|  |
| --- |
| Machine generated alternative text: MFA with CLI  • To use MFA with the CLI, you must create a temporary session  • To do so, you must run the STS GetSessionToken API call  • aws Sts get-session-token --serial-number am-of-the-mfa-device --token-  code code-from-token --duration-seconds 3600  "Credentials":  "SecretAccessKey": "secret—access—key" ,  "SessionToken": "temporary—session—token" ,  " Expiration": ,  "AccessKeyId" :      **Step 1)**    **Enabled mfa in security credential of user iam**    Machine generated alternative text: avvS  Iden tity and Access  Management (IAM)  Identity providers  settings  Access reports  activity  Sewice Control  Resource Groups  Uses  Summary  creation tin.  Sign-in credentials  2018&-191323 uTC*01m  Global  Ena—  password  MFA  Access keys  •use acces to REST HTTP AVG APB_ you *tare wdh AS a  we key rotatm  Create ac•ss k"  Access key ID  2018-11-2614:21 UTC*01cn 2020-os.ca-49  Active  Make inactive    Machine generated alternative text: aws Sts get-session—token help  aws Sts get—session—token —serial—number arn:aws:iam: :387124123361:mfa/stephane —token—code 82846*    **Note : now we will get credential**    Machine generated alternative text: "Credentials" .  "AccessKeY1d": "ASIAVUITFK3Q61NEXA5K" ,  ' 'SecretAccessKey" : "XEucPd1SiCOG50zFFeOGyJzvzCquARxkq2n6jm+T" ,  "SessionToken": "IQoJb3JpZ21uX2VjEFoaCWILXd1c3QtMSJ+1EUCIAN01+VRyYAdQgPd5a6FkodfL46egGauG9EKF6XBhvWOAiEA2T5Yk1TOsGSuPpzKp1nmbbh  y/CQrWZ093nFH17bJcoqsOE1k// // EiDAC1 FfReoRyddoOD6SqFAZITUf1Dwn8/080VOKØHCoFOrB136VZH59ØntGqKn/DIXk1 ITJtRDx  3 nGt+8Kpe4LLZi IGeegxzj j u r7 j æxY4Br334BhX1fpgZRk-w8YDgsQCSbsq6gVR9+pQø8witXG9QlJ63gE  ZG040NR-J j J Les BIG keBiC1uøseLJUV/n+0isRxeGmhSygbrFJPXayC3n9rK19e1vibkB19kvBz51JuXxLpøt9ZseDRQlJykEWQ rm1Ms IWROJMOPLmk+XhL rtgupi 171hLXj zppq8W  do IDØwcZk+dMOJEK3Pzk11YU-" ,  "Expiration  ( END)    Machine generated alternative text: aws Sts get-session—token help  aws Sts get—session—token —serial—number arn:aws:iam: :387124123361:mfa/stephane  aws Sts get—session—token —serial—number  aws configure —profile mfa  AWS Access Key ID (None) : ASIAVUITFK3QIJO'WRTSW1  AWS Secret Access Key (None) : M9dqxXYLIQfdXi+QOOiuX/FPMgNp2RL8mHYudzNB  Default region name (Nonel :  Default output format (None):  —token-code 828463  —token-code 889485      Machine generated alternative text: AVVS SDK Overview  • What if you want to perform actions on AWS directly from your applications  code ? (without using the CLI).  • You can use an SDK (software development kit) !  • Official SDKs are...  • Java  • .NET  Node.js  •  • Python (named bot03 / botocore)  • Ruby    Machine generated alternative text: AVVS SDK Overview  • We have to use the AWS SDK when coding againstAWS Services such  as DynamoDB  • Fun fact... the AWS CLI uses the Python SDK (bot03)  • The exam expects you to know when you should use an SDK  • We'll practice the AWS SDK when we get to the Lambda functions  • Good to know: if you don't specify or configure a default region, then  us-east- I will be chosen by default    Machine generated alternative text: AWS Limits (Quotas)  • API Rate Limits  • Describelnstances API for EC2 has a limit of 100 calls per seconds  • GetObject on S3 has a limit of 5500 GET per second per prefix  • For Intermittent Errors: implem Expo tial Backoff  • For Consistent Errors: request limit increase  • Service Ouotas (Service Limits)  • Running On-Demand Standard Instances: 1 152 vCPU  • You can request a service limit increase by opening a ticket  • You can request a service quota increase by using the Service Quotas API    **Note : if we get throtling exception will use exponential backoff**  **Increase time of double for api call**  Machine generated alternative text: Exponential Backoff (any AWS service)  • If you get ThrottlingException intermittently, use exponential backoff  • Retry mechanism included in SDK API calls  • Must implement yourself if using the API as is or in specific cases    Machine generated alternative text: AWS CLI Credentials Provider Chain  • The CLI will look for credentials in this order  2.  