Politiques d'accès aux buckets et aux groupes

StorageGRID software

NetApp
December 03, 2025

Sommaire

Politiques d’accès aux buckets et aux groupes

Utiliser des politiques d’accès aux buckets et aux groupes

StorageGRID utilise le langage de stratégie Amazon Web Services (AWS) pour permettre aux locataires S3 de contrôler l’accès aux buckets et aux objets au sein de ces buckets. Le système StorageGRID implémente un sous-ensemble du langage de politique de l’API REST S3. Les politiques d’accès pour l’API S3 sont écrites en JSON.

Aperçu de la politique d’accès

Il existe deux types de politiques d’accès prises en charge par StorageGRID.

- **Stratégies de bucket**, qui sont gérées à l’aide des opérations API S3 GetBucketPolicy, PutBucketPolicy et DeleteBucketPolicy ou de l’API Tenant Manager ou Tenant Management. Les stratégies de bucket sont attachées aux buckets, elles sont donc configurées pour contrôler l’accès des utilisateurs du compte propriétaire du bucket ou d’autres comptes au bucket et aux objets qu’il contient. Une politique de bucket s’applique à un seul bucket et éventuellement à plusieurs groupes.
- **Stratégies de groupe**, qui sont configurées à l’aide de Tenant Manager ou de l’API Tenant Management. Les stratégies de groupe sont attachées à un groupe dans le compte, elles sont donc configurées pour permettre à ce groupe d’accéder à des ressources spécifiques appartenant à ce compte. Une stratégie de groupe s’applique à un seul groupe et éventuellement à plusieurs compartiments.

Il n’y a aucune différence de priorité entre les politiques de groupe et de compartiment.

Les stratégies de bucket et de groupe StorageGRID suivent une grammaire spécifique définie par Amazon. À l’intérieur de chaque politique se trouve un ensemble d’énoncés de politique, et chaque énoncé contient les éléments suivants :

- ID de relevé (Sid) (facultatif)
- Effet
- Principal/Non principal
- Ressource/PasRessource
- Action/Pas d’action
- Condition (facultatif)

Les instructions de politique sont construites à l’aide de cette structure pour spécifier les autorisations : Accorder <Effet> pour autoriser/refuser à <Principal> d’effectuer <Action> sur <Ressource> lorsque <Condition> s’applique.

Chaque élément de politique est utilisé pour une fonction spécifique :

Élément	Description
Sid	L’élément Sid est facultatif. Le Sid est uniquement destiné à servir de description pour l’utilisateur. Il est stocké mais non interprété par le système StorageGRID .

Élément	Description
Effet	Utilisez l'élément Effet pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) sur les buckets ou les objets à l'aide des mots-clés d'élément Action pris en charge.
Principal/Non principal	Vous pouvez autoriser les utilisateurs, les groupes et les comptes à accéder à des ressources spécifiques et à effectuer des actions spécifiques. Si aucune signature S3 n'est incluse dans la demande, l'accès anonyme est autorisé en spécifiant le caractère générique (*) comme principal. Par défaut, seul le root du compte a accès aux ressources appartenant au compte. Il vous suffit de spécifier l'élément Principal dans une stratégie de bucket. Pour les stratégies de groupe, le groupe auquel la stratégie est attachée est l'élément principal implicite.
Ressource/PasRessource	L'élément Ressource identifie les buckets et les objets. Vous pouvez autoriser ou refuser des autorisations sur des buckets et des objets à l'aide du nom de ressource Amazon (ARN) pour identifier la ressource.
Action/Pas d'action	Les éléments Action et Effet sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à cette ressource lui est accordé ou refusé. L'accès est refusé à moins que vous n'attribuiez spécifiquement des autorisations, mais vous pouvez utiliser un refus explicite pour remplacer une autorisation accordée par une autre politique.
Condition	L'élément Condition est facultatif. Les conditions vous permettent de créer des expressions pour déterminer quand une politique doit être appliquée.

Dans l'élément Action, vous pouvez utiliser le caractère générique (*) pour spécifier toutes les opérations ou un sous-ensemble d'opérations. Par exemple, cette action correspond aux autorisations telles que s3:GetObject, s3:PutObject et s3:DeleteObject.

```
s3:*Object
```

Dans l'élément Ressource, vous pouvez utiliser les caractères génériques (*) et (?). Alors que l'astérisque (*) correspond à 0 ou plusieurs caractères, le point d'interrogation (?) correspond à n'importe quel caractère unique.

