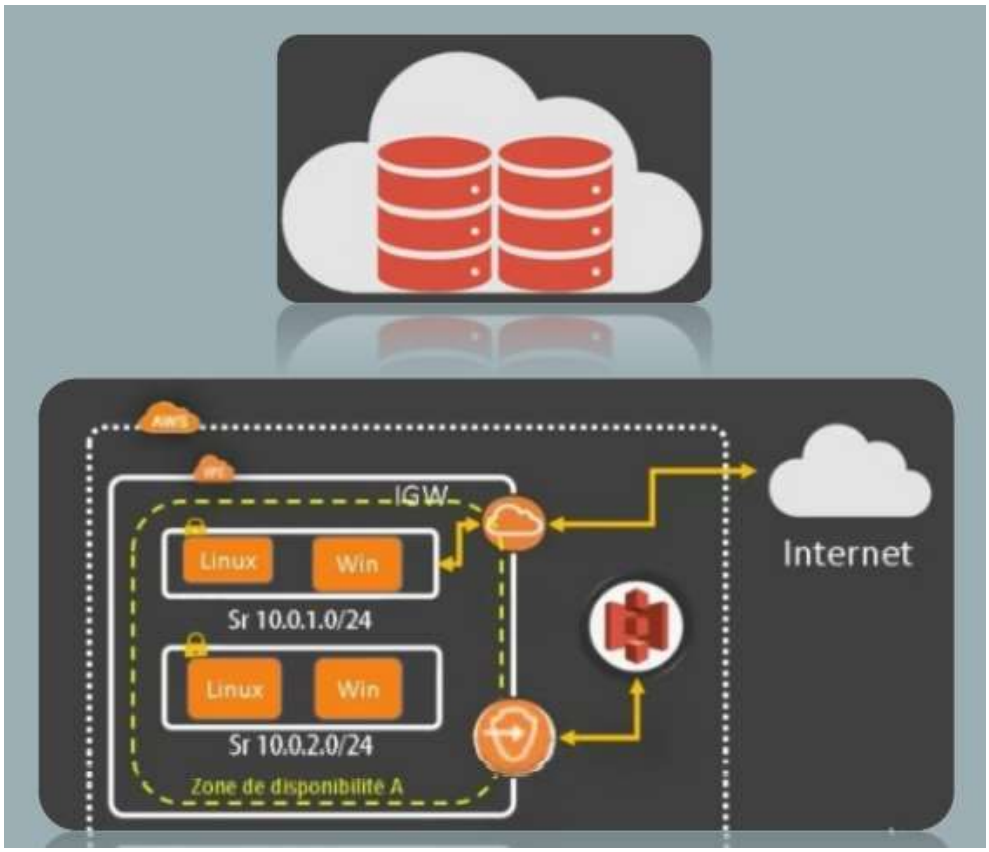
AWS - S3

jeudi 16 février 2023 14:58

Formateur : Mohamed AIJJOU

https://aws.amazon.com/fr/s3/

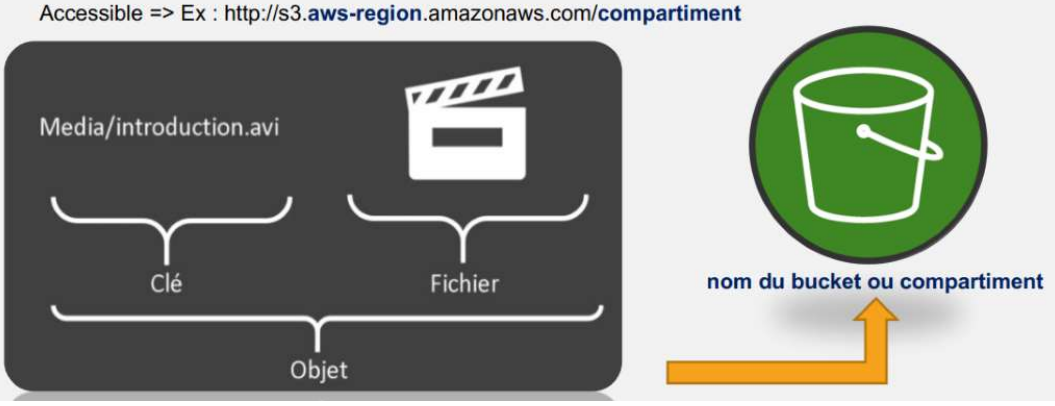


- ***Service entièrement géré de stockage dans le cloud.***
- ***Stoker virtuellement un nombre illimité d'objets.***
- **Accessible à tous moments, de n'importe ou.**
- **Niveau de sécurité très élevé.**

Niveau de sécurité : plusieurs réplicas des données à différents endroit pour garantir leur sauvegarde

8 – 2 – Objet S3

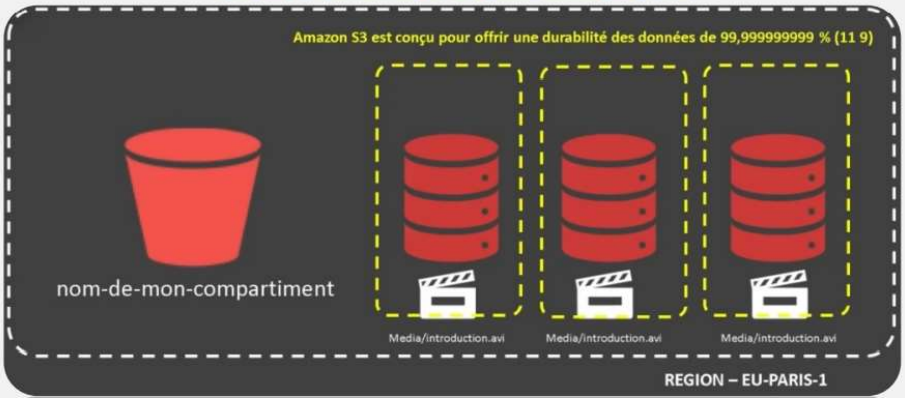
Accessible => Ex : http://s3.**aws-region**.amazonaws.com/**compartiment**



8 – 3 – Service redondant

Service redondant dans une même Région

Données chiffrées en transit et coté serveur.

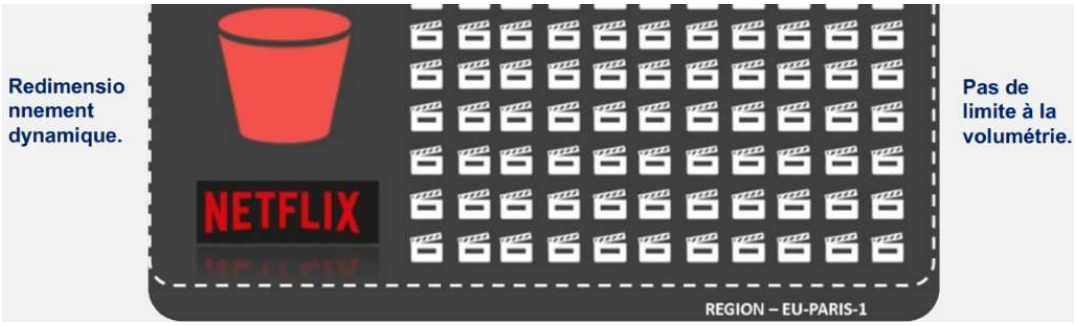


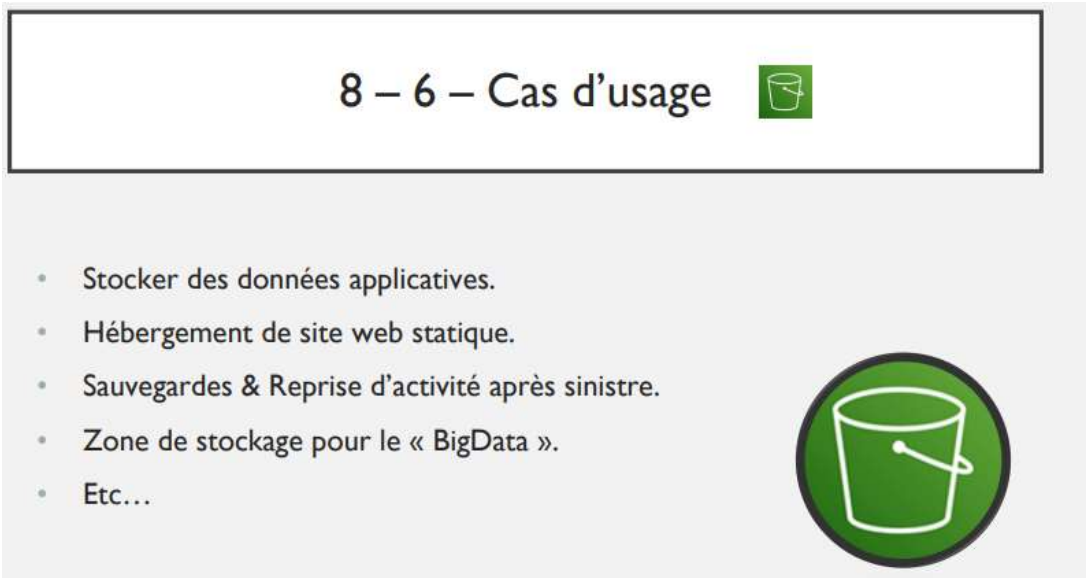
8 – 4 – Mise à l'échelle dynamique

On ne paye que ce que l'on consomme.

L'import des objets est gratuit. Par internet, si < 1 To.

8 – 4 – Mise à l'échelle dynamique





Créer un compartiment S3 :

Sélectionner un compartiment

Propriété d'objets Info

Contrôlez la propriété des objets écrits dans ce compartiment à partir d'autres comptes AWS et l'utilisation des listes de contrôle d'accès (ACL). La propriété des objets détermine qui peut spécifier l'accès aux objets.

- (•) Listes ACL désactivées (recommandé)
  Tous les objets de ce compartiment sont gérés par ce compte. L'accès à ce compartiment et à ses objets est spécifié en utilisant uniquement des politiques.
- ( ) Listes ACL activées
  Les objets de ce compartiment peuvent être gérés par d'autres comptes AWS. L'accès à ce compartiment et à ses objets peut être spécifié à l'aide des listes ACL.

Propriété d'objets

Propriétaire du compartiment appliqué

Modifications d'autorisation à venir pour désactiver les listes ACL
À partir d'avril 2023, pour désactiver les listes ACL lors de la création de compartiments à l'aide de la console S3, vous n'aurez plus besoin de l'autorisation `s3:PutBucketOwnershipControls`. En savoir plus

Paramètres de blocage de l'accès public pour ce compartiment

L'accès public aux compartiments et aux objets est accordé via des listes de contrôle d'accès (ACL), des stratégies de compartiment, de point d'accès ou tous ces éléments à la fois. Pour bloquer l'accès public à votre compartiment et aux objets qu'il contient, activez le paramètre Bloquer tous les accès publics. Il s'applique uniquement à ce compartiment et à ses points d'accès. AWS recommande de bloquer tous les accès publics, mais avant d'appliquer ces paramètres, vérifiez que vos applications fonctionneront correctement sans accès public. Si vous souhaitez autoriser un certain niveau d'accès public pour votre compartiment ou ses objets, vous pouvez personnaliser les paramètres individuels ci-dessous en fonction de vos besoins en stockage. En savoir plus

- [x] **Bloquer *tous* les accès publics**
  L'activation de ce paramètre revient à activer les quatre paramètres ci-dessous. Chacun des paramètres suivants est indépendant l'un de l'autre.
  - [x] **Bloquer l'accès public aux compartiments et aux objets, accordé via de *nouvelles* listes de contrôle d'accès (ACL)**
    S3 bloque les autorisations d'accès public appliquées aux compartiments ou objets récemment ajoutés et empêche la création de listes ACL d'accès public pour les compartiments et objets existants. Ce paramètre ne modifie pas les autorisations existantes qui permettent l'accès public aux ressources S3 qui utilisent les listes ACL.
  - [x] **Bloquer l'accès public aux compartiments et aux objets, accordé via *n'importe quelles* listes de contrôle d'accès (ACL)**
    S3 ignore toutes les listes ACL qui accordent l'accès public aux compartiments et aux objets.
  - [x] **Bloquer l'accès public aux compartiments et aux objets, accordé via de *nouvelles* stratégies de compartiment ou de point d'accès public**
    S3 bloque les nouvelles stratégies de compartiment et de point d'accès qui accordent un accès public aux compartiments et objets. Ce paramètre ne modifie pas les stratégies existantes qui autorisent l'accès public aux ressources S3.
  - [x] **Bloquer l'accès public et entre comptes aux compartiments et objets via *n'importe quelles* stratégies de compartiment ou de point d'accès public**
    S3 ignore l'accès public et entre comptes pour les compartiments ou points d'accès avec des stratégies qui accordent l'accès public aux compartiments et aux objets.

Modifications d'autorisation à venir pour activer tous les paramètres de blocage d'accès public
À partir d'avril 2023, pour activer tous les paramètres de blocage d'accès public lors de la création de compartiments à l'aide de la console S3, vous n'aurez plus besoin de l'autorisation `s3:PutBucketPublicAccessBlock`. En savoir plus

Gestion des versions de compartiment

La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans le même compartiment. Vous pouvez utiliser la gestion des versions pour conserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. Grâce à la gestion des versions, vous pouvez aisément récupérer en cas d'actions involontaires des utilisateurs et de défaillances des applications. En savoir plus

Gestion des versions de compartiment

- ( ) Désactiver
- (•) Activer

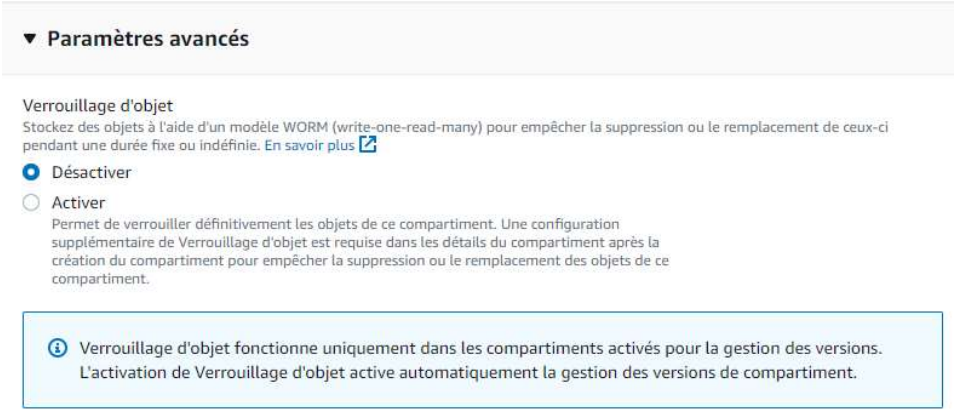
Si activé : permet le versionning des fichiers

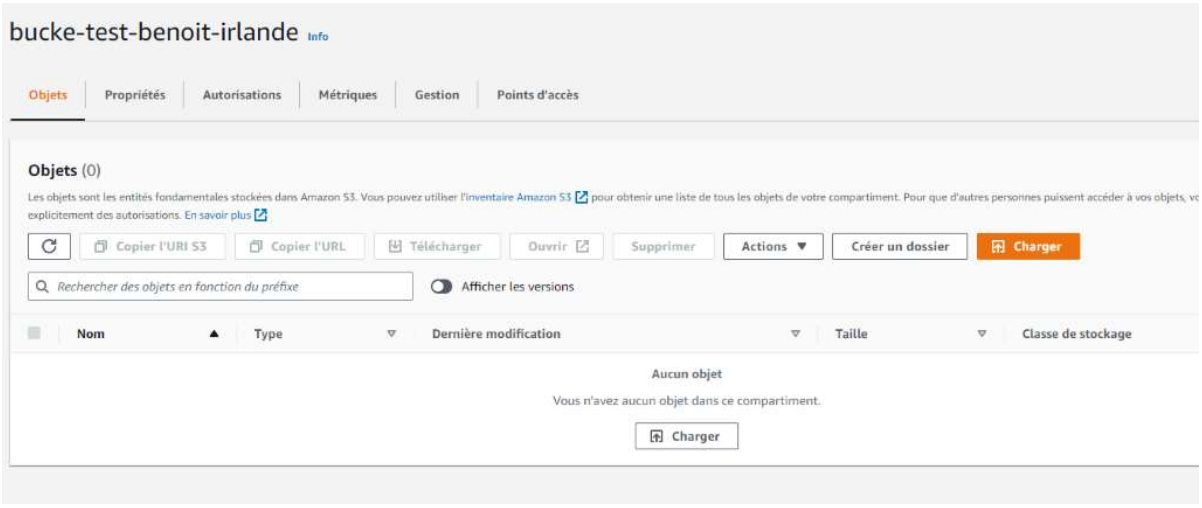
Balises (0) - *facultatif*

Vous pouvez utiliser des balises de compartiment afin de suivre les coûts de stockage et organiser les compartiments. En savoir plus

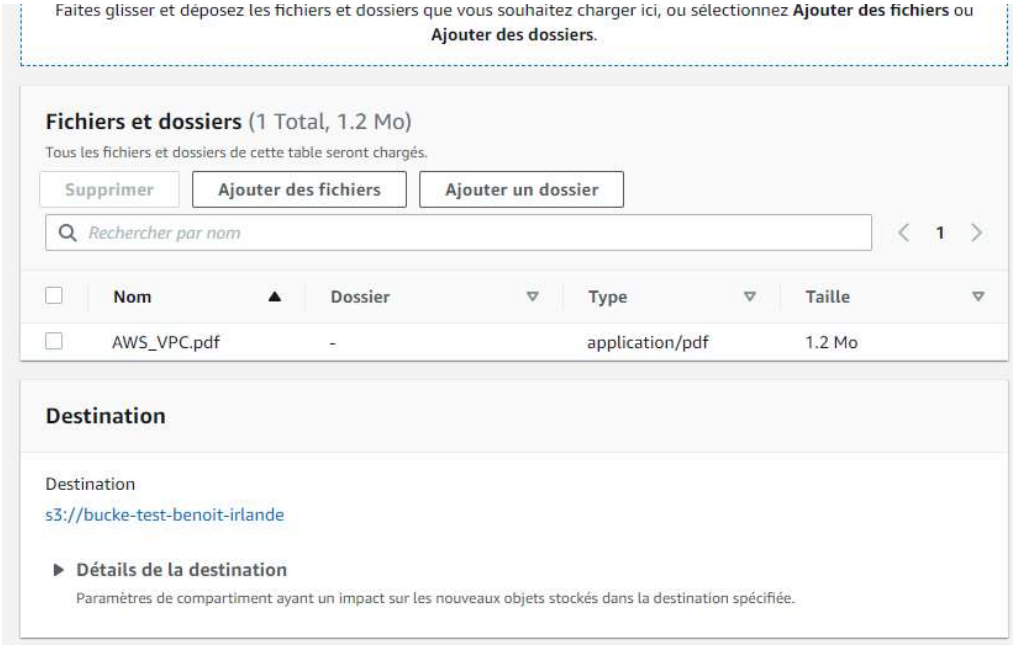
Aucune balise n'est associée à ce compartiment.

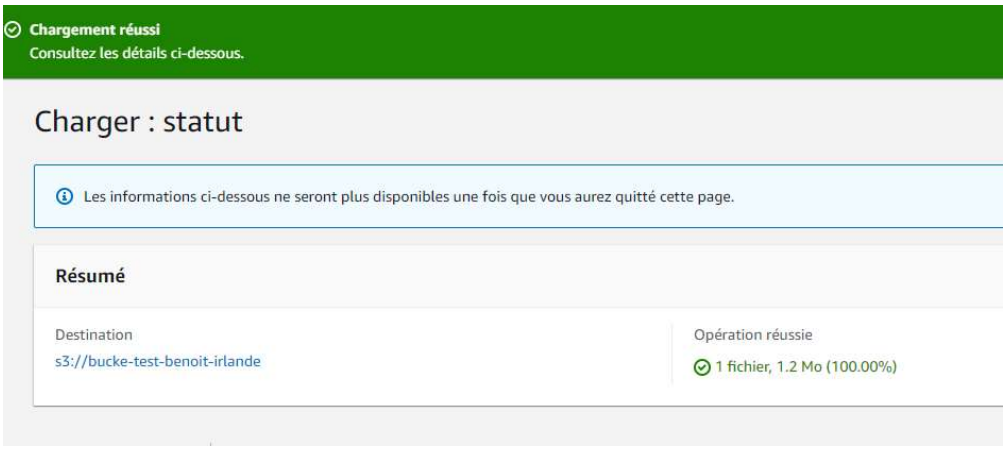
Ajouter une balise





Charger un fichier :





Il y a différentes offres qui permettent de stocker différents types de fichier en fonction de leur utilisation :

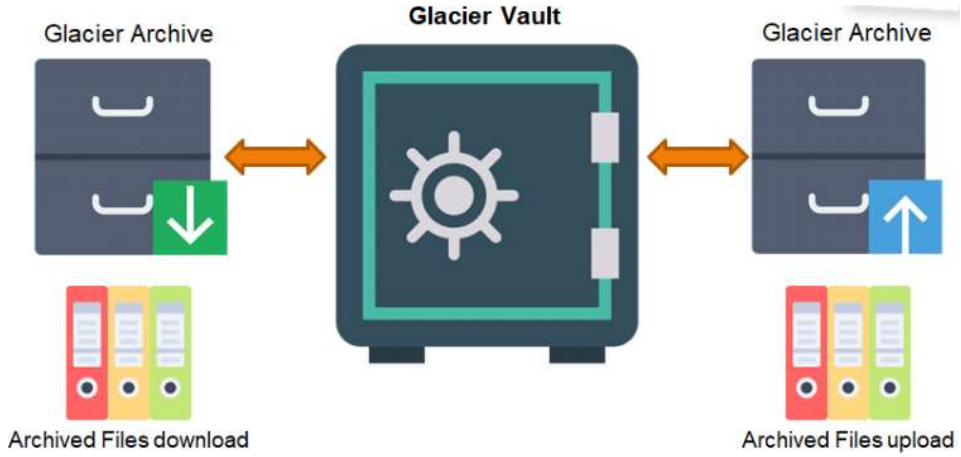
Classe de stockage

Amazon S3 propose une gamme de classes de stockage conçues pour différents cas d'utilisation. En savoir plus ou consulter la tarification Amazon S3.

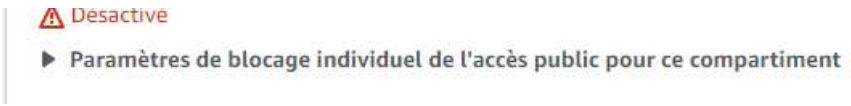
	Classe de stockage	Conçue pour	Zones de disponibilité	Durée de stockage minimale	T r c f
◉	Standard	Données consultées fréquemment (plusieurs fois par mois) avec un accès en millisecondes	≥ 3	-	-
○	Hiérarchie intelligente	Données comportant des modèles d'accès changeants ou inconnus	≥ 3	-	-
○	Standard – Accès peu fréquent	Données consultées rarement (une fois par mois) avec un accès en millisecondes	≥ 3	30 jours	1
○	Unizone – Accès peu fréquent	Données pouvant être recréées et consultées peu fréquemment (une fois par mois) stockées dans une seule zone de disponibilité avec un accès en millisecondes	1	30 jours	1
○	Glacier Instant Retrieval	Données d'archivage à longue durée consultées une fois par trimestre avec extraction instantanée en millisecondes	≥ 3	90 jours	1
	Glacier				

○	Glacier Flexible Retrieval (anciennement Glacier)	Données d'archivage à longue durée de vie consultées une fois par an avec temps d'extraction en minutes ou en heures	≥ 3	90 jours	-

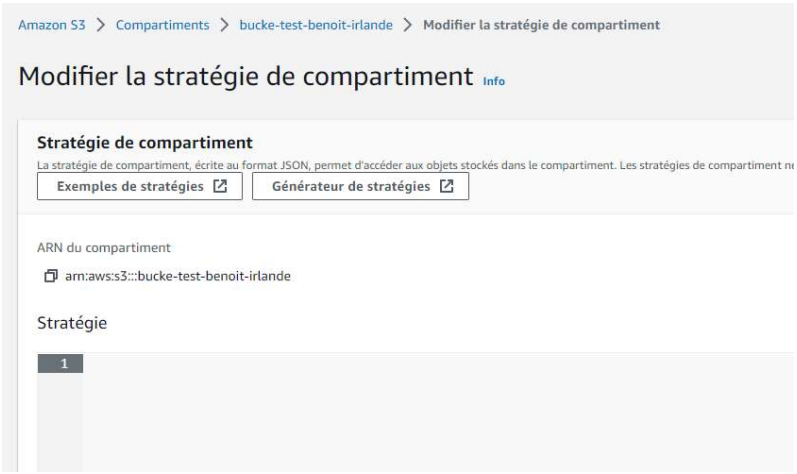
Offre glacier permet de stocker des documents peu consulté à moindre coût : la contrepartie est qu'on ne peut pas accéder tout de suite aux fichiers : il faut faire une demande à AWS



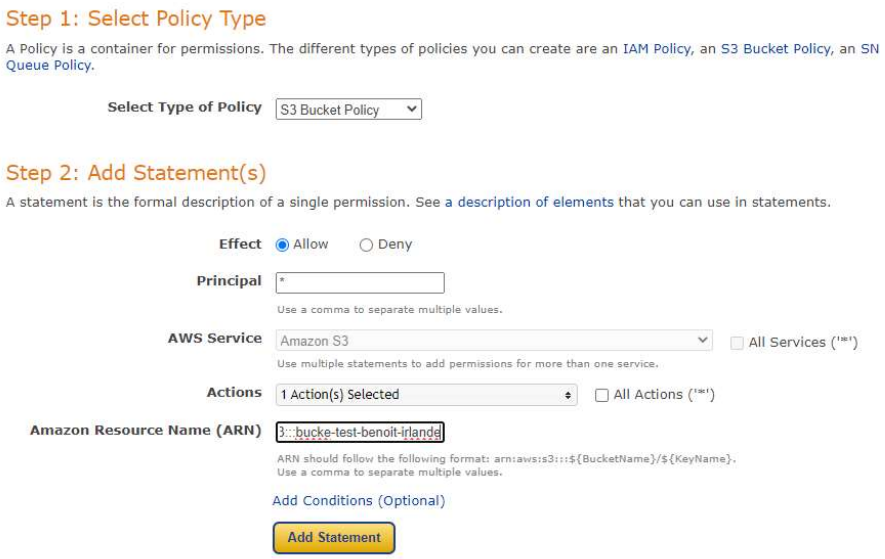
Pour accéder au fichier que nous avons stocké, il faut rendre le bucket public :

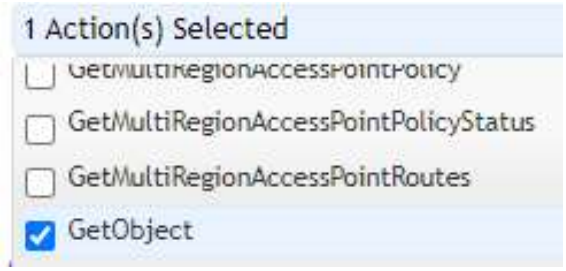


Notre bucket n'est pas encore rendu publique : pour le rendre accessible et manipulable, il faut modifier la stratégie de compartiment :



Dans générateur de stratégie, il faut définir :





Il génère un fichier JSON

```
{
  "Id": "Policy1676559343976",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1676559326009",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucke-test-benoit-irlande",
      "Principal": "*"
    }
  ]
}
```


Stratégie


```
{
  "Id": "Policy1676559365776",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1676559326009",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucke-test-benoit-irlande/*",
      "Principal": "*"
    }
  ]
}
```


Il faut rajouter un **/*** à la ligne **resource: arn** pour accéder à tout le contenu du bucket

Mon bucket est accessible publique suite à ces modifications :

Test d'accès à la ressource :