3.  4.  5.  6.  Command line options — —region, --output, and --profile  Environment variables-AWS ACCESS KEY ID,AWS SECRET ACCESS KEY,  and  CLI credentials file —aws configure  —/.aws/credentials on Linux / Mac & C:wsersxuserx.awsxcredentials on Windows  CLI configuration file — aws configure  —/.aws/config on Linux / macOS & C:XUsersXUSERNAMEX.awsXconfig on Windows  Container credentials — for ECS tasks  Instance profile credentials — for EC2 Instance Profiles      Machine generated alternative text: AWS SDK Default Credentials Provider Chain  • The Java SDK (example) will look for credentials in this order  2.  3.  4.  5.  Environment variables —  AVVS ACCESS KEY ID and ANS SECRET ACCESS KEY  Java system properties — aws.accessKeyld and aws.secretKey  The default credential profiles file — ex at: —/.aws/credentials, shared by  many SDK  Amazon ECS container credentials — for ECS containers  Instance profile credentials— used on EC2 instances    Machine generated alternative text: AWS Credentials Scenario  • An application deployed on an EC2 instance is using environment variables  with credentials from an IAM user to call the Amazon S3 API.  • The IAM user has S3FullAccess permissions.  • The application only uses one S3 bucket, so according to best practices:  • An IAM Role & EC2 Instance Profile was created for the EC2 instance  • The Role was assigned the minimum permissions to access that one S3 bucket  • The IAM Instance Profile was assigned to the EC2 instance, but it still had  access to all S3 buckets.VVhy?  the credentials chain is still giving priorities to the environment variables      Machine generated alternative text: AWS Credentials Best Practices  • Overall, NEVER EVER STORE AWS CREDENTIALS IN YOUR CODE  • Best practice is for credentials to be inherited from the credentials chain  • If using working within AWS, use IAM Roles  • EC2 Instances Roles for EC2 Instances  • ECS Roles for ECS tasks  • Lambda Roles for Lambda functions  • If working outside ofAWS, use environment variables / named profiles    Machine generated alternative text: Signing AWS API requests  • When you call the AWS HITP API, you sign the request so that AWS  can identify you, using your AWS credentials (access key & secret key)  • Note: some requests to Amazon S3 don't need to be signed  • If you use the SDK or CLI, the HTV P requests are signed for you  • You should sign an AWS HIT P request using Signature v4 (SigV4)  to    Machine generated alternative text: SigV4 Request examples  • HIT P Header option  GET https://iam.amazonaws.com/?ActionzListUsers&Versionz2ØIØ—Ø5—Ø8 HTTP/I.I  Authorization: AWS4-MAC-SHA256 Credential-AKIDEWPLE/2Ø15Ø83Ø/us-east-1/iam/aws4_request  SignedHeade host ; ,  Signatu  content—type: charseteutf—8  host: iam.amazonaws.com  x-amz-date: 2Ø15Ø83ØT1236ØØZ  • Query String option (ex: S3 pre-signed URLs)  GET https://iam.amazonaws.com?ActioneListUsers&Versione2ø1ø—ø5—ø8S  x-Amz-c redentia  i r ignedHeade r secon ten t— type*3Bhos t'  X-Amz-Signature-37ac2f4fdeøøbøac9bd9eadeb459b1bbee224158d66e7ae5fcadb7Øb2d181dø2 HTTP/I.I  content—type: charset:utf—8  host: iam.amazonaws.com      **Section 9) Advanced S3 and Athena**    **S3 MFA delete ( only can be done through CLI)**    Machine generated alternative text: S3 MFA-Delete  • MFA (multi factor authentication) forces user to generate a code on a device (usually a  mobile phone or hardware) before doing important operations on S3  • To use MFA-Delete, enable Versioning on the 3 bucket  • You will need MFA to  • permanently delete an object version  • suspend versioning on the bucket  • You won't need MFA for  • enabling versioning  • listing deleted versions  • Only the bucket owner (root account) can enable/disable MFA-Delete  • MFA-Delete currently can only be enabled using the CLI    Machine generated alternative text: Ultimate AWS Certified Developer Associate 2020 - NEW!  p  EXPLORER  OPEN EDITORS  commands.txt  ebs  efs.sh efs  x mfa-delete,sh s3  CODE  asg  beanstalk  cloudformation  efs  mfa  ssm  efssh  generate root access keys  aws configure —profile root—datacumulus  # enable mfa delete  awS s3api —bucket —versioning—conf iguration  Status—E led,HFADeletezEnabled —mfa "arn-of—nfa-device mfa—code" —profile root-datacumulus  8  9  disable mfa delete  awS s3api —bucket  Status—Enab —mfa  # delete the root credentials in the IAN  —versioning—conf iguration  mfa—code" —profile root—datacumulus  console!      **NOTE:** if we enabled mfa delete from cli we can't delete file version under s3    S3 default encryption    Machine generated alternative text: S3 Default Encryption vs Bucket Policies  • The old way to enable default encryption was to use a bucket policy  and refuse any HIT P command without the proper headers:  •put051 Icy •  *Sid • : -oenyunEnCryptedOtjeCtupIoadS• ,  • Deny • .  •Act Ion •  • s': Mutotlect•  • Resource •  true  • The new way is to use the "default encryption" option in S3  • Note: Bucket Policies are evaluated before "default encryption"    Machine generated alternative text: aws  Amazon S3  I BLAZkets  Public access settings  for this account  Resource Gro•u" v  Create bucket  AM CENdTra• "icing C?  Aw•s  Tyse to mh  custom  Global  Support  Quick tips  2018 3:59:49 PM  20'8 PM  2018 PM  2018 PM  2018 2*07 PM  2018 606:10 PM  2018 PM  Man.rne  Monnor r |
| Access Logs  Machine generated alternative text: S3 Access Logs  • For audit purpose, you may want to log all access to S3  buckets  • Any request made to S3, from any account, authorized or  denied, will be logged into another S3 bucket  • That data can be analyzed using data analysis tools...  • Or Amazon Athena as we'll see later in this section!  • The log format is at:  https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFo  rmat.html  requests  My-bucket  Log all  requests  Logging Bucket      NOTE: always separate application bucket and logging bucket    Machine generated alternative text: S3 Access Logs: Warning  • Do not set your logging bucket to be the monitored bucket  • It will create a logging loop, and your bucket will grow in size exponentially  Logging loop  PutObject  App Bucket &  Logging Bucket  e written a note here.  Do not try this at home O      NOTE: keep separate application bucket and log bucket    Create bucket  1) saurabh-s3logs (note all logs will come here)  Application )my-sample-bucket-saurabh-monitored    Now go to bucket created for application and enable sever access logging    Machine generated alternative text: my-sample-bucket-monitor-saurabh  Management  Access points  Properties  Versioning  Keep multiple versions of an object in the  same bucket  Learn more  Disabled  Permissions  Server access logging  Enable logging  Target bucket  saurabh-s310gs  Target prefix  Enter target prefix  C) Disable logging  Disabled  o  Cancel    NOTE: it will take few hour to log into bucket |
