Règles d'accès au compartiment et au groupe

StorageGRID 11.7

NetApp
April 12, 2024

Sommaire

Règles d’accès au compartiment et au groupe

Utilisez les règles d’accès au compartiment et au groupe

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

Présentation de la stratégie d’accès

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

- **Les règles de compartiment**, qui sont configurées à l’aide de la stratégie DE compartiment, DE LA règle DE compartiment PUT et DES opérations de L’API S3 de la politique de compartiment. Les règles de compartiment sont liées aux compartiments. Elles sont donc configurées de façon à contrôler l’accès des utilisateurs du compte du propriétaire du compartiment ou d’autres comptes au compartiment et aux objets. Une politique de compartiment s’applique à un seul compartiment et peut-être à plusieurs groupes.
- **Stratégies de groupe**, qui sont configurées à l’aide du Gestionnaire de locataires ou de l’API de gestion des locataires. Les stratégies de groupe sont associées à un groupe du compte, de sorte qu’elles sont configurées de manière à 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 peut-être plusieurs compartiments.

> La priorité est la même entre les politiques de groupe et de compartiment.

Les règles de compartiment et de groupe StorageGRID respectent une grammaire spécifique définie par Amazon. À l’intérieur de chaque règle se trouve un ensemble d’énoncés de politique, et chaque instruction contient les éléments suivants :

- ID de déclaration (ID) (facultatif)
- Effet
- Principal/notPrincipal
- Ressource/NotResource
- Action/NotAction
- Condition (en option)

Les instructions de règles sont créées à l’aide de cette structure pour spécifier les autorisations : accorder <effet> pour autoriser/refuser <principal> d’exécuter <action> sur <ressource> lorsque <condition> s’applique.

Chaque élément de règle est utilisé pour une fonction spécifique :

Elément	Description
SID	L’élément Sid est facultatif. Le SID n’est destiné qu’à la description de l’utilisateur. Il est stocké mais non interprété par le système StorageGRID.

Elément	Description
Effet	Utilisez l'élément d'effet pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) les compartiments ou les objets à l'aide des mots clés action Element pris en charge.
Principal/notPrincipal	Vous pouvez autoriser les utilisateurs, groupes et 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 peut accéder aux ressources qui lui sont propres. Il vous suffit de spécifier l'élément principal dans une stratégie de rubrique. Pour les stratégies de groupe, le groupe auquel la stratégie est associée est l'élément principal implicite.
Ressource/NotResource	L'élément ressource identifie les compartiments et les objets. Vous pouvez autoriser ou refuser des autorisations pour les compartiments et les objets en utilisant le nom de ressource Amazon (ARN) pour identifier la ressource.
Action/NotAction	Les éléments action et effet sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à la ressource est accordé ou refusé. L'accès est refusé sauf si vous attribuez des autorisations spécifiques, mais vous pouvez utiliser le refus explicite pour remplacer une autorisation accordée par une autre stratégie.
Condition	L'élément condition est facultatif. Les conditions vous permettent de créer des expressions pour déterminer quand une stratégie 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 à des 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 caractères ou plus, le point d'interrogation (?) correspond à n'importe quel caractère.

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

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

Dans l'exemple suivant, l'instruction utilise les éléments effet, principal, action et ressource. Cet exemple