Dans l'élément Principal, les caractères génériques ne sont pas pris en charge, sauf pour définir un accès anonyme, qui accorde une autorisation à tout le monde. Par exemple, vous définissez le caractère générique (*) comme valeur principale.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

Dans l'exemple suivant, l'instruction utilise les éléments Effet, Principal, Action et Ressource. Cet exemple montre une déclaration de politique de compartiment complète qui utilise l'effet « Autoriser » pour donner aux principaux, le groupe d'administrateurs `federated-group/admin` et le groupe financier `federated-group/finance` , autorisations pour effectuer l'action `s3:ListBucket` sur le seau nommé `mybucket` et l'action `s3:GetObject` sur tous les objets à l'intérieur de ce seau.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

La politique de compartiment a une limite de taille de 20 480 octets et la politique de groupe a une limite de taille de 5 120 octets.

Cohérence des politiques

Par défaut, toutes les mises à jour que vous apportez aux stratégies de groupe sont finalement cohérentes. Lorsqu'une stratégie de groupe devient cohérente, les modifications peuvent prendre 15 minutes supplémentaires pour prendre effet, en raison de la mise en cache des stratégies. Par défaut, toutes les mises à jour que vous apportez aux stratégies de compartiment sont fortement cohérentes.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour de la stratégie de compartiment. Par exemple, vous souhaiterez peut-être qu'une modification apportée à une stratégie de compartiment soit disponible en cas de panne du site.

Dans ce cas, vous pouvez soit définir le `Consistency-Control` en-tête dans la demande PutBucketPolicy, ou vous pouvez utiliser la demande de cohérence PUT Bucket. Lorsqu'une stratégie de compartiment devient cohérente, les modifications peuvent prendre 8 secondes supplémentaires pour prendre effet, en raison de la

mise en cache de la stratégie.

> Si vous définissez la cohérence sur une valeur différente pour contourner une situation temporaire, assurez-vous de redéfinir le paramètre au niveau du bucket sur sa valeur d'origine lorsque vous avez terminé. Dans le cas contraire, toutes les futures demandes de bucket utiliseront le paramètre modifié.

Utiliser l'ARN dans les déclarations de politique

Dans les déclarations de politique, l'ARN est utilisé dans les éléments Principal et Ressource.

- Utilisez cette syntaxe pour spécifier l'ARN de la ressource S3 :

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilisez cette syntaxe pour spécifier l'ARN de la ressource d'identité (utilisateurs et groupes) :

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Autres considérations :

- Vous pouvez utiliser l'astérisque (*) comme caractère générique pour faire correspondre zéro ou plusieurs caractères à l'intérieur de la clé d'objet.
- Les caractères internationaux, qui peuvent être spécifiés dans la clé d'objet, doivent être codés à l'aide de JSON UTF-8 ou à l'aide de séquences d'échappement JSON \u. Le codage en pourcentage n'est pas pris en charge.

  "Syntaxe URN RFC 2141"

  Le corps de la requête HTTP pour l'opération PutBucketPolicy doit être codé avec charset=UTF-8.

Spécifier les ressources dans une politique

Dans les instructions de politique, vous pouvez utiliser l'élément Ressource pour spécifier le compartiment ou l'objet pour lequel les autorisations sont accordées ou refusées.

- Chaque déclaration de politique nécessite un élément Ressource. Dans une politique, les ressources sont désignées par l'élément `Resource` , ou alternativement, `NotResource` pour l'exclusion.
- Vous spécifiez les ressources avec un ARN de ressource S3. Par exemple:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Vous pouvez également utiliser des variables de politique à l'intérieur de la clé d'objet. Par exemple:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- La valeur de la ressource peut spécifier un compartiment qui n'existe pas encore lors de la création d'une stratégie de groupe.

Spécifier les principaux dans une politique

Utilisez l'élément Principal pour identifier le compte d'utilisateur, de groupe ou de locataire auquel l'accès à la ressource est autorisé/refusé par l'instruction de stratégie.