| S3 replication(Cross region and same Region)    Machine generated alternative text: S3 Replication (CRR & SRR)  • Must enable versioning in source and destination  • Cross Region Replication (CRR)  • Same Region Replication (SRR)  • Buckets can be in different accounts  • Copying is asynchronous  • Must give proper IAM permissions to S3  eu-west-l  • CRR - Use cases: compliance, lower latency access,  accounts  • SRR — Use cases: log aggregation, live replication  and test accounts  Asynchronous  replication  us-east-I    NOTE: **any delete operation is not replicated**    Machine generated alternative text: S3 Replication — Notes  • After activating, only new objects are replicated (not retroactive)  • For DELETE operations:  • If you delete without a version ID, it adds a delete marker, not replicated  • If you delete with a version ID, it deletes in the source, not replicated  • There is no "chaining" of replication  • If bucket I has replication into bucket 2, which has replication into bucket 3  • Then objects created in bucket I are not replicated to bucket 3  **### demo means copy from one bucket to another**    Step 1) **create 2 bucket ( in different region)**    **Saurabh-origin-bucket**  **Saurabh-replica-bucket**    Step 2) upload file in saurabh-origin-bucket    **Step 3)** enable versioning in both bucket to make sure we can set up replica    Step 4) enable replication in first bucket under management    Machine generated alternative text: stephane-origin-bucket  Overview Properties  + Add rule  Pem  You haven't creat  Same-Region Replication  Of  äZketS AWS  AVVS by  Cross-Region Replication  AWS  by AWS  e have written a note here.      Step 5) Add rule    Machine generated alternative text: Set source  IAM role  Create new role  Rule name  replicationdemd  Status  o  Enabled  Disabled  Replication rule  x  Review  Next  Set destination  3 Configure rule options  Previous    Machine generated alternative text: Lifecycle  Replication  Analytics  Metrics  Permissions  IAM role  Inventory  Edit global settings  Viewing 1 to 1 of 1  Replication configuration updated successfully.  Destination  Bucket  saurabh-replica-bucket  Region  EU (Paris)  Actions v  Source  Bucket  saurabh-origin-bucket  Region  s3crr_role for_saurabh-origin-  bucket to_saurabh-replica-bucket  Bucket policy  Copy  EU (Ireland)  + Add rule  Edit priorities      NOTE : IAM role is created for me    Machine generated alternative text: Management ('AM)  Dashboard  Access management  Groups  Users  Roles  Policies  Identity providers  Account settings  Access reports  Access analyzer  Archive rules  Analyzers  Settings  Create role  Q Search  Delete role  Trusted entities  AWS service: spotfleet  AWS service: elasticfilesystem (Service-Link...  AWS service: autoscaling (Service-Linked role)  AWS service: backup (Service-Linked role)  AWS service: elasticloadbalancing (Service-...  AWS service: rds (Service-Linked role)  AWS service: support (Service-Linked role)  AWS service: trustedadvisor (Service-Linked .  AWS service: ec2  AWS service: s3  Showing 10 results  Last activity  None  2 days  2 days  Today  2 days  2 days  None  None  Today  None  Role name  aws-ec2-spot-fleet-tagging-role  AWSServiceRole rAmazonElasti...  AWSServiceRoleFo utoScaling  AWSServiceRoleFor ckup  AWSServiceR01eForEl sticLoadB...  AWSServiceR01eForRD  AWSServiceRoleForSupp  AWSServiceRoleForTrusted  Visor  MyFirstEc2R01e  s3crr_role for_saurabh-origin-buc |
| NOTE:  **Delete marker not worked for replication** |