montre une instruction de stratégie de compartiment complète qui utilise l'effet « Autoriser » pour donner les responsables, le groupe admin `federated-group/admin` et le groupe financier `federated-group/finance`, Autorisations d'exécution de l'action `s3:ListBucket` sur le compartiment nommé `mybucket` Et l'action `s3:GetObject` sur tous les objets à l'intérieur de ce godet.

```
{
  "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:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

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

Paramètres de contrôle de cohérence des règles

Par défaut, toutes les mises à jour apportées aux stratégies de groupe sont cohérentes. Une fois la stratégie de groupe cohérente, les modifications peuvent prendre 15 minutes supplémentaires à appliquer en raison de la mise en cache des règles. Par défaut, toutes les mises à jour effectuées sur les règles de compartiment sont également cohérentes en définitive.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour des règles de compartiment. Par exemple, il peut être intéressant de vouloir modifier cette règle afin qu'elle devienne effective dès que possible pour des raisons de sécurité.

Dans ce cas, vous pouvez définir le `Consistency-Control` L'en-tête de la demande de stratégie PUT Bucket ou vous pouvez utiliser la demande DE cohérence PUT Bucket. Lorsque vous modifiez le contrôle de cohérence pour cette demande, vous devez utiliser la valeur **All**, qui fournit la garantie la plus élevée de cohérence de lecture après écriture. Si vous spécifiez une autre valeur de contrôle de cohérence dans un en-tête pour la demande DE cohérence PUT Bucket, la demande sera rejetée. Si vous spécifiez une autre valeur pour une demande de stratégie PUT Bucket, la valeur sera ignorée. Une fois la règle de compartiment cohérente, les modifications peuvent prendre 8 secondes supplémentaires pour effet, grâce à la mise en cache des règles.

Si vous définissez le niveau de cohérence sur **All** pour forcer une nouvelle stratégie de godet à devenir efficace plus tôt, veillez à remettre le contrôle au niveau du godet à sa valeur d'origine lorsque vous avez terminé. Sinon, toutes les futures demandes de rubrique utiliseront le paramètre **tous**.

Utilisez ARN dans les énoncés de politique

Dans les instructions de politique, le ARN est utilisé dans les éléments principal et ressource.

- Utilisez cette syntaxe pour spécifier la ressource S3 ARN :

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

- Utilisez cette syntaxe pour spécifier la ressource d'identité ARN (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 correspondre à zéro ou plus de caractères dans 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 de séquences d'échappement JSON \u. Le codage pourcentage n'est pas pris en charge.

  "Syntaxe RFC 2141 URN"

  Le corps de requête HTTP pour l'opération de stratégie PUT Bucket doit être codé avec charset=UTF-8.

Spécifiez les ressources dans une stratégie

Dans les instructions de stratégie, vous pouvez utiliser l'élément ressource pour spécifier le compartiment ou l'objet pour lequel les autorisations sont autorisées ou refusées.

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

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

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

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

- La valeur de ressource peut spécifier un compartiment qui n'existe pas encore lorsqu'une stratégie de groupe est créée.

Spécifiez les entités de gestion dans une stratégie

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

- Chaque énoncé de politique dans une politique de rubrique doit inclure un élément principal. Les énoncés de politique dans une stratégie de groupe n'ont pas besoin de l'élément principal car le groupe est considéré comme le principal.
- Dans une politique, les principes sont indiqués par l'élément « principal » ou « notprincipal » pour exclusion.
- Les identités basées sur les comptes doivent être spécifiées à l'aide d'un ID ou d'un ARN :

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

- Dans cet exemple, le compte locataire utilise l'ID 27233906934684427525, qui inclut le compte root 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 (« gestionnaires ») :

```
"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 que Alex quitte l'entreprise et le nom d'utilisateur `Alex` est supprimé. Si un nouveau Alex rejoint l'organisation et est affecté de la même façon `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.

Spécifiez les autorisations dans une stratégie

Dans une stratégie, 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 stratégie, qui sont désignées par l'élément « action » ou par « NotAction » pour exclusion. Chacun de ces éléments est associé à des opérations spécifiques d'API REST S3.

Le tableau répertorie les autorisations qui s'appliquent aux compartiments et aux autorisations qui s'appliquent aux objets.

> Amazon S3 utilise désormais l'autorisation s3:PutReplicationConfiguration pour les opérations de réplication de compartiments PUT et DELETE. StorageGRID utilise des autorisations distinctes pour chaque action, qui correspond à la spécification Amazon S3 d'origine.

> Une SUPPRESSION est effectuée lorsqu'un PUT est utilisé pour remplacer une valeur existante.

