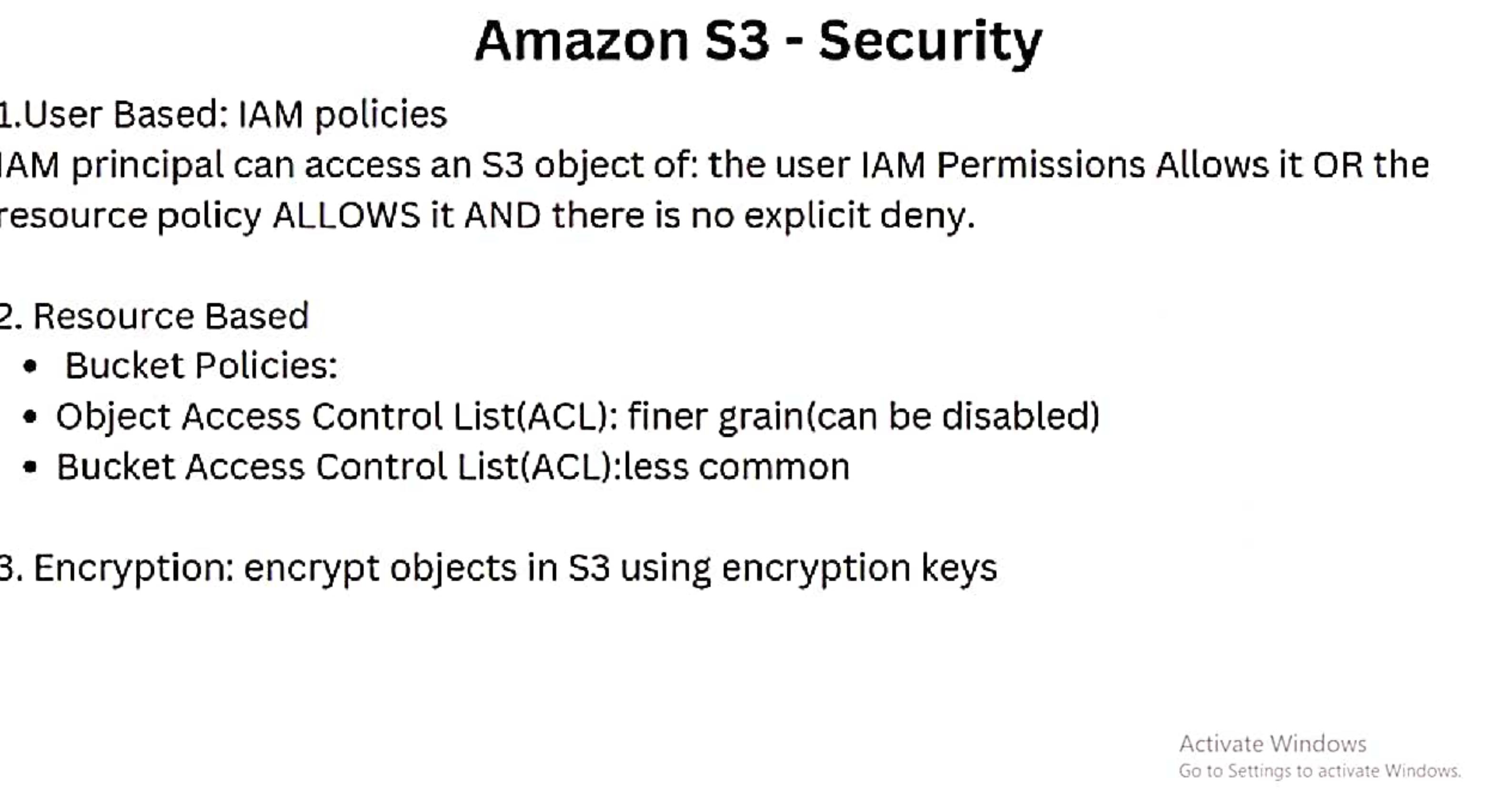
SESSION 9



Amazon S3 - Security

1.User Based: IAM policies

IAM principal can access an S3 object of: the user IAM Permissions Allows it OR the resource policy ALLOWS it AND there is no explicit deny.

2. Resource Based

- Bucket Policies:
- Object Access Control List(ACL): finer grain(can be disabled)
- Bucket Access Control List(ACL):less common

3. Encryption: encrypt objects in S3 using encryption keys

S3 Bucket Policy

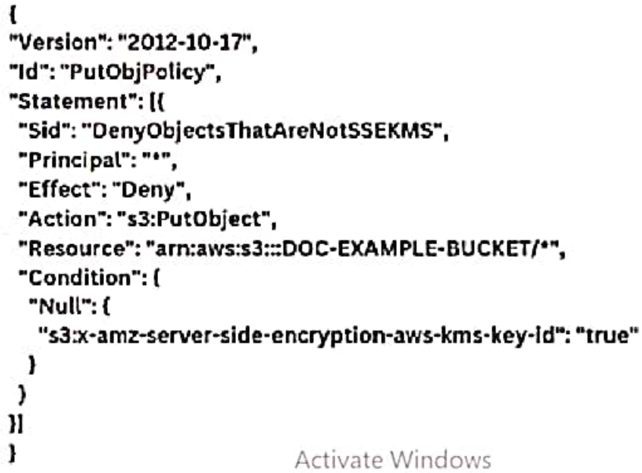
With Amazon S3 bucket policies, you can secure access to objects in your buckets, so that only users with the appropriate permissions can access them. You can even prevent authenticated users without the appropriate permissions from accessing your Amazon S3 resources.

It is JSON based policies

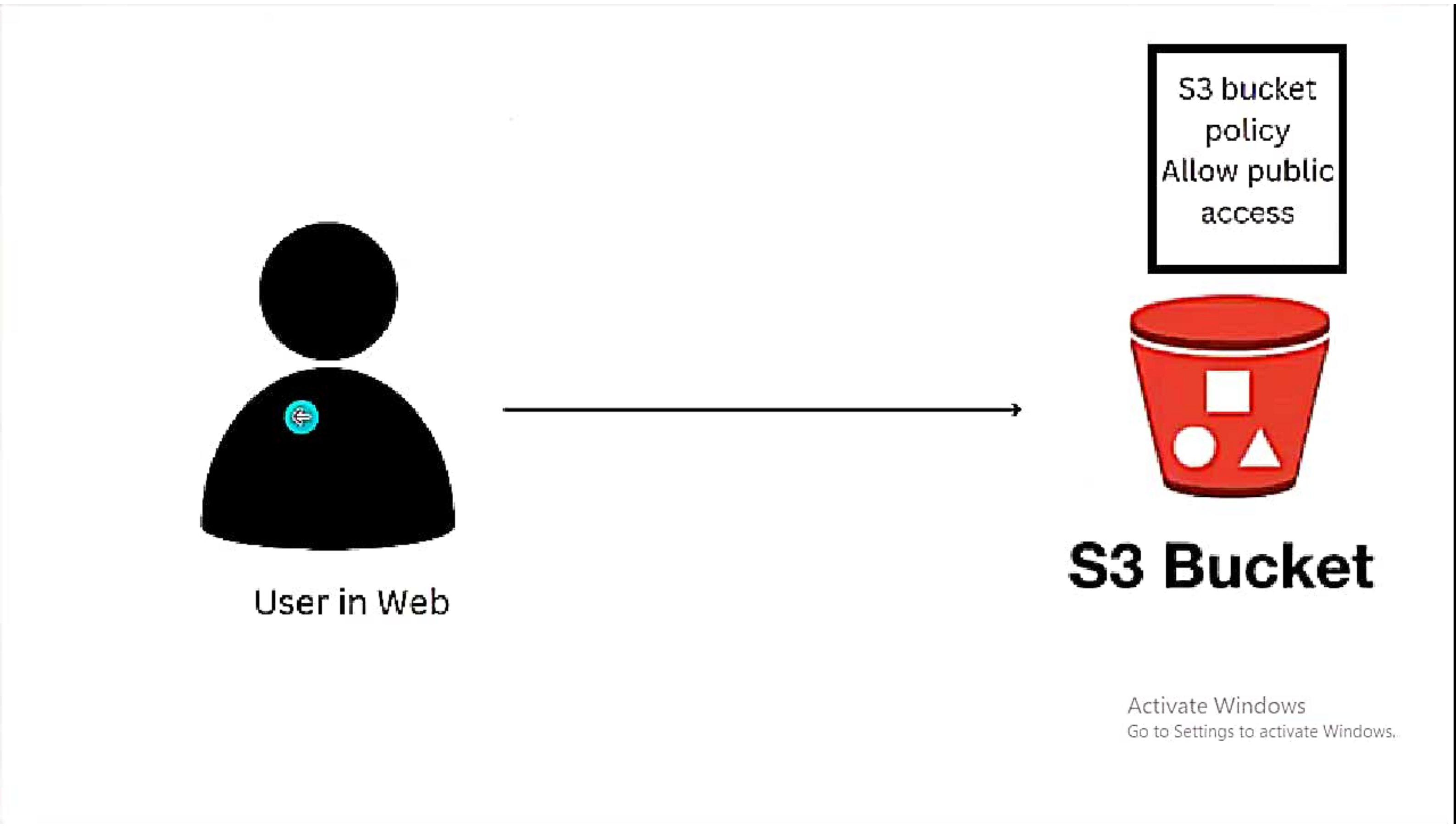
- Resources: buckets and objects
- Effect Allow/Deny →
- Actions: Set of API to allow/Deny
- Principal: the account/user to apply the policy to