S3 pre signed URL

Specific case

Machine generated alternative text:
S3 pre-signed URLs 
• Can generate pre-signed URLs using SDK or CLI 
• For downloads (easy, can use the CLI) 
• For uploads (harder, must use the SDK) 
• Valid for a default of 3600 seconds, can change timeout with --expires-in 
argument 
• Users given a pre-signed URL inherit the permissions of the person who 
generated the URL tor GET / PUT 
• Examples 
• Allow only logged-in users to download a premium video on your S3 bucket 
• Allow an ever changing list of users to download files by generating URLs dynamically 
• Allow temporarily a user to upload a file to a precise location in our bucket 

NOTE: we want to give accessto someone of coffee.jpg so we need to use pre signed URL

Machine generated alternative text:
Amazon S3 
my-sample-bucket-monitor-saurabh 
Management 
Access point 
Last modified 
Oct 5, 2020 11:00 
GMT+0530 
coffee.jpg 
Download Copy path 
Latest version 
x 
Select from 
coffee.jpg 
65.3 KB 
NIA 
NIA 
lef66f833a1 b5bObaef8c56aea09da8 
Oct 5, 2020 CMF0530 
nttps:i/rny-sample-bucket-monitor. 
saurabh.s3.eu-west- 
3-amazonaws.com/coffee.jpg 
my-sample-bucket-monitor-saurabh 
Overview 
Properties 
Permissions 
Key 
Size 
Expiration date 
Expiration rule 
ETag 
Last modified 
Object URL 
Type a prefix and press Enter to search. Press ESC to clear. 
Upload 
Name 
+ Create folder 
Download 
Actions v 
Overview 
coffee-jpg 

Above url will not access

Machine generated alternative text:
aws s3 presign help 
aws configure set default.s3.signature_version s3v4 
rs 
aws s3 presign —expires—in 30 —region 
https://my—sample—bucket—monitored—stephane.s3.amazonaws.com/beach.jpg 
affefØ15be6c744b73Øbc7eb77347bØ897ØcbØ95bØ6d9e89af96c49d5Øb35acc 

Storage Tiers + Glacier

Machine generated alternative text:
S3 Storage Classes 
• Amazon S3 Standard - General Purpose 
• Amazon S3 Standard-Infrequent Access (IA) 
• Amazon S3 One Zone-Infrequ 
• Amazon S3 Intelligent Tiering 
• Amazon Glacier 
• Amazon Glacier Deep Archive 
• Amazon S3 Reduced Redundancy Storage (deprecated - omitted) 

Machine generated alternative text:
S3 Standard — General Purpose 
• High durability (99.999999999%) of objects across multiple AZ 
• If you store 1 objects with Amazon S3, you can on average 
expect to incur a loss of a single ject once every 10,000 years 
• 99.99% Availability over a give y 
• Sustain 2 concurrent facility fa lu 
• Use Cases: Big Data analytics, mobile & gaming applications, content 
distribution... 

Machine generated alternative text:
S3 Standard — Infrequent Access (IA) 
• Suitable for data that is less frequently accessed, but requires rapid 
access when needed 
• High durability (99.999999999% ofobjects across multiple AZs 
. 99.9% Availability 
• Low cost compared to Amaz n —can ard 
• Sustain 2 concurrent facility fail 
for disaster recovery, backups... 

Machine generated alternative text:
S3 One Zone - Infrequent Access (IA) 
• Same as IA but data is stored in a single AZ 
• High durability (99.999999999%) of objects in a single AZ; data lost when 
is destroyed 
• 99.5% Availability 
• Low latency and high throughput performance 
• Supports SSI- for data at transit and encryption at rest 
• Low cost compared to IA (by 20%) 
• Use Cases: Storing secondary backup copies of on-premise data, or storing 

Machine generated alternative text:
S3 Intelligent Tiering 
• Same low latency and high throughput performance ofS3 Standard 
• Small monthly monitoring and auto-tiering fee 
• Automatically moves objects between two access tiers based on 
changing access patterns 
• Designed for durability of 99.999999999% of objects across multiple 
Availability Zones 
• Resilient against events that impact an entire Availability Zone 
• Designed for 99.9% availability over a given year 

Machine generated alternative text:
Amazon Glacier 
• Low cost object storage meant for archiving / backup 
• Data is retained for the longer term (IOS of years) 
• Alternative to on-premise magnetretape storage 
• Average annual durability is 9 .99' A999 9% 
• Cost per storage per month $0.dU4'j G ) + retrieval cost 
• Each item in Glacier is called "AFchive/(up to 40 T B) 
• Archives are stored in "Vautts" 

Machine generated alternative text:
Amazon Glacier & Glacier Deep Archive 
• Amazon Glacier — 3 retrieval options: 
• Expedited (I to 5 minutes) 
• Standard (3 to 5 hours) 
• Bulk (5 to 12 hours) 
• Minimum storage duration of 90 days 
• Amazon Glacier Deep Archive — for long term storage — cheaper: 
• Standard (12 hours) 
• Bulk (48 hours) 
• Minimum storage duration of 1 80 days 