Autorisations qui s'appliquent aux compartiments

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:CreateBucket	PLACER le godet	
s3:DeleteBucket	SUPPRIMER le compartiment	
s3:DeleteBuckeMetadatanotification	SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Oui.
s3:DeleteBucketPolicy	SUPPRIMER la règle de compartiment	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:DeleteReplicationConfiguration	SUPPRIMER la réplication du compartiment	Oui, séparer les autorisations pour PUT et DELETE*
s3:GetBucketAcl	OBTENIR l'ACL du compartiment	
s3:GetBuckeCompliance	GARANTIR la conformité des compartiments (obsolète)	Oui.
s3:persistance GetBucketConsistency	OPTIMISEZ la cohérence des compartiments	Oui.
s3:GetBucketCORS	OBTENIR les godets	
s3:GetEncryptionConfiguration	CHIFFREMENT des compartiments	
s3:GetBucketLastAccessTime	HEURE du dernier accès au compartiment	Oui.
s3:GetBucketLocation	ACCÉDER à l'emplacement du compartiment	
s3:GetBucketMetadatanotification	CONFIGURATION DES notifications de métadonnées de compartiment	Oui.
s3:GetBuckenotification	GET Bucket notification	
s3:GetBuckeObjectLockConfiguration	OBTENIR la configuration de verrouillage d'objet	
s3:GetBucketPolicy	GET Bucket policy	
s3:GetBucketTagging	GET Bucket tagging	
s3:GetBucketVersioning	GESTION des versions des compartiments	
s3:GetLifecyclConfiguration	OPTIMISEZ le cycle de vie des compartiments	
s3:GetReplicationTM	RÉPLICATION des compartiments	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:ListAllMyseaux	• ACCÉDER au service • DÉCOUVREZ l'utilisation du stockage	Oui, pour BÉNÉFICIER DE l'utilisation DU stockage
s3:ListBucket	• OBTENIR le compartiment (liste d'objets) • Godet DE TÊTE • Restauration POST-objet	
s3:ListBuckMultipartUploads	• Liste des téléchargements partitionnés • Restauration POST-objet	
s3:ListBuckeVersions	OBTENIR les versions de compartiment	
s3:PutBuckeCompliance	MISE en conformité des compartiments (obsolète)	Oui.
s3:persistance de PutBuckeConsistency	PRÉSERVER la cohérence du godet	Oui.
s3:PutBuckeCORS	• SUPPRIMER les godets† • PLACEZ les godets	
s3:PutEncryptionConfiguration	• SUPPRIMER le chiffrement du compartiment • PUT Bucket Encryption	
s3:PutBuckeLastAccessTime	METTRE l'heure du dernier accès au compartiment	Oui.
s3:PutBuckeMetadanotification	CONFIGURATION de notification des métadonnées de compartiment	Oui.
s3:PutBuckenotification	PUT Bucket notification	
s3:PutBuckObjectLockConfiguration	• PLACEZ le godet avec le `x-amz-bucket-object-lock-enabled: true` En-tête de demande (nécessite également l'autorisation s3:CreateBucket) • CONFIGURATION du verrouillage de l'objet	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutBuckePolicy	PUT Bucket policy	
s3:PutBuckeTagging	• SUPPRIMER le marquage du compartiment† • PUT Bucket tagging	
s3:PutBuckeVersioning	GESTION des versions du compartiment	
s3:PutLifecyclConfiguration	• SUPPRIMER le cycle de vie du godet† • CYCLE de vie des compartiments	
s3:PutReplicationTM	RÉPLICATION des compartiments	Oui, séparer les autorisations pour PUT et DELETE*

