

02. S3 Security

Par défaut, quand tu crées un bucket S3, tout est fermé. Personne n'a accès à rien, sauf le créateur du compte.

1. Les deux outils pour ouvrir l'accès

Pour donner une permission, tu choisis l'une de ces deux méthodes (ou les deux) :

Method A : La méthode "Utilisateur" (IAM Policy)

- **C'est quoi ?** Une feuille de permission que tu donnes à un utilisateur ou un rôle précis.
- **Logique :** Tu dis à l'utilisateur : *"Toi, tu as le droit d'aller lire le bucket X."*

Method B : La méthode "Bucket" (Bucket Policy)

- **C'est quoi ?** Une feuille de permission collée directement sur le bucket.
 - **Logique :** Le bucket dit : *"J'autorise telle personne ou tel compte externe à venir chez moi."*
-

2. Comment S3 prend sa décision ?

Quand quelqu'un clique sur un fichier dans S3, AWS vérifie les permissions dans cet ordre :

1. **Y a-t-il une interdiction (Deny) ?** Si une règle dit "Interdit", c'est fini. L'accès est bloqué immédiatement, même si une autre règle disait oui.
 2. **Y a-t-il une autorisation (Allow) ?** S'il n'y a pas de Deny, il faut au moins un Allow (soit sur l'utilisateur, soit sur le bucket) pour que ça passe.
-

3. Trois cas particuliers pour l'examen

Scénario 1 : Bloquer les fuites de données sur Internet

- **Le besoin :** Tu veux une sécurité absolue pour qu'aucun employé ne puisse rendre le bucket public par erreur.
- **La solution : Block Public Access (BPA).** C'est un gros bouton de sécurité activé par défaut qui bloque tout Internet.

Scénario 2 : Partager un fichier privé avec un client externe

- **Le besoin :** Un client (qui n'a pas de compte AWS) doit télécharger une facture privée ou uploader sa photo.

- **La solution : Presigned URL (URL Présignée).** Tu lui génères un lien magique, sécurisé et temporaire (valable 15 minutes par exemple).

Scénario 3 : Connecter tes serveurs privés à S3

- **Le besoin :** Tes serveurs AWS sont isolés du monde (pas d'Internet). Ils ont pourtant besoin de parler à S3.
- **La solution : VPC Gateway Endpoint.** Un tunnel privé qui relie tes serveurs à S3 sans jamais passer par Internet.

Revision #4

Created 2026-05-28 10:02:15 UTC by Victor

Updated 2026-05-29 13:59:03 UTC by Victor