Talk

Operating a meteorological risk report map in a sovereign cloud with 3 classes of object storage

S3 APIs and storage cloud services

May 2023

Charlotte Letamentdia

Product Manager Storage, OVHcloud

Laurent Song

Product Owner Object Storage, OVHcloud

As a dev.sec.ops I respect good practices and work in peace !
My cloud provider takes care of the infrastructure for me.

My data is my asset

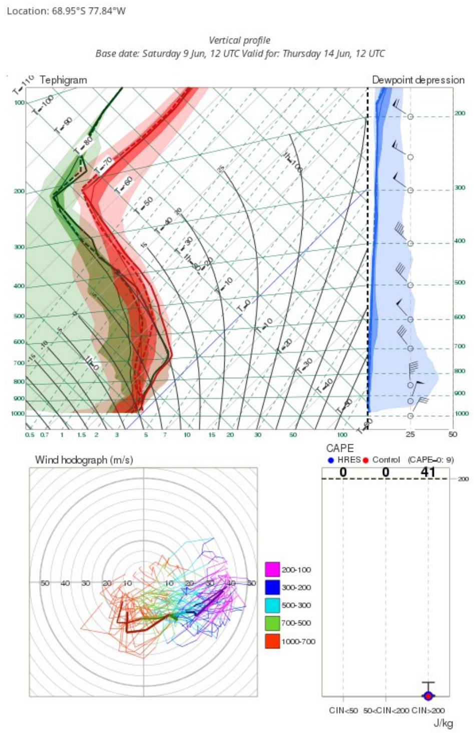
- ► I understand the value of my data assets
- ► I am concerned by attacks and risks
- ► I manage data with S3 API

Let’s share together the best practice in data security

Website delivery – High availability and security

Data protection with S3 API

SENSITIVE REPORT



Risks

Human errors

Deletion

Non predictables

Software issues, hardware issues, datacenter downtime, geographical disaster

Cyberattacks

Malware, ransomware & viruses, act of sabotage, DDoS

PROTECTION MEANS

- ✓ Versioning ●
- ✓ Immutability (S3 lock) ●
- ✓ Several copies (3-2-1) ●
- ✓ Encryption ●
- ✓ Controle the access ● ●

OVHcloud

Rule n° 1 - versioning

```
aws s3api put-bucket-versioning --bucket mybackup –versioning-configuration
Status=Enabled
```

- Protection against accidental overwriting
- Reversing after accidental delete
- Fetch any version
- Lifecycle to store not too long old versions

Rule n° 2 -

```
aws s3api put-object-lock-configuration --bucket my_bucket --object-lock-
configuration '{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention":
{ "Mode": "GOVERNANCE", "Days": 10 }}}'
```

Primary storage systems must be open and available

Your backup data should be isolated and immutable

tention periods
r legal hold

vernance mode
compliance mode

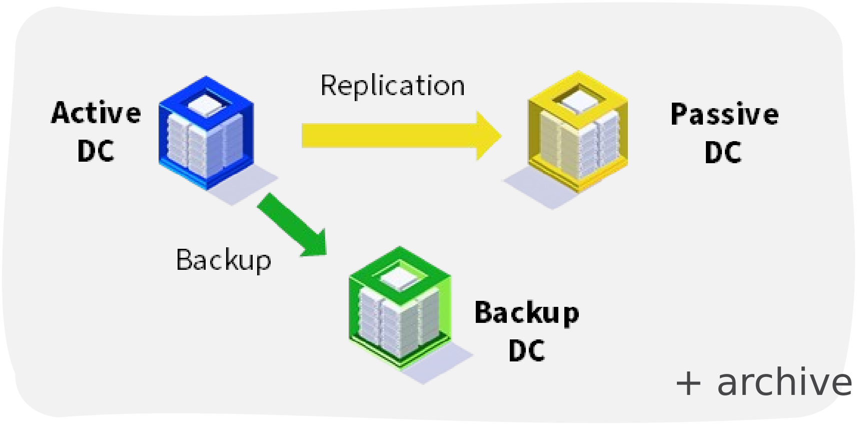
Write **O**nce, **R**ead **M**any (WORM) model

