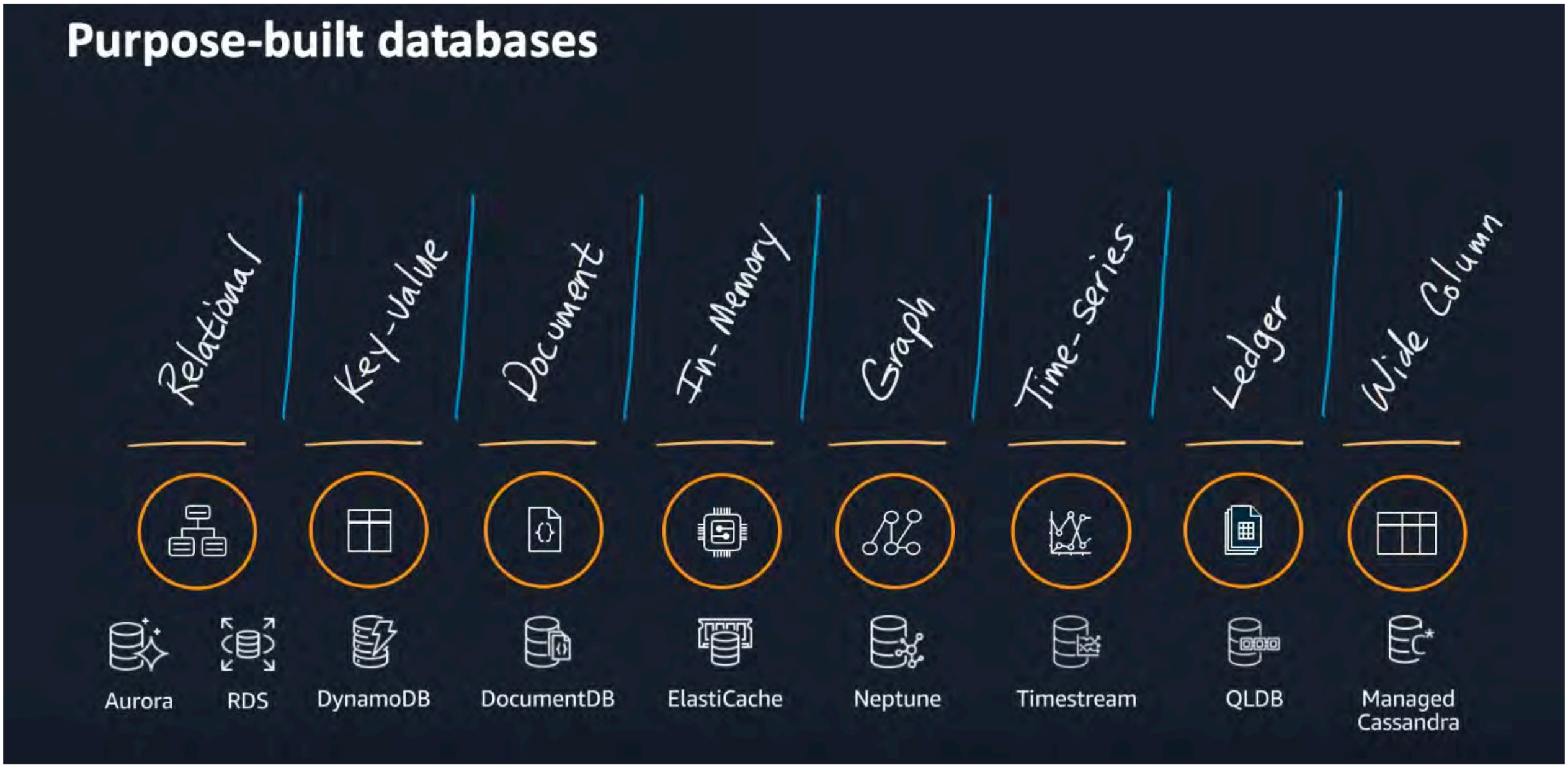
Social media

Online gaming

Shared economy

Users	1M+
Data volume	Terabytes–petabytes
Locality	Global
Performance	Microsecond latency
Request rate	Millions per second
Access	Mobile, IoT, devices
Scale	Up, down, out, or in
Economics	Pay-as-you-go
Developer access	Open API

Purpose-built databases



queries



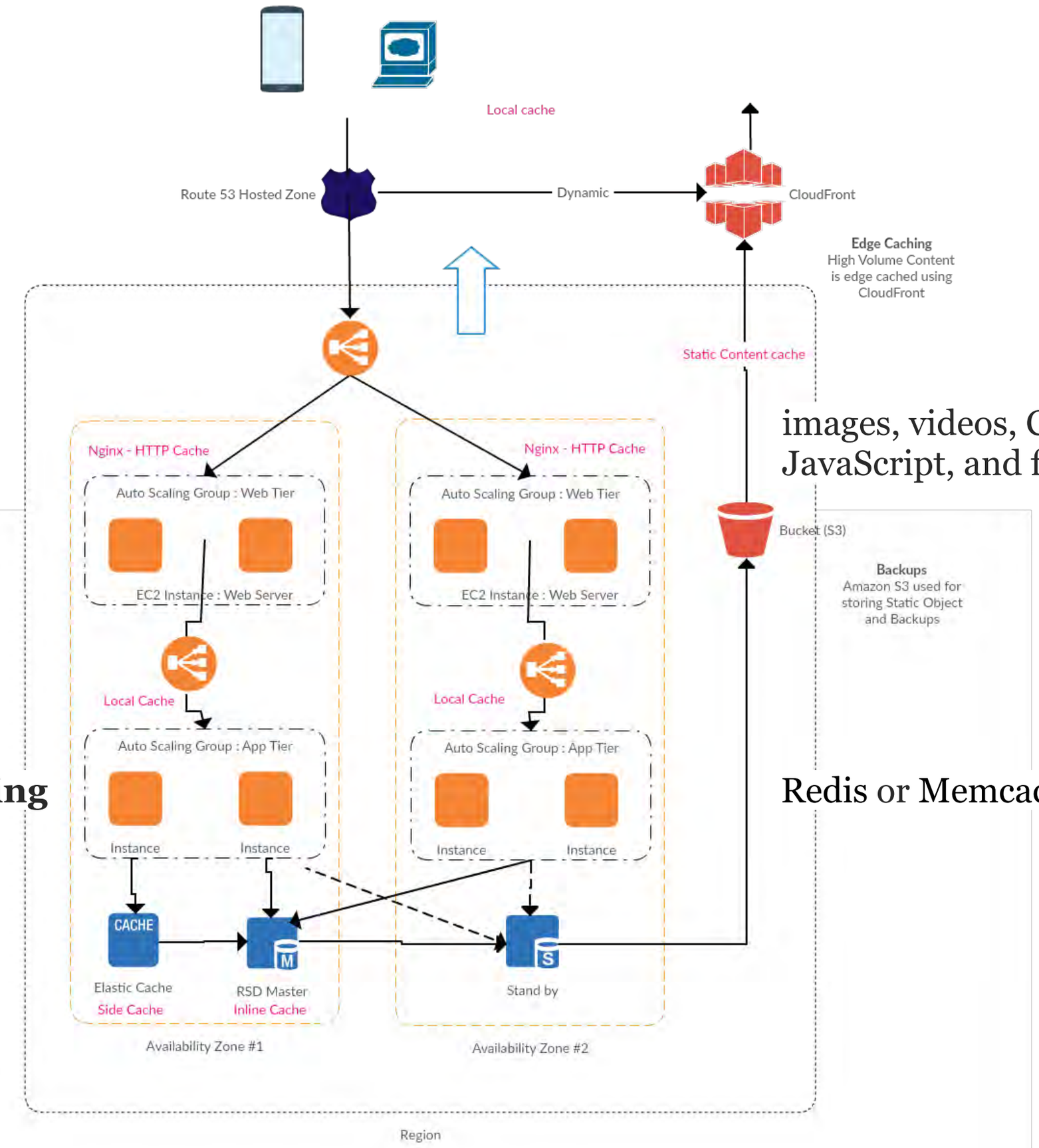

How to Increase performance?

page caching

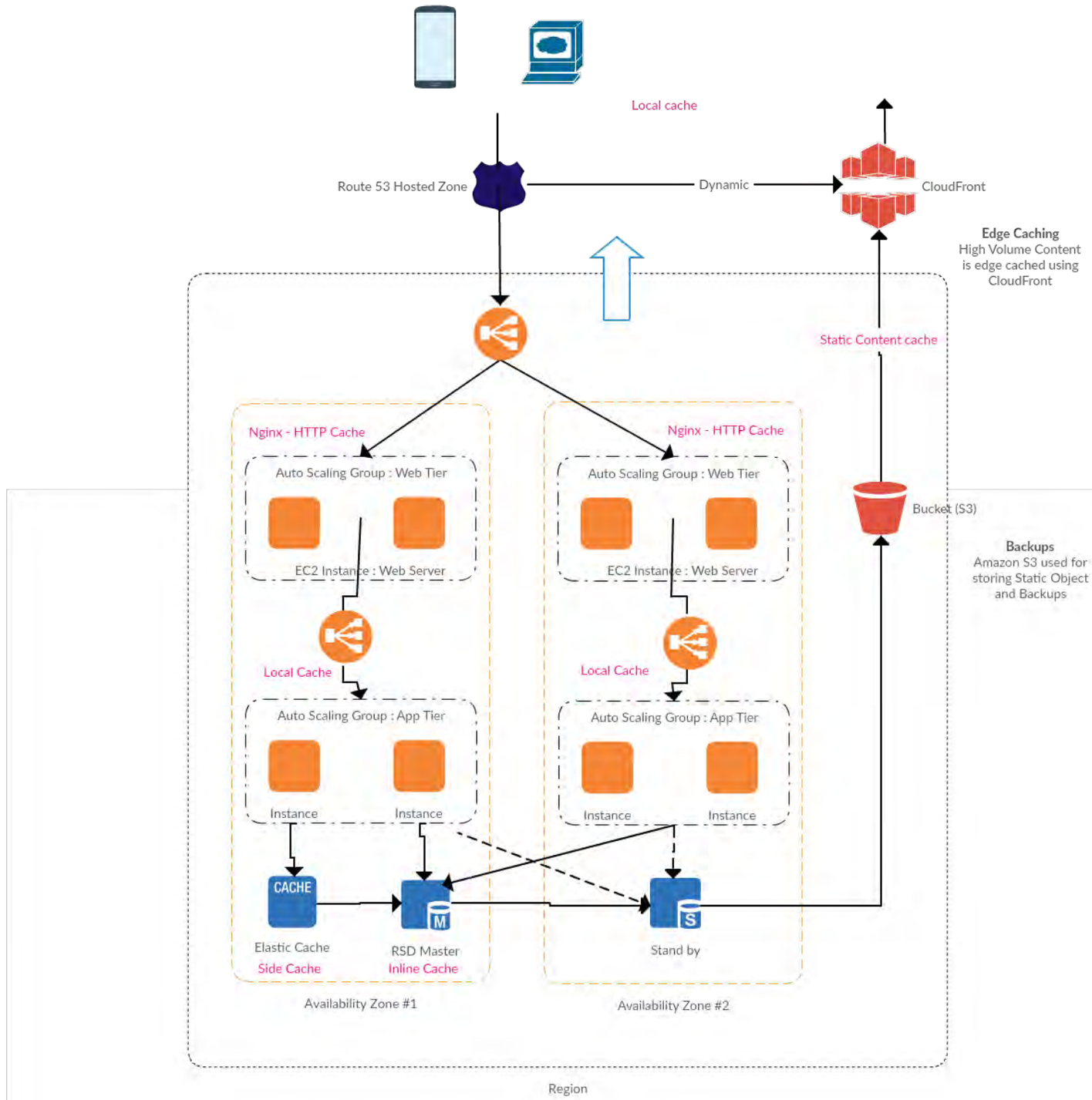
images, videos, CSS, JavaScript, and fonts

in-memory caching

Redis or Memcached

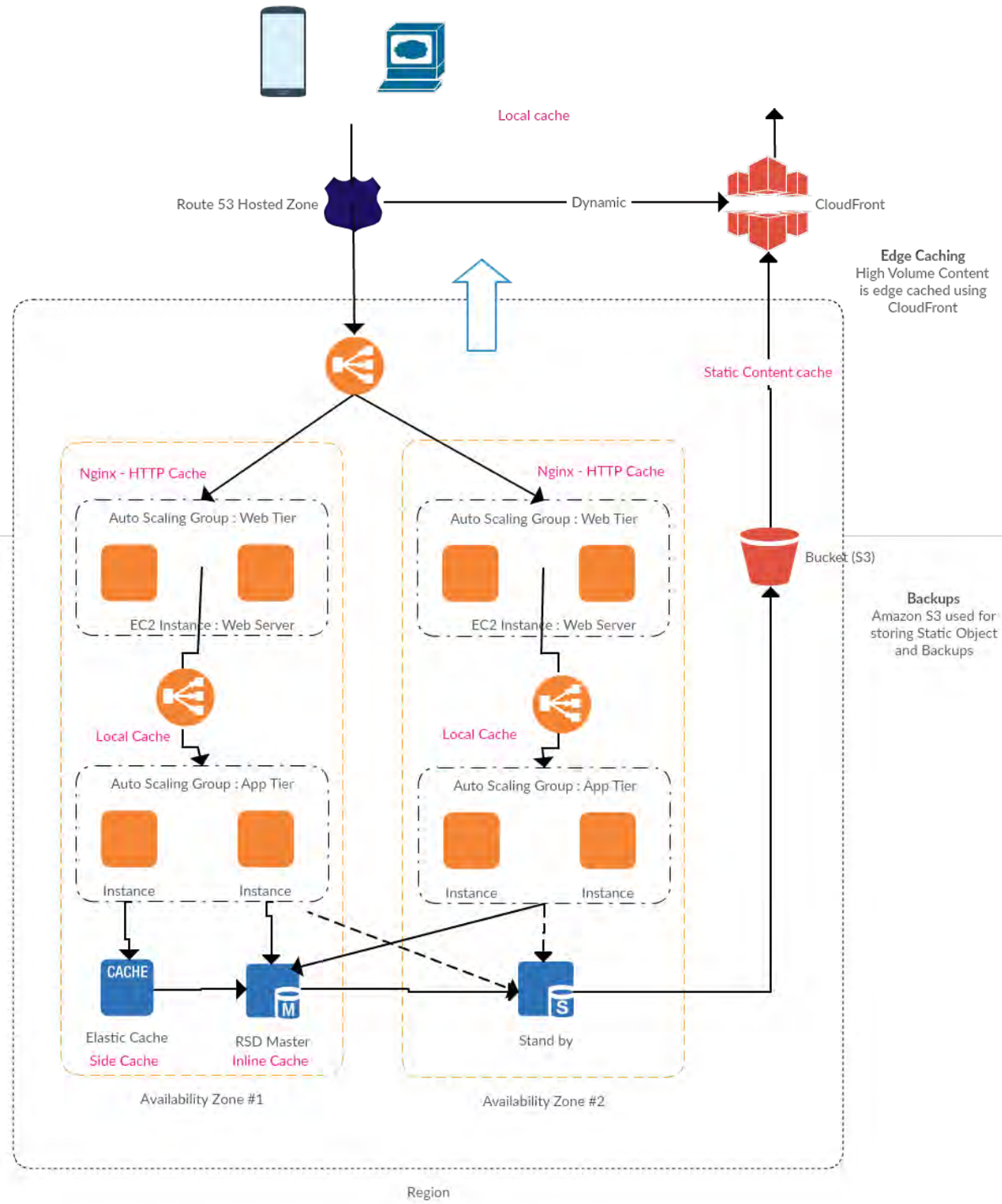


How long we should cache the data?

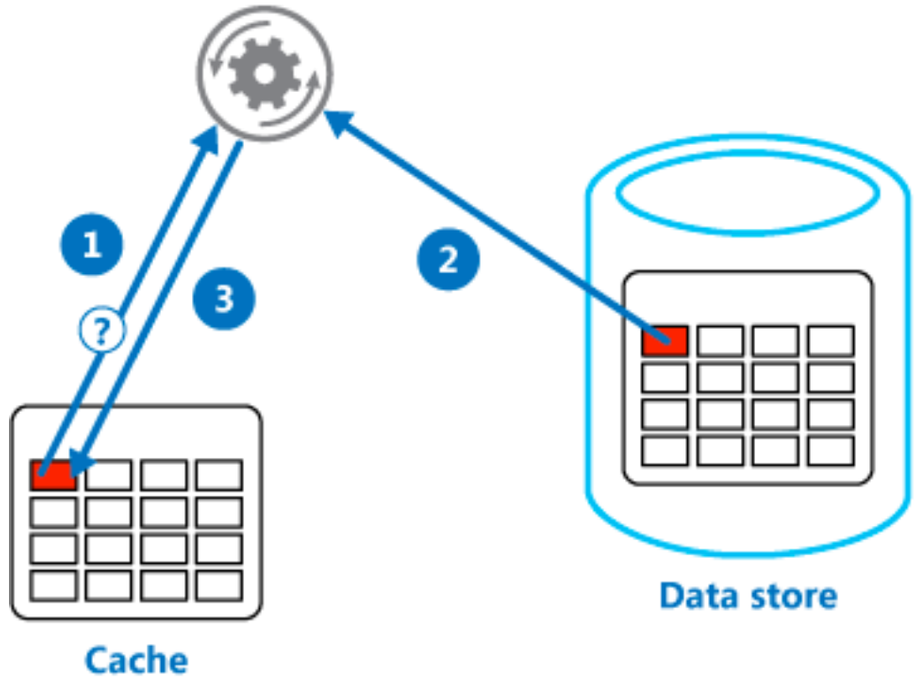


How long we should cache the data?

- Expiration period
- Cost of retrieval
- Most Recently Used
- Consistency



When to use Side Cache Cache-Aside?



1: Determine whether the item is currently held in the cache.
2: If the item is not currently in the cache, read the item from the data store.
3: Store a copy of the item in the cache.

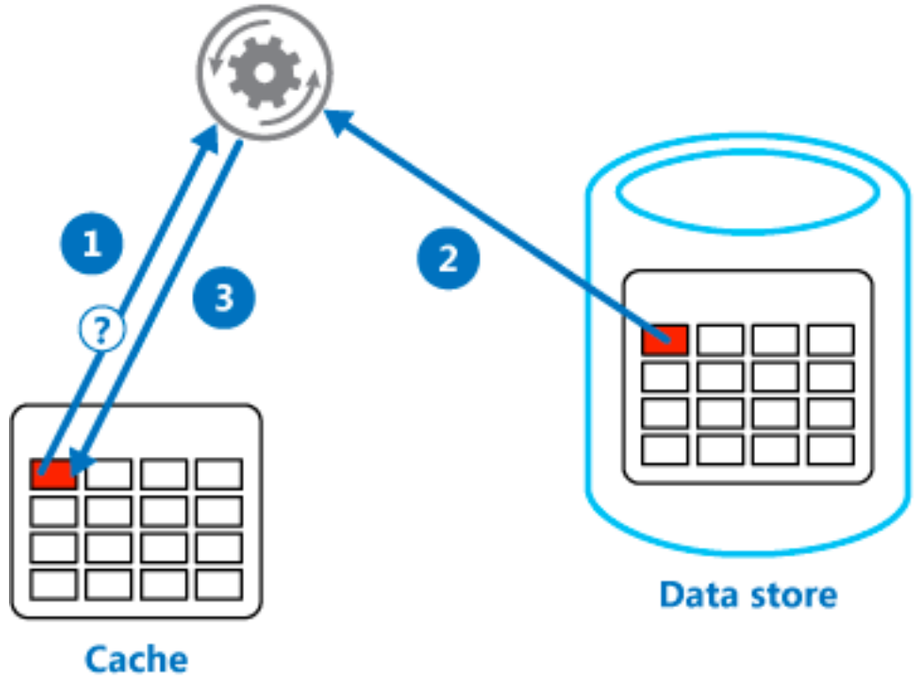
When to use Side Cache Cache-Aside?

When to Use?

- No Read through and Write through actions
- Demand is unpredictable

When to Not to Use?

- Data set is static:
    - Startup
- Data size considerations



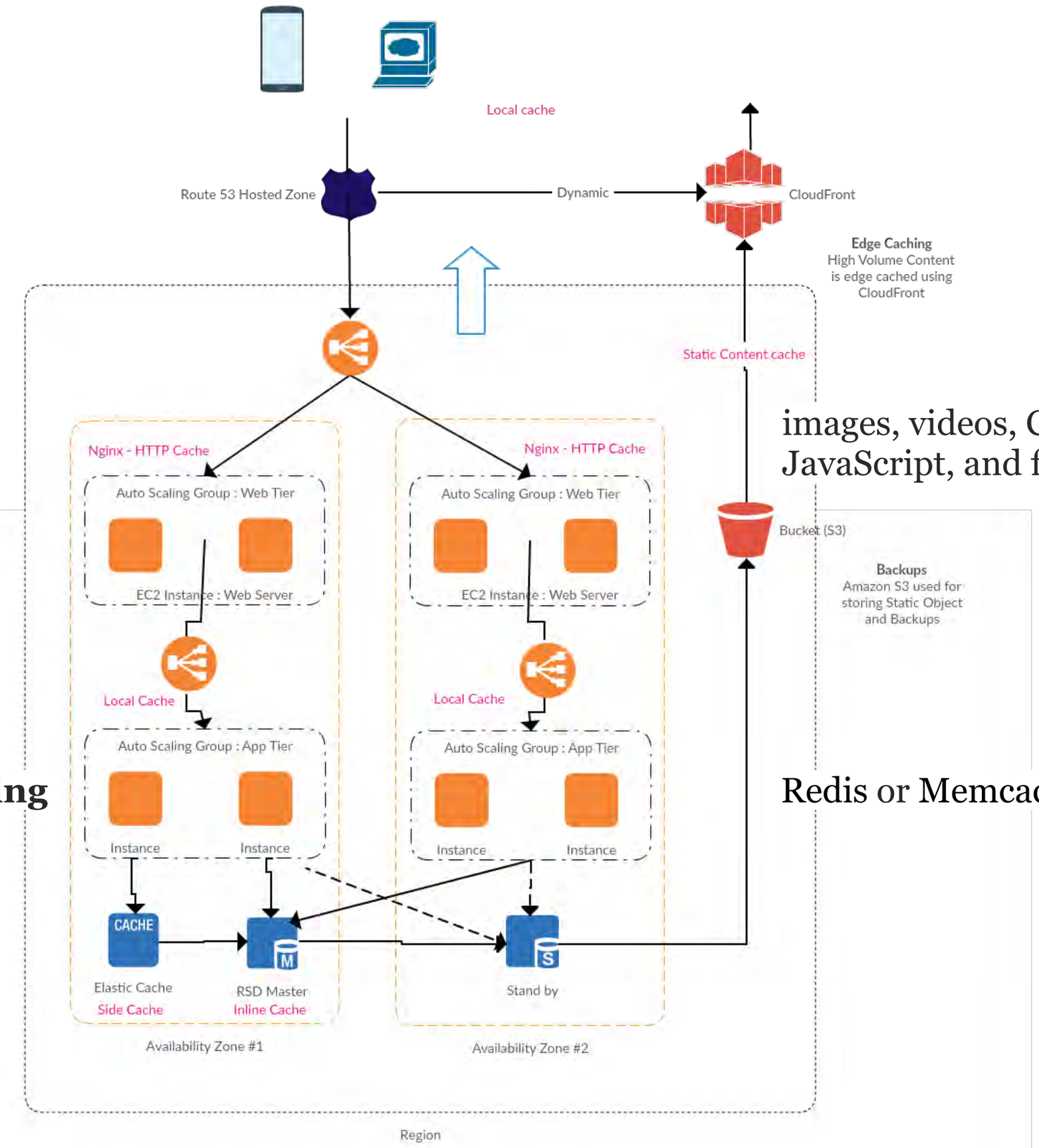
1: Determine whether the item is currently held in the cache.
2: If the item is not currently in the cache, read the item from the data store.
3: Store a copy of the item in the cache.

page caching

images, videos, CSS, JavaScript, and fonts

in-memory caching

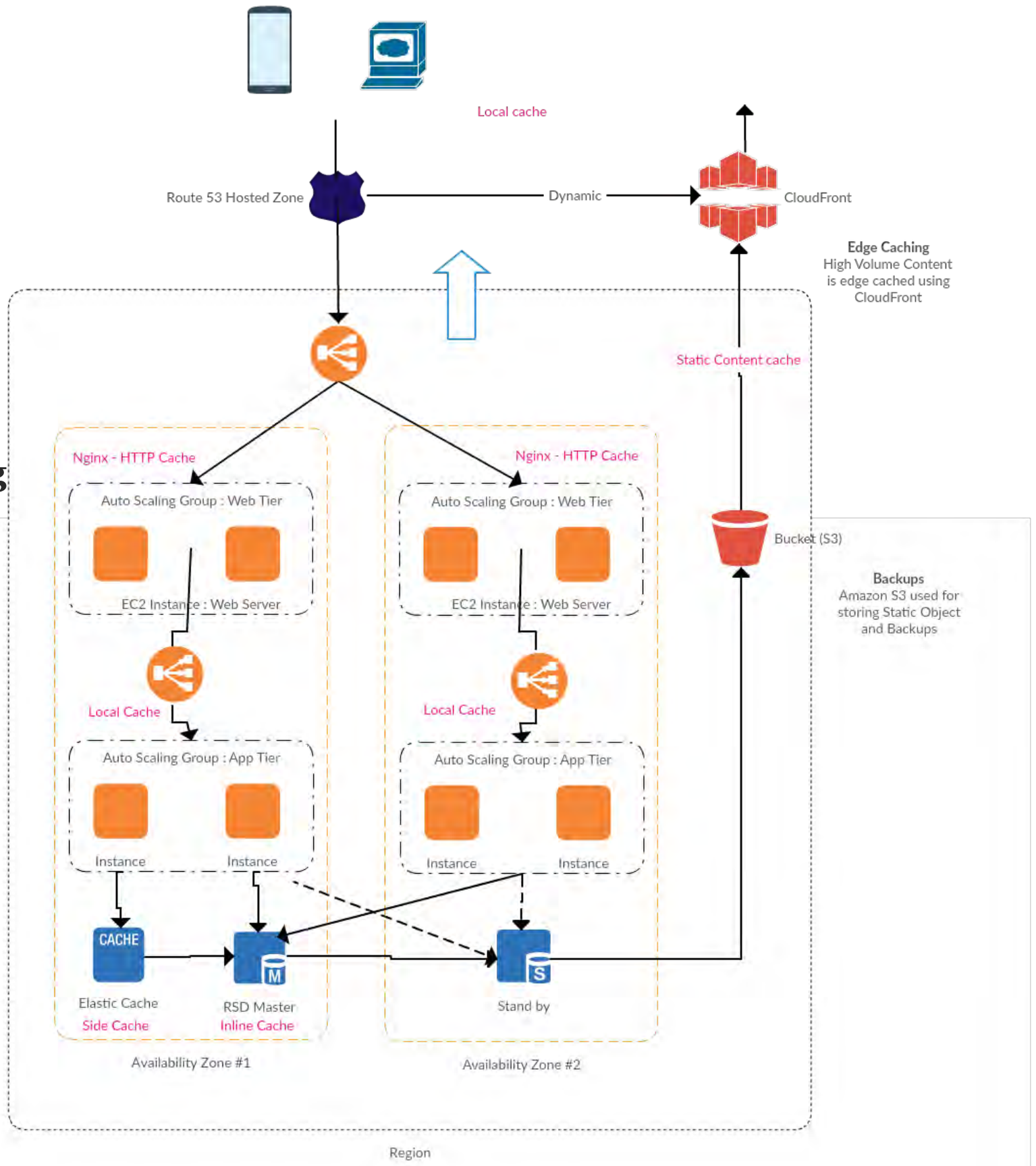
Redis or Memcached



100000 requests

Cache miss

request coalescing
“waiting rooms”

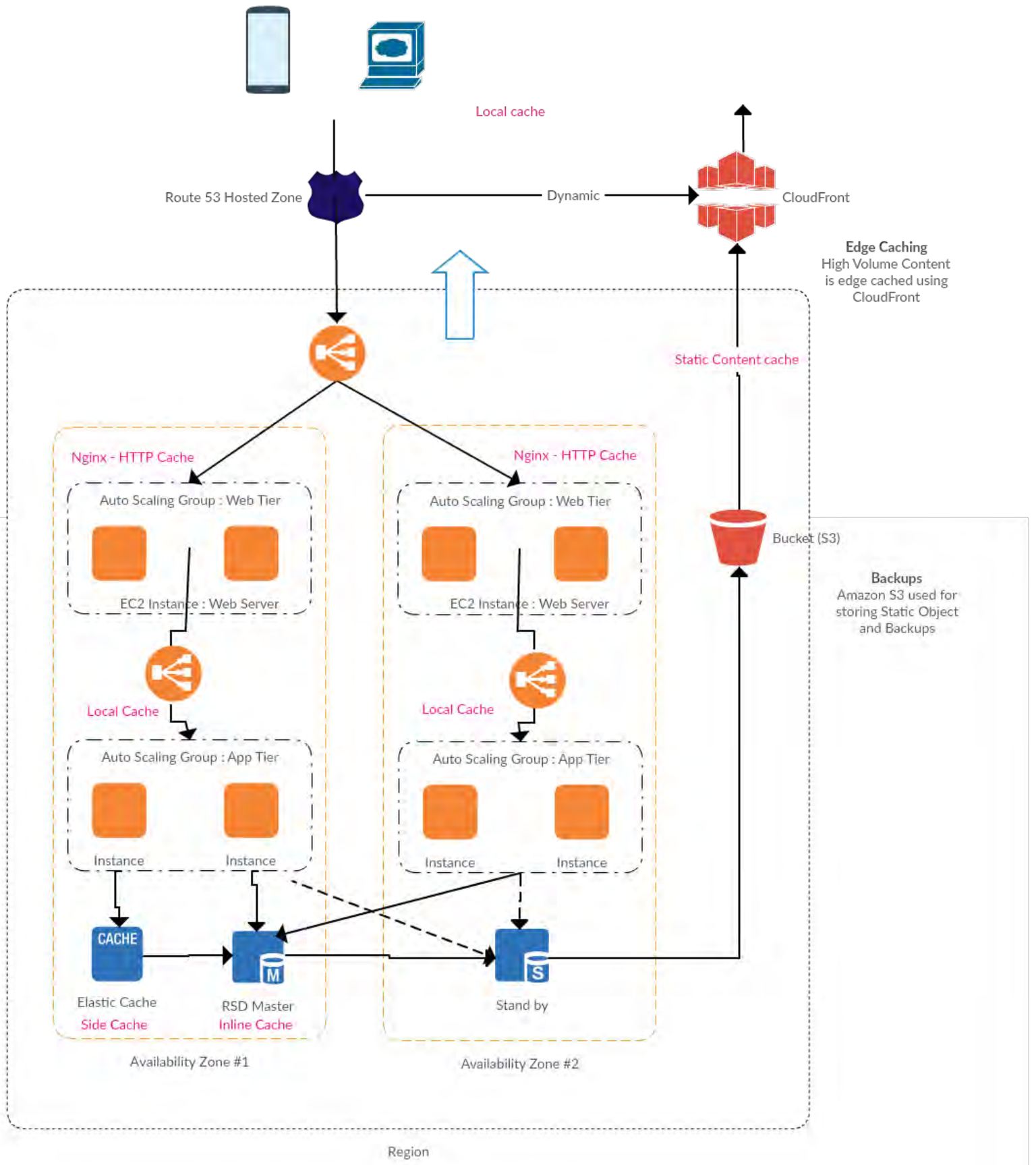


page caching

in-memory caching

Cache-aside
See Cache then DB

Inline-cache



Key-Value Store

Redis Cache

Use Cases for In-Memory Datastores

Caching

Real-time analytics

Gaming leaderboards

Geospatial

Media streaming

Session store

Chat apps

Message queues

Machine learning

Need for Speed

FAST: Memory is at least 50x faster than SSDs

PREDICTABLE: Key-based index, no disk seek time

µs is the new ***ms***

Amazon
ElastiCache

Need for Speed

FAST: Memory is at least 50x faster than SSDs

PREDICTABLE: Key-based index, no disk seek time

Slow site?

Need for Speed

“A 100-millisecond delay in website load time can hurt conversion rates by 7 percent"

"A two-second delay in web page load time increases bounce rate by 103 percent"

– 2017 Akamai Study

Comparison

Feature	In-memory	Disk-based
Writes/Reads	Memory	Disk
Durability	Periodic or none	Continuous
Engine Response	Microseconds (µs)	Milliseconds (ms)
Throughput	High	Moderate
Performance Bottleneck	Network	Disk
Data	Flexible data structures	Forced models

Amazon ElastiCache for Memcached

ElastiCache
for Memcached

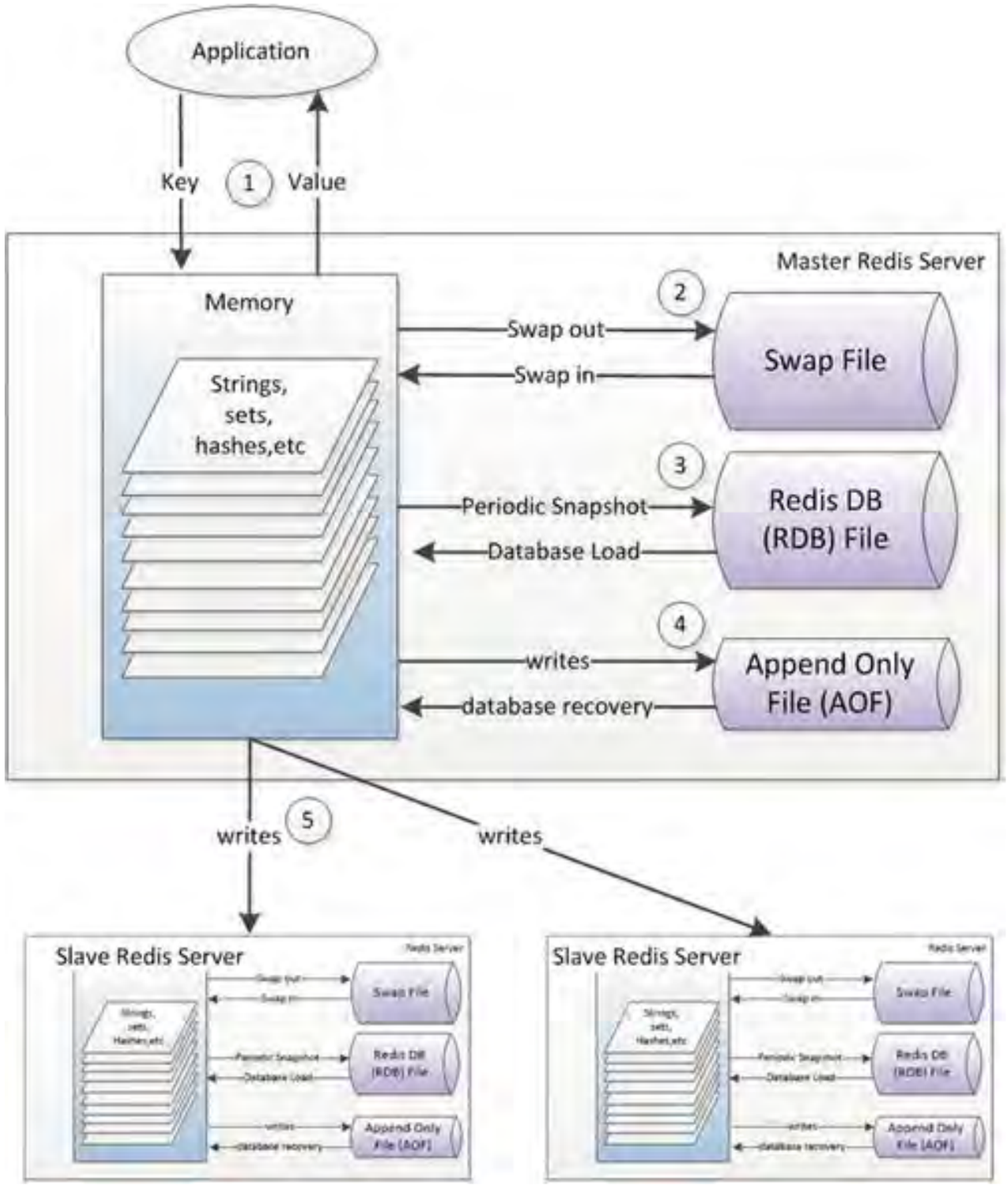
- OSS Memcached initially released in 2003
- Simple, in-memory, LRU cache
- Simple key-value (string-string) store
- Supports strings, objects
- Multi-threaded
- Sharding via client-side library
- Easy to Scale
- No persistence or replication

Amazon ElastiCache for Redis

ElastiCache
for Redis

- OSS Redis initially released in 2009
- In-memory data structure server:
  Strings, Lists, Sets, Sorted Sets, Hash Tables,
  HyperLogLog, Geospatial, and Streams
- ~200 commands plus LUA scripting
- Multi-key atomic operations
- High-availability through replication
- Scalability through online sharding
- Persistence via snapshot / restore

Redis (Remote Dictionary Server)



Amazon ElastiCache

When	Amazon ElastiCache Engine
Building real-time apps across versatile use cases like gaming, geospatial service, caching, session stores, or queuing, with advanced data structures, replication, and point-in-time snapshot support. Persistence, Atomic operations, Pub/sub, Read replica/failover, Cluster mode/sharded clusters	Amazon ElastiCache for Redis
Building a simple, scalable caching layer for your data-intensive apps. Multi threading, Low maintenance.	Amazon ElastiCache for Memcached

Do you see issue with duplicate values?

New Customer Onboarding

SALES & MARKETING

Enter Customer Data

Check

- Customer Code
- Name
- Contact Information
- Credit Terms
- Account Manager Details

FINANCE & ACCOUNTING

Update Customer Data

Check

- Payment Terms
- Reconciliation Accounts
- Bank Information
- Freight Cost Terms

LOGISTICS & SHIPPING

Update Customer Data

Check

- Shipping Information
- Source and Destination Locations
- Freight Terms
- Routes

https://wisdomschema.com/how-mdm-works-collecting-data/

DON'T WORRY, IT'S ONLY MARKETERS COLLECTING OUR PERSONAL DATA SO THEY CAN CREATE MORE RELEVANT ADVERTISING FOR US.

TOM FISH BURNE

https://marketoonist.com/2019/05/data-privacy-consent-fatigue-and-gdpr.html

State	Abbreviation	Postal Code
Alabama	Ala.	AL
Alaska	Alaska	AK
American Samoa		AS
Arizona	Ariz.	AZ
Arkansas	Ark.	AR
California	Calif.	CA
Colorado	Colo.	CO
Connecticut	Conn.	CT
Delaware	Del.	

Reference Data

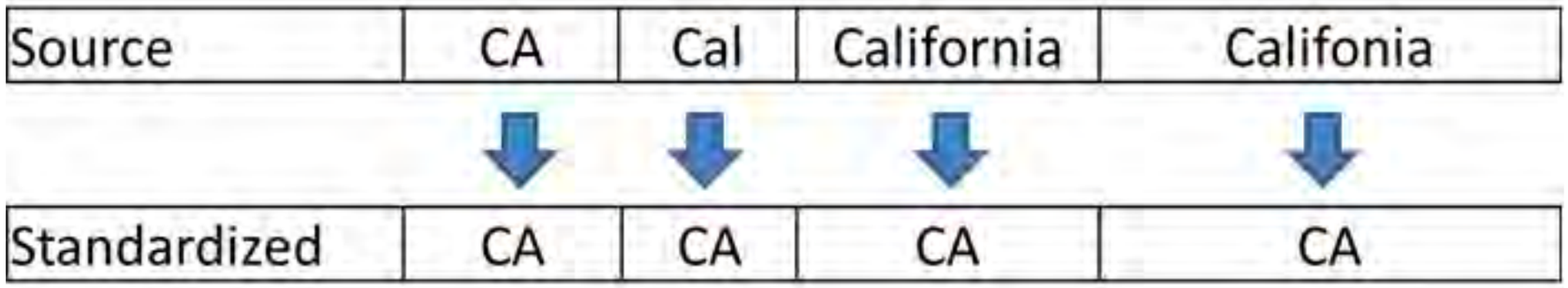
Application A	Application B	Application C
Jon Smith	John Smith	John Smith
965 Fremont St	965 Fremont St	965 Fremont Street

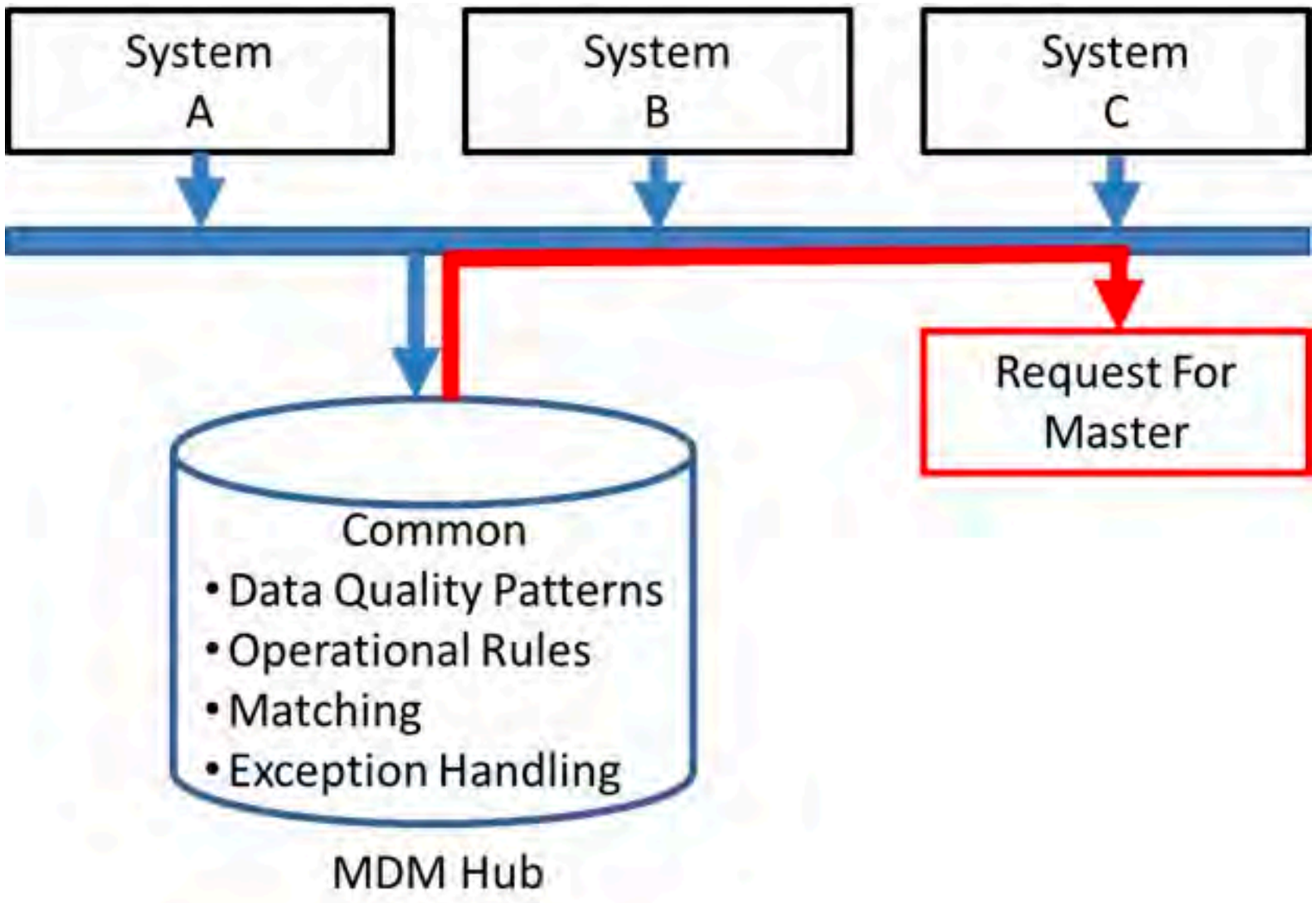
John Smith
965 Fremont St

Master Data

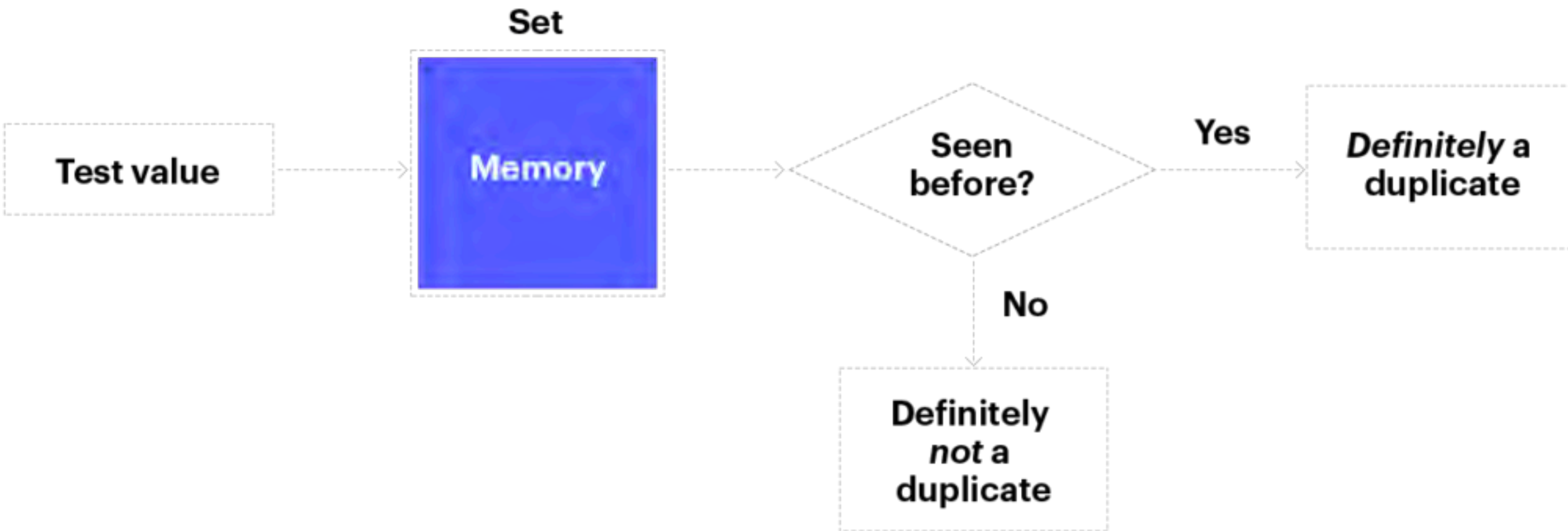
https://brianhooverblog.wordpress.com/2012/12/14/practical-master-data-management/

Data quality




System
A
System
B
System
C
Request For
Master
Common
• Data Quality Patterns
• Operational Rules
• Matching
• Exception Handling
MDM Hub

Compliance - Audit, legislative and regulatory

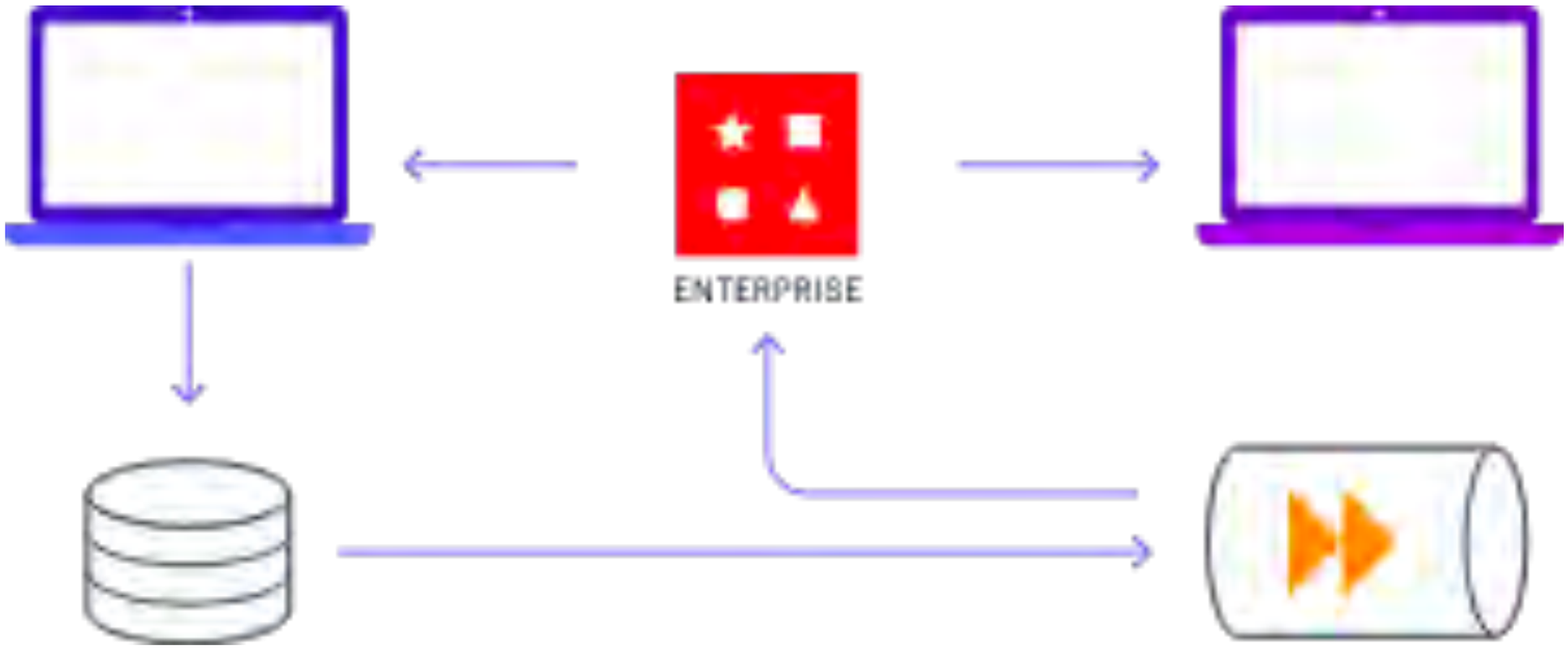


https://redis.com/solutions/use-cases/deduplication/

Can we solve this problem using FIFO Queue?

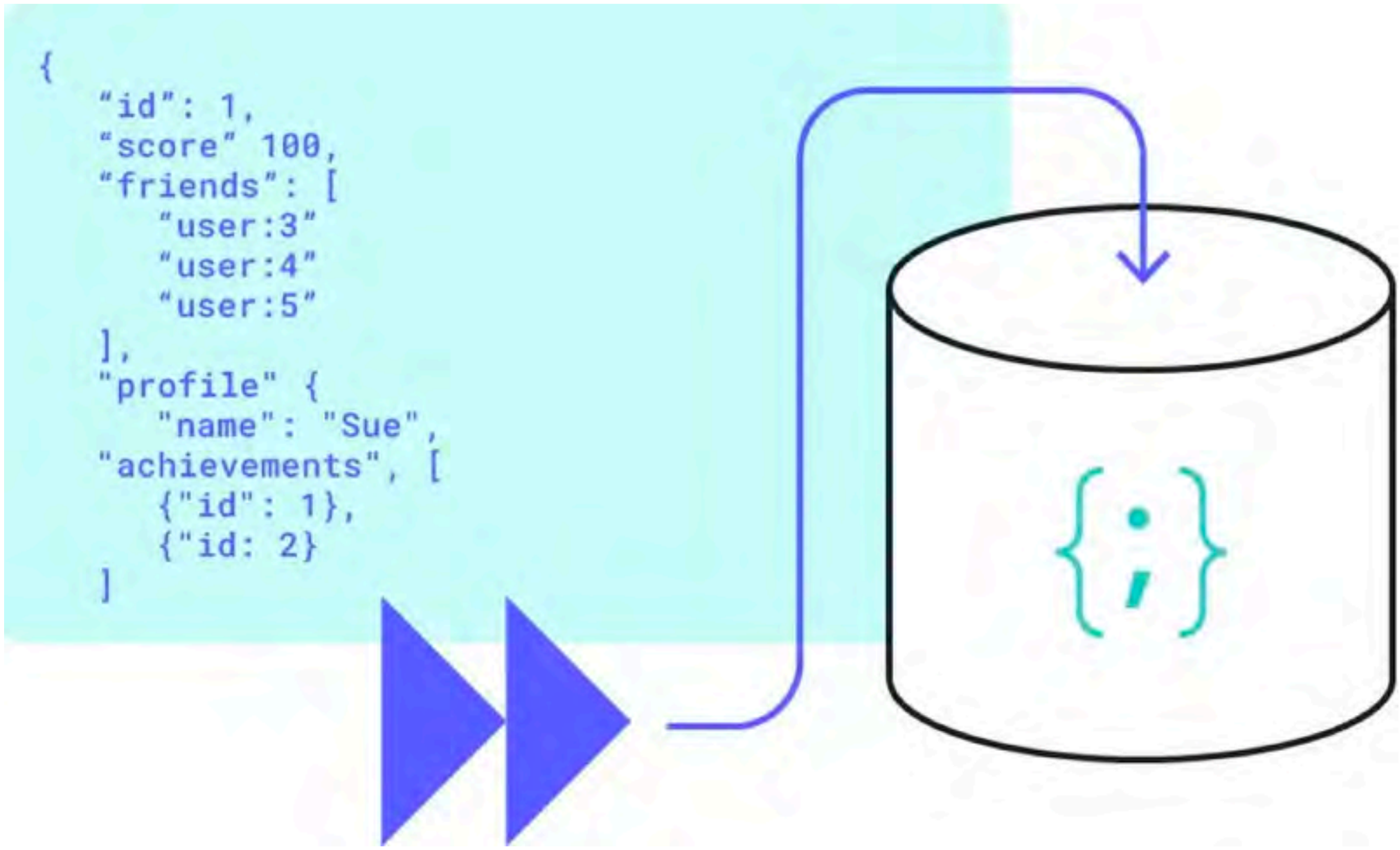
What type of operations are good?

Heavy Read operations



Change Data Capture

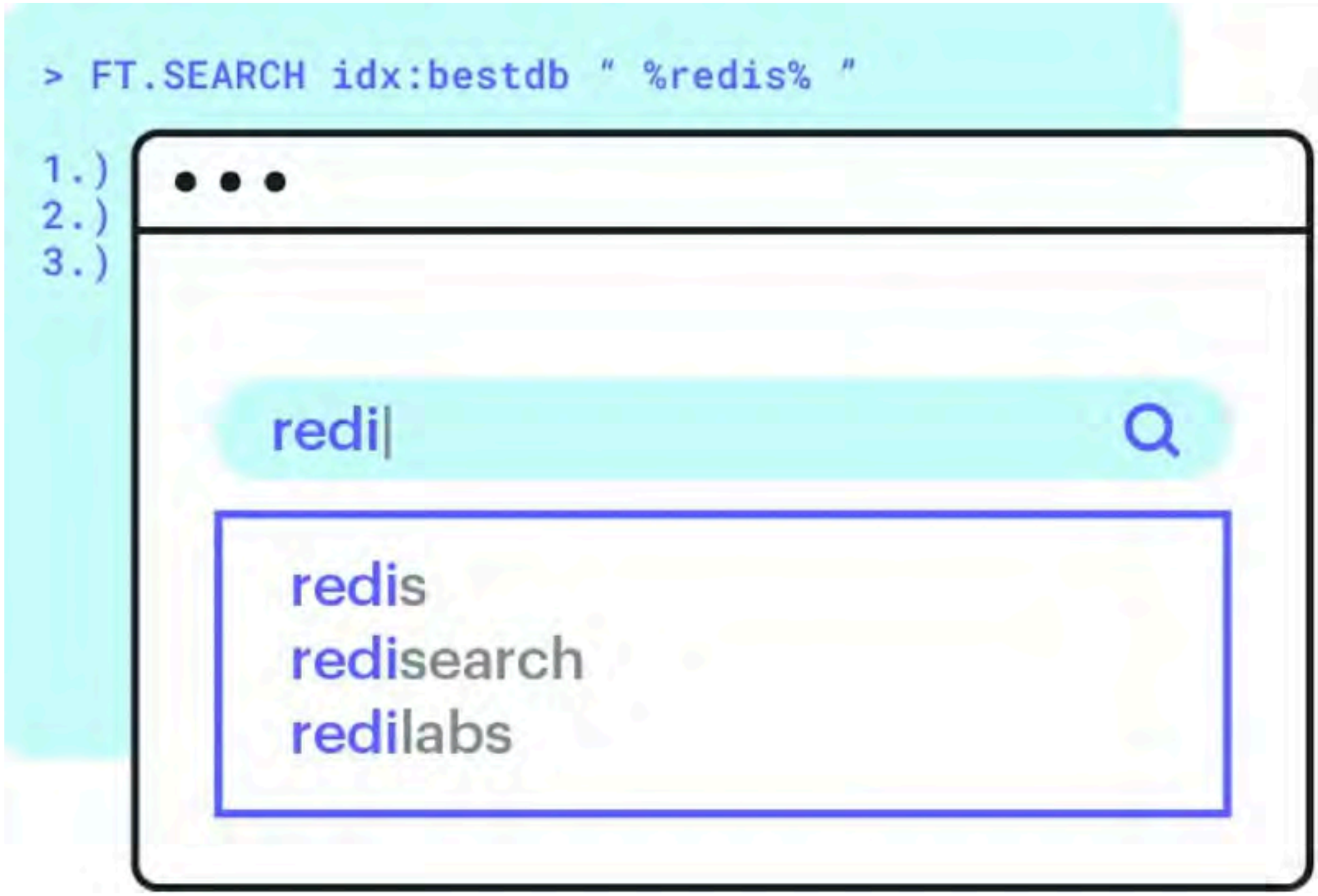
Redis JSON



https://redis.com/modules/redis-json/

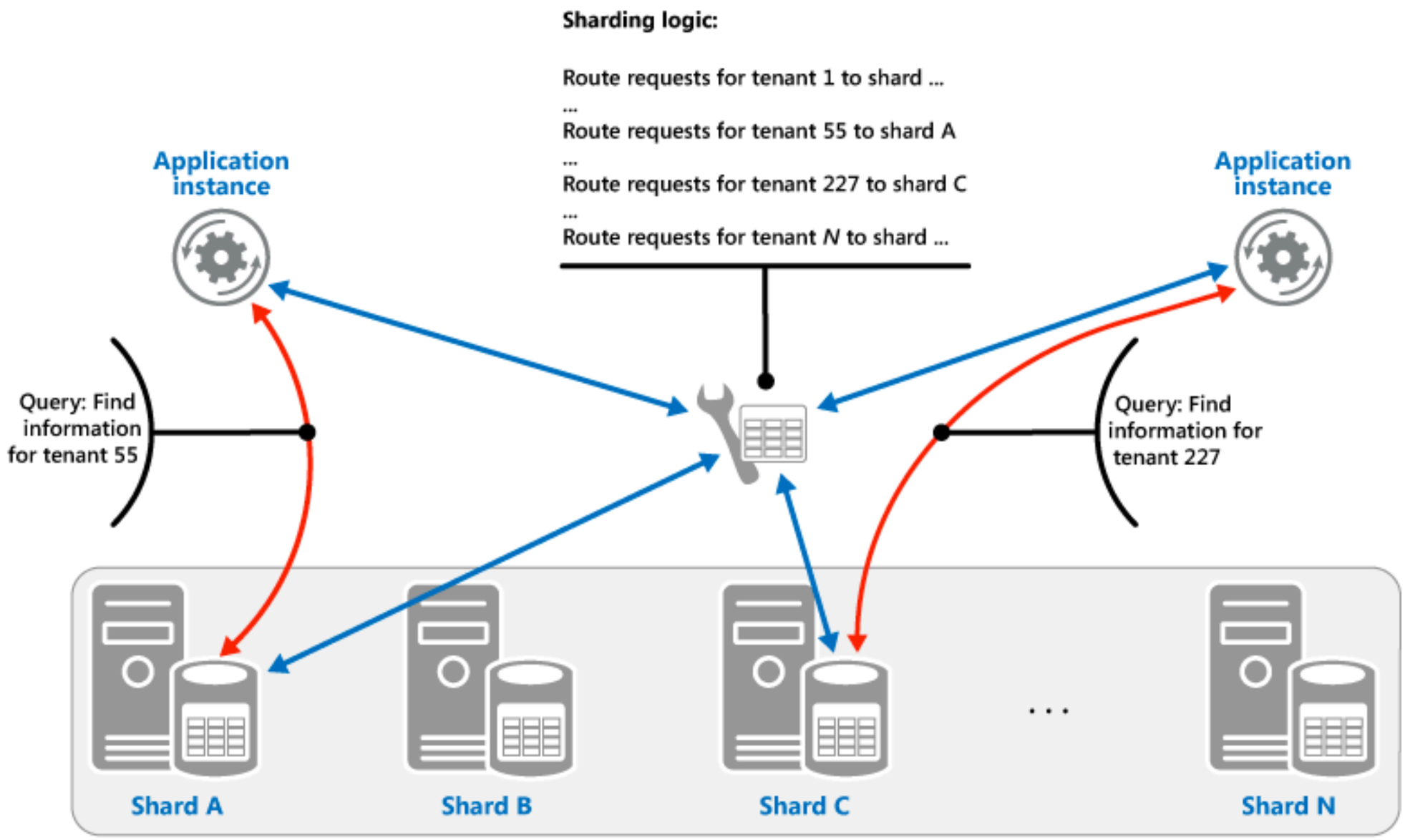
Indexing

Full-text and fuzzy search



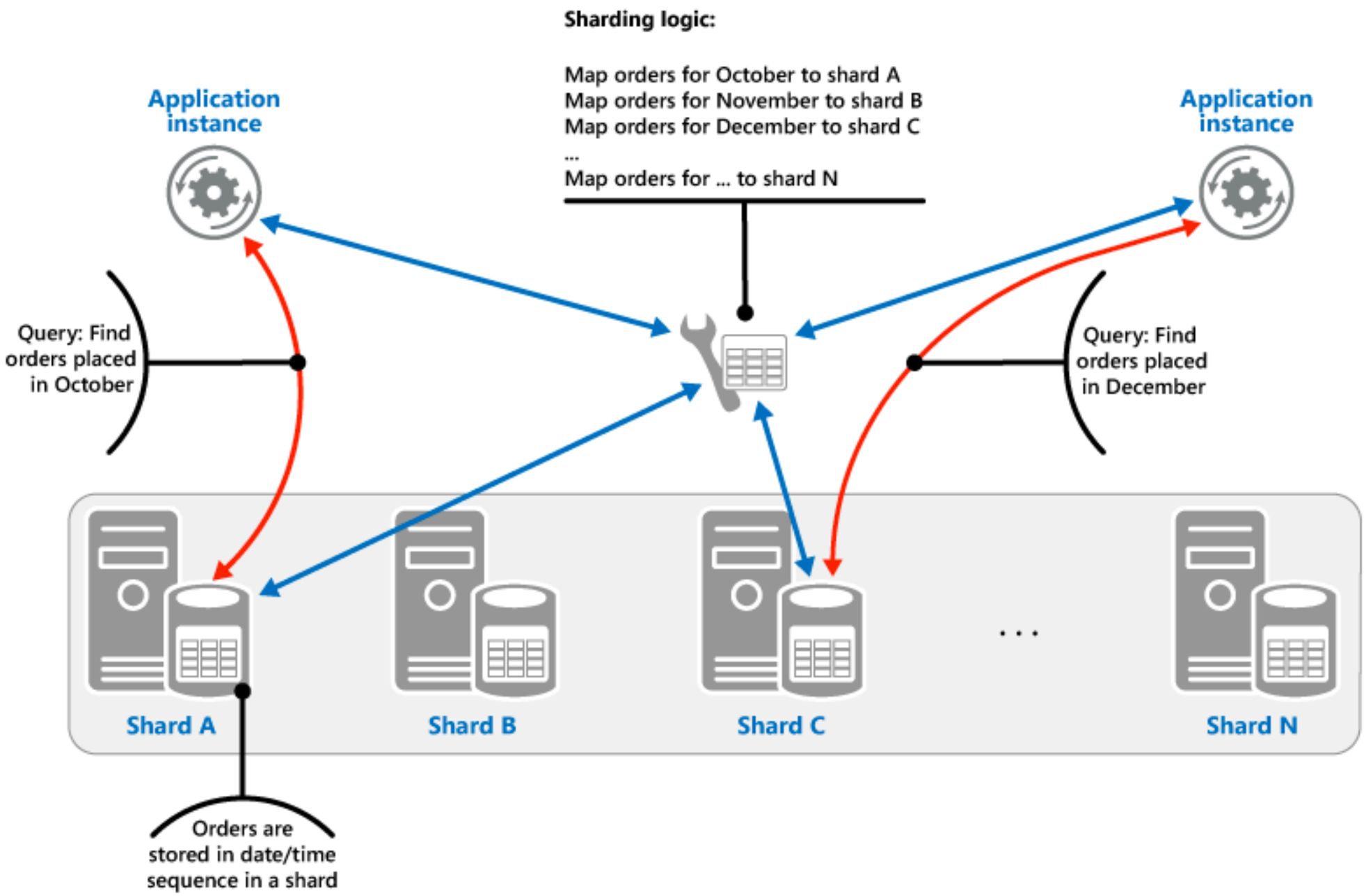
Sharding

Lookup Strategy



- Tenant ID, keep data together
- More controlled Virtual Shard
- State management
- Rebalance Shards

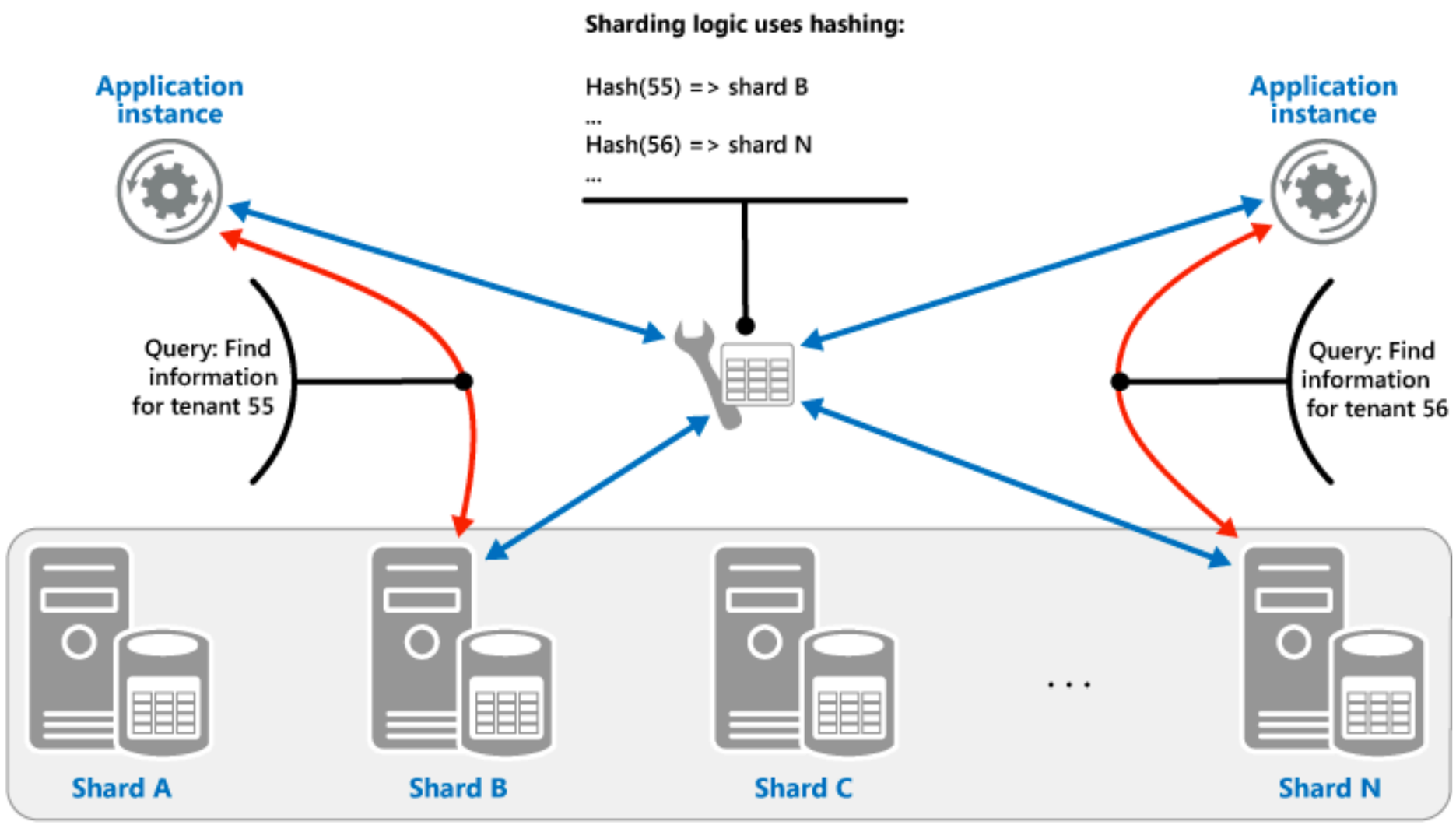
Range Strategy



- Given Month
- Given Qtr

- State management
- No balancing between shards

Hash strategy

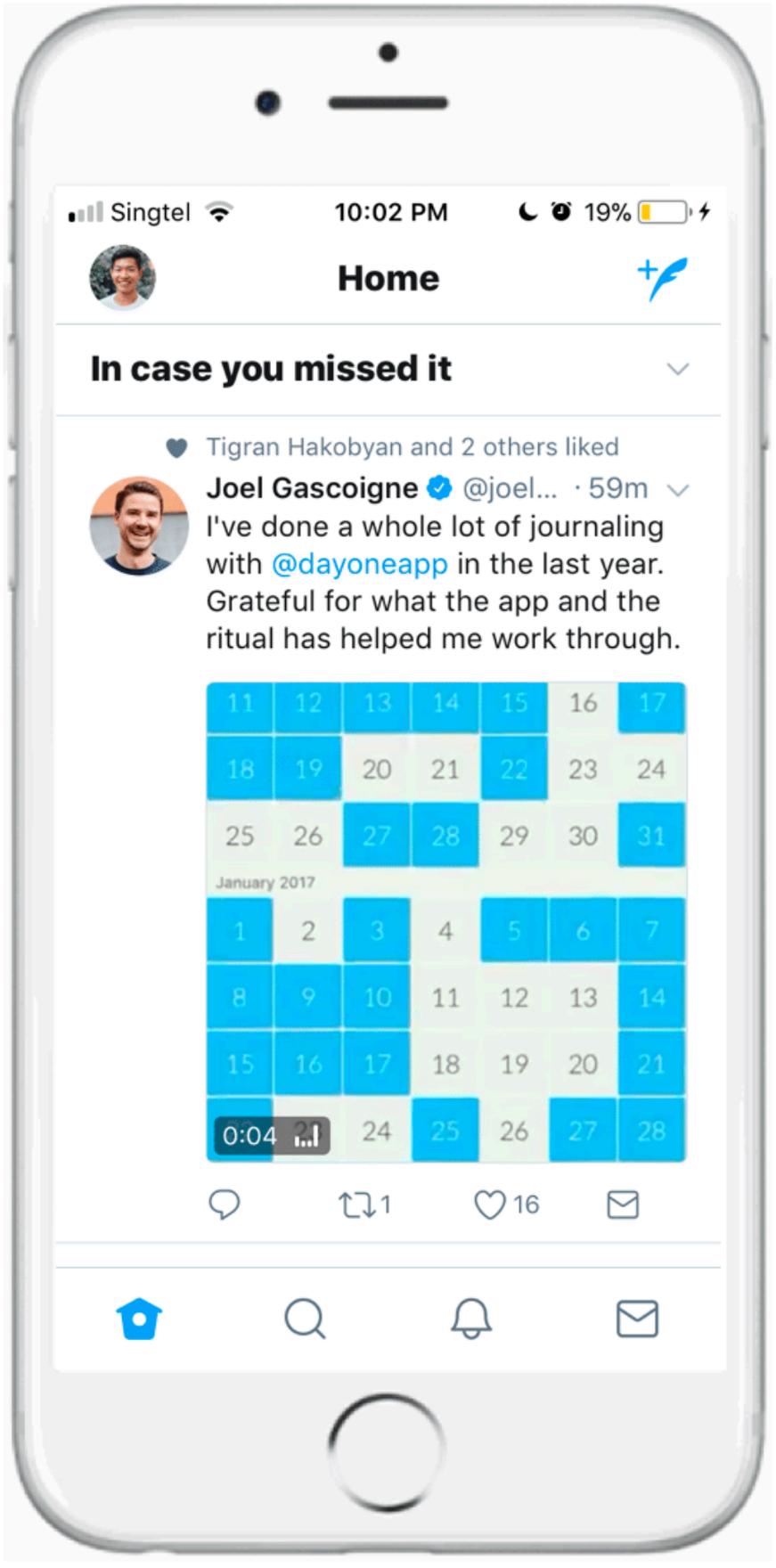


- Data Skew
- Even Distribution
- Rebalancing is difficult

Redis Demo


twitter

Twitter



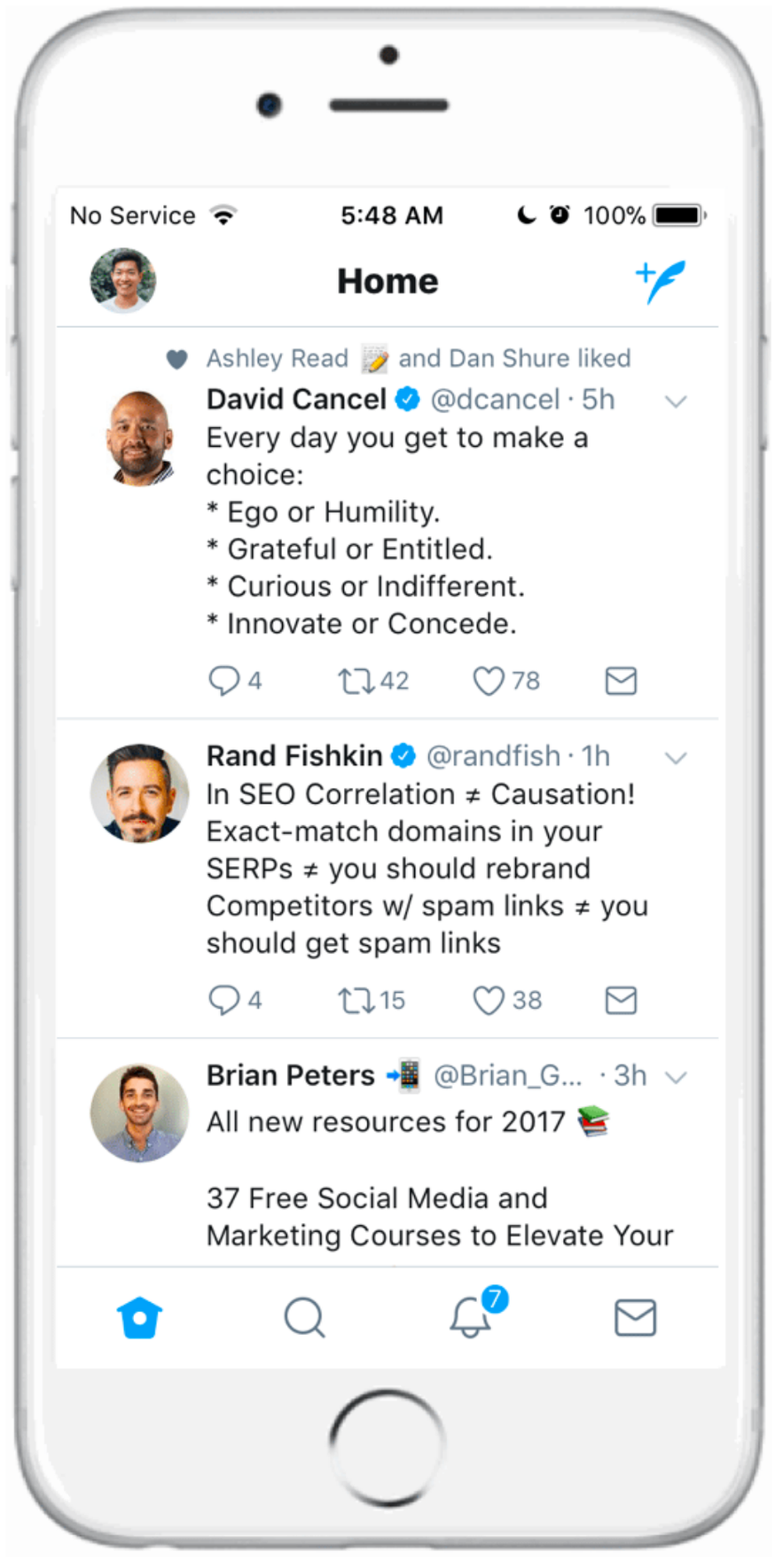
THE TWITTER TIMELINE ALGORITHM

1. Ranked tweets

2. “In case you missed it”

3. Remaining tweets in reverse-chronological order

https://buffer.com/library/twitter-timeline-algorithm/

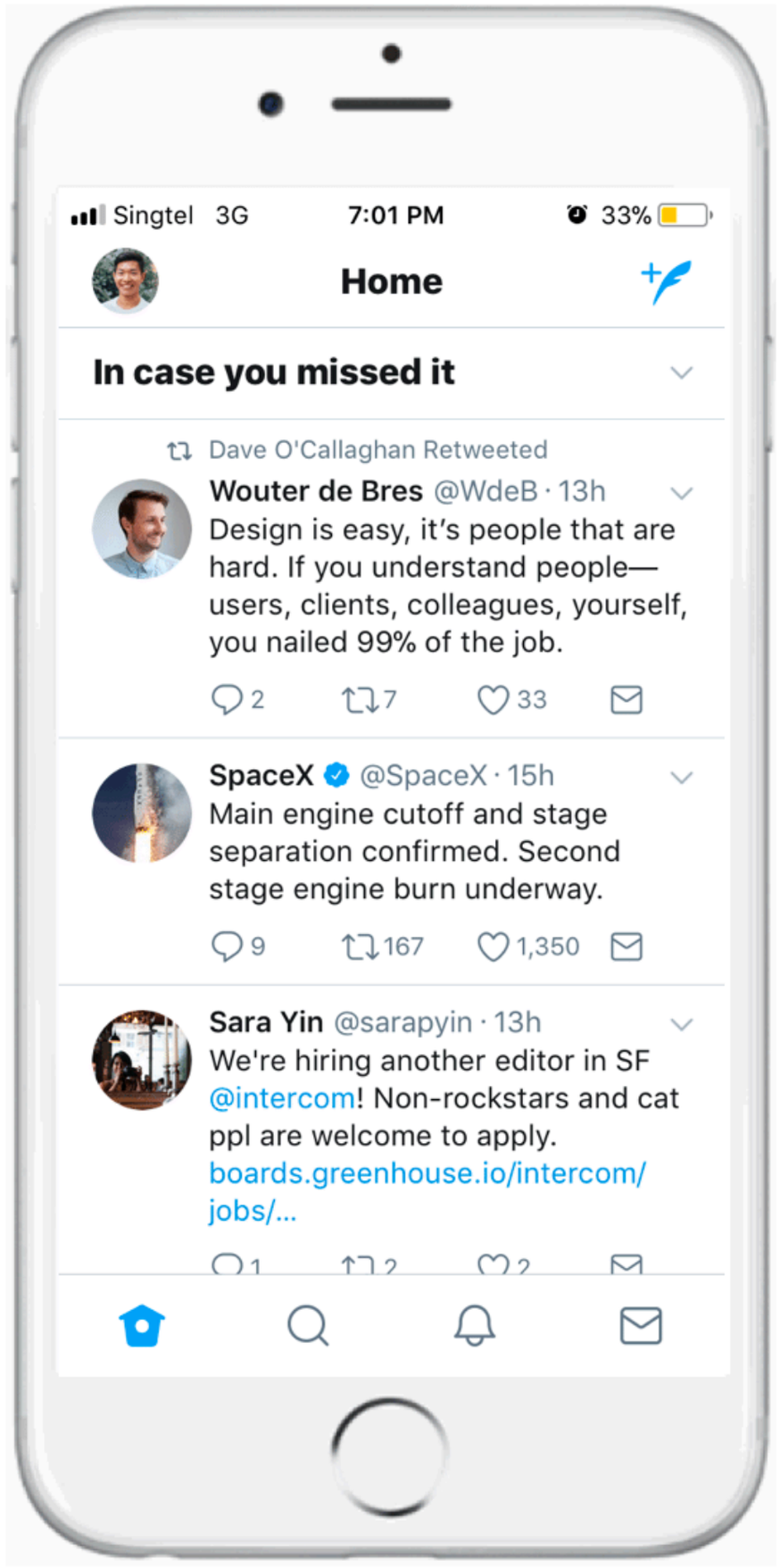


RANKED TWEETS

5 hours ago

1 hour ago

3 hours ago

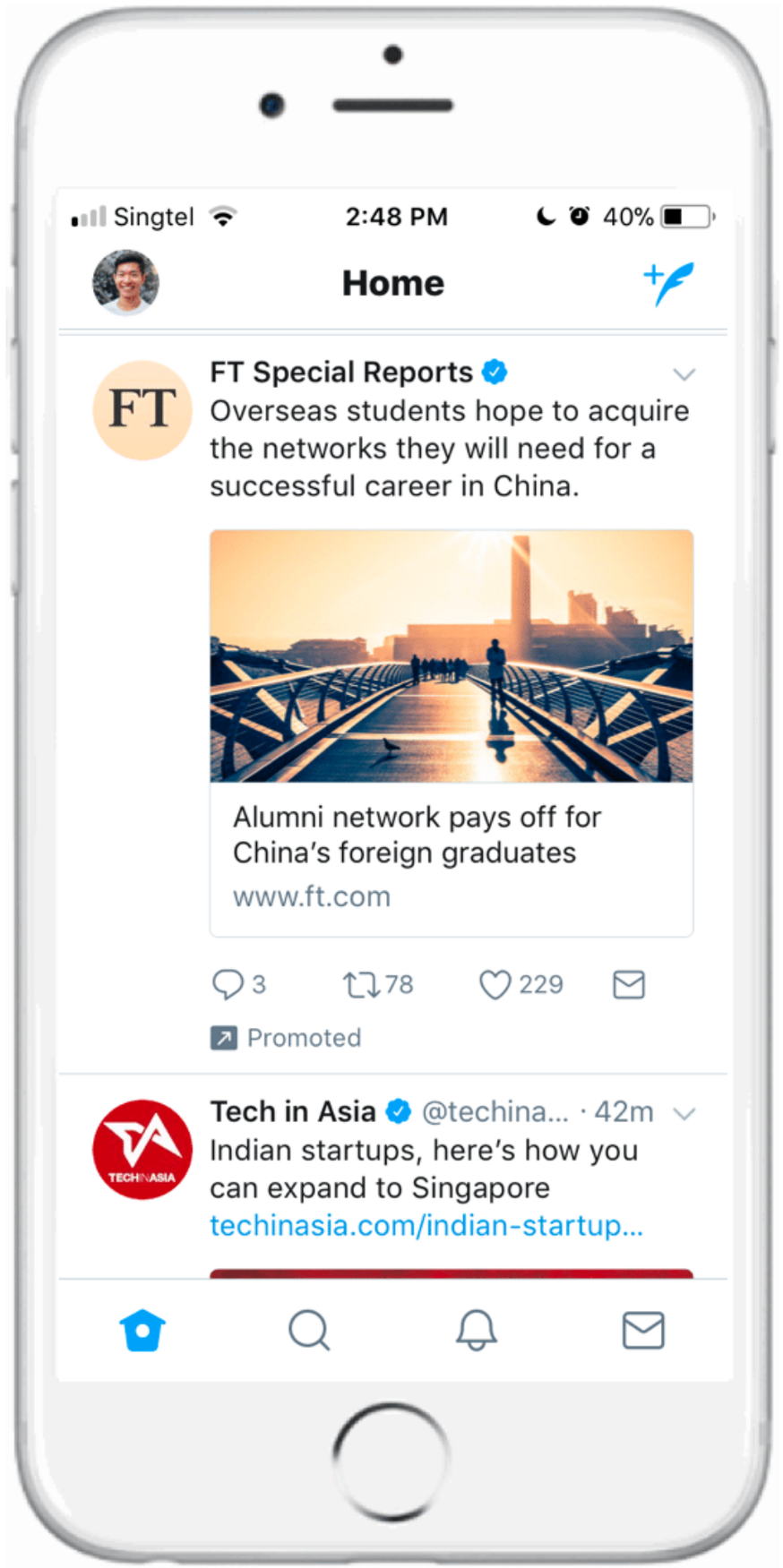


"IN CASE YOU MISSED IT"

13 hours ago

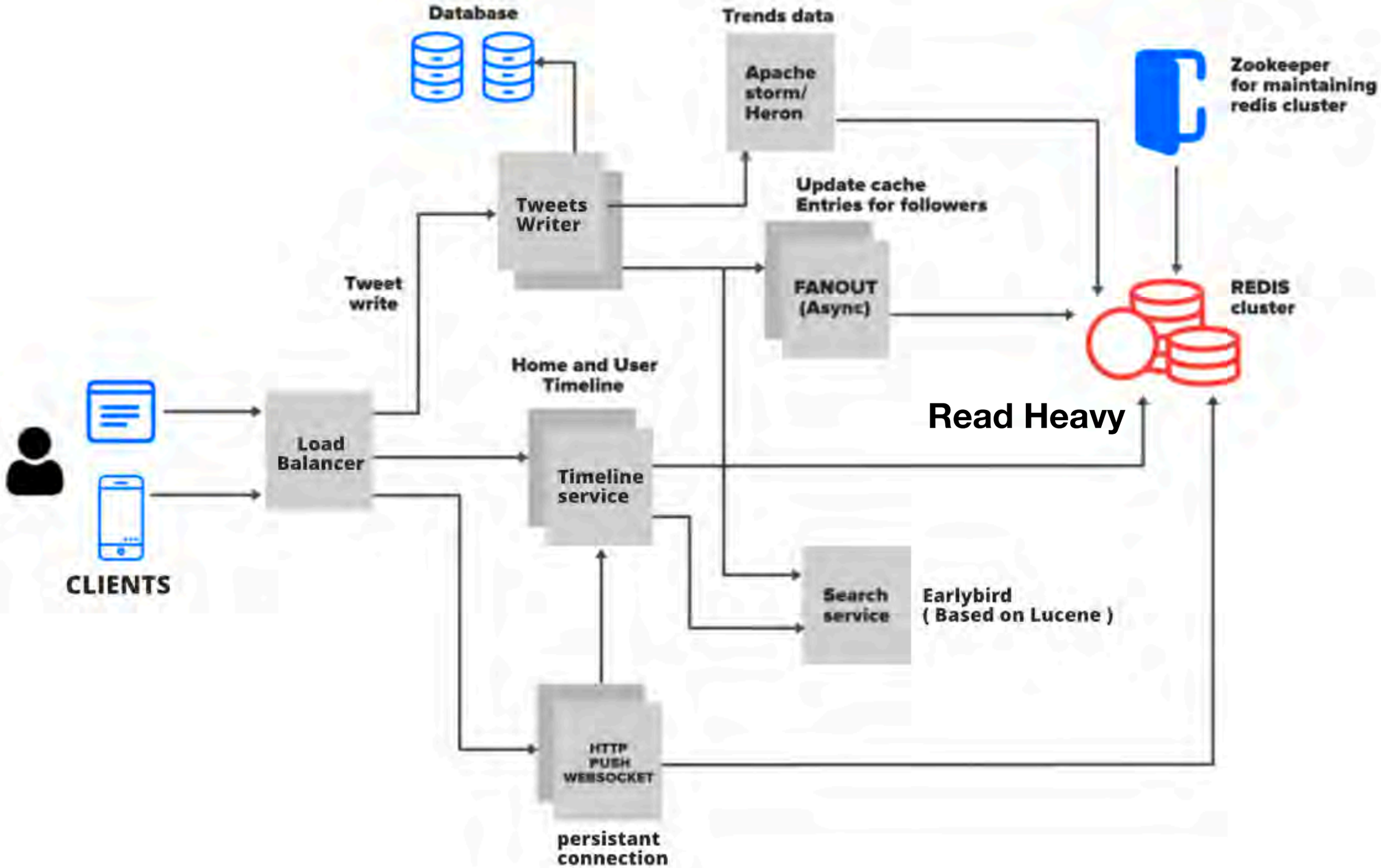
15 hours ago

13 hours ago

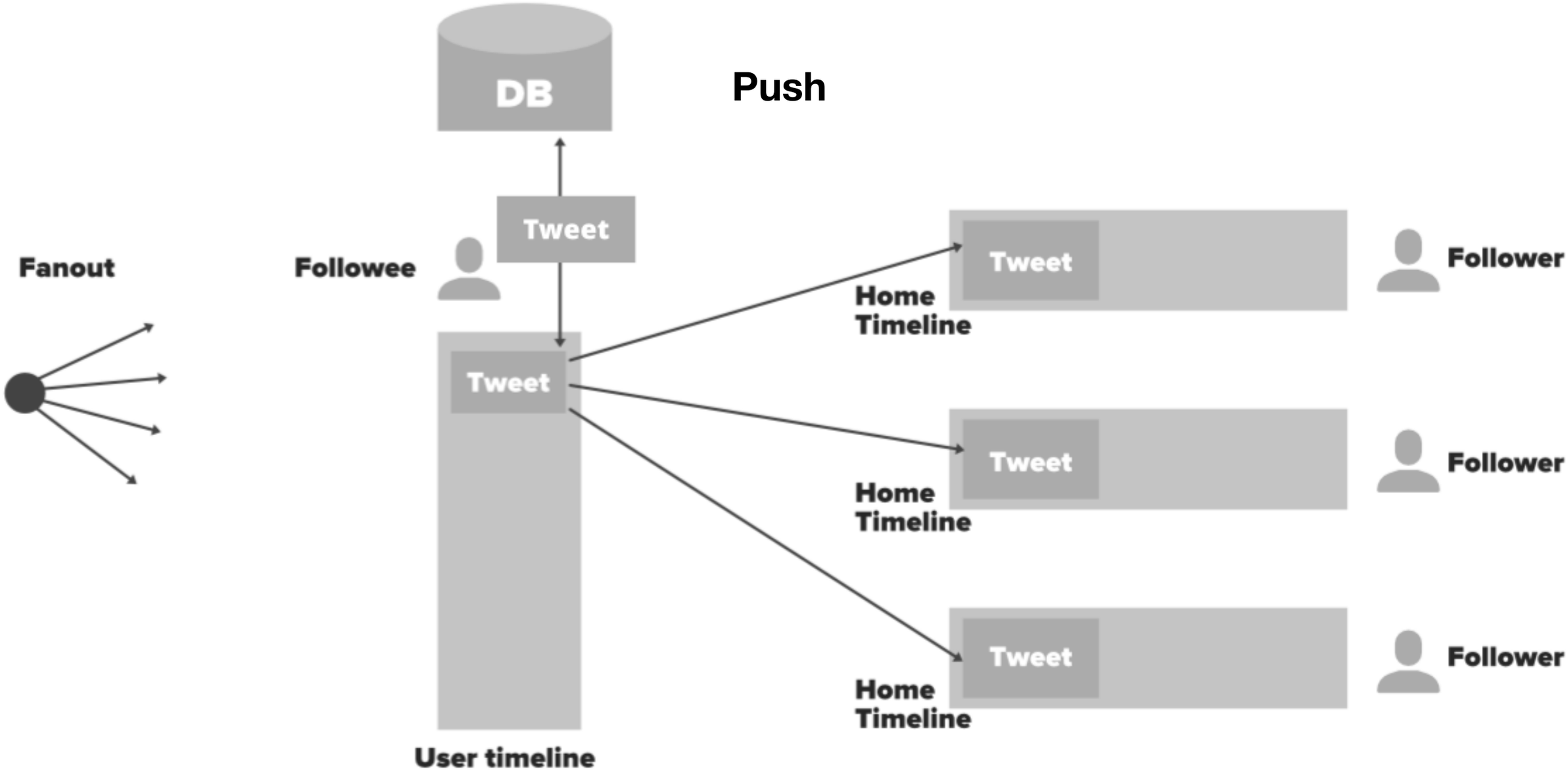


REMAINING TWEETS

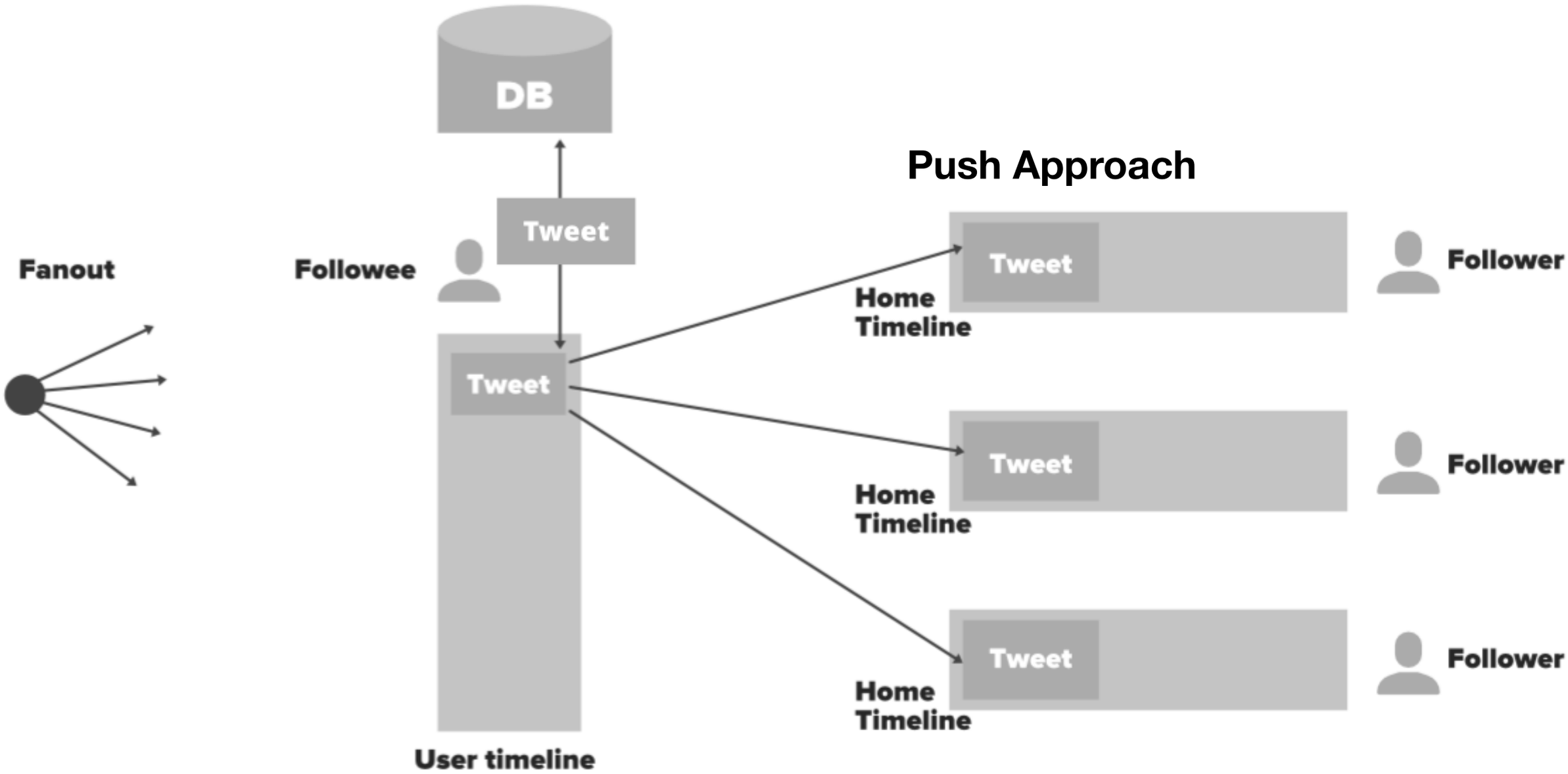
- Retweets
- Promoted tweets
- Suggested accounts
- More



https://www.geeksforgeeks.org/design-twitter-a-system-design-interview-question/



What happen to celebrity who has 30 million follows?



What happen to celebrity who has 30 million follows?
Pull Approach

- If we have 1 million tweets sent each second with average tweet size 1 KB we need to calculate how much data will be generated in next 5 years?

If we have 1 million tweets sent each second with average tweet size 1 KB we need to calculate how much data will be generated in next 5 years?

- 1 Million * 1KB = 1000000 KB in 1 second = 1000MB in 1 second = 1 GB in 1 second

- 1GB * 60 * 60 * 24 in 1 day = 1 * 3600 * 24 = 4000 GB * 25 = 100,000 GB = 100 TB in 1 day

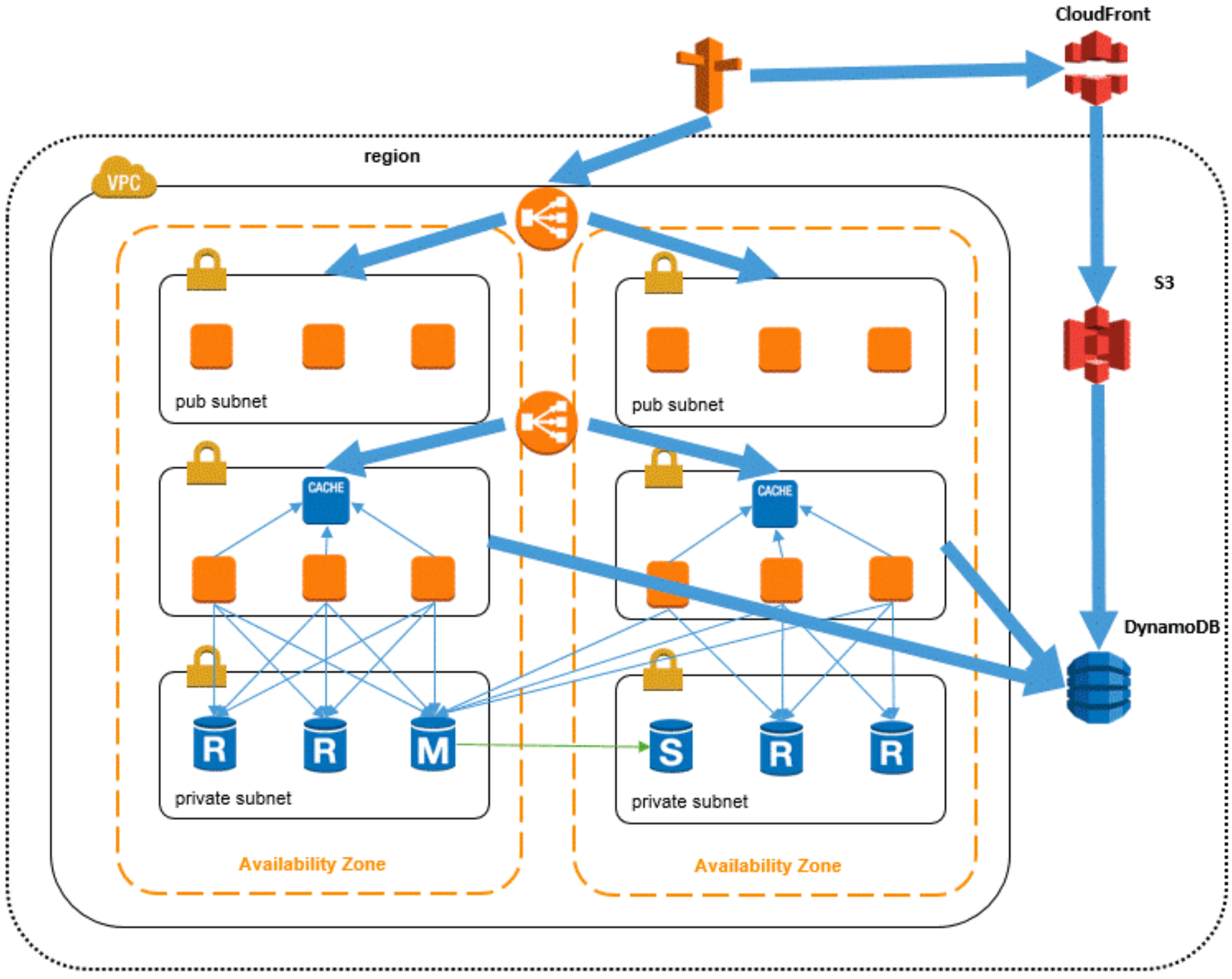
- In 1 year we have 365 * 100TB = 36500 TB = 40000 TB = 40 PB

- In 5 years we have 40 PB * 5 = 200 Petabytes.

- Considering that we should not use more that 70% of our capacity we have 200 * 100 / 70 = 2000/7 = 300 PB

- Reads are almost 50 times more than writes. So we will read 1 GB * 50 = 50 GB in 1 second.

How to take care of variable load?



Question

- You are developing a highly available web application using stateless web servers. Which services are suitable for storing session state data? Choose 3 answers

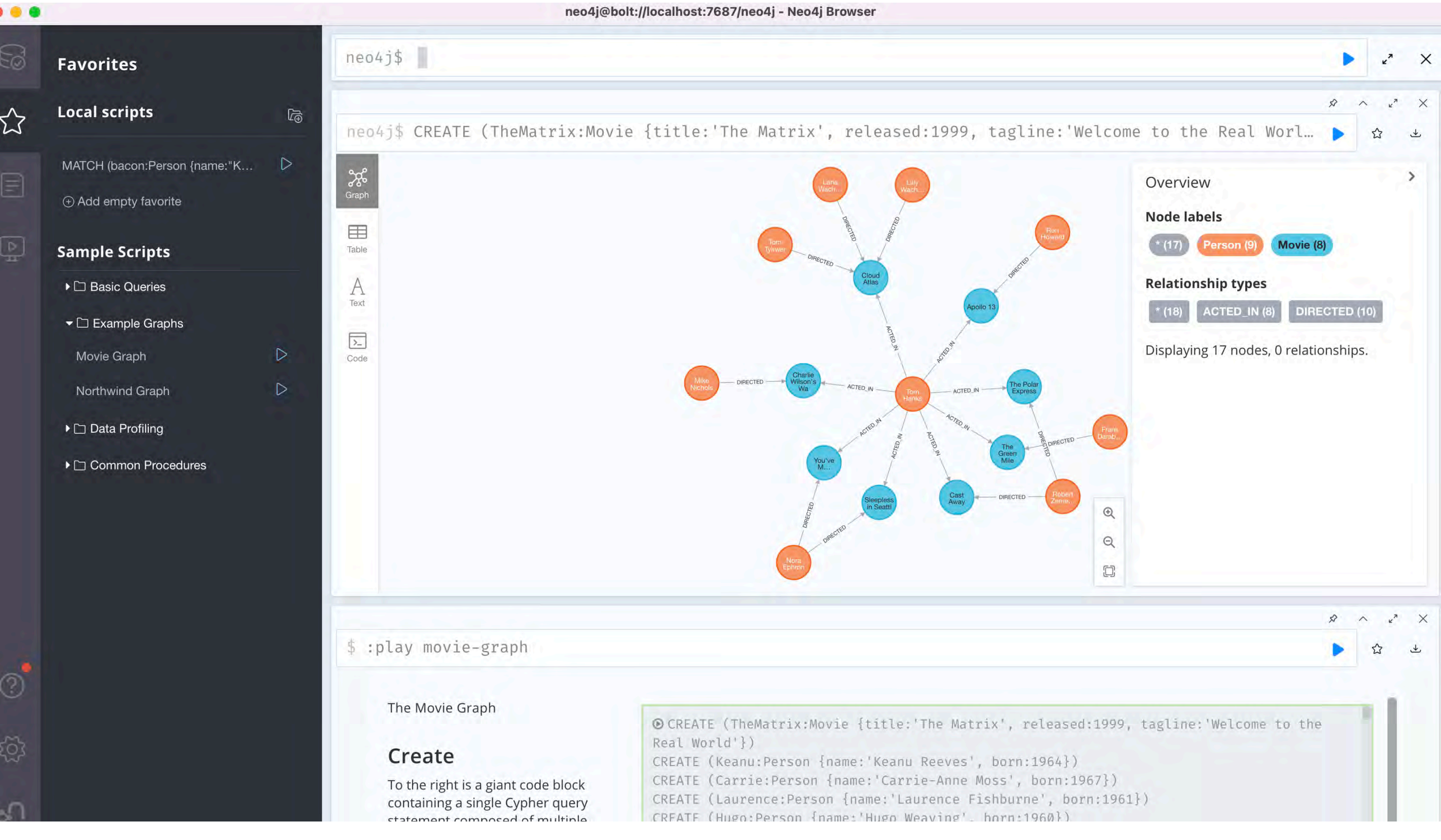
1. Amazon DynamoDB
2. Amazon CloudWatch
3. Elastic Load Balancing
4. Amazon ElasticCache
5. AWS Storage Gateway
6. Amazon Relational Database Service (RDS)

Answer

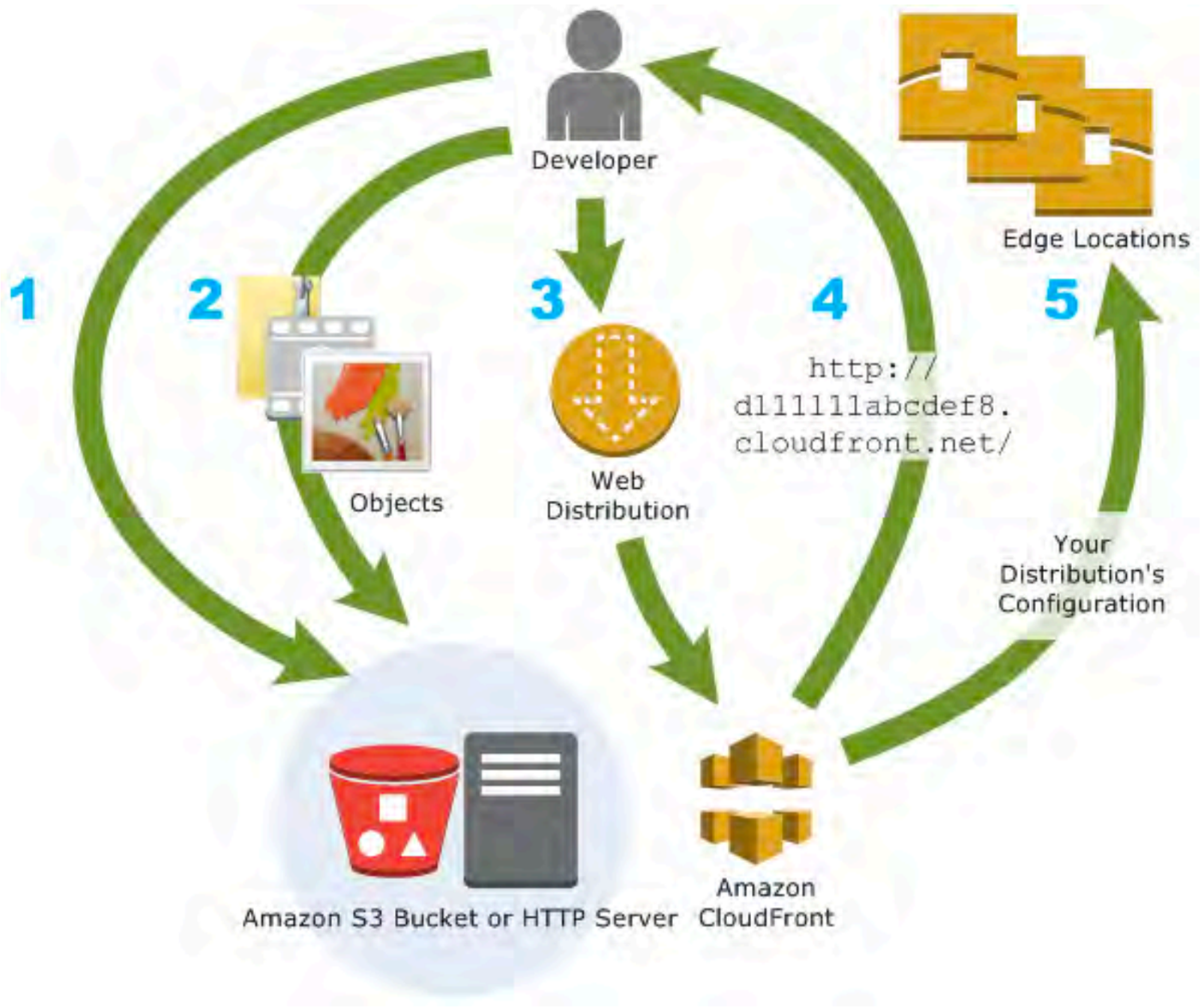
- You are developing a highly available web application using stateless web servers. Which services are suitable for storing session state data? Choose 3 answers

1. **Amazon DynamoDB**
2. Amazon CloudWatch
3. Elastic Load Balancing
4. **Amazon ElasticCache**
5. AWS Storage Gateway
6. **Amazon Relational Database Service (RDS)**

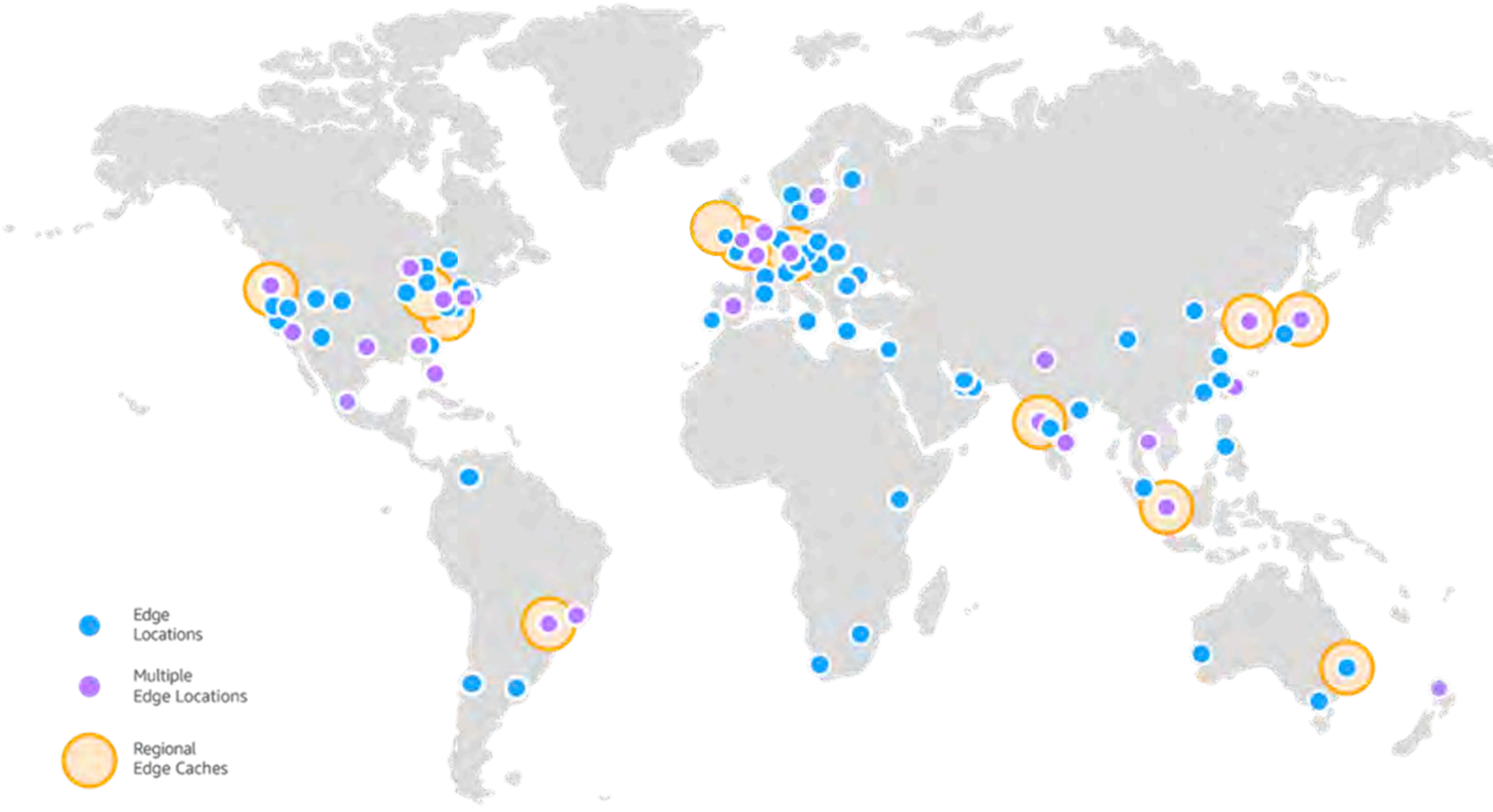
Graph Database-Neo4J



Cloudfront



Global

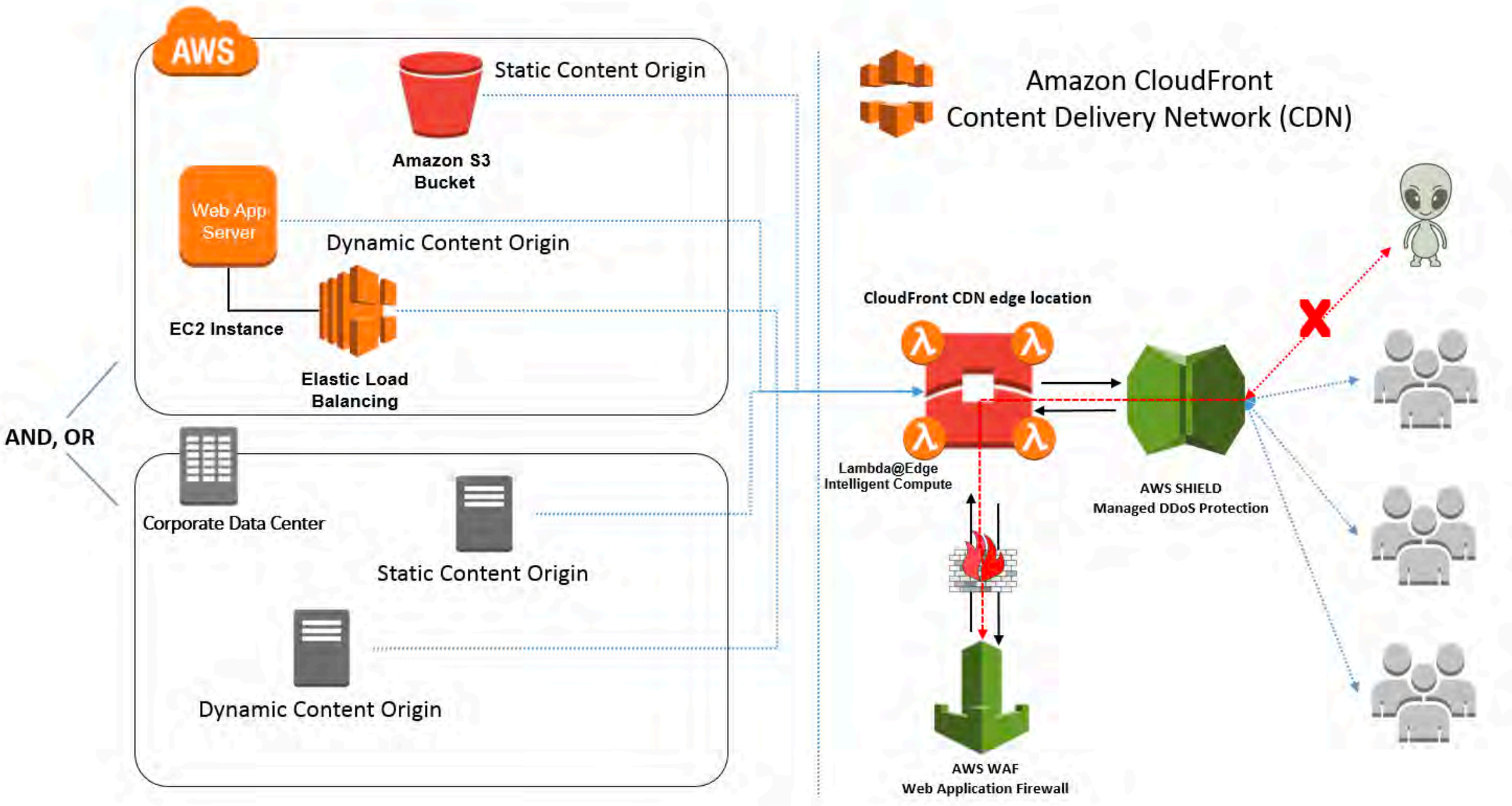


https://aws.amazon.com/cloudfront/features/


S3
Edge
Locations
Multiple
Edge Locations
Regional
Edge Caches


S3
Edge
Locations
Multiple
Edge Locations
Regional
Edge Caches

What strategy to choose for CDN networks like Cloudfront to solve the caching requirements for static and Dynamic content?



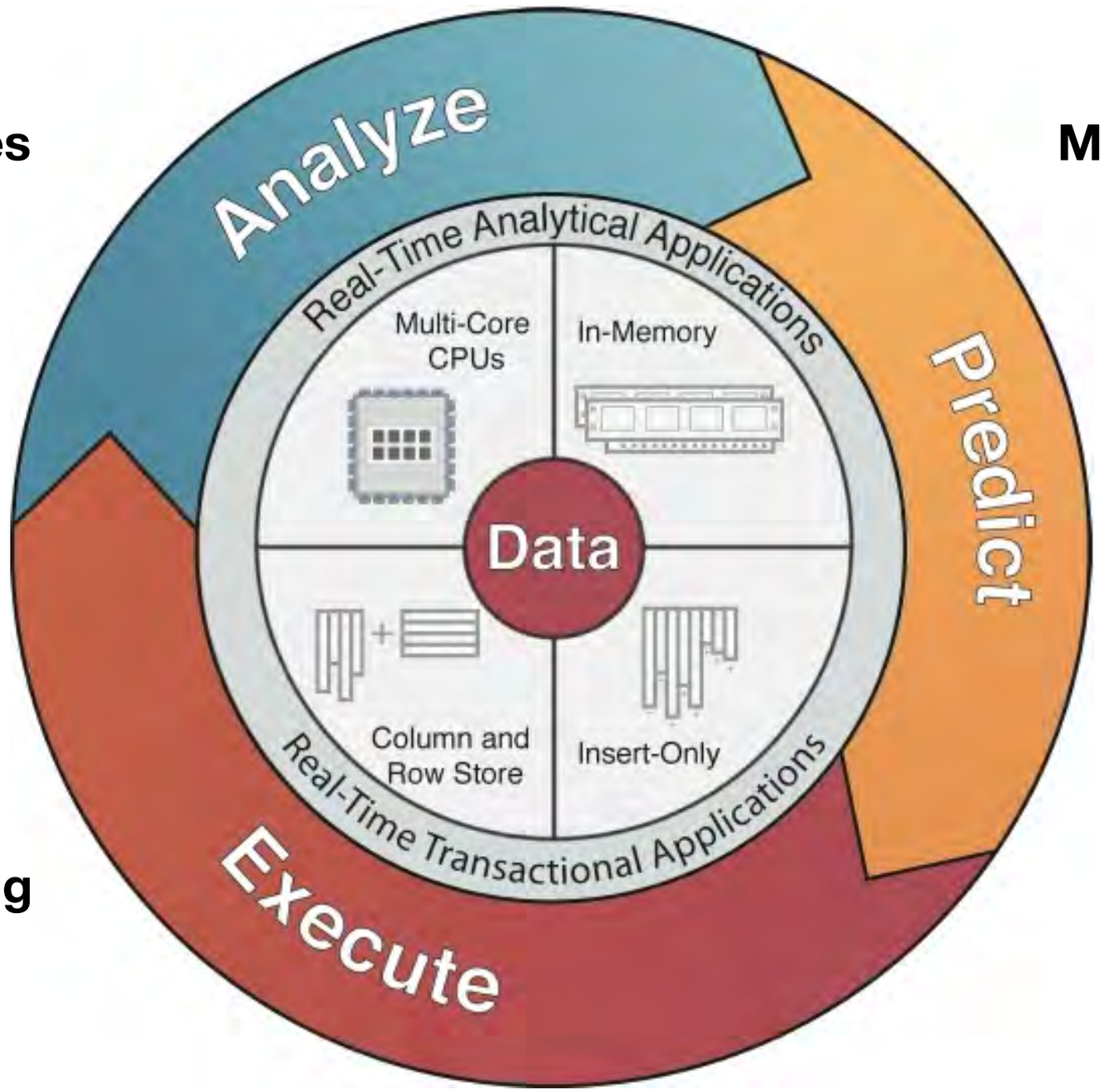
https://aws.amazon.com/caching/cdn/

Amazon CloudFront

- Content - Static and dynamic
- Origins - S3, EC2, ELB, HTTP servers
- Protect private content (SSL)
- Improved Security
  - AWS Shield Standard and Advanced - DOS attacks
  - AWS WAF

Democratize advanced technologies as a Service

No SQL Databases



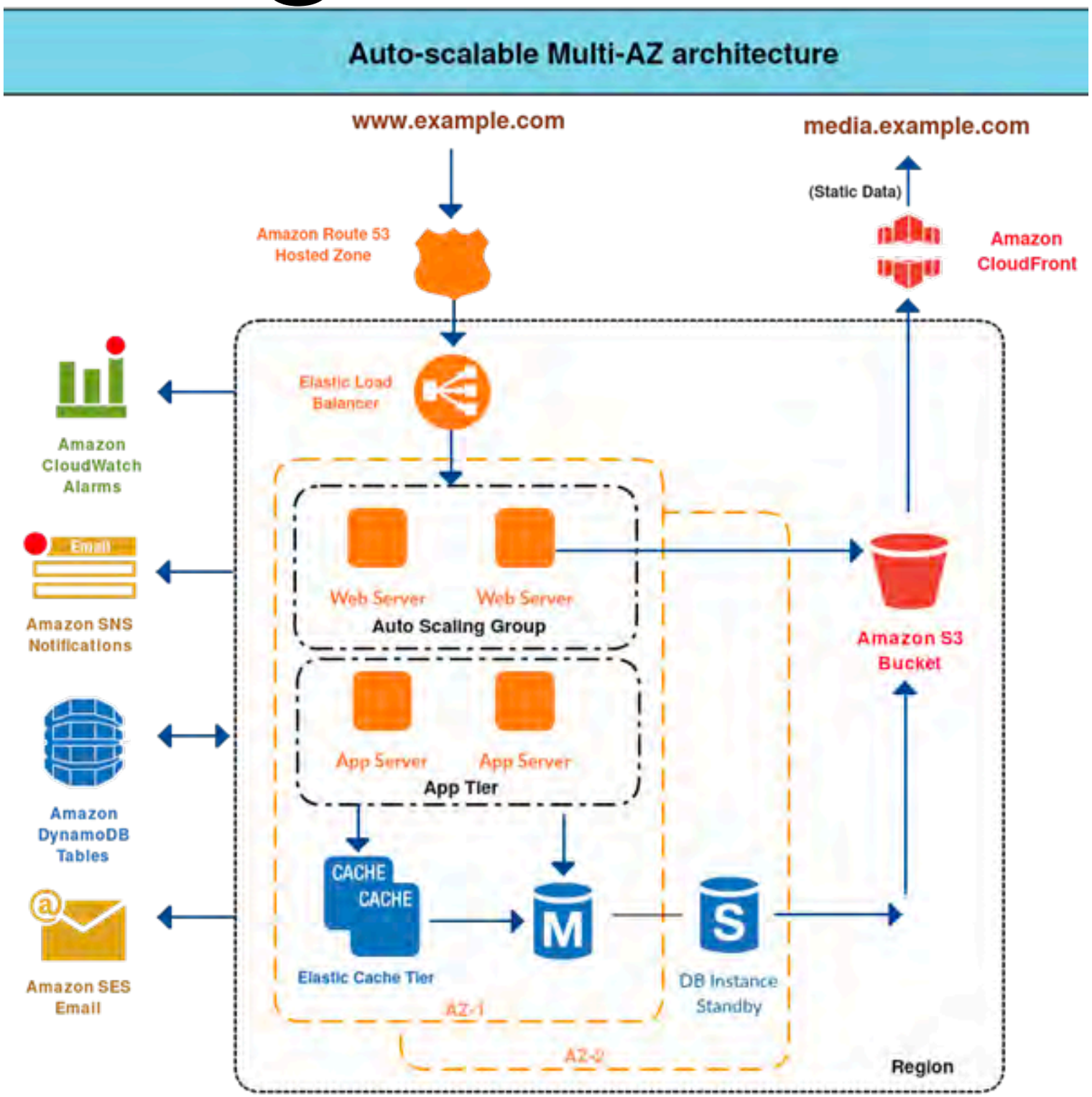
Machine Learning

Media Transcoding

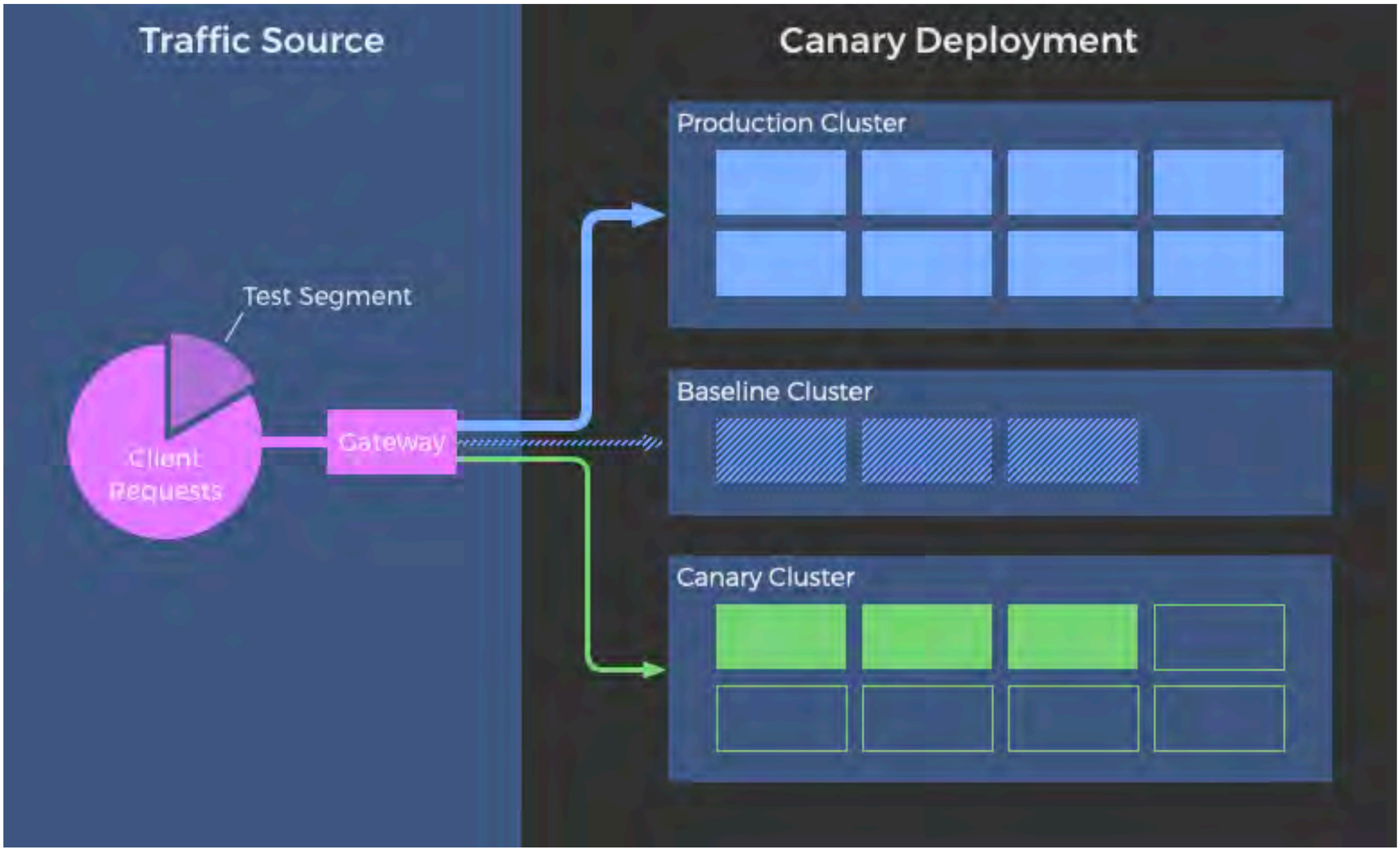
Blockchain

How to monitor and set alarms for performance and network issues?

Scaling Performance



How do you evolve your workload to take advantage of new releases?

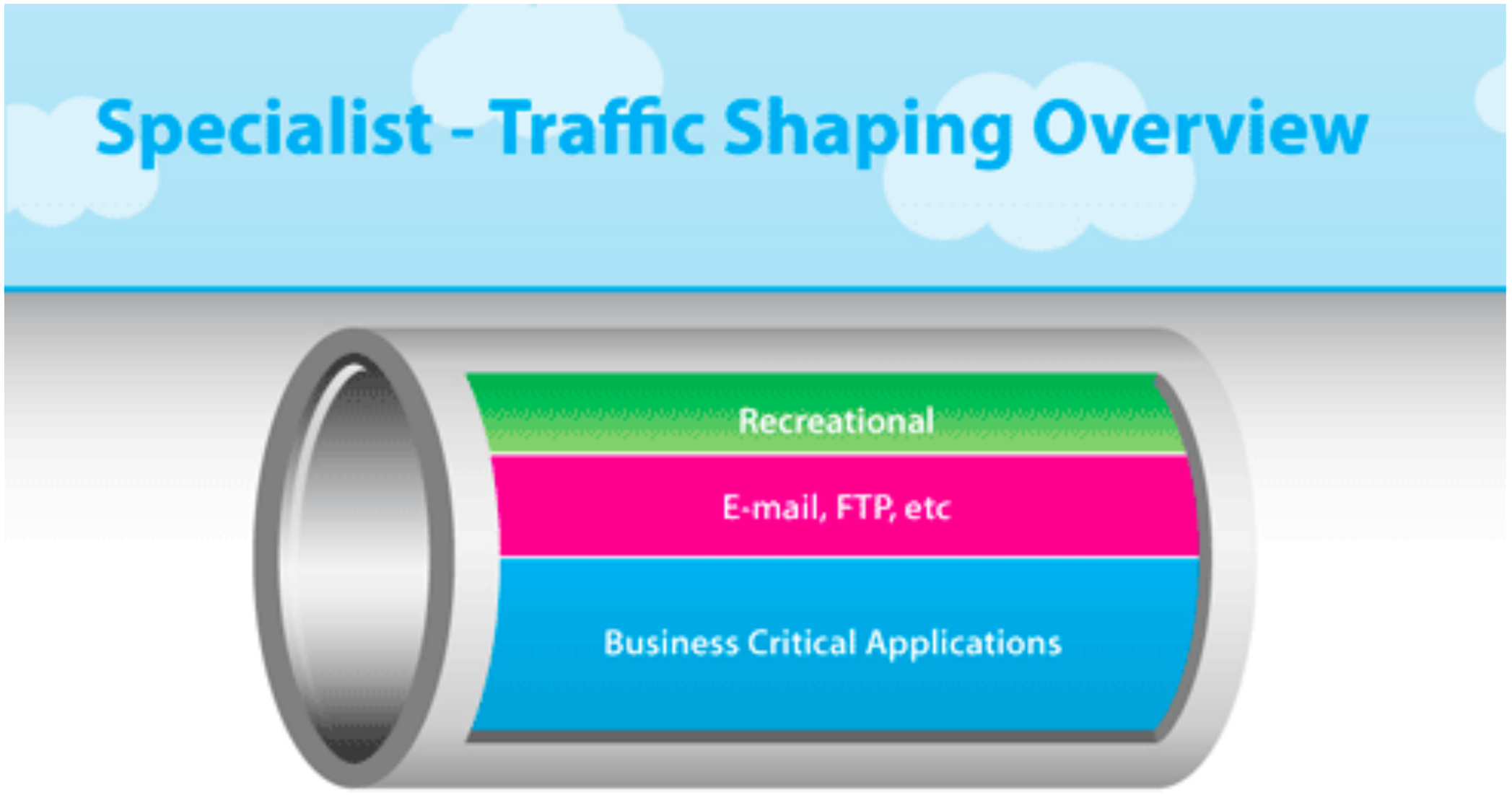


https://glasnostic.com/blog/how-canary-deployments-work-1-kubernetes-istio-linkerd

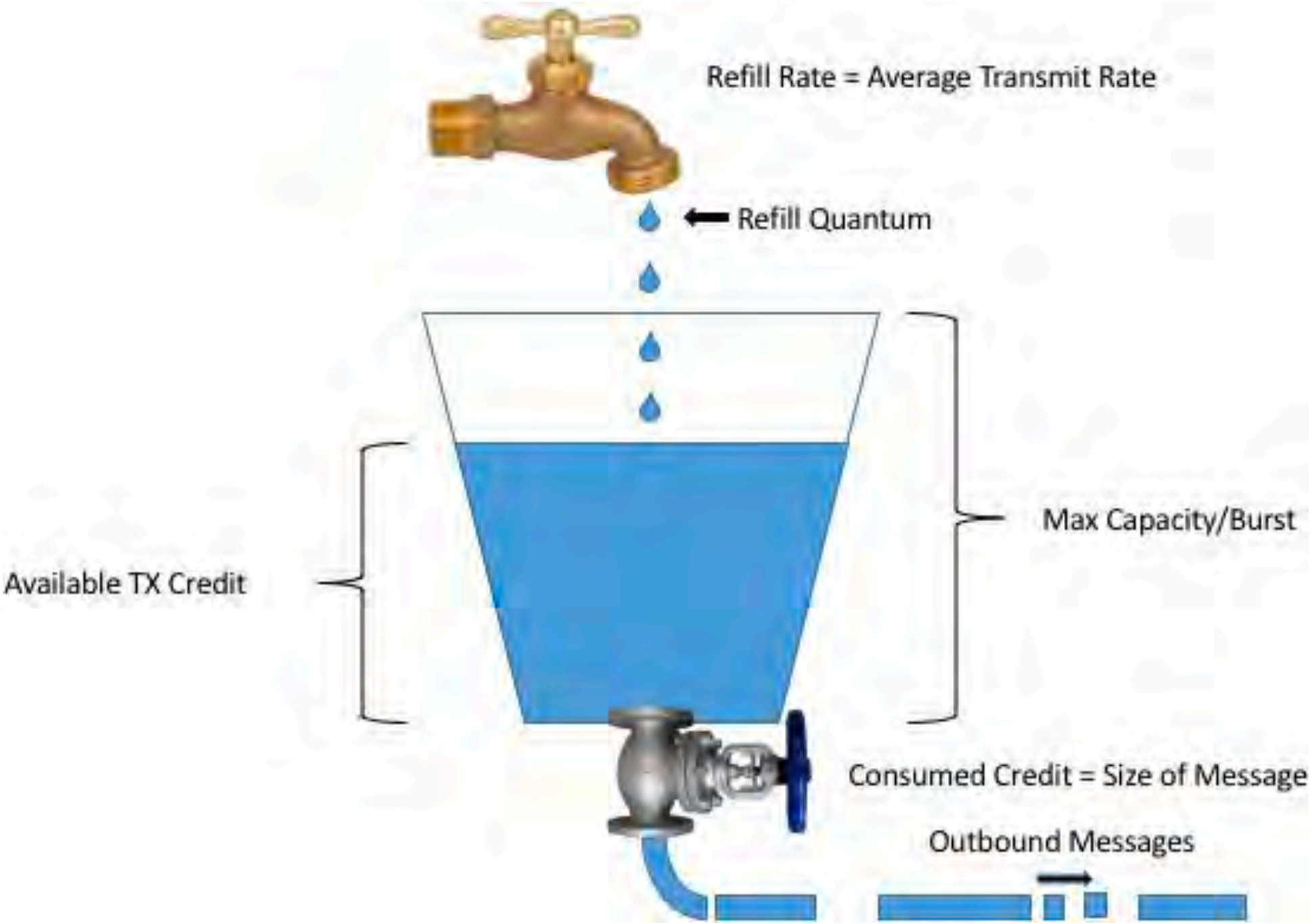
Specialist - Traffic Shaping Overview

Usage without shaping.

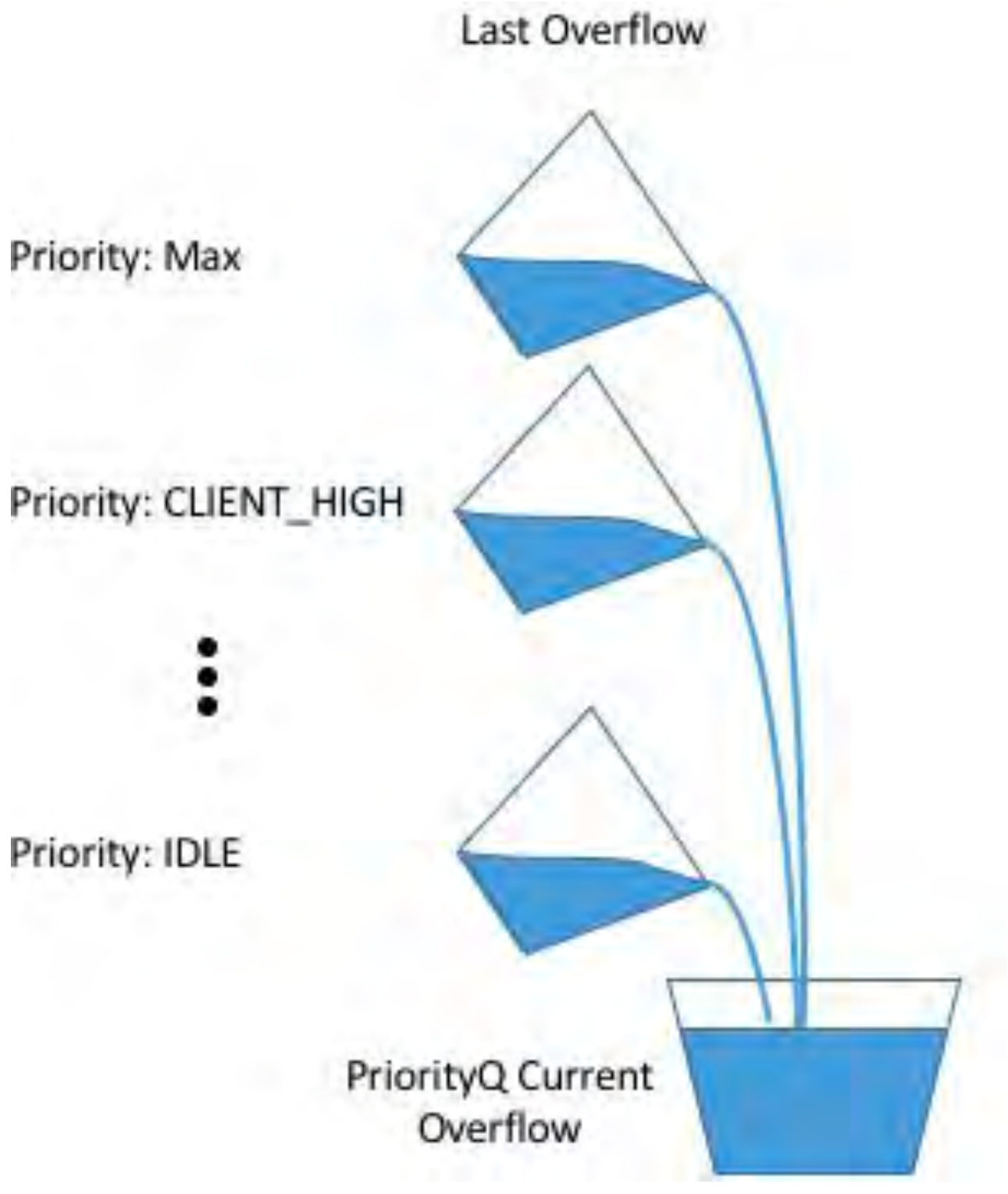
https://linebroker.co.uk/trafficshaping.php

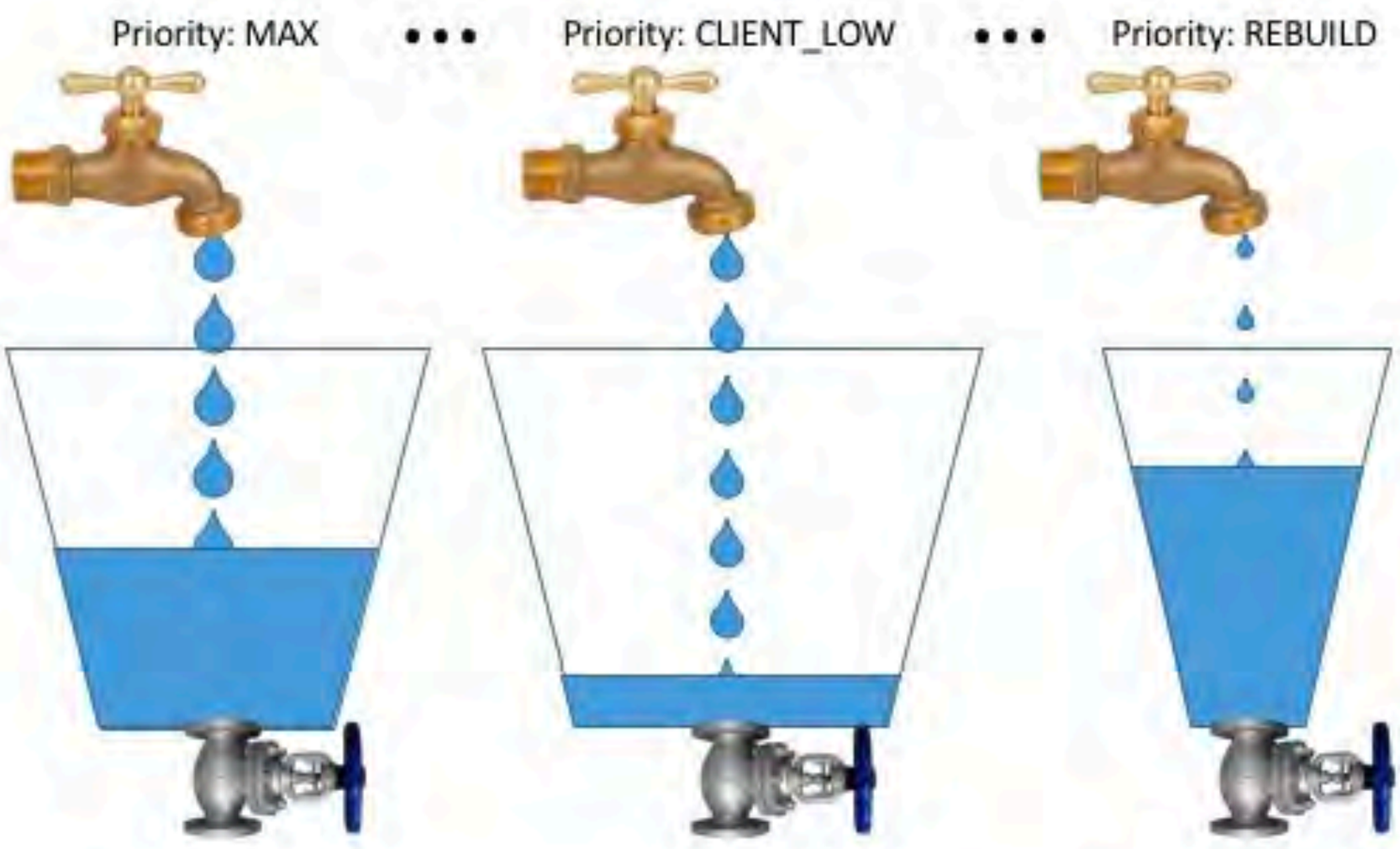


Usage with shaping.



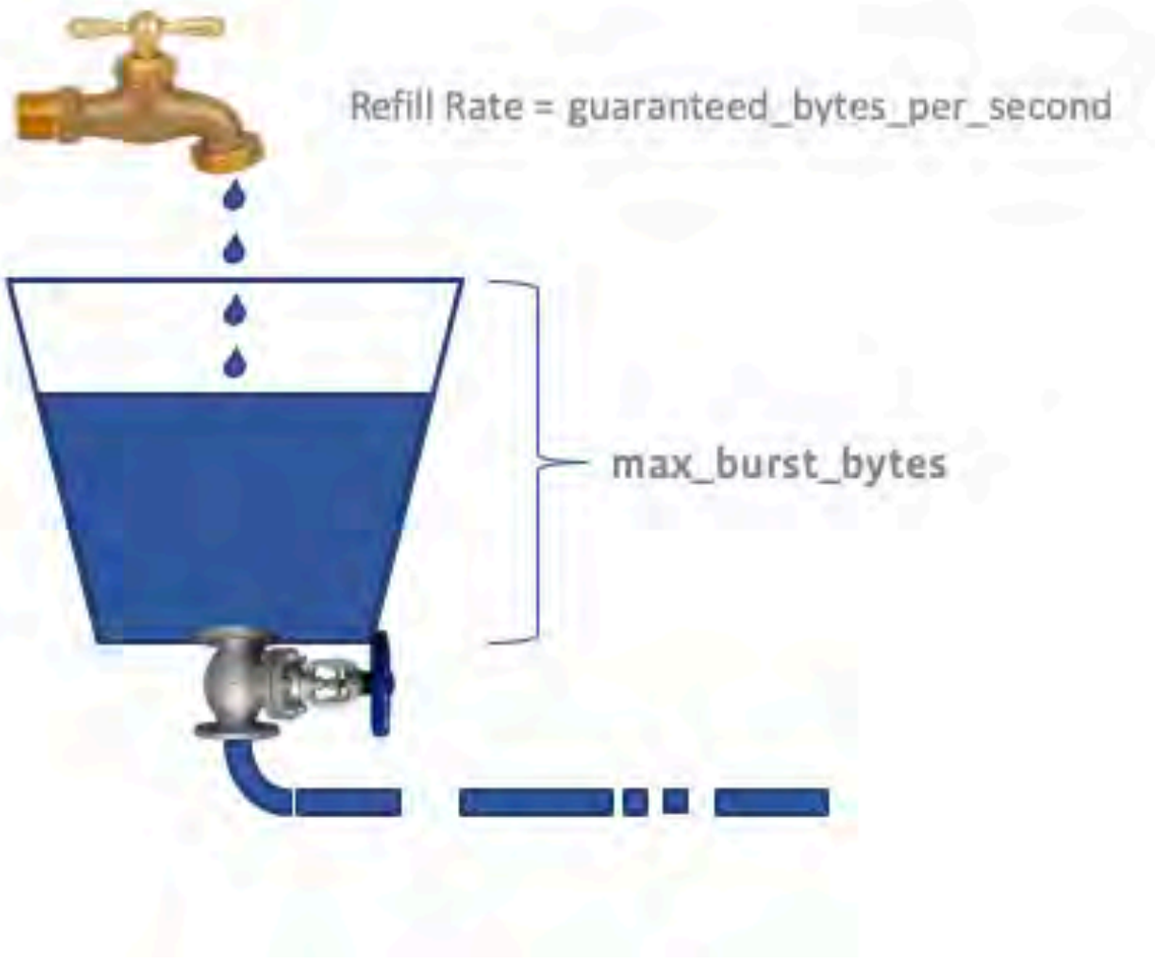
https://logdevice.io/docs/TrafficShaping.html


Last Overflow
Priority: Max
Priority: CLIENT_HIGH
Priority: IDLE
PriorityQ Current
Overflow



Max burst and refill rate can be adjusted independently for each priority.

Configuring



ChatOps

At Shopify

#war-room

417 | 1 | No incidents right now.

Search

Daniella Niyonkuru 1:23 PM
spy incident start me order fraud analysis outage

spy APP 1:23 PM
🔥 An incident was reported at 2017-04-06 16:25:01 UTC. @daniella is the IMOC.
Status summary: order fraud analysis outage
Incident was bound to #war-room. Please use #war-room for communications, or rebind the incident with /incident channel.

spy APP 1:23 PM
set the channel topic: 🔥 @daniella is IMOC for incident: order fraud analysis outage

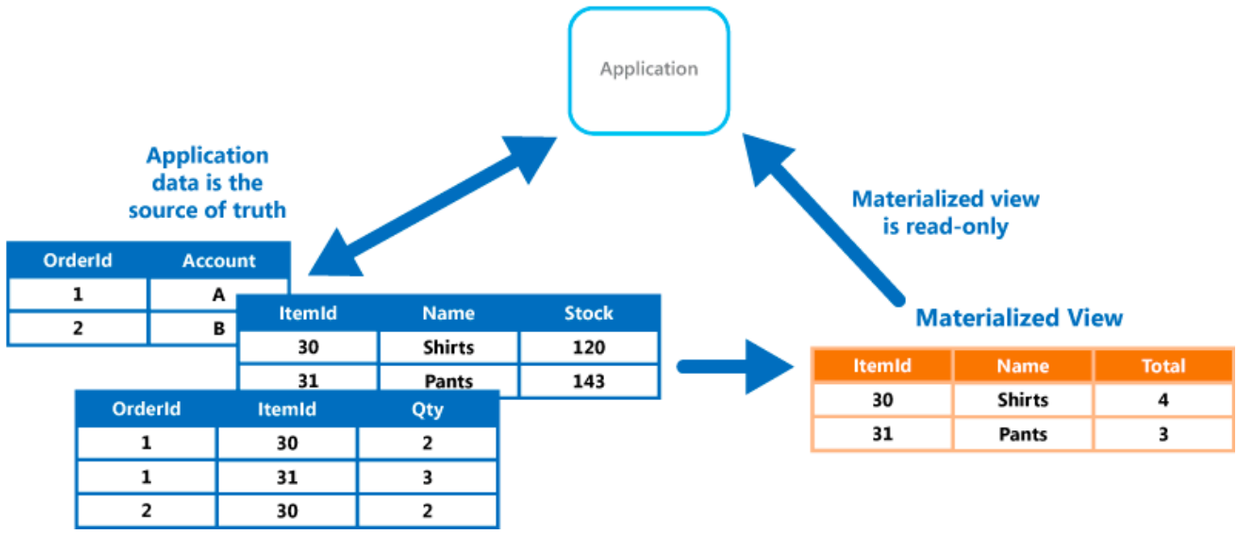
[redacted]

spy APP 1:23 PM
Status Page Summary
*** Components Report ***
Admin : operational
Checkout : operational
Reports and Dashboards : operational
Storefront : operational
API & Mobile : operational
Support : operational
Third party services : operational
*** Unresolved Incidents Report ***
No reported unresolved incidents.

How to handle skewed data?
How to make it performant?

Materialized view

- Domain Driven Design
- Different Data stores
- Eventually consistent
- Query performance



Order table

Partition key	Row key	Order date	Shipping address	Total invoice	Order status
001 (Customer ID)	1 (Order ID)	11082013	One Microsoft way Redmond, WA 98052	$400	In process
005	2	11082013	One Microsoft way Redmond, WA 98052	$200	Shipped

OrderItem table

Partition key	Row key	Product	Unit Price	Amount	Total
1 (Order ID)	001_1 (OrderItem ID)	XX	$100	2	$200
1	001_2	YY	$40	5	$200
2	002_1	ZZ	$200	1	$200

Customer table

Partition key	Row key	Billing Information	Shipping address	Gender	Age
US East (region)	001 (Customer ID)	*****0001	One Microsoft way Redmond, WA 98052	Female	30
US East	002	*****2006	One Microsoft way Redmond, WA 98052	Male	40

Materialized View

Partition key	Row key	Product Name	Total sold	Number of customers
Electronics (Product category)	001 (Product ID)	XX	$30,000	500
Electronics	002	YY	$100,000	400

What if we have billions of rows of data for multiple customers, multiple locations, multiple divisions?

Think Amazon
Coke

Horizontal Partitioning (Sharding)

Key	Name	Description	Stock	Price	LastOrdered
ARC1	Arc welder	250 Amps	8	119.00	25-Nov-2013
BRK8	Bracket	250mm	46	5.66	18-Nov-2013
BRK9	Bracket	400mm	82	6.98	1-Jul-2013
HOS8	Hose	1/2"	27	27.50	18-Aug-2013
WGT4	Widget	Green	16	13.99	3-Feb-2013
WGT6	Widget	Purple	76	13.99	31-Mar-2013

Key	Name	Description	Stock	Price	LastOrdered
ARC1	Arc welder	250 Amps	8	119.00	25-Nov-2013
BRK8	Bracket	250mm	46	5.66	18-Nov-2013
BRK9	Bracket	400mm	82	6.98	1-Jul-2013

Key	Name	Description	Stock	Price	LastOrdered
HOS8	Hose	1/2"	27	27.50	18-Aug-2013
WGT4	Widget	Green	16	13.99	3-Feb-2013
WGT6	Widget	Purple	76	13.99	31-Mar-2013

What else can be partition?
Think GDPR
Think PII data

Vertical Partitioning

Key	Name	Description	Stock	Price	LastOrdered
ARC1	Arc welder	250 Amps	8	119.00	25-Nov-2013
BRK8	Bracket	250mm	46	5.66	18-Nov-2013
BRK9	Bracket	400mm	82	6.98	1-Jul-2013
HOS8	Hose	1/2"	27	27.50	18-Aug-2013
WGT4	Widget	Green	16	13.99	3-Feb-2013
WGT6	Widget	Purple	76	13.99	31-Mar-2013

Materialized View

Key	Name	Description	Price
ARC1	Arc welder	250 Amps	119.00
BRK8	Bracket	250mm	5.66
BRK9	Bracket	400mm	6.98
HOS8	Hose	1/2"	27.50
WGT4	Widget	Green	13.99
WGT6	Widget	Purple	13.99

Static data

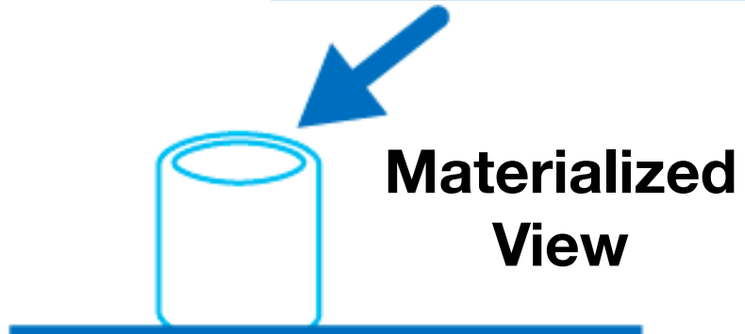
Key	Stock	LastOrdered
ARC1	8	25-Nov-2013
BRK8	46	18-Nov-2013
BRK9	82	1-Jul-2013
HOS8	27	18-Aug-2013
WGT4	16	3-Feb-2013
WGT6	76	31-Mar-2013

Dynamic data

Where we would do this?

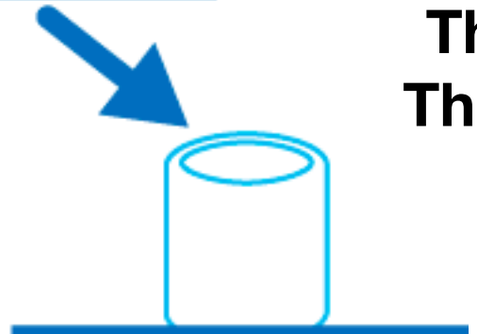
Vertical Partitioning

Key	Name	Description	Stock	Price	LastOrdered
ARC1	Arc welder	250 Amps	8	119.00	25-Nov-2013
BRK8	Bracket	250mm	46	5.66	18-Nov-2013
BRK9	Bracket	400mm	82	6.98	1-Jul-2013
HOS8	Hose	1/2"	27	27.50	18-Aug-2013
WGT4	Widget	Green	16	13.99	3-Feb-2013
WGT6	Widget	Purple	76	13.99	31-Mar-2013



Key	Name	Description	Price
ARC1	Arc welder	250 Amps	119.00
BRK8	Bracket	250mm	5.66
BRK9	Bracket	400mm	6.98
HOS8	Hose	1/2"	27.50
WGT4	Widget	Green	13.99
WGT6	Widget	Purple	13.99

Static data



Key	Stock	LastOrdered
ARC1	8	25-Nov-2013
BRK8	46	18-Nov-2013
BRK9	82	1-Jul-2013
HOS8	27	18-Aug-2013
WGT4	16	3-Feb-2013
WGT6	76	31-Mar-2013

Dynamic data

How about different Systems?

Functional Partitioning

Corporate data domain

Key	Name	Description	Price	...
ARC1	Arc welder	250 Amps	119.00	...
BRK8	Bracket	250mm	5.66	...
BRK9	Bracket	400mm	6.98	...
HOS8	Hose	1/2"	27.50	...
WGT4	Widget	Green	13.99	...
WGT6	Widget	Purple	13.99	...

Key	Customer	Address	Phone	...
1630	[name]	[address]	12345	...
1631	[name]	[address]	12345	...
1648	[name]	[address]	12345	...
1842	[name]	[address]	12345	...
2055	[name]	[address]	12345	...
2139	[name]	[address]	12345	...

Bounded Contexts

Inventory

Key	Name	Description	Price	...
ARC1	Arc welder	250 Amps	119.00	...
BRK8	Bracket	250mm	5.66	...
BRK9	Bracket	400mm	6.98	...
HOS8	Hose	1/2"	27.50	...
WGT4	Widget	Green	13.99	...
WGT6	Widget	Purple	13.99	...

Customer

Key	Customer	Address	Phone	...
1630	[name]	[address]	12345	...
1631	[name]	[address]	12345	...
1648	[name]	[address]	12345	...
1842	[name]	[address]	12345	...
2055	[name]	[address]	12345	...
2139	[name]	[address]	12345	...

What to do when data is not volatile or not skewed?

Primary Key (Customer ID)	Customer Data
1	LastName: Smith, Town: Redmond, …
2	LastName: Jones, Town: Seattle, …
3	LastName: Robinson, Town: Portland, …
4	LastName: Brown, Town: Redmond, …
5	LastName: Smith, Town: Chicago, …
6	LastName: Green, Town: Redmond, …
7	LastName: Clarke, Town: Portland, …
8	LastName: Smith, Town: Redmond, …
9	LastName: Jones, Town: Chicago, …
…	…
1000	LastName: Clarke, Town: Chicago, …
…	…

- Select by city ; Select by last name

Index table

Secondary Key (Town)	Customer Data
Chicago	ID: 5, LastName: Smith, Town: Chicago, ...
Chicago	ID: 9, LastName: Jones, Town: Chicago, ...
Chicago	ID: 1000, LastName: Clarke, Town: Chicago, ...
...	...
Portland	ID: 3, LastName: Robinson, Town: Portland, ...
Portland	ID: 7, LastName: Clarke, Town: Portland, ...
Redmond	ID: 1, LastName: Smith, Town: Redmond, ...
Redmond	ID: 4, LastName: Brown, Town: Redmond, ...
Redmond	ID: 6, LastName: Green, Town: Redmond, ...
Redmond	ID: 8, LastName: Smith, Town: Redmond, ...
Seattle	ID: 2, LastName: Jones, Town: Seattle, ...
...	...

Secondary Key (LastName)	Customer Data
Brown	ID: 4, LastName: Brown, Town: Redmond, ...
Clarke	ID: 7, LastName: Clarke, Town: Portland, ...
Clarke	ID: 1000, LastName: Clarke, Town: Chicago, ...
Green	ID: 6, LastName: Green, Town: Redmond, ...
Jones	ID: 2, LastName: Jones, Town: Seattle, ...
Jones	ID: 9, LastName: Jones, Town: Chicago, ...
...	...
Robinson	ID: 3, LastName: Robinson, Town: Portland, ...
Smith	ID: 1, LastName: Smith, Town: Redmond, ...
Smith	ID: 5, LastName: Smith, Town: Chicago, ...
Smith	ID: 8, LastName: Smith, Town: Redmond, ...
...	...

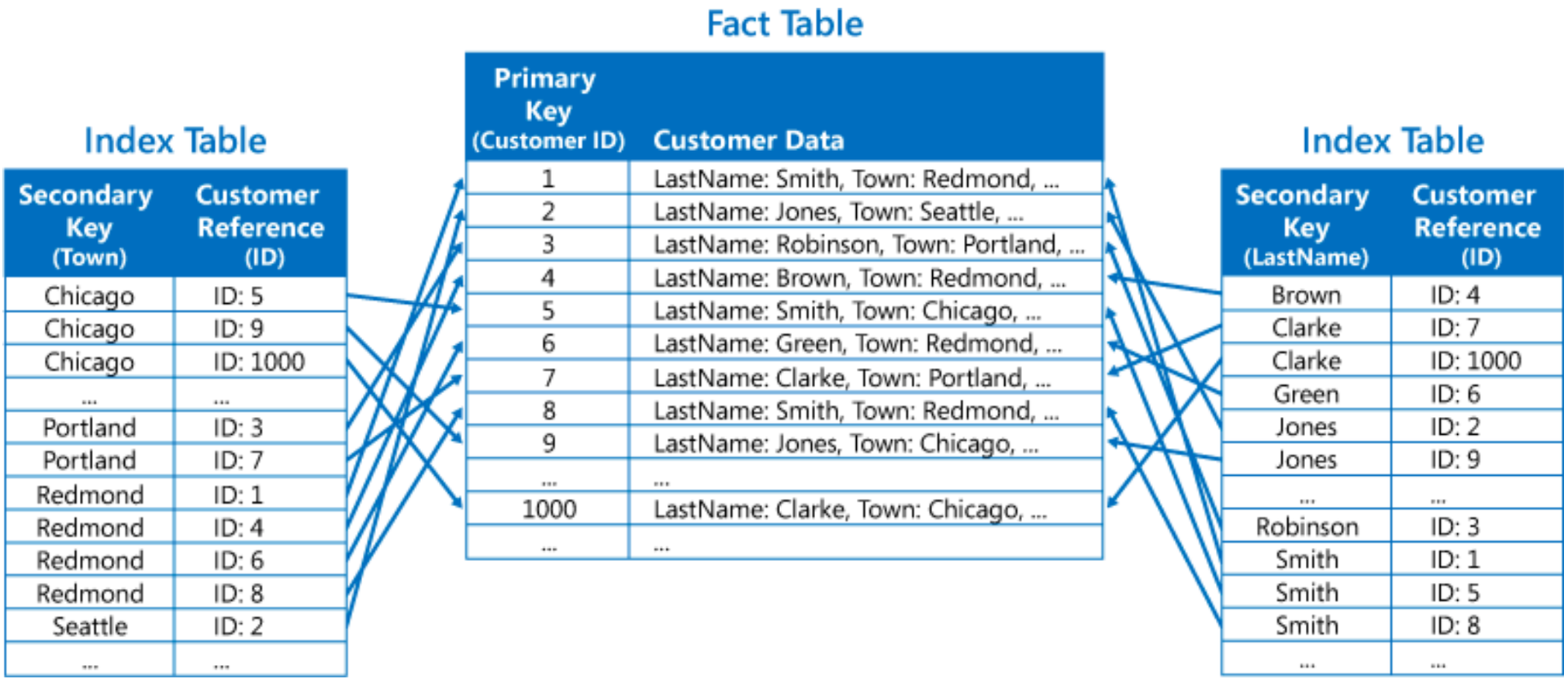
- Static data
- Amount of data is low

What to do when data is volatile or skewed?

Primary Key (Customer ID)	Customer Data
1	LastName: Smith, Town: Redmond, …
2	LastName: Jones, Town: Seattle, …
3	LastName: Robinson, Town: Portland, …
4	LastName: Brown, Town: Redmond, …
5	LastName: Smith, Town: Chicago, …
6	LastName: Green, Town: Redmond, …
7	LastName: Clarke, Town: Portland, …
8	LastName: Smith, Town: Redmond, …
9	LastName: Jones, Town: Chicago, …
…	…
1000	LastName: Clarke, Town: Chicago, …
…	…

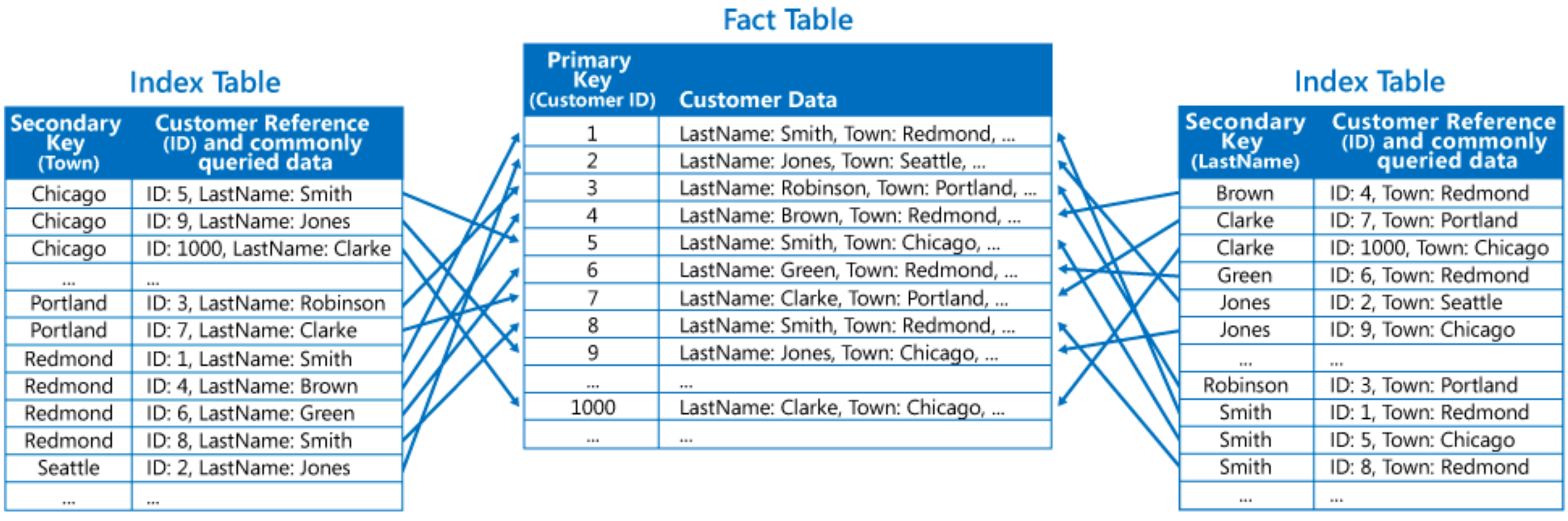
- Select by city ; Select by last name

Fact Table

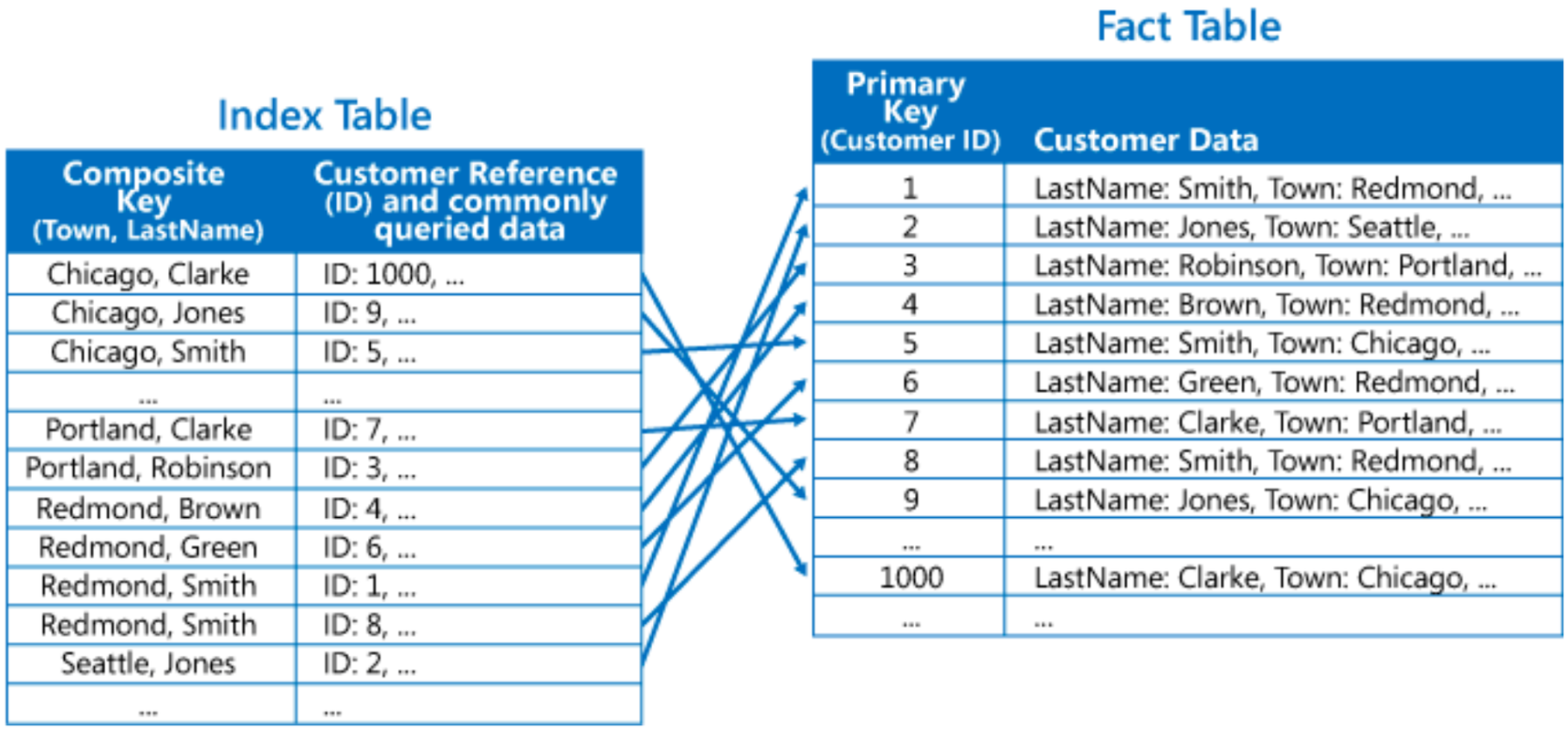


- Saves space
- Costly lookup join

Normalized index tables

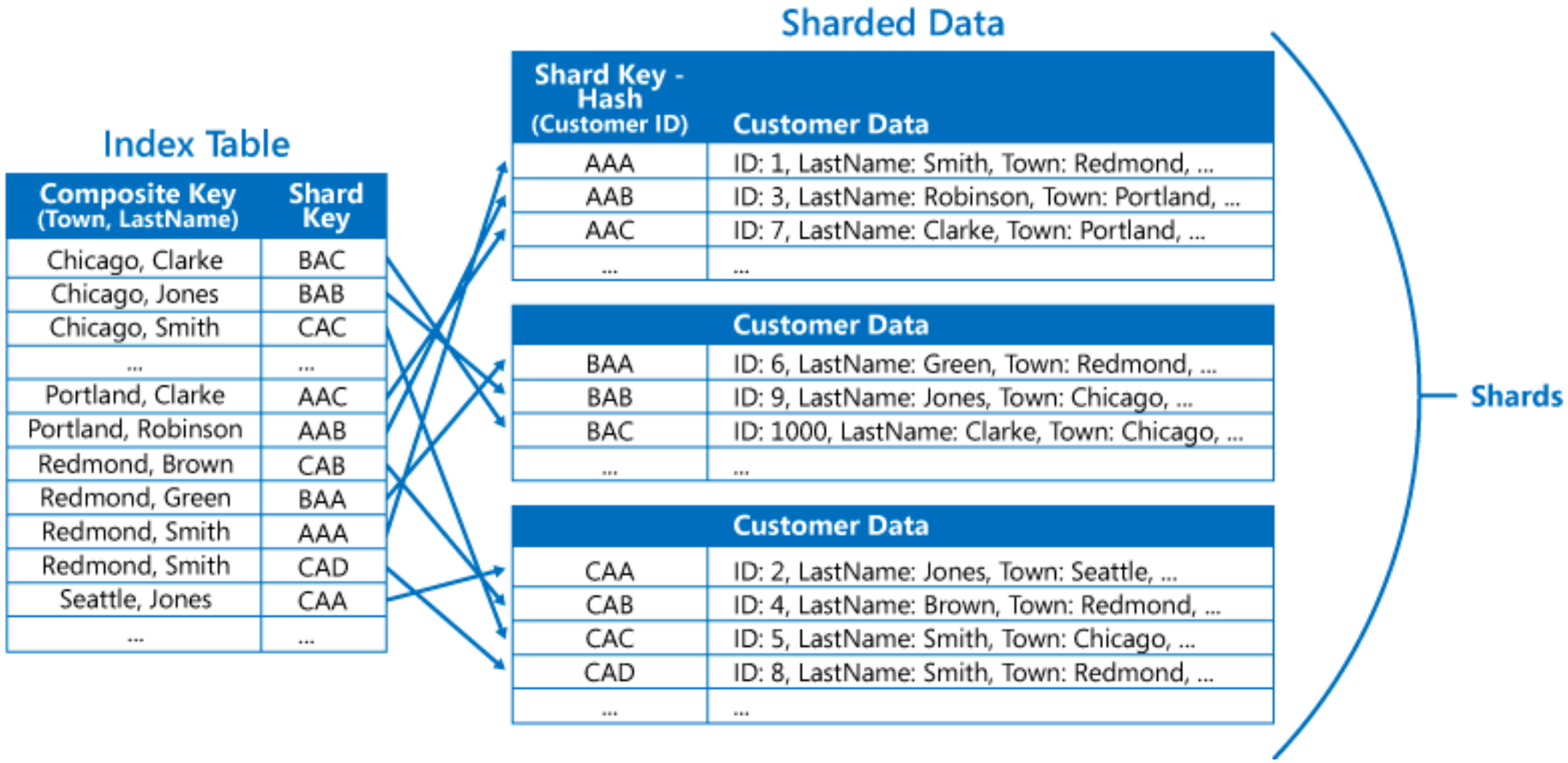


Select by City and Last Name



- How to make this faster?

Shard Key


Sharded Data
Index Table
Composite Key (Town, LastName)
Shard Key
Chicago, Clarke
BAC
Chicago, Jones
BAB
Chicago, Smith
CAC
...
...
Portland, Clarke
AAC
Portland, Robinson
AAB
Redmond, Brown
CAB
Redmond, Green
BAA
Redmond, Smith
AAA
Redmond, Smith
CAD
Seattle, Jones
CAA
...
...
Shard Key - Hash (Customer ID)
Customer Data
AAA
ID: 1, LastName: Smith, Town: Redmond, ...
AAB
ID: 3, LastName: Robinson, Town: Portland, ...
AAC
ID: 7, LastName: Clarke, Town: Portland, ...
...
...
Customer Data
BAA
ID: 6, LastName: Green, Town: Redmond, ...
BAB
ID: 9, LastName: Jones, Town: Chicago, ...
BAC
ID: 1000, LastName: Clarke, Town: Chicago, ...
...
...
Customer Data
CAA
ID: 2, LastName: Jones, Town: Seattle, ...
CAB
ID: 4, LastName: Brown, Town: Redmond, ...
CAC
ID: 5, LastName: Smith, Town: Chicago, ...
CAD
ID: 8, LastName: Smith, Town: Redmond, ...
...
...
Shards

New Relic ONE™

Quick find | Chart builder

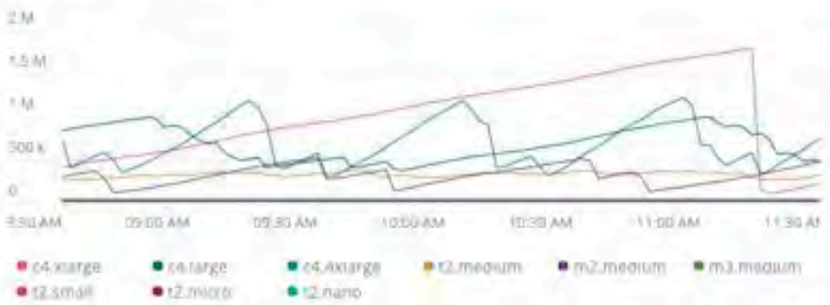
Dashboards / ☆ WAF - Reliability - Scaling & Availability

Default

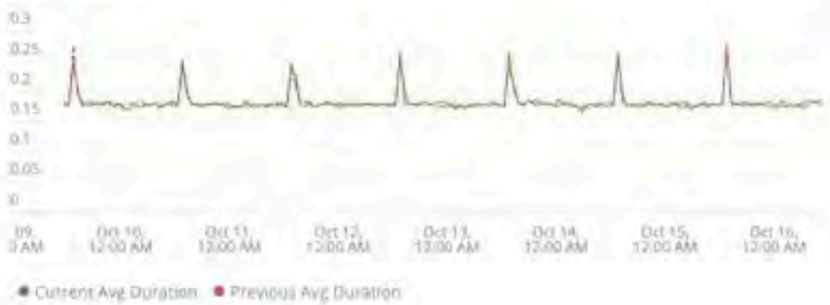
Search for any attribute or value

Instances per region
Since 1 hour ago

AWS Memory Footprint Utilization
Since 3 hours ago



Response Time
Since 1 week ago compared with 1 week earlier



Application Availability
Since 1 week ago

100 %

Availability %

Infrastructure Availability
Since 1 week ago

100 %

Availability %

Error Rate
Since 1 week ago compared with 1 week earlier

Auto Scaling group status
Since 1 hour ago until 10 minutes ago

Load by Host
Since 10 minutes ago

CONTAINERS (252)*

Other	34	13.49 %
ip-172-20-41-207	28	11.11 %
ip-172-20-58-240	28	11.11 %
ip-172-20-56-220	28	11.11 %
ip-172-20-46-35	28	11.11 %

* This pie chart uses uniqueCount, which may result in the facet sum exceeding 100%. Learn more in our documentation.

Throughput
Since 1 week ago compared with 1 week earlier

Design Resilient Architectures

Design Cost-Optimized Architectures

Sustainability Architectures

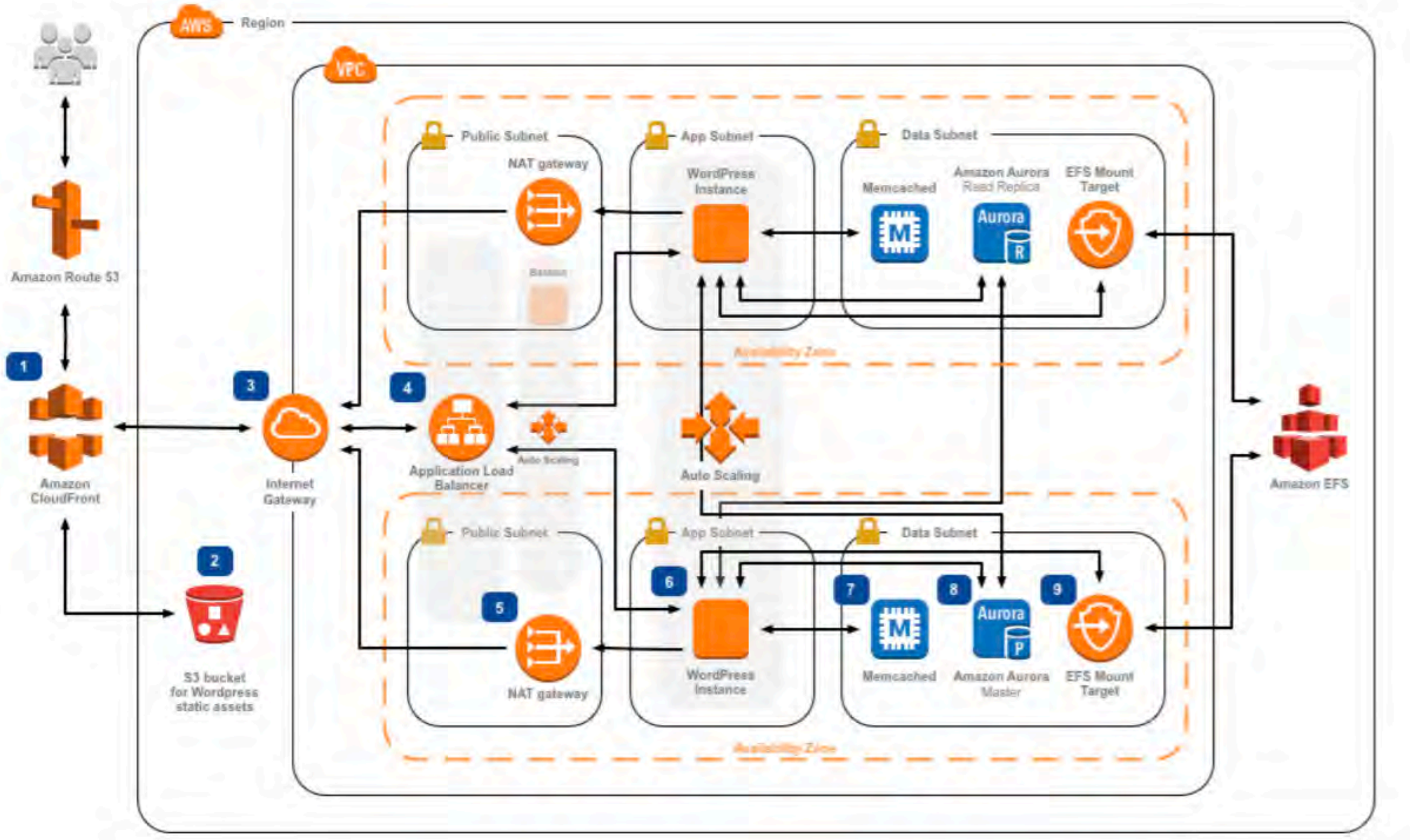
Design Performant Architectures

Operationally Excellent Architectures

Specify Secure Applications

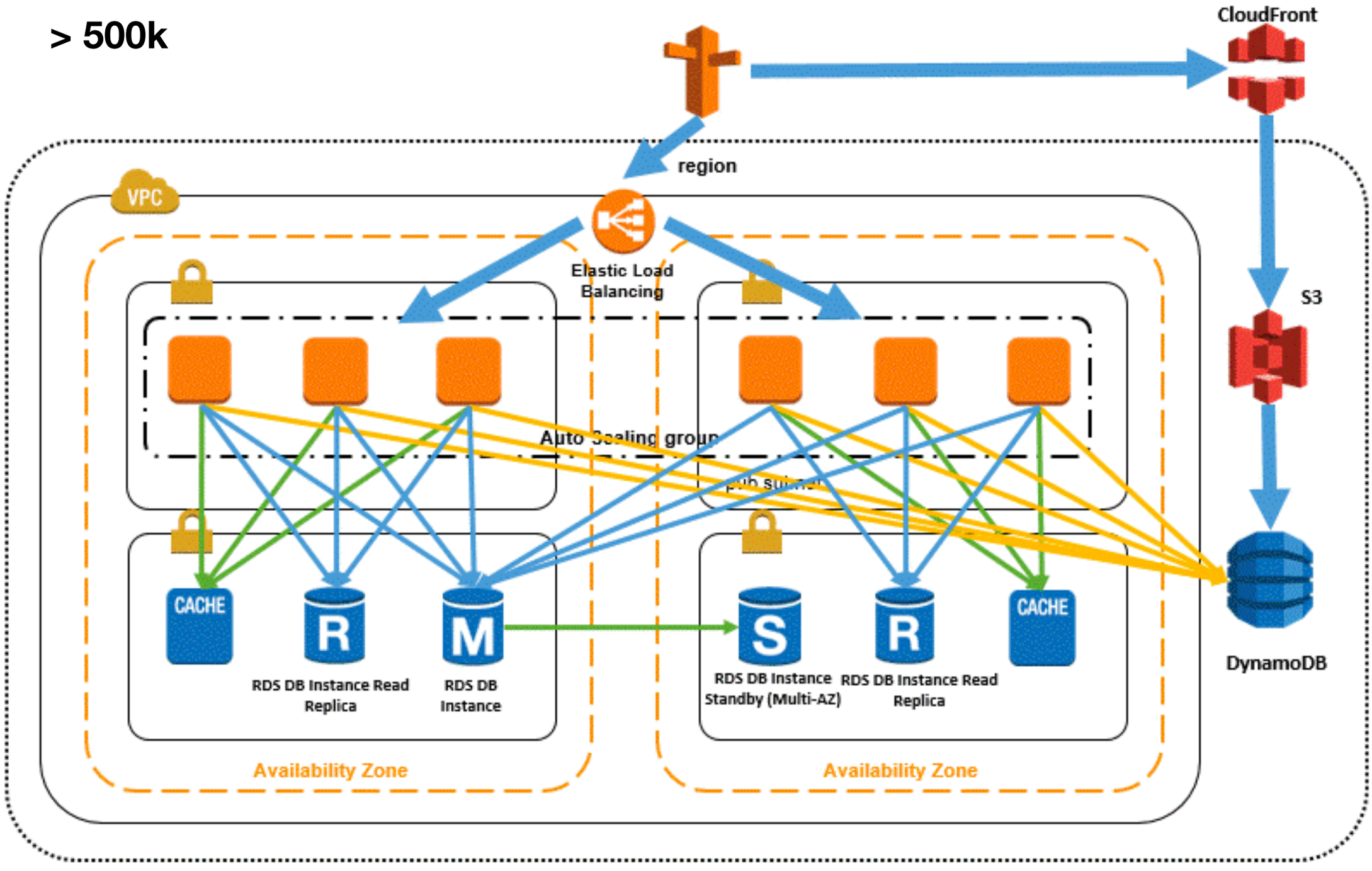
Well Architected Framework

AWS Best Practices

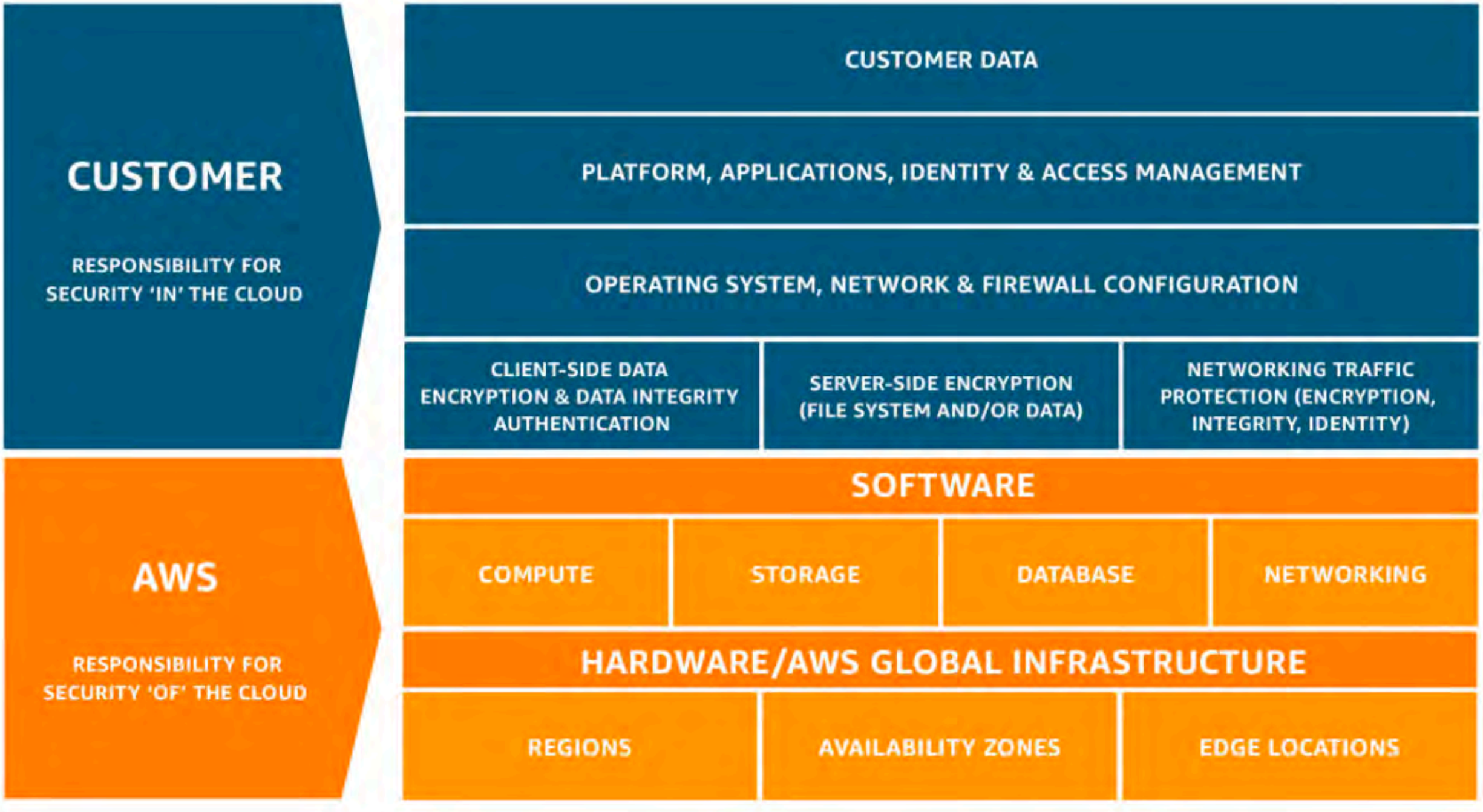


https://aws.amazon.com/blogs/architecture/wordpress-best-practices-on-aws/

> 500k


CloudFront
region
VPC
Elastic Load Balancing
S3
Auto Scaling group
CACHE
R
M
S
R
CACHE
RDS DB Instance Read Replica
RDS DB Instance
RDS DB Instance Standby (Multi-AZ)
RDS DB Instance Read Replica
DynamoDB
Availability Zone
Availability Zone

Security



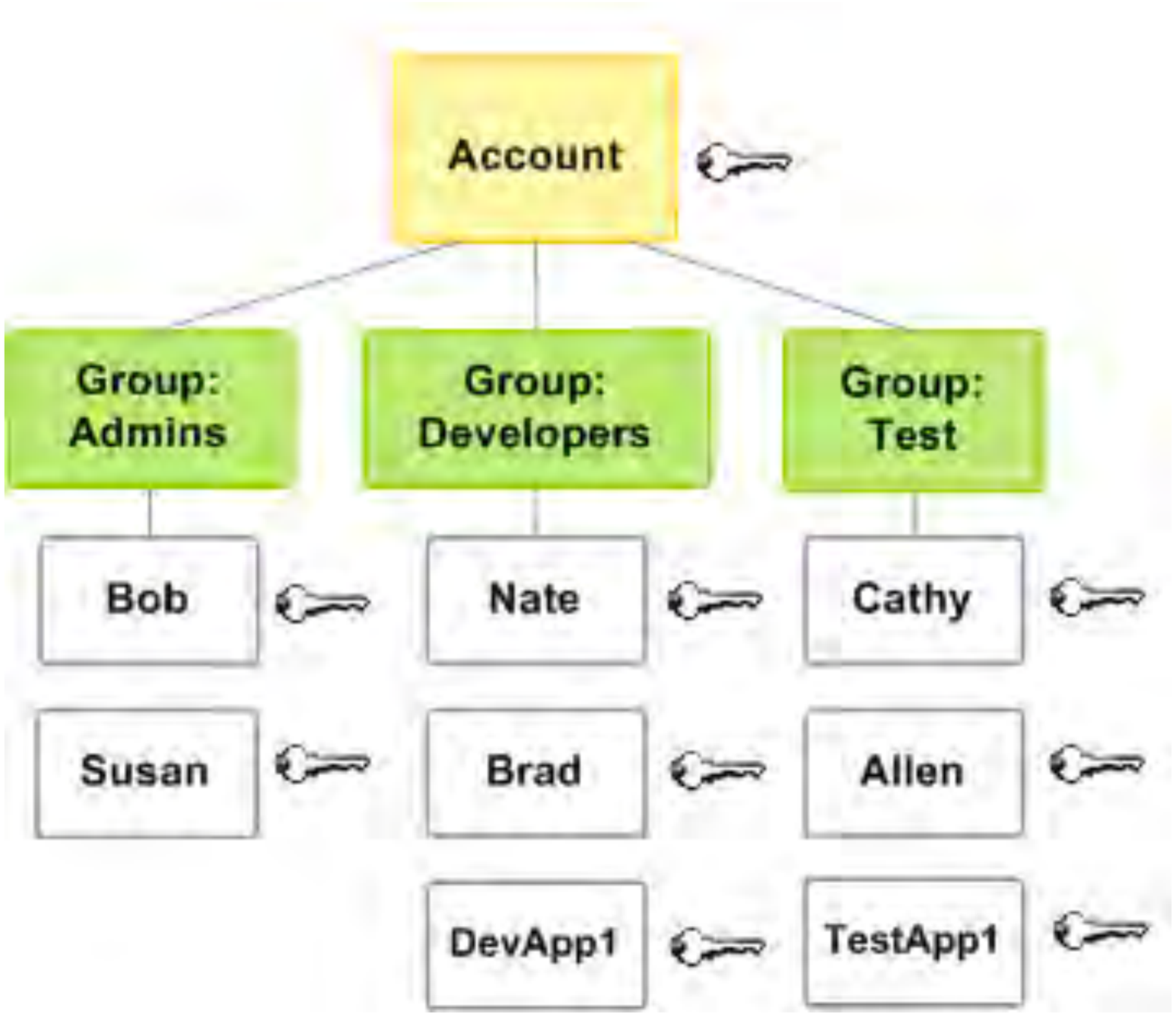
https://aws.amazon.com/compliance/shared-responsibility-model/

Principle of Least Privilege

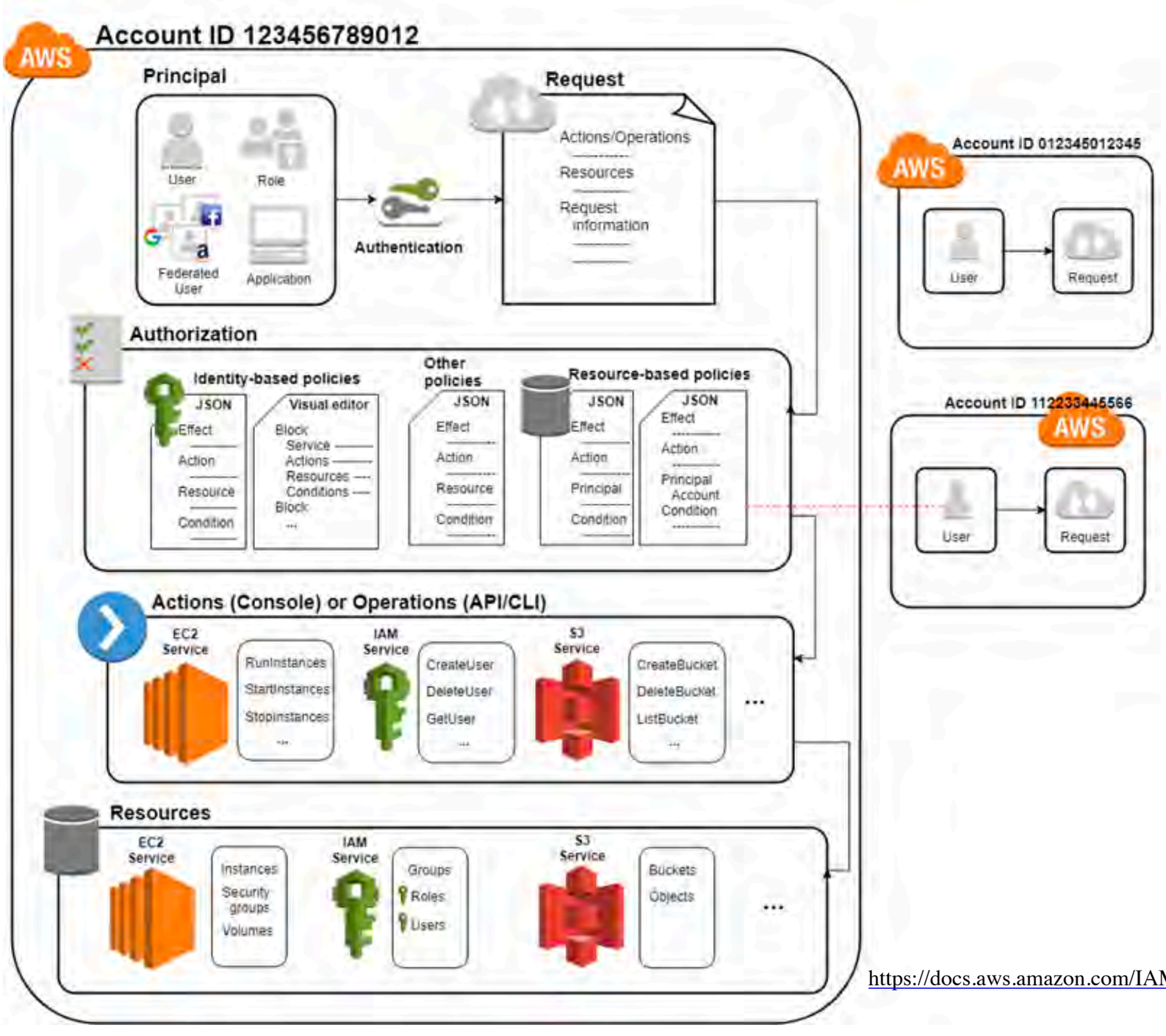
- Persons or processes can perform all activities they need to perform, and no more.

How do you manage identities for people and machines?

Identity Access


Account
Group: Admins
Group: Developers
Group: Test
Bob
Susan
Nate
Brad
DevApp1
Cathy
Allen
TestApp1

AWS Identity and Access Management (IAM)



https://docs.aws.amazon.com/IAM/latest/UserGuide/intro-structure.html

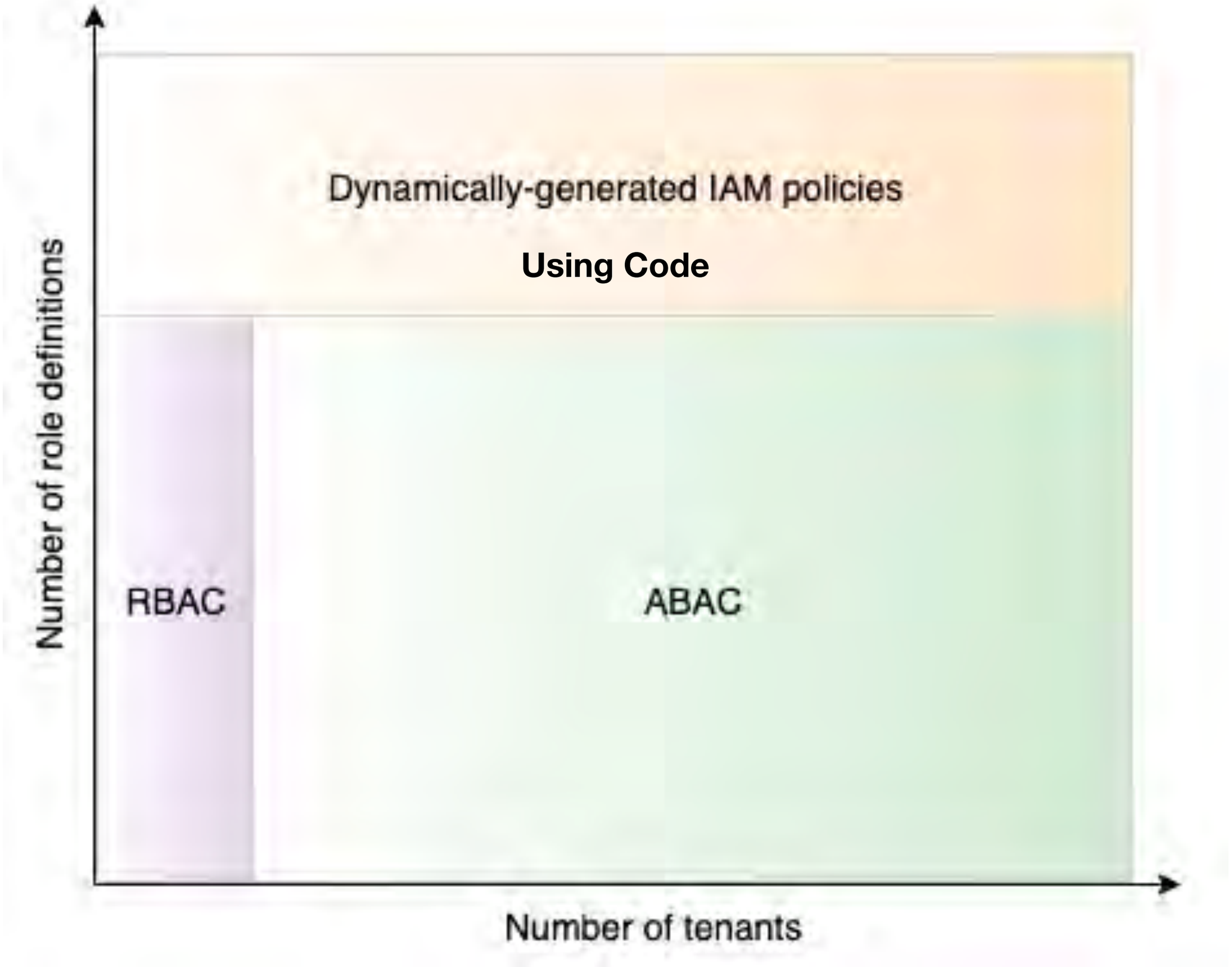
Access

- Identity Access
- Role Based Access
- Attribute Based Access

Tagging Best Practices

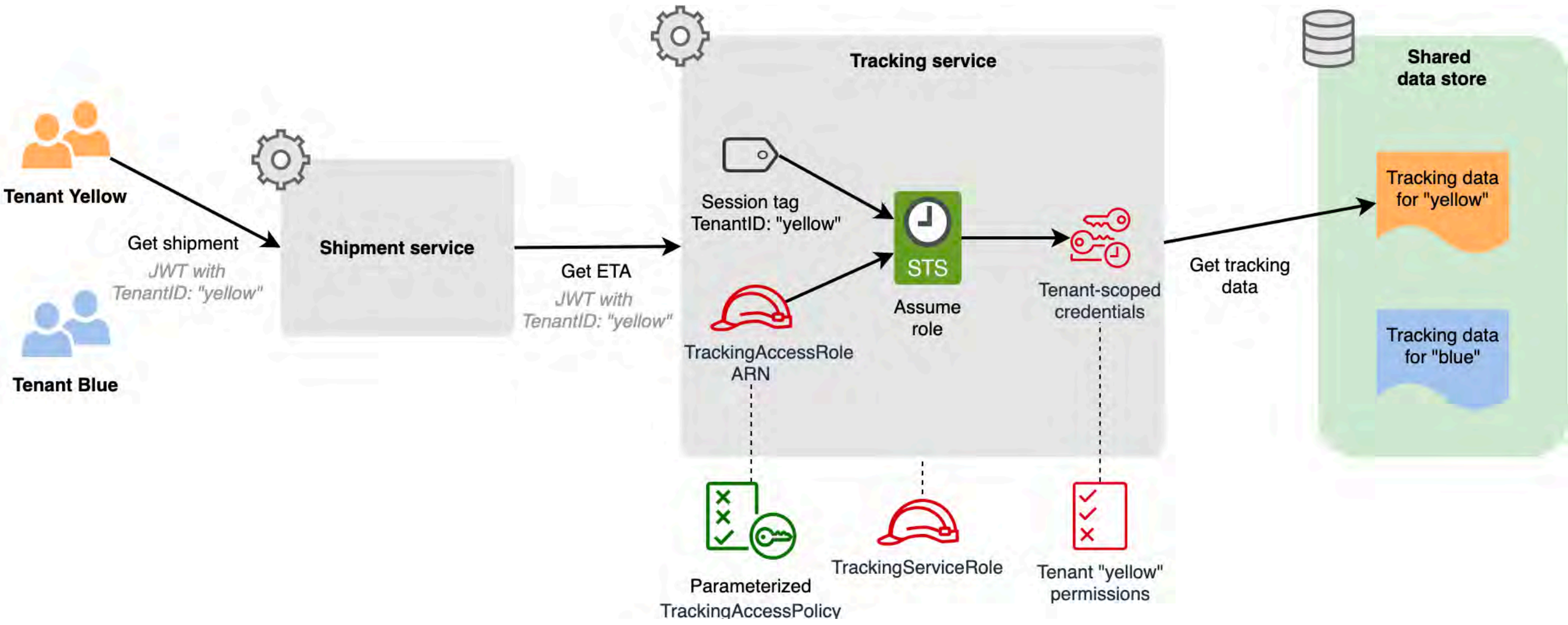
Technical Tags	Tags for Automation	Business Tags	Security Tags
• **Name** – Identify individual resources • **Application ID** – Identify resources that are related to a specific application • **Application Role** – Describe the function of a particular resource (such as web server, message broker, database)	• **Date/Time** – Identify the date or time a resource should be started, stopped, deleted, or rotated • **Opt in/Opt out** – Indicate whether a resource should be included in an automated activity such as starting, stopping, or resizing instances • **Security** – Determine requirements, such as encryption or enabling of Amazon VPC flow logs; identify route	• **Project** – Identify projects that the resource supports • **Owner** – Identify who is responsible for the resource • **Cost Center/Business Unit** – Identify the cost center or business unit associated with a resource, typically for cost allocation and tracking • **Customer** – Identify a specific client that a particular group of	• **Confidentiality** – An identifier for the specific data confidentiality level a resource supports • **Compliance** – An identifier for workloads that must adhere to specific compliance requirements

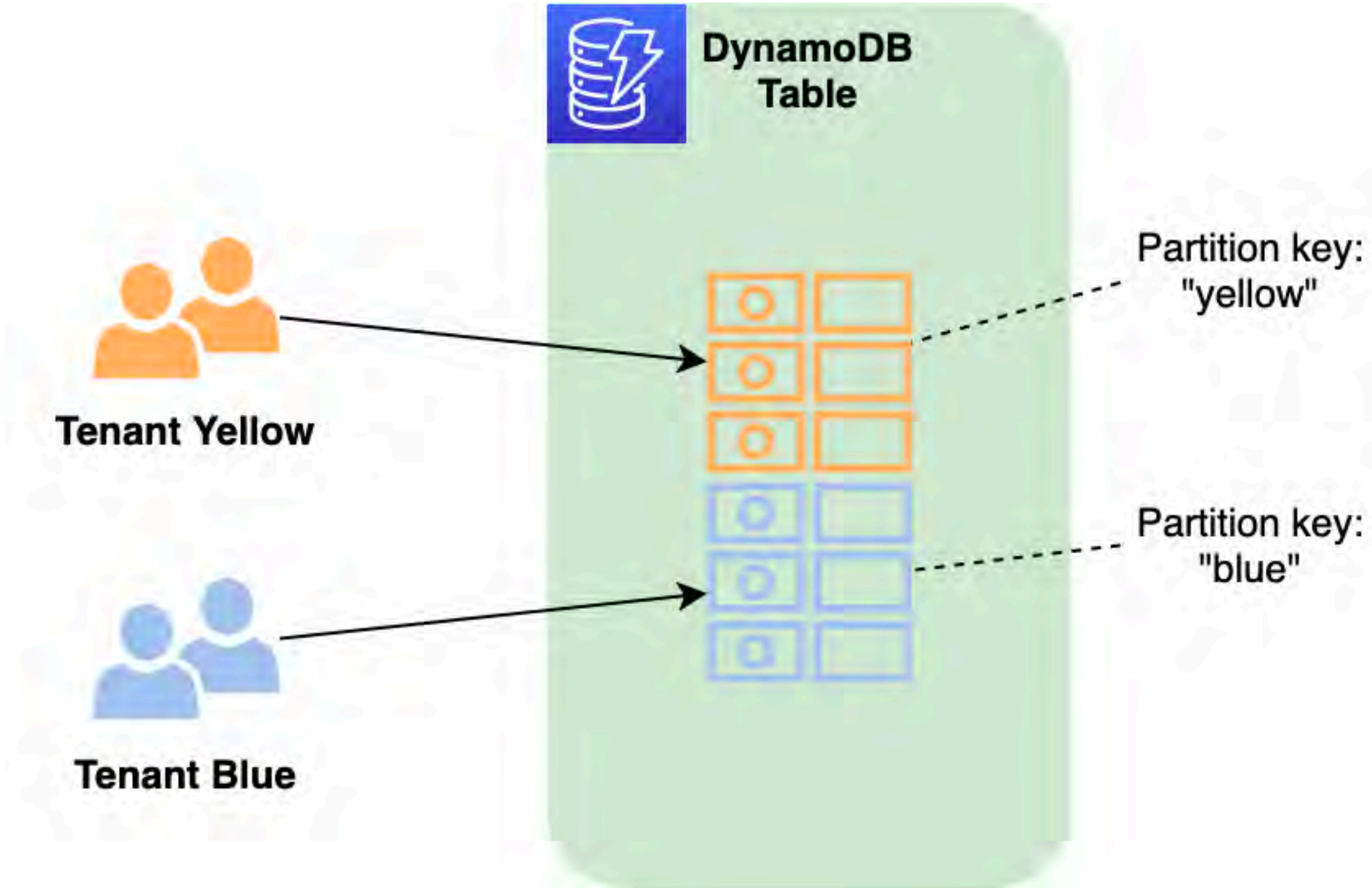
https://docs.aws.amazon.com/general/latest/gr/aws_tagging.html

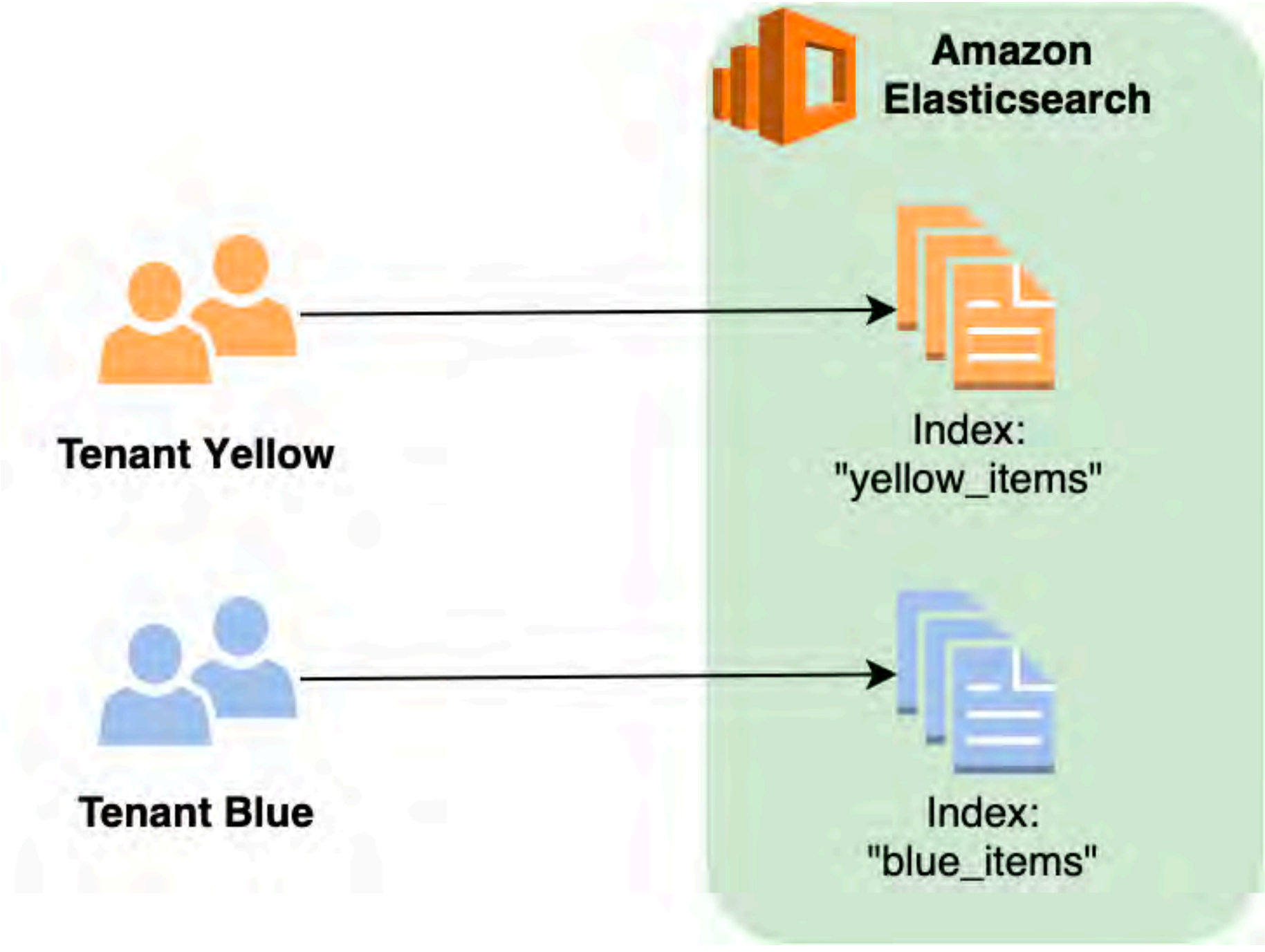


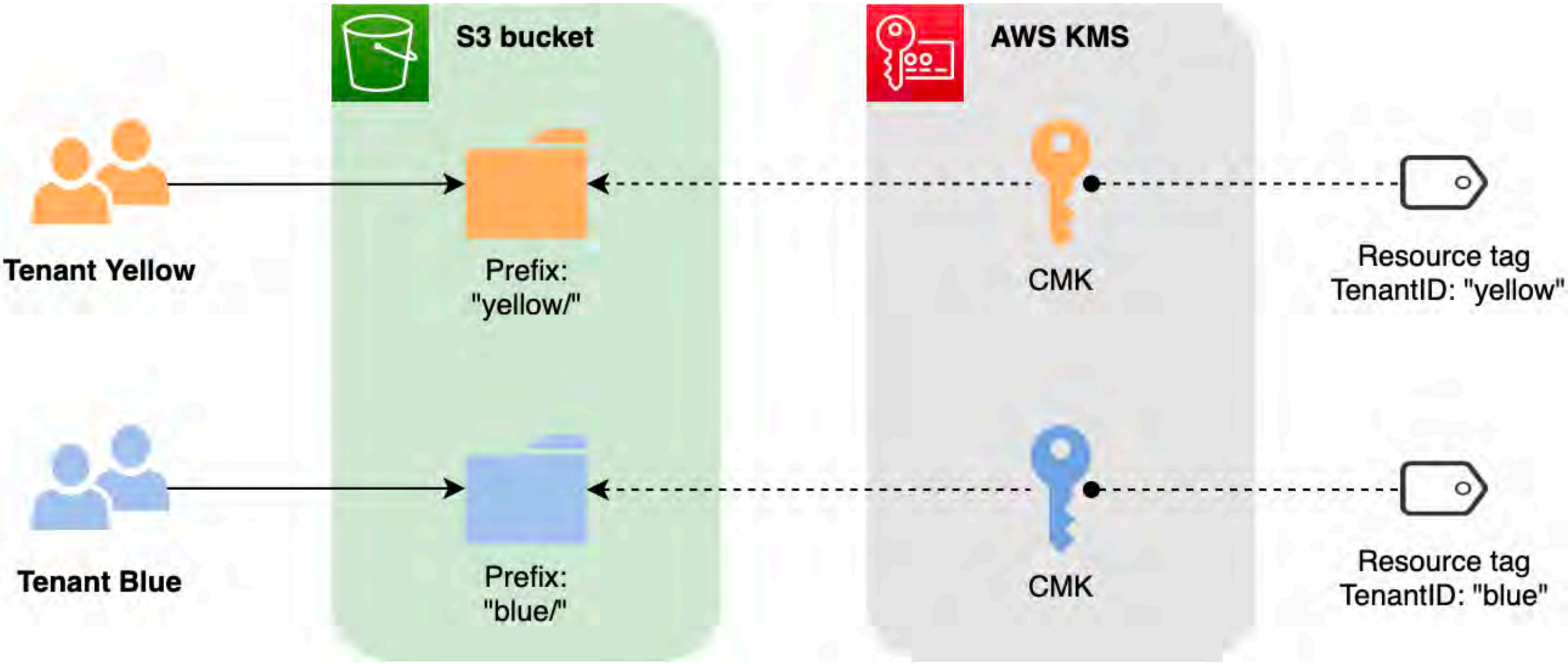
https://aws.amazon.com/blogs/security/how-to-implement-saas-tenant-isolation-with-abac-and-aws-iam/

How to implement SaaS tenant isolation with ABAC and AWS IAM?


Tenant Yellow
Tenant Blue
Get shipment
JWT with
TenantID: "yellow"
Shipment service
Get ETA
JWT with
TenantID: "yellow"
Tracking service
Session tag
TenantID: "yellow"
STS
Assume
role
TrackingAccessRole
ARN
Tenant-scoped
credentials
Get tracking
data
Shared
data store
Tracking data
for "yellow"
Tracking data
for "blue"
Parameterized
TrackingAccessPolicy
TrackingServiceRole
Tenant "yellow"
permissions


DynamoDB
Table
Partition key:
"yellow"
Tenant Yellow
Partition key:
"blue"
Tenant Blue


Amazon
Elasticsearch
Tenant Yellow
Index:
"yellow_items"
Tenant Blue
Index:
"blue_items"


S3 bucket
AWS KMS
Tenant Yellow
Prefix:
"yellow/"
CMK
Resource tag
TenantID: "yellow"
Tenant Blue
Prefix:
"blue/"
CMK
Resource tag
TenantID: "blue"


VPC
Availability Zone A
Availability Zone B
Availability Zone C
VPC
10.0.0.0/16
AWS
Region

https://cidr.xyz/

CIDR.xyz

AN INTERACTIVE IP ADDRESS AND CIDR RANGE VISUALIZER

CIDR is a notation for describing blocks of IP addresses and is used heavily in various networking configurations. IP addresses contain 4 octets, each consisting of 8 bits giving values between 0 a
decimal value that comes after the slash is the number of bits consisting of the routing prefix. This in turn can be translated into a netmask, and also designates how many available addresses ar

10 . 88 . 135 . 144 / 28

0	0	0	0	1	0	1	0	0	1	0	1	1	0	0	0	1	0	0	0	0	1	1	1	1	0	0	1				

255.255.255.240	10.88.135.145	10.88.135.158	16
NETMASK	FIRST USABLE IP	LAST USABLE IP	COUNT

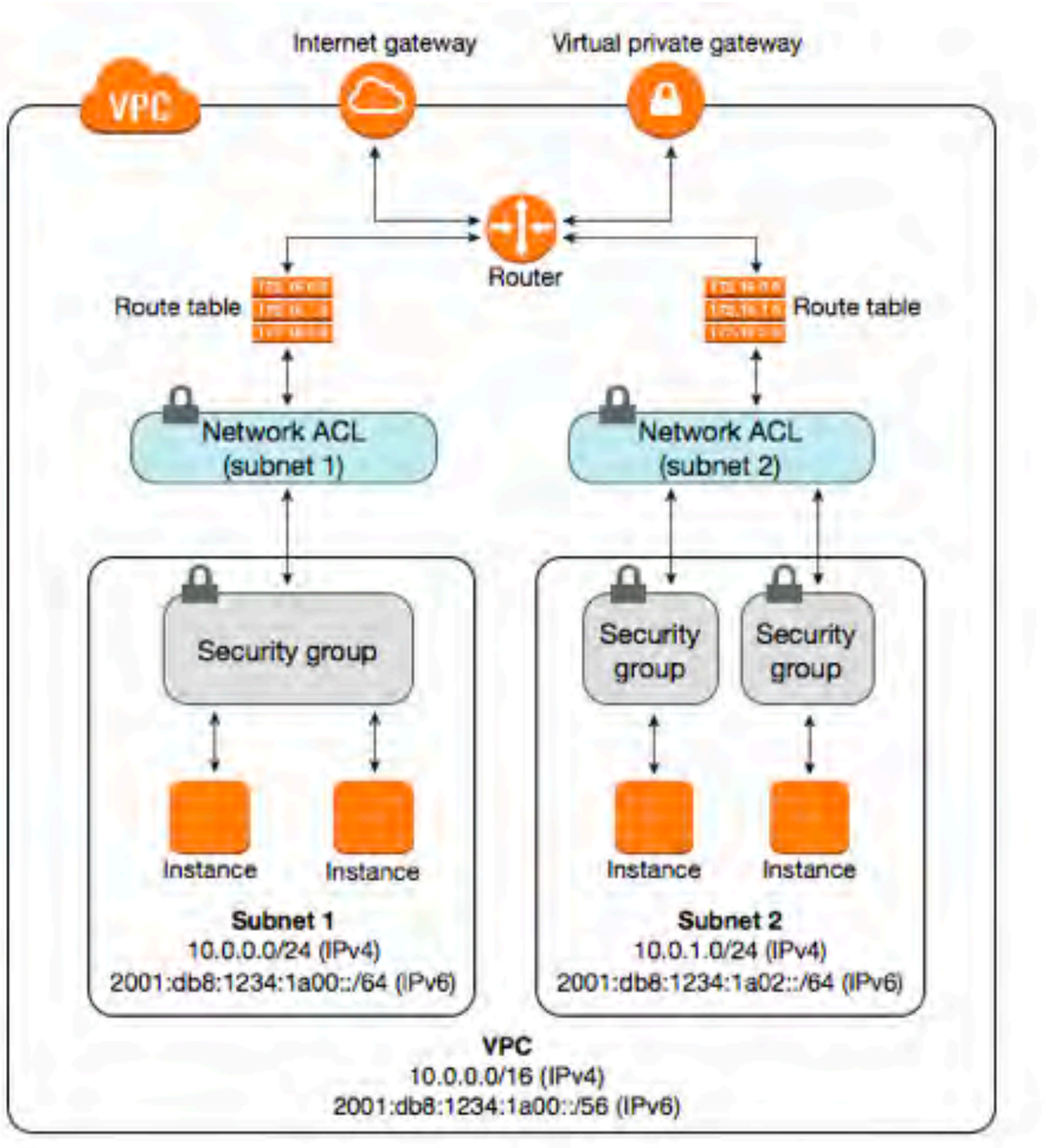
* For routing mask values <= 30, first and last IPs are base and broadcast addresses and are unusable.

Created by Yuval Adam. Source available on Github.

Classless inter domain routing

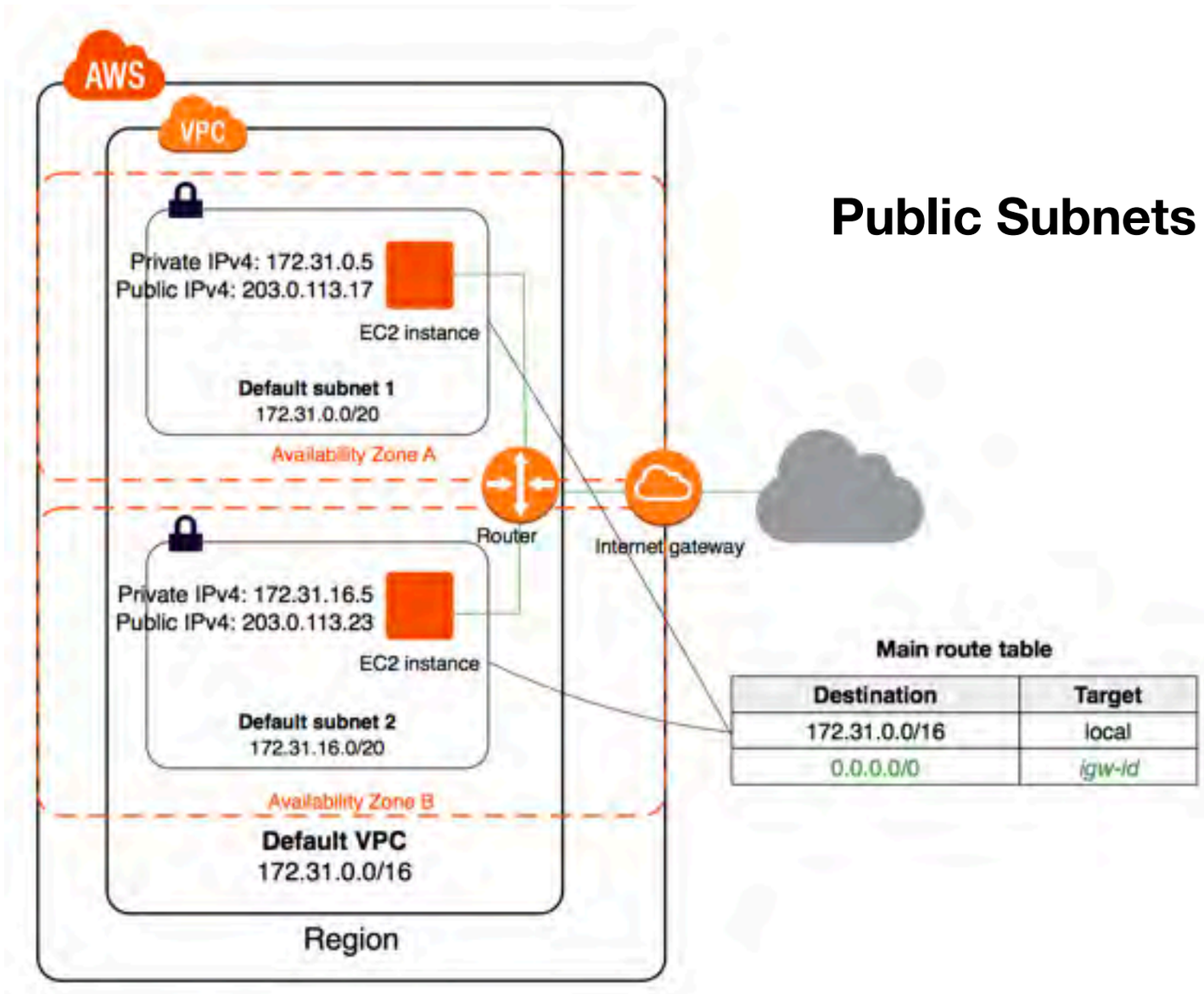
CIDR	Subnet mask (decimal)	Subnet mask (binary)	Available addresses	
/0	0.0.0.0	00000000.00000000.00000000.00000000	4.294.967.296	2^{32}
/1	128.0.0.0	10000000.00000000.00000000.00000000	2.147.483.648	2^{31}
/2	192.0.0.0	11000000.00000000.00000000.00000000	1.073.741.824	2^{30}
/3	224.0.0.0	11100000.00000000.00000000.00000000	536.870.912	2^{29}
/4	240.0.0.0	11110000.00000000.00000000.00000000	268.435.456	2^{28}
/5	248.0.0.0	11111000.00000000.00000000.00000000	134.217.728	2^{27}
/6	252.0.0.0	11111100.00000000.00000000.00000000	67.108.864	2^{26}
/7	254.0.0.0	11111110.00000000.00000000.00000000	33.554.432	2^{25}
/8	255.0.0.0	11111111.00000000.00000000.00000000	16.777.216	2^{24}
/9	255.128.0.0	11111111.10000000.00000000.00000000	8.388.608	2^{23}
/10	255.192.0.0	11111111.11000000.00000000.00000000	4.194.304	2^{22}
/11	255.224.0.0	11111111.11100000.00000000.00000000	2.097.152	2^{21}
/12	255.240.0.0	11111111.11110000.00000000.00000000	1.048.576	2^{20}
/13	255.248.0.0	11111111.11111000.00000000.00000000	524.288	2^{19}
/14	255.252.0.0	11111111.11111100.00000000.00000000	262.144	2^{18}
/15	255.254.0.0	11111111.11111110.00000000.00000000	131.072	2^{17}
/16	255.255.0.0	11111111.11111111.00000000.00000000	65.536	2^{16}
/17	255.255.128.0	11111111.11111111.10000000.00000000	32.768	2^{15}
/18	255.255.192.0	11111111.11111111.11000000.00000000	16.384	2^{14}
/19	255.255.224.0	11111111.11111111.11100000.00000000	8.192	2^{13}
/20	255.255.240.0	11111111.11111111.11110000.00000000	4.096	2^{12}
/21	255.255.248.0	11111111.11111111.11111000.00000000	2.048	2^{11}
/22	255.255.252.0	11111111.11111111.11111100.00000000	1.024	2^{10}
/23	255.255.254.0	11111111.11111111.11111110.00000000	512	2^{9}
/24	255.255.255.0	11111111.11111111.11111111.00000000	256	2^{8}
/25	255.255.255.128	11111111.11111111.11111111.10000000	128	2^{7}
/26	255.255.255.192	11111111.11111111.11111111.11000000	64	2^{6}
/27	255.255.255.224	11111111.11111111.11111111.11100000	32	2^{5}
/28	255.255.255.240	11111111.11111111.11111111.11110000	16	2^{4}
/29	255.255.255.248	11111111.11111111.11111111.11111000	8	2^{3}
/30	255.255.255.252	11111111.11111111.11111111.11111100	4	2^{2}
/31	255.255.255.254	11111111.11111111.11111111.11111110	2	2^{1}
/32	255.255.255.255	11111111.11111111.11111111.11111111	1	2^{0}

VPC



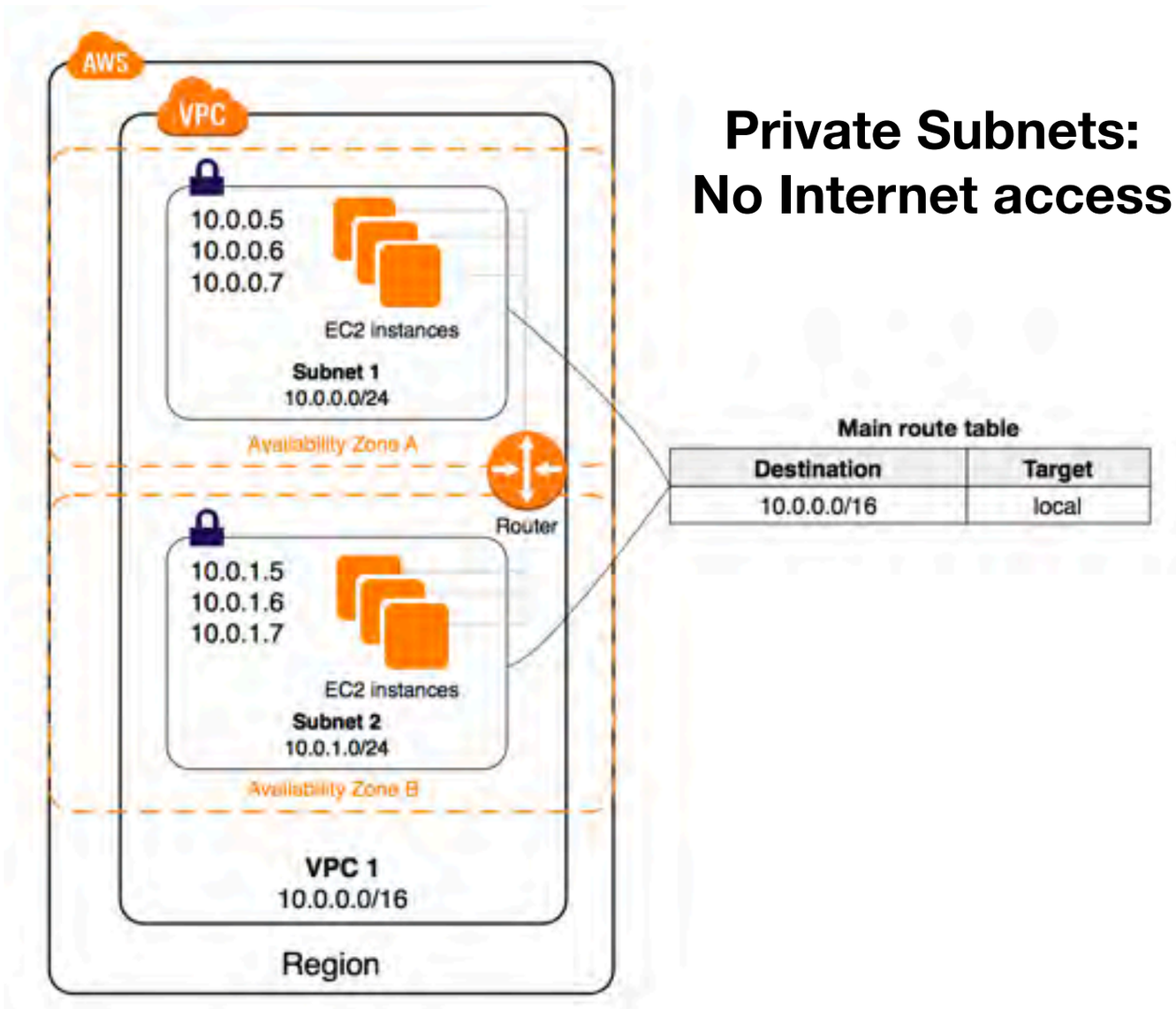
https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Security.html

Internet Gateway: Accessing internet



https://docs.aws.amazon.com/vpc/latest/userguide/how-it-works.html

Default Settings



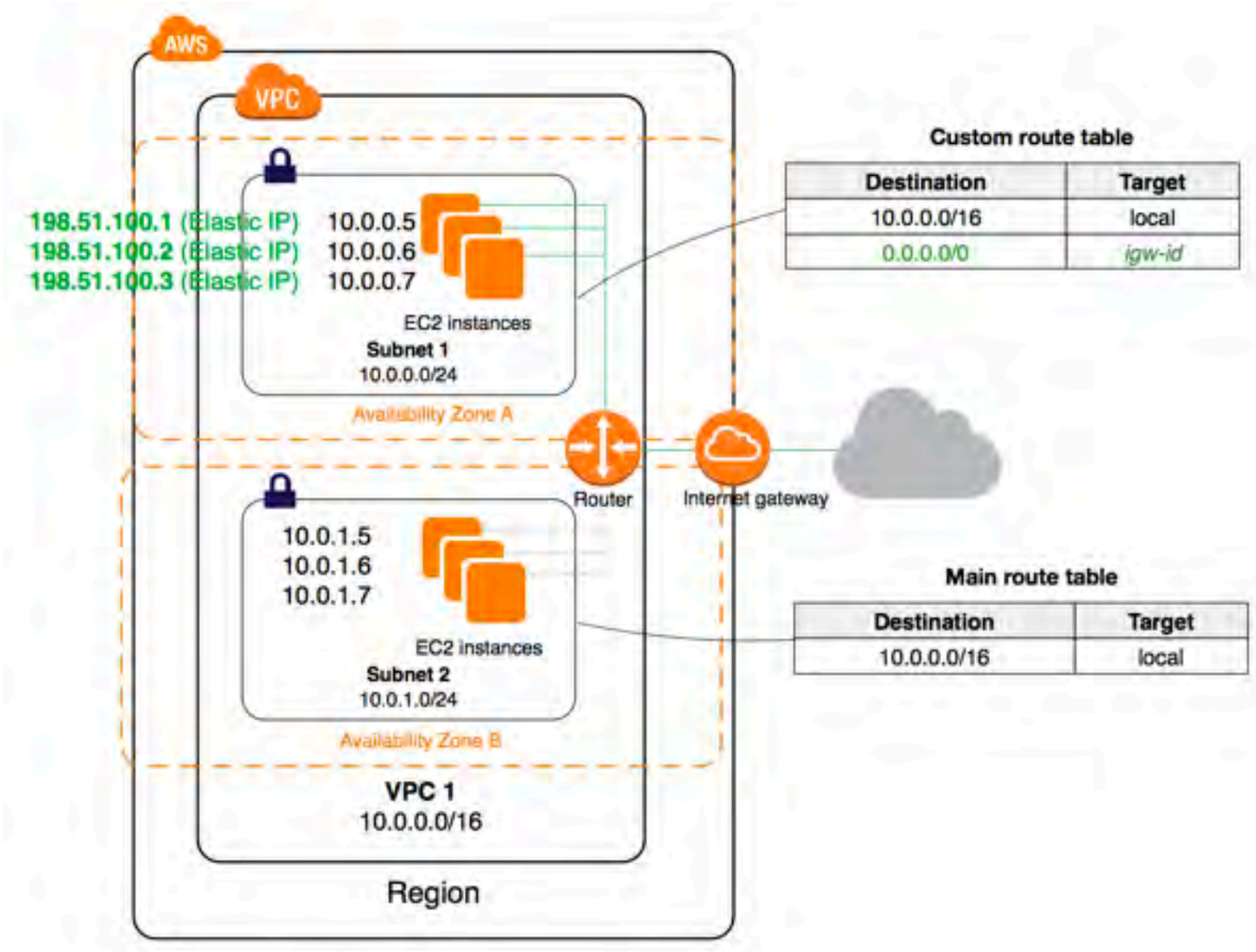
Private Subnets:
No Internet access

Main route table

Destination	Target
10.0.0.0/16	local

Allowing subnet 1 to access internet

Web Servers



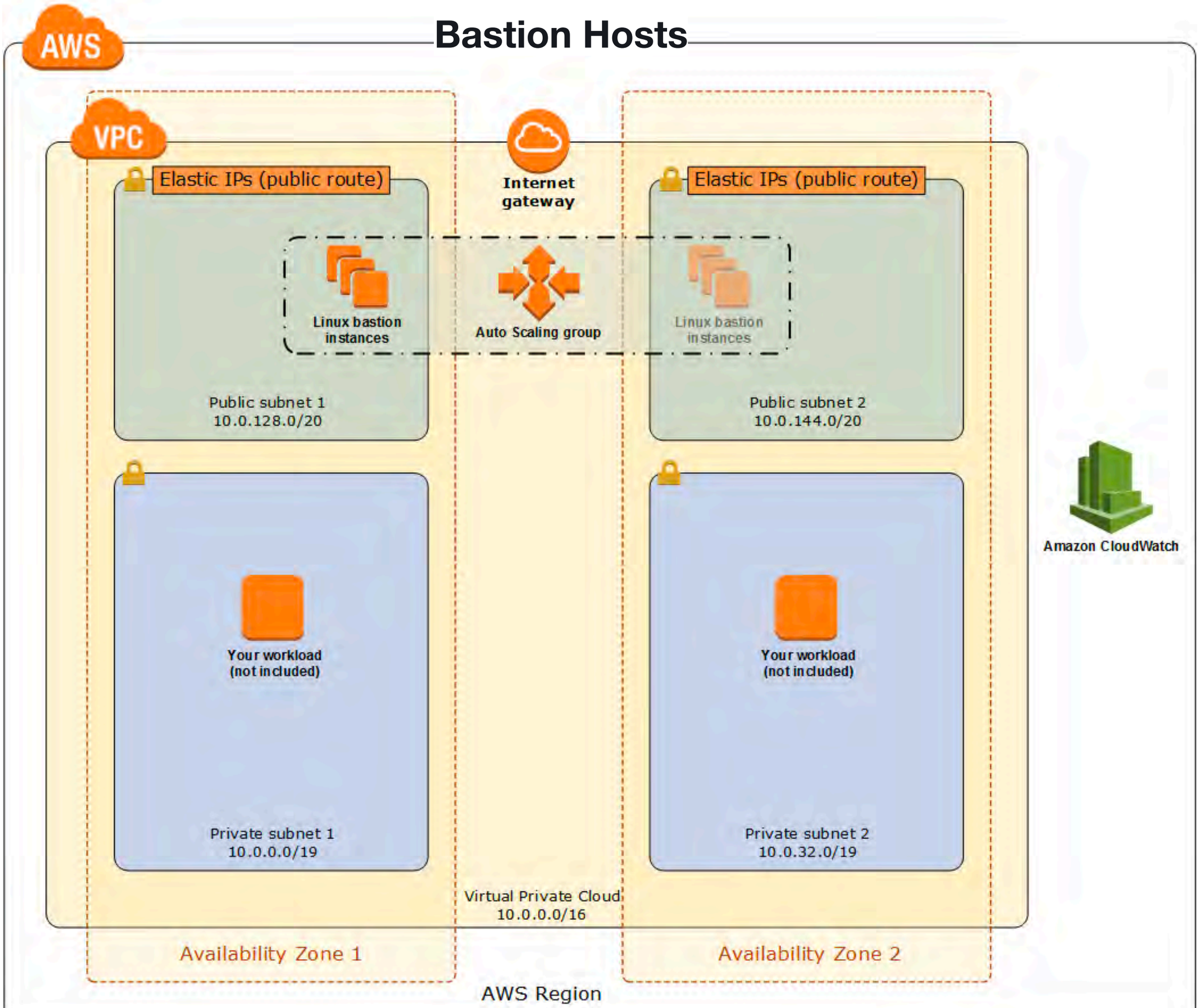
Public Subnet

DB Servers

Private Subnet

Enforce non-overlapping private IP address ranges in all private address spaces where they are connected

Bastion Hosts



Question

- What is the most secure option to connect to instances without Internet connectivity in private subnet VPC?

1. Configure IAM policy to restrict access to the instances

2. Using a bastion host server to connect to the instances

3. Enable internet connectivity and configure security group to connect to the instances

4. Enable internet connectivity and configure NACL and security group to connect to the instances

Answer

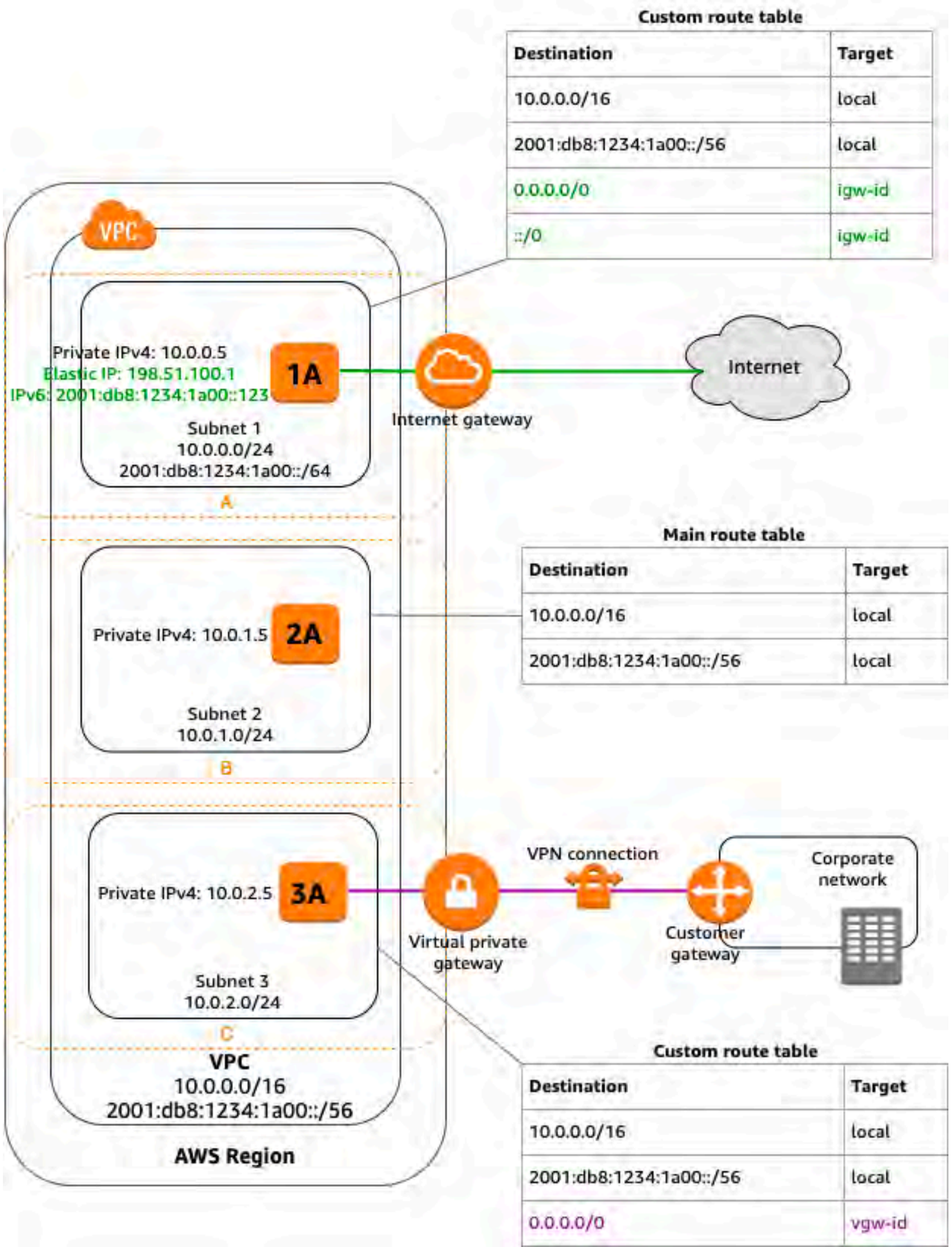
- What is the most secure option to connect to instances without Internet connectivity in private subnet VPC?

1. Configure IAM policy to restrict access to the instances

2. **Using a bastion host server to connect to the instances**

3. Enable internet connectivity and configure security group to connect to the instances

4. Enable internet connectivity and configure NACL and security group to connect to the instances


Custom route table
Destination
Target
10.0.0.0/16
local
2001:db8:1234:1a00::/56
local
0.0.0.0/0
igw-id
::/0
igw-id
VPC
Private IPv4: 10.0.0.5
Elastic IP: 198.51.100.1
IPv6: 2001:db8:1234:1a00::123
1A
Subnet 1
10.0.0.0/24
2001:db8:1234:1a00::/64
A
Internet gateway
Internet
Main route table
Destination
Target
10.0.0.0/16
local
2001:db8:1234:1a00::/56
local
Private IPv4: 10.0.1.5
2A
Subnet 2
10.0.1.0/24
B
Private IPv4: 10.0.2.5
3A
Subnet 3
10.0.2.0/24
C
VPC
10.0.0.0/16
2001:db8:1234:1a00::/56
AWS Region
VPN connection
Virtual private gateway
Customer gateway
Corporate network
Custom route table
Destination
Target
10.0.0.0/16
local
2001:db8:1234:1a00::/56
local
0.0.0.0/0
vgw-id

Virtual Private Cloud

- Organization: Subnets
- Security: Security groups/Access Control Lists
- Network isolation: Internet Gateways/virtual private gateways/NAT gateways
- Traffic direction: Routes

Security Group vs Network ACL

Security group	Network ACL
Operates at the instance level	Operates at the subnet level
Supports allow rules only	Supports allow rules and deny rules
Is stateful: Return traffic is automatically allowed, regardless of any rules	Is stateless: Return traffic must be explicitly allowed by rules
We evaluate all rules before deciding whether to allow traffic	We process rules in order, starting with the lowest numbered rule, when deciding whether to allow traffic
Applies to an instance only if someone specifies the security group when launching the instance, or associates the security group with the instance later on	Automatically applies to all instances in the subnets that it's associated with (therefore, it provides an additional layer of defense if the security group rules are too permissive)

Question

- You are setting up a VPC and you need to set up a public subnet within that VPC. What following requirement must be met for this subnet to be considered a public subnet?

1. Subnet's traffic is not routed to an Internet gateway but has its traffic routed to a virtual private gateway.

2. None of these answers can be considered a public subnet

3. Subnet's traffic is not routed to an Internet gateway

4. Subnet's traffic is routed to an Internet gateway

Answer

- You are setting up a VPC and you need to set up a public subnet within that VPC. What following requirement must be met for this subnet to be considered a public subnet?

1. Subnet's traffic is not routed to an Internet gateway but has its traffic routed to a virtual private gateway.

2. None of these answers can be considered a public subnet

3. Subnet's traffic is not routed to an Internet gateway

4. **Subnet's traffic is routed to an Internet gateway**

Question

- You can use _____ and _____ to help secure the instances in your VPC.

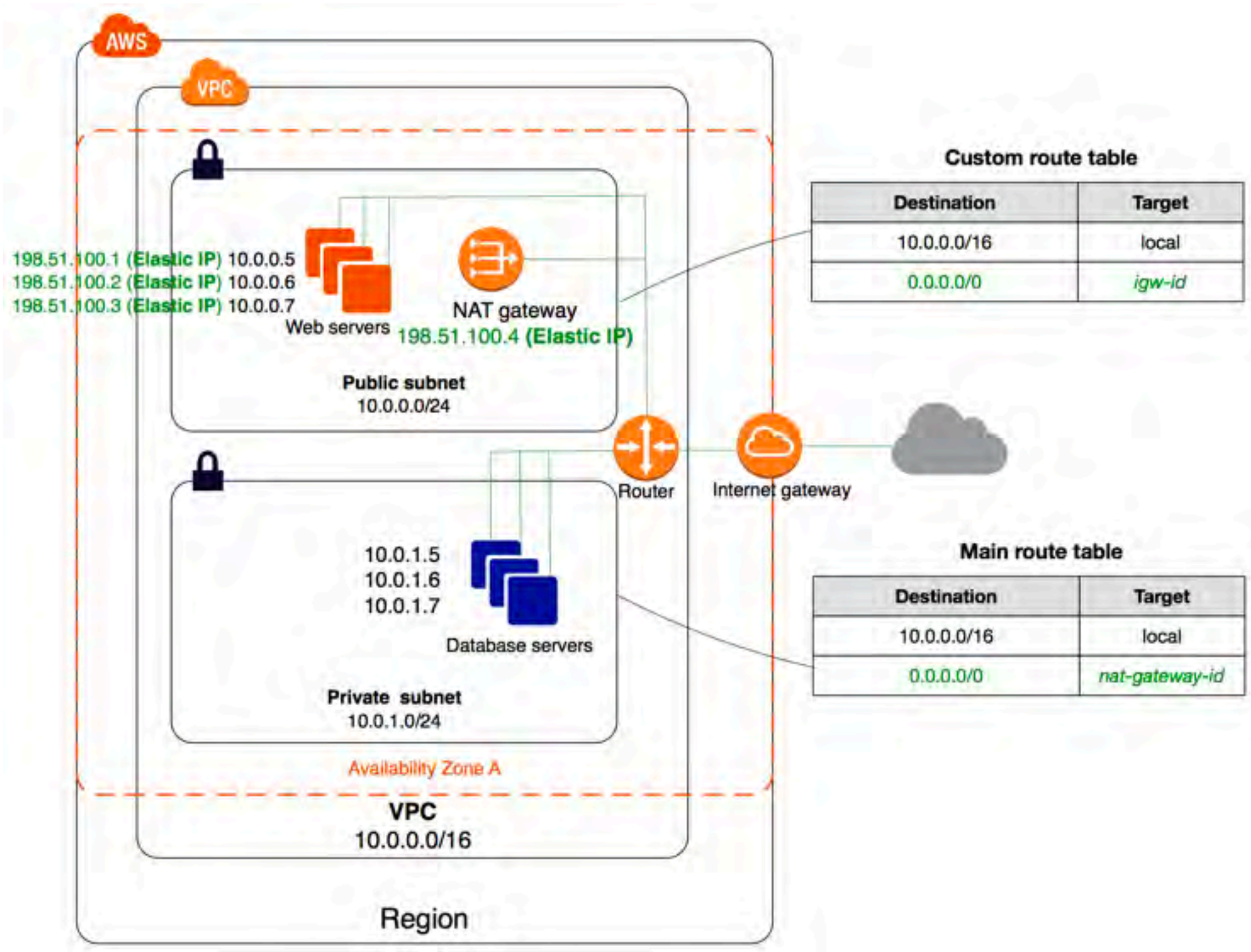
1. Security groups and 2-factor authentication
2. Security groups and biometric authentication
3. Security groups and network ACLs
4. Security groups and multi-factor authentication

Answer

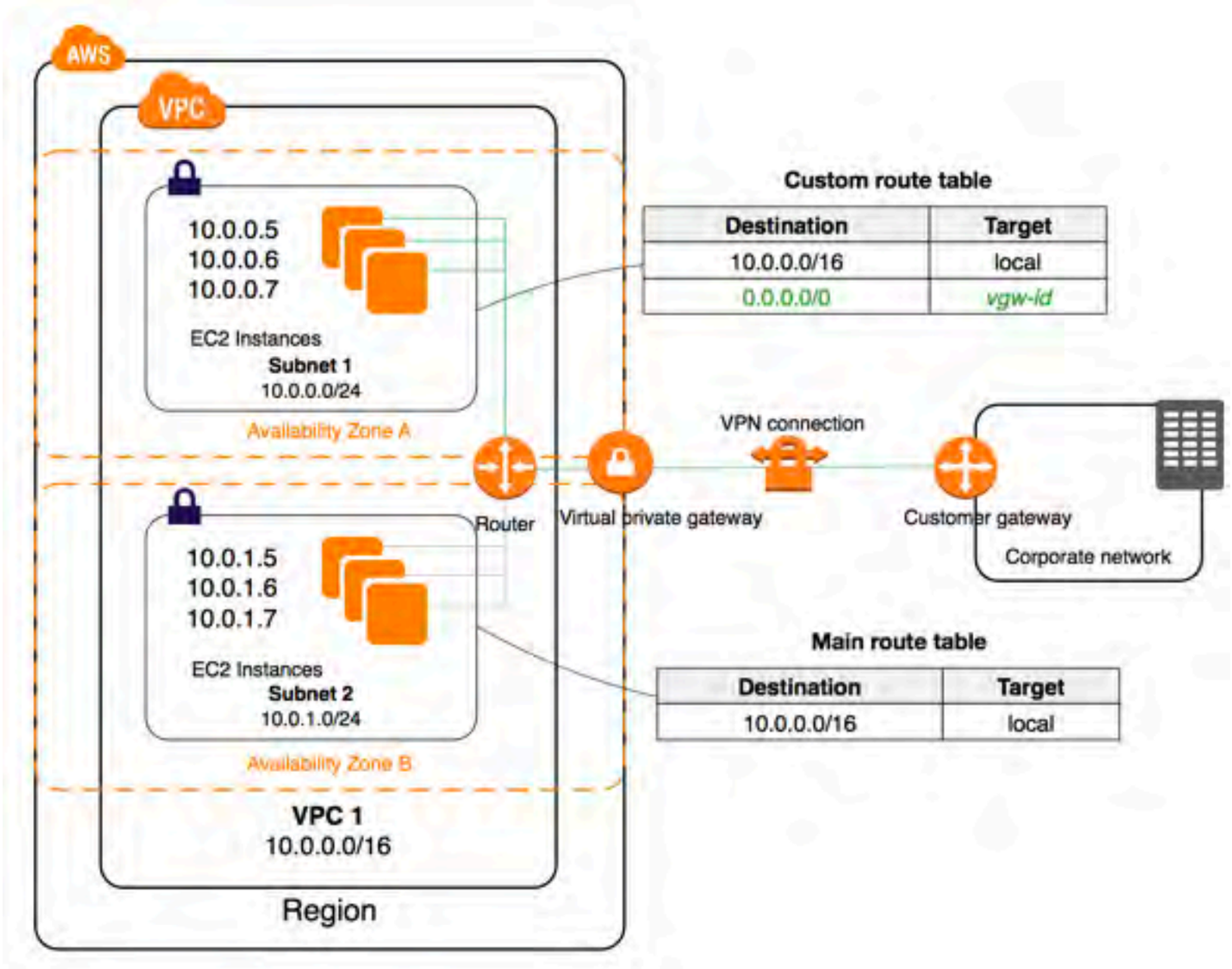
- You can use _____ and _____ to help secure the instances in your VPC.

1. Security groups and 2-factor authentication
2. Security groups and biometric authentication
3. **Security groups and network ACLs**
4. Security groups and multi-factor authentication

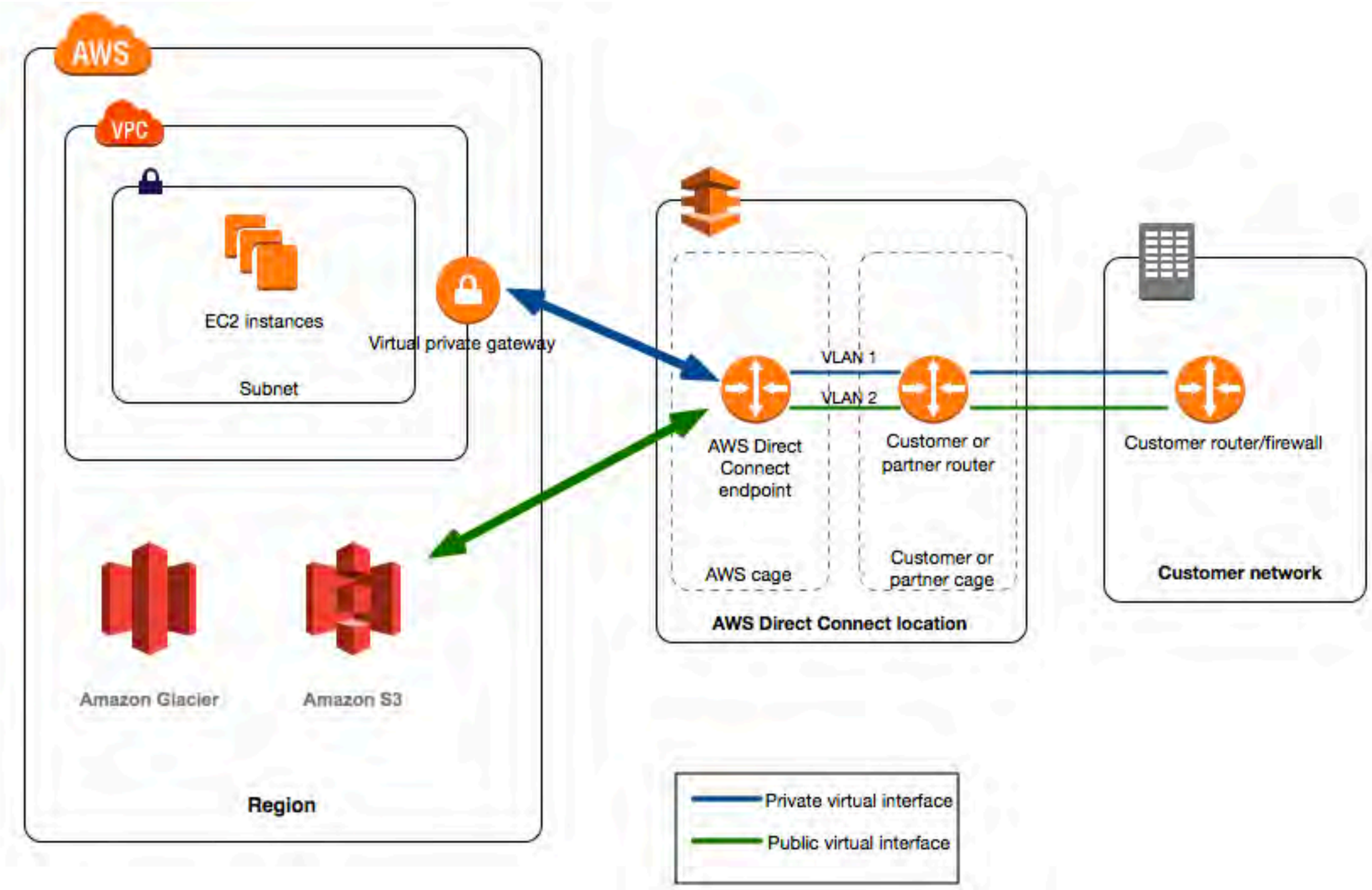
NAT gateways



VPN: Accessing a corporate or home network



AWS Direct Connect



Question

- What action is required to establish an Amazon Virtual Private Cloud (VPC) VPN connection between an on-premises data center and an Amazon VPC virtual private gateway?

1. Use a dedicated network address translation instance in the public subnet

2. Assign a static Internet-routable IP address to an Amazon VPC customer gateway.

3. Establish a dedicated networking connection using AWS Direct Connect.

4. Modify the main route table to allow traffic to a network address translation instance.

Answer

- What action is required to establish an Amazon Virtual Private Cloud (VPC) VPN connection between an on-premises data center and an Amazon VPC virtual private gateway?

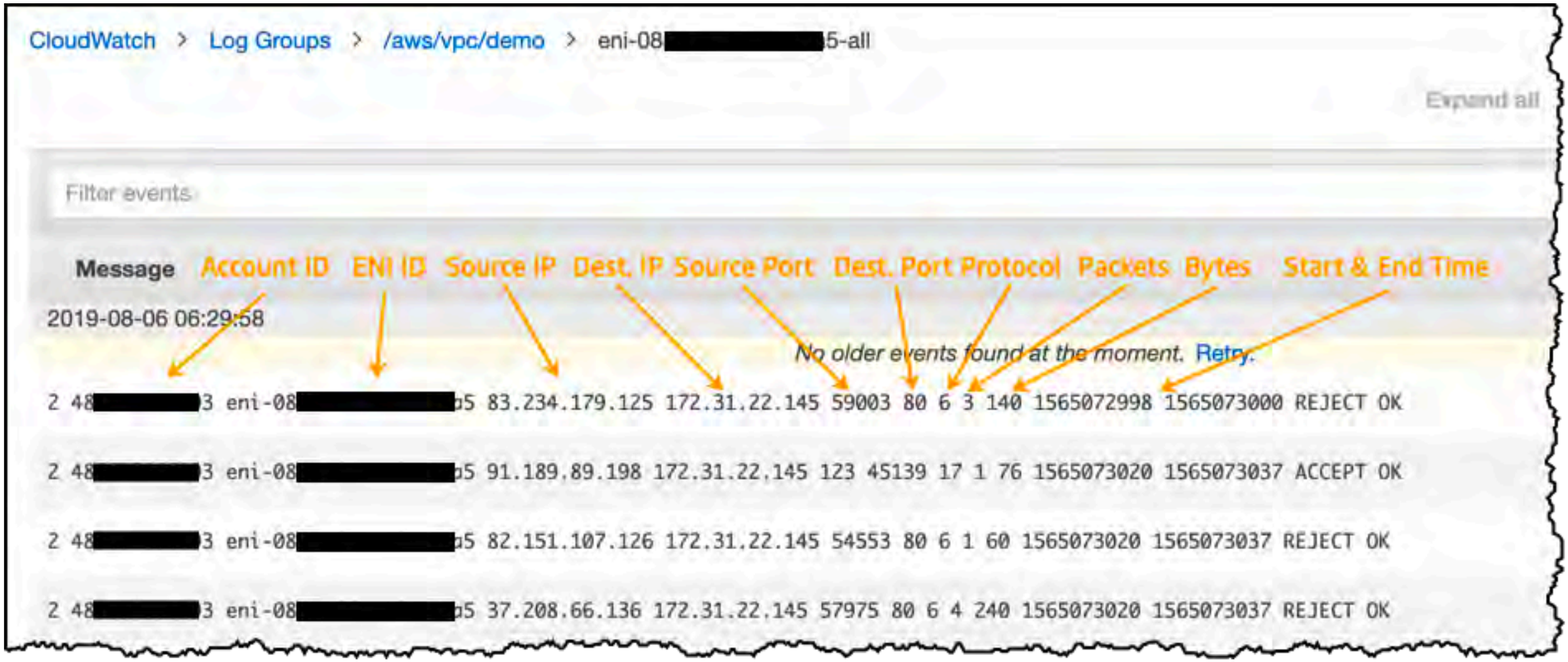
1. Use a dedicated network address translation instance in the public subnet

2. Assign a static Internet-routable IP address to an Amazon VPC customer gateway.

3. Establish a dedicated networking connection using AWS Direct Connect.

4. Modify the main route table to allow traffic to a network address translation instance.

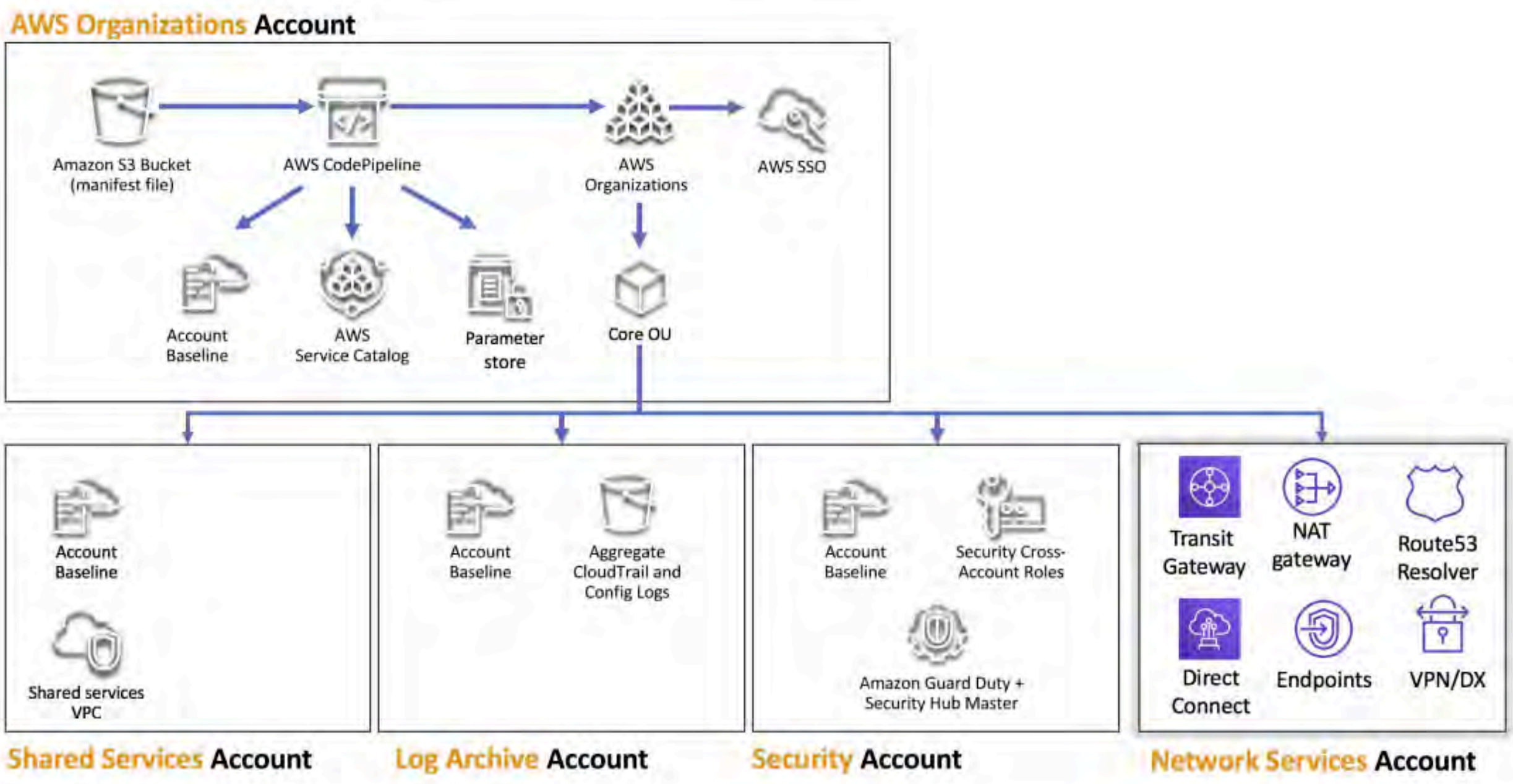
VPC Flow Logs



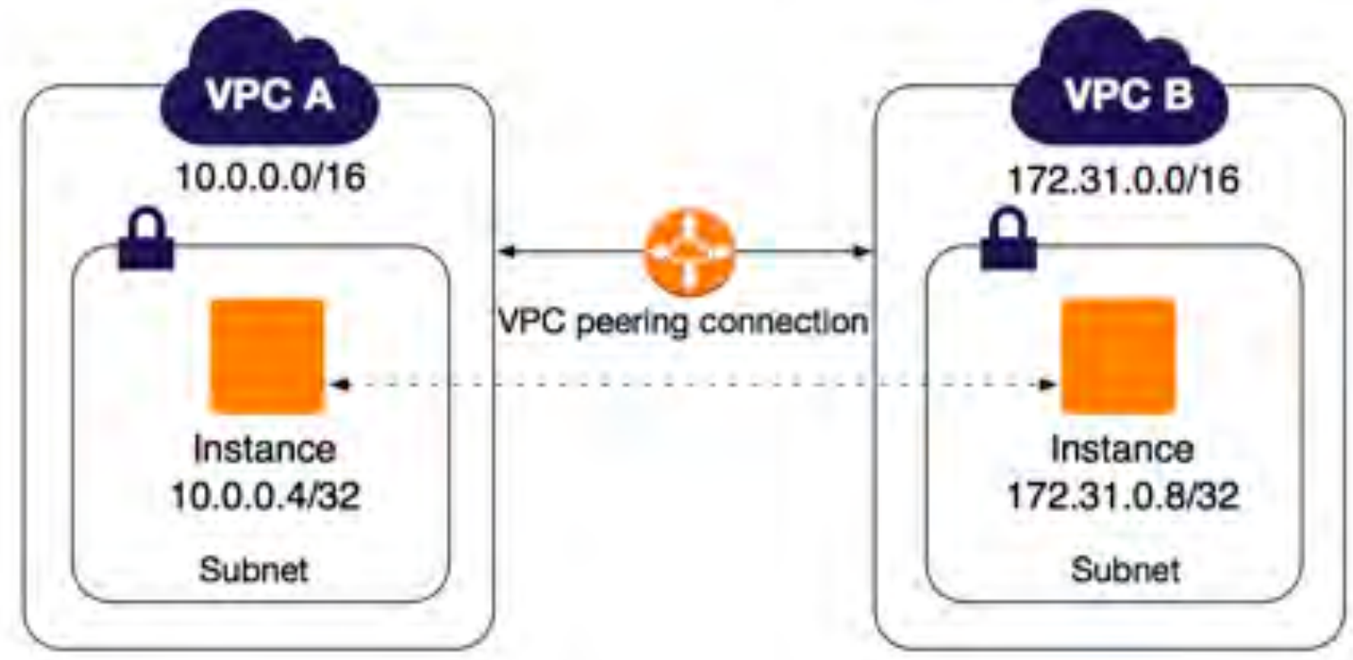
IP traffic

[Amazon CloudWatch Logs] or [Amazon Simple Storage Service (S3)].

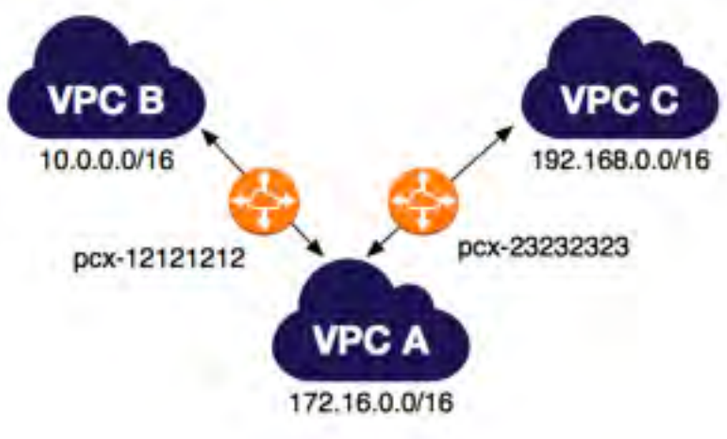
Multi-VPC Pattern



VPC Peering

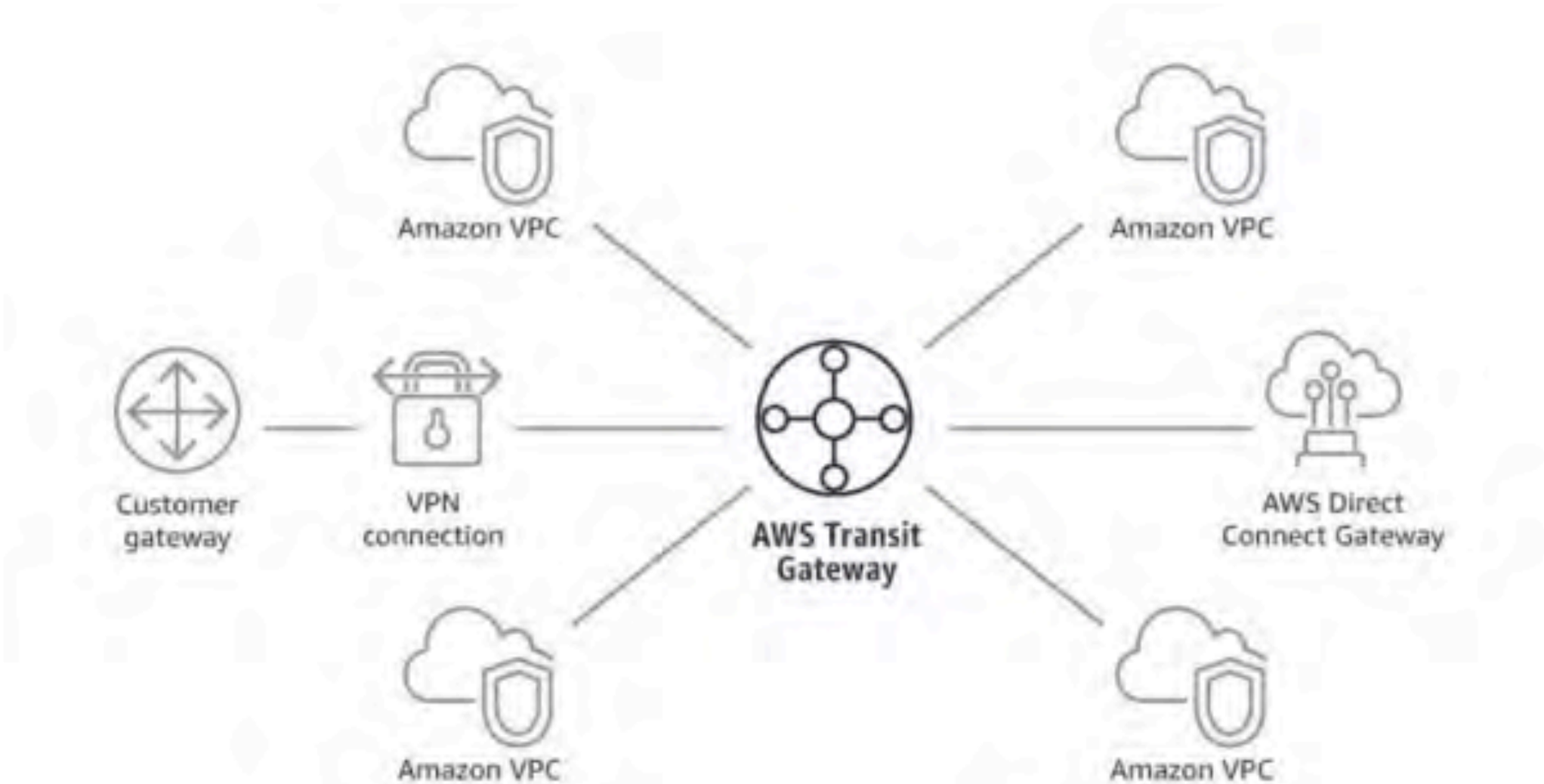


- Use private IP addresses
- IP Spaces - no overlap
- One peering resource
- Can be between different AWS Accounts



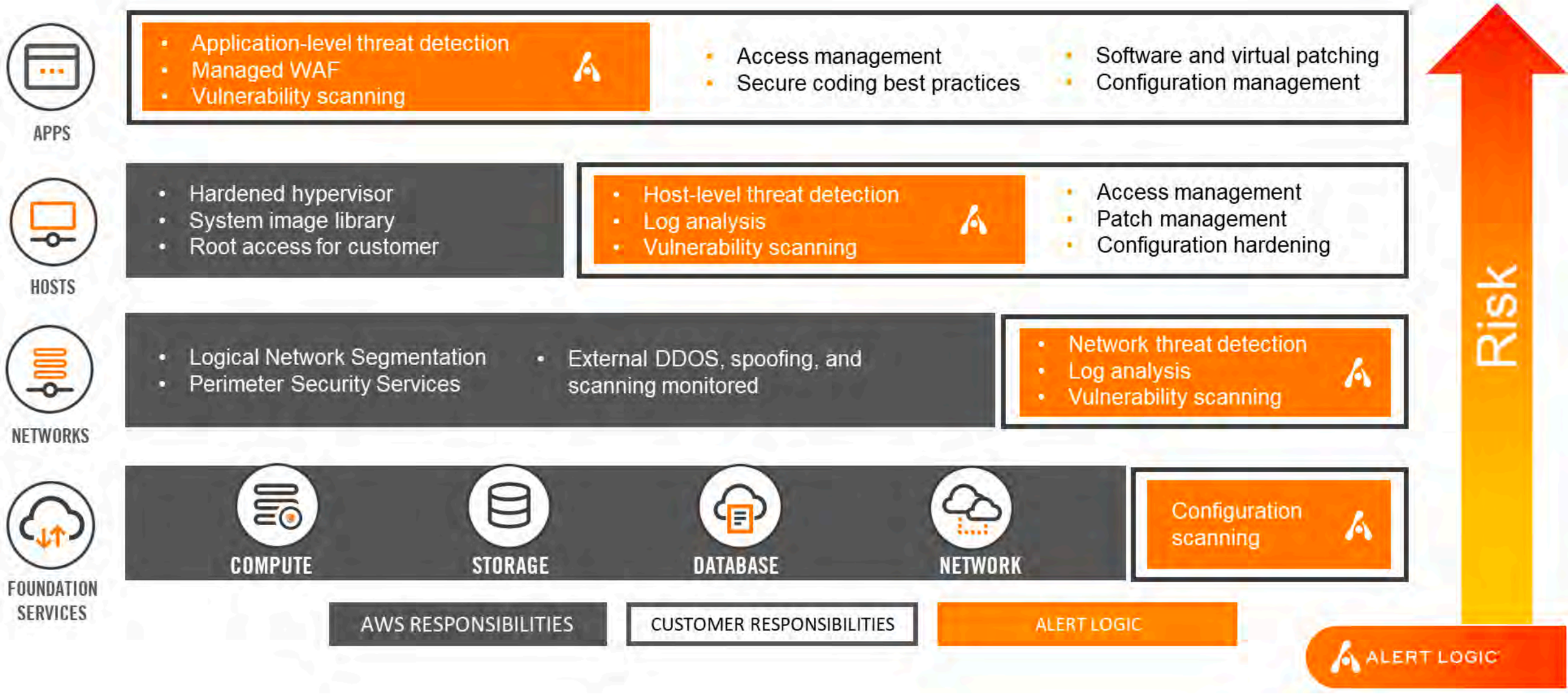
B can not talk to C

Transit Gateway



Hub and Spoke design

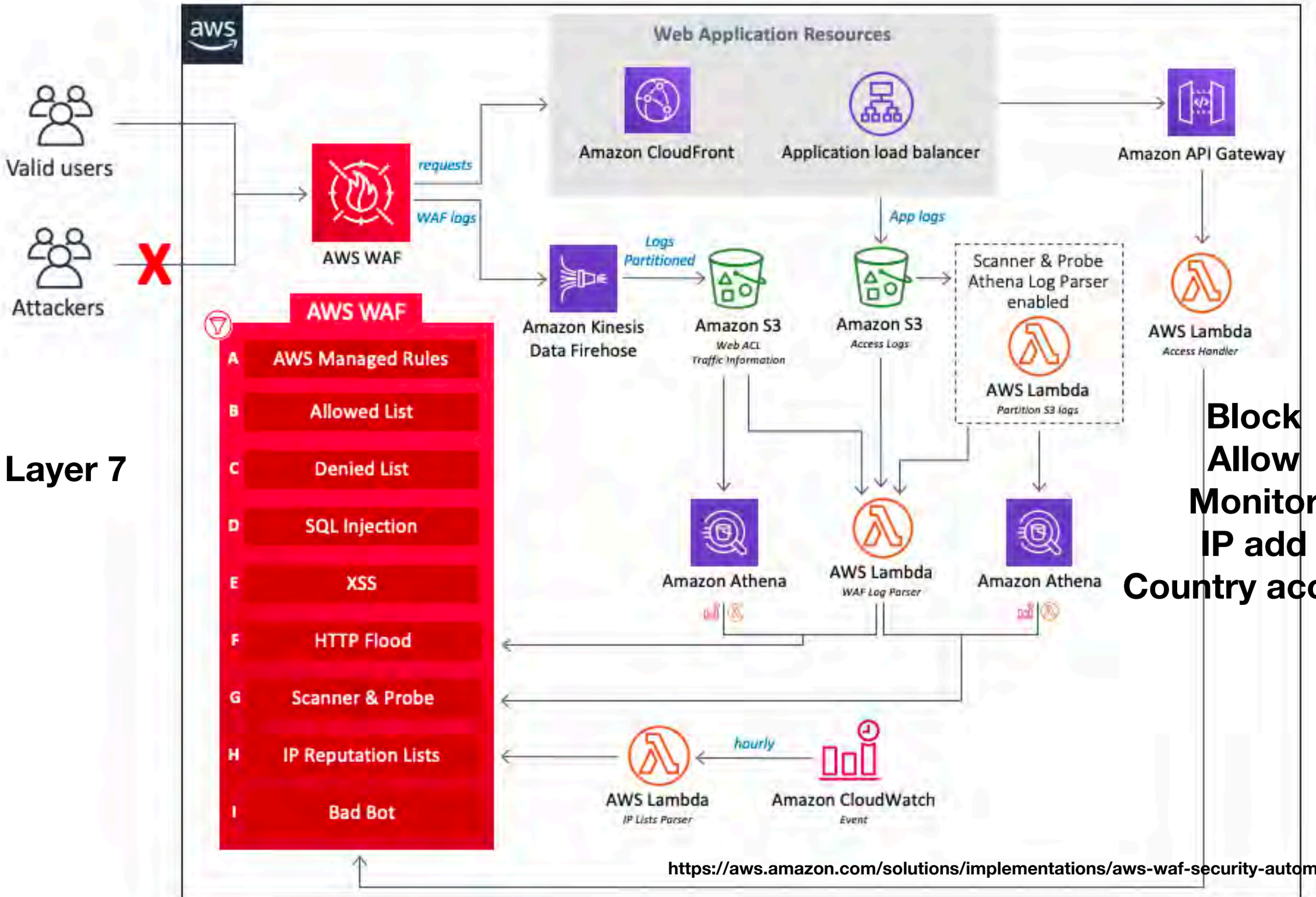
Security is a shared responsibility



https://aws.amazon.com/blogs/apn/7-key-best-practices-for-cloud-security-from-alert-logic/

IDENTIFY & RECON	Manage exposures Coding best practices		
INITIAL ATTACK	Coding best practices Application monitoring	Network monitoring	
COMMAND & CONTROL	Vulnerability management Least privilege access	Role-based Access Network monitoring	Log correlation
DISCOVER & SPREAD	Vulnerability management User lifecycle management	Network monitoring Log correlation	File integrity monitoring
EXTRACT & EXFILTRATE	Application response monitoring Network monitoring	Least privilege access Role-based access	

AWS WAF Security Automations



Non-overlapping private IP address ranges

- Enforce non-overlapping private IP address ranges in all private address spaces where they are connected

Data Tier

- Data In Transit
    - In and out of AWS
    - Within AWS
- Data at Rest
    - Amazon S3
    - Amazon EBS

Data in Transit

- Data in and out of AWS infrastructure
    - SSL over web
    - VPN for IPsec
        - IPsec over AWS direct Connect
        - Import/Export/Snowball
- Data sent to the AWS API
    - AWS API calls use HTTPs/SSL (Default)

Data at Rest

- Server-side encryption options
  - Amazon S3-Managed Keys (SSE-S3)
  - KMS-Managed Keys (SSE-KMS)
  - Customer-Provided Keys (SSE-C)
- Client-side encryption options
  - KMS managed master encryption keys (CSE-KMS)
  - Customer managed master encryption keys (CSE-C)

Question

- What does the “Server Side Encryption” option an Amazon S3 provide?

1. It encrypts the files that you send to Amazon S3, on the server side.

2. It provides an encrypted virtual disk in the cloud

3. It allows to upload files using an SSL endpoint, for a secure transfer.

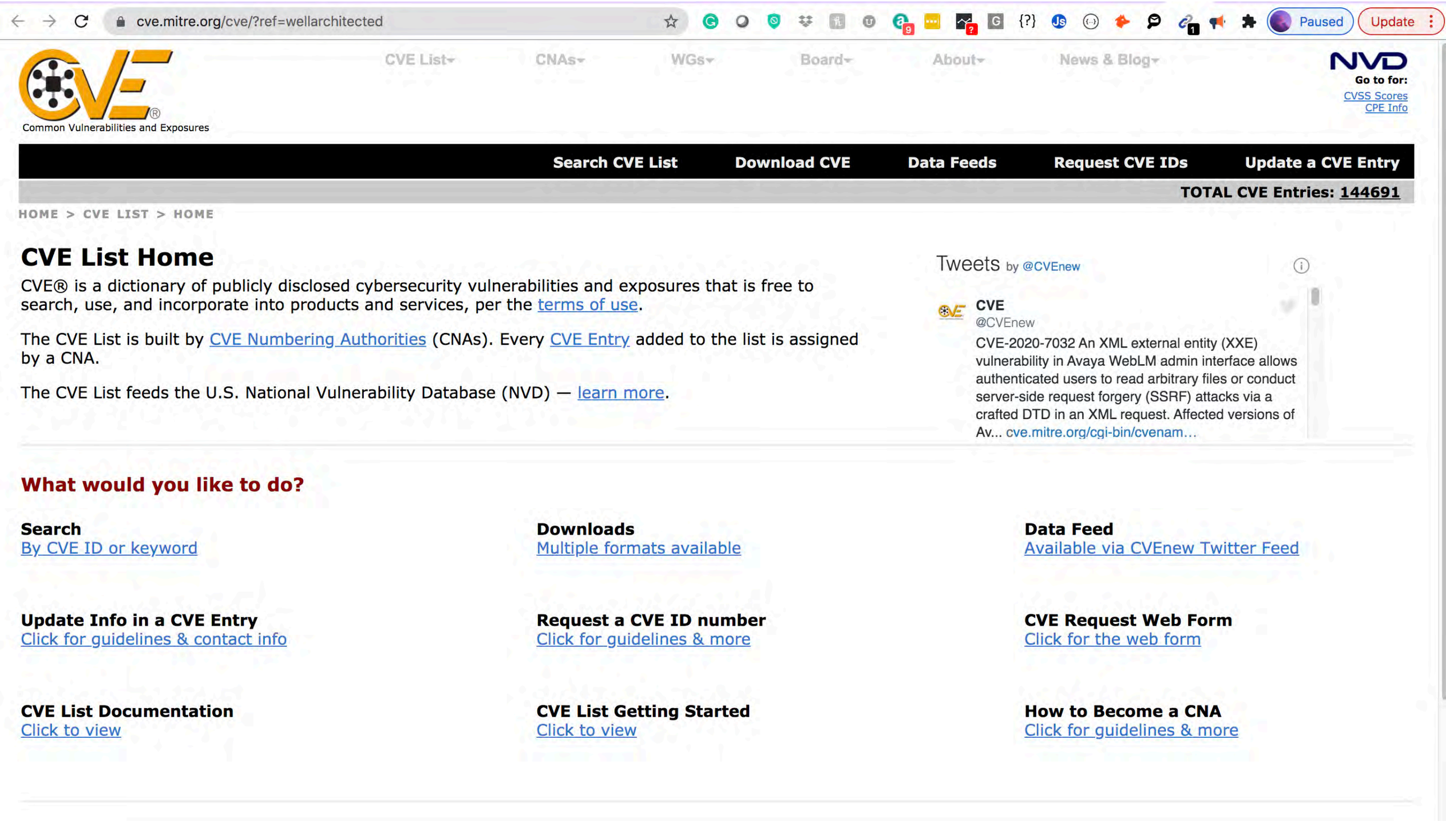
4. It doesn’t exist for Amazon S3, but only for Amazon EC2

Question

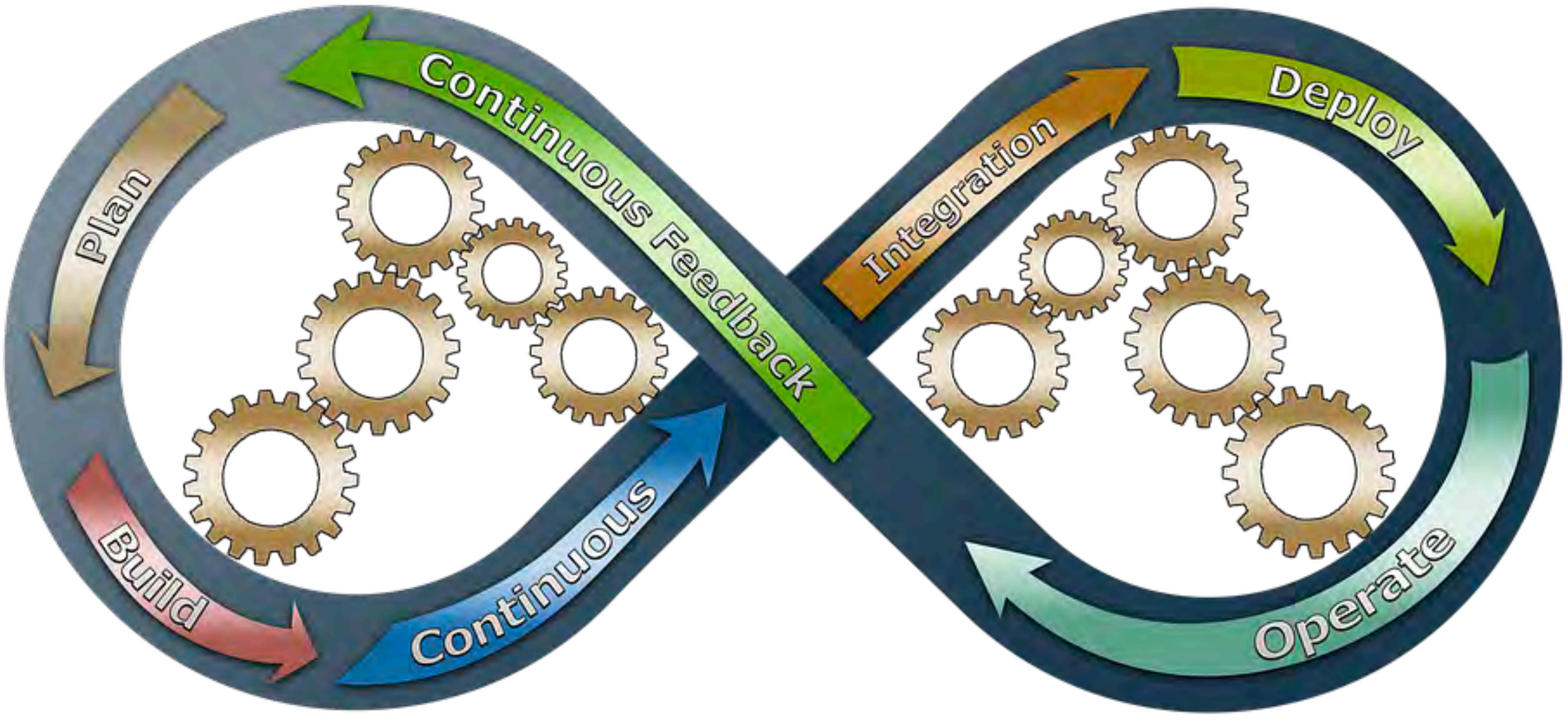
- What does the “Server Side Encryption” option an Amazon S3 provide?

1. **It encrypts the files that you send to Amazon S3, on the server side.**
2. It provides an encrypted virtual disk in the cloud
3. It allows to upload files using an SSL endpoint, for a secure transfer.
4. It doesn’t exist for Amazon S3, but only for Amazon EC2

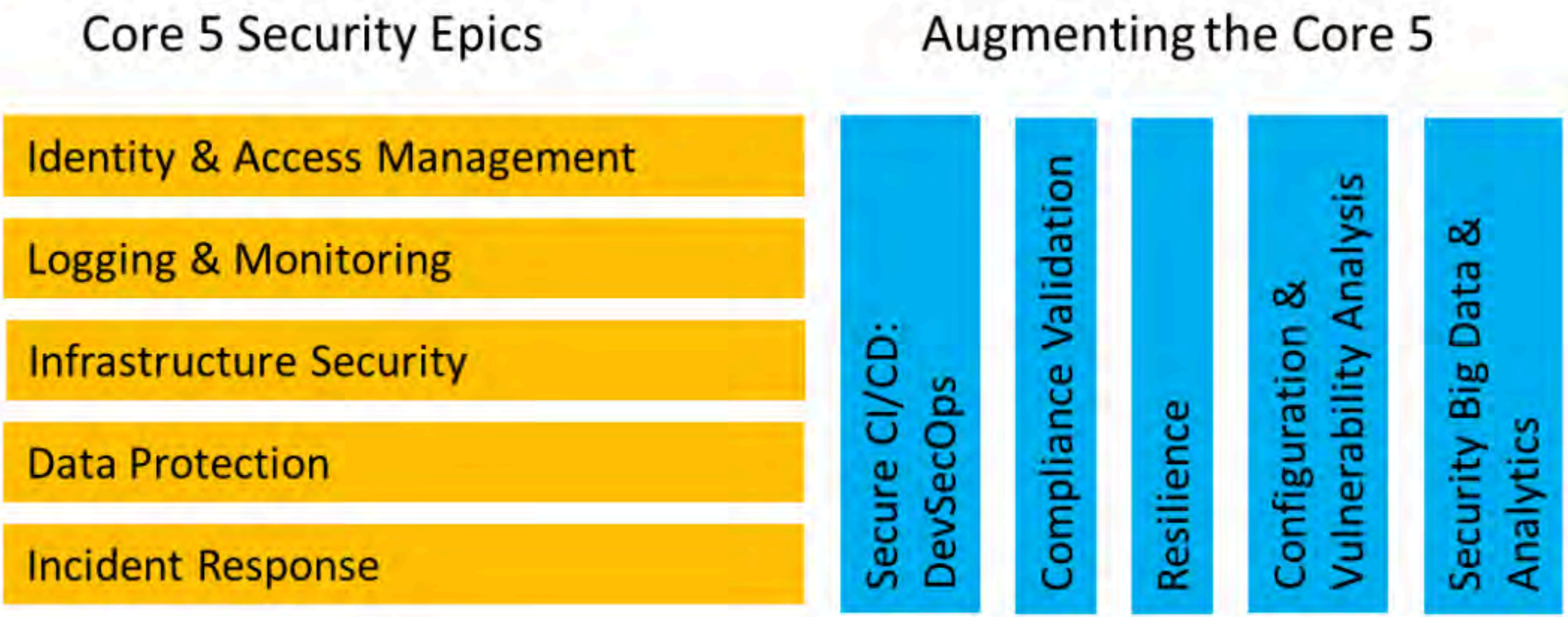
Subscribe to industry news



Automate security best practices



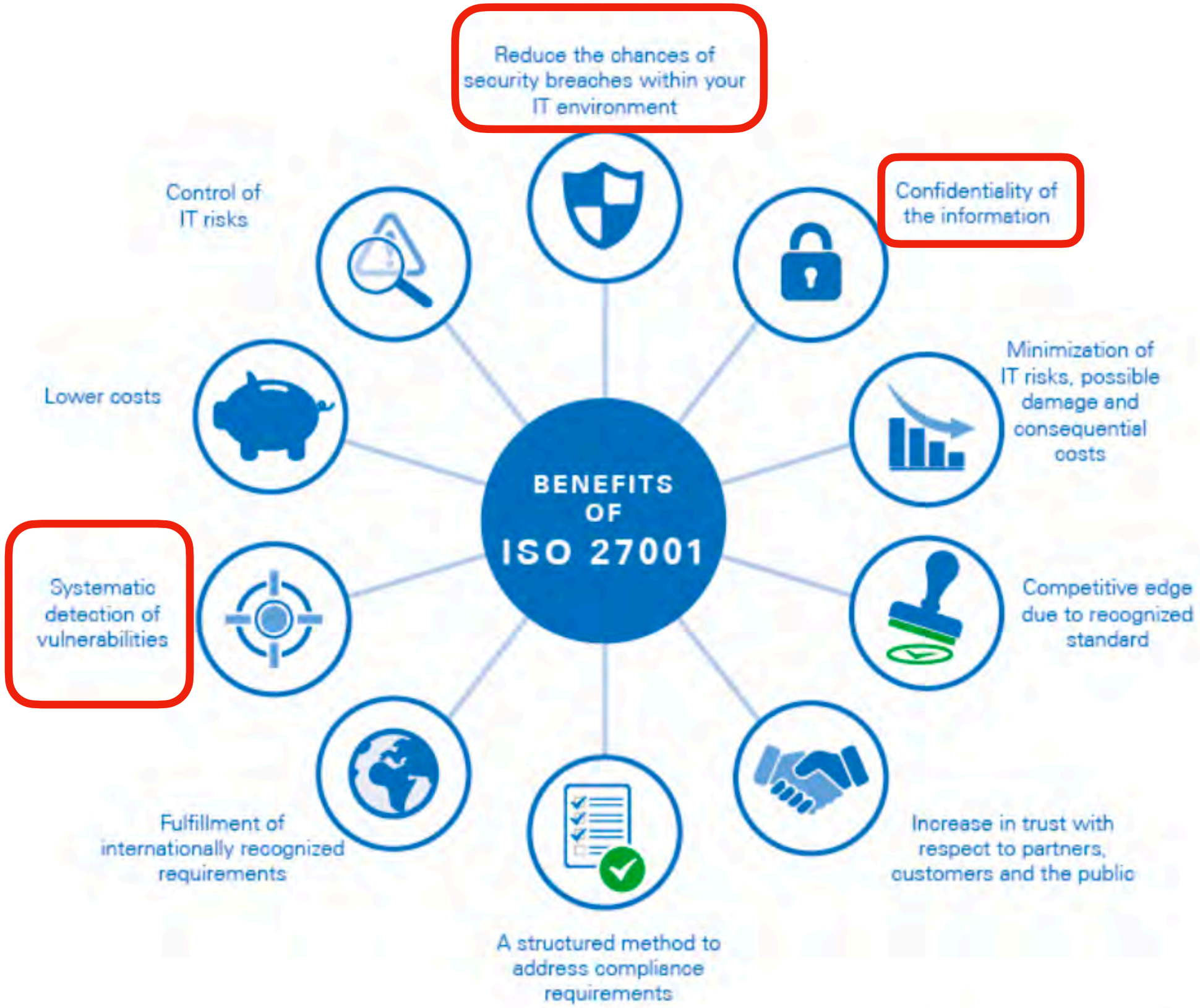
AWS guidelines



Privacy and Security Laws

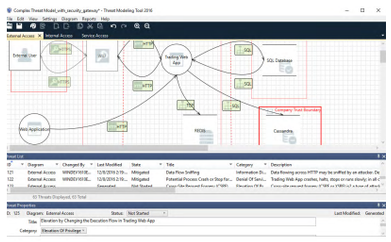
- US laws and Regulations

- International laws and regulation



TÜVRheinland®
Precisely Right.

Continuous Integration Stage



Design

Review Architecture

Coding Tests

Static Tests

Dynamic Tests

Threat Modeling

Input Validation

Config Management

Cryptography

Auditing

PCI, HIPPA

Authentication

Authorization

Fuzz tests

Contract First

Contract

Lint

Stress

Sanitizer

Component

Benchmark

Mutation

Dependency Checker

GitRob

Checkmarx

SonarQube

Coverity

Blackduck

OWASP ZAP

Lynis

OpenVas

evident.io

GAUNTLT

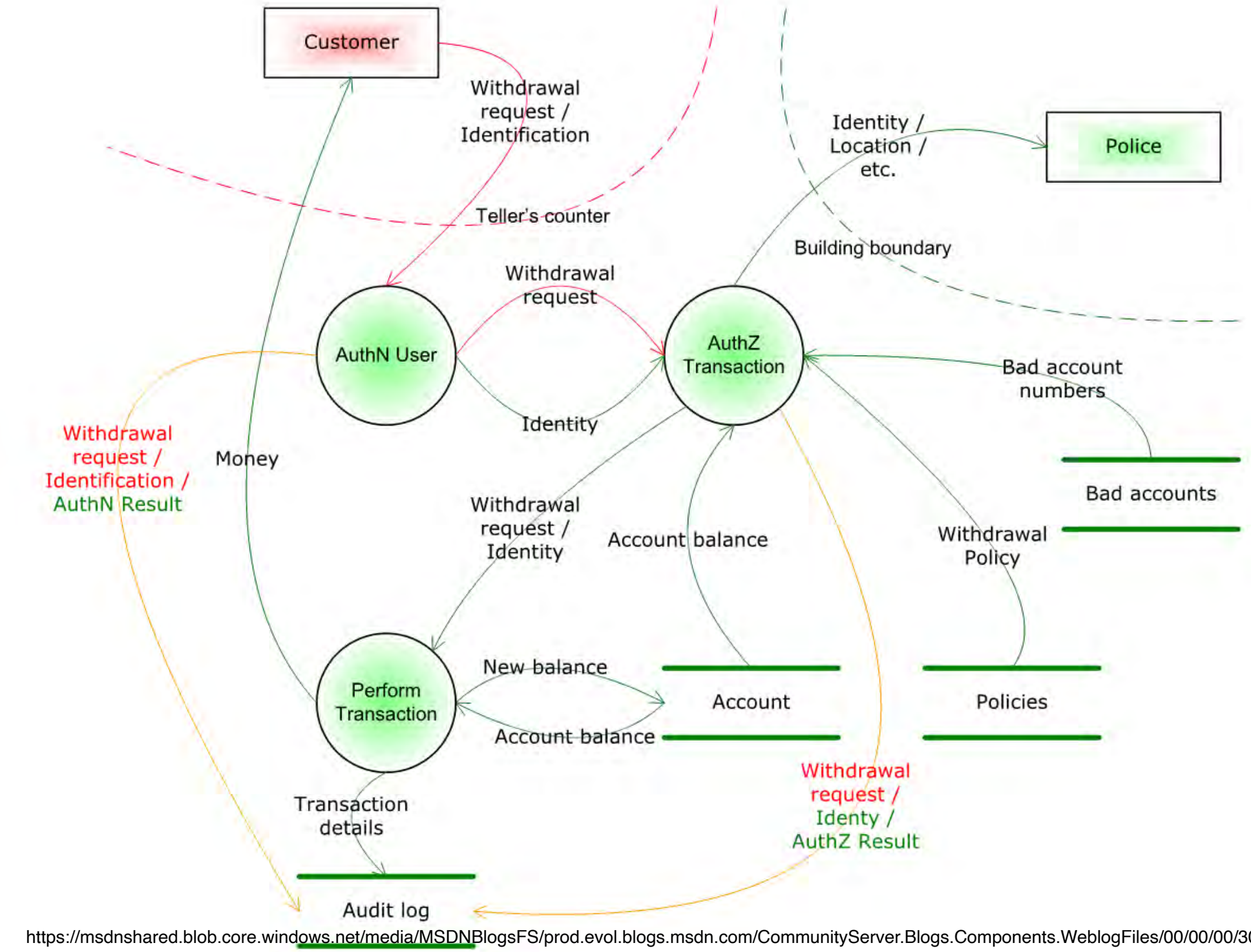
Burp Suite

Threat Modeling Process


Repudiation
Information Disclosure
Tampering
Denial Of Service
Spoofing
Security Development Lifecycle
Elevation of Privilege
STRIDE Threat Model

Threat	Mitigation Feature
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiaton
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

Threat modeling

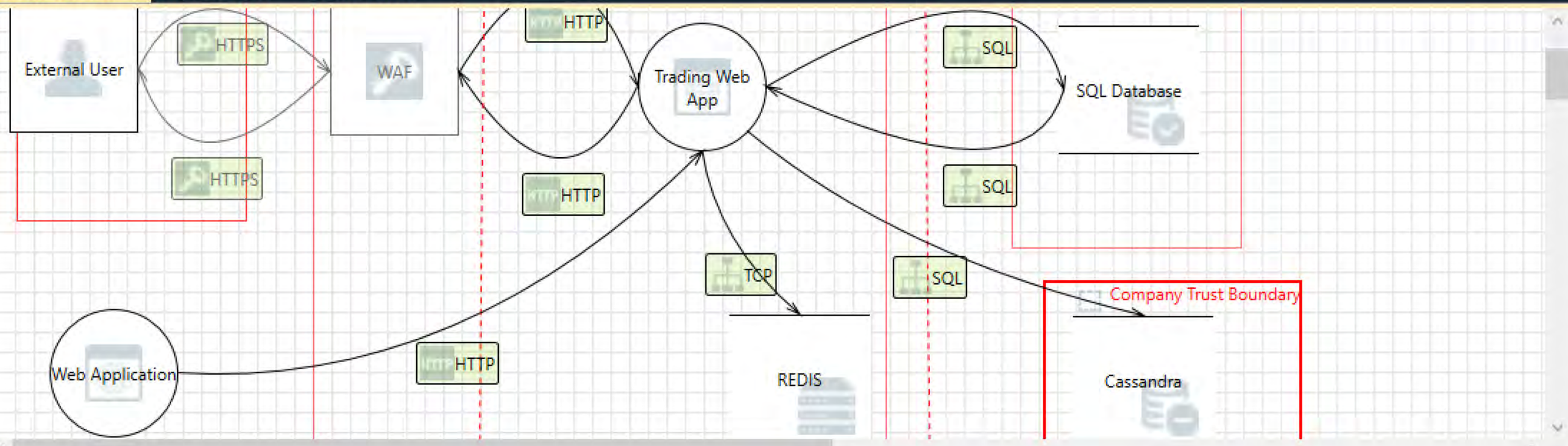


https://msdnshared.blob.core.windows.net/media/MSDNBlogsFS/prod.evol.blogs.msdn.com/CommunityServer.Blogs.Components.WeblogFiles/00/00/00/30/21/6685.AfterThreatModelling

Complex Threat Model_with_security_gateway* - Threat Modeling Tool 2016

File Edit View Settings Diagram Reports Help

External Access | Internal Access | Service Access



Threat List

ID	Diagram	Changed By	Last Modified	State	Title	Category	Description
121	External Access	WINDEV1610E...	12/8/2016 2:19:...	Mitigated	Data Flow Sniffing	Information Di...	Data flowing across HTTP may be sniffed by an attacker. De
122	External Access	WINDEV1610E...	12/8/2016 2:19:...	Mitigated	Potential Process Crash or Stop for...	Denial Of Servi...	Trading Web App crashes, halts, stops or runs slowly; in all c
123	External Access		Generated	Not Started	Cross-Site Request Forgery (CSRF)	Elevation Of Pr...	Cross-site request forgery (CSRF or XSRF) is a type of attack

63 Threats Displayed, 63 Total

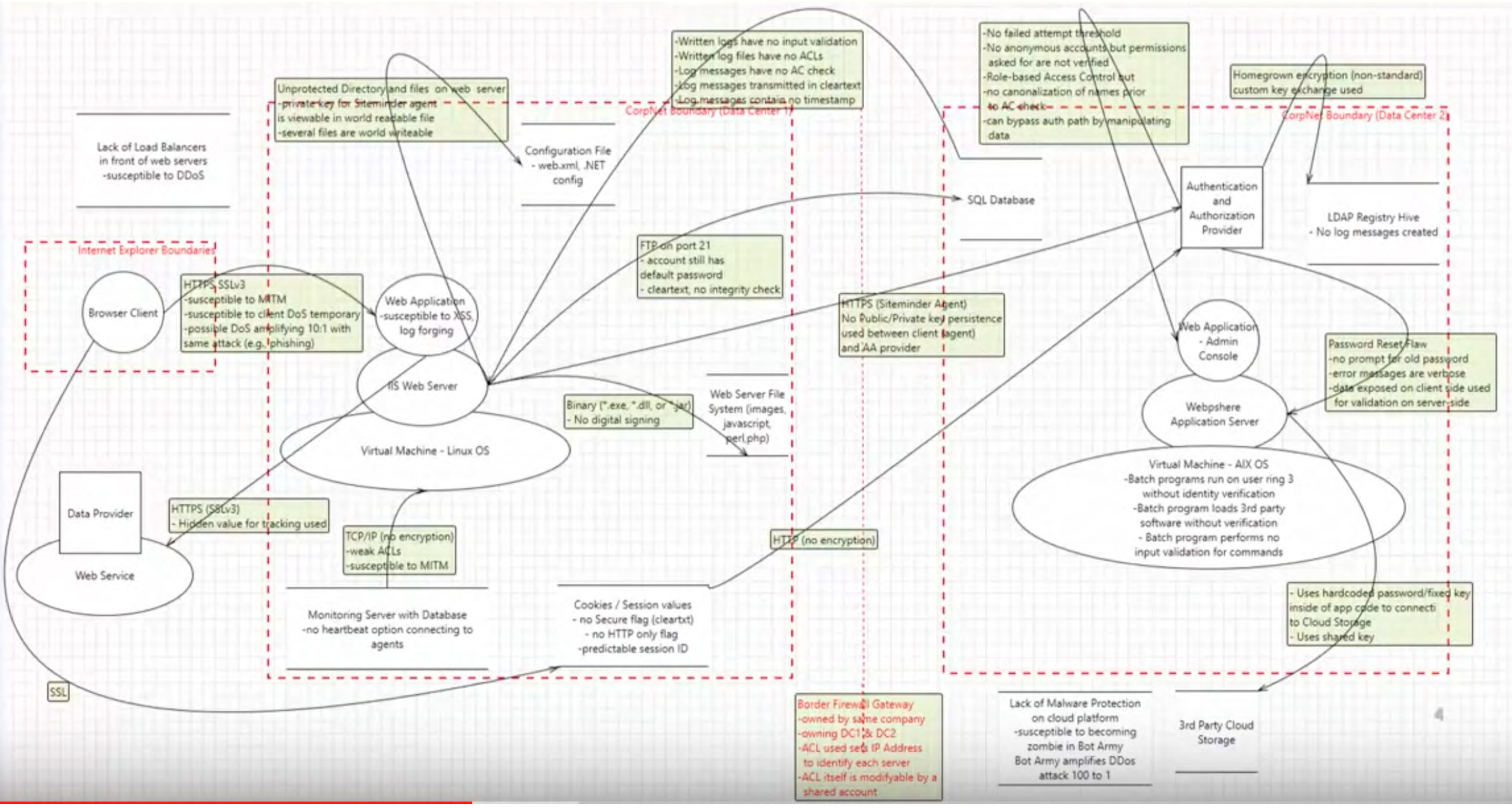
Threat Properties

ID: 125 Diagram: External Access Status: Not Started Last Modified: Generated

Title: Elevation by Changing the Execution Flow in Trading Web App

Category: Elevation Of Privilege

https://www.microsoft.com/en-us/SDL/adopt/eop.aspx


Lack of Load Balancers
in front of web servers
-susceptible to DDoS
Unprotected Directory and files on web server
-private key for Siteminder agent
is viewable in world readable file
-several files are world writeable
Configuration File
- web.xml, .NET
config
-Written logs have no input validation
-Written log files have no ACLs
-Log messages have no AC check
-Log messages transmitted in cleartext
-Log messages contain no timestamp
-No failed attempt threshold
-No anonymous accounts but permissions
asked for are not verified
-Role-based Access Control but
-no canonalization of names prior
to AC check
-can bypass auth path by manipulating
data
Homegrown encryption (non-standard)
custom key exchange used
CorpNet Boundary (Data Center 1)
CorpNet Boundary (Data Center 2)
SQL Database
Authentication
and
Authorization
Provider
LDAP Registry Hive
- No log messages created
Internet Explorer Boundaries
Browser Client
HTTPS SSLv3
-susceptible to MITM
-susceptible to client DoS temporary
-possible DoS amplifying 10:1 with
same attack (e.g., phishing)
Web Application
-susceptible to XSS,
log forging
FTP on port 21
- account still has
default password
- cleartext, no integrity check
HTTPS (Siteminder Agent)
No Public/Private key persistence
used between client (agent)
and AA provider
Web Application
- Admin
Console
Password Reset Flaw
-no prompt for old password
-error messages are verbose
-data exposed on client side used
for validation on server-side
IIS Web Server
Binary (*.exe, *.dll, or *.jar)
- No digital signing
Web Server File
System (images,
javascript,
perl,php)
Webpshere
Application Server
Virtual Machine - Linux OS
Virtual Machine - AIX OS
-Batch programs run on user ring 3
without identity verification
-Batch program loads 3rd party
software without verification
- Batch program performs no
input validation for commands
Data Provider
Web Service
HTTPS (S8Lv3)
- Hidden value for tracking used
TCP/IP (no encryption)
-weak ACLs
-susceptible to MITM
HTTP (no encryption)
- Uses hardcoded password/fixed key
inside of app code to connecti
to Cloud Storage
- Uses shared key
Monitoring Server with Database
-no heartbeat option connecting to
agents
Cookies / Session values
- no Secure flag (cleartxt)
- no HTTP only flag
-predictable session ID
SSL
Border Firewall Gateway
-owned by same company
-owning DC1 & DC2
-ACL used sets IP Address
to identify each server
-ACL itself is modifyable by a
shared account
Lack of Malware Protection
on cloud platform
-susceptible to becoming
zombie in Bot Army
Bot Army amplifies DDos
attack 100 to 1
3rd Party Cloud
Storage
4

OWASP Security Knowledge Framework

What is SKF?

Over 15 years of experience in web application security bundled into a single application. The Security Knowledge Framework is a vital asset to the coding toolkit of your development team. Use SKF to learn and integrate security by design in your web application.

SKF is an open source security knowledgebase including manageable projects with checklists and best practice code examples in multiple programming languages showing you how to prevent hackers gaining access and running exploits on your application.

In a nutshell

- Training your developers in writing secure code
- Security by design, early feedback of possible security issues
- Code examples for secure coding guidance
- Knowledge base items for deeper understanding of the security controls
- Security labs to improve your verification skills
- Machine learning chatbot for easy support

https://owasp.org/www-project-security-knowledge-framework/

https://owasp-skf.gitbook.io/asvs-write-ups/

Security Knowledge Framework

Search...

Logout

Dashboard | Manage Projects | Code Examples | Checklists | Knowledgebase | Users | Labs

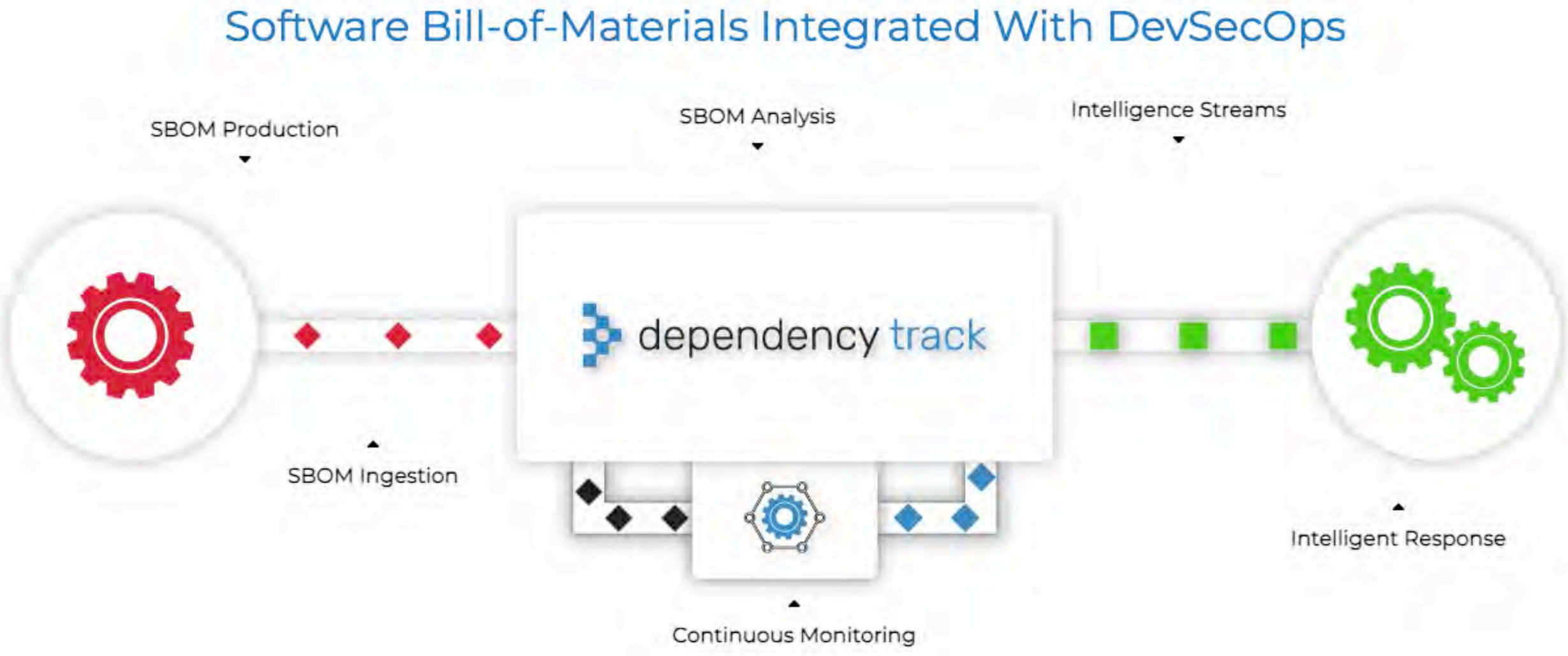
LABS

Labs / View

Search Lab

#	Name	Label	Level	Status	Write-up	Action
	Path traversal (LFI)	SKF-labs	1		Click here	Start
	Cross Site Scripting	SKF-labs	1		Click here	Start
	Cross site scripting (attribute)	SKF-labs	1		Click here	Start
	Cross site scripting (href)	SKF-labs	1	Lab is Running	Click here	Stop
	Insecure file upload	SKF-labs	1		Click here	Start
	Clickjacking	SKF-labs	1		Click here	Start
	Rate-limiting	SKF-labs	1		Click here	Start

OWASP Dependency-Track



https://dependencytrack.org/

Supported Bill-of-Material Formats

CycloneDX

SPDX

Supported Notification Platforms

slack

Microsoft Teams

webhooks

Vulnerability Intelligence

NVD

npm

VulnDB

Sonatype OSS Index

dependency track

API Integration

OPENAPI INITIATIVE

Jenkins

Supported Repositories

RubyGems

hex

Maven

pypi

npm

nuget

https://dependencytrack.org/

Vulnerability Aggregation

ThreadFix

FORTIFY

KENNA Security

Security Compass

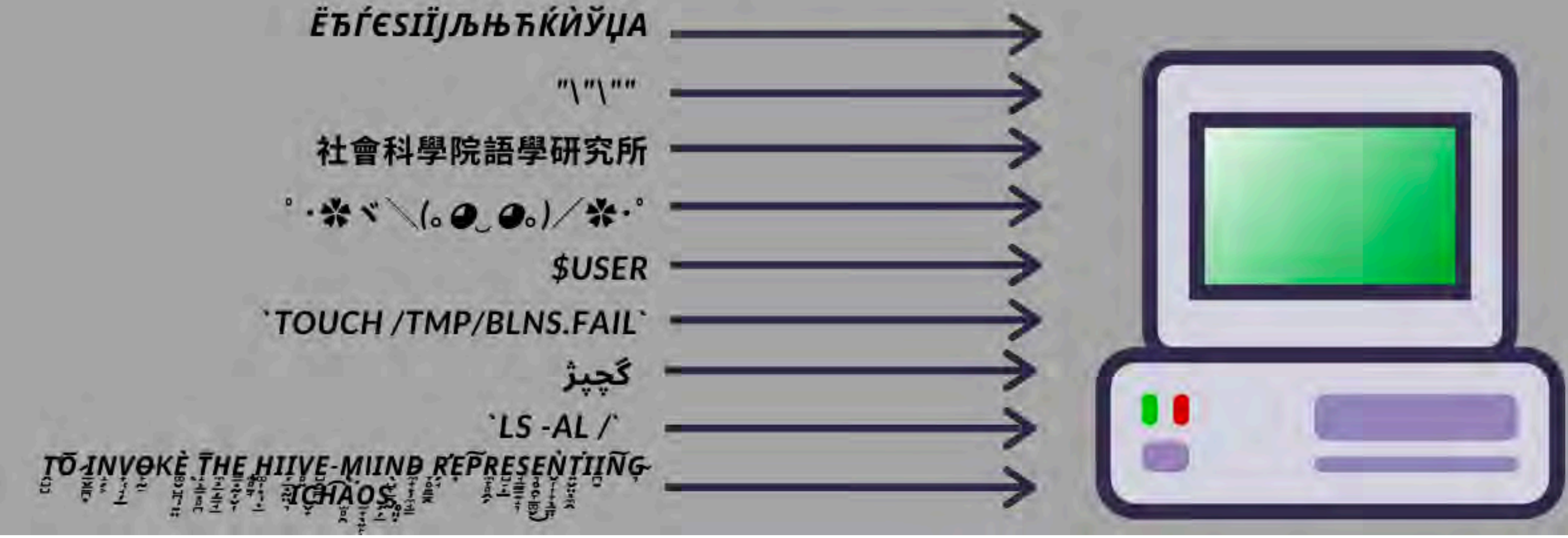
DEFECTDOJO

OWASP Dependency-Track Features

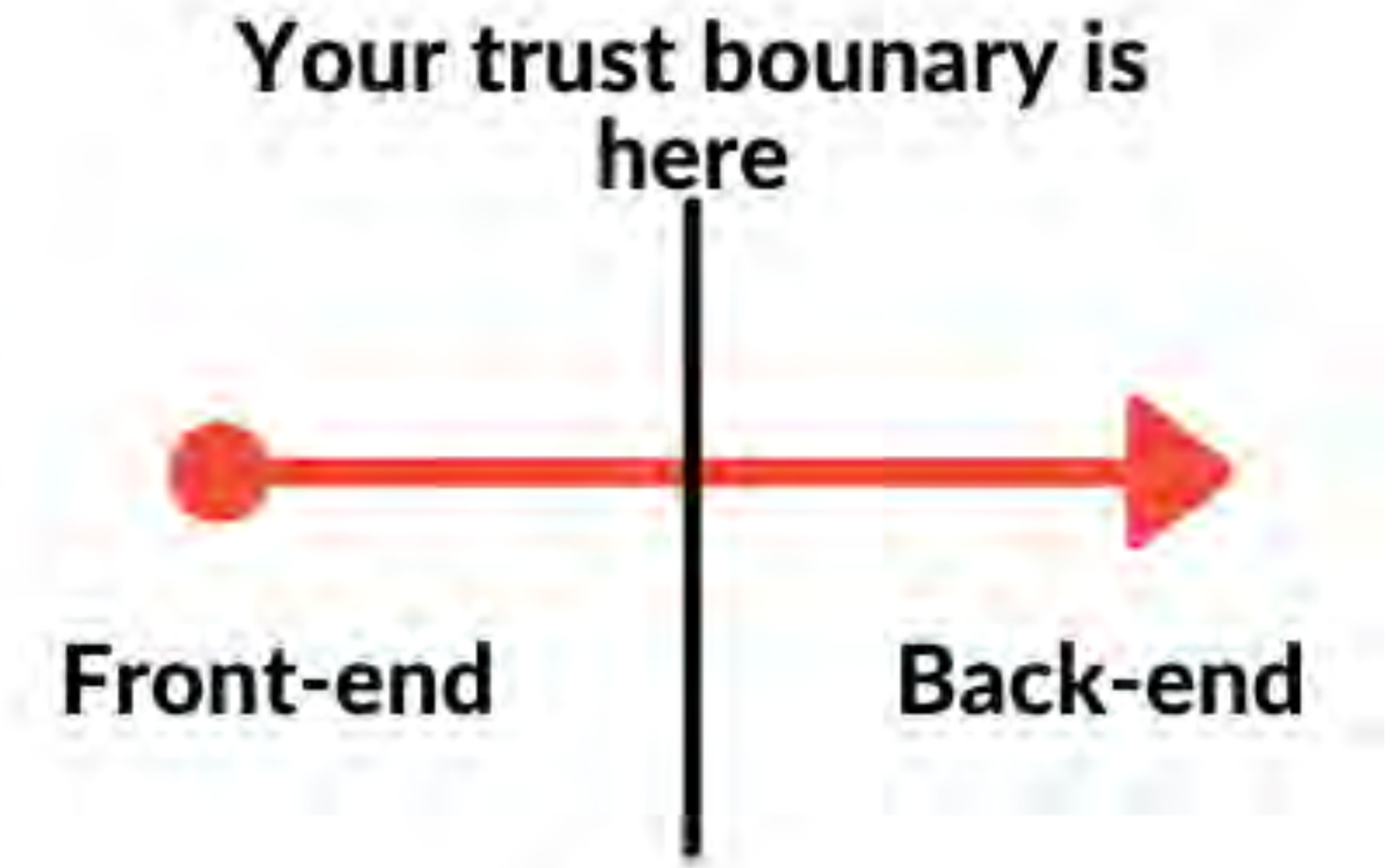
- Tracks application, library, framework, operating system, and hardware components
- Tracks component usage across all version of every application in an organizations portfolio
- Identifies multiple forms of risk including
- Components with known vulnerabilities
- Out-of-date components
- Modified components
- License risk

https://owasp.org/www-project-dependency-track/

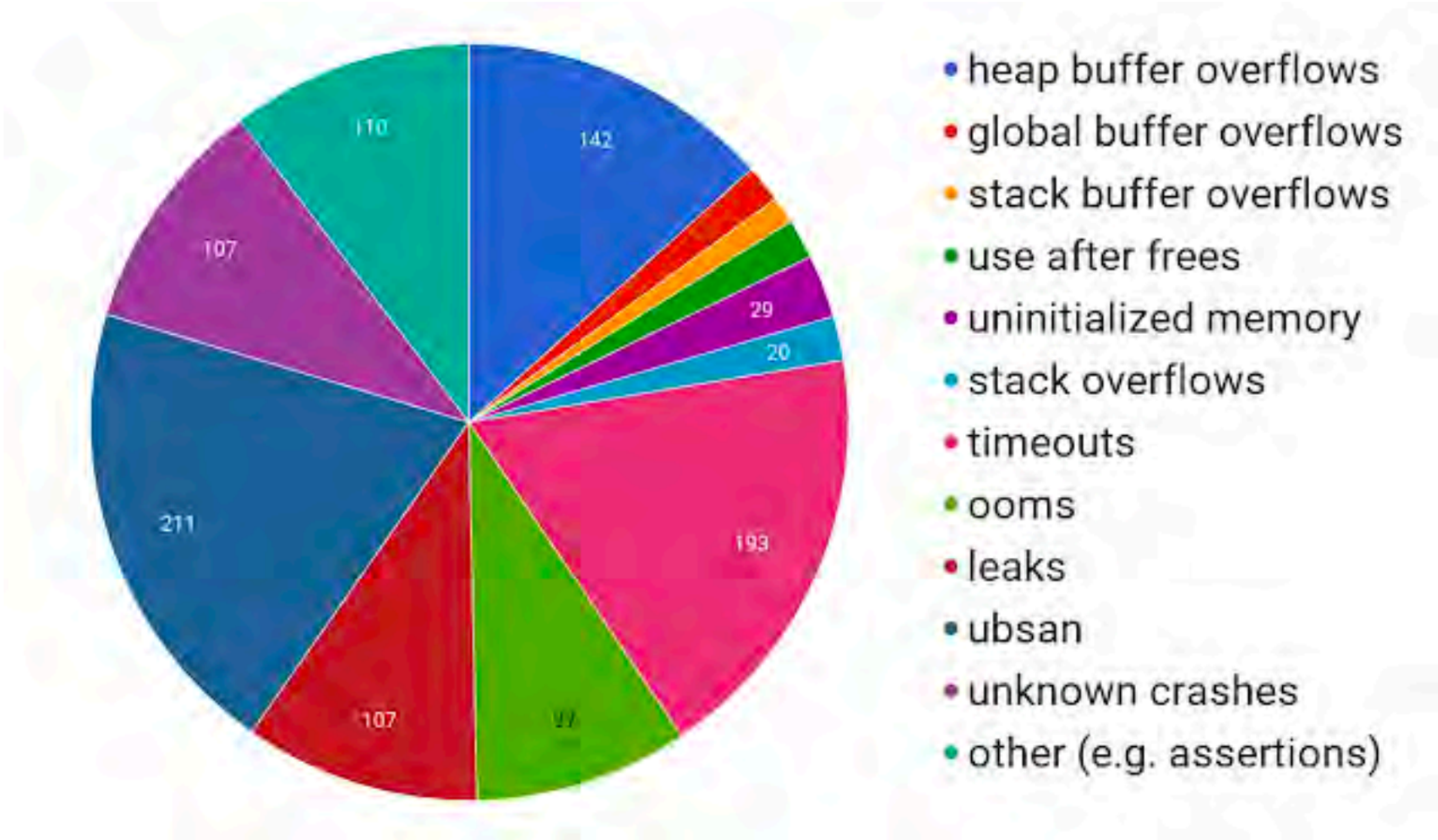
WHAT IS FUZZING?



https://www.freecodecamp.org/news/whats-fuzzing-fuzz-testing-explained/


Your trust bounary is here
Front-end
Back-end

OSS-Fuzz

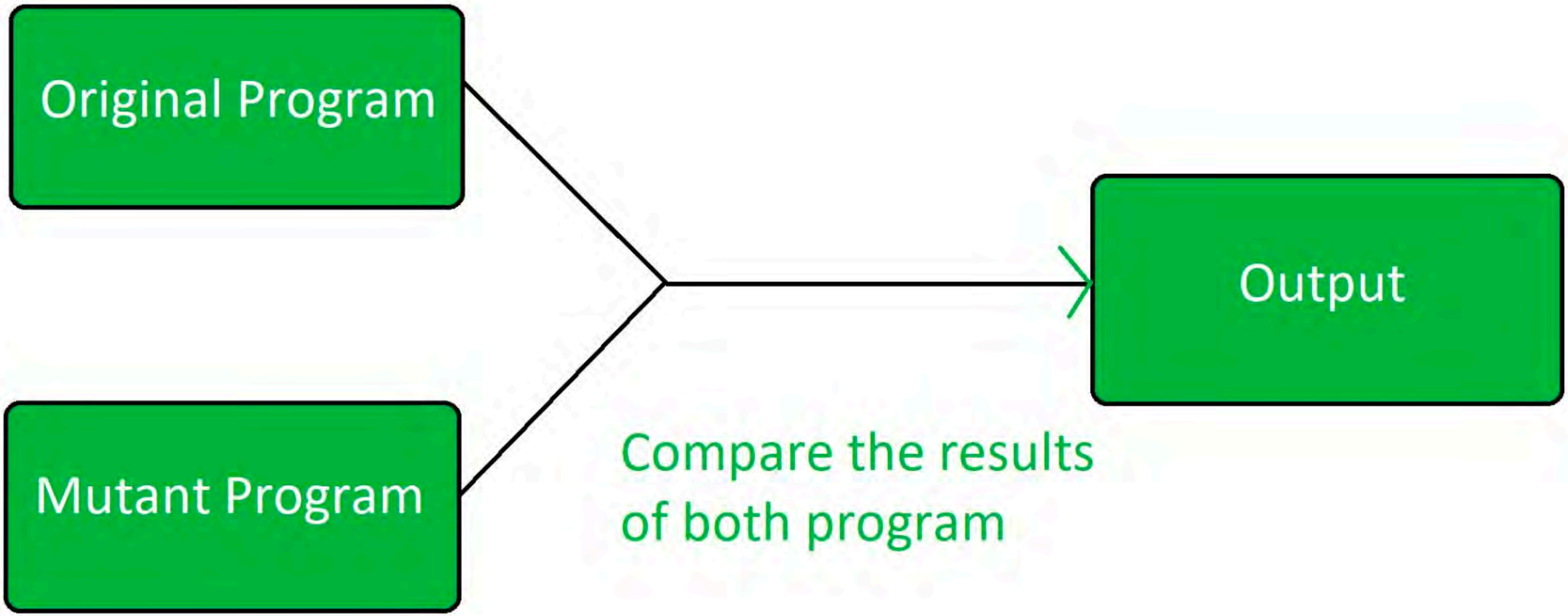


25,000+ bugs in Google Chrome code

https://github.com/google/oss-fuzz

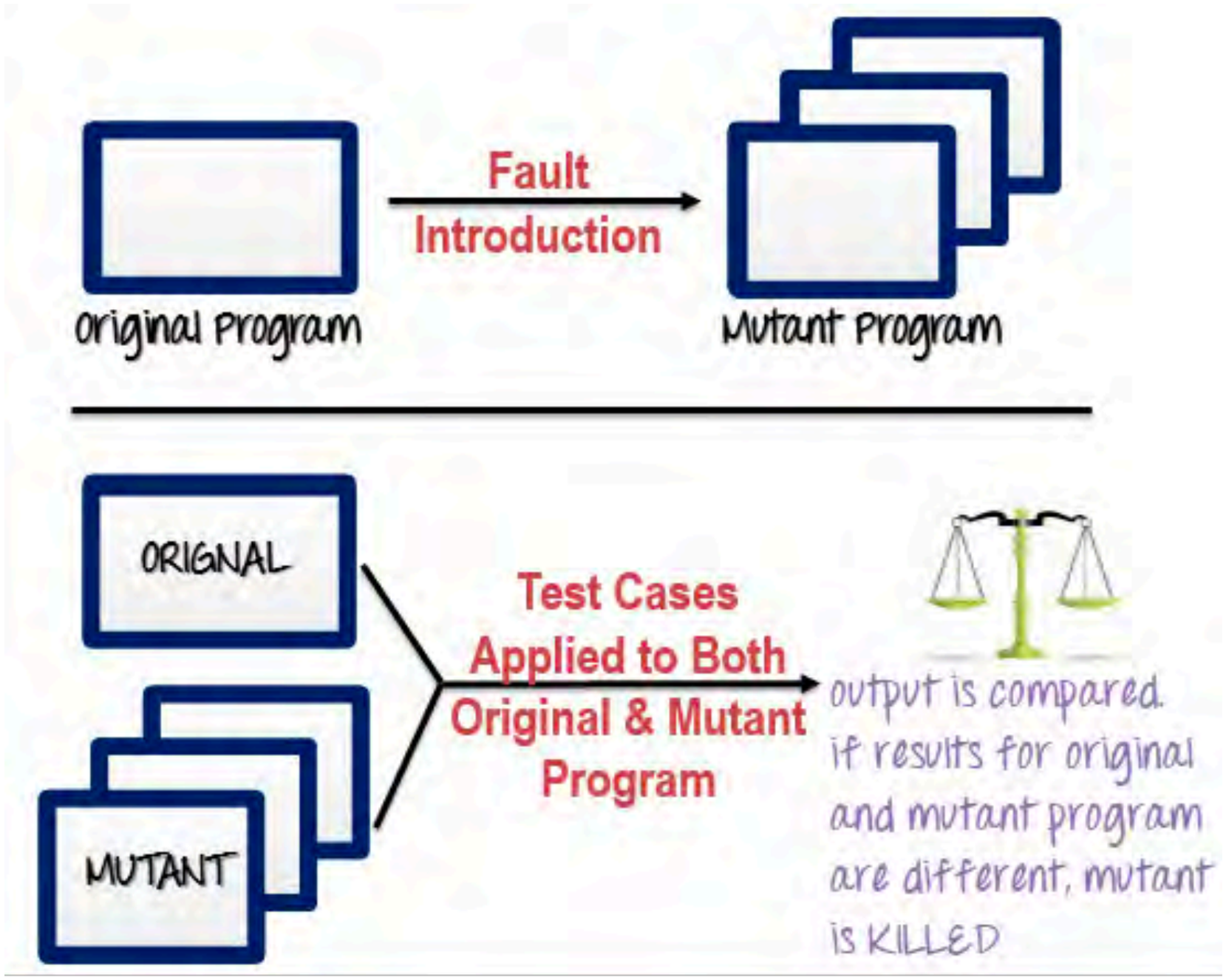
Sanitizer

- AddressSanitizer
- MemorySanitizer
- ThreadSanitizer
- LeakSanitizer



https://www.geeksforgeeks.org/software-testing-mutation-testing/

Mutation

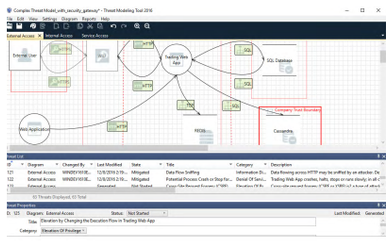


https://www.guru99.com/mutation-testing.html

Cryptography

https://www.kerryveenstra.com/cryptosystem.html

Continuous Integration Stage



Design

Review Architecture

Coding Tests

Static Tests

Dynamic Tests

Threat Modeling

Input Validation

Config Management

Cryptography

Auditing

PCI, HIPPA

Authentication

Authorization

Fuzz tests

Contract First

Contract

Lint

Stress

Sanitizer

Component

Benchmark

Mutation

Dependency Checker

GitRob

Checkmarx

SonarQube

Coverity

Blackduck

OWASP ZAP

Lynis

OpenVas

evident.io

GAUNTLT

Burp Suite

Key Principles of GDPR

Personal Data must be handled according to the key principles.

LEGITIMATE PURPOSE

Personal Data can only be collected for a legitimate purpose. Data use must be limited, explicit and for specific purposes.

DATA DELETION

Personal Data must be deleted if it is no longer required for the original purpose.

SECURE

Data must be kept secure and measures put in place to prevent unauthorised access, disclosure, loss, destruction or alteration.

CONSENT

Consent to collect and store personal data must be 'freely given, specific, informed, and unambiguous'. It can be revoked.

ACCURATE

Personal Data collected must be accurate and kept up to date.

ACCOUNTABLE

Data is handled according to GDPR principles and demonstrate compliance via record keeping and reporting.

Individual Rights under GDPR

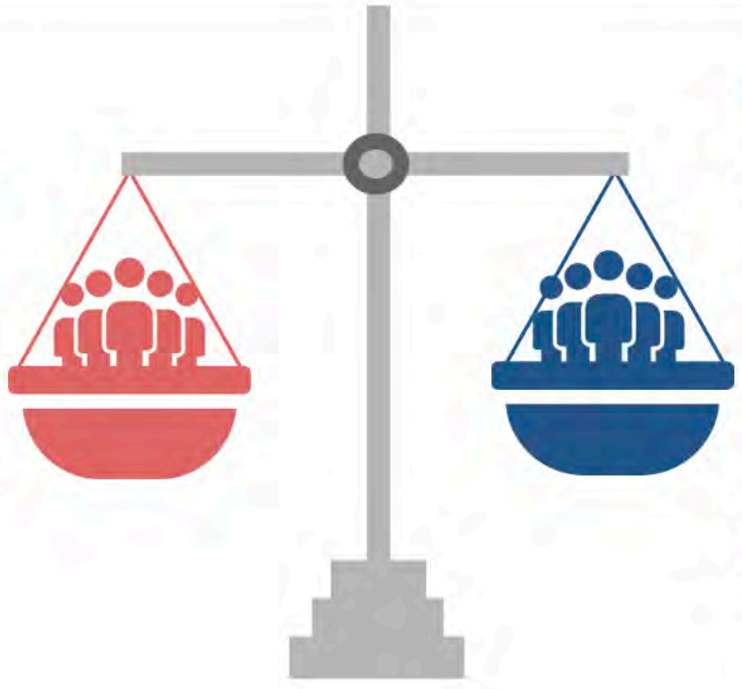
Individuals have a number of rights concerning their personal data.

RIGHT OF ACCESS

Individuals have the right to know exactly what information is held about them and how it is processed.

RIGHT OF RECTIFICATION

Individuals have the right to have inaccurate or incomplete personal data rectified.



RIGHT TO BE INFORMED

Organizations must be completely transparent in how they are using personal data.

RIGHT TO ERASURE

Individuals have the right to have their personal data deleted or removed in certain situations.

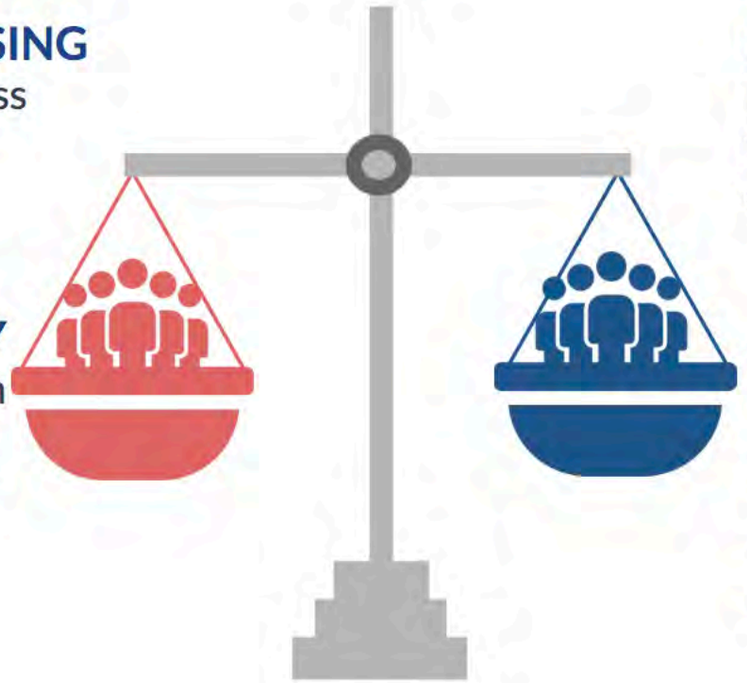
Individual Rights under GDPR

RIGHT TO RESTRICT PROCESSING

Individual's right to block or suppress processing of their personal data.

RIGHT TO DATA PORTABILITY

Right to receive the personal data in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller.

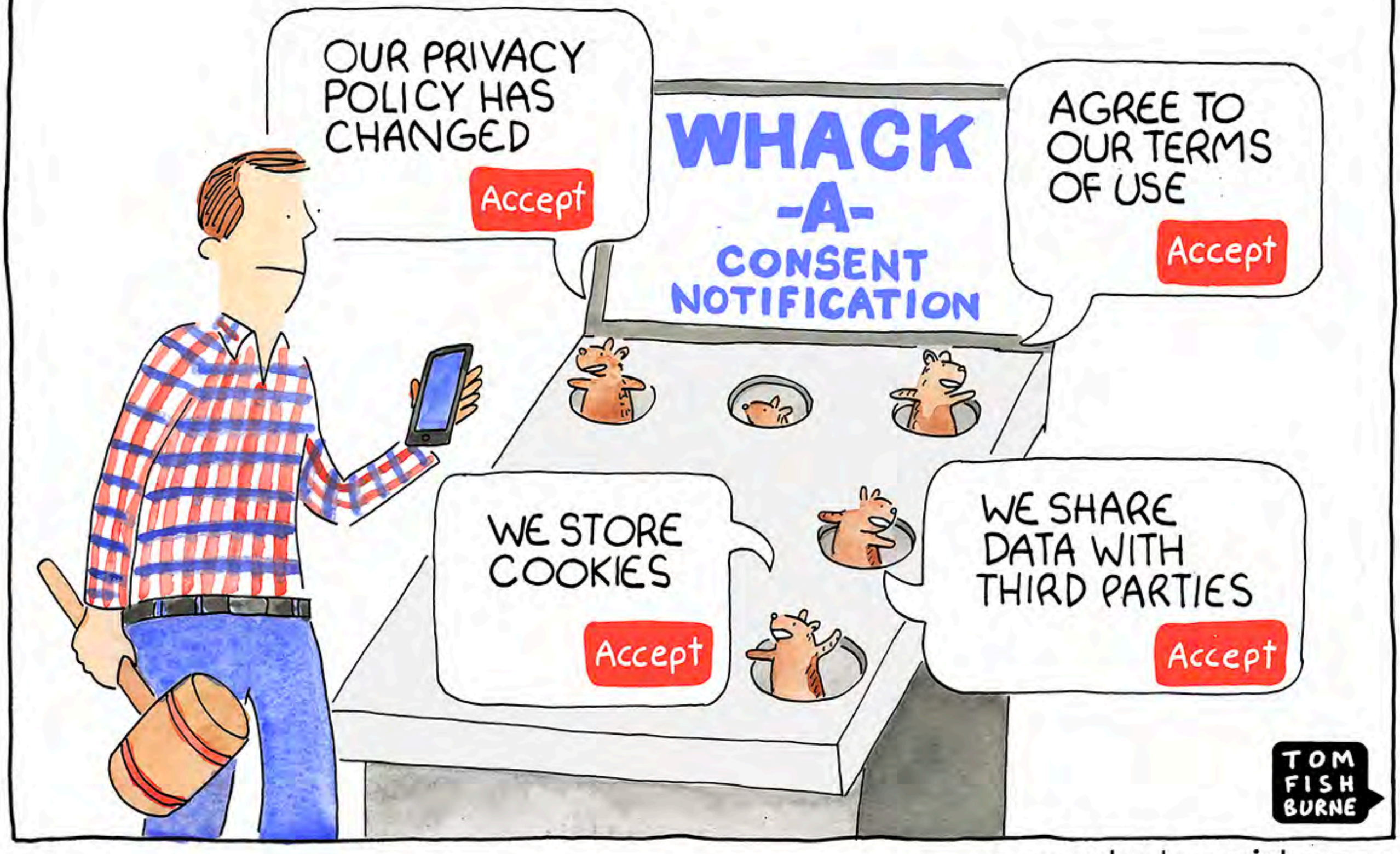


RIGHT TO OBJECT

Individuals have the right to object to their personal data being used, e.g. for direct marketing.

RIGHTS OF AUTOMATED DECISION-MAKING & PROFILING

Right not to be subject to a decision based solely on automated processing, including profiling.



https://marketoonist.com/2019/05/data-privacy-consent-fatigue-and-gdpr.html

Examples of Personal and Sensitive Personal Data

PERSONAL DATA

- Name
- Title
- Address
- Phone number
- Date of birth
- Email address

SENSITIVE DATA

- Social security numbers
- Bank account numbers
- Passport information
- Healthcare related information
- Medical records and insurance information
- Credit and debit card numbers
- Drivers license and State ID information

Data Retention Policy

A data retention policy is a statement of how long data will be stored by the organization including how the data is deleted or otherwise treated.

		
Companies are **obligated to erase personal data** when "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed".	Data needs to be **catalogued** and lists the **type** of data, **purpose**, how it is used and the **classification** level.	Need to define how long the data is required, **when** it will be **deleted, anonymized or archived**.

Remember

- Lock down the root user
- Security groups only allow. Network ACLs allow explicit deny
- Prefer IAM Roles to access keys

Design Resilient Architectures

Design Cost-Optimized Architectures

Sustainability Architectures

Design Performant Architectures

Operationally Excellent Architectures

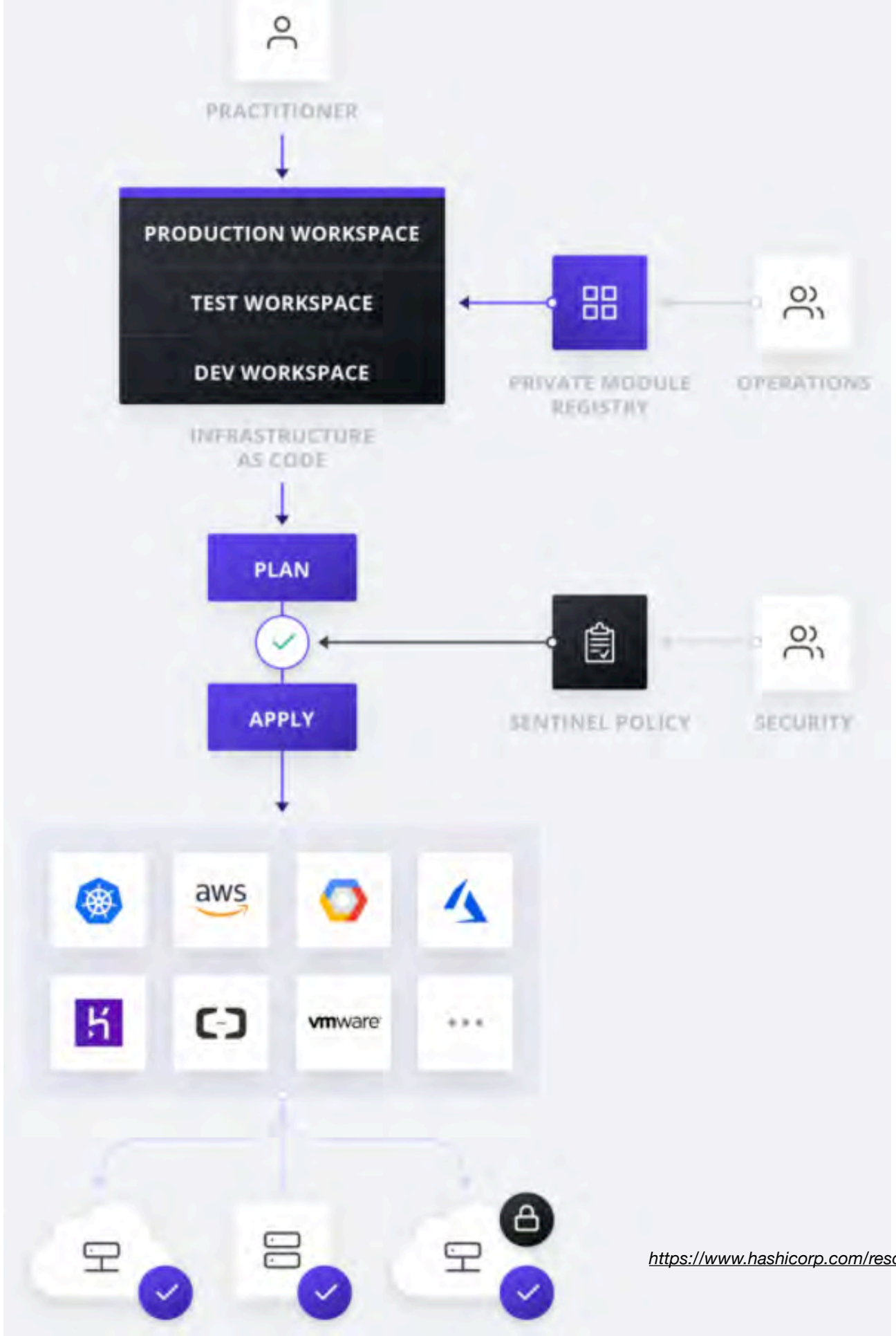
Specify Secure Applications

Well Architected Framework

Operational Excellence

Perform Operation Infrastructure as code

Vendor lockin



https://www.hashicorp.com/resources/enabling-multi-cloud-with-hashicorp-terraform

Continuous Deployment Stage

Infrastructure Testing

Release Testing

Monitoring

Incident Response

Production Testing

Infrastructure

Load Tests

Shadowing

Network

Soak

Tap Compare

Canary

Traffic Shaping

Feature toggle

Exception

Metrics

Nagios

AWS Cloud Watch

Traffic Shaping

Exception Tracking

API Gateways

Slack integration

ChatOps

JIRA

PagerDuty

Cyphon

Diagnostic

Profiling

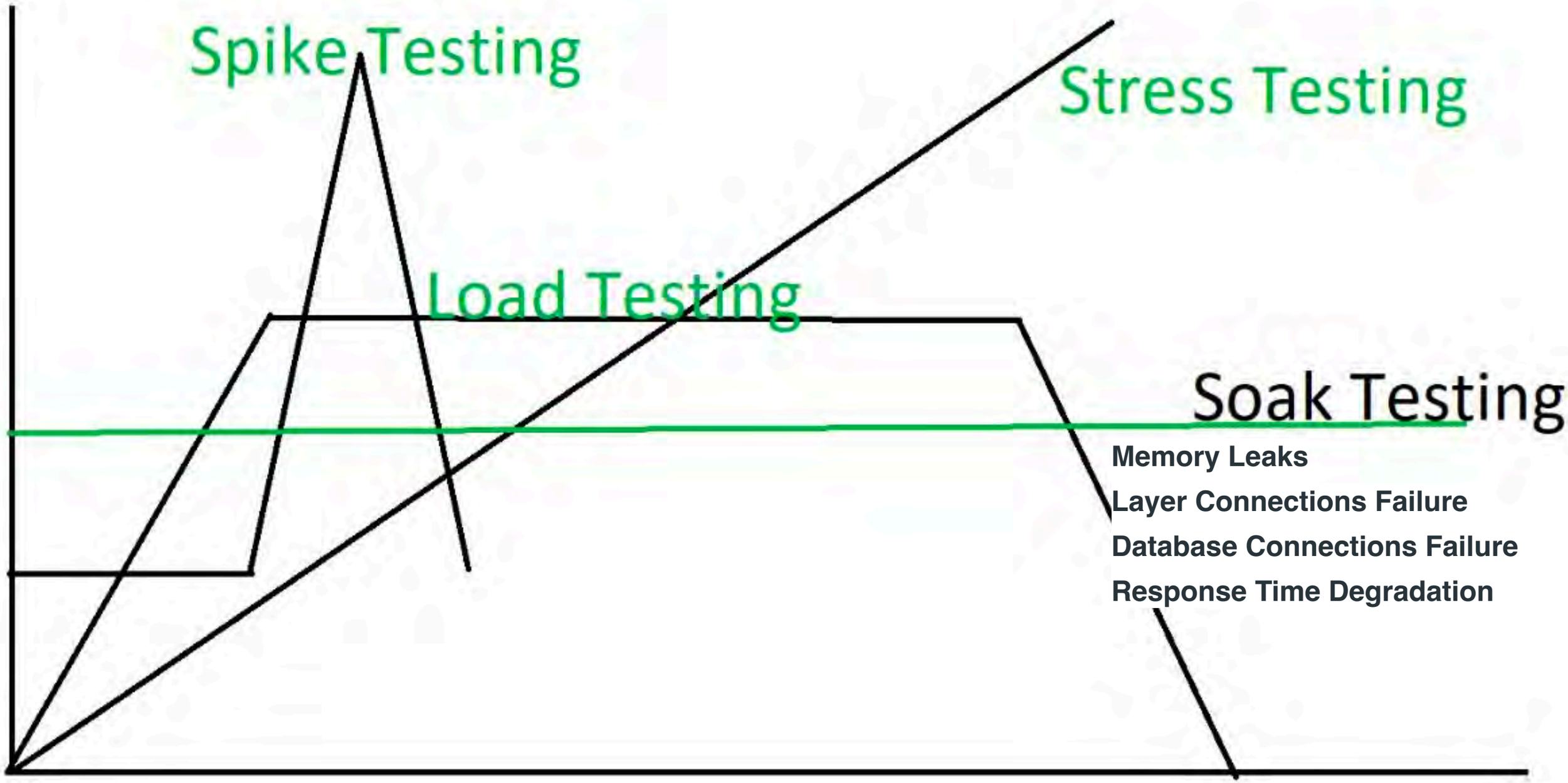
Chaos

Recovery

A/B Tests

Tracing

Auditing



https://www.geeksforgeeks.org/soak-testing/

mockaroo SCHEMAS DATASETS SCENARIOS APIS PROJECTS

New Schema

Field Name	Type	Options
id	Row Number	blank: 0 %
first_name	First Name	blank: 0 %
last_name	Last Name	blank: 0 %
email	Email Address	blank: 0 %
gender	Gender	blank: 0 %
ip_address	IP Address v4	blank: 0 %

Add another field

Rows: 1000 Format: CSV Line Ending: Unix (LF) Include: header BOM

Download Data Preview Save This Schema More

https://www.mockaroo.com/help/scenarios

generatedata.com

Login | English

Generate | About | News | Donate

Datasets

SAVE

COUNTRY-SPECIFIC DATA

All countries

DATA SET

Order	Column Title	Data Type	Examples	Options	Help	Del
1	Name	Names	John Smith	MaleName Surname	?	
2	Phone	Phone / Fax	Canada (1)	1-Xxx-Xxx-xxxx	?	
3	Address	Street Address	No examples available.	No options available.	?	
4	Zip	Postal / Zip	No examples available.		?	
5	isEmployee	Boolean	Yes or No	Yes|No	?	
Order	Column Title	Data Type	Examples	Options	Help	Del

Add 1 Row(s)

EXPORT TYPES

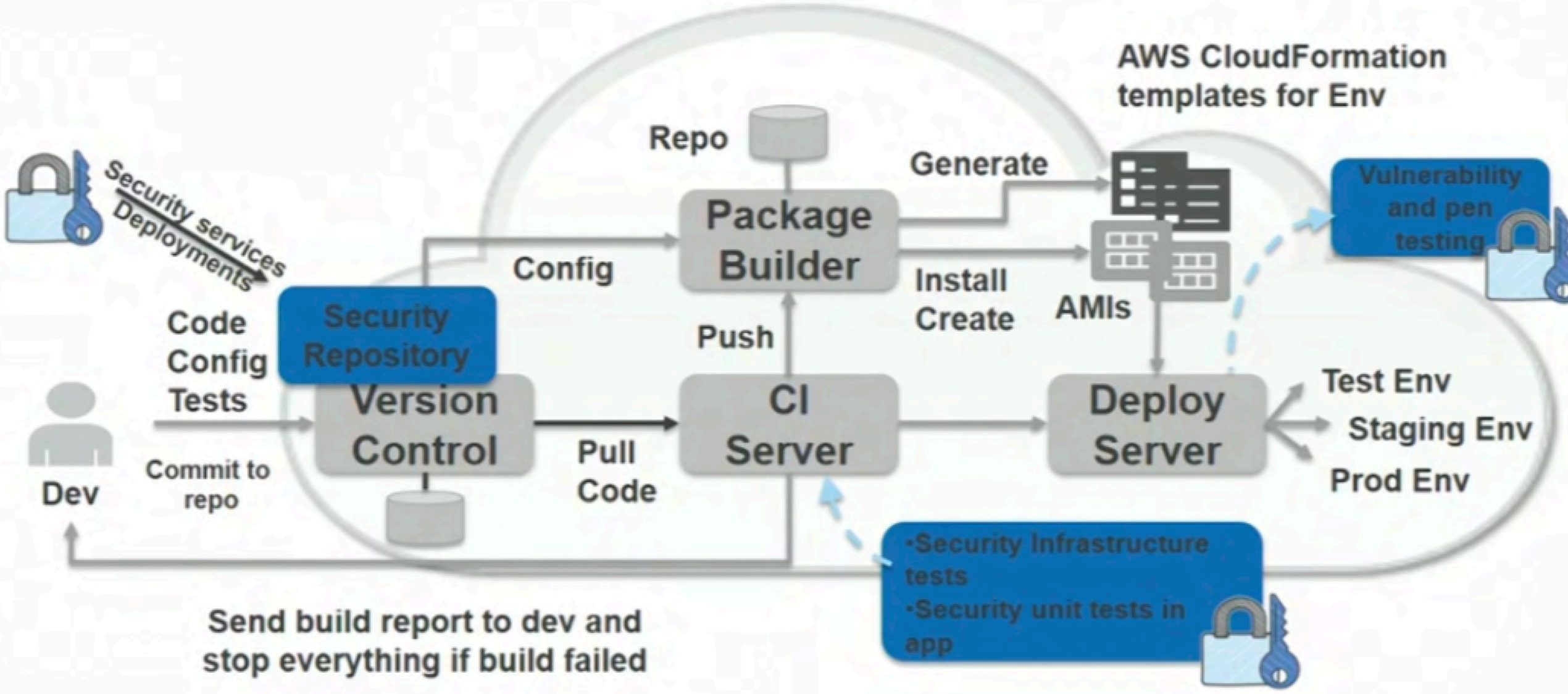
CSV | Excel | HTML | JSON | LDIF | Programming Language | SQL | XML — hide data format options

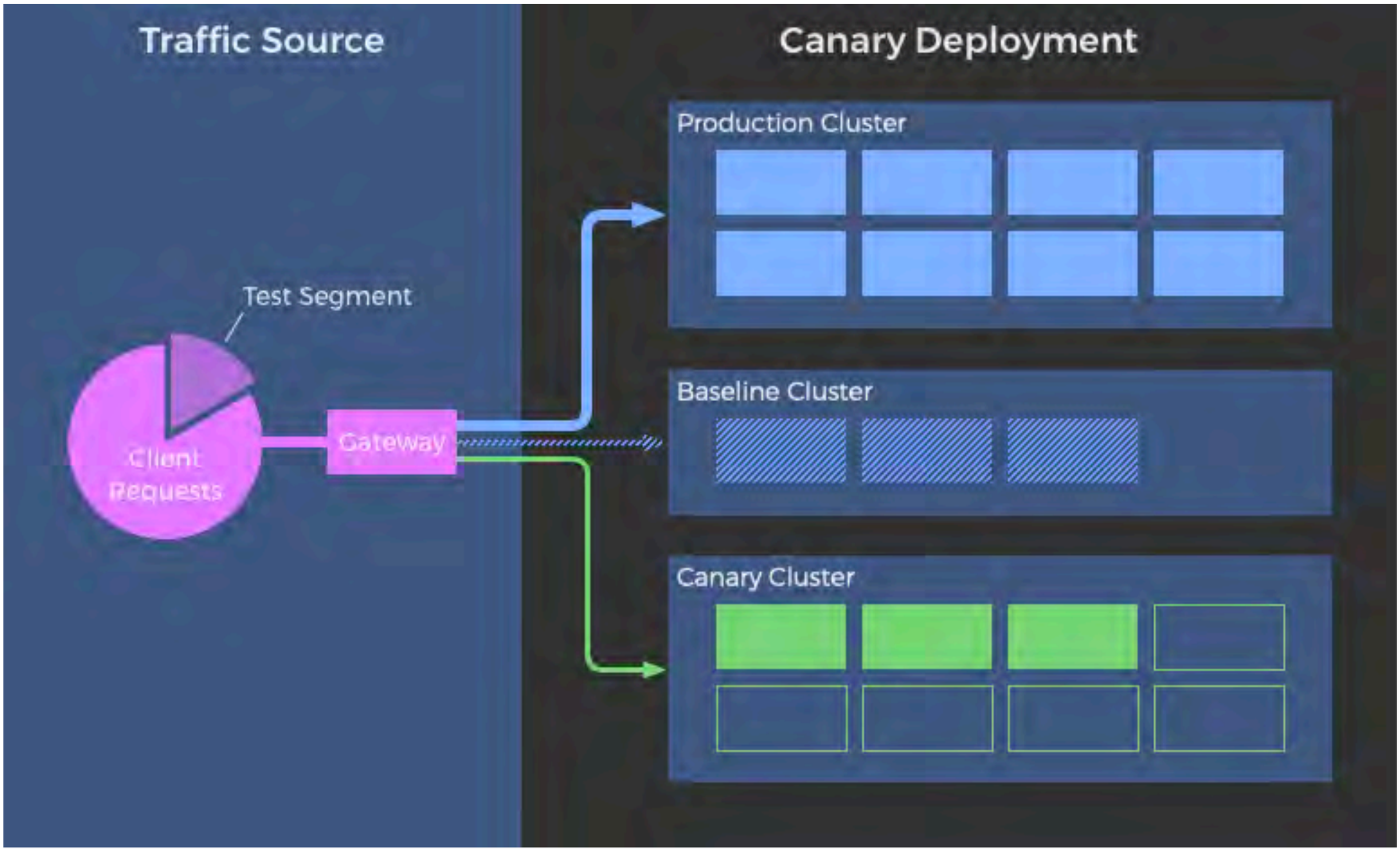
Delimiter char(s) | End of line character: Mac

Generate 100 rows | Generate in-page | New window/tab | Prompt to download | Generate

https://generatedata.com/

3.4.1 | Documentation | Report a bug

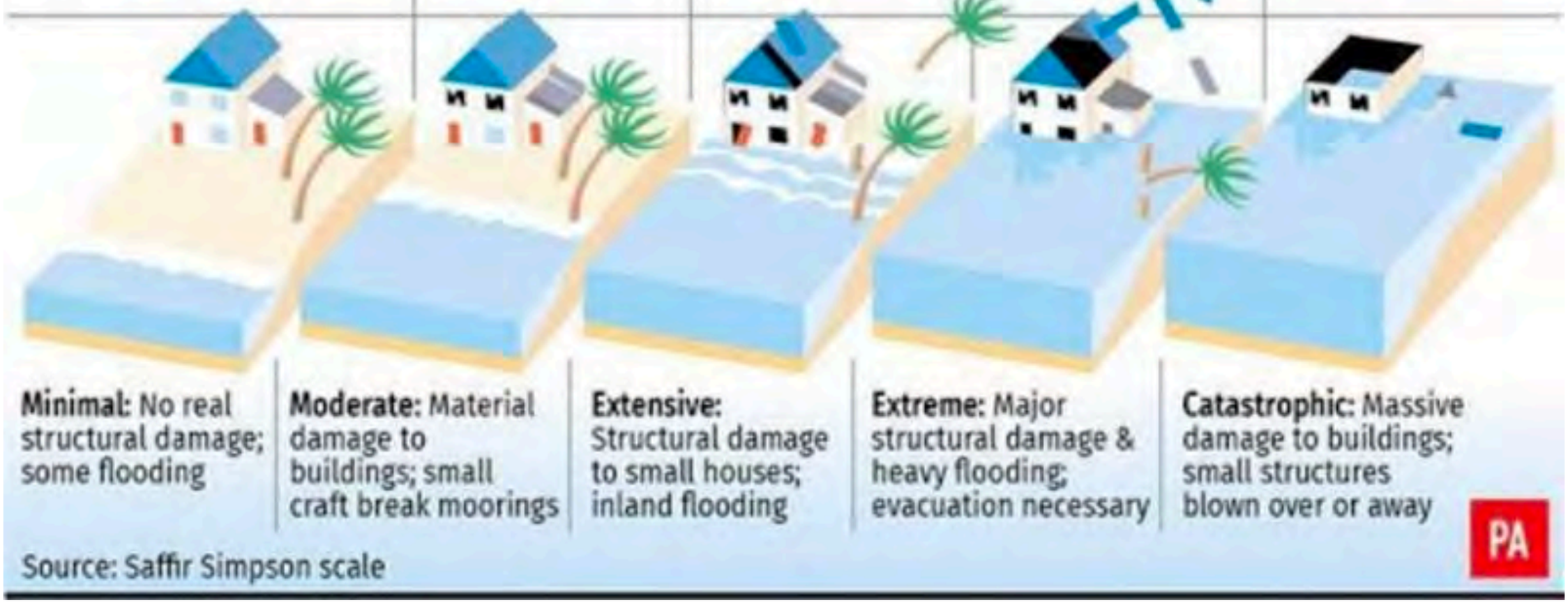

AWS CloudFormation templates for Env
Repo
Generate
Package Builder
Config
Install Create
AMIs
Vulnerability and pen testing
Security services Deployments
Code
Config
Tests
Security Repository
Push
Version Control
CI Server
Deploy Server
Test Env
Staging Env
Prod Env
Commit to repo
Dev
Pull Code
•Security Infrastructure tests
•Security unit tests in app
Send build report to dev and stop everything if build failed



https://glasnostic.com/blog/how-canary-deployments-work-1-kubernetes-istio-linkerd

Categories of hurricane

	Category 1	Category 2	Category 3	Category 4	Category 5
Wind	74-95mph	96-110mph	111-130mph	131-155mph	Over 155mph
Storm surge	4-5ft	6-8ft	9-12ft	13-16ft	Over 18ft



Essential Features

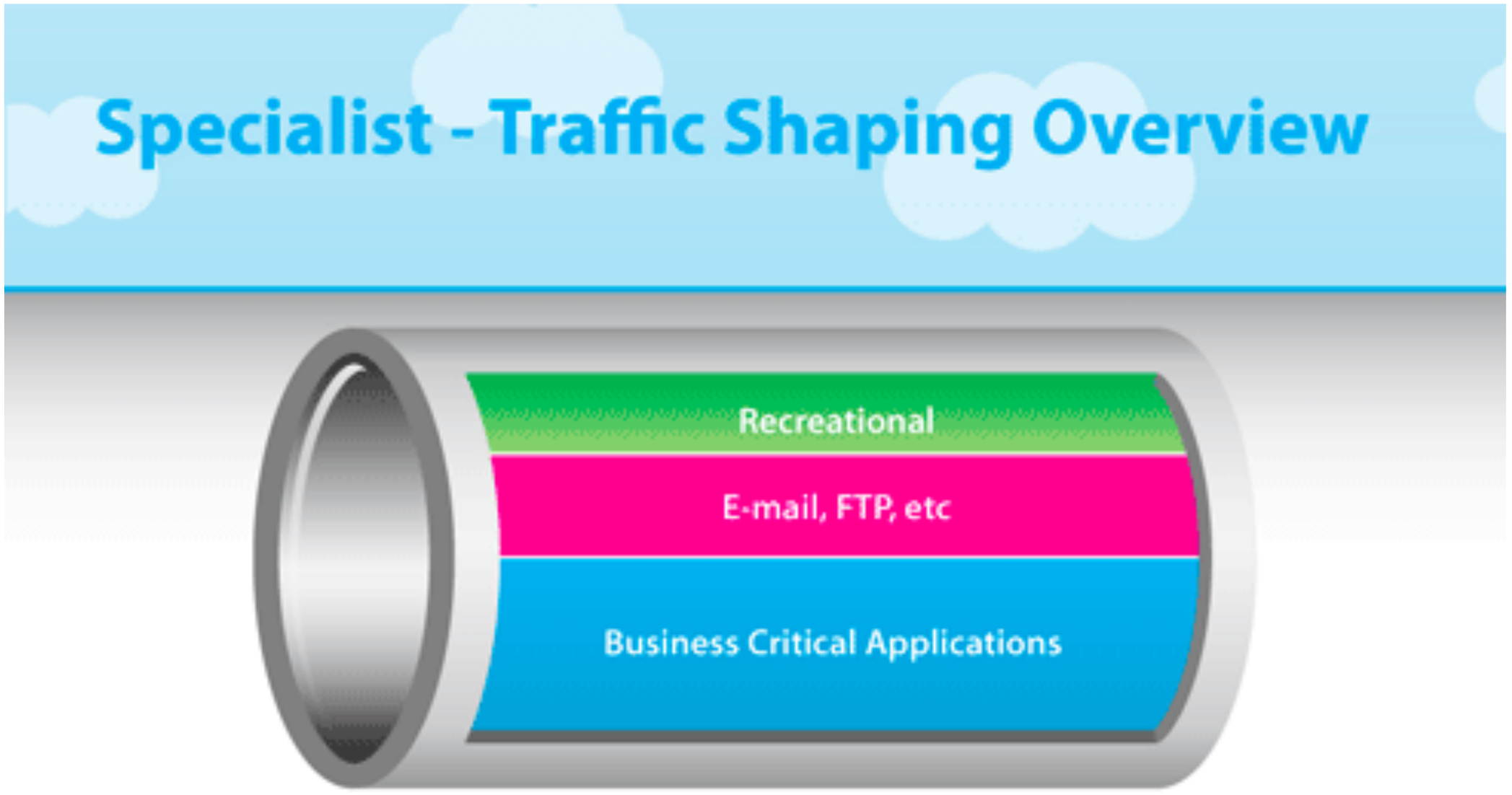
Non Essential Features

https://earthsky.org/earth/hurricane-dorian-why-its-so-destructive/attachment/hurricane-categories-chart/

Specialist - Traffic Shaping Overview

Usage without shaping.

https://linebroker.co.uk/trafficshaping.php



Usage with shaping.

ChatOps

At Shopify

#war-room

417 | 1 | No incidents right now.

Search

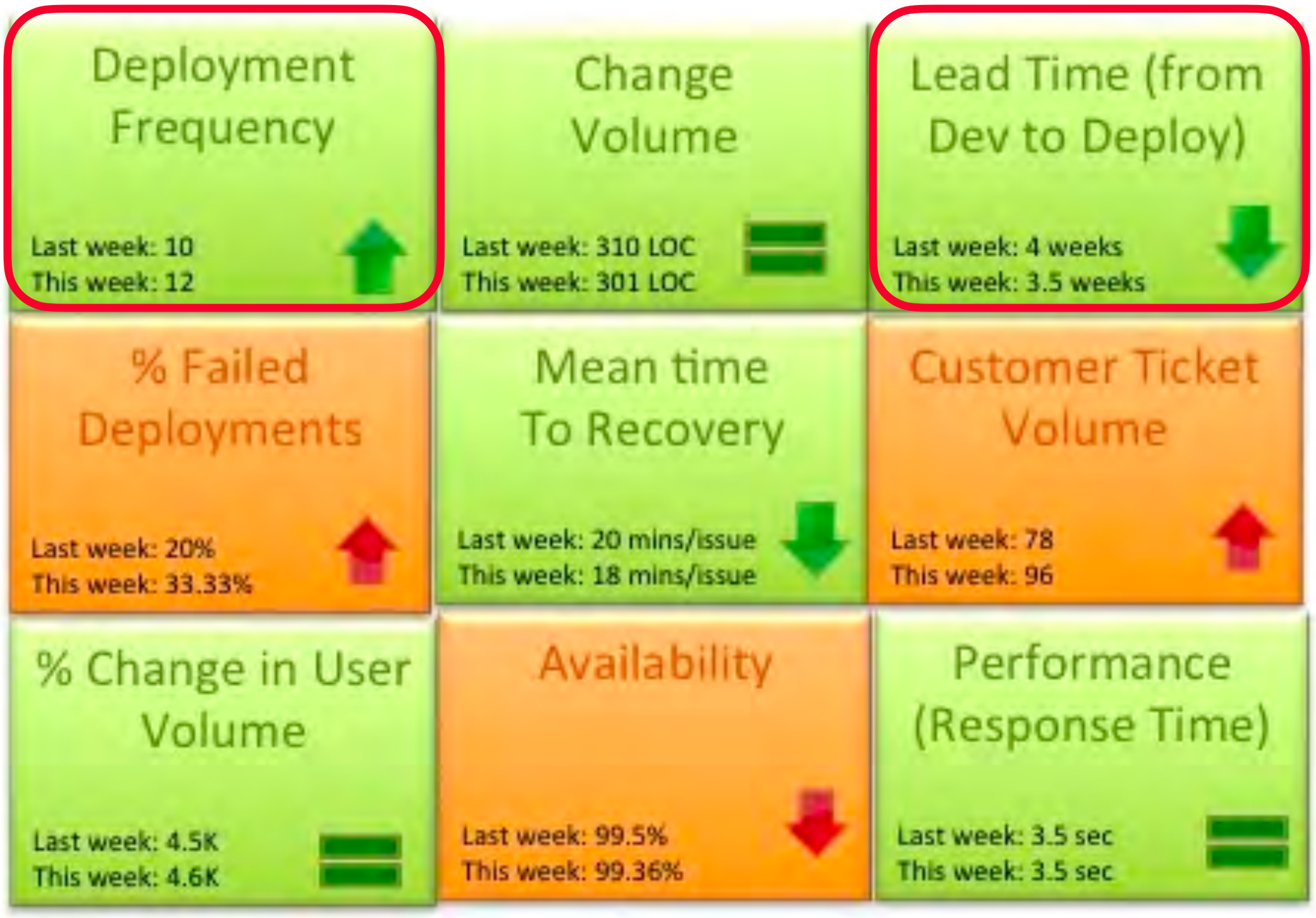
Daniella Niyonkuru 1:23 PM
spy incident start me order fraud analysis outage

spy APP 1:23 PM
🔥 An incident was reported at 2017-04-06 16:25:01 UTC. @daniella is the IMOC.
Status summary: order fraud analysis outage
Incident was bound to #war-room. Please use #war-room for communications, or rebind the incident with /incident channel.

spy APP 1:23 PM
set the channel topic: 🔥 @daniella is IMOC for incident: order fraud analysis outage

[redacted]

spy APP 1:23 PM
Status Page Summary
*** Components Report ***
Admin : operational
Checkout : operational
Reports and Dashboards : operational
Storefront : operational
API & Mobile : operational
Support : operational
Third party services : operational
*** Unresolved Incidents Report ***
No reported unresolved incidents.



https://devopedia.org/devops-metrics

Why Lead time is important?

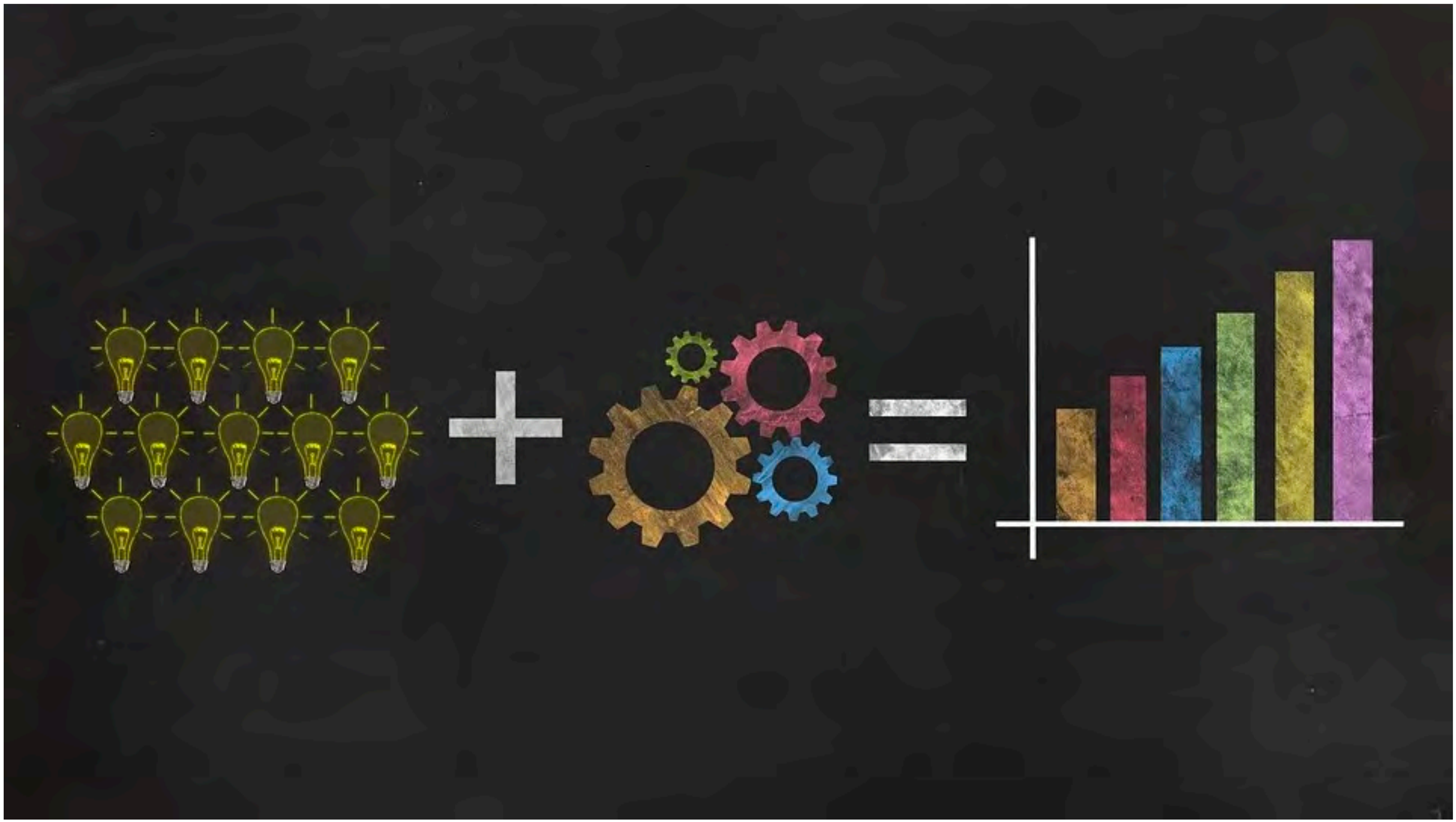
- Indicator of Value
- Realistic SLAs
- Predictability
- Reduce waiting
- Accelerate delivery, stay lean
- Improve performance

Annotate Documentation - PlayBooks - Part of code

Runbooks - Server down

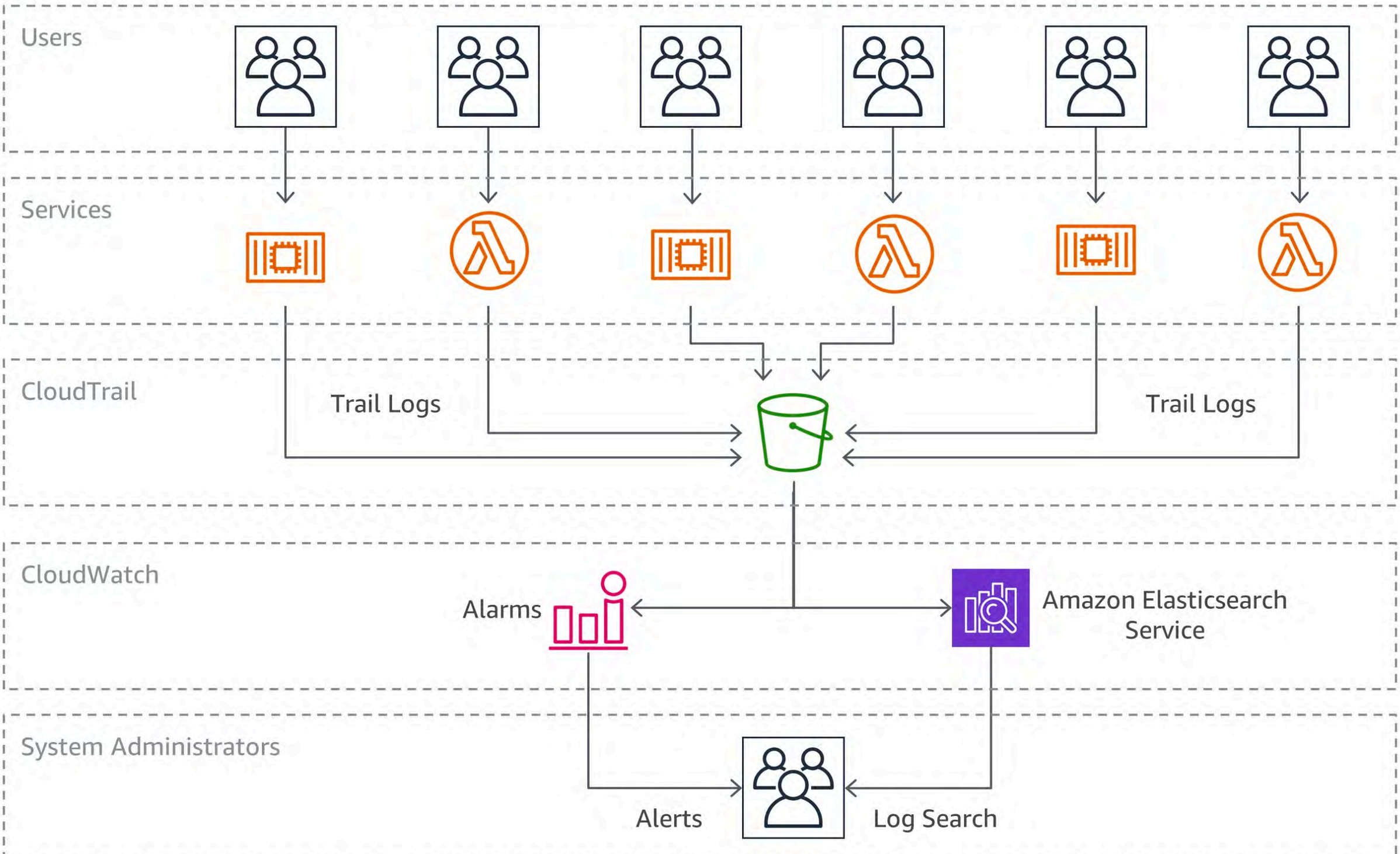
Make frequent, small, reversible changes

Refine operations procedures

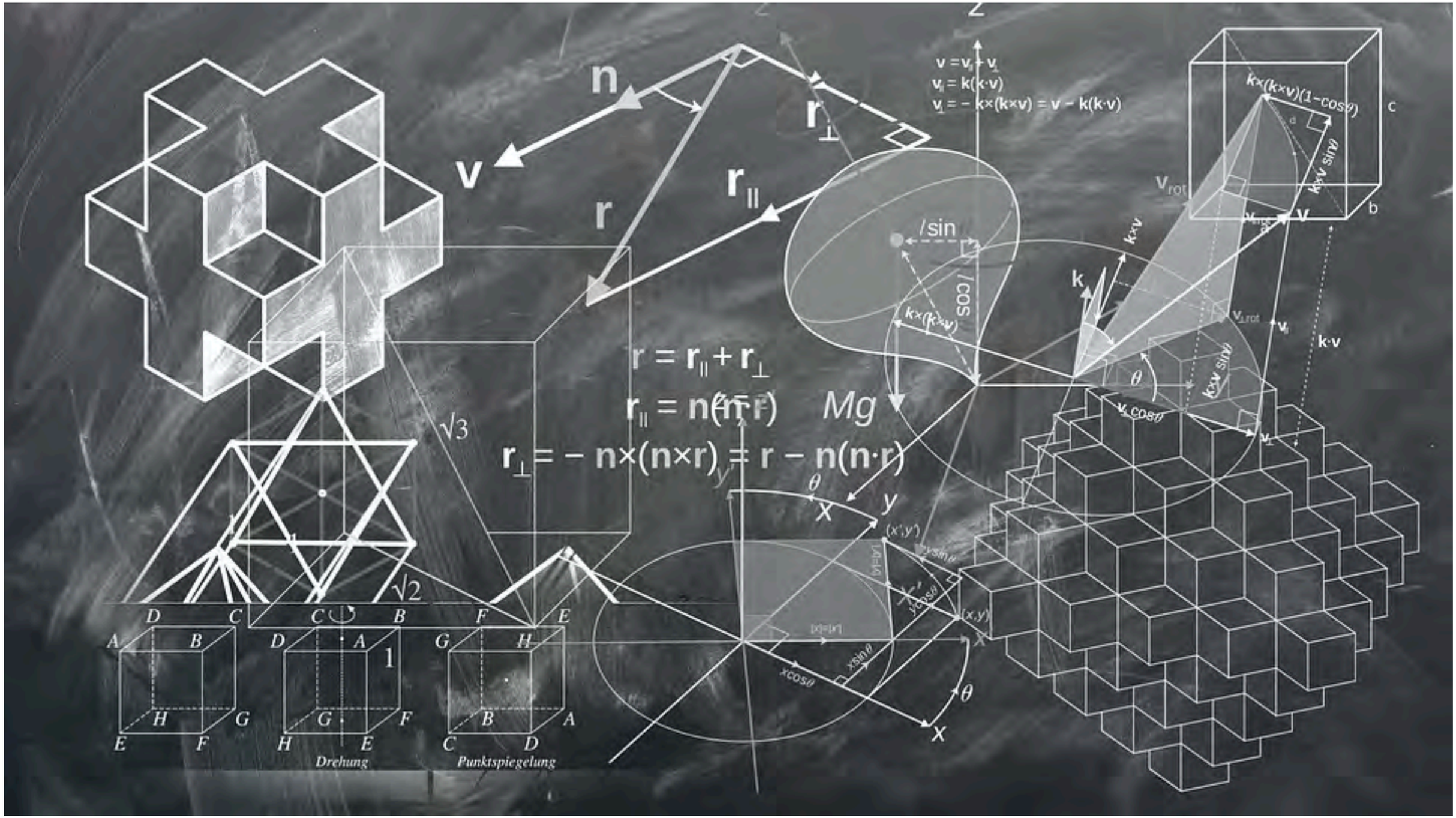


Anticipate Failures

Events and Real-Time Actions

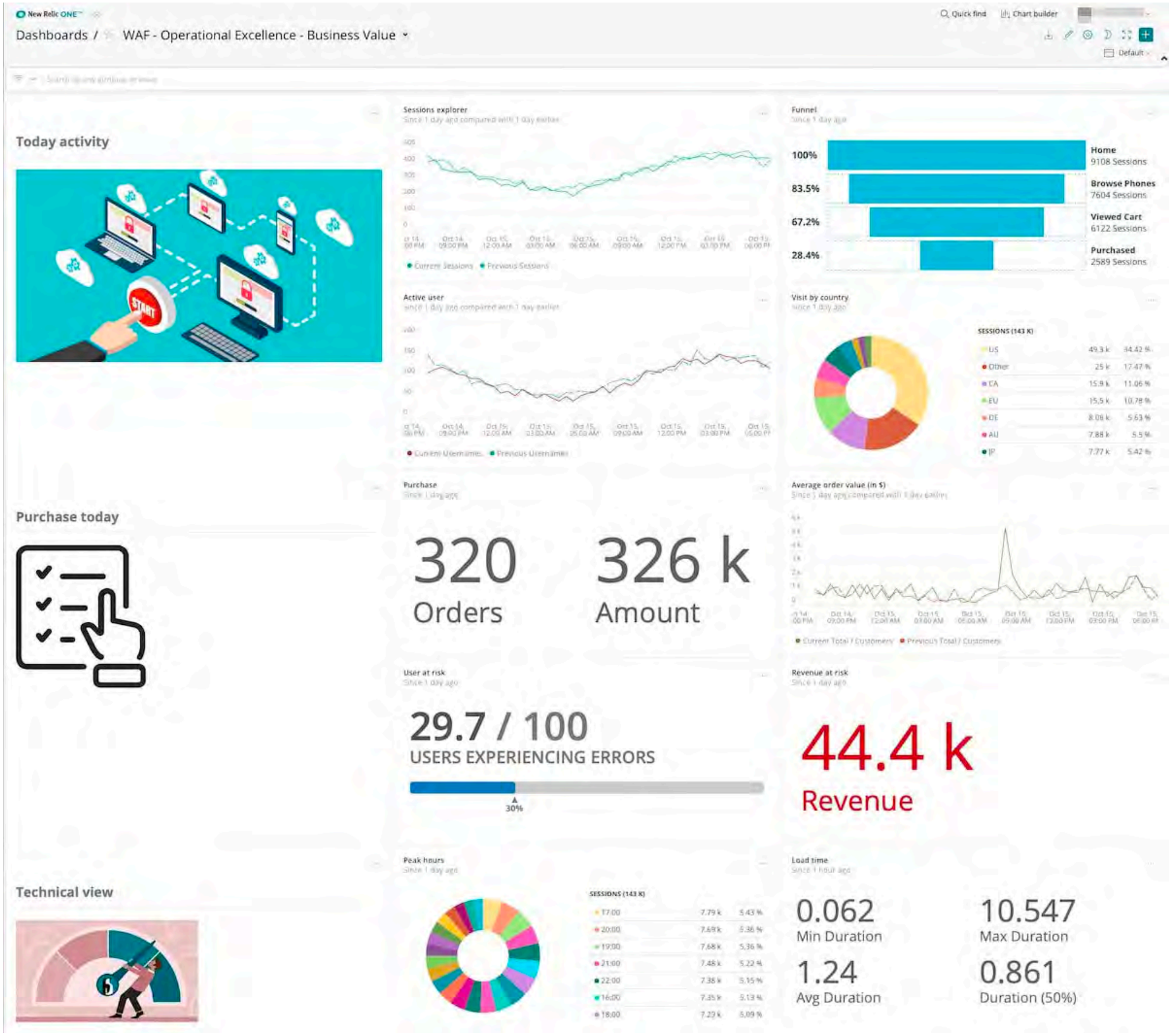


Learn from all Operational failures



How to measure Business Value?

Create a KPI dashboard



How about build changes and KPIs?

APPS Proxy-East

SERVERS All servers

09/12, 21:54 DEPLOYMENT AT | jenkins DEPLOYER | 19 REVISION

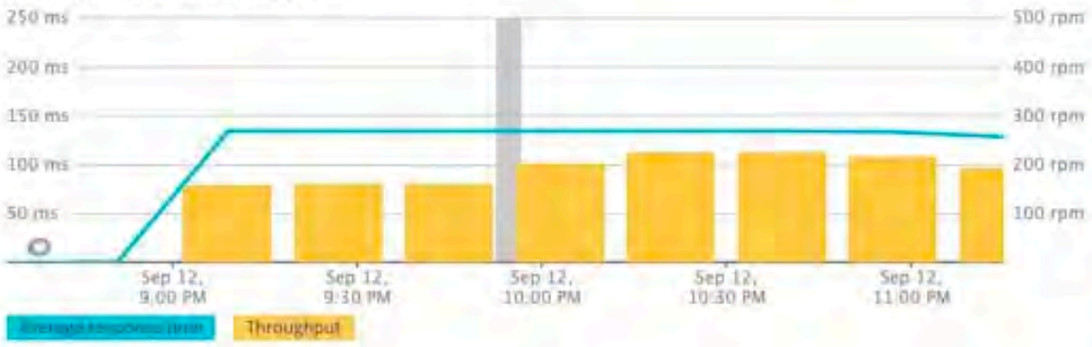
Apdex 0.99 0.5 Errors 0% Resp. time 131 ms CPU NA DB NA Memory 85.45 MB Throughput 211 rpm
PERFORMANCE SUMMARY

← All Proxy-East deployments ↑ Previous deployment

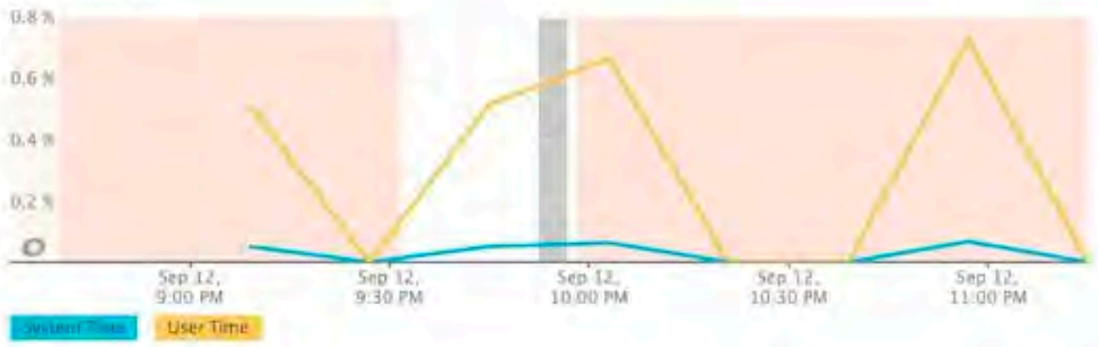
Deploy using master sha: 34a90ecb289d35337877d914d9e343567f7bf927

Overview | Change report

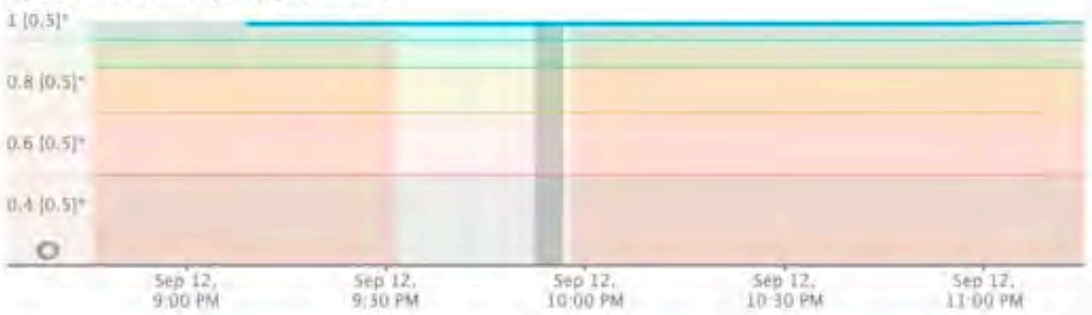
Response time and throughput



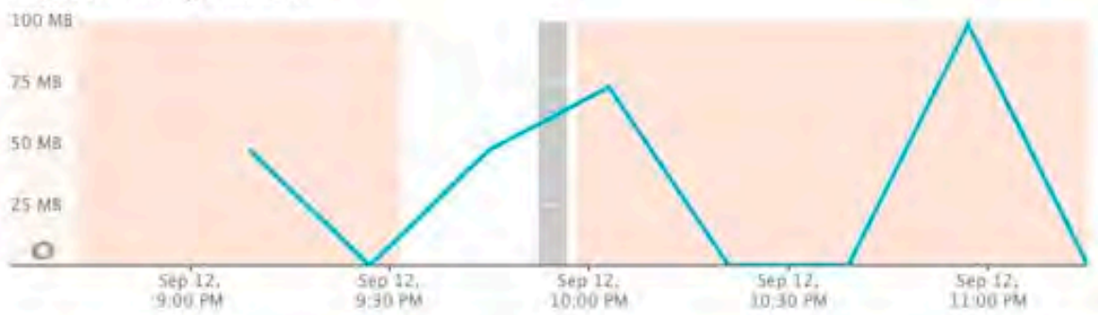
CPU utilization



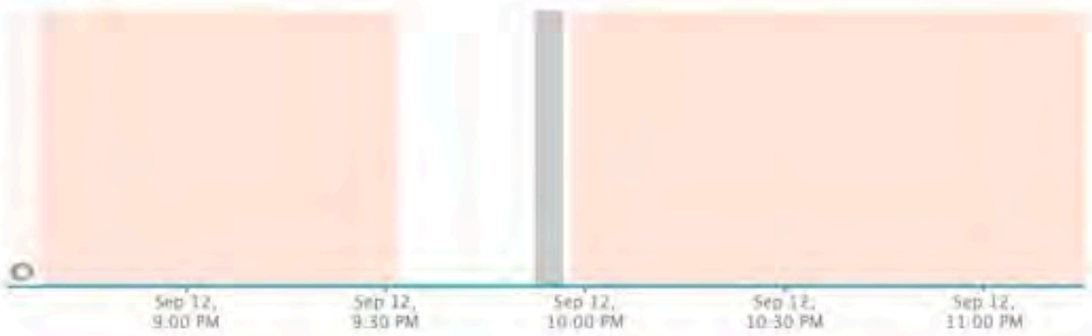
Apdex score: 0.99 [0.5] (Excellent)



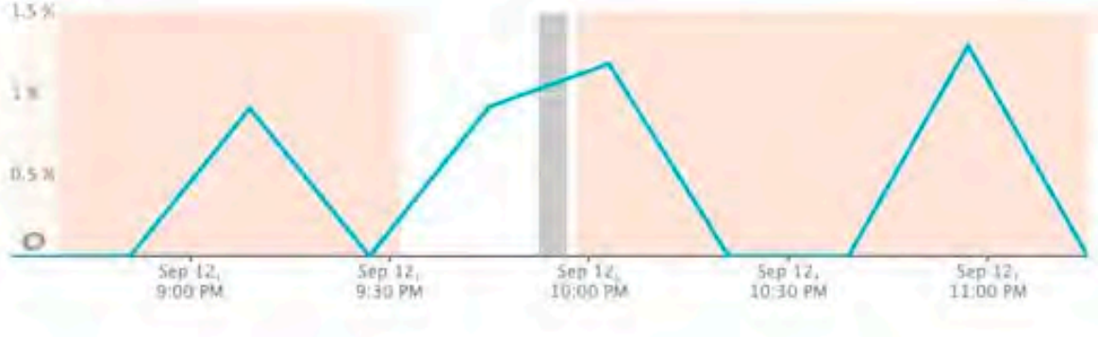
Physical memory utilization

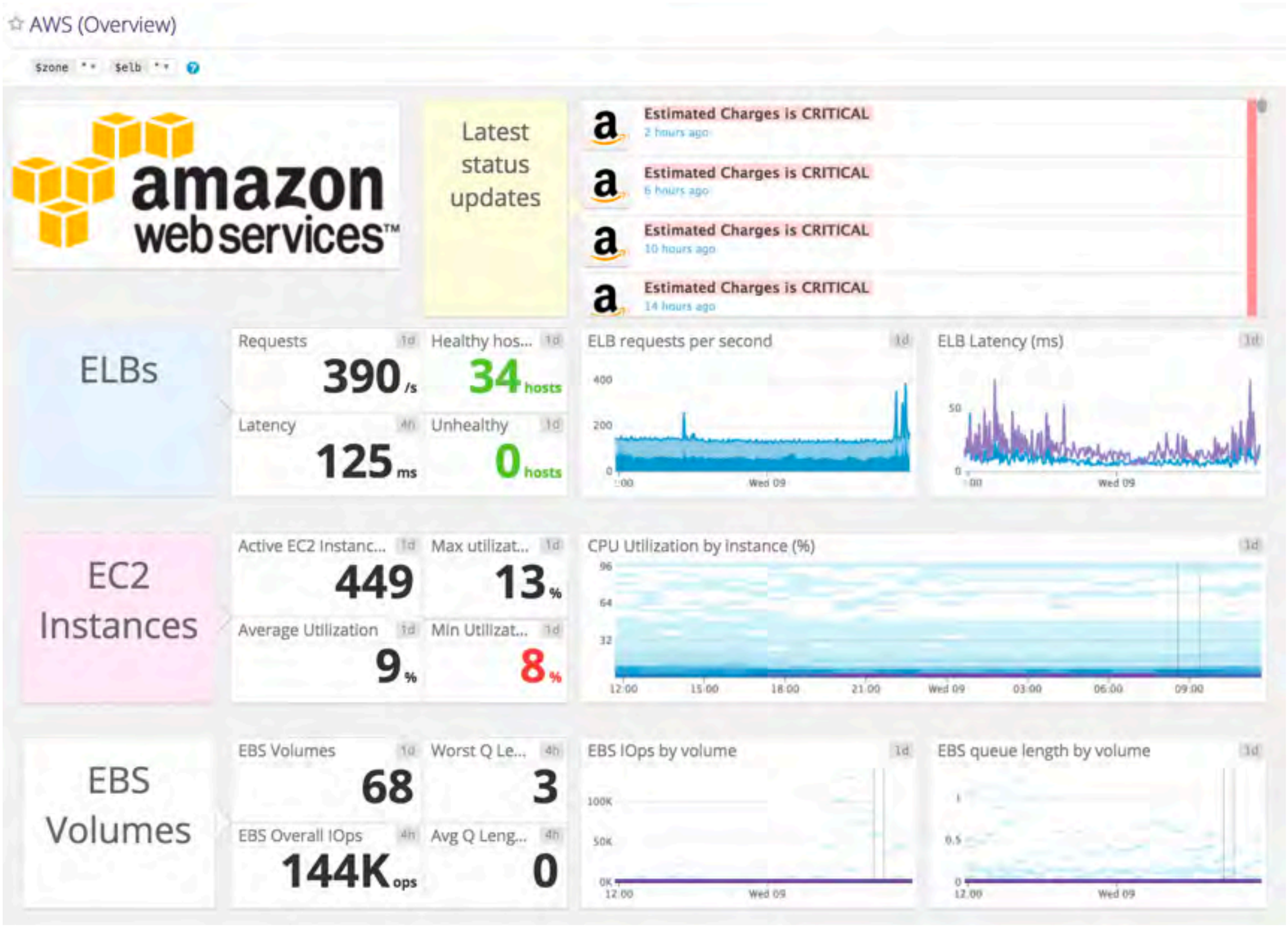


Error rate



Database



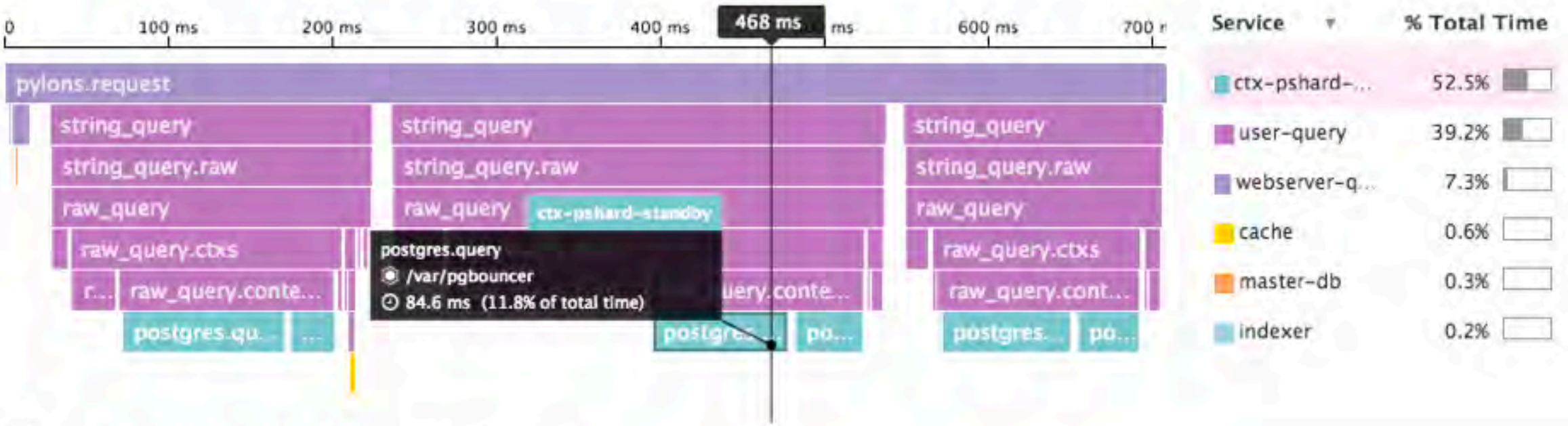


https://aws.amazon.com/blogs/apn/why-next-generation-msps-need-next-generation-monitoring/

webserver-query | user.batch_query

Sep 20 20:38 PM **717 ms** POST /user/batch_query **200 OK**

See trace →

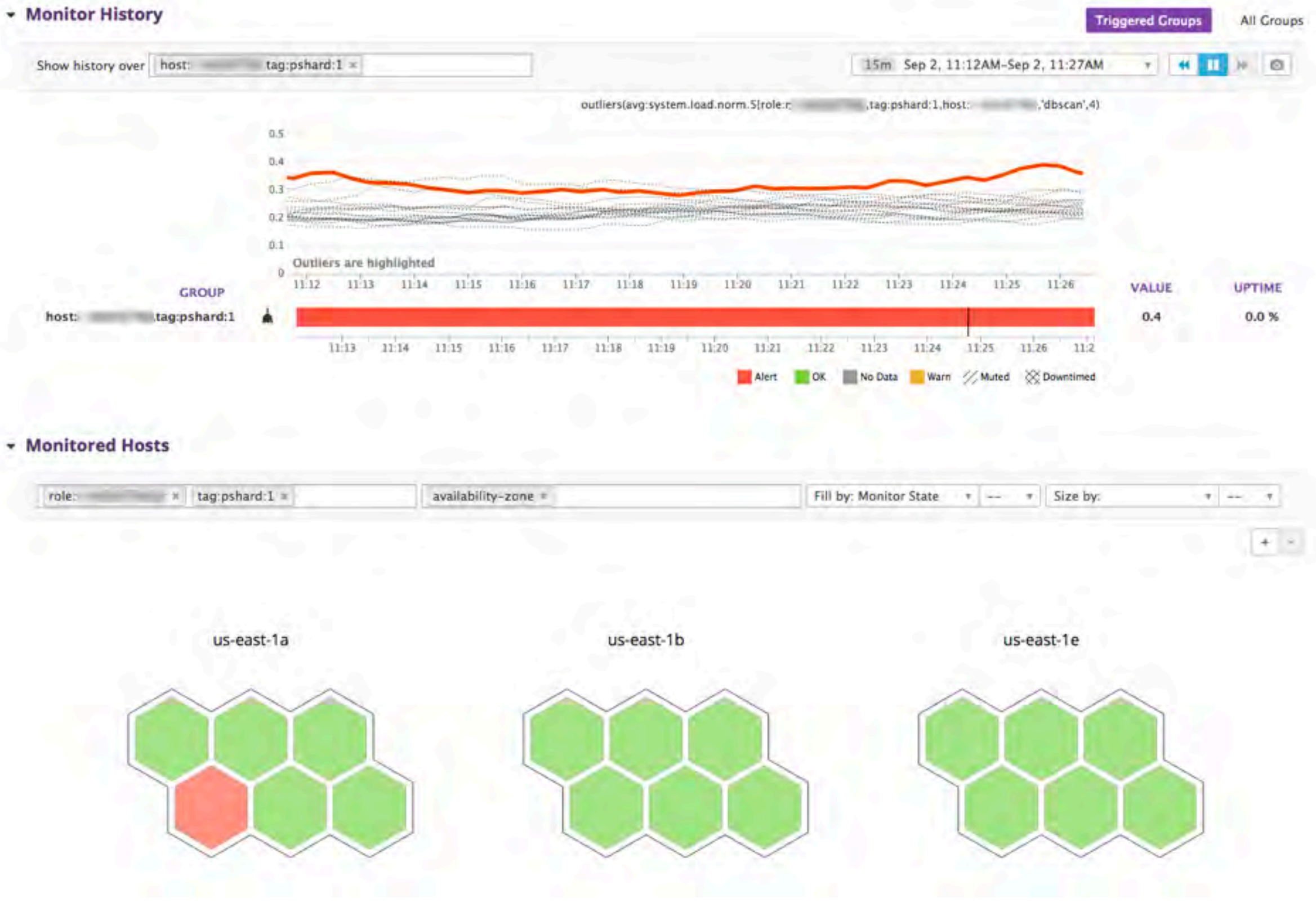


ctx-pshard-standby | postgres.query

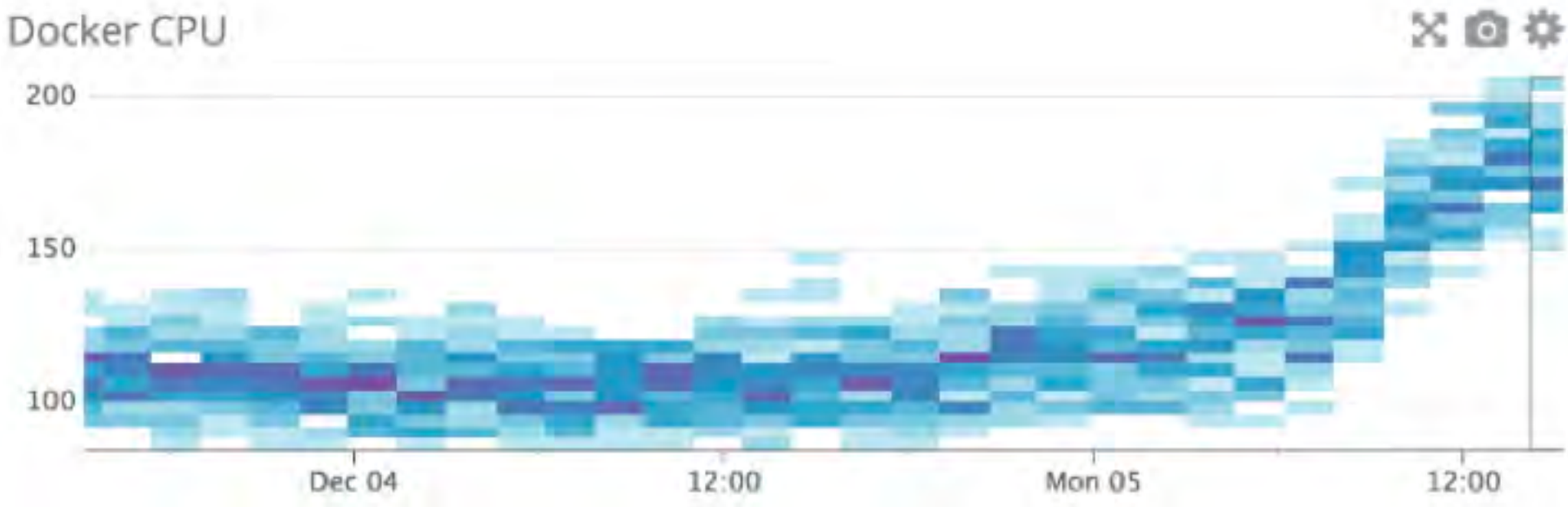
/var/pgbouncer 84.6 ms (11.8% of total time)

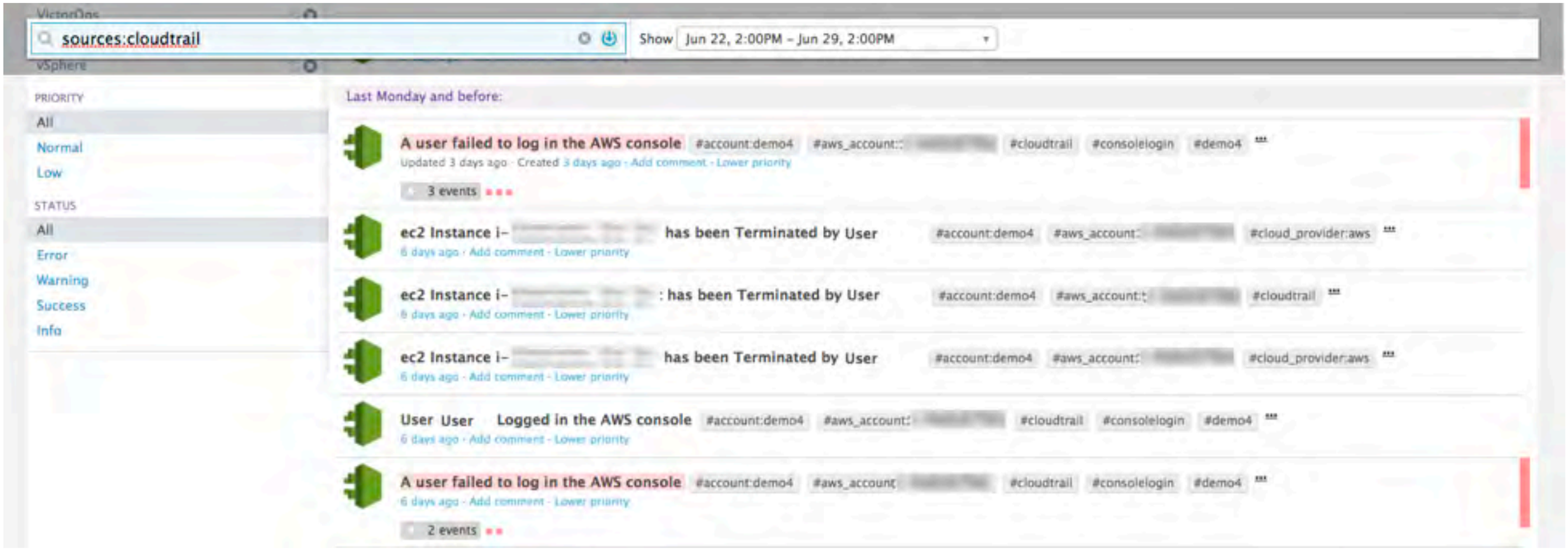
```
-- get_contexts_sub_query[[org:9543 query_id:e4675c5b33 batch:0]]
WITH sub_contexts as (

--
--
SELECT key,
```

Anomaly detection, Outlier Detection

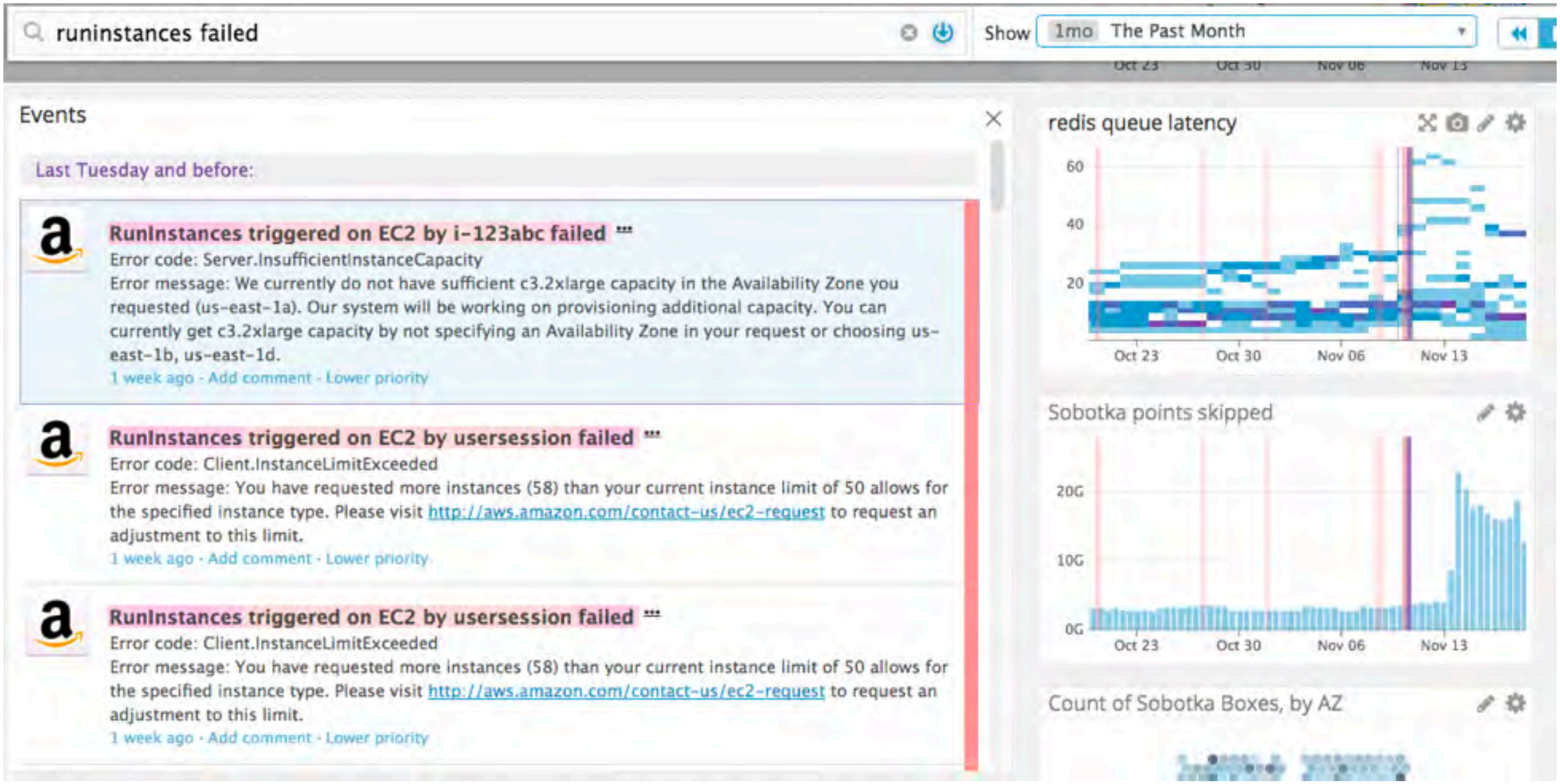


Heat Maps: Docker CPU Usage



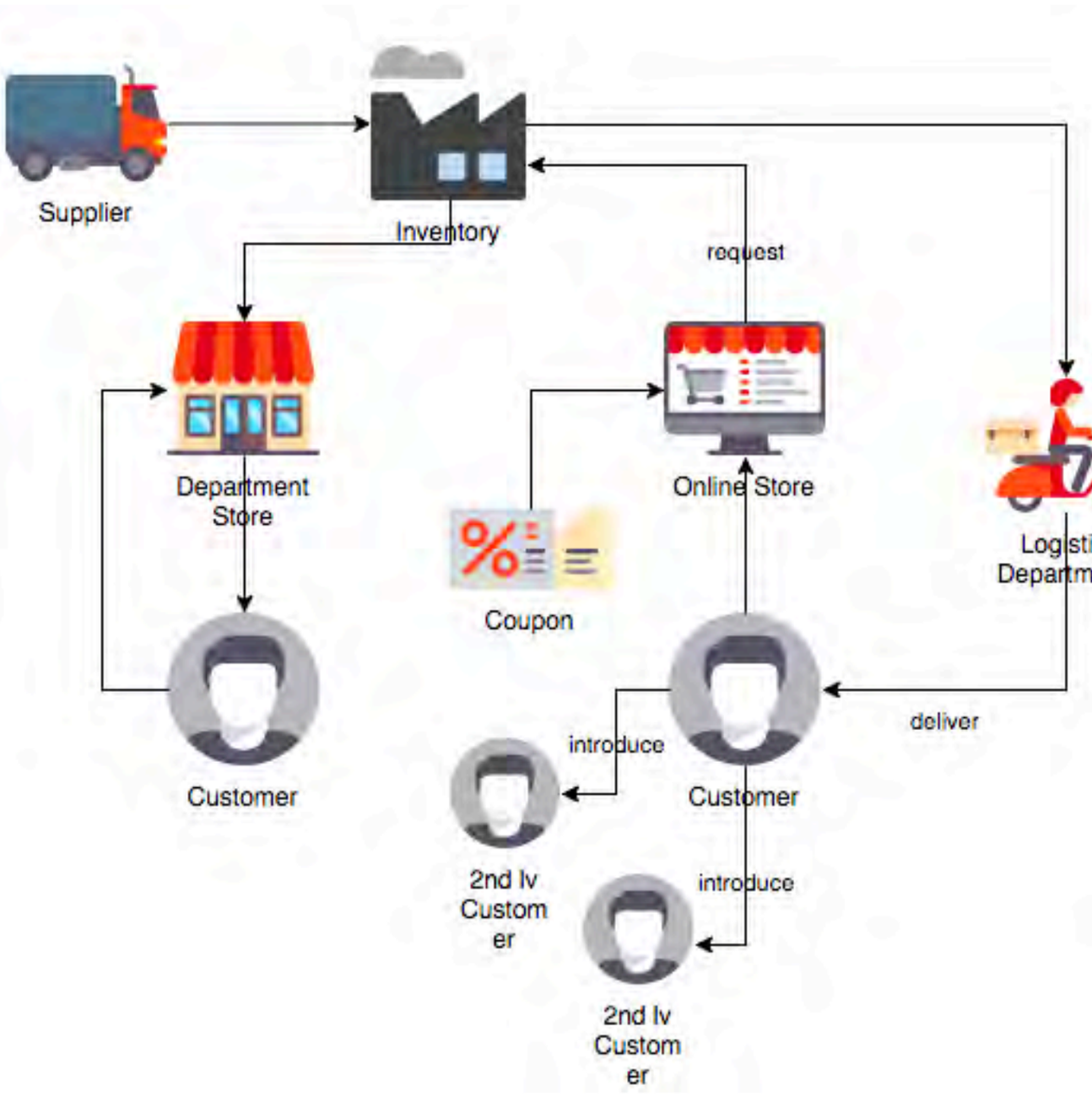

sources:cloudtrail
Show
Jun 22, 2:00PM – Jun 29, 2:00PM
PRIORITY
All
Normal
Low
STATUS
All
Error
Warning
Success
Info
Last Monday and before:
A user failed to log in the AWS console
#account:demo4
#aws_account::
#cloudtrail
#consolelogin
#demo4
Updated 3 days ago · Created 3 days ago · Add comment · Lower priority
3 events
ec2 Instance i-
has been Terminated by User
#account:demo4
#aws_account:
#cloud_provider:aws
6 days ago · Add comment · Lower priority
ec2 Instance i-
: has been Terminated by User
#account:demo4
#aws_account:
#cloudtrail
6 days ago · Add comment · Lower priority
ec2 Instance i-
has been Terminated by User
#account:demo4
#aws_account:
#cloud_provider:aws
6 days ago · Add comment · Lower priority
User User
Logged in the AWS console
#account:demo4
#aws_account:
#cloudtrail
#consolelogin
#demo4
6 days ago · Add comment · Lower priority
A user failed to log in the AWS console
#account:demo4
#aws_account
#cloudtrail
#consolelogin
#demo4
6 days ago · Add comment · Lower priority
2 events

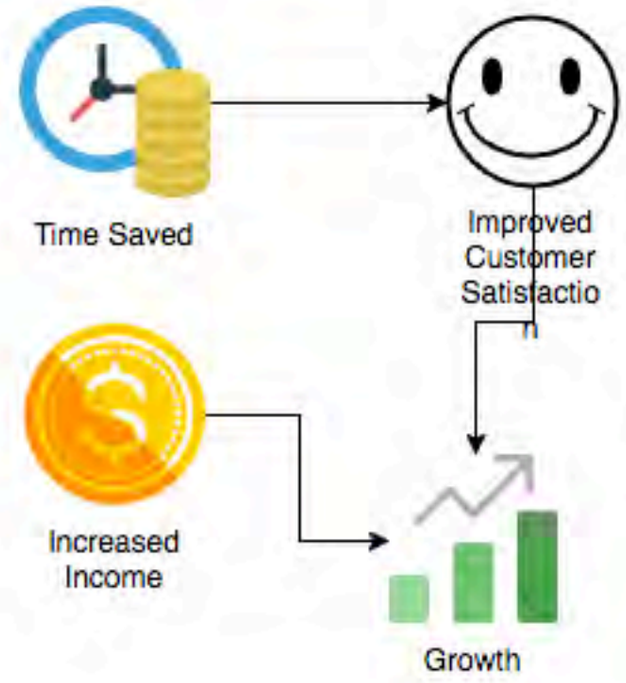
Alerts

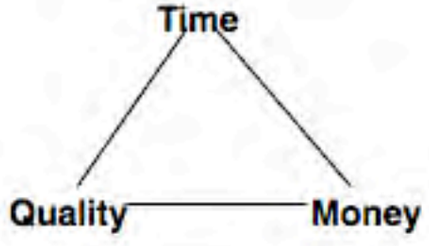


Successful logins and EC2 termination

ZOmazon







Amazon, Flipkart, EBay

Functional Requirements

- Sellers should be able to add, delete and modify products they want to sell.
- The website should include a catalog of products.
- Buyers can search products by name, keyword or category.
- Buyers can add, delete or update items in a cart.
- Buyers can purchase items in the cart and make payments.
- Buyers can view their previous orders.
- Buyers can review and rate purchased products.

https://medium.com/double-pointer/system-design-interview-amazon-flipkart-ebay-or-similar-e-commerce-applications-35a0bc764421

Non-Functional requirements

- Availability : 99.95%
- High Consistency: How to achieve in distributed system?
- Low Latency: Response time: < 250 ms

4 9s (99.99%) Scenario

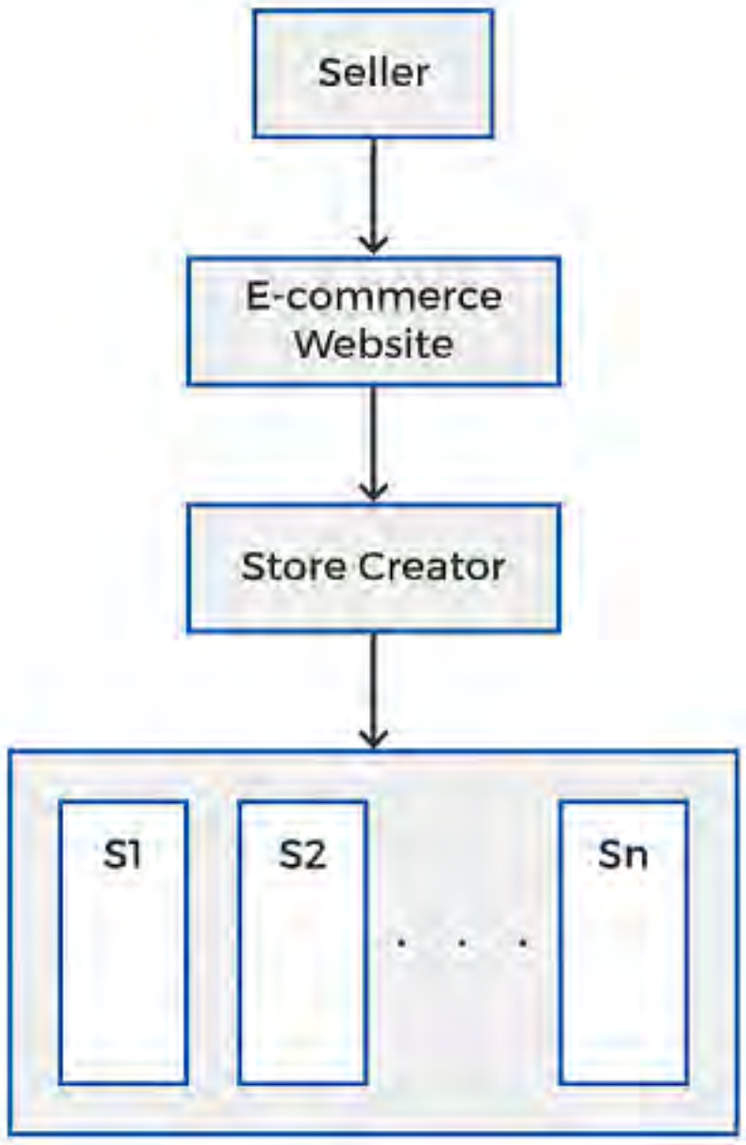
Online Commerce, Point of Sale

52 minutes

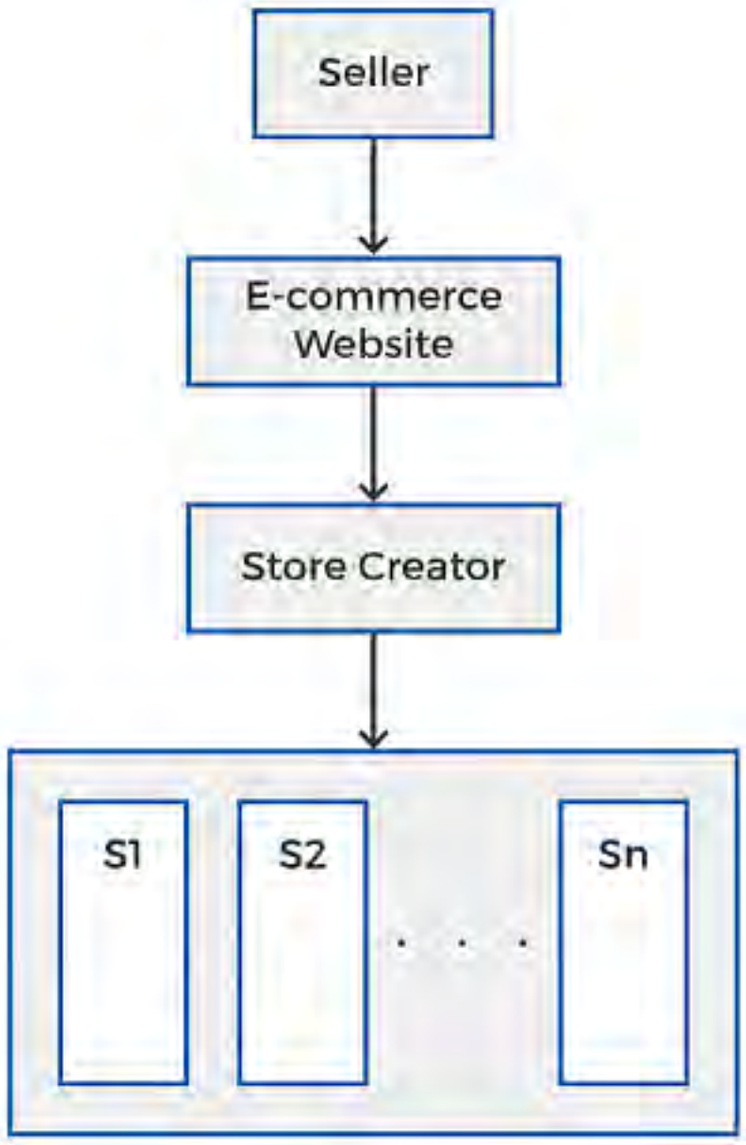
4 9s (99.99%) Scenario

Topic	Implementation
Monitor resources	Health checks at all layers and on KPIs;
Adapt to changes in	ELB for web and automatic scaling application tier; automatic scaling storage and read replicas in multiple zones
Implement change	Automated deploy via canary or blue/green and automated rollback when KPIs or alerts indicate undetected problems
Back up data	Automated backups via RDS to meet RPO and automated restoration that is practiced regularly in a game day.
Architect for resiliency	Implemented fault isolation zones for the application; auto scaling to provide self-healing web and application tier;
Test resiliency	Component and isolation zone fault testing is in pipeline and practiced with operational staff regularly in a game day
Plan for disaster	Encrypted backups via RDS to same AWS Region that is practiced in a game day.

Business to Business to Customer B2B2C

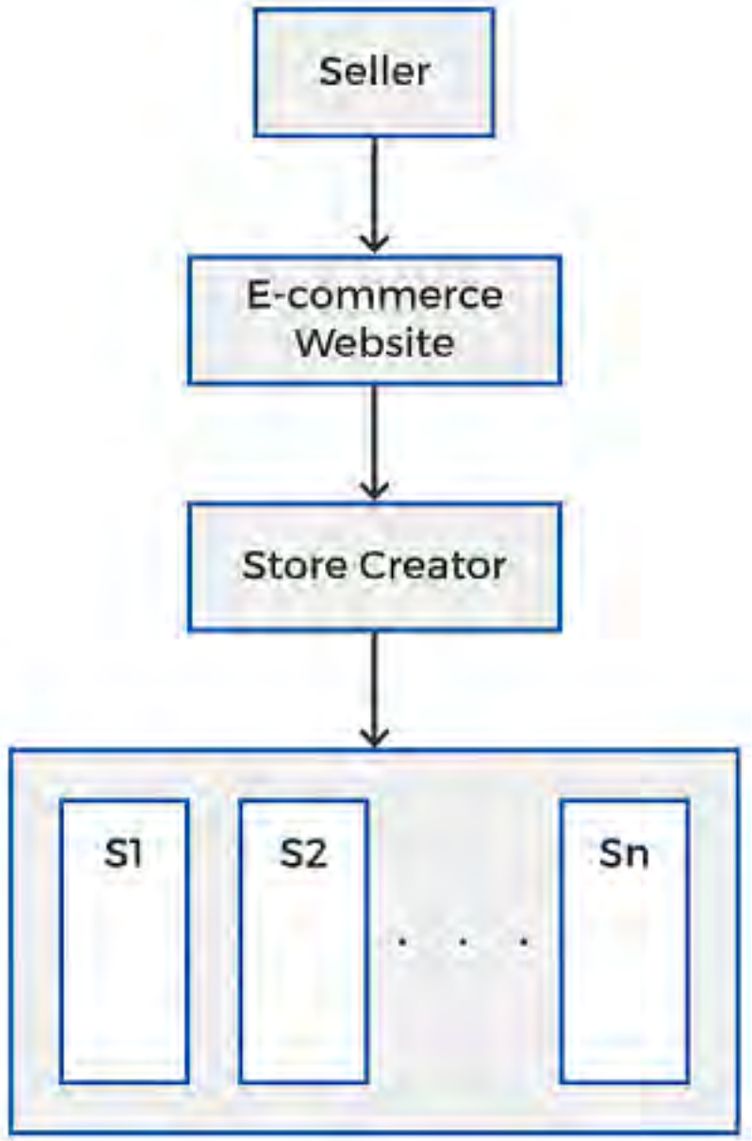


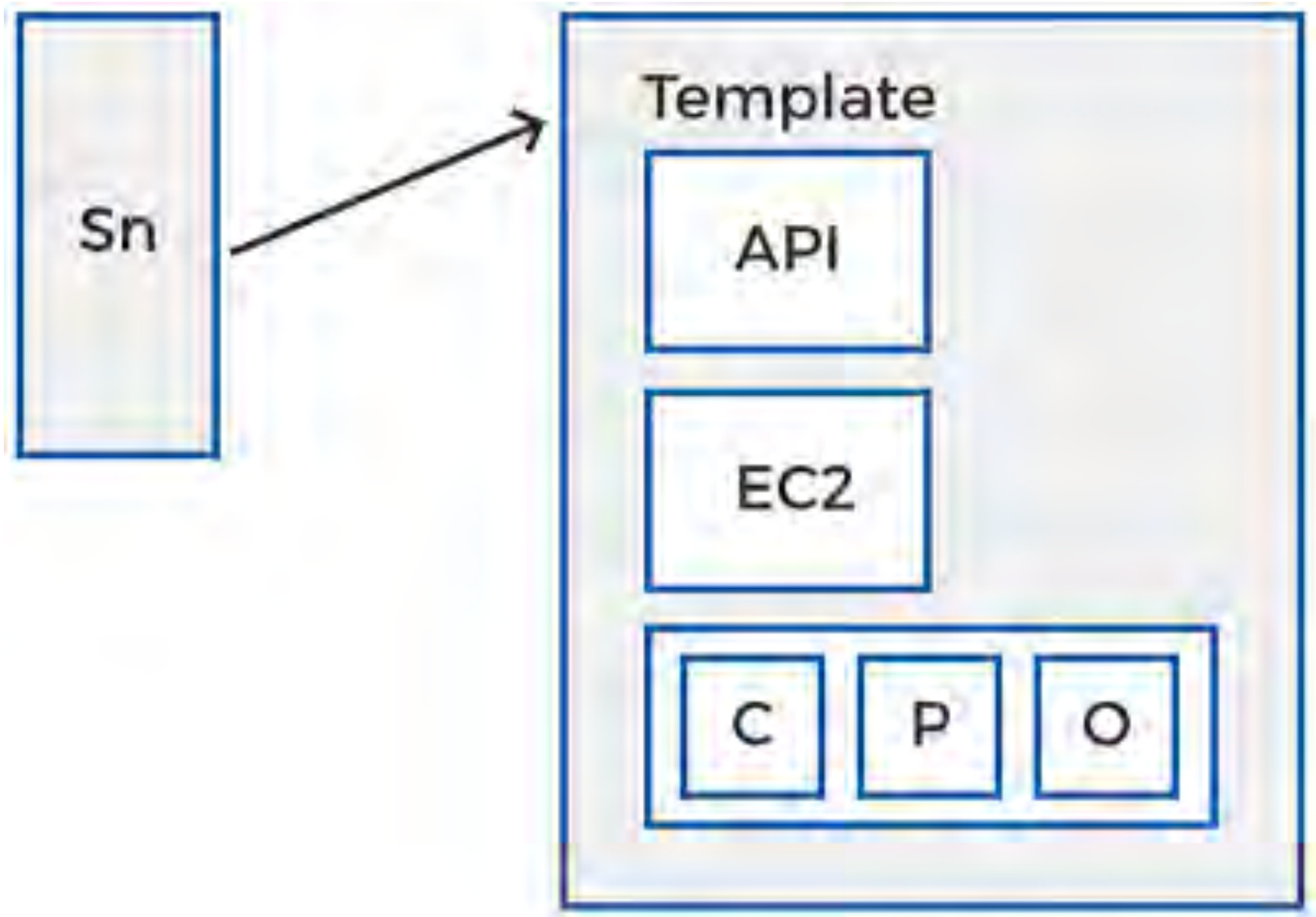
Business to Business to Customer B2B2C



- Customers
- Products
- Orders
- Payment methods

B2B2C - Multitenant





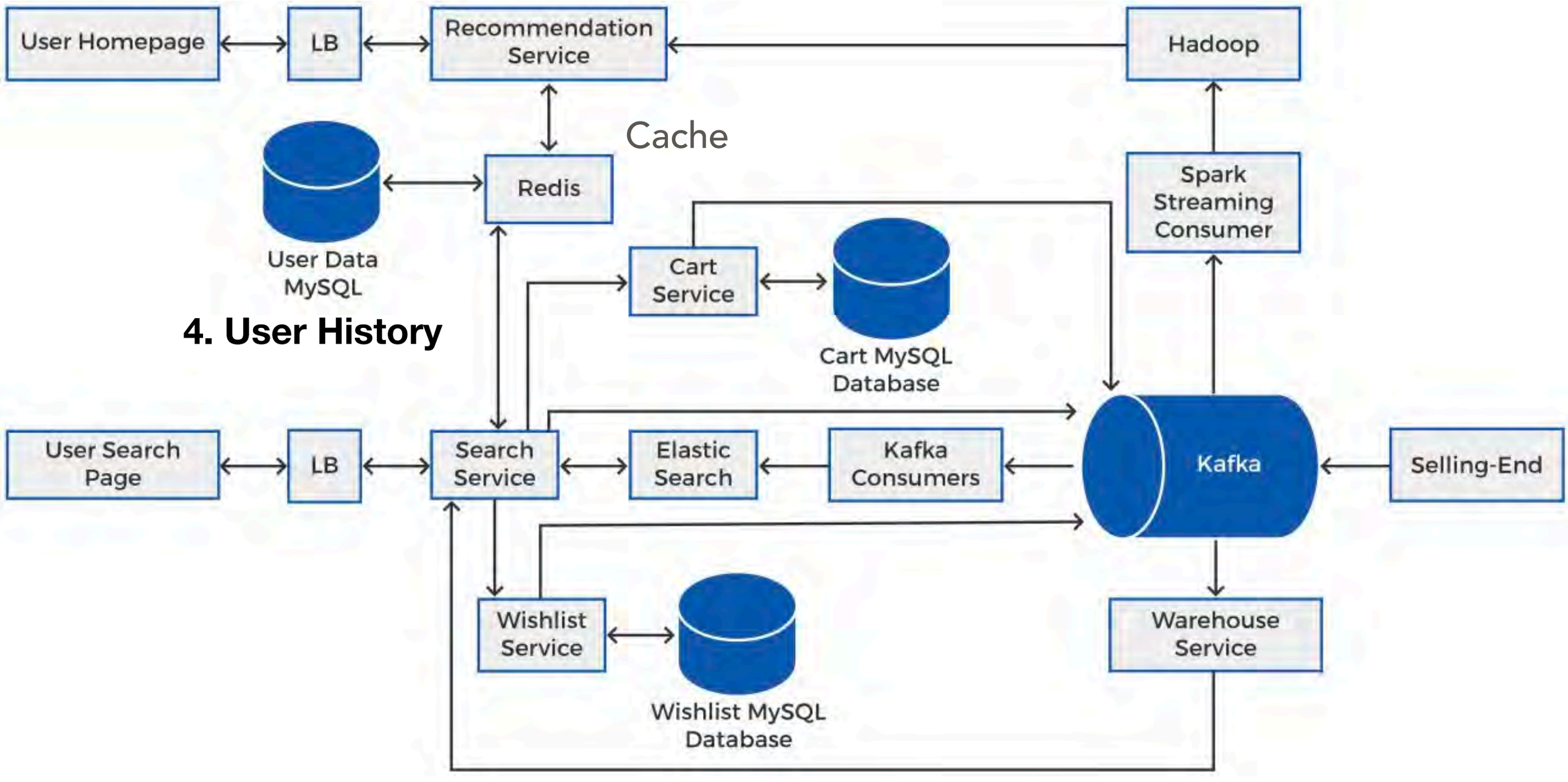
C = Customer Table

P = Products Table

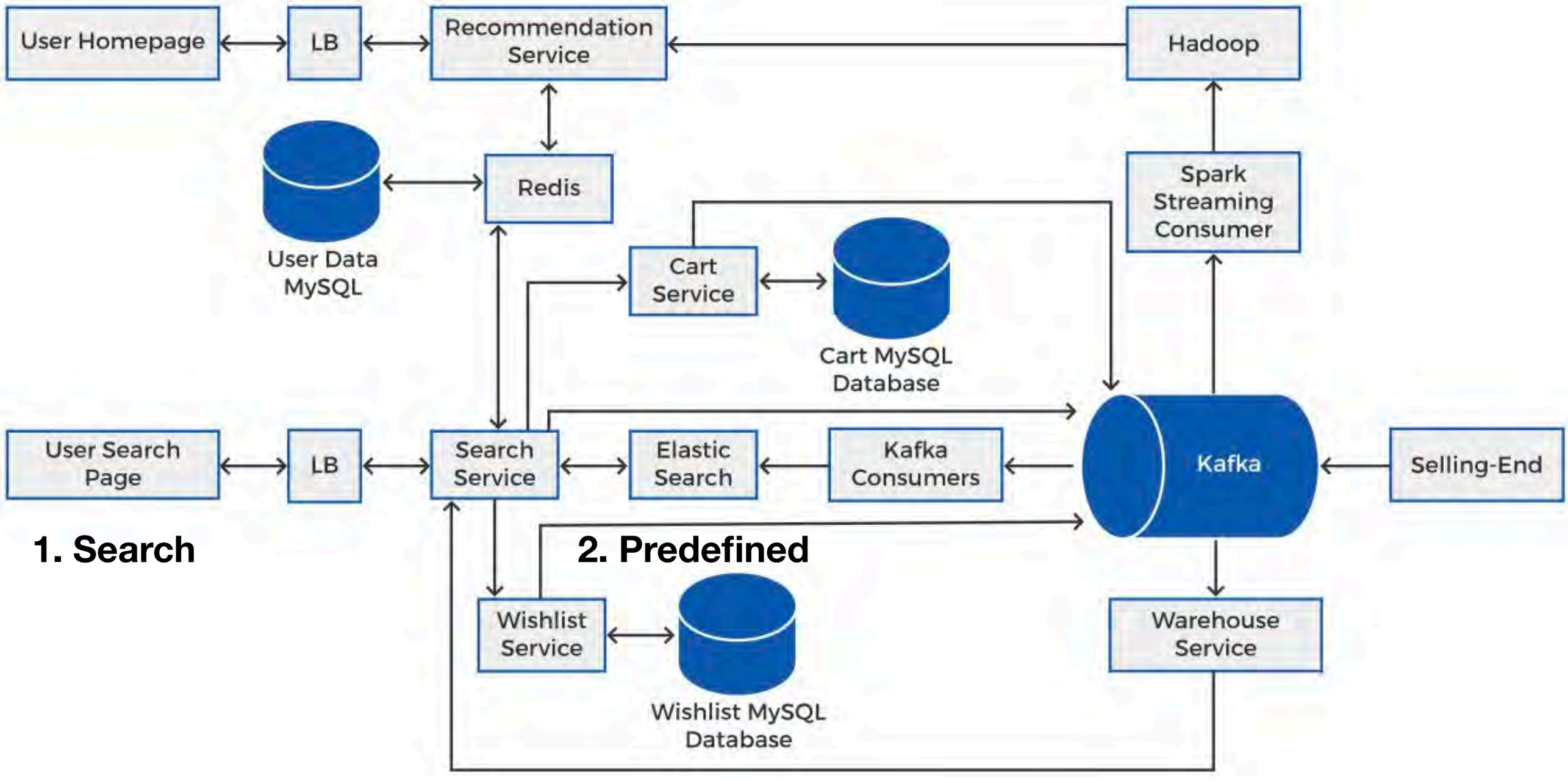
1. Login

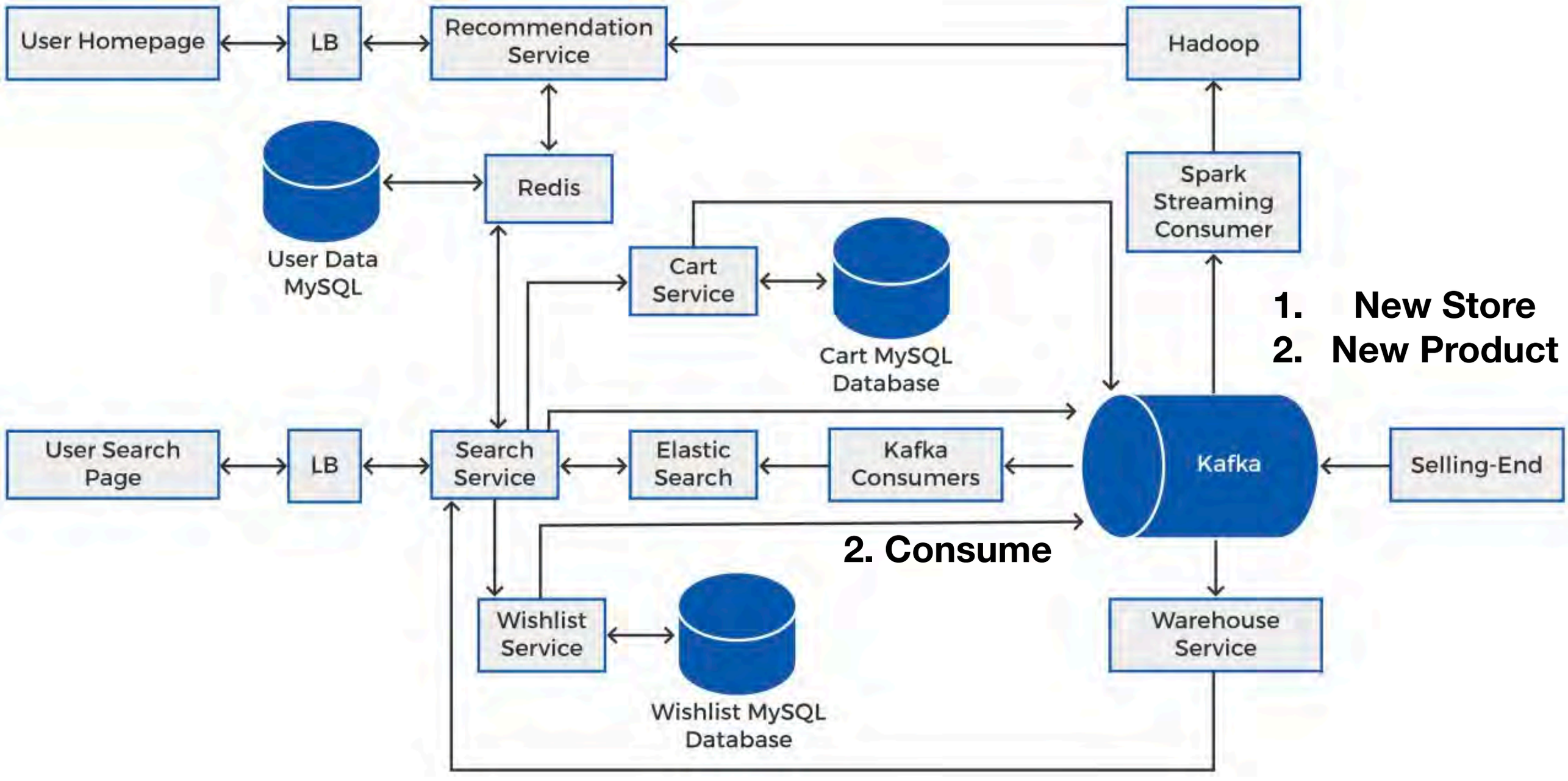
2. Recommend

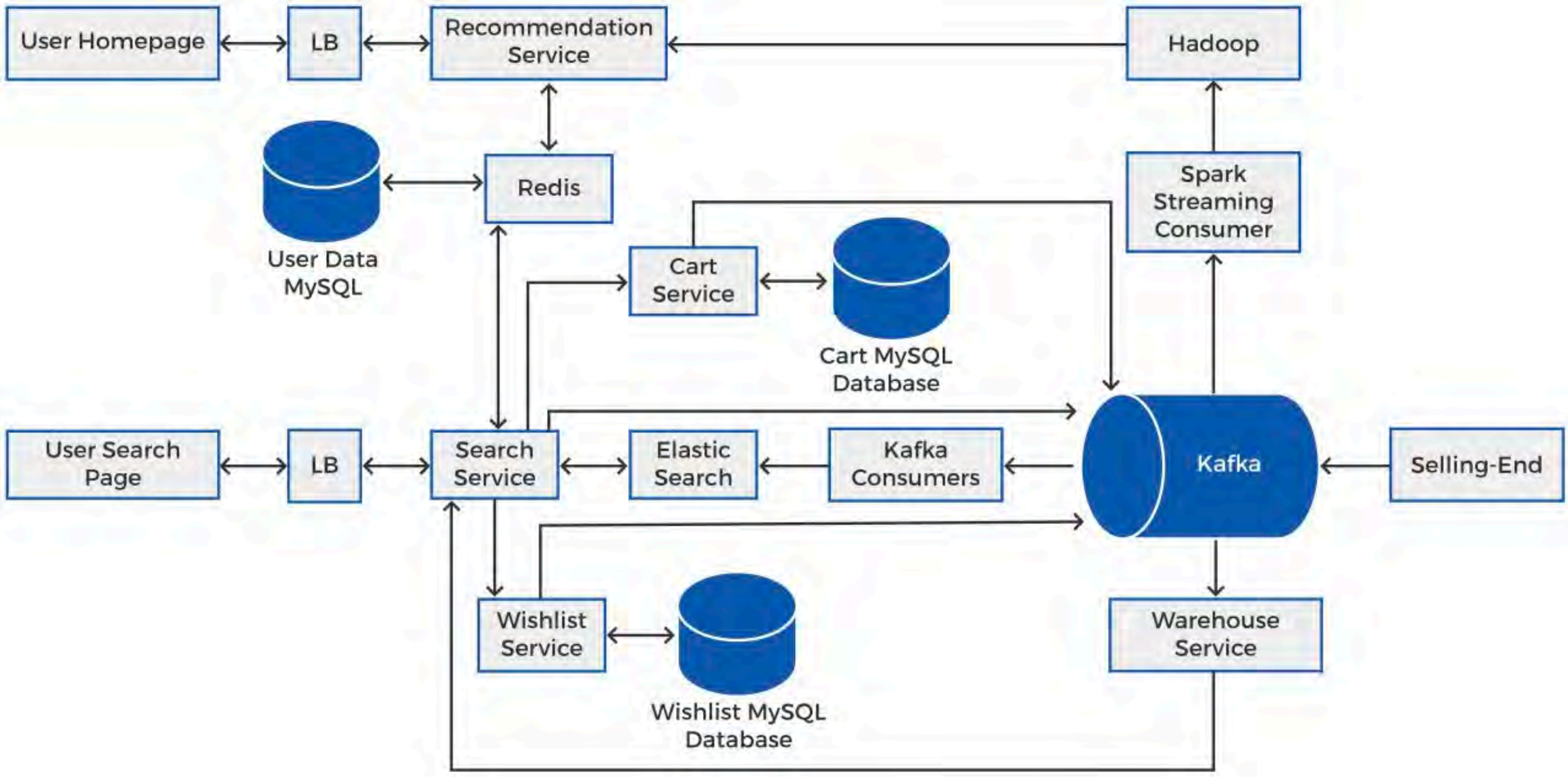
3. Products



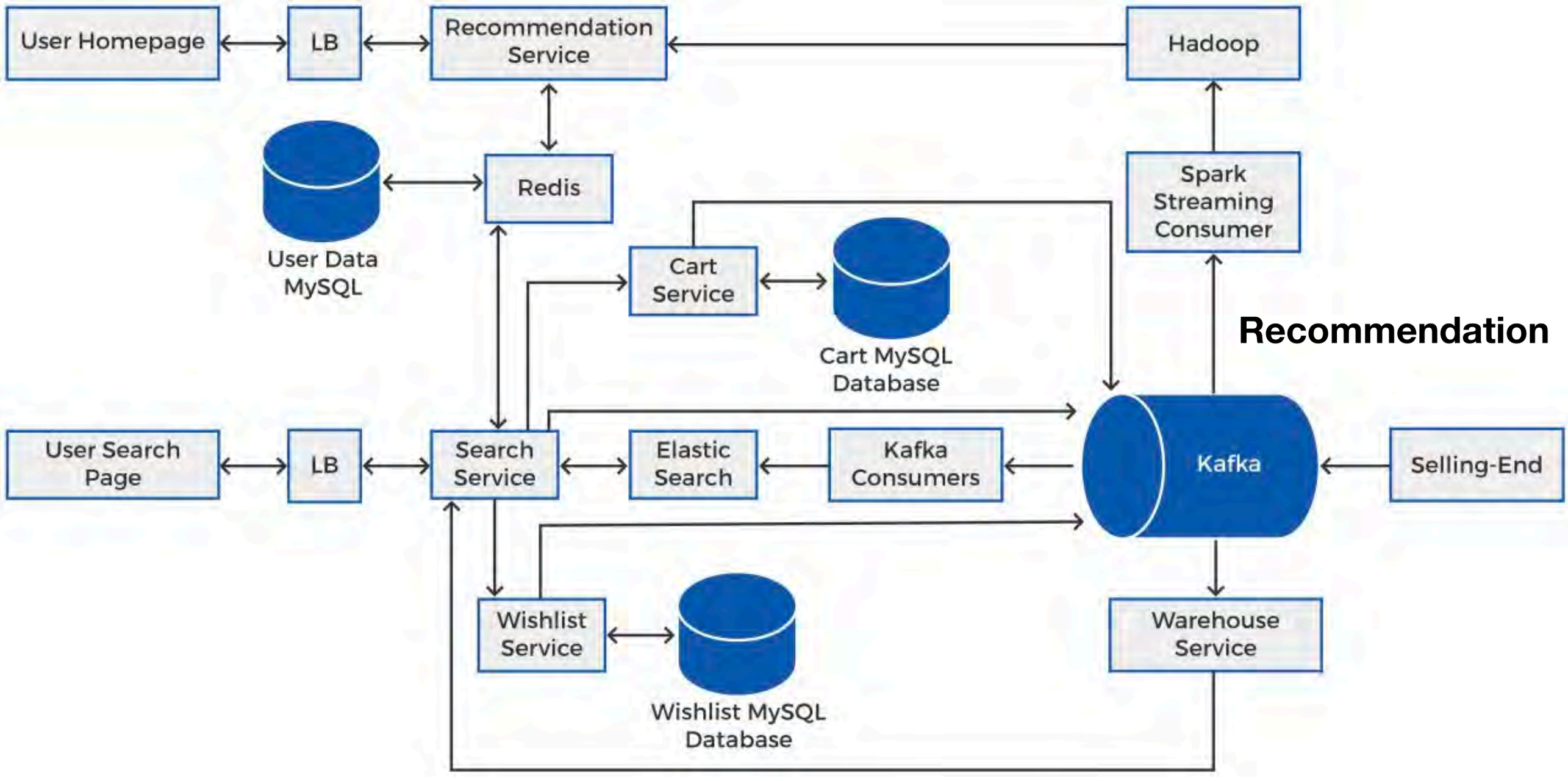
4. User History


User Homepage
LB
Recommendation Service
Hadoop
User Data MySQL
Redis
Spark Streaming Consumer
Cart Service
Cart MySQL Database
User Search Page
LB
Search Service
Elastic Search
Kafka Consumers
Kafka
Selling-End
1. Search
2. Predefined
Wishlist Service
Wishlist MySQL Database
Warehouse Service

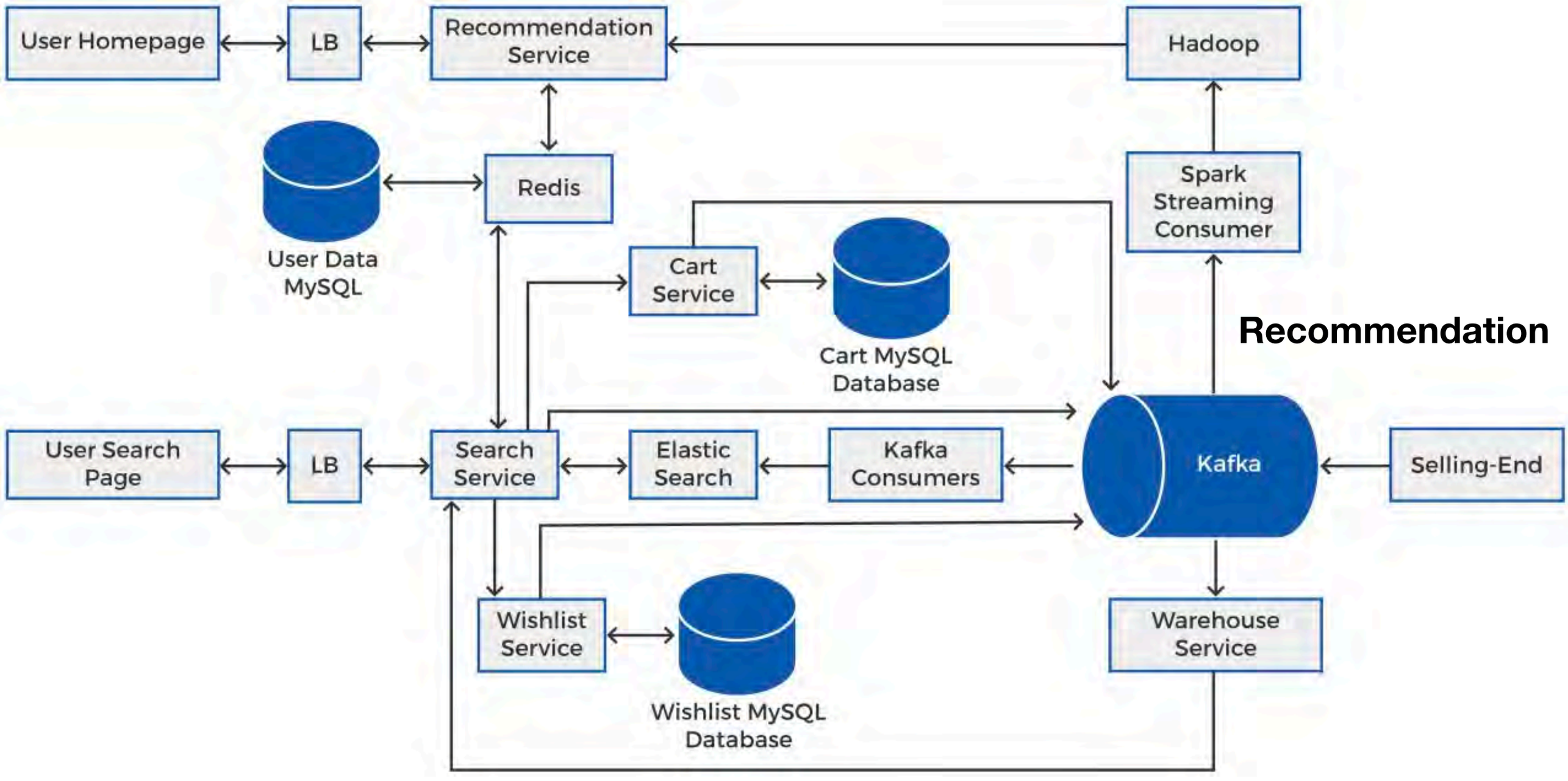

User Homepage
LB
Recommendation Service
Hadoop
User Data MySQL
Redis
Spark Streaming Consumer
Cart Service
Cart MySQL Database
1. New Store
2. New Product
User Search Page
LB
Search Service
Elastic Search
Kafka Consumers
Kafka
Selling-End
2. Consume
Wishlist Service
Wishlist MySQL Database
Warehouse Service



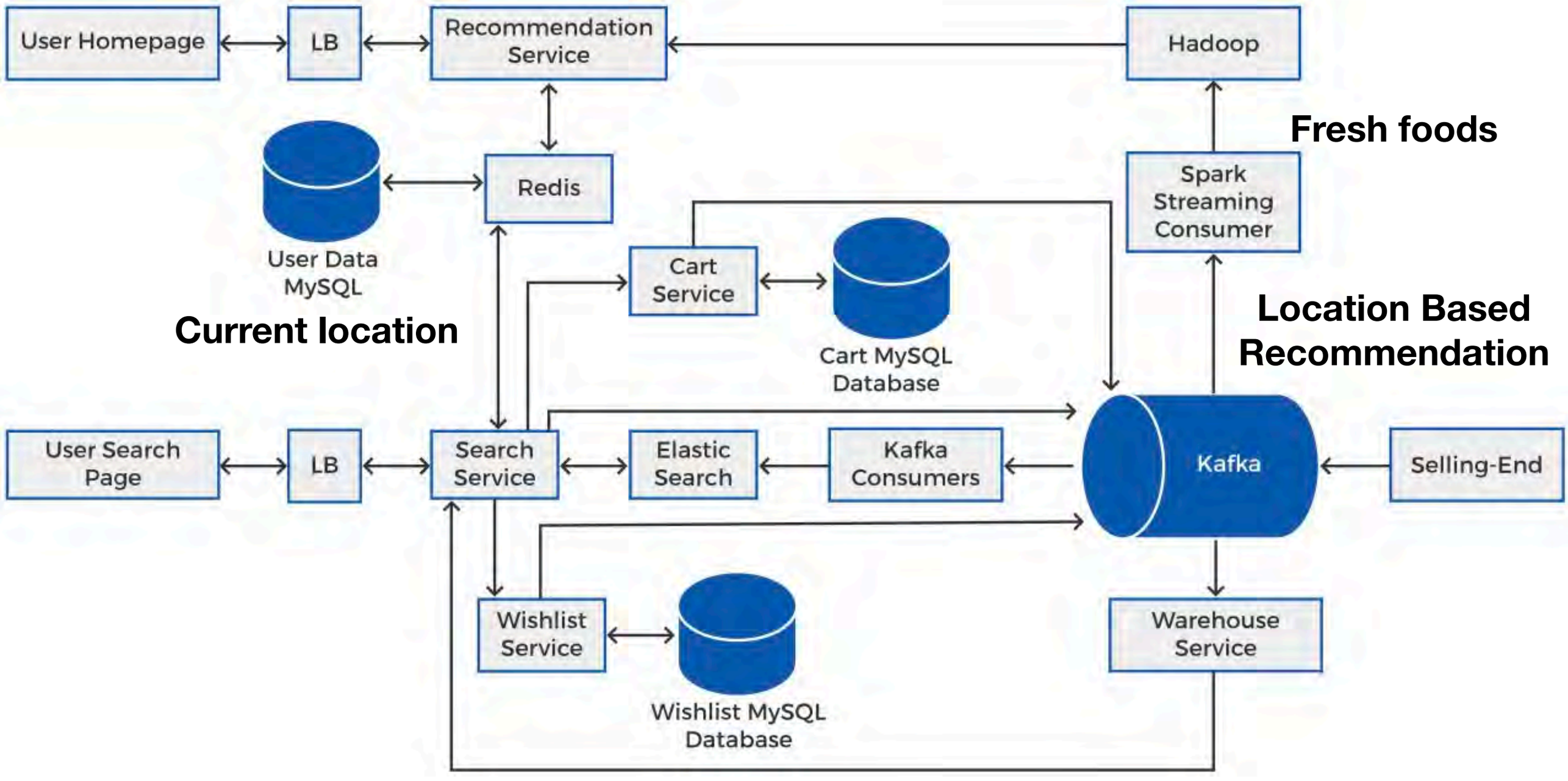
Why separate databases for Wishlist and Cart?



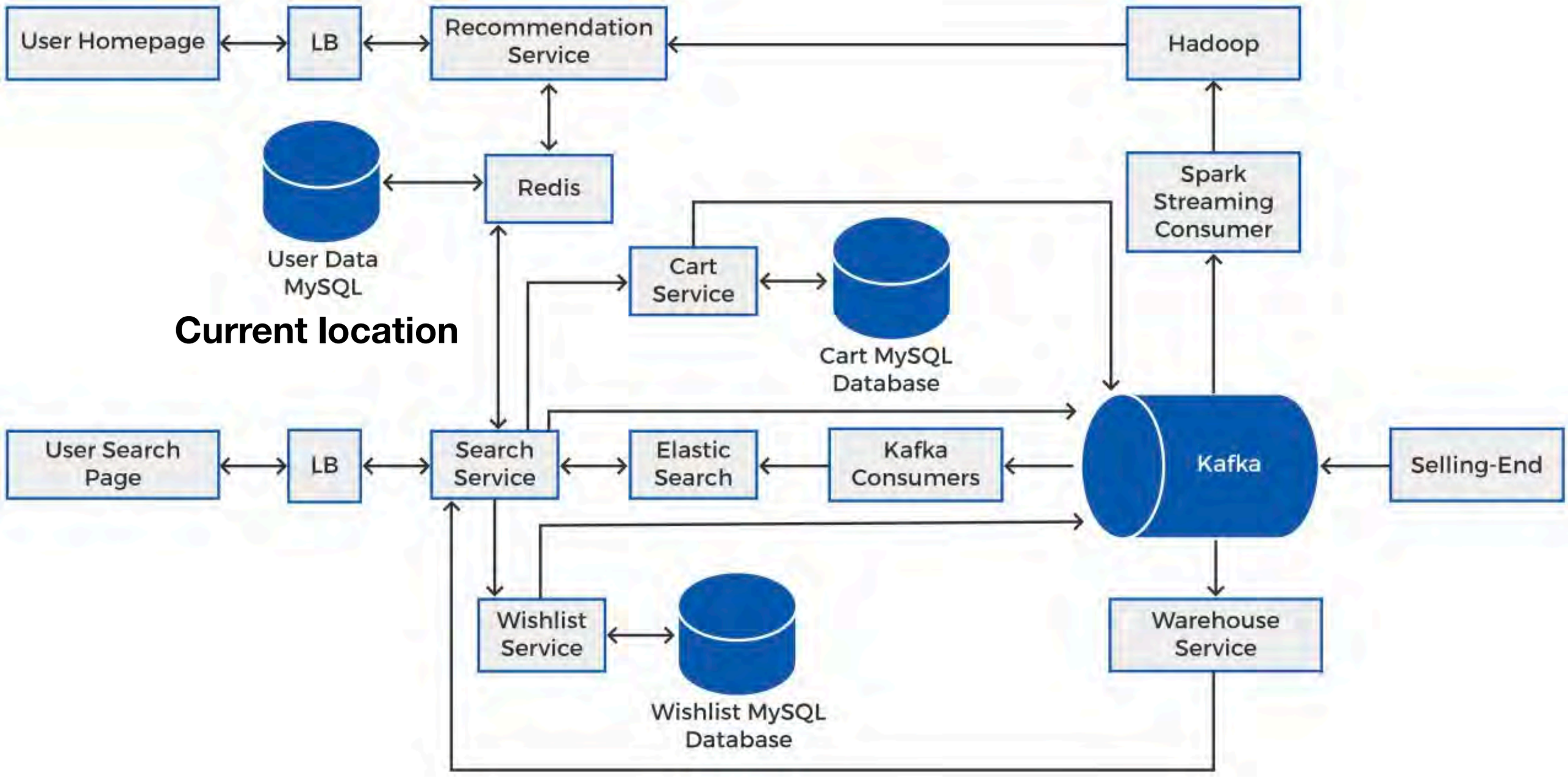
Why separate databases for Wishlist and Cart?



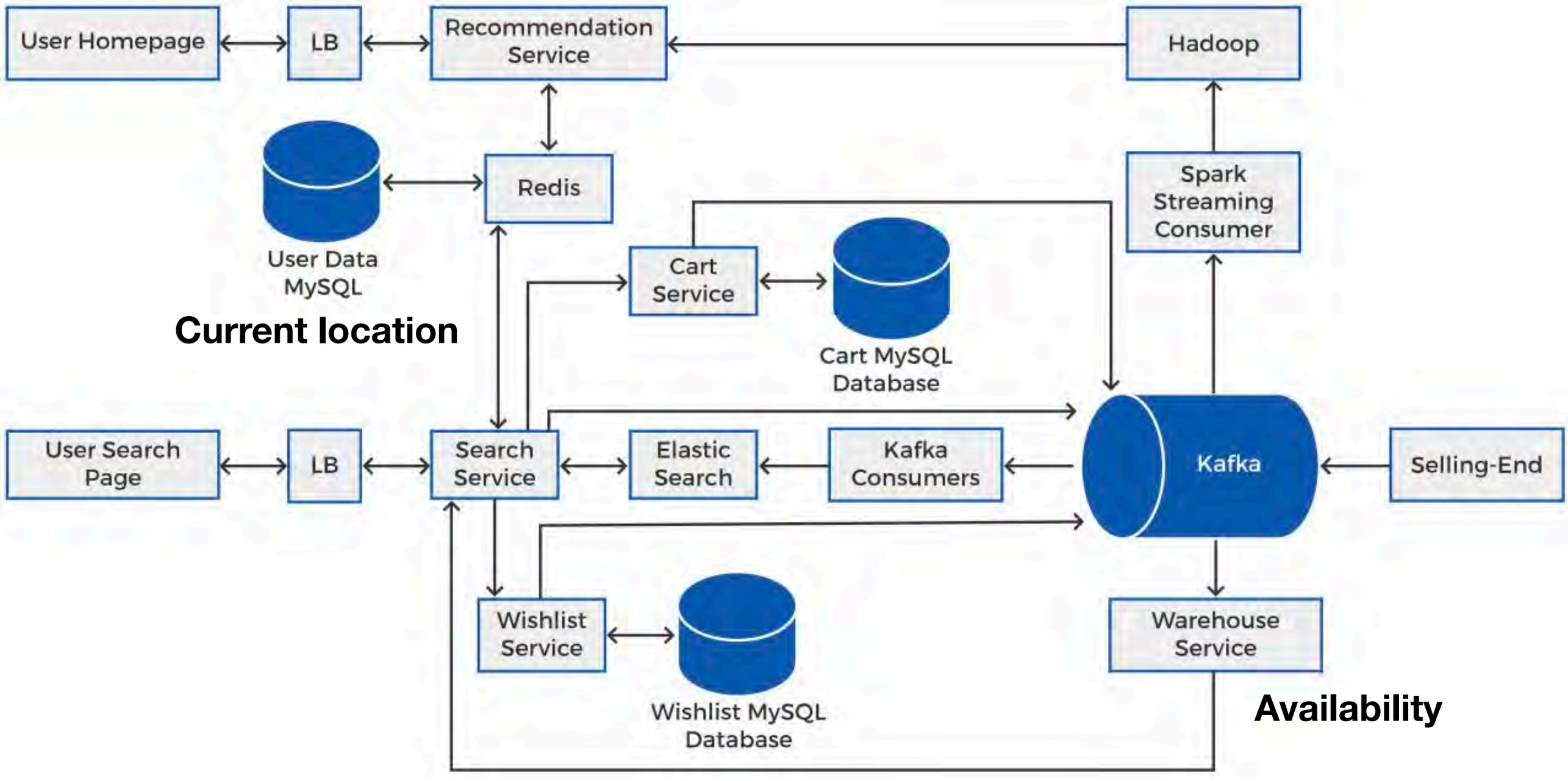
What can we store in User Data?



What can we store in User Data?

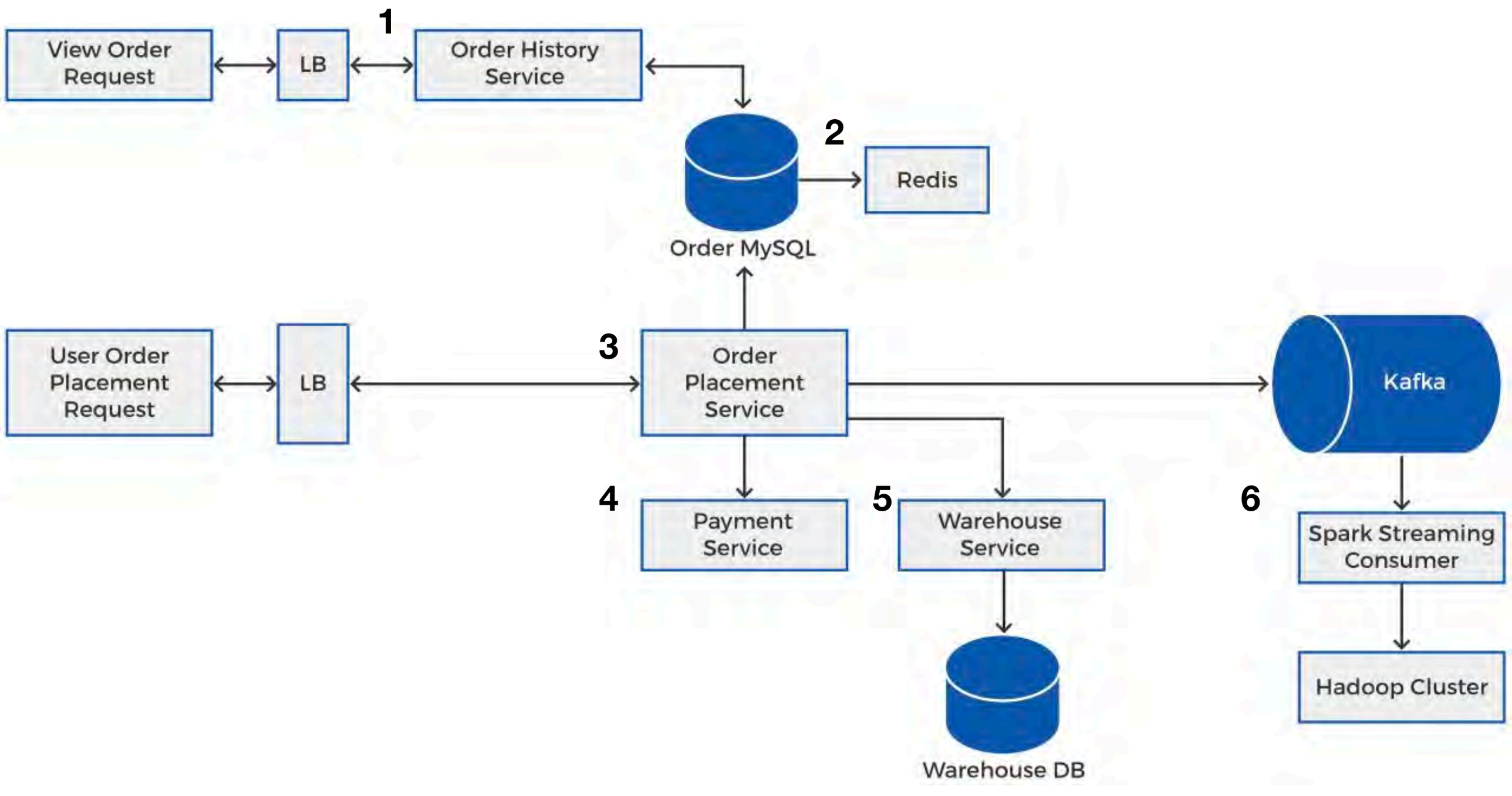


How to find the product is available or not?



How to find the product is available or not?

Order Placement

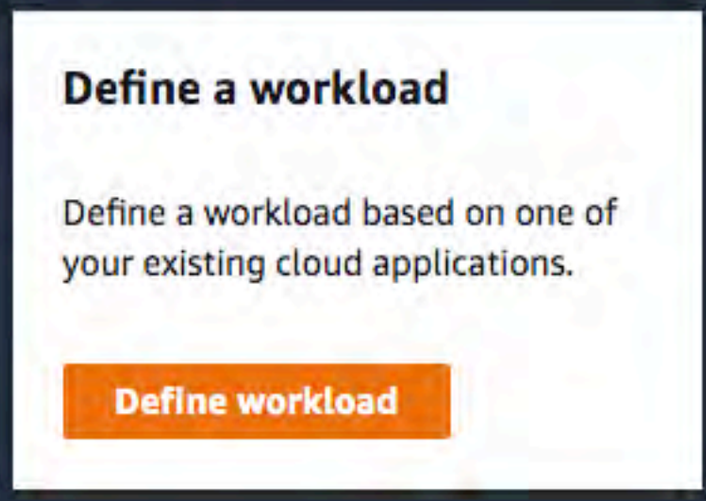


Management Tools

AWS Well-Architected Tool

Learn, measure, and build using architectural best practices

The AWS Well-Architected Tool helps you review your workloads against current AWS best practices and provides guidance on how to improve your cloud architectures. This tool is based on the AWS Well-Architected Framework.



- **Dashboard**
  - Cost Optimization
  - Performance
  - Security
  - Fault Tolerance
  - Service Limits
- Preferences

Trusted Advisor Dashboard

Cost Optimization	Performance	Security	Fault Tolerance	Service Limits
0 ✓ 0 ⚠ 0 !	0 ✓ 0 ⚠ 0 !	2 ✓ 0 ⚠ 0 !	0 ✓ 0 ⚠ 0 !	0 ✓ 0 ⚠ 0 !

Recommended Actions

Amazon EBS Public Snapshots — *Refreshed: a few seconds ago*

Checks the permission settings for your Amazon Elastic Block Store (Amazon EBS) volume snapshots and alerts you if any snapshots are marked as public.

0 EBS snapshots are marked as public.

Amazon RDS Public Snapshots — *Refreshed: a few seconds ago*

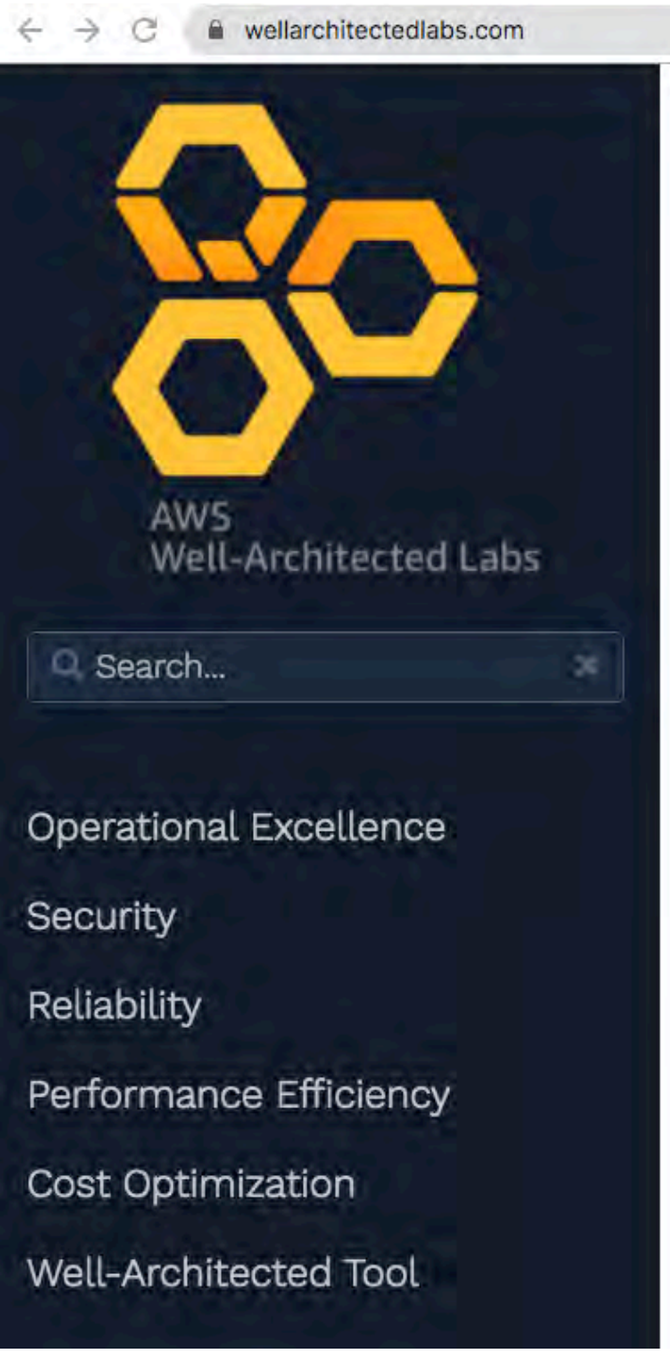
Checks the permission settings for your Amazon Relational Database Service (Amazon RDS) DB snapshots and alerts you if any snapshots are marked as public.

0 RDS snapshots are marked as public.

Security Groups - Specific Ports Unrestricted

Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports.

https://wellarchitectedlabs.com/



Introduction

The Well-Architected framework has been developed to help cloud architects build the most secure, high-performing, resilient, and efficient infrastructure possible for their applications. This framework provides a consistent approach for customers and partners to evaluate architectures, and provides guidance to help implement designs that will scale with your application needs over time.

This repository contains documentation and code in the format of hands-on labs to help you learn, measure, and build using architectural best practices. The labs are categorized into levels, where 100 is introductory, 200/300 is intermediate and 400 is advanced.

Prerequisites:

An AWS account that you are able to use for testing, that is not used for production or other purposes. NOTE: You will be billed for any applicable AWS resources used if you complete this lab that are not covered in the AWS Free Tier.

The Amazon Builders' Library Overview Authors FAQs

The Amazon Builders' Library

How Amazon builds and operates software

> There's no question the world will be a better place if everyone can innovate more quickly and efficiently. And if stuff just works better. For that reason, I'm excited that we are sharing what we've learned with you in The Amazon Builders' Library.
>
> **-Charlie Bell, SVP, Amazon Web Services**

Read the full article

Explore the library

Filter by:

Clear all

▼ **Content Category**

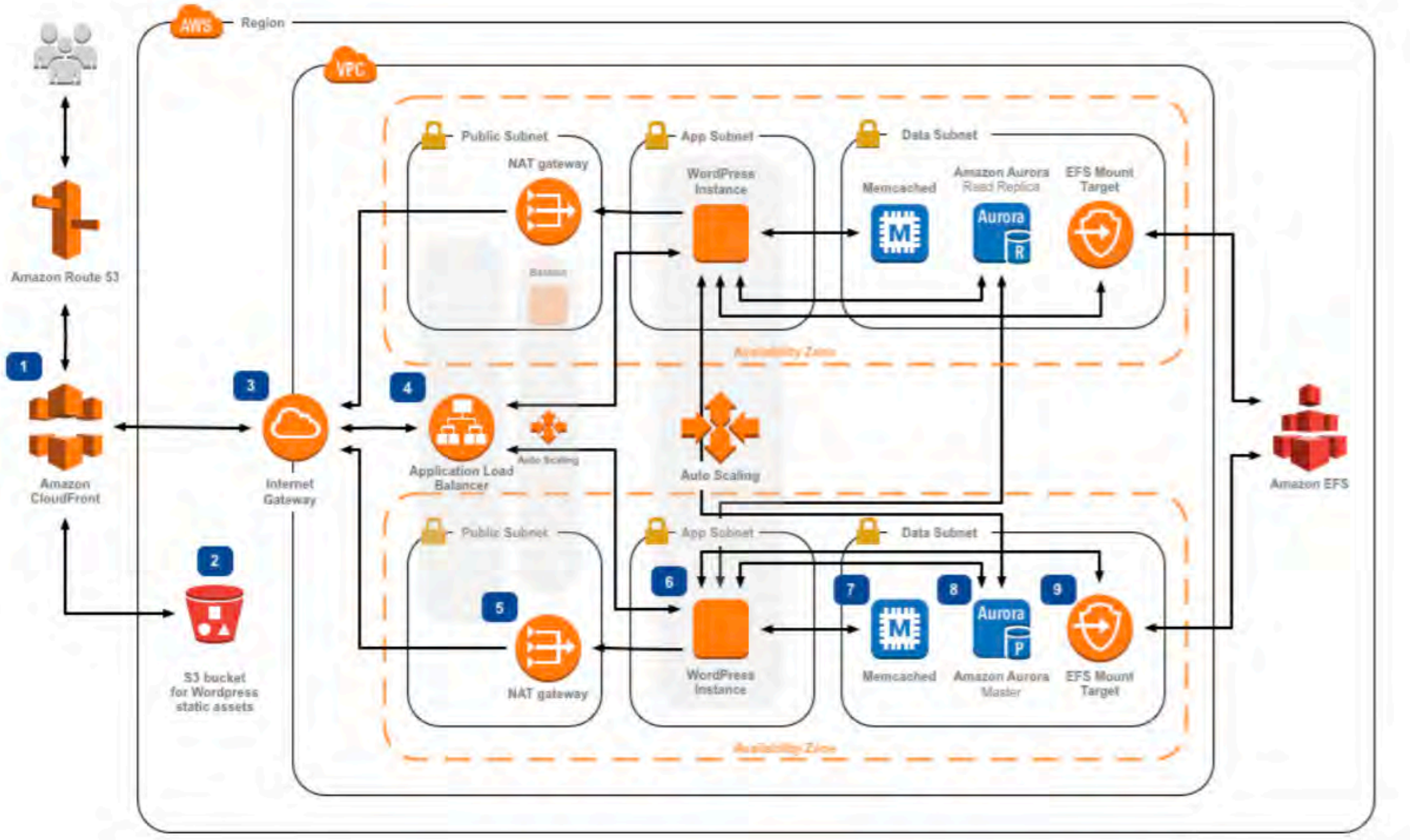
☐ Architecture

Search library

ARCHITECTURE NEW	SOFTWARE DELIVERY AND OPERATIONS NEW	SOFTWARE DELIVERY AND OPERATIONS NEW

https://aws.amazon.com/builders-library

AWS Best Practices



https://aws.amazon.com/blogs/architecture/wordpress-best-practices-on-aws/

Design Resilient Architectures

Design Cost-Optimized Architectures

Sustainability Architectures

Design Performant Architectures

Operationally Excellent Architectures

Specify Secure Applications

Well Architected Framework

tinyurl.com/DesigningWellArchitected

Thanks

Rohit Bhardwaj

Hands-on Senior Architect, Salesforce

Founder: ProductiveCloudInnovation.com
Twitter: rbhardwaj1
LinkedIn: www.linkedin.com/in/rohit-bhardwaj-cloud

tinyurl.com/DesigningWellArchitected

https://www.productivecloudinnovation.com/lessons