- Chaque déclaration de politique dans une politique de compartiment doit inclure un élément Principal. Les instructions de politique dans une politique de groupe n'ont pas besoin de l'élément Principal car le groupe est considéré comme le principal.
- Dans une politique, les mandants sont désignés par l'élément « Principal » ou « NotPrincipal » pour l'exclusion.
- Les identités basées sur un compte doivent être spécifiées à l'aide d'un ID ou d'un ARN :

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- Cet exemple utilise l'ID de compte locataire 27233906934684427525, qui inclut la racine du compte et tous les utilisateurs du compte :

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Vous pouvez spécifier uniquement la racine du compte :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Vous pouvez spécifier un utilisateur fédéré spécifique (« Alex ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Vous pouvez spécifier un groupe fédéré spécifique (« Managers ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Vous pouvez spécifier un principal anonyme :

```
"Principal": "*"
```

- Pour éviter toute ambiguïté, vous pouvez utiliser l'UUID de l'utilisateur au lieu du nom d'utilisateur :

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

  Par exemple, supposons qu'Alex quitte l'organisation et le nom d'utilisateur `Alex` est supprimé. Si un nouvel Alex rejoint l'organisation et se voit attribuer le même `Alex` nom d'utilisateur, le nouvel utilisateur peut hériter involontairement des autorisations accordées à l'utilisateur d'origine.

- La valeur principale peut spécifier un nom de groupe/utilisateur qui n'existe pas encore lors de la création d'une stratégie de compartiment.

Spécifier les autorisations dans une politique

Dans une politique, l'élément Action est utilisé pour autoriser/refuser des autorisations à une ressource. Il existe un ensemble d'autorisations que vous pouvez spécifier dans une politique, qui sont indiquées par l'élément « Action » ou, alternativement, « NotAction » pour l'exclusion. Chacun de ces éléments correspond à des opérations spécifiques de l'API REST S3.

Les tableaux répertorient les autorisations qui s'appliquent aux buckets et les autorisations qui s'appliquent aux objets.

> Amazon S3 utilise désormais l'autorisation s3:PutReplicationConfiguration pour les actions PutBucketReplication et DeleteBucketReplication. StorageGRID utilise des autorisations distinctes pour chaque action, ce qui correspond à la spécification Amazon S3 d'origine.

> Une suppression est effectuée lorsqu'un put est utilisé pour écraser une valeur existante.

Autorisations qui s'appliquent aux buckets

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3:Créer un bucket	Créer un bucket	Oui. **Remarque** : À utiliser uniquement dans la stratégie de groupe.
s3 : Supprimer le bucket	Supprimer le bucket	
s3 : Supprimer la notification des métadonnées du bucket	SUPPRIMER la configuration de notification des métadonnées du bucket	Oui

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Supprimer la politique de bucket	Supprimer la politique de bucket	
s3 : Supprimer la configuration de réplication	SupprimerBucketReplication	Oui, des autorisations distinctes pour PUT et DELETE
s3 : Obtenir l'Acl du bucket	ObtenirBucketAcl	
s3 : Obtenir la conformité du bucket	Conformité du bucket GET (obsolète)	Oui
s3 : GetBucketConsistency	Cohérence du bucket GET	Oui
s3:Obtenir le bucket CORS	ObtenirBucketCors	
s3 : Obtenir la configuration du chiffrement	Obtenir le chiffrement du bucket	
s3 : Obtenir l'heure du dernier accès au bucket	Heure du dernier accès au bucket GET	Oui
s3 : Obtenir l'emplacement du bucket	Obtenir l'emplacement du bucket	
s3 : GetBucketMetadataNotification	Configuration de la notification des métadonnées du bucket GET	Oui
s3 : Obtenir une notification de bucket	Configuration de GetBucketNotification	
s3 : GetBucketObjectLockConfiguration	Obtenir la configuration du verrouillage de l'objet	
s3 : Obtenir la politique du bucket	Obtenir la politique de Bucket	
s3 : Obtenir le balisage du bucket	Obtenir le balisage du bucket	
s3 : Obtenir la gestion des versions du bucket	Obtenir la gestion des versions du bucket	
s3 : Obtenir la configuration du cycle de vie	GetBucketLifecycleConfiguration	
s3 : Obtenir la configuration de réplication	Réplication GetBucket	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : ListeTousMesSeaux	• Listes de seaux • Utilisation du stockage GET	Oui, pour l'utilisation du stockage GET. **Remarque** : À utiliser uniquement dans la stratégie de groupe.
s3:ListBucket	• Liste d'objets • Tête de godet • Restaurer l'objet	
s3 : ListBucketMultipartUploads	• ListeMultipartUploads • Restaurer l'objet	
s3 : ListBucketVersions	Versions du bucket GET	
s3 : PutBucketCompliance	Conformité du compartiment PUT (obsolète)	Oui
s3 : PutBucketConsistency	Cohérence du seau PUT	Oui
s3:PutBucketCORS	• SupprimerBucketCors† • PutBucketCors	
s3 : PutEncryptionConfiguration	• Supprimer le chiffrement du bucket • Cryptage PutBucket	
s3 : PutBucketLastAccessTime	Heure du dernier accès au bucket PUT	Oui
s3 : PutBucketMetadataNotification	Configuration des notifications de métadonnées du compartiment PUT	Oui
s3 : PutBucketNotification	Configuration de PutBucketNotification	
s3 : PutBucketObjectLockConfiguration	• CreateBucket avec le `x-amz-bucket-object-lock-enabled: true` en-tête de requête (nécessite également l'autorisation s3:CreateBucket) • Configuration de PutObjectLock	
s3 : PutBucketPolicy	Politique de PutBucket	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Mettre en place le balisage du bucket	• Supprimer le balisage du bucket† • Balisage de PutBucket	
s3 : PutBucketVersioning	Gestion des versions de PutBucket	
s3 : PutLifecycleConfiguration	• Supprimer le cycle de vie du bucket† • Configuration du cycle de vie de PutBucket	
s3 : PutReplicationConfiguration	Réplication de PutBucket	Oui, des autorisations distinctes pour PUT et DELETE

Autorisations qui s'appliquent aux objets

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Abandonner le téléchargement en plusieurs parties	• Abandonner le téléchargement en plusieurs parties • Restaurer l'objet	
s3 : Contournement de la gouvernance et de la rétention	• Supprimer l'objet • Supprimer les objets • PutObjectRetention	
s3:Supprimer l'objet	• Supprimer l'objet • Supprimer les objets • Restaurer l'objet	
s3 : Supprimer le balisage d'objet	Supprimer l'étiquetage des objets	
s3 : Supprimer le balisage de version d'objet	DeleteObjectTagging (une version spécifique de l'objet)	
s3 : Supprimer la version de l'objet	DeleteObject (une version spécifique de l'objet)	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3:Obtenir l'objet	• Obtenir l'objet • HeadObject • Restaurer l'objet • Sélectionner le contenu de l'objet	
s3:GetObjectAcl	ObtenirObjectAcl	
s3 : GetObjectLegalHold	Obtenir la conservation légale de l'objet	
s3 : Obtenir la rétention d'objet	Obtenir la rétention d'objet	
s3 : Obtenir le balisage des objets	Obtenir l'étiquetage des objets	
s3 : Obtenir le balisage de la version de l'objet	GetObjectTagging (une version spécifique de l'objet)	
s3 : Obtenir la version de l'objet	GetObject (une version spécifique de l'objet)	
s3 : ListeMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• Mettre l'objet • Copier l'objet • Restaurer l'objet • Créer un téléchargement multi-parties • Téléchargement complet en plusieurs parties • Télécharger une partie • TéléchargerPartCopy	
s3 : PutObjectLegalHold	MettreObjetLegalHold	
s3 : PutObjectRetention	PutObjectRetention	
s3 : Mettre en place un balisage d'objet	Balisage d'objets	
s3 : Mettre en place la version de l'objet	PutObjectTagging (une version spécifique de l'objet)	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : PutOverwriteObject	• Mettre l'objet • Copier l'objet • Balisage d'objets • Supprimer l'étiquetage des objets • Téléchargement complet en plusieurs parties	Oui
s3:RestoreObject	Restaurer l'objet	

Utiliser l'autorisation PutOverwriteObject

L'autorisation s3:PutOverwriteObject est une autorisation StorageGRID personnalisée qui s'applique aux opérations qui créent ou mettent à jour des objets. Le paramètre de cette autorisation détermine si le client peut écraser les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'un objet S3.

Les paramètres possibles pour cette autorisation incluent :

- **Autoriser**: Le client peut écraser un objet. Il s'agit du paramètre par défaut.
- **Refuser** : Le client ne peut pas écraser un objet. Lorsqu'elle est définie sur Refuser, l'autorisation PutOverwriteObject fonctionne comme suit :
  - Si un objet existant est trouvé sur le même chemin :
    - Les données de l'objet, les métadonnées définies par l'utilisateur ou le balisage de l'objet S3 ne peuvent pas être écrasés.
    - Toutes les opérations d'ingestion en cours sont annulées et une erreur est renvoyée.
    - Si le contrôle de version S3 est activé, le paramètre Refuser empêche les opérations PutObjectTagging ou DeleteObjectTagging de modifier le TagSet d'un objet et ses versions non actuelles.
  - Si aucun objet existant n'est trouvé, cette autorisation n'a aucun effet.
- Lorsque cette autorisation n'est pas présente, l'effet est le même que si Autoriser était défini.

> Si la stratégie S3 actuelle autorise l'écrasement et que l'autorisation PutOverwriteObject est définie sur Refuser, le client ne peut pas écraser les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'un objet. De plus, si la case à cocher **Empêcher la modification du client** est sélectionnée (**CONFIGURATION** > **Paramètres de sécurité** > **Réseau et objets**), ce paramètre remplace le paramètre de l'autorisation PutOverwriteObject.

Spécifier les conditions dans une politique

Les conditions définissent quand une politique sera en vigueur. Les conditions sont constituées d'opérateurs et de paires clé-valeur.

Les conditions utilisent des paires clé-valeur pour l'évaluation. Un élément Condition peut contenir plusieurs conditions, et chaque condition peut contenir plusieurs paires clé-valeur. Le bloc de condition utilise le format suivant :

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

Dans l'exemple suivant, la condition IpAddress utilise la clé de condition SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Opérateurs de condition pris en charge

Les opérateurs de condition sont classés comme suit :

- Chaîne
- Numérique
- Booléen
- adresse IP
- Vérification nulle

Opérateurs de condition	Description
Chaîne égale	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (sensible à la casse).
Chaîne non égale	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (sensible à la casse).
Chaîne égale à Ignorer la casse	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (ignore la casse).
Chaîne non égale à ignorer la casse	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (ignore la casse).
Comme une chaîne	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (sensible à la casse). Peut inclure les caractères génériques * et ?.
ChaînePasComme	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (sensible à la casse). Peut inclure les caractères génériques * et ?.

Opérateurs de condition	Description
NumériqueÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance exacte.
NumériqueNonÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance négative.
Numérique supérieur à	Compare une clé à une valeur numérique en fonction d'une correspondance « supérieure à ».
Numérique supérieur à égal	Compare une clé à une valeur numérique en fonction d'une correspondance « supérieure ou égale ».
NumériqueInférieurÀ	Compare une clé à une valeur numérique en fonction d'une correspondance « inférieure à ».
NumériqueInférieurÀÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance « inférieure ou égale ».
Booléen	Compare une clé à une valeur booléenne en fonction d'une correspondance « vrai ou faux ».
Adresse IP	Compare une clé à une adresse IP ou à une plage d'adresses IP.
Pas d'adresse IP	Compare une clé à une adresse IP ou à une plage d'adresses IP en fonction d'une correspondance négative.
Nul	Vérifie si une clé de condition est présente dans le contexte de la demande actuelle.

Clés de condition prises en charge

Clés de condition	Actions	Description
aws:SourceIP	opérateurs IP	Sera comparé à l'adresse IP à partir de laquelle la demande a été envoyée. Peut être utilisé pour les opérations de bucket ou d'objet. **Remarque :** si la requête S3 a été envoyée via le service d'équilibrage de charge sur les nœuds d'administration et les nœuds de passerelle, elle sera comparée à l'adresse IP en amont du service d'équilibrage de charge. **Remarque** : si un équilibreur de charge tiers non transparent est utilisé, cela sera comparé à l'adresse IP de cet équilibreur de charge. N'importe lequel `X-Forwarded-For` l'en-tête sera ignoré car sa validité ne peut pas être vérifiée.
aws:nom d'utilisateur	Ressource/Identité	Sera comparé au nom d'utilisateur de l'expéditeur à partir duquel la demande a été envoyée. Peut être utilisé pour les opérations de bucket ou d'objet.
s3:délimiteur	s3:ListBucket et s3:Autorisations ListBucketVersions	Sera comparé au paramètre délimiteur spécifié dans une demande ListObjects ou ListObjectVersions.

Clés de condition	Actions	Description
s3:ExistingObjectTag/<clé-balise>	s3 : Supprimer le balisage d'objet s3 : Supprimer le balisage de version d'objet s3:Obtenir l'objet s3:GetObjectAcl 3 : Obtenir le balisage des objets s3 : Obtenir la version de l'objet s3 : ObtenirObjectVersion Acl s3 : Obtenir le balisage de la version de l'objet s3:PutObjectAcl s3 : Mettre en place un balisage d'objet s3:PutObjectVersionAcl s3 : Mettre en place la version de l'objet	Nécessitera que l'objet existant possède la clé et la valeur de balise spécifiques.
s3:max-clés	s3:ListBucket et s3:Autorisations ListBucketVersions	Sera comparé au paramètre max-keys spécifié dans une requête ListObjects ou ListObjectVersions.
s3 : jours de conservation restants pour le verrouillage d'objet	s3:PutObject	Comparable à la date de conservation spécifiée dans le `x-amz-object-lock-retain-until-date` en-tête de demande ou période de conservation par défaut calculée à partir du compartiment pour garantir que ces valeurs se situent dans la plage autorisée pour les demandes suivantes : • Mettre l'objet • Copier l'objet • Créer un téléchargement multi-parties

Clés de condition	Actions	Description
s3 : jours de conservation restants pour le verrouillage d'objet	s3 : PutObjectRetention	Compare la date de conservation spécifiée dans la demande PutObjectRetention pour garantir qu'elle se situe dans la plage autorisée.
s3:préfixe	s3:ListBucket et s3:Autorisations ListBucketVersions	Sera comparé au paramètre de préfixe spécifié dans une demande ListObjects ou ListObjectVersions.
s3:RequestObjectTag/<clé-balise>	s3:PutObject s3 : Mettre en place un balisage d'objet s3 : Mettre en place la version de l'objet	Nécessitera une clé et une valeur de balise spécifiques lorsque la demande d'objet inclut le balisage.

Spécifier les variables dans une politique

Vous pouvez utiliser des variables dans les politiques pour renseigner les informations de politique lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de politique dans le `Resource` élément et dans les comparaisons de chaînes dans le `Condition` élément.

Dans cet exemple, la variable `${aws:username}` fait partie de l'élément Ressource :

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

Dans cet exemple, la variable `${aws:username}` fait partie de la valeur de condition dans le bloc de condition :

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variable	Description
`${aws:SourceIp}`	Utilise la clé SourceIp comme variable fournie.
`${aws:username}`	Utilise la clé du nom d'utilisateur comme variable fournie.
`${s3:prefix}`	Utilise la clé de préfixe spécifique au service comme variable fournie.

Variable	Description
`${s3:max-keys}`	Utilise la clé max-keys spécifique au service comme variable fournie.
`${*}`	Caractère spécial. Utilise le caractère comme un caractère * littéral.
`${?}`	Caractère spécial. Utilise le caractère comme un caractère ? littéral.
`${$}`	Caractère spécial. Utilise le caractère comme un caractère $ littéral.

Créer des politiques nécessitant un traitement spécial

Parfois, une politique peut accorder des autorisations dangereuses pour la sécurité ou pour la poursuite des opérations, comme le verrouillage de l'utilisateur root du compte. L'implémentation de l'API REST StorageGRID S3 est moins restrictive lors de la validation des politiques qu'Amazon, mais tout aussi stricte lors de l'évaluation des politiques.

Description de la politique	Type de politique	Comportement d'Amazon	Comportement de StorageGRID
Refuser toute autorisation sur le compte root	Seau	Valide et appliqué, mais le compte utilisateur root conserve l'autorisation pour toutes les opérations de stratégie de compartiment S3	Même
Se refuser toute autorisation d'utilisateur/groupe	Groupe	Valide et appliqué	Même
Autoriser un groupe de comptes étrangers à accorder n'importe quelle autorisation	Seau	Principal invalide	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée lorsqu'elles sont autorisées par une stratégie
Autoriser un compte root ou un utilisateur étranger à accéder à n'importe quelle autorisation	Seau	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée lorsqu'elles sont autorisées par une stratégie	Même

Description de la politique	Type de politique	Comportement d'Amazon	Comportement de StorageGRID
Accorder à tout le monde des autorisations pour toutes les actions	Seau	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée pour la racine du compte étranger et les utilisateurs	Même
Refuser à tout le monde les autorisations pour toutes les actions	Seau	Valide et appliqué, mais le compte utilisateur root conserve l'autorisation pour toutes les opérations de stratégie de compartiment S3	Même
Le principal est un utilisateur ou un groupe inexistant	Seau	Principal invalide	Valide
La ressource est un bucket S3 inexistant	Groupe	Valide	Même
Principal est un groupe local	Seau	Principal invalide	Valide
La politique accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations pour placer des objets.	Seau	Valide. Les objets appartiennent au compte créateur et la politique de compartiment ne s'applique pas. Le compte créateur doit accorder des autorisations d'accès à l'objet à l'aide des listes de contrôle d'accès (ACL) d'objet.	Valide. Les objets appartiennent au compte propriétaire du bucket. La politique des seaux s'applique.

Protection WORM (écriture unique, lecture multiple)

Vous pouvez créer des buckets WORM (Write-Once-Read-Many) pour protéger les données, les métadonnées d'objet définies par l'utilisateur et le balisage d'objet S3. Vous configurez les buckets WORM pour permettre la création de nouveaux objets et pour empêcher l'écrasement ou la suppression du contenu existant. Utilisez l'une des approches décrites ici.

Pour garantir que les écrasements sont toujours refusés, vous pouvez :

- Depuis le Gestionnaire de grille, accédez à **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité** > **Réseau et objets**, puis cochez la case **Empêcher la modification du client**.
- Appliquez les règles et politiques S3 suivantes :
  - Ajoutez une opération PutOverwriteObject DENY à la stratégie S3.
  - Ajoutez une opération DeleteObject DENY à la stratégie S3.

◦ Ajoutez une opération PutObject ALLOW à la stratégie S3.

> La définition de DeleteObject sur DENY dans une stratégie S3 n'empêche pas ILM de supprimer des objets lorsqu'une règle telle que « zéro copie après 30 jours » existe.

> Même lorsque toutes ces règles et politiques sont appliquées, elles ne protègent pas contre les écritures simultanées (voir situation A). Ils protègent contre les écrasements séquentiels terminés (voir situation B).

Situation A : Écritures simultanées (non protégées)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situation B : Écrasements séquentiels terminés (protégés contre)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Informations connexes

- "Comment les règles ILM de StorageGRID gèrent les objets"
- "Exemples de politiques de compartiment"
- "Exemples de stratégies de groupe"
- "Gérer les objets avec ILM"
- "Utiliser un compte locataire"

Exemples de politiques de compartiment

Utilisez les exemples de cette section pour créer des politiques d'accès StorageGRID pour les buckets.

Les stratégies de compartiment spécifient les autorisations d'accès pour le compartiment auquel la stratégie est attachée. Vous configurez une stratégie de bucket en utilisant l'API S3 PutBucketPolicy via l'un de ces outils :

- "Gestionnaire de locataires" .
- AWS CLI utilisant cette commande (reportez-vous à"Opérations sur les godets"):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Exemple : autoriser tout le monde à accéder en lecture seule à un bucket

Dans cet exemple, tout le monde, y compris les personnes anonymes, est autorisé à répertorier les objets du bucket et à effectuer des opérations GetObject sur tous les objets du bucket. Toutes les autres opérations seront refusées. Notez que cette politique peut ne pas être particulièrement utile car personne, à l'exception de la racine du compte, n'a l'autorisation d'écrire dans le bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Exemple : autoriser tous les utilisateurs d'un compte à accéder pleinement à un bucket et tous les utilisateurs d'un autre compte à accéder en lecture seule à un bucket.

Dans cet exemple, toutes les personnes d'un compte spécifié sont autorisées à accéder pleinement à un compartiment, tandis que toutes les personnes d'un autre compte spécifié sont uniquement autorisées à répertorier le compartiment et à effectuer des opérations GetObject sur les objets du compartiment commençant par le `shared/` préfixe de clé d'objet.

> Dans StorageGRID, les objets créés par un compte non propriétaire (y compris les comptes anonymes) appartiennent au compte propriétaire du bucket. La politique de bucket s'applique à ces objets.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Exemple : autoriser tout le monde à accéder en lecture seule à un compartiment et à accorder un accès complet au groupe spécifié

Dans cet exemple, tout le monde, y compris les anonymes, est autorisé à répertorier le bucket et à effectuer des opérations GetObject sur tous les objets du bucket, tandis que seuls les utilisateurs appartenant au groupe `Marketing` dans le compte spécifié, un accès complet est autorisé.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemple : autoriser tout le monde à accéder en lecture et en écriture à un bucket si le client se trouve dans la plage d'adresses IP

Dans cet exemple, tout le monde, y compris les personnes anonymes, est autorisé à répertorier le bucket et à effectuer toutes les opérations d'objet sur tous les objets du bucket, à condition que les demandes proviennent d'une plage d'adresses IP spécifiée (54.240.143.0 à 54.240.143.255, sauf 54.240.143.188). Toutes les autres opérations seront refusées et toutes les demandes en dehors de la plage IP seront refusées.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Exemple : autoriser l'accès complet à un bucket exclusivement par un utilisateur fédéré spécifié

Dans cet exemple, l'utilisateur fédéré Alex est autorisé à accéder pleinement au `examplebucket` seau et ses objets. Tous les autres utilisateurs, y compris « root », se voient explicitement refuser toutes les opérations. Notez cependant que « root » ne se voit jamais refuser les autorisations pour Put/Get/DeleteBucketPolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemple : autorisation PutOverwriteObject

Dans cet exemple, le `Deny` L'effet pour PutOverwriteObject et DeleteObject garantit que personne ne peut écraser ou supprimer les données de l'objet, les métadonnées définies par l'utilisateur et le balisage de l'objet S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Exemples de stratégies de groupe

Utilisez les exemples de cette section pour créer des politiques d'accès StorageGRID pour les groupes.

Les stratégies de groupe spécifient les autorisations d'accès pour le groupe auquel la stratégie est attachée. Il n'y a pas de `Principal` élément de la politique car il est implicite. Les stratégies de groupe sont configurées à l'aide du gestionnaire de locataires ou de l'API.

Exemple : définir une stratégie de groupe à l'aide de Tenant Manager

Lorsque vous ajoutez ou modifiez un groupe dans le gestionnaire de locataires, vous pouvez sélectionner une stratégie de groupe pour déterminer les autorisations d'accès S3 dont disposeront les membres de ce groupe. Voir "Créer des groupes pour un locataire S3" .

- **Pas d'accès S3** : option par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une stratégie de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root aura accès aux ressources S3 par défaut.
- **Accès en lecture seule** : les utilisateurs de ce groupe ont un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent répertorier les objets et lire les données, les métadonnées et les balises des objets. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe en lecture seule apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : les utilisateurs de ce groupe ont un accès complet aux ressources S3, y compris aux buckets. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe à accès complet apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Atténuation des ransomwares** : cet exemple de politique s'applique à tous les compartiments de ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement les objets des buckets pour lesquels le contrôle de version des objets est activé.

  Les utilisateurs de Tenant Manager qui disposent de l'autorisation Gérer tous les compartiments peuvent remplacer cette stratégie de groupe. Limitez l'autorisation Gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA) lorsqu'elle est disponible.

- **Personnalisé** : les utilisateurs du groupe bénéficient des autorisations que vous spécifiez dans la zone de texte.

Exemple : autoriser le groupe à accéder à tous les compartiments

Dans cet exemple, tous les membres du groupe sont autorisés à accéder pleinement à tous les compartiments appartenant au compte locataire, sauf si cela est explicitement refusé par la politique de compartiment.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemple : autoriser l'accès en lecture seule du groupe à tous les compartiments

Dans cet exemple, tous les membres du groupe ont un accès en lecture seule aux ressources S3, sauf si cela est explicitement refusé par la politique de bucket. Par exemple, les utilisateurs de ce groupe peuvent répertorier les objets et lire les données d'objet, les métadonnées et les balises.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemple : autoriser les membres du groupe à accéder pleinement à leur « dossier » dans un compartiment

Dans cet exemple, les membres du groupe sont uniquement autorisés à répertorier et à accéder à leur dossier spécifique (préfixe de clé) dans le compartiment spécifié. Notez que les autorisations d'accès provenant d'autres stratégies de groupe et de la stratégie de compartiment doivent être prises en compte lors de la détermination de la confidentialité de ces dossiers.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```