Machine generated alternative text:
S3 Storage Classes Comparison 
S3 Glacier 
99.999999999% 
(11 9's) 
99.99% 
99.9% 
40KB 
90 days 
per GB retrieved 
S3 Glacier 
Deep Archive 
99.999999999% 
(11 9's) 
99.99% 
99.9% 
40KB 
180 days 
per GB retriev 
Designed for 
durability 
Designed for 
availability 
Availability SLA 
Availability 
Zones 
Minimum 
capacity charge 
per Object 
Minimum 
storage duration 
charge 
Retrieval fee 
S3 Standard 
99.999999999% 
(11 9's) 
99.99% 
99.9% 
N/A 
N/A 
N/A 
S3 Intelligent- 
Tiering 
99.999999999% 
(11 9's) 
99.9% 
23 
N/A 
30 days 
N/A 
S3 Standard-IA 
99.999999999% 
(11 9's) 
99.9% 
128KB 
30 days 
per GB retrieved 
S3 one Zone-IA 
99.999999999% 
(11 9's) 
99.5% 
128KB 
30 days 
per GB retrieved 

Machine generated alternative text:
S3 Storage Classes — Price Comparison 
Example us-east-2 
S3 Intelligent- 
Tiering 
$0.0125 - 
$0.023 
GET $0.0004 
Instantaneou 
9.0025 
S3 one Zone-IA 
$0.01 
GET $0.001 
Instantaneous 
S3 Glacier 
SO.004 
Minimum 90 days 
GET $0.0004 + 
Expedited - $10.00 
Standard - $0.05 
Bulk - $0.025 
Expedited (1 to 5 
minutes) 
Standard (3 to 5 hours) 
Bulk (5 to 12 hours) 
Storage Cost 
(per GB per 
month) 
Retrieval Cost 
(per 1000 
requests) 
Time to retrieve 
Monitoring Cost 
(per 1000 objects) 
S3 Standard 
$0.023 
GET 
$0.0004 
instantaneo 
S3 Glacier 
Deep Archive 
$0.00099 
Minimum 180 days 
GET $0.0004 + 
Standard - $0.10 
Bulk - $0.025 
Standard (12 
hours) 
Bulk (48 hours) 
S3 Standard-IA 
9.0125 
GET 90.001 
Instantaneous 

Read the description

Machine generated alternative text:
Select files 
Standard 
Intelligent-Tering 
Standard-IA 
One Zone-IA 
Glacier 
Glacier Deep Archive 
Set permissions 
Frequently accessed data 
Long-lived data with changing or 
unknown access pattems 
Long-lived, infrequently accessed 
data 
Long-lived, infrequently accessed, 
non-critical data 
Archive data with retrieval times 
ranging from minutes to hours 
Archive data that rarely, if ever, needs 3 
to be accessed with retrieval times in 
hours 
Upload 
Set properties 
x 
Review 
Per-GB fees 
apply 
Per-GB fees 
apply 
Per-GB fees 
apply 
Per-GB fees 
apply 
128KB 
128KB 
40KB 
40KB 
30 days 
30 days 
30 days 
90 days 
180 days 
Per-object fees 
apply 

S3 lifecycle Policies

Machine generated alternative text:
S3 — Moving between storage classes 
• You can transition objects 
between storage classes 
• For infrequently accessed object, 
move them to STANDARD IA 
• For archive objects you don't 
need in real-time, GLACIER or 
DEEP ARCHIVE 
• Moving obiects can be 
automated using a lifecycle 
configuration 
STANDARD_IA 
INTaL1æNT_T1æ1NG 
STAND"D 
ONEZONE_IA 
REIN-ICED 
—REWNDANCY 
GLACIER 
DEEP_ARCHIVE 