We use S3 bucket policy to:

- Grant public access to the bucket
- Force objects to be encrypted at upload
- Grant Access to another account



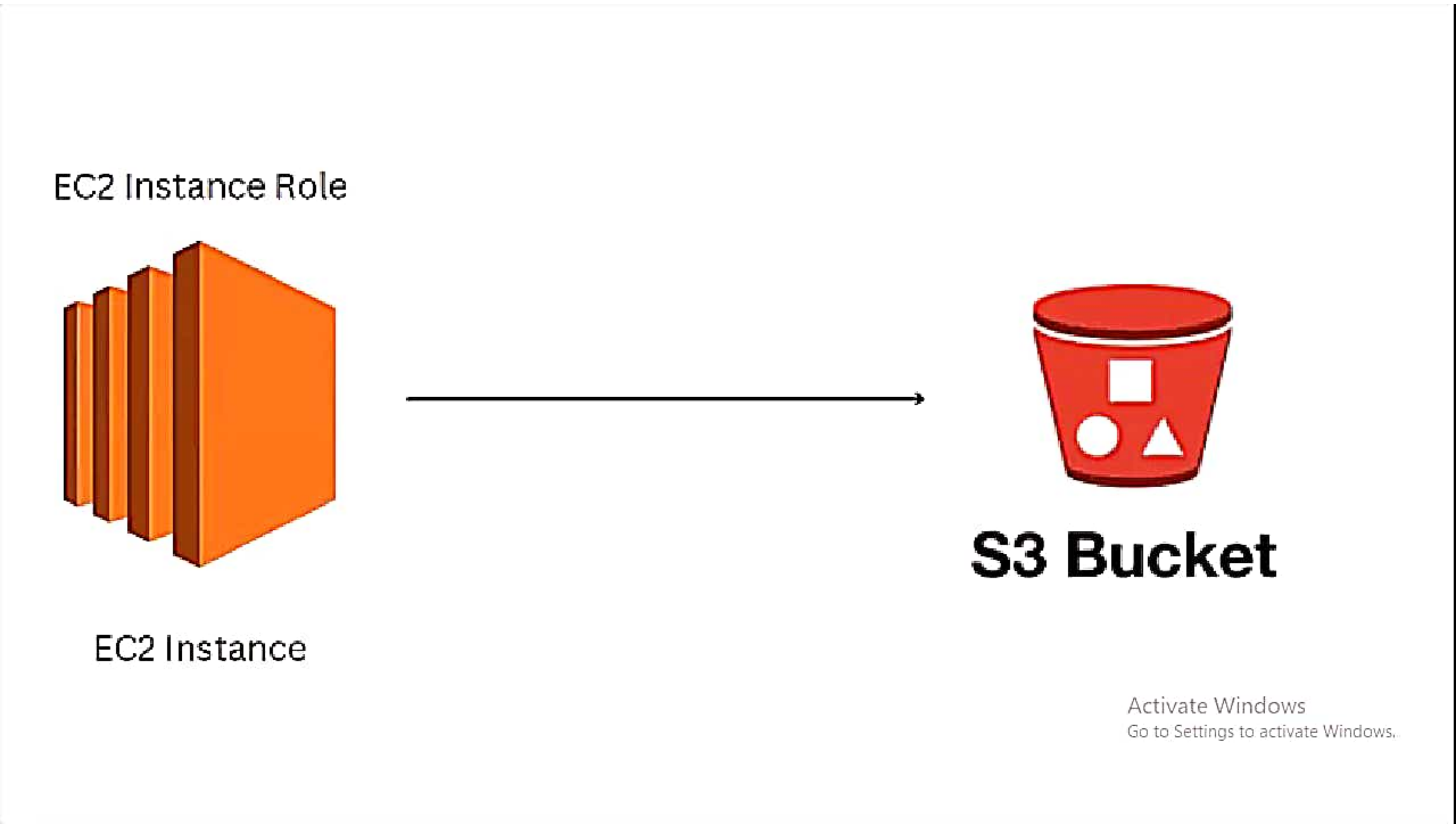
```
{
"Version": "2012-10-17",
"Id": "PutObjPolicy",
"Statement": [{
 "Sid": "DenyObjectsThatAreNotSSEKMS",
 "Principal": "*",
 "Effect": "Deny",
 "Action": "s3:PutObject",
 "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
 "Condition": {
  "Null": {
   "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
  }
 }
}]
}
```

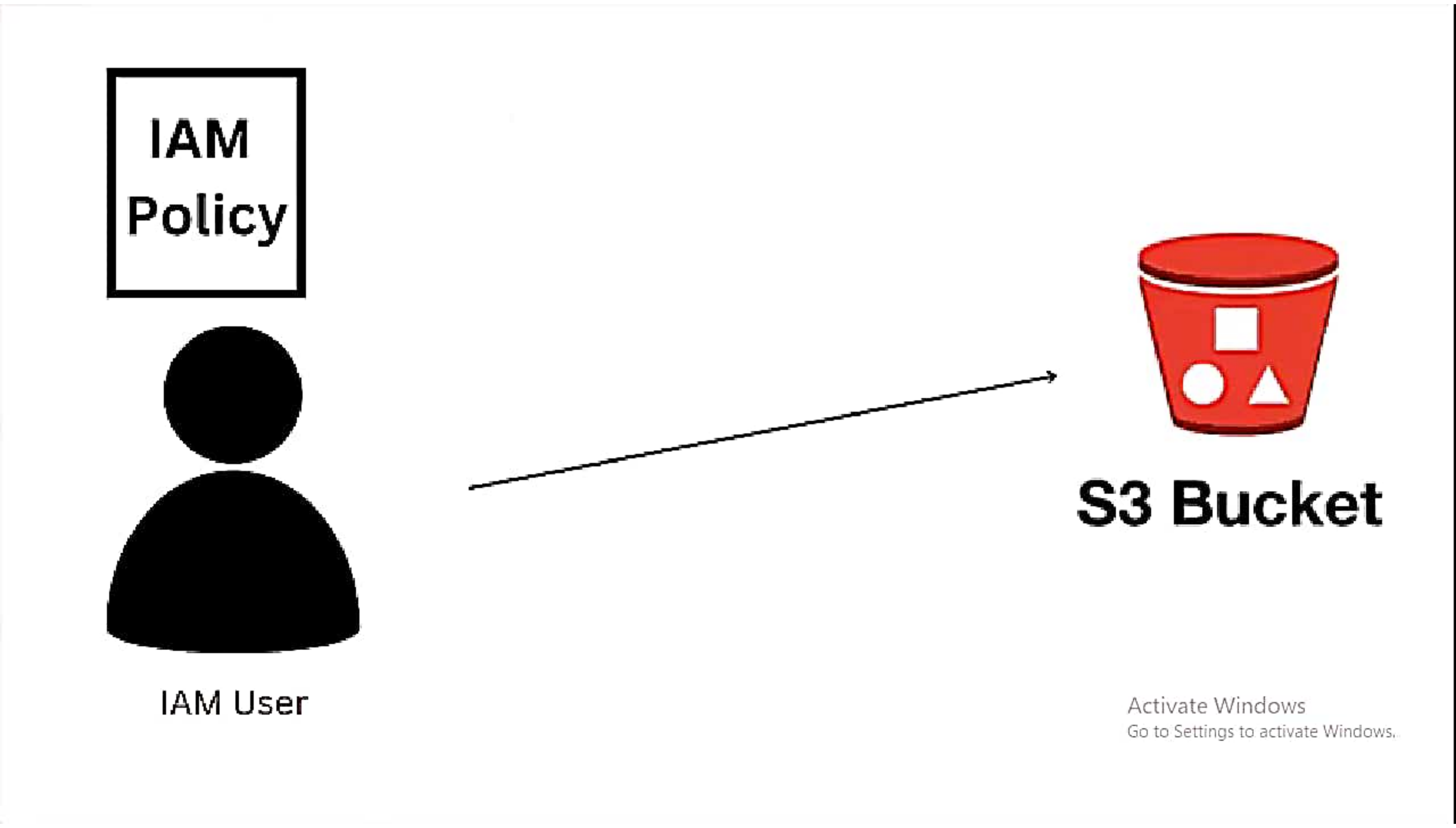


S3 bucket policy Allow public access

User in Web

S3 Bucket

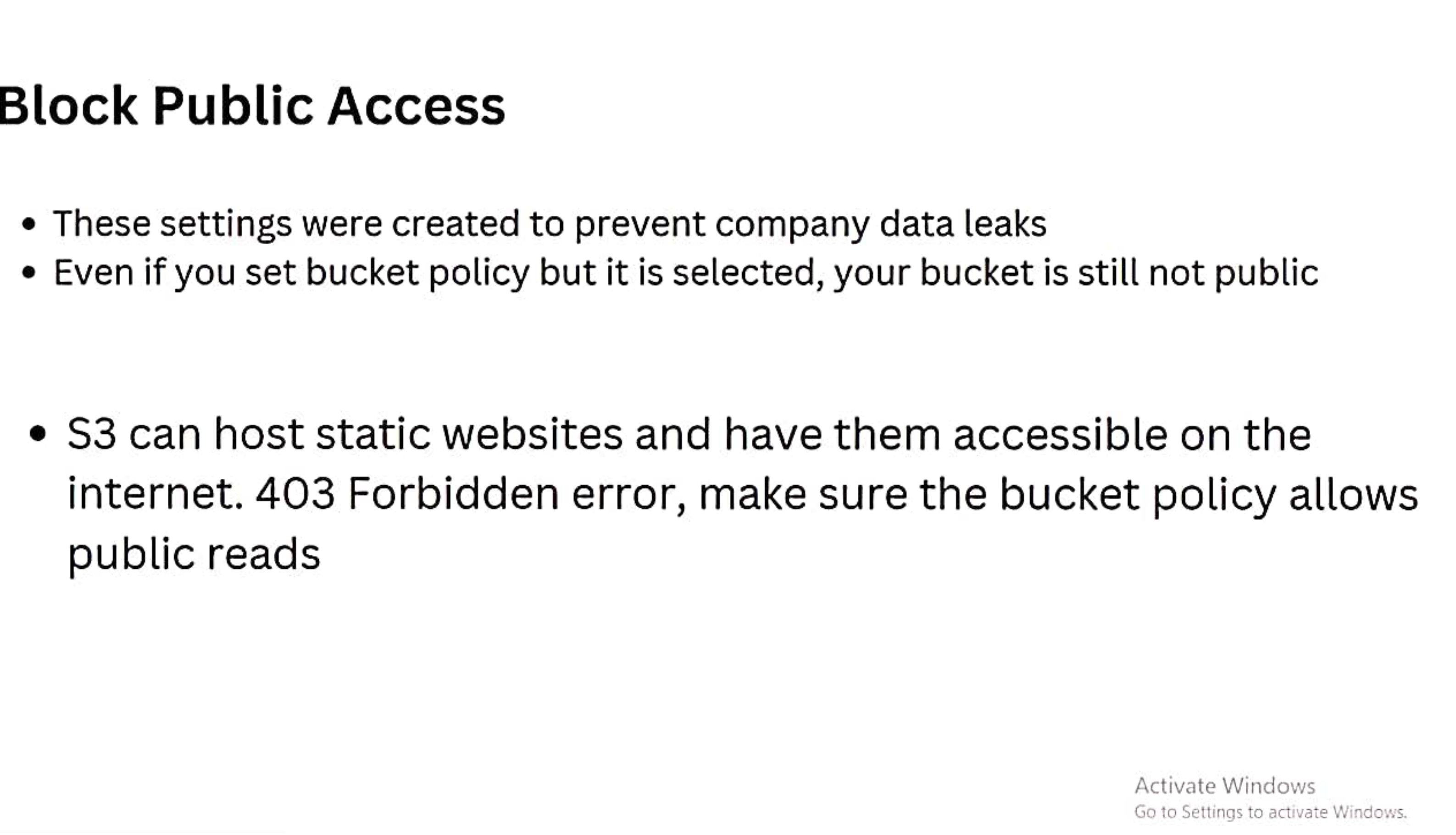

EC2 Instance Role
EC2 Instance
S3 Bucket
Activate Windows
Go to Settings to activate Windows.



IAM Policy

IAM User

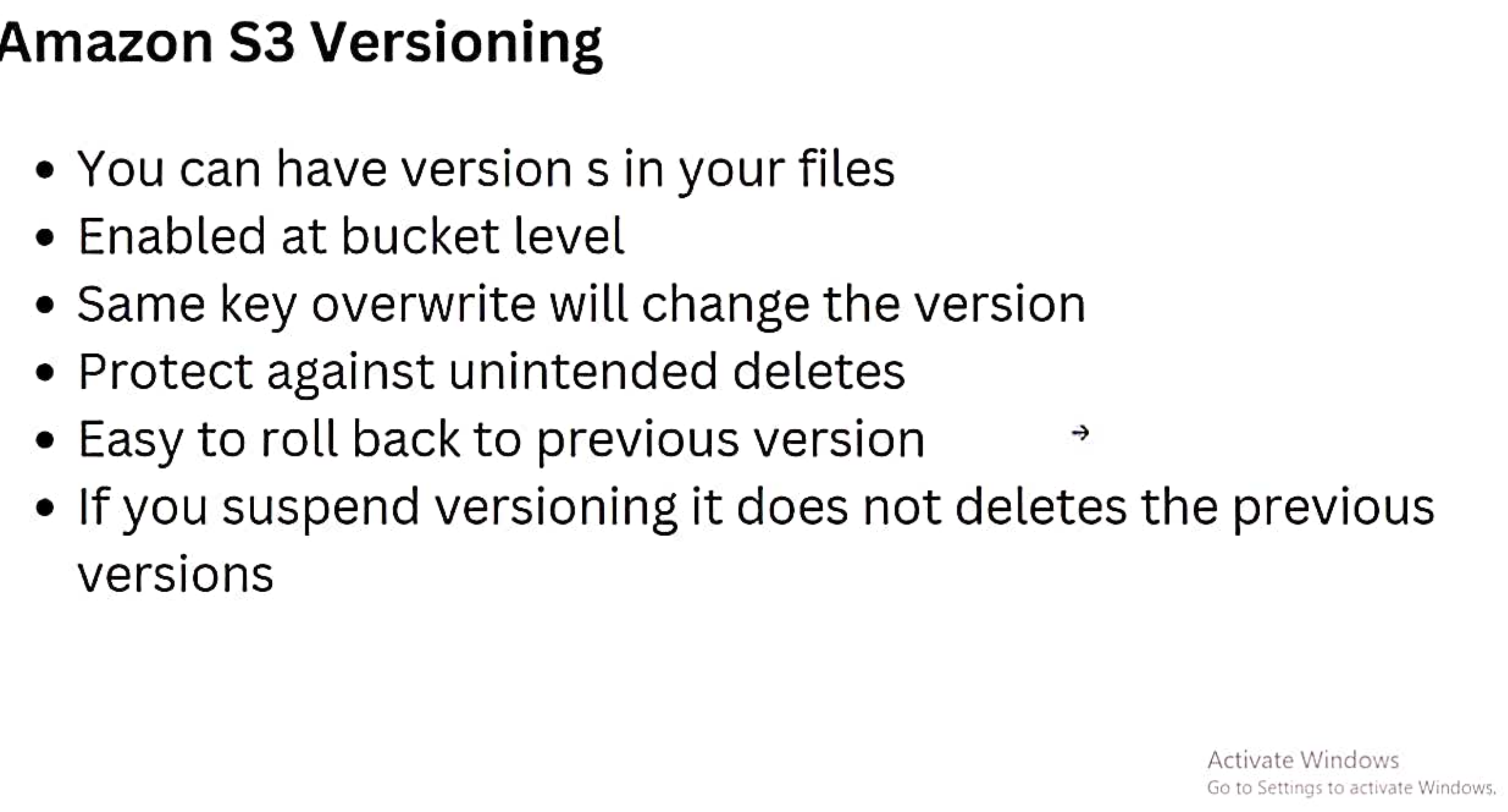
S3 Bucket



Block Public Access

- These settings were created to prevent company data leaks
- Even if you set bucket policy but it is selected, your bucket is still not public

- S3 can host static websites and have them accessible on the internet. 403 Forbidden error, make sure the bucket policy allows public reads

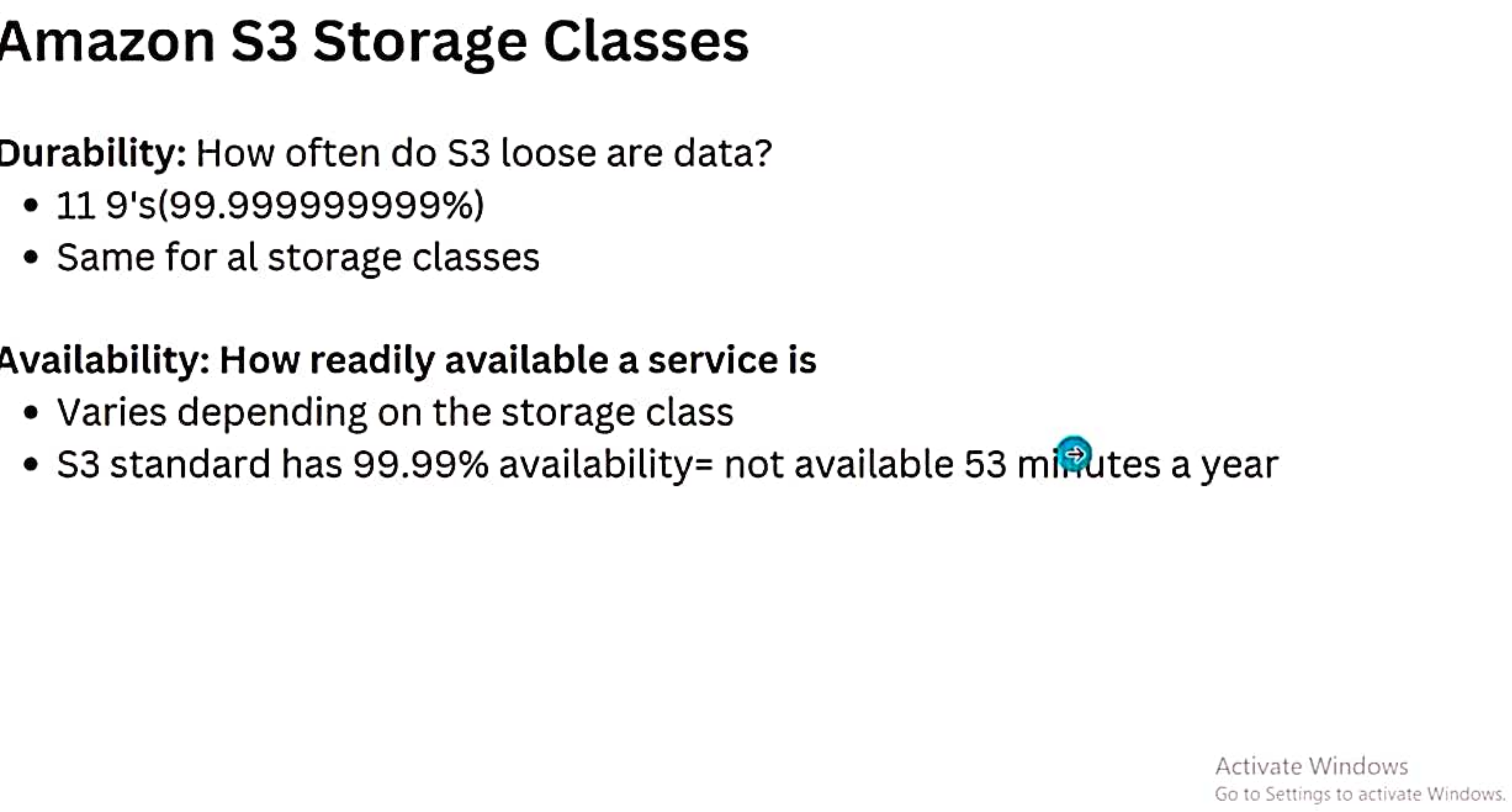


Amazon S3 Versioning

- You can have version s in your files
- Enabled at bucket level
- Same key overwrite will change the version
- Protect against unintended deletes
- Easy to roll back to previous version
- If you suspend versioning it does not deletes the previous versions

S3 Encryption

- **Server -Side Encryption(Default)** always on. Server encrypts the file after recieving it
- **Client_Side Encryption:** Clients encrypts the file before uploading it.



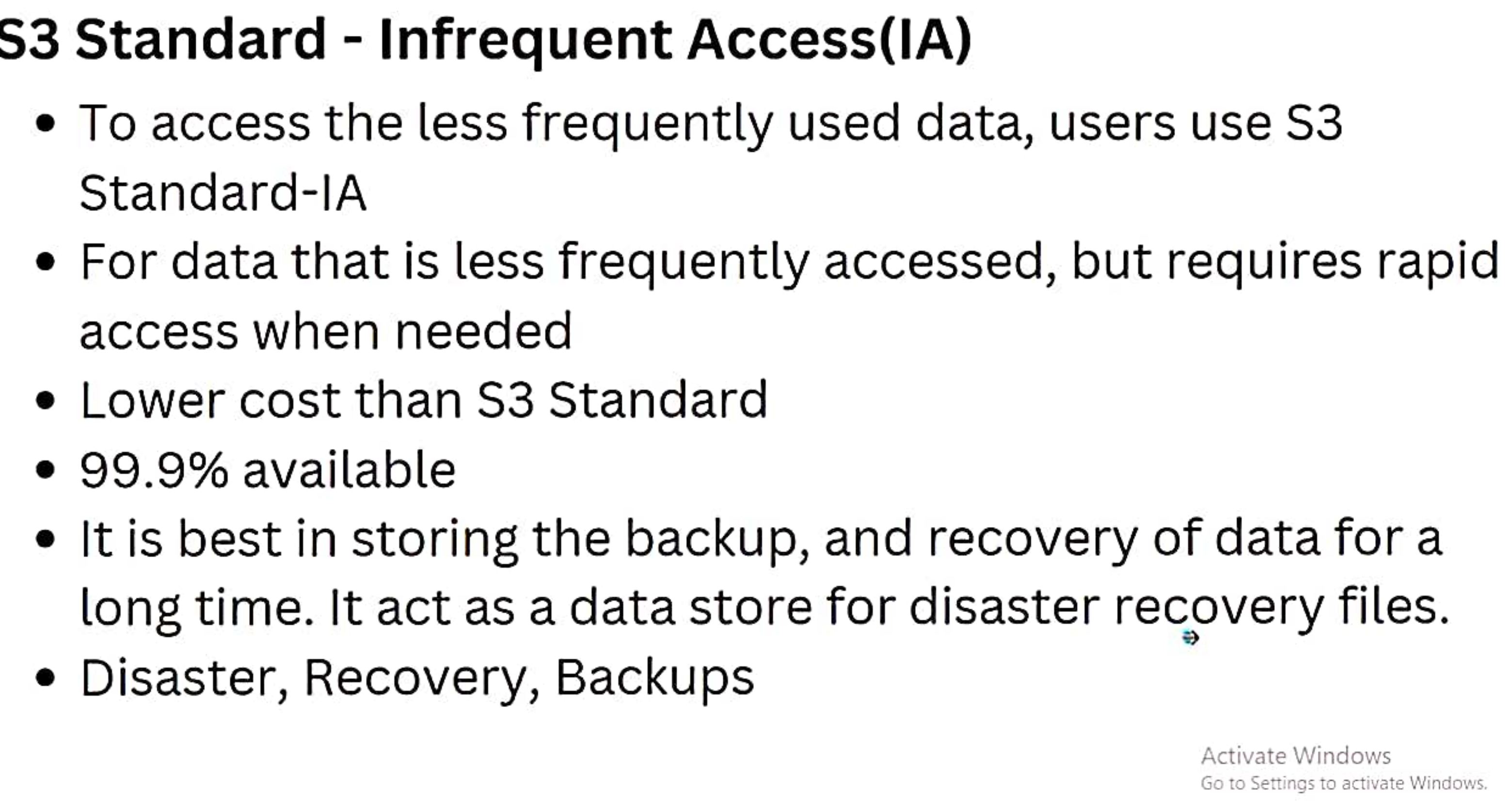
Amazon S3 Storage Classes

Durability: How often do S3 loose are data?

- 11 9's(99.999999999%)
- Same for al storage classes

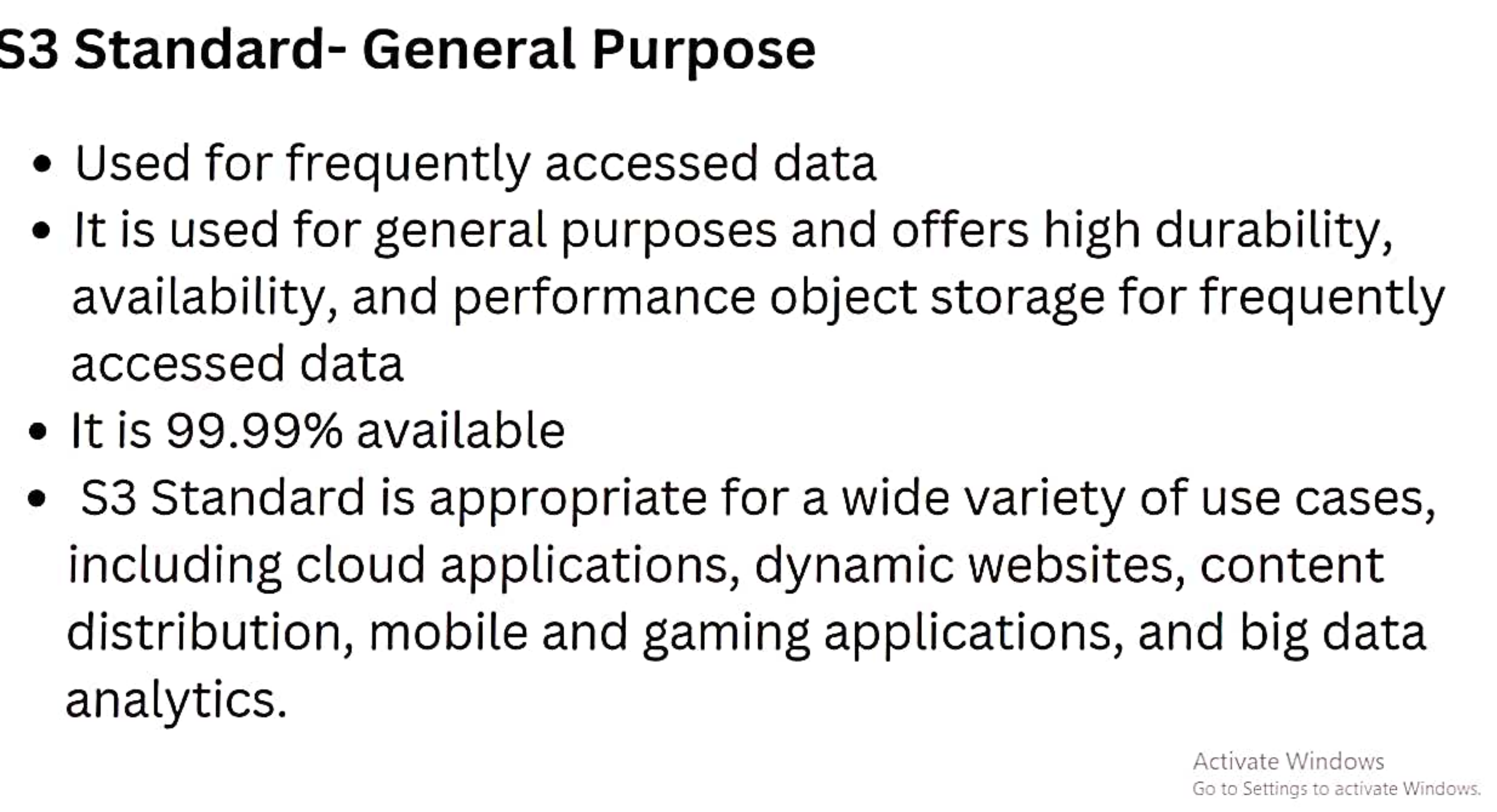
Availability: How readily available a service is

- Varies depending on the storage class
- S3 standard has 99.99% availability= not available 53 minutes a year



S3 Standard - Infrequent Access(IA)

- To access the less frequently used data, users use S3 Standard-IA
- For data that is less frequently accessed, but requires rapid access when needed
- Lower cost than S3 Standard
- 99.9% available
- It is best in storing the backup, and recovery of data for a long time. It act as a data store for disaster recovery files.
- Disaster, Recovery, Backups



S3 Standard- General Purpose

- Used for frequently accessed data
- It is used for general purposes and offers high durability, availability, and performance object storage for frequently accessed data
- It is 99.99% available
- S3 Standard is appropriate for a wide variety of use cases, including cloud applications, dynamic websites, content distribution, mobile and gaming applications, and big data analytics.

Amazon S3 One Zone-Infrequent Access(IA)

- S3 Storage Classes which store data in a minimum of three Availability Zones, S3 One Zone-IA stores data in a single Availability Zone.
- Data is lost when AZ is destroyed.
- 99.5% Available
- It’s a very good choice for storing secondary backup copies of on-premises data or easily re-creatable data.

S3 Glacier Storage Class

- Low cost object storage meant for archiving or backup
- Pricing= price of storage+object retrieval cost

S3 Glacier Instant Retrieval

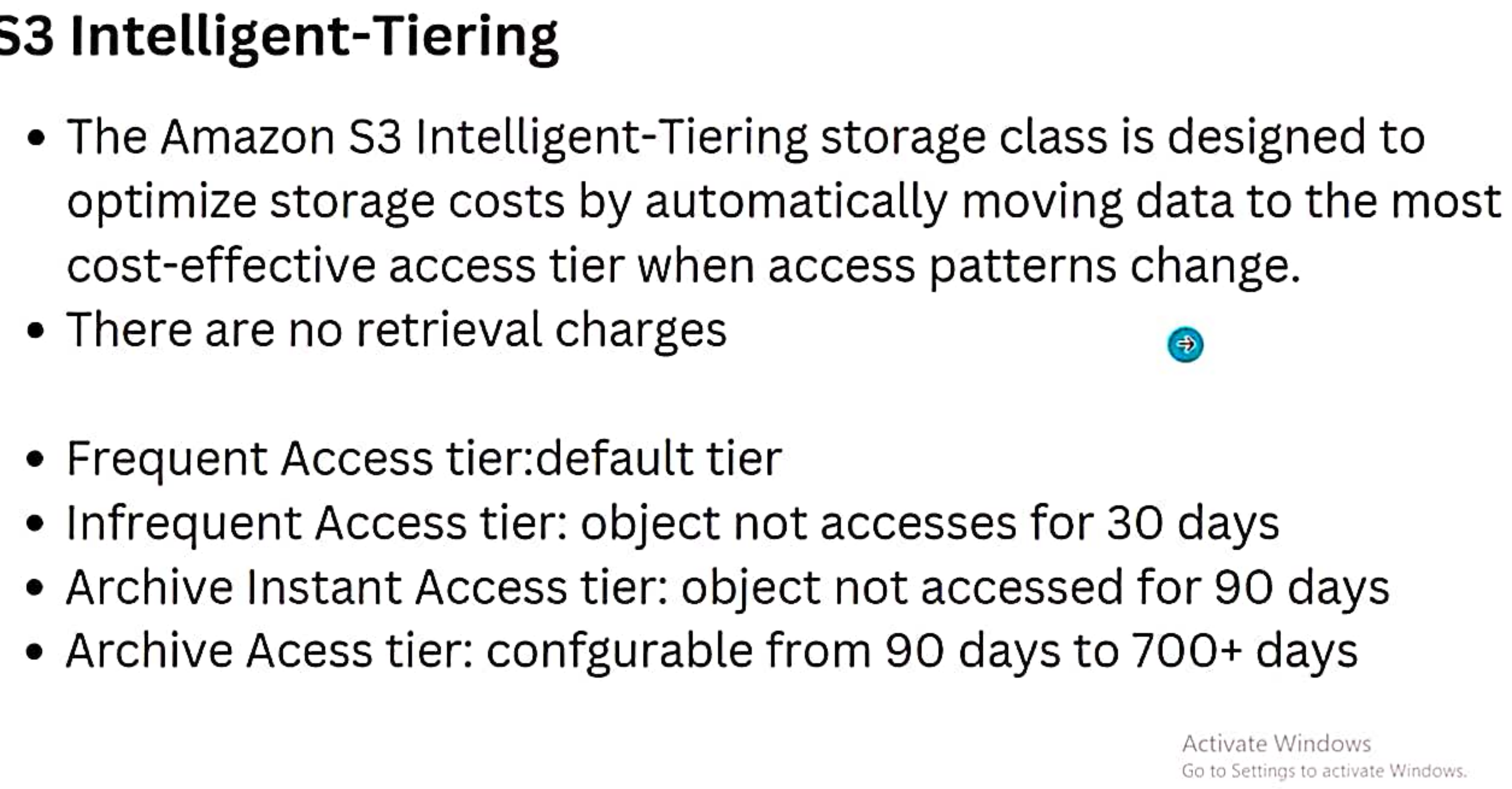
- It just takes milliseconds to recover the data
- Minimum storage duration=90 days

S3 Glacier Flexible Retrieval

- It provides low-cost storage compared to S3 Glacier Instant Retrieval.
- Expedite(1 to 5 min), Standard(3-5 hrs), Bulk(5 to 12 hrs)
- Minimum storage duration=90 days

S3 Glacier Deep Archive

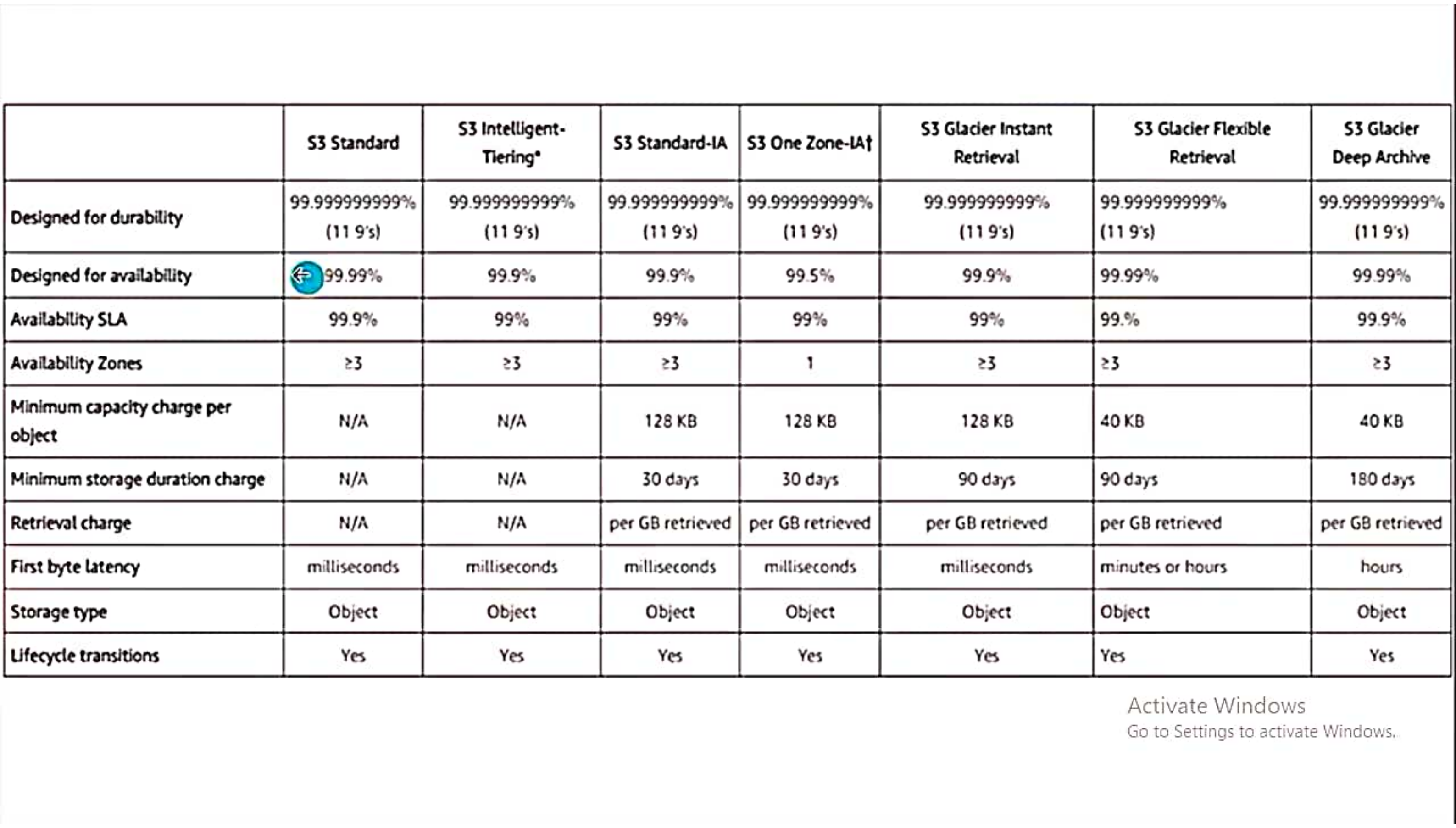
- For long term storage
- Standard(12 hours), Bulk(48 hrs)
- Minimum storage duration=180 days



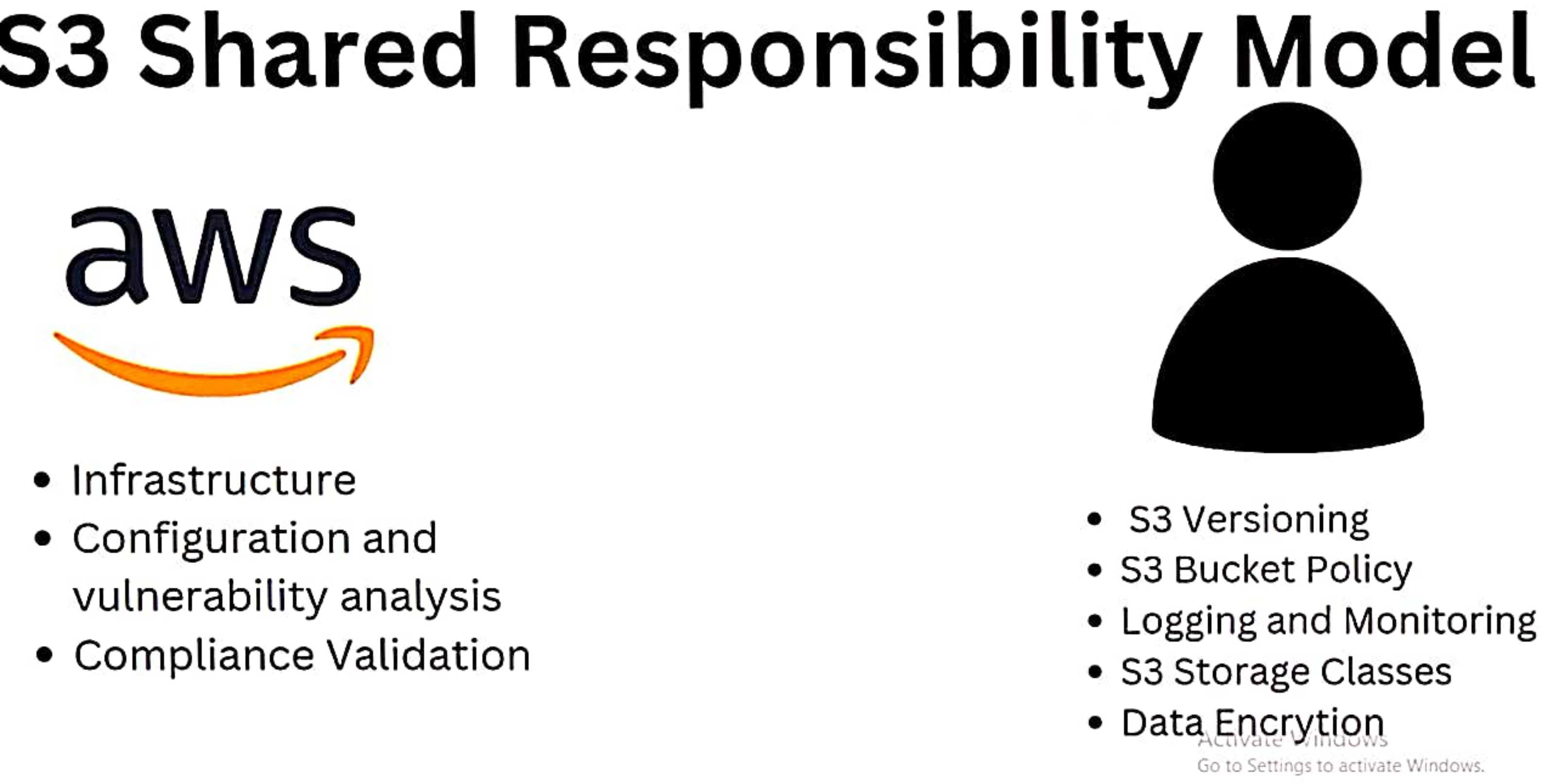
S3 Intelligent-Tiering

- The Amazon S3 Intelligent-Tiering storage class is designed to optimize storage costs by automatically moving data to the most cost-effective access tier when access patterns change.
- There are no retrieval charges

- Frequent Access tier:default tier
- Infrequent Access tier: object not accesses for 30 days
- Archive Instant Access tier: object not accessed for 90 days
- Archive Acess tier: confgurable from 90 days to 700+ days



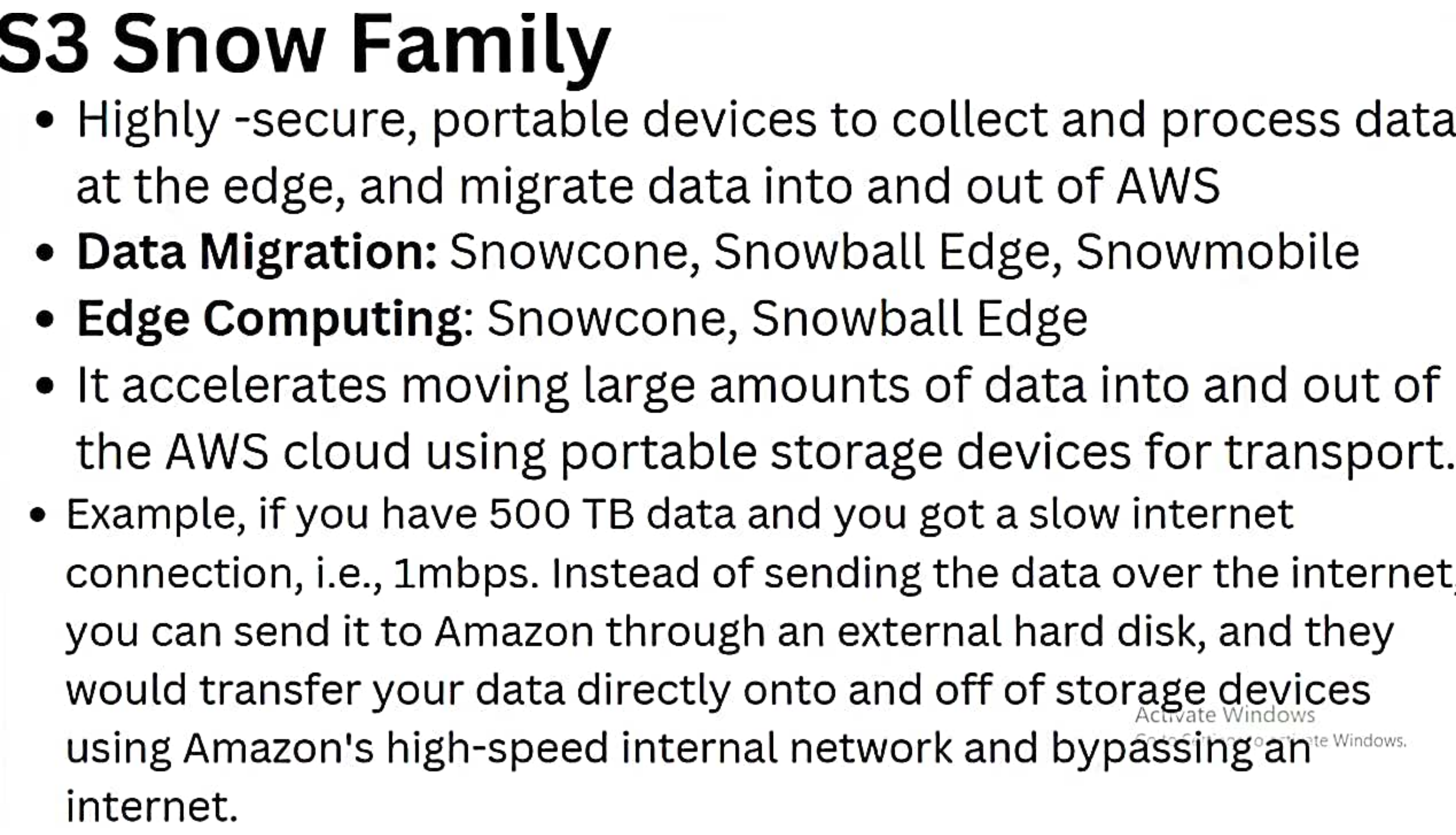
	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier Instant Retrieval	S3 Glacier Flexible Retrieval	S3 Glacier Deep Archive
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	99.9%	99.99%	99.99%
Availability SLA	99.9%	99%	99%	99%	99%	99.%	99.9%
Availability Zones	≥3	≥3	≥3	1	≥3	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128 KB	128 KB	128 KB	40 KB	40 KB
Minimum storage duration charge	N/A	N/A	30 days	30 days	90 days	90 days	180 days
Retrieval charge	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	milliseconds	milliseconds	milliseconds	milliseconds	minutes or hours	hours
Storage type	Object	Object	Object	Object	Object	Object	Object
Lifecycle transitions	Yes	Yes	Yes	Yes	Yes	Yes	Yes



S3 Shared Responsibility Model

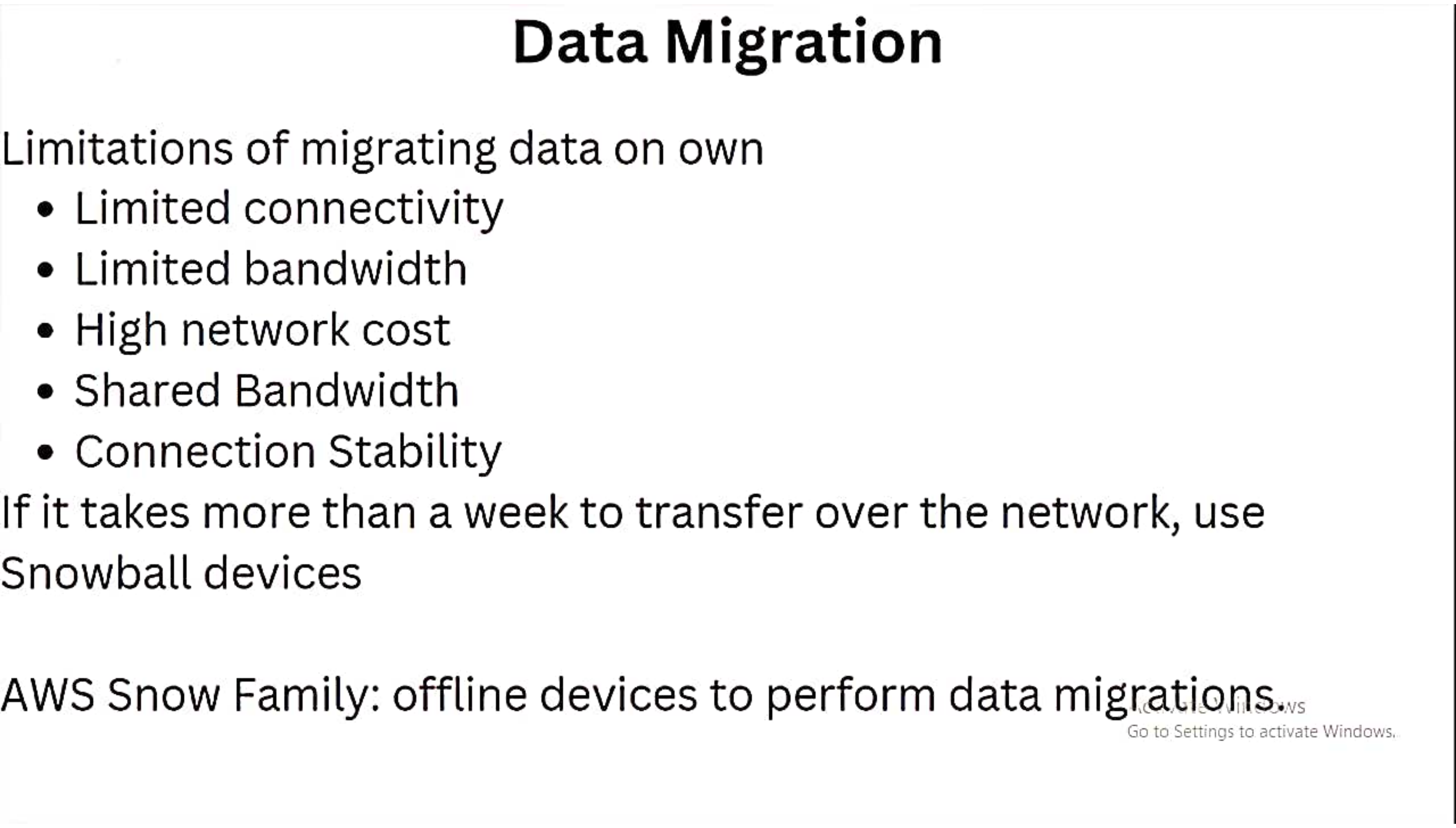
- Infrastructure
- Configuration and vulnerability analysis
- Compliance Validation

- S3 Versioning
- S3 Bucket Policy
- Logging and Monitoring
- S3 Storage Classes
- Data Encrytion



S3 Snow Family

- Highly -secure, portable devices to collect and process data at the edge, and migrate data into and out of AWS
- **Data Migration:** Snowcone, Snowball Edge, Snowmobile
- **Edge Computing**: Snowcone, Snowball Edge
- It accelerates moving large amounts of data into and out of the AWS cloud using portable storage devices for transport.
- Example, if you have 500 TB data and you got a slow internet connection, i.e., 1mbps. Instead of sending the data over the internet you can send it to Amazon through an external hard disk, and they would transfer your data directly onto and off of storage devices using Amazon's high-speed internal network and bypassing an internet.



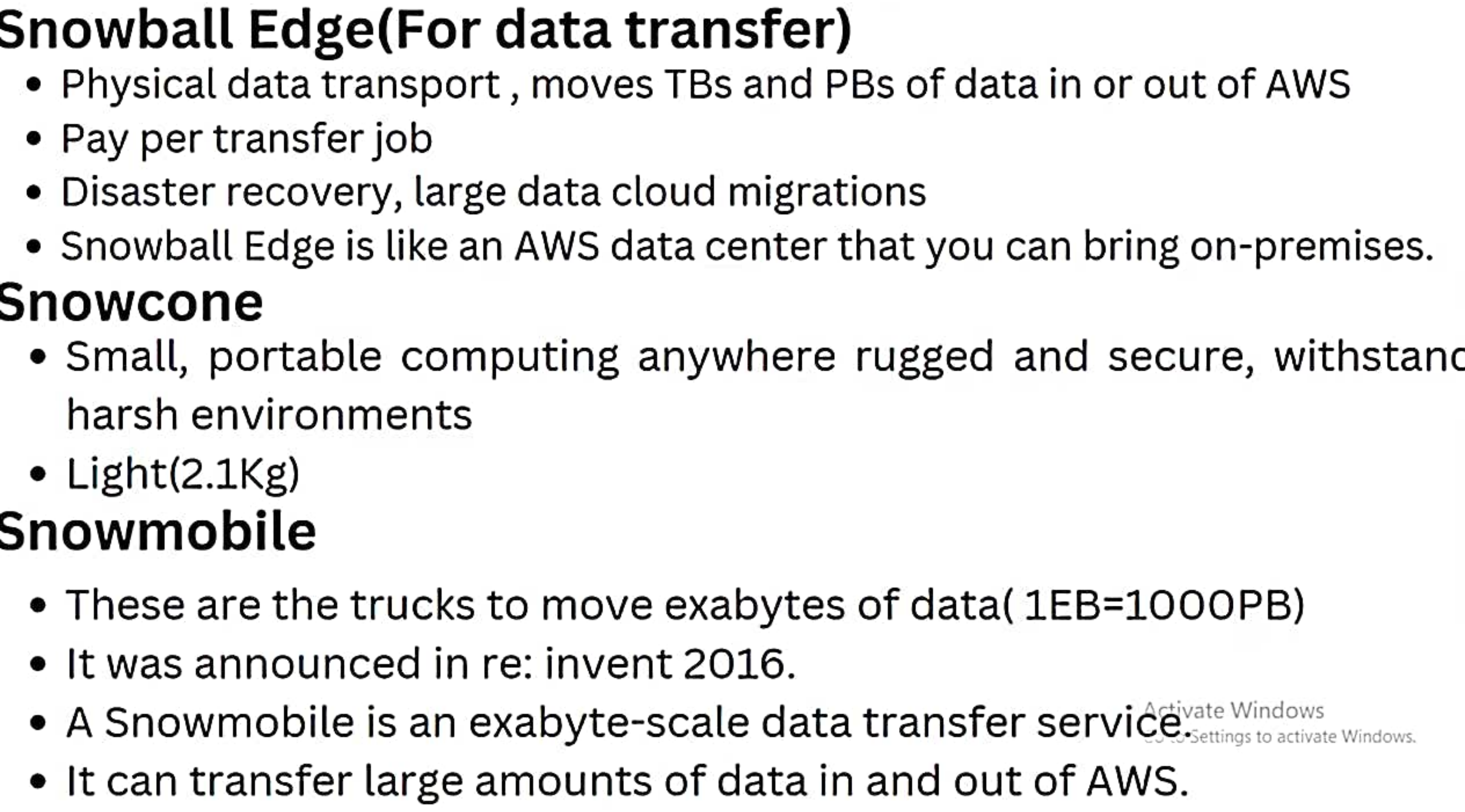
Data Migration

Limitations of migrating data on own

- Limited connectivity
- Limited bandwidth
- High network cost
- Shared Bandwidth
- Connection Stability

If it takes more than a week to transfer over the network, use Snowball devices

AWS Snow Family: offline devices to perform data migrations.



Snowball Edge(For data transfer)

- Physical data transport , moves TBs and PBs of data in or out of AWS
- Pay per transfer job
- Disaster recovery, large data cloud migrations
- Snowball Edge is like an AWS data center that you can bring on-premises.

Snowcone

- Small, portable computing anywhere rugged and secure, withstand harsh environments
- Light(2.1Kg)

Snowmobile

- These are the trucks to move exabytes of data(1EB=1000PB)
- It was announced in re: invent 2016.
- A Snowmobile is an exabyte-scale data transfer service.
- It can transfer large amounts of data in and out of AWS.

Edge Computing

- Process data while it's being created on an edge location(a truck, a ship). These locations may have limited/ no internet access.
- We setup a Snowball Edge/Snowcone device to do edge computing

Questions

1. Which S3 Storage Class is the most cost-effective for archiving data with no retrieval requirement
2. What is a petabyte-scale data moving service in or out of AWS with computing capabilities
3. Which is an exabyte scale data moving service in or out of AWS
4. What are objects not composed of: Key, Value, Access Key, Metadata
5. Where are objects stored in Amazon S3?

1. S3 Glacier Deep Archive 2. Snowball Edge 3. Snowmobile
4. Access Key 5. Bucket