S3 lock

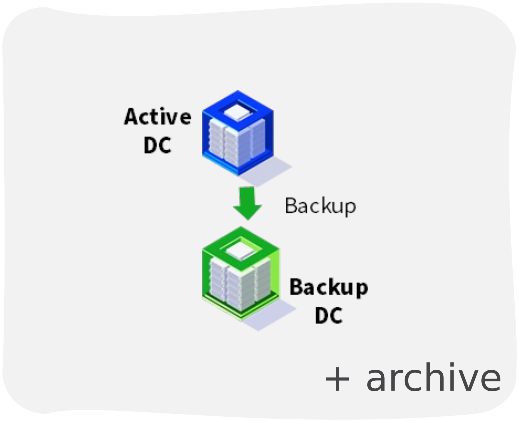
Rule n°3 - replication

```
aws s3api put-bucket-replication --bucket my-data --replication-configuration '{"Rules":
[{"ID": "my-rule","Priority": 1,"Status": "Enabled","Destination": {"Bucket": "my-
backup","StorageClass": "STANDARD"},"DeleteMarkerReplication": {"Status": "Enabled"}}]}'
```

Essential applications
RPO > 1h & RTO > 4h



Non-Critical Application
RPO > 24h & RTO > 24h



Retention policy

Non business critical	Weekly
Business critical	Every day during 1 month than monthly during 1 year
Archive	> 1 year

3 copies of data + 2 supports + 1 off site

Rule n°4 - encryption

```
aws s3api put-object \ --body /etc/my-object \ --bucket <bucket_name> \ --key encrypt_my-object
\ --sse-customer-algorithm AES256 \ --sse-customer-key $encKey \ --sse-customer-key-md5 $md5Key
```

Encrypt your data

Encryption at rest

SSE-C : with customer key
Based on AES-256

Encryption in transit

Cli, Api with Https / TLS

Rule n°5 - user policies

```
{ "Statement":[{ "Sid":"ROContainer", "Effect":"Allow", "Action":
["s3:GetObject","s3:ListBucket","s3:ListMultipartUploadParts","s3:ListBucketMultipartUploads"],
"Resource":["arn:aws:s3:::hp-bucket","arn:aws:s3:::hp-bucket/*"] }] }
```

Grant only the permissions that are required to perform a task

User policy

Bucket policy

```
{ "Statement":
[{ "Sid":"FullAccess",
"Effect":"Allow",
"Action":["s3:*"],
"Resource":["*"] }] }
```

Best practice with 5 rules

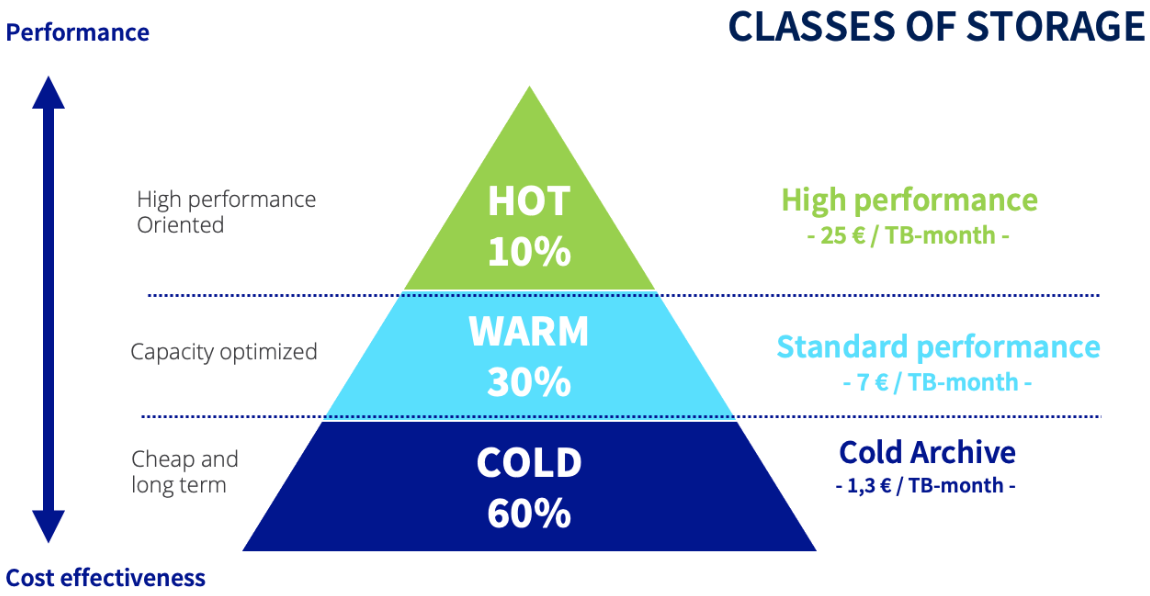
- ☑ Versioning
- ☑ Immutability (S3 lock)
- ☑ Several copies (3-2-1)
- ☑ Encryption
- ☑ Controle the access

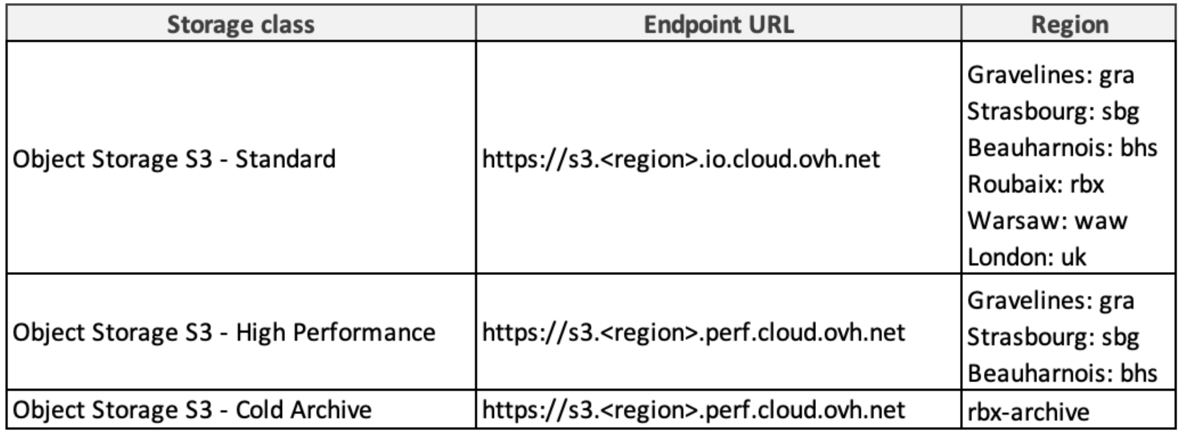
Be uncompromising in the implementation of security compliance.

Website delivery – Storage classes

Tiering, putting the data in the right place in the right moment with S3 API

- ✓ Project Public Cloud (tenant, openstackID)
- ✓ Credentials S3 (access key, secret key)
- ✓ Endpoint





Storage class	Endpoint URL	Region
Object Storage S3 - Standard	https://s3.<region>.io.cloud.ovh.net	Gravelines: gra Strasbourg: sbg Beauharnois: bhs Roubaix: rbx Warsaw: waw London: uk
Object Storage S3 - High Performance	https://s3.<region>.perf.cloud.ovh.net	Gravelines: gra Strasbourg: sbg Beauharnois: bhs
Object Storage S3 - Cold Archive	https://s3.<region>.perf.cloud.ovh.net	rbx-archive

Website delivery – Sovereinghty

A trusted cloud

Confidentiality requirements

- Not subject to extraterritorial laws
- Operation in compliance with the GDPR

Data security

- Protection tools
- Strong operational relationships with security communities

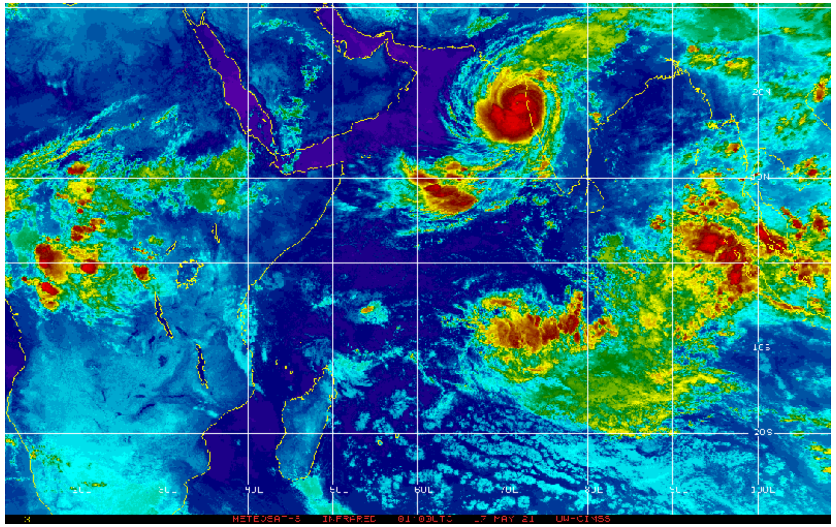
Transparency

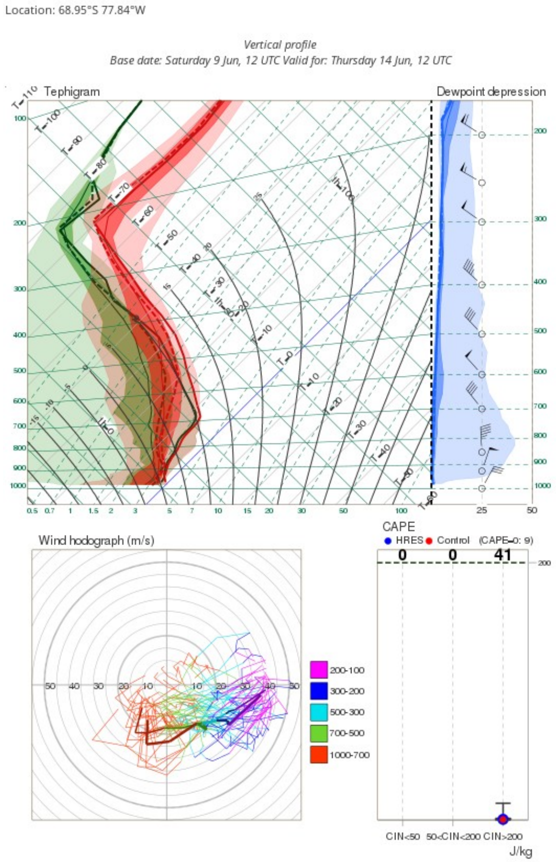
- Transparency
- Reversibility

Let me show you my use case!

Demonstration

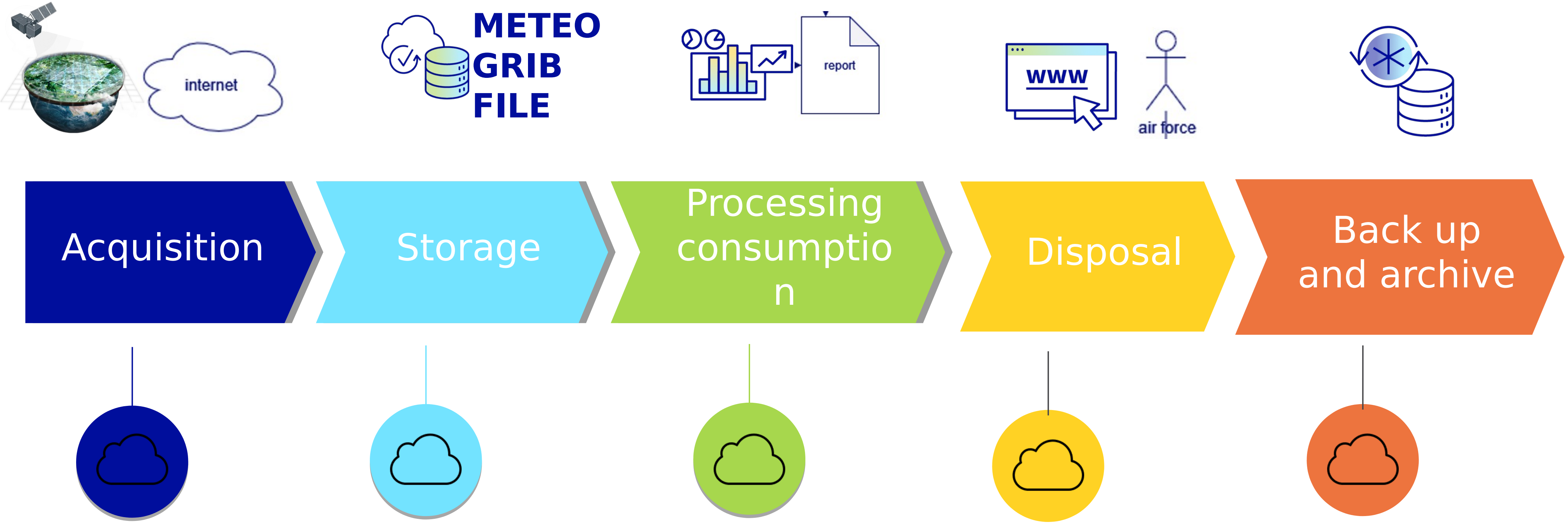
Use case: meteorological risks report generation app





Workflow

data lifecycle in 5 steps



METEO
GRIB
FILE

Acquisition

Object Storage class
High Performance
RW ++++

Storage

Object Storage class
Standard
Capacitive

Processing consumption

Block/file storage
R/W ++++++++

Object Storage class
High Performance
RW ++++

Disposal

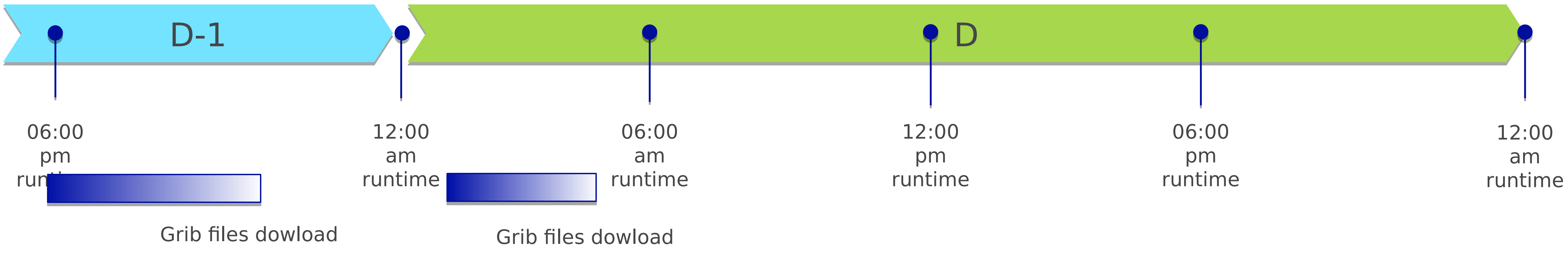
Object Storage class
Standard
Capacitive

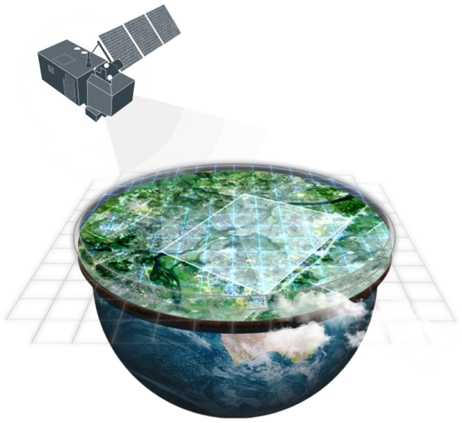
Back up and archive

Archive
Cold

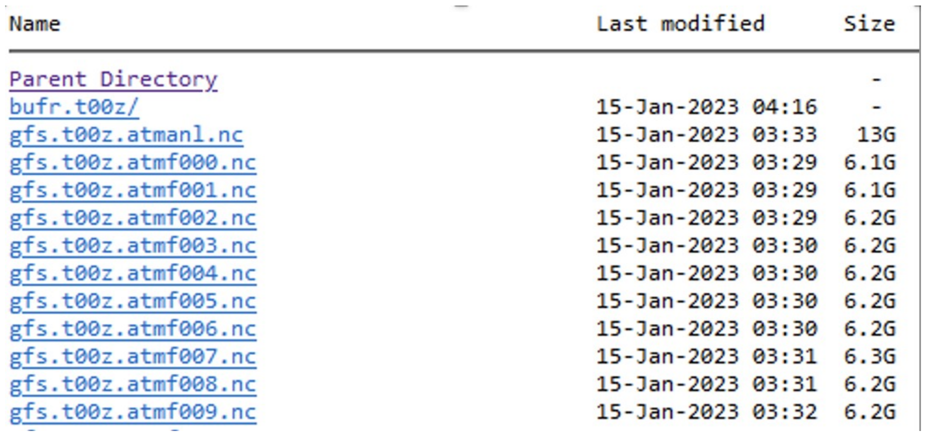
Input data

forecast model runtimes





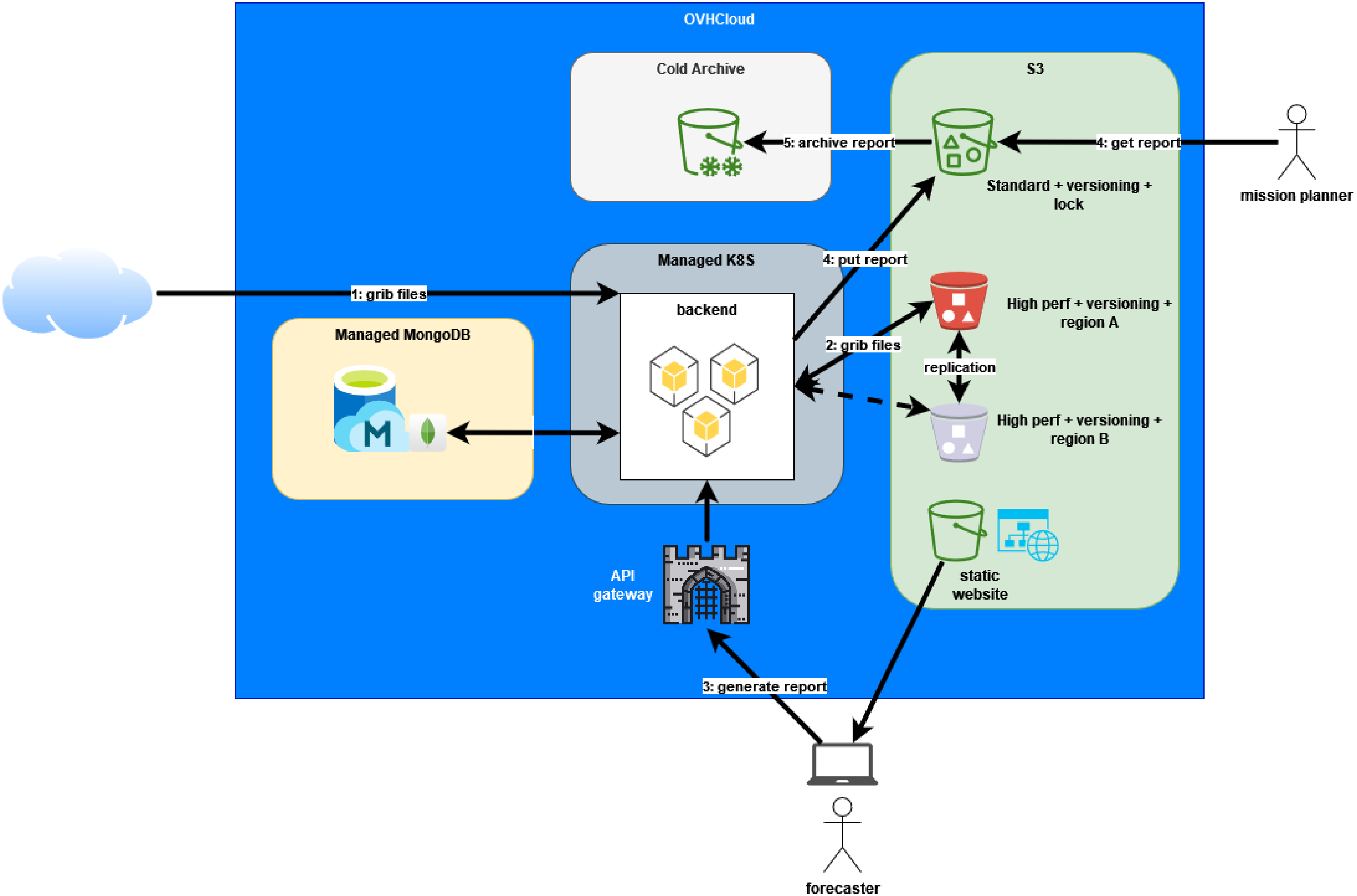
IO intensive!



```
Name                                              Last modified      Size

Parent Directory                                                      -
bufr.t00z/                                        15-Jan-2023 04:16   -
gfs.t00z.atmanl.nc                                15-Jan-2023 03:33  13G
gfs.t00z.atmf000.nc                               15-Jan-2023 03:29  6.1G
gfs.t00z.atmf001.nc                               15-Jan-2023 03:29  6.1G
gfs.t00z.atmf002.nc                               15-Jan-2023 03:29  6.2G
gfs.t00z.atmf003.nc                               15-Jan-2023 03:30  6.2G
gfs.t00z.atmf004.nc                               15-Jan-2023 03:30  6.2G
gfs.t00z.atmf005.nc                               15-Jan-2023 03:30  6.2G
gfs.t00z.atmf006.nc                               15-Jan-2023 03:30  6.2G
gfs.t00z.atmf007.nc                               15-Jan-2023 03:31  6.3G
gfs.t00z.atmf008.nc                               15-Jan-2023 03:31  6.2G
gfs.t00z.atmf009.nc                               15-Jan-2023 03:32  6.2G
```

Bird's-eye view of architecture



Find us online

Charlotte.letamendia

laurentsong

https://docs.ovh.com/us/en/storage/

https://github.com/ovh/public-cloud-roadmap