Autorisations qui s'appliquent aux objets

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:AbortMultipartUpload	• Abandonner le téléchargement de pièces multiples • Restauration POST-objet	
s3:BipassGovernanceRetention	• SUPPRIMER l'objet • SUPPRIMER plusieurs objets • CONSERVATION des objets	
s3:DeleteObject	• SUPPRIMER l'objet • SUPPRIMER plusieurs objets • Restauration POST-objet	
s3:DeleteObjectTagging	SUPPRIMER le balisage d'objets	
s3:DeleteObjectVersionTagging	SUPPRIMER le balisage d'objets (une version spécifique de l'objet)	
s3:DeleteObjectVersion	SUPPRIMER l'objet (une version spécifique de l'objet)	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:GetObject	• OBTENIR l'objet • Objet TÊTE • Restauration POST-objet • SÉLECTIONNEZ contenu de l'objet	
s3:GetObjectAcl	OBTENIR l'ACL d'objet	
s3:GetObjectLegalHold	OBTENIR la mise en attente légale de l'objet	
s3:GetObjectRetention	OBTENIR la conservation des objets	
s3:GetObjectTagging	OBTENIR le balisage d'objets	
s3:GetObjectVersionTagging	OBTENIR le balisage d'objets (une version spécifique de l'objet)	
s3:GetObjectVersion	OBTENIR objet (une version spécifique de l'objet)	
s3:ListMultipartUploadParts	Répertorier les pièces, POST-restauration d'objet	
s3:PutObject	• PLACER l'objet • PLACER l'objet - Copier • Restauration POST-objet • Lancer le téléchargement de pièces multiples • Chargement de pièces multiples complet • Télécharger la pièce • Télécharger la pièce - Copier	
s3:PutObjectLegalHold	METTRE l'objet en attente légale	
s3:PutObjectRetention	CONSERVATION des objets	
s3:PutObjectTagging	PLACER le balisage d'objets	
s3:PutObjectVersionTagging	PUT Object Tagging (une version spécifique de l'objet)	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutOverwriteObject	• PLACER l'objet • PLACER l'objet - Copier • PUT Object tagging • SUPPRIMER le balisage d'objets • Chargement de pièces multiples complet	Oui.
s3:RestoreObject	Restauration POST-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 remplacer les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'objets S3.

Les paramètres possibles pour cette autorisation sont les suivants :

- **Autoriser** : le client peut écraser un objet. Il s'agit du paramètre par défaut.
- **Deny** : le client ne peut pas écraser un objet. Lorsque cette option est définie sur Deny, l'autorisation PutOverwriteObject fonctionne comme suit :
  - Si un objet existant se trouve sur le même chemin :
    - Les données de l'objet, les métadonnées définies par l'utilisateur ou le balisage d'objets S3 ne peuvent pas être remplacés.
    - Toutes les opérations d'entrée en cours sont annulées et une erreur est renvoyée.
    - Si la gestion des versions S3 est activée, le paramètre Deny empêche les opérations PUT Object tagging ou DELETE Object tagging 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 autorisation a été définie.

> Si la règle 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'objet. En outre, si la case **empêcher la modification du client** est cochée (**CONFIGURATION** > **Paramètres de sécurité** > **réseau et objets**), ce paramètre remplace le paramètre de l'autorisation PutOverwriteObject.

Spécifiez les conditions dans une stratégie

Les conditions définissent le moment où une police sera en vigueur. Les conditions sont constituées d'opérateurs et de paires de clé-valeur.

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

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

Dans l'exemple suivant, la condition ipaddress utilise la clé 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
- Valeur numérique
- Booléen
- Adresse IP
- Vérification nulle

Opérateurs de condition	Description
Equals à jambes de chaîne	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse).
Equals stringNotEquals	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse).
StringEqualisIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance exacte (ignore case).
StringNotEqualisIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance nérée (ignore le cas).
StringLike	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse). Peut inclure * et ? caractères génériques.
StringNotLike	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse). Peut inclure * et ? caractères génériques.

Opérateurs de condition	Description
Valeurs numériques	Compare une touche à une valeur numérique en fonction de la correspondance exacte.
NumericNotEquals	Compare une touche à une valeur numérique basée sur la correspondance annulée.
NumericGreaterThan	Compare une clé à une valeur numérique basée sur la comparaison « supérieure à ».
NumericGreaterThanEquals	Compare une clé à une valeur numérique basée sur la comparaison « supérieure ou égale ».
NumericLessThan	Compare une clé à une valeur numérique basée sur la comparaison « moins que ».
NumericLessThanEquals	Compare une clé à une valeur numérique basée sur la comparaison « inférieure à ou égale ».
BOOL	Compare une clé à une valeur booléenne basée sur la correspondance « vrai ou faux ».
Adresse IP	Compare une clé à une adresse IP ou une plage d'adresses IP.
Adresse de la note	Compare une clé à une adresse IP ou une plage d'adresses IP basée sur la correspondance annulée.
Nul	Vérifie si une clé condition est présente dans le contexte de demande actuel.

Touches de condition prises en charge

Catégorie	Touches de condition applicables	Description
Opérateurs IP	aws:SourceIp	Compare à l'adresse IP à partir de laquelle la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet. **Remarque :** si la requête S3 a été envoyée via le service Load Balancer sur les nœuds Admin et les passerelles, cela se compare à l'adresse IP en amont du service Load Balancer. **Remarque** : si un équilibreur de charge tiers non transparent est utilisé, il sera comparé à l'adresse IP de cet équilibreur de charge. Toutes `X-Forwarded-For` l'en-tête sera ignoré car sa validité ne peut pas être établie.
Ressource/identité	aws:nom d'utilisateur	Compare le nom d'utilisateur de l'expéditeur à partir duquel la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet.
s3:ListBucket et s3:permissions ListBuckeVersions	s3:délimiteur	Compare avec le paramètre de délimiteur spécifié dans une demande GET Bucket ou GET Bucket Object versions.
s3:ListBucket et s3:permissions ListBuckeVersions	s3:touches max	Compare au paramètre max-keys spécifié dans une demande GET Bucket ou GET Bucket Object versions.
s3:ListBucket et s3:permissions ListBuckeVersions	s3:préfixe	Compare au paramètre de préfixe spécifié dans une demande GET Bucket ou GET Bucket Object versions.
s3:PutObject	s3 :conservation des jours restants avec un verrouillage objet	Compare à la date de conservation spécifiée dans le `x-amz-object-lock-retain-until-date` demander l'en-tête ou calculé à partir de la période de rétention par défaut du compartiment pour s'assurer que ces valeurs se situent dans la plage autorisée pour les demandes suivantes : • PLACER l'objet • PLACER l'objet - Copier • Lancer le téléchargement de pièces multiples

Catégorie	Touches de condition applicables	Description
s3:PutObjectRetention	s3 :conservation des jours restants avec un verrouillage objet	Compare à la date de conservation spécifiée dans la demande DE conservation D'objet PUT pour s'assurer qu'elle se trouve dans la plage autorisée.

Spécifiez les variables d'une règle

Vous pouvez utiliser des variables dans les règles pour remplir les informations relatives aux règles lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de règle dans le `Resource` comparaisons d'éléments et de chaînes dans `Condition` elément.

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 condition :

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

Variable	Description
`${aws:SourceIp}`	Utilise la touche SourceIp comme variable fournie.
`${aws:username}`	Utilise la clé de nom d'utilisateur comme variable fournie.
`${s3:prefix}`	Utilise la clé de préfixe spécifique au service comme variable fournie.
`${s3:max-keys}`	Utilise la touche max-keys spécifique au service comme variable fournie.
`${*}`	Caractère spécial. Utilise le caractère comme caractère littéral *.
`${?}`	Caractère spécial. Utilise le caractère comme littéral ? caractère.
`${$}`	Caractère spécial. Utilise le caractère comme caractère littéral $.

Créez des règles nécessitant une gestion spéciale

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

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Refusez vous-même toutes les autorisations sur le compte racine	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique
Refusez vous-même les autorisations d'accès à l'utilisateur/au groupe	Groupe	Valide et appliquée	Identique
Autoriser un groupe de comptes étrangers toute autorisation	Godet	Principal non valide	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle
Autoriser un utilisateur ou une racine de compte étranger à accorder toute autorisation	Godet	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle	Identique
Autoriser tout le monde à autoriser toutes les actions	Godet	Valide, mais les autorisations pour toutes les opérations de politique de compartiment S3 renvoient une erreur 405 méthode non autorisée pour la racine du compte étranger et les utilisateurs	Identique
Refuser les autorisations de tous pour toutes les actions	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Le principal est un utilisateur ou un groupe inexistant	Godet	Principal non valide	Valide
La ressource est un compartiment S3 inexistant	Groupe	Valide	Identique
Principal est un groupe local	Godet	Principal non valide	Valide
La police accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations pour METTRE des objets	Godet	Valide. Les objets sont détenus par le compte de créateur et la stratégie 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 d'objet.	Valide. Les objets sont la propriété du compte du propriétaire du compartiment. La politique de compartiment s'applique.

Protection WORM (Write-once, Read-many)

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

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

- Dans 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 suivantes et les règles S3 :
  - Ajoutez une opération DE REFUS PutOverwriteObject à la règle S3.
  - Ajoutez une opération DE REFUS DeleteObject à la règle S3.
  - Ajouter une opération D'AUTORISATION PLACER l'objet à la règle S3.

> La définition de DeleteObject sur DENY dans une politique 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 contre)

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

Situation B: Remplacements séquentiels terminés (protégés contre)

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

Informations associées

- "Gestion des objets par les règles StorageGRID ILM"
- "Exemples de politiques de compartiments"
- "Exemples de stratégies de groupe"
- "Gestion des objets avec ILM"
- "Utilisez un compte de locataire"

Exemples de politiques de compartiments

Utilisez les exemples de cette section pour créer des règles d'accès StorageGRID pour les compartiments.

Les politiques de compartiment spécifient les autorisations d'accès pour le compartiment à lequel la politique est attachée. Les règles de compartiment sont configurées à l'aide de l'API S3 PutBuckPolicy. Voir "Opérations sur les compartiments".

Il est possible de configurer une politique de compartiment à l'aide de l'interface de ligne de commandes AWS, comme indiqué dans la commande suivante :

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

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

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à lister les objets dans le compartiment et à effectuer des opérations get Object sur tous les objets du compartiment. 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, ne peut écrire dans le compartiment.

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

Exemple : autoriser l'accès complet de tous les utilisateurs d'un compte et permettre à chacun d'un autre compte d'accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde d'un compte spécifié peut accéder intégralement à un compartiment, tandis que les utilisateurs d'un autre compte spécifié ne sont autorisés qu'à répertorier le compartiment et effectuer des opérations GetObject sur les objets du compartiment en commençant par le `shared/` préfixe de clé d'objet.

> Dans StorageGRID, les objets créés par un compte autre que le propriétaire (y compris les comptes anonymes) sont détenus par le compte du propriétaire du compartiment. La politique de compartiment 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 accéder entièrement au groupe spécifié

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer des opérations GET Object sur tous les objets du compartiment, tandis que seuls les utilisateurs appartenant au groupe `Marketing` le compte spécifié est autorisé à accéder pleinement.

```
{
  "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 lire et à écrire l'accès à un compartiment si le client se trouve dans la plage IP

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer toutes les opérations objet sur tous les objets du compartiment, à condition que les demandes proviennent d'une plage 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 un accès complet à un compartiment exclusivement par un utilisateur fédéré spécifié

Dans cet exemple, l'utilisateur fédéré Alex est autorisé à accéder pleinement au `examplebucket` le godet et ses objets. Tous les autres utilisateurs, y compris « root », sont explicitement refusés à toutes les opérations. Notez toutefois que « root » n'est jamais refusé les autorisations de mettre/obtenir/DeleteBuckePolicy.

```
{
  "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` 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 d'objets 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 stratégies d'accès StorageGRID pour les groupes.

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

Exemple : définissez la stratégie de groupe à l'aide du Gestionnaire de locataires

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 les membres de ce groupe auront accès. Voir "Créez 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 règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
- **Accès en lecture seule** : les utilisateurs de ce groupe ont accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : les utilisateurs de ce groupe ont accès aux ressources S3, y compris aux compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Atténuation des ransomware** : cet exemple de politique s'applique à tous les compartiments pour ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels la gestion des versions d'objet est activée.

  Les utilisateurs du Gestionnaire de locataires disposant 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), le cas échéant.

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

Exemple : autoriser l'accès complet du groupe à toutes les rubriques

Dans cet exemple, tous les membres du groupe sont autorisés à accéder à tous les compartiments appartenant au compte du locataire, sauf s'ils sont explicitement refusés 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, à moins qu'ils ne soient explicitement refusés par la règle de compartiment. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des 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 : permettre aux membres du groupe d'accéder pleinement à leur « dossier » uniquement dans un compartiment

Dans cet exemple, les membres du groupe ne sont autorisés qu'à répertorier et accéder à leur dossier spécifique (préfixe de clé) dans le compartiment spécifié. