



CODESTAR

Storage

CodeStar Academy

Nội dung chính

- Storage
- S3
- EFS



CODESTAR

Storage

Block



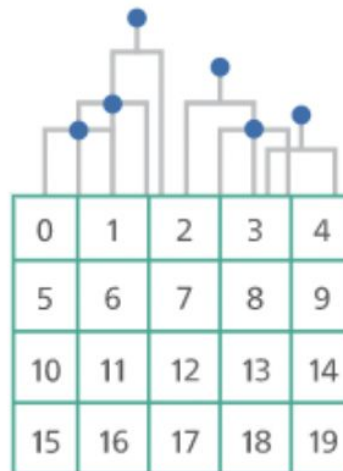
Client Via OS

Fixed Sys Attributes

Transactional Data

Performance

File



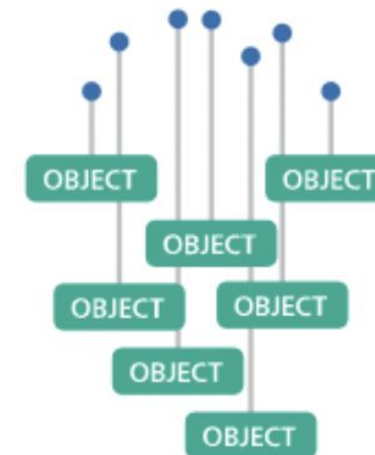
Client Via OS

Fixed Sys Attributes

Shared Changing File

Access, Single Site

Object



Client is App

Custom Metadata

Shared Semi-Static File

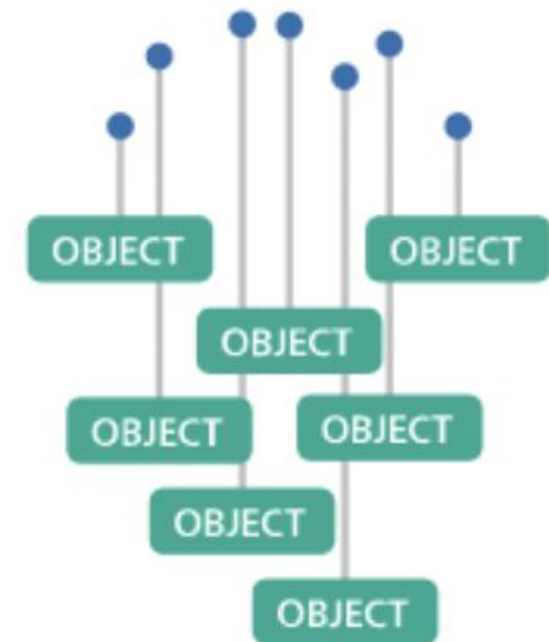
Scalable, Multi-Site

Storage

S3 là dịch vụ storage cơ bản và cũng quan trọng nhất trên AWS:

- Là managed Object storage
- Mặc định đã có HA
- Cho phép lưu trữ không giới hạn
- Lưu trữ tối đa 1 file là 5TB

Object



Storage

Các loại Storage class

- **Standard**
- **Standard IA**
- **Express OneZone**
- **One Zone-IA**
- **Intelligent Tiering**
- **Glacier Instant Retrieval**
- **Glacier Flexible Retrieval**
- **Glacier Deep Archive**

Chi phí lưu
trữ giảm

Độ HA giảm

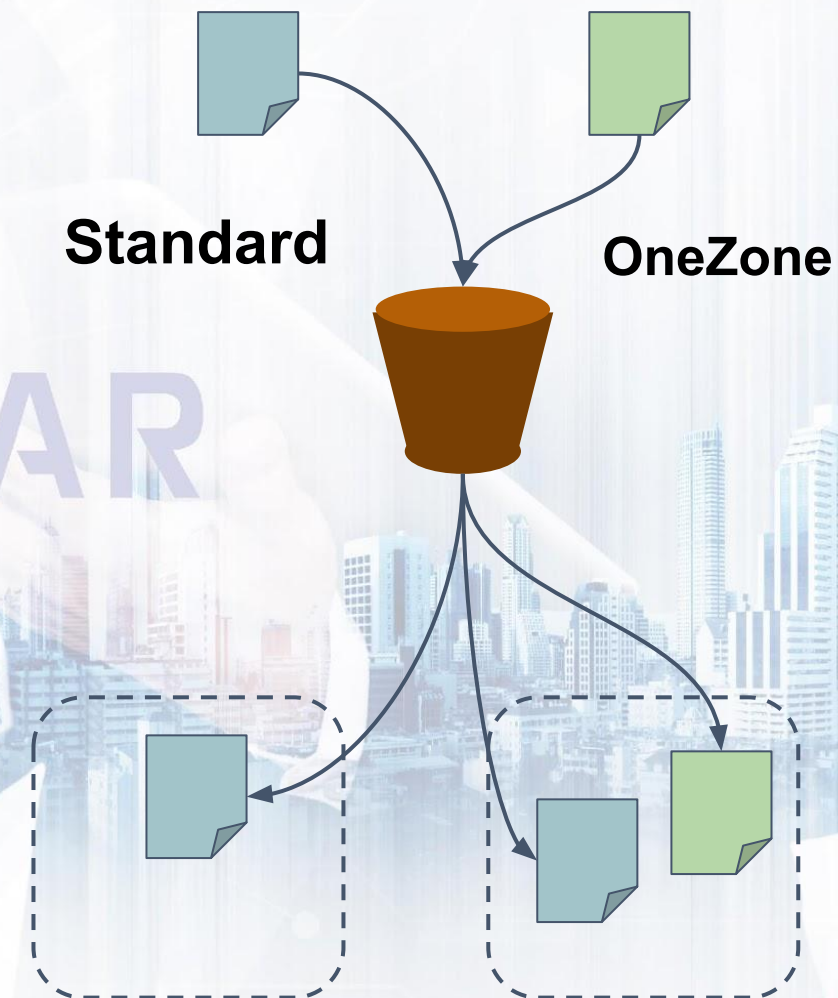
Thời gian truy
xuất tăng

Chi phí truy xuất
tăng

Storage

Các loại Storage class: nhóm **Standard**, **IA**, **Express OneZone** và **One-Zone IA**

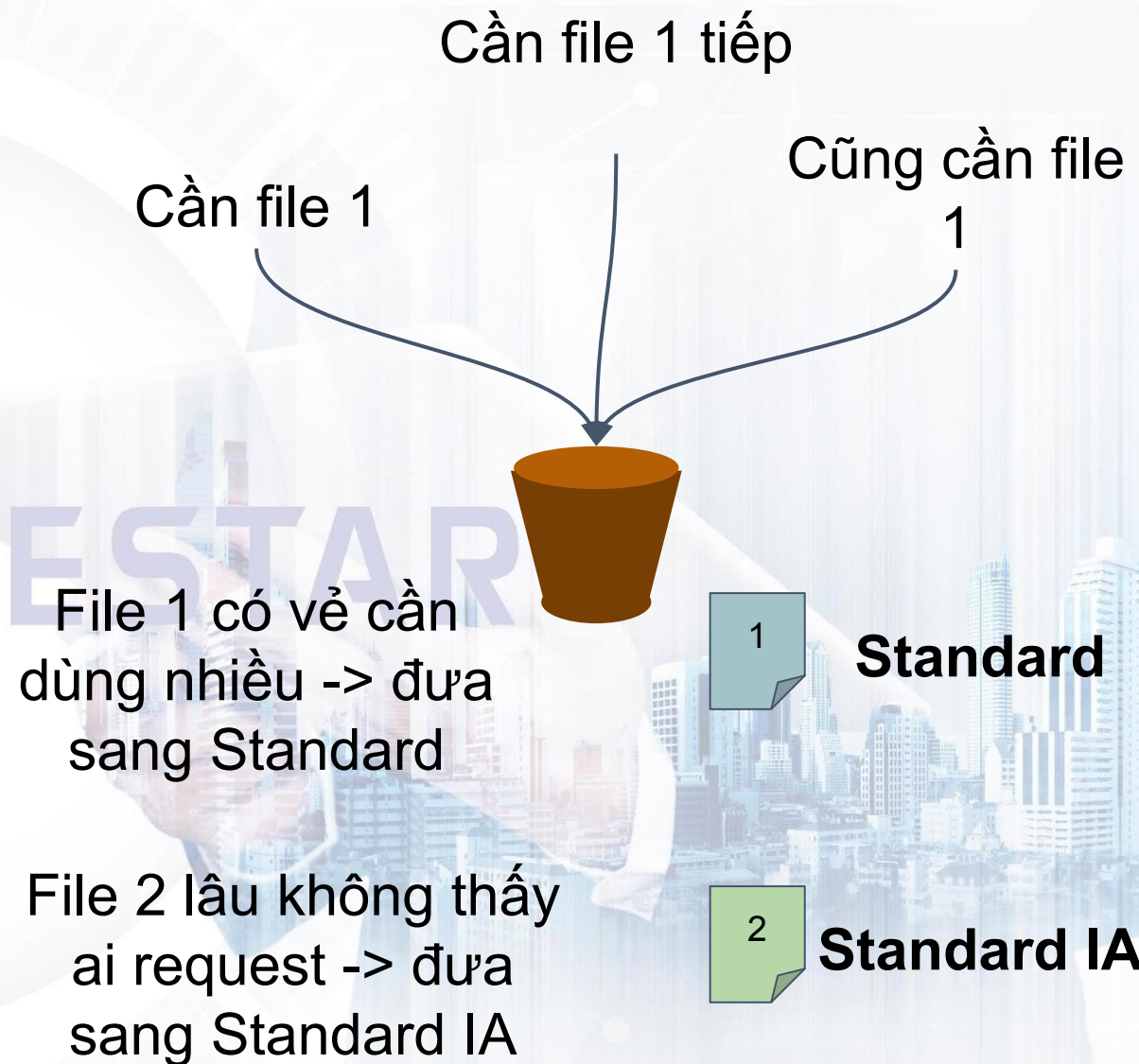
- Nhóm Storage Class Cho phép truy xuất ngay lập tức
- **Standard** dùng lưu trữ file cần truy xuất ngay lập tức, thường xuyên
- **Standard IA** dùng lưu trữ file cần truy xuất ngay lập tức, nhưng không truy xuất thường xuyên.
- **OneZone IA** dùng lưu trữ file cần truy xuất ngay lập tức, không thường xuyên, và cũng không quan trọng, có thể tái tạo được (OneZone IA có HA thấp hơn vì chỉ lưu ở 1 AZ)
- **Express OneZone**: Loại SC mới, cho phép truy cập tốc độ cao (10x so với Standard)



Storage

Các loại Storage class: **Intelligent Tiering**

- Nếu file lưu trữ không rõ là có thường xuyên hay không, không dự đoán trước được mức độ (unpredicted pattern), chúng ta có thể sử dụng **Intelligent Tiering** (Auto detect Storage class dựa trên lịch sử truy cập).



Storage

Các loại Storage class: **nhóm Glacier Archive**

- **Glacier Instant Retrieval** cho phép truy cập ngay lập tức
- **Glacier Flexible Retrieval** có 3 loại Retrieval:
 - + Bulk Retrieval: Truy xuất lâu (5h-12h), nhưng free
 - + Standard Retrieval: Truy xuất lâu (3h-5h), giá TB
 - + Expedited Retrieval: Truy xuất nhanh (1-5 phút), giá đắt nhất.
- **Glacier Deep Archive**: cũng có 2 loại Retrieval:
 - + Standard Retrieval: Truy xuất rất lâu (24h - 48h)
 - + Expedited Retrieval: Truy xuất lâu (12-24h)

Storage

Use-case cơ bản trên S3: **Lifecycle**

Đặt lịch chuyển
đổi Storage Class
cho các object
trong bucket

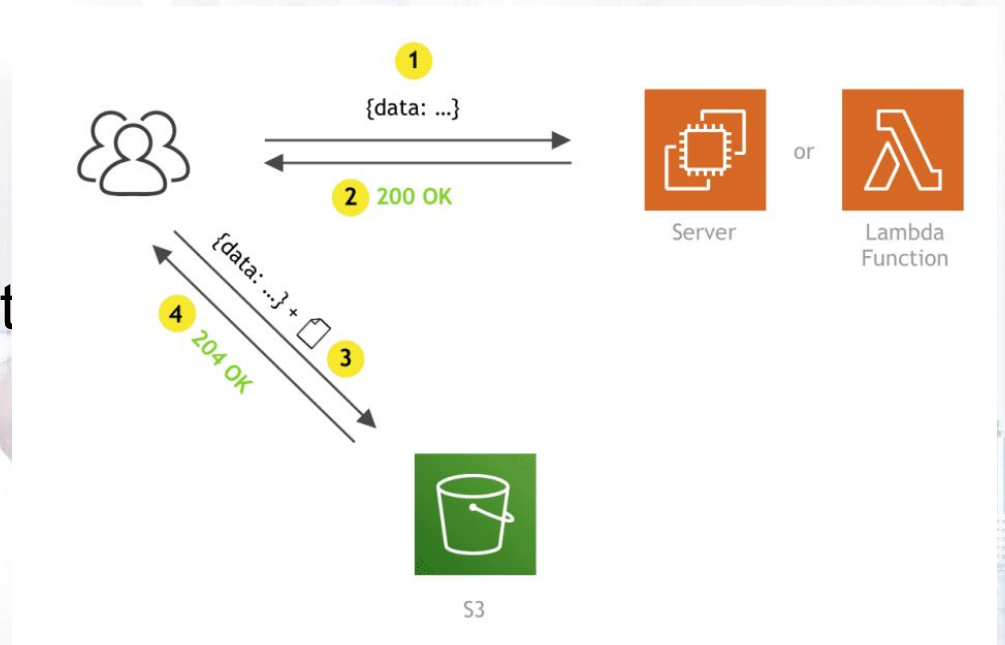


Storage

Use-case cơ bản trên S3: **Presign URL**

Giúp:

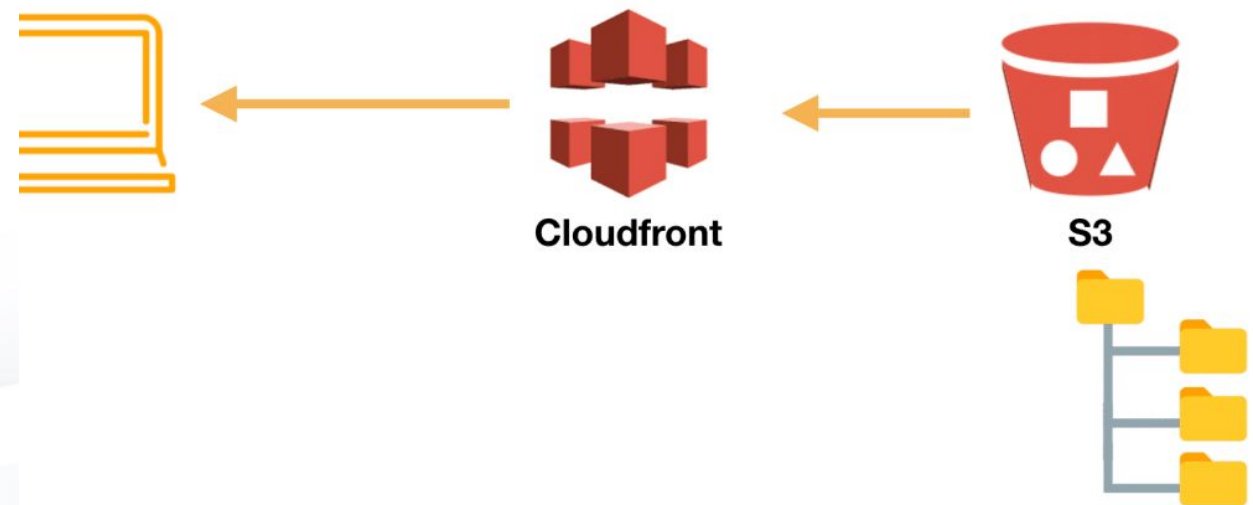
- Tăng performance
- Cắt giảm lượng traffic đi ra ngoài internet
- Phía client tương tác trực tiếp với hệ thống AWS, không cần đi qua server.



Storage

Use-case cơ bản trên S3: **Static Website Hosting**

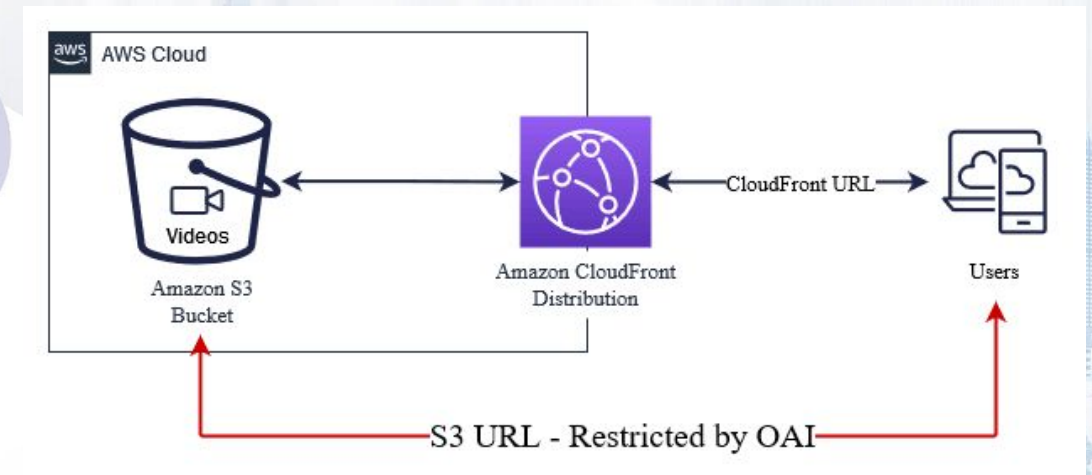
- Khi các data là static
- Muốn cắt giảm chi phí server.
- Khi hệ thống sử dụng cả dynamic và static -> đưa phần dynamic lên lambda, phần static ở S3
- Kết hợp thêm CloudFront khi muốn dùng global.



Storage

OAI/OAC use-case:

- Cung cấp content **global** hoặc **around the world** -> Sử dụng kèm CloudFront
- Sử dụng CloudFront trước S3 bucket để cache -> giảm độ trễ, tăng performance.
- Đảm bảo bảo mật: Sử dụng OAI trên bucket policy cho phép Chỉ CloudFront được phép truy cập vào S3 bucket, không kết nối vào S3 bucket trực tiếp.



Storage

S3 Bucket Policy



- Quy tắc cộng: Nếu bất kỳ IAM Policy, Bucket Policy, ACL allow và không có deny -> allow access object
- Quy tắc Deny explicit: Bất kỳ IAM Policy, S3 Policy, ACL deny -> deny
- Default Bucket: Private và chỉ có ACL allow cho những thực thể có quyền truy cập. (ACL chỉ có allow, không có deny)

Storage

Use-case cơ bản trên S3: **Object Lock**

WORM Model: Write Once Read Many

Dùng để tránh việc file bị ghi đè hoặc xóa trong 1 khoảng thời gian nhất định.

Governance mode: Hạn chế người dùng được phép ghi đè hoặc xóa trong 1 khoảng thời gian cố định

Compliance mode: Không cho phép người dùng được phép ghi đè hoặc xóa trong 1 khoảng thời gian cố định.

Legal hold: Không cho phép người dùng được phép ghi đè hoặc xóa cho tới khi tắt legal hold.

Object lock

Prevent objects from being deleted in order to help ensure data integrity and regulatory compliance. [Learn more](#)

Retention mode

☒ Enable governance mode
Governance mode can be disabled by AWS accounts that have specific IAM permissions.

☐ Enable compliance mode
Compliance mode cannot be disabled by any user, including the root account.

☐ Disable

Retain until date

2018-11-27

Legal hold

Legal hold prevents an object from being deleted regardless of its retain until date. Legal hold can be applied and removed by AWS accounts that have specific IAM permissions.

☐ Enable

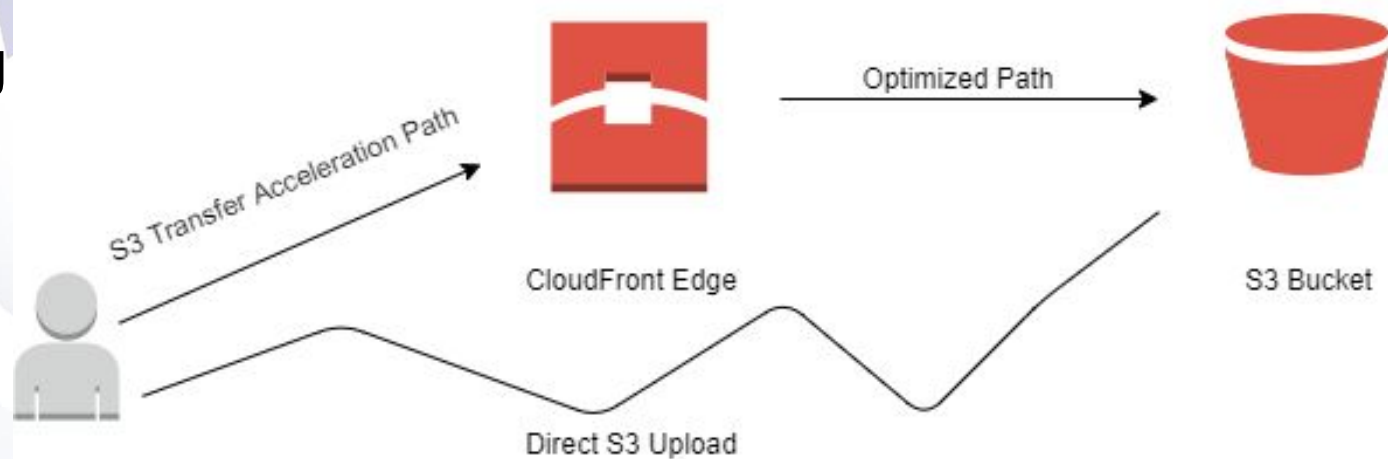
☒ Disable

Cancel Save

Storage

S3 Transfer Acceleration:

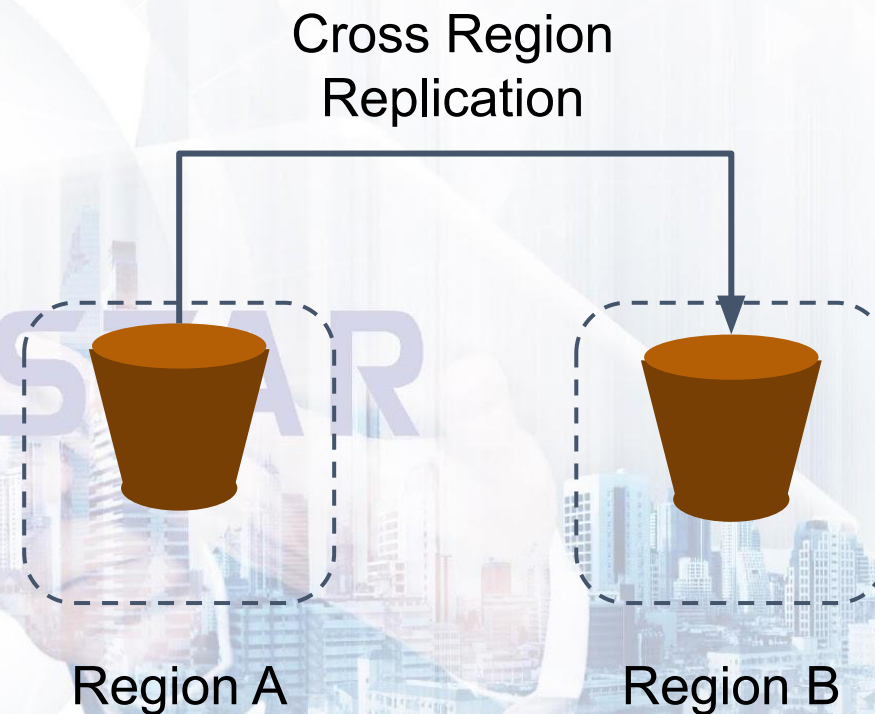
- Là dịch vụ giúp tăng tốc độ truyền dữ liệu tới Bucket thông qua các đường truyền tốc độ cao.
- Thường dùng trong use-case muốn tăng tốc độ truyền tải tới các Region.



Storage

S3 Replication:

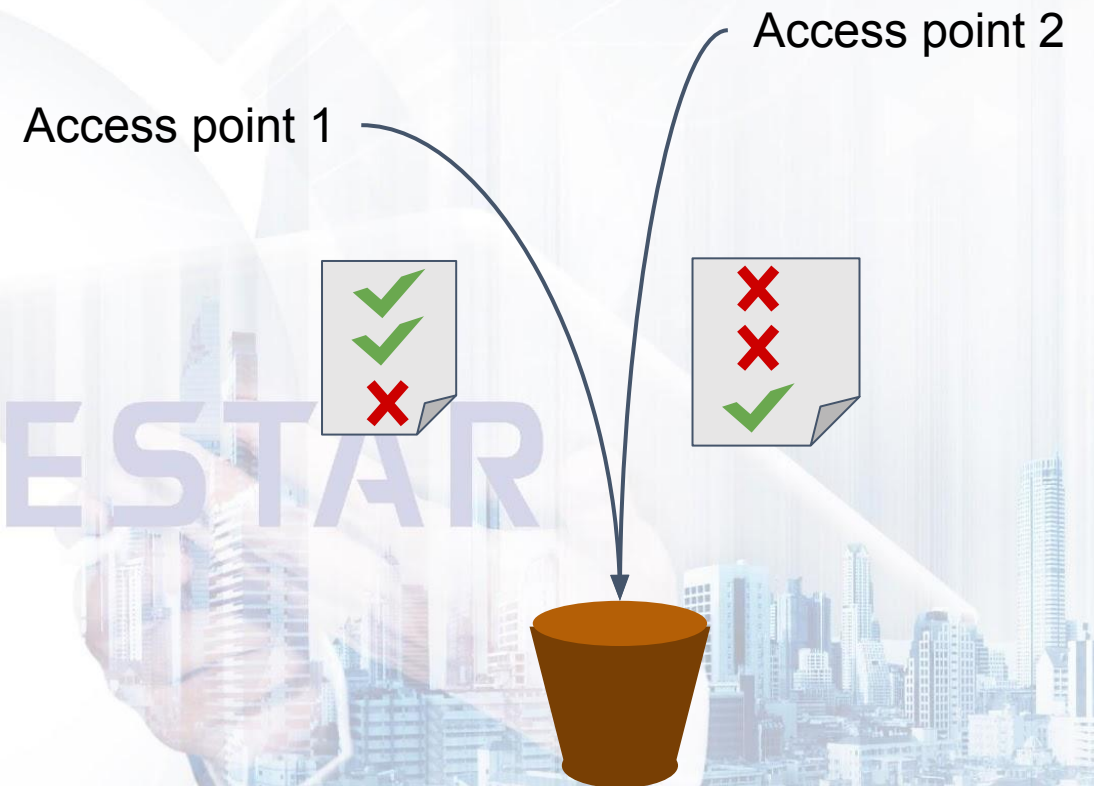
- Đồng bộ giữa các bucket bằng Cross Region Replication (CRR) hoặc Same Region Replication (SRR)
- Live Replication trong 15 phút
- Batch Replication với Batch Operations.



Storage

S3 Access Point:

- Access point trở về cùng một S3 bucket, nhưng có Bucket Policy khác
- => Quản lý nhiều Bucket Policy mà không cần sử dụng chung vào một Bucket Policy tổng.

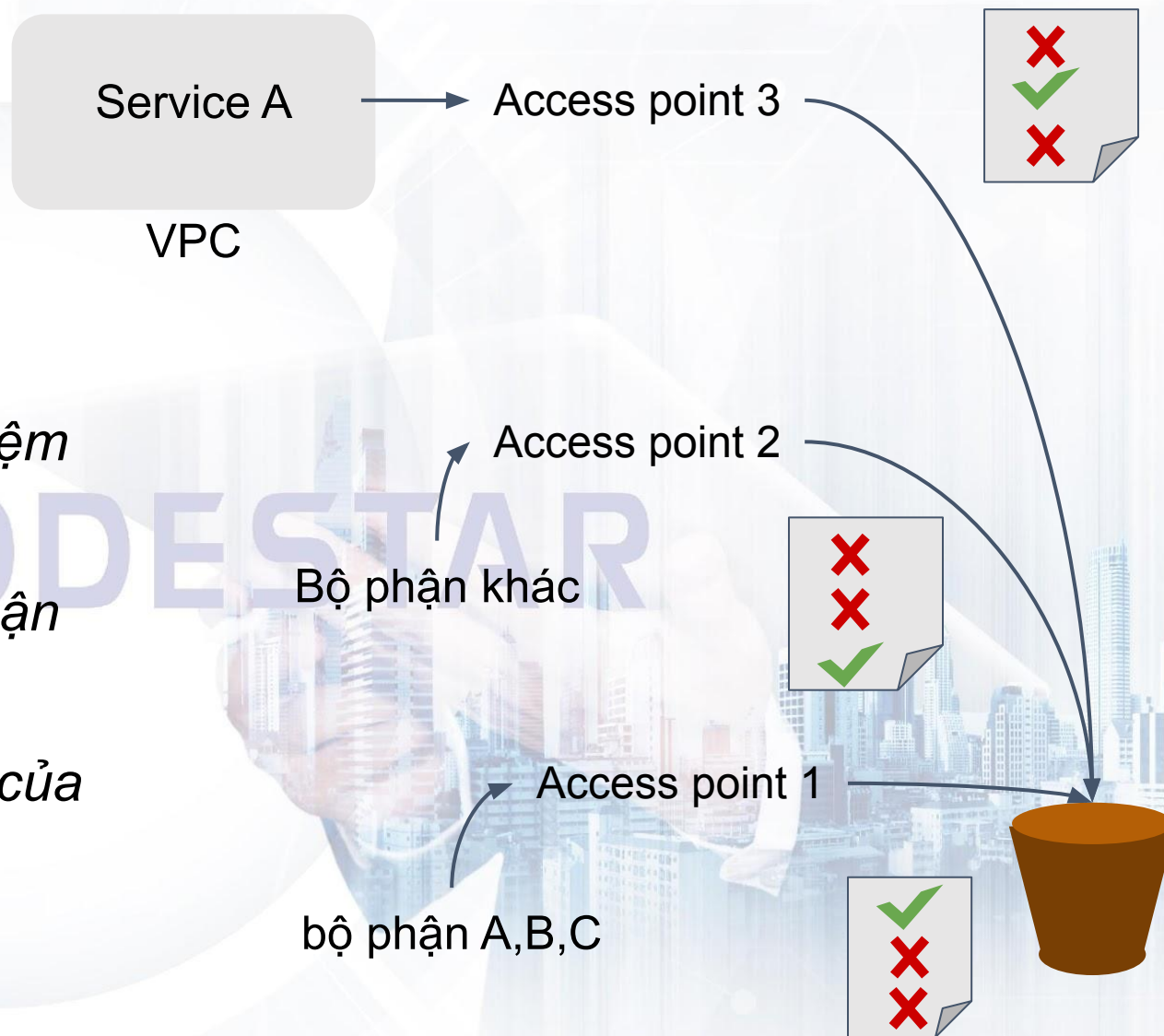


Storage

S3 Access Point:

Use case:

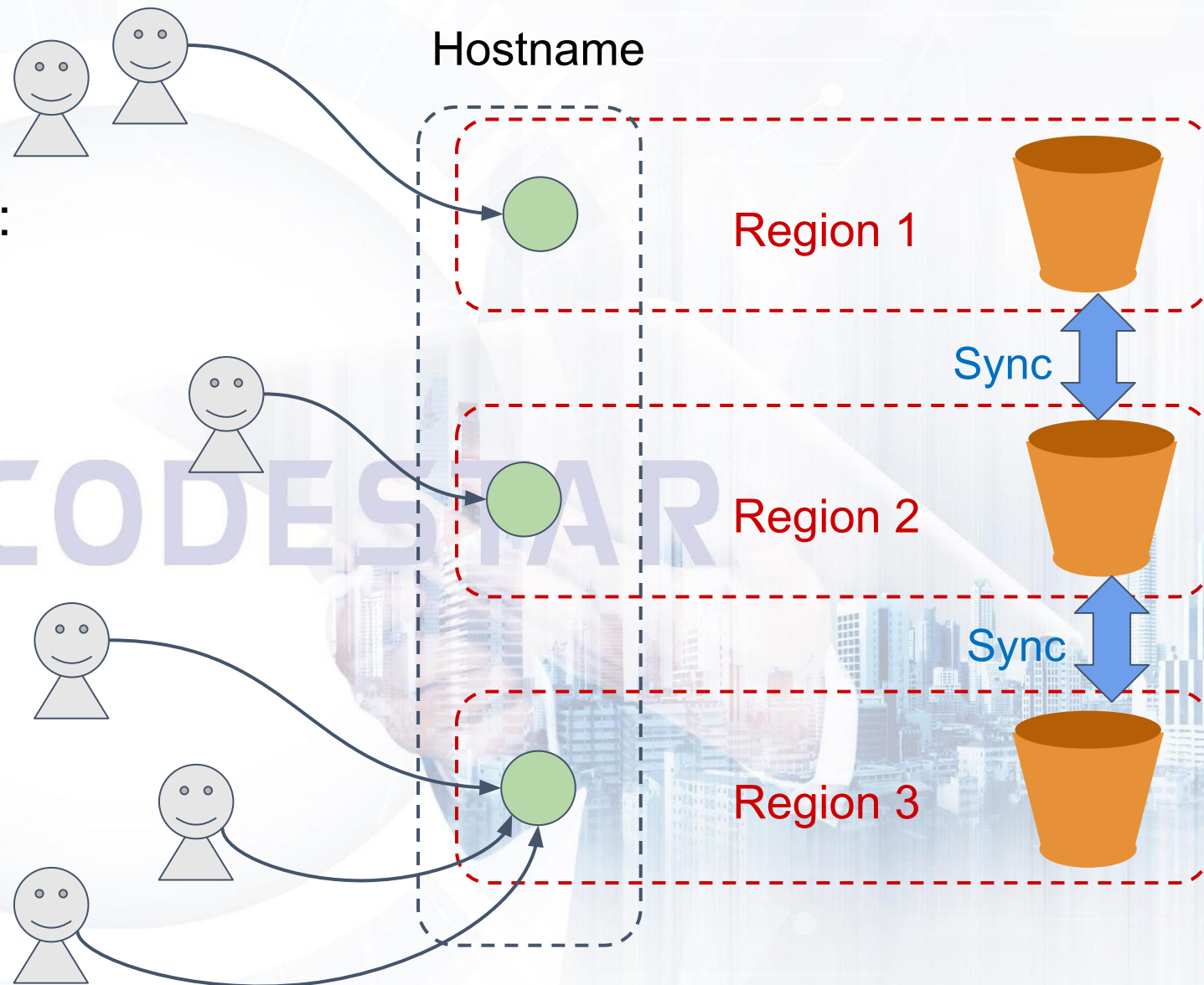
- Công ty có bộ phận A,B,C làm nhiệm vụ update thông tin lên bucket
- Các bộ phận khác lấy file từ bộ phận A,B,C để xử lý.
- Công ty có hệ thống chạy dịch vụ của bộ phận A trên VPC có thể xóa tự động file trên bucket.



Storage

S3 Multi Region Access Point:

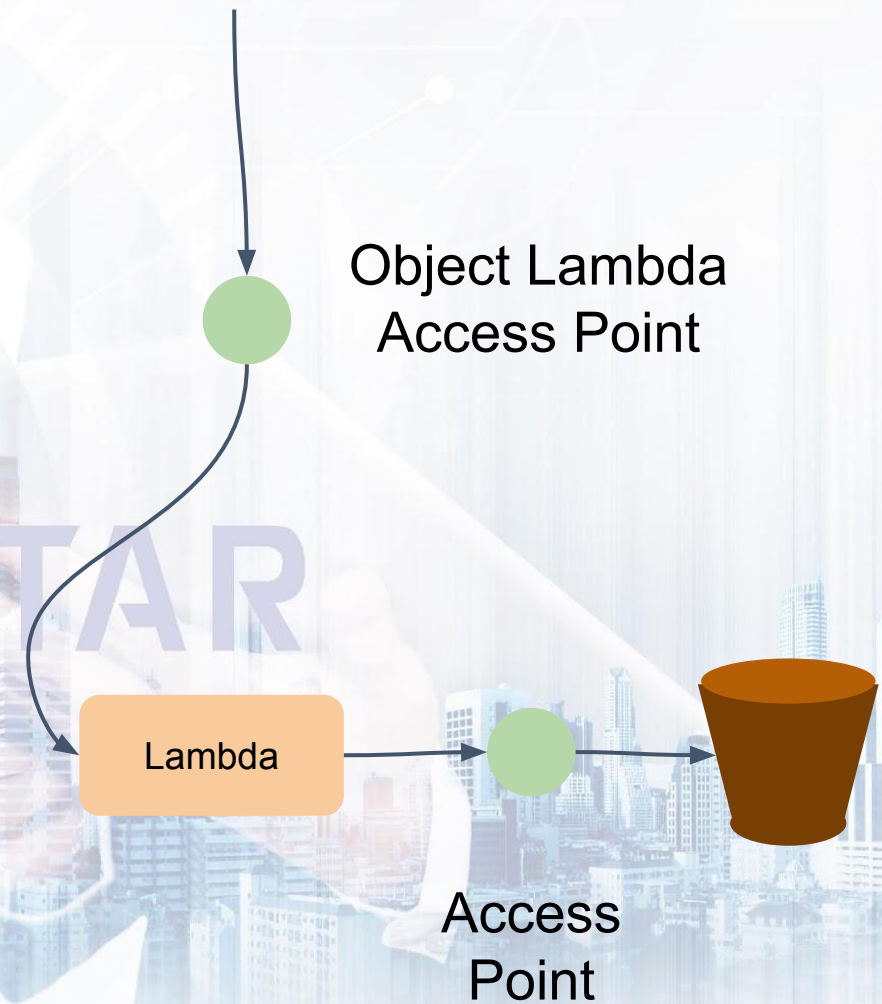
Sử dụng cùng một Endpoint,
nhưng kết nối tới Region nào
gần hơn (dựa trên latency)



Storage

S3 Object Lambda Access Point:

Thiết lập mô hình đi qua lambda để update/thay đổi thông tin, sau đó truy cập tới Access Point và trả lại thông tin mới.

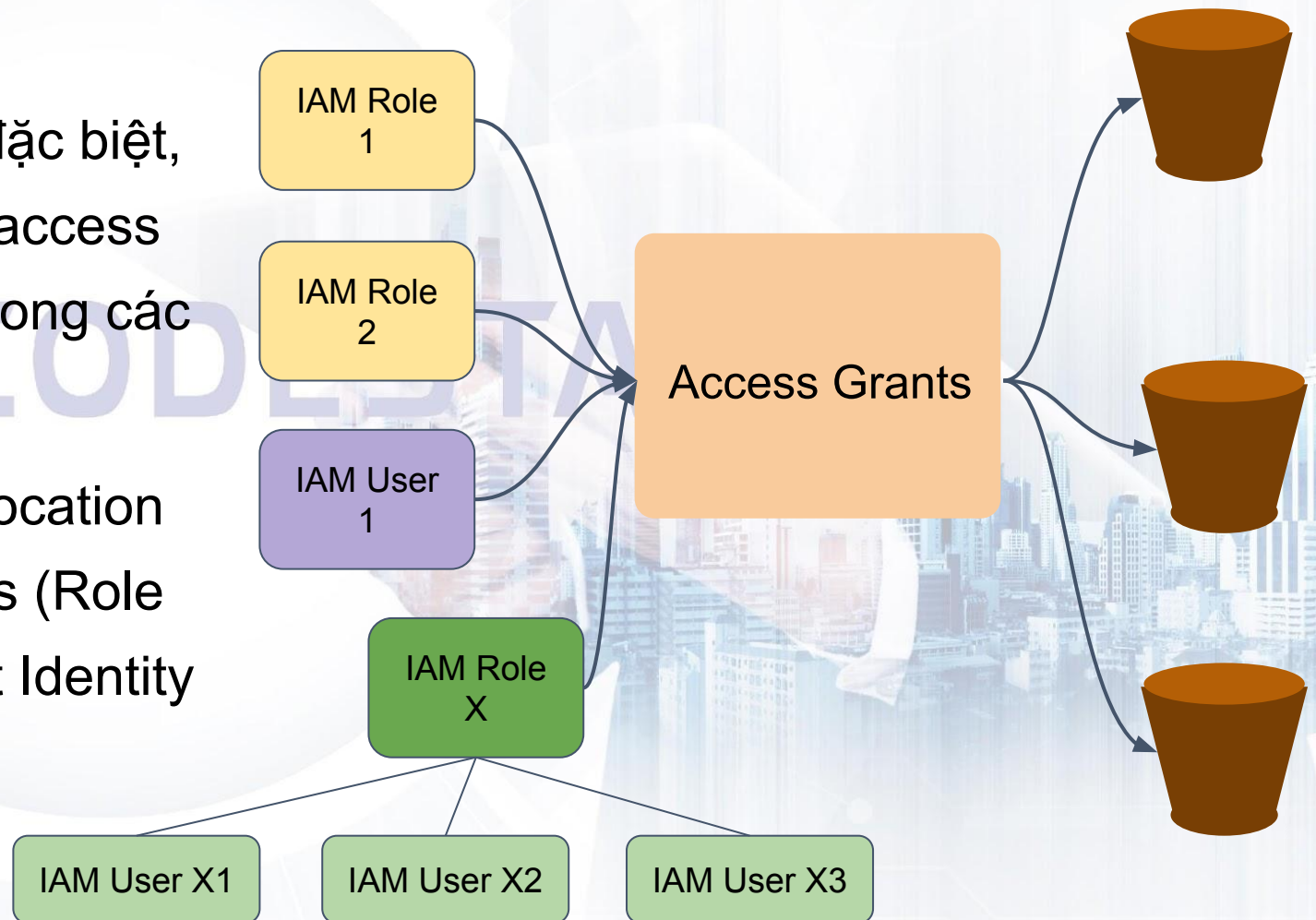


Storage

S3 Access Grant:

Access Grants là một tính năng đặc biệt, cho phép nhiều Role/User được access tới một/một số file/Prefix cụ thể trong các bucket.

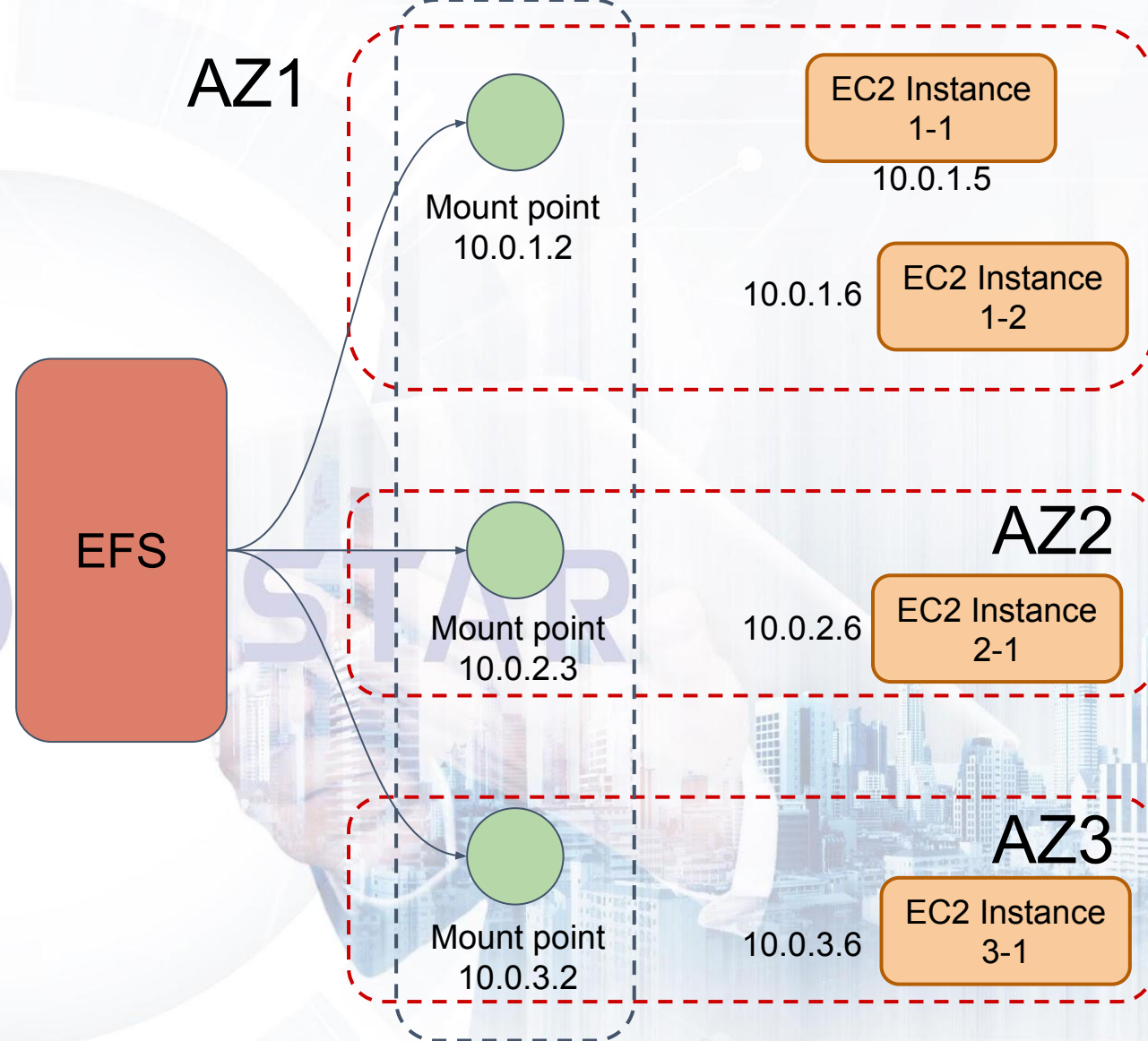
Access Grants cho phép nhiều Location (tại nhiều bucket) và nhiều Grants (Role hoặc Users, hoặc trong cùng một Identity Federation).



Storage: EFS

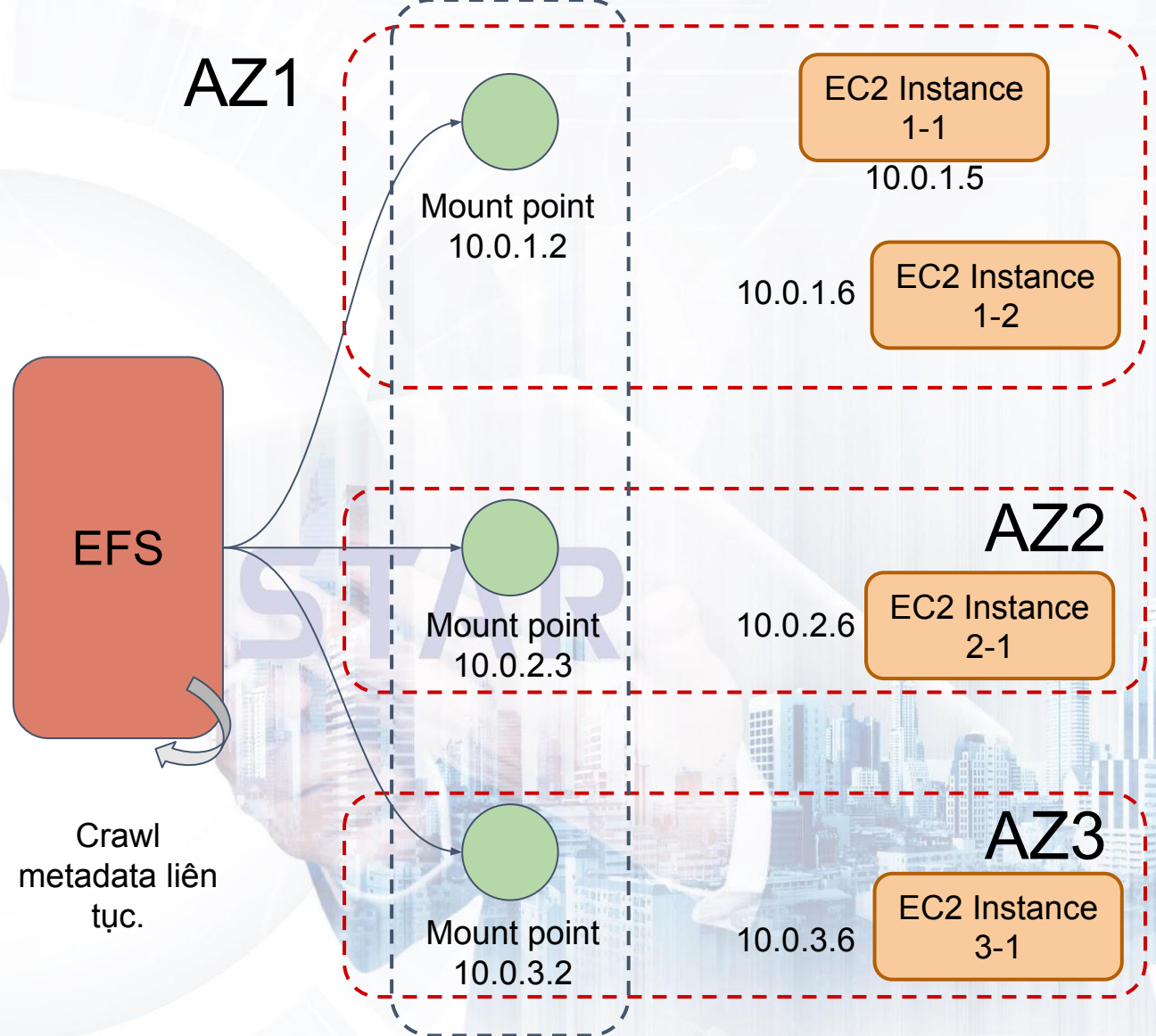
Dịch vụ cho phép tạo một Volume, sau đó mount vào các instance.

Tại vị trí mount (EC2 instance), EFS hoạt động như một ổ cứng, tương tự EBS Volume.



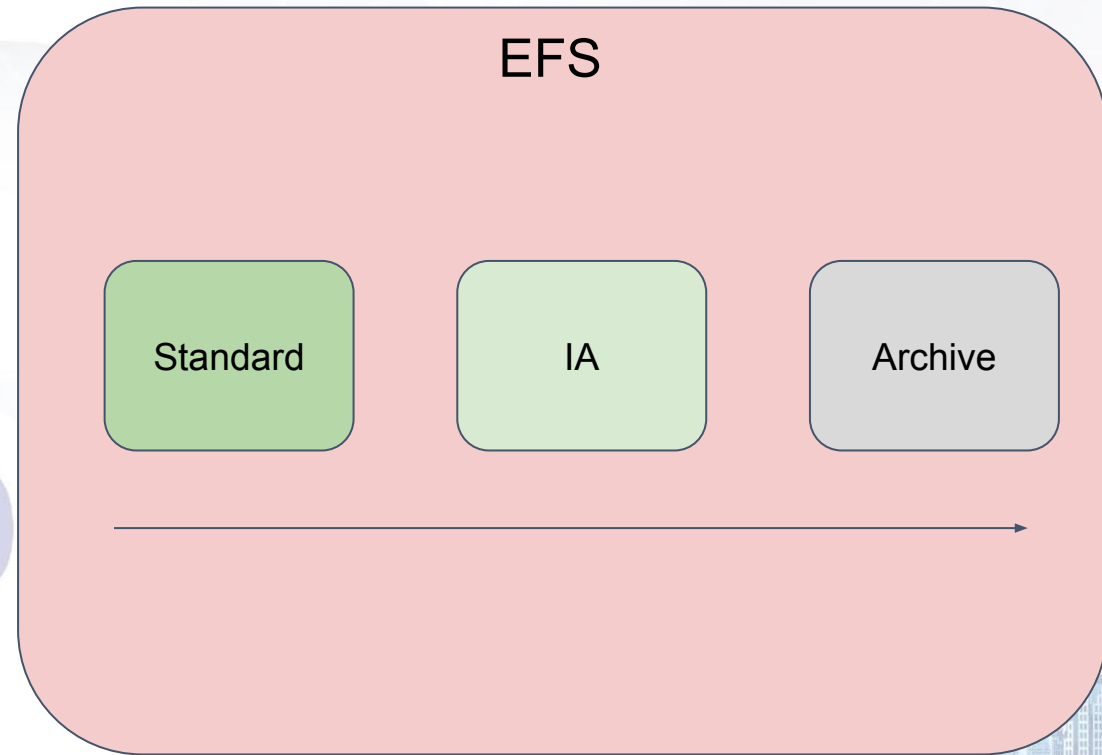
Storage: EFS

- EFS không hiển thị chính xác kích thước của ổ tại thời điểm hiện tại mà có độ trễ
- Kích cỡ của ổ được mount bởi EFS mặc định là 8 Exabyte = $8 \times 1024 \times 1024 \times 1024$ GB.
- Một EFS có thể mount vào nhiều EC2 Instance và hoạt động đồng thời với nhau.



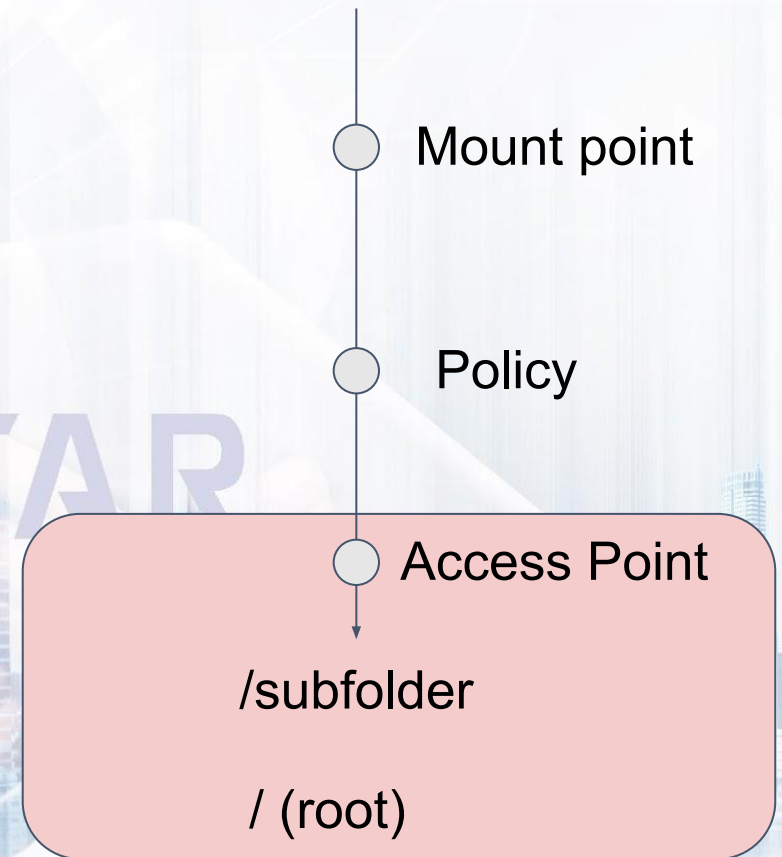
Storage: EFS

- EFS có các loại Storage Class:
- **Standard**: Lưu trữ dữ liệu truy xuất thường xuyên
- **Infrequent Access (IA)**: Lưu trữ dữ liệu ít truy cập
- **Archive**: Lưu trữ dữ liệu.



Storage: EFS

- EFS có thể gắn **File system Policy** để cho phép những service khác được sử dụng resource của mình.
- **Access point**: tạo ra một điểm truy cập vào folder con nằm trong EFS.
- **Mount point**: Điểm truy cập từ bên ngoài cho phép các thành phần trong mạng có thể truy cập tới.





THANK YOU