Machine generated alternative text:
S3 Lifecycle Rules 
• Transition actions: It defines when objects are transitioned to another storage 
class. 
• Move objects to Standard IA class 60 days after creation 
• Move to Glacier for archiving after 6 months 
• Expiration actions: configure objects to expire (delete) after some time 
• Access log files can be set to delete after a 365 days 
• Can be used to delete old versions of files (if versioning is enabled) 
• Can be used to delete incomplete multi-part uploads 
• Rules can be created for a certain prefix (ex - s3://mybucket/mp3/*) 
• Rules can be created for certain objects tags (ex - Department: Finance) 

Machine generated alternative text:
S3 Lifecycle Rules — Scenario I 
• Your application on EC2 creates images thumbnails after profile photos 
are uploaded to Amazon S3.These thumbnails can be easily recreated, 
and only need to be kept for 45 days. The source images should be able 
to be immediately retrieved for these 45 days, and aftenwards, the user 
can wait up to 6 hours. How would you design this? 
• S3 source images can be on STANDARD, with a lifecycle configuration 
to transition them to GLACIER after 45 days. 
• S3 thumbnails can be on ONEZONE_IA, with a lifecycle configuration 
to expire them (delete them) after 45 days. 

Machine generated alternative text:
S3 Lifecycle Rules — Scenario 2 
• A rule in your company states that you should be able to recover your 
deleted S3 objects immediately for 1 5 days, although this may happen rarely. 
After this time, and for up to 365 days, deleted objects should be recoverable 
within 48 hours. 
• You need to enable S3 versioning in order to have object versions, so that 
"deleted objects" are in fact hidden by a "delete marker" and can be 
recovered 
• You can transition these "noncurrent versions" of the object to S3 IA 
• You can transition afterwards these "noncurrent versions" to 
DEEP ARCHIVE 

NOTE: we can add lifecycle like when object will get removed from bucket

Machine generated alternative text:
aws 
Resou Groups 
Lifecycle rule 
C-t_rrmt 
For current versions of objects 
to LA after 
after 
A Transitioning small Glacier Deep 
Archive will increase costs. 
a tr. to 
to Lifey& 
stephane-s3-storage-class-dem 
Rep I •ation 
+ Add 

Machine generated alternative text:
stephane-s3-storage-class-demo 
kCtÉvø 
+ Add lifecycle 
Lifecy-& 
MyFirstRu1e 
Delete 
to 

**S3 Performance**

Machine generated alternative text:
S3 — Baseline Performance 
• Amazon S3 automatically scales to high request rates, latency 100-200 ms 
• Your application can achieve at least 3,500 PUT/COPY/POST/DELETE and 
5,500 GET/HEAD requests per second per prefix in a bucket. 
• There are no limits to the number'6f'BF6 es in a bucket. 
• Example (object path prefix : 
• bucket/folderl /sub l/fle /folderl / 
• bucket/folderl /sub2/fIe /foIdeFl/sub2/ 
• bucket/l/file 
• bucket/2/fiIe 
• If you spread reads across all four prefixes evenly, you can achieve 22,000 
requests per second for GET and HEAD 

Machine generated alternative text:
S3 — KMS Limitation 
• If you use SSE-KMS, you may be impacted 
by the KMS limits 
• When you upload, it calls the 
GenerateDataKey KMS API 
• When you download, it calls the Decrypt 
• Count towards the KMS quota per second 
(5500, 1 0000, 30000 req/s based on region) 
• As of today, you cannot request a quota 
increase for KMS 
S3 Bucket 
KMS Key 
API call 
Upload / download 
SSE-KMS 
Users 

Machine generated alternative text:
S3 Performance 
• Multi-Part upload: 
• recommended for files IOOMB, 
must use for files 5GB 
• Can help parallelize uploads (speed 
• S3 Transfer Acceleration (upload only) 
• Increase transfer speed by transferring 
file to an AWS edge location which will 
forward the data to the S3 bucket in the 
target region 
• Compatible with multi-part upload 
Fast 
Fast 
(private AWS) 
up transfers) 
Divide 
In parts 
BIG file 
Parallel uploads 
Amazon S3 
Edge Location 
File in USA 
USA 
S3 Bucket 
Australia 

Machine generated alternative text:
S3 Performance — S3 Byte-Range Fetches 
• Parallelize GETS by requesting specific 
byte ranges 
• Better resilience in case of failures 
Can be used to speed up downloads 
Can be used to retrieve only partial 
data (for example the head of a file) 
File in S3 
Byte-range request for header 
(first XX bytes) 
header 
Part 1 
tephane Maarek 
File in S3 
Part 2 
Part N 
Requests in parallel 

**S3 select and Glacier select**

Machine generated alternative text:
S3 Select & Glacier Select 
• Retrieve less data using SQL by performing server side filtering 
• Can filter by rows & columns (simple SQL statements) 
• Less network transfer, less CPU cost client-side 
Amazon S3 
up to 400% Faster 
3 Select 
CSV file 
Get CSV with S3 Select 
Send filtered dataset 
Amazon S3 
Server-side filtering 
Amazon S3 
up to 80% Cheaper 
https://as•.'s.amazon.com/blogs/aws/s3-glacier-selectI 
O Stephane Maarek 

**S3 Event Notification**

Machine generated alternative text:
S3 Event Notifications 
• S3:ObjectCreated, S3:ObjectRemoved, 
S3:ObjectRestore, S3:Replication... 
• Object name filtering possible (*.jpg) 
• Use case: generate thumbnails of images uploaded to S3 
• Can create as many "S3 events" as desired 
• S3 event notifications typically deliver events in seconds 
but can sometimes take a minute or longer 
• If two writes are made to a single non-versioned object 
at the same time, it is possible that only a single event 
notification will be sent 
• If you want to ensure that an event notification is sent 
for every successful write, you can enable versioning on 
your bucket. 
SNS 
SQS 
Lambda Function 
events 
Amazon S3 

**S3 event notification demo**

1)Create bucket saurabh-event-notification-demo

2)Enable versioning

3)create event

Machine generated alternative text:
Events 
New event 
Name O 
Multipart upload cornpleted 
A events 
O*ct in RRS lost 
Perrnanentty deleted 
Due 
Requester pays 
r—tS 

Machine generated alternative text:
Prefix 
e.g. images/ 
o 
Suffix 
e.g. .ypg 
Send to 
SQS Queue 
SQS 
Add SQS queue ARN 
SQS queue ARN 
https://sqs.eu-west-3.amazonaws.com/398678778168/demo-s3-eventd 
0 Active notifications 
Cancel 
Save 

**Step4) create sqs**

Machine generated alternative text:
aws 
Services v 
You can now send and receive messages. 
Queues demo-s3-event 
Amazon SQS 
demo-s3-event 
Details 
Info 
Name 
Odemo-s3-event 
Encryption 
Disabled 
More 
Type 
Standard 
URL 
https://sqs.eu-west- 
3.amazonaws.com/398678778168/demo-s3- 
event 
Edit 
Delete 
ARN 
saurabh @ awsdeveloperlearn v 
Paris v 
sup 
Purge 
Send and receive messages 
fil arn:aws:sqs:eu-west-3:398678778168:demo- 
s3-event 
Dead-letter queue 
Disabled 

**Note: anytime will upload file in s3 message will reach to sqs(amazon simple queue service)**

**Athena (query data in s3 using sql)**

Machine generated alternative text:
AWS Athena 
• Serverless service to perform analytics directly against S3 files 
• Uses SQL language to query the files 
• Has a JDBC / ODBC driver 
• Charged per query and amount of data scanned 
• Supports CSV, JSON, ORC, Avro, and Parquet (built on Presto) 
• Use cases: Business intelligence / analytics / reporting, analyze & query 
VPC Flow Logs, ELB Logs, CloudTrail trails, etc... 
• Exam Tip: Analyze data directly on S3 use Athena 

Machine generated alternative text:
S3 Object Lock & Glacier Vault Lock 
• S3 Object Lock 
• Adopt a WORM (Write Once Read 
Many) model 
• Block an object version deletion for a 
specified amount of time 
• Glacier Vault Lock 
• Adopt a WORM (Write Once Read 
Many) model 
• Lock the policy for future edits (can no 
longer be changed) 
• Helpful for compliance and data retention 
Object 
Vault Lock Policy 
Object can't be deleted 

|  |
| --- |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |