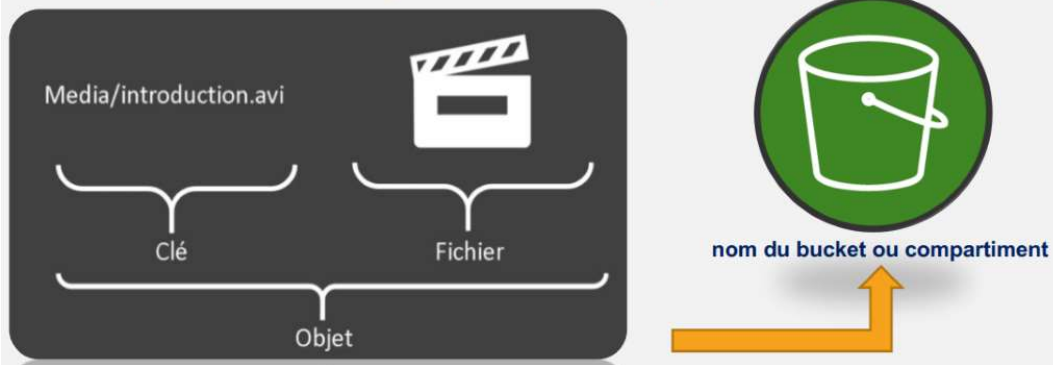


- ***Service entièrement géré de stockage dans le cloud.***
- ***Stoker virtuellement un nombre illimité d'objets.***
- ***Accessible à tous moments, de n'importe où.***
- ***Niveau de sécurité très élevé.***

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.

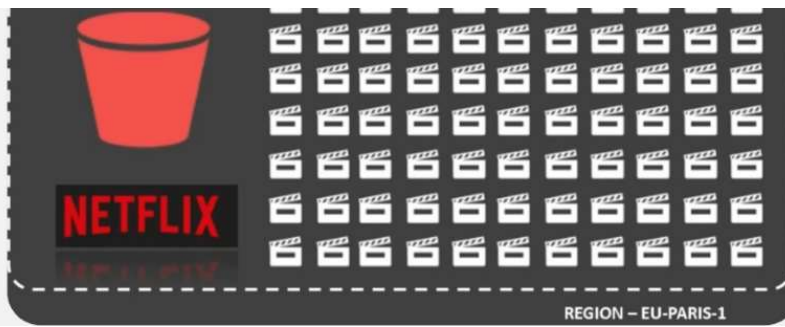


L'import des
objets est
gratuit.
Par internet,
si < 1 To.

8 – 4 – Mise à l'échelle dynamique



Redimensionnement dynamique.

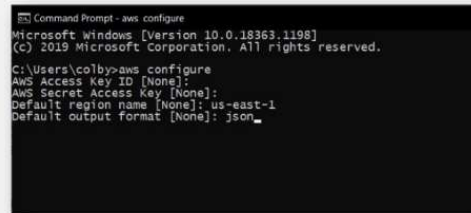


Pas de limite à la volumétrie.

8 – 5 – Gestion des données



Console d'Administration



CLI AWS



AWS SDK

8 – 6 – Cas d'usage



- Stocker des données applicatives.
- Hébergement de site web statique.
- Sauvegardes & Reprise d'activité après sinistre.
- Zone de stockage pour le « BigData ».
- Etc...



Créer un compartiment S3 :

Créer un compartiment [Info](#)

Les compartiments sont des conteneurs pour les données stockées dans S3. [En savoir plus](#)

Configuration générale

Nom du compartiment

bucket_test_benoit_irlande

Le nom du compartiment doit être unique mondialement et ne peut pas contenir d'espaces ni de majuscules. Voir les règles de [dénomination des compartiments](#)

Région AWS

UE (Irlande) eu-west-1

Copier les paramètres depuis un compartiment existant - *facultatif*

Seuls les paramètres de compartiment dans la configuration suivante sont copiés.

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](#)

☒ 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.

☒ 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.

☒ 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.

☒ 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.

☒ 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

Chiffrement par défaut [Info](#)

Le chiffrement côté serveur est automatiquement appliqué aux nouveaux objets stockés dans ce compartiment.

Type de clé de chiffrement [Info](#)

- ☒ Clés gérées par Amazon S3 (SSE-S3)
- ☐ Clé AWS Key Management Service (SSE-KMS)

Clé de compartiment

Lorsque le chiffrement KMS est utilisé pour chiffrer de nouveaux objets dans ce compartiment, la clé du compartiment réduit les coûts de chiffrement en réduisant les appels à AWS KMS. [En savoir plus](#)

- ☐ Désactiver
- ☒ Activer

▼ Paramètres avancés

Verrouillage d'objet

Stockez des objets à l'aide d'un modèle WORM (write-one-read-many) pour empêcher la suppression ou le remplacement de ceux-ci pendant une durée fixe ou indéfinie. [En savoir plus](#)

- ☒ Désactiver

- ☐ Activer

Permet de verrouiller définitivement les objets de ce compartiment. Une configuration supplémentaire de Verrouillage d'objet est requise dans les détails du compartiment après la création du compartiment pour empêcher la suppression ou le remplacement des objets de ce compartiment.

i Verrouillage d'objet fonctionne uniquement dans les compartiments activés pour la gestion des versions. L'activation de Verrouillage d'objet active automatiquement la gestion des versions de compartiment.

Compartiments (81) [Info](#)

Les compartiments sont des conteneurs pour les données stockées dans S3. [En savoir plus](#)

1 correspondance

Nom



Région AWS

☐ bucke-test-benoit-irlande

UE (Irlande) eu-west-1

bucke-test-benoit-irlande [Info](#)

Objets | Propriétés | Autorisations | Métriques | Gestion | Points d'accès

Objets (0)

Les objets sont les entités fondamentales stockées dans Amazon S3. Vous pouvez utiliser l'[Inventaire Amazon S3](#) pour obtenir une liste de tous les objets de votre compartiment. Pour que d'autres personnes puissent accéder à vos objets, vous devez configurer des autorisations. [En savoir plus](#)

☐ Afficher les versions

☐ Nom ☐ Type ☐ Dernière modification ☐ Taille ☐ Classe de stockage

Aucun objet

Vous n'avez aucun objet dans ce compartiment.

Charger un fichier :

Amazon S3 > Compartiments > bucke-test-benoit-irlande > Charger

Charger [Info](#)

Ajoutez les fichiers et dossiers que vous souhaitez charger dans S3. Pour charger un fichier d'une taille supérieure à 160 Go, utilisez la CLI AWS, le kit SDK AWS ou l'API REST Amazon S3. [En savoir plus](#)

Faites glisser et déposez les fichiers et dossiers que vous souhaitez charger ici, ou sélectionnez **Ajouter des fichiers** ou **Ajouter des dossiers**.

Fichiers et dossiers (1 Total, 1.2 Mo)

Tous les fichiers et dossiers de cette table seront chargés.

Ajouter des fichiers

[Ajouter un dossier](#)

🔍 Rechercher par nom

< 1 >

<input type="checkbox"/>	Nom ▲	Dossier ▼	Type ▼	Taille ▼
<input type="checkbox"/>	AWS_VPC.pdf	-	application/pdf	1.2 Mo

Destination

Destination

s3://bucke-test-benoit-irlande

► **Détails de la destination**

Paramètres de compartiment ayant un impact sur les nouveaux objets stockés dans la destination spécifiée.

Chargement réussi

Consultez les détails ci-dessous.

Charger : statut

 Les informations ci-dessous ne seront plus disponibles une fois que vous aurez quitté cette page.

Résumé

Destination

s3://bucke-test-benoit-irlande

Opération réussie

✔ 1 fichier, 1.2 Mo (100.00%)

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

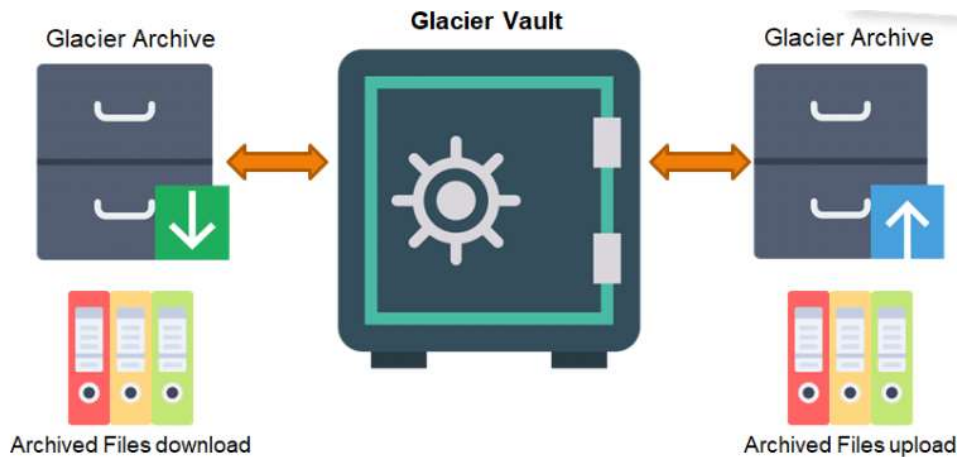
Classe de stockage

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	Taux de disponibilité
<input checked="" type="radio"/>	Standard	Données consultées fréquemment (plusieurs fois par mois) avec un accès en millisecondes	≥ 3	-	-
<input type="radio"/>	Hiérarchie intelligente	Données comportant des modèles d'accès changeants ou inconnus	≥ 3	-	-
<input type="radio"/>	Standard – Accès peu fréquent	Données consultées rarement (une fois par mois) avec un accès en millisecondes	≥ 3	30 jours	1
<input type="radio"/>	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
<input type="radio"/>	Glacier Instant Retrieval	Données d'archivage à longue durée consultées une fois par trimestre avec extraction instantanée en millisecondes	≥ 3	90 jours	1

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

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 :

bucket-test-benoit-irlande
[Info](#)

Objets
Propriétés
Autorisations
Métriques
Gestion
Points d'accès

Présentation des autorisations

Accéder
Compartiment et objets non publics

Modifier Bloquer l'accès public (paramètres de compartiment)

[Info](#)

Bloquer l'accès public (paramètres de compartiment)

L'accès public aux compartiments et objets est accordé via des listes de contrôle d'accès (ACL), des stratégies de compartiment, des stratégies de point d'accès ou tous ces éléments à la fois. Pour bloquer l'accès public à tous vos compartiments et objets S3, activez « Bloquer tous les accès publics ». Ces paramètres s'appliquent uniquement à ce compartiment et ses points d'accès. AWS recommande d'activer « Bloquer tous les accès publics ». Toutefois, avant d'appliquer ces paramètres, vérifiez que vos applications fonctionneront correctement sans accès public. Si vous avez besoin d'un certain niveau d'accès public à vos compartiments ou objets, vous pouvez personnaliser les paramètres individuels ci-dessous en fonction de vos cas d'utilisation de stockage spécifiques. [En savoir plus](#)

☐ **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.

Bloquer l'accès public (paramètres de compartiment)

L'accès public aux compartiments et objets est accordé via des listes de contrôle d'accès (ACL), des stratégies de compartiment, des stratégies de point d'accès ou tous ces éléments à la fois. Pour bloquer l'accès public à tous vos compartiments et objets S3, activez « Bloquer tous les accès publics ». Ces paramètres s'appliquent uniquement à ce compartiment et ses points d'accès. AWS recommande d'activer « Bloquer tous les accès publics ». Toutefois, avant d'appliquer ces paramètres, vérifiez que vos applications fonctionneront correctement sans accès public. Si vous avez besoin d'un certain niveau d'accès public à vos compartiments ou objets, vous pouvez personnaliser les paramètres individuels ci-dessous en fonction de vos cas d'utilisation de stockage spécifiques. [En savoir plus](#)

Modifier

Bloquer tous les accès publics

⚠ Désactive

► Paramètres de blocage individuel de l'accès public pour ce compartiment

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

Amazon S3 > Compartiments > bucke-test-benoit-irlande > Modifier la stratégie de compartiment

Modifier la stratégie de compartiment [Info](#)

Stratégie de compartiment
La stratégie de compartiment, écrite au format JSON, permet d'accéder aux objets stockés dans le compartiment. Les stratégies de compartiment ne peuvent pas être supprimées.

[Exemples de stratégies](#) [Générateur de stratégies](#)

ARN du compartiment
arn:aws:s3::bucke-test-benoit-irlande

Stratégie

1

Dans générateur de stratégie, il faut définir :

Step 1: Select Policy Type

A Policy is a container for permissions. The different types of policies you can create are an IAM Policy, an S3 Bucket Policy, an SN Queue Policy.

Select Type of Policy S3 Bucket Policy

Step 2: Add Statement(s)

A statement is the formal description of a single permission. See [a description of elements](#) that you can use in statements.

Effect ☒ Allow ☐ Deny

Principal
Use a comma to separate multiple values.

AWS Service Amazon S3 ☐ All Services ^(*)
Use multiple statements to add permissions for more than one service.

Actions 1 Action(s) Selected ☐ All Actions ^(*)

Amazon Resource Name (ARN)
ARN should follow the following format: arn:aws:s3:::{BucketName}/{KeyName}. Use a comma to separate multiple values.

Add Conditions (Optional)

[Add Statement](#)

1 Action(s) Selected

<input type="checkbox"/>	GetMultiRegionAccessPointPolicy
<input type="checkbox"/>	GetMultiRegionAccessPointPolicyStatus
<input type="checkbox"/>	GetMultiRegionAccessPointRoutes
<input checked="" type="checkbox"/>	GetObject

You added the following statements. Click the button below to Generate a policy.

Principal(s)	Effect	Action	Resource
*	Allow	s3:GetObject	arn:aws:s3::bucke-test-benoit-irlande

Step 3: Generate Policy

A policy is a document (written in the Access Policy Language) that acts as a container for one or more statements.

[Generate Policy](#) [Start Over](#)

Il génère un fichier JSON

Policy JSON Document

Click below to edit. To save the policy, copy the text below to a text editor. Changes made below will not be reflected in the policy generator tool.


```

{
  "Id": "Policy1676559343976",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmnt1676559326009",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucke-test-benoit-irlande",
      "Principal": "*"
    }
  ]
}

```

Stratégie

```

1  {
2    "Id": "Policy1676559365776",
3    "Version": "2012-10-17",
4    "Statement": [
5      {
6        "Sid": "Stmnt1676559326009",
7        "Action": [
8          "s3:GetObject"
9        ],
10       "Effect": "Allow",
11       "Resource": "arn:aws:s3:::bucke-test-benoit-irlande/*",
12       "Principal": "*"
13     }
14   ]
15 }

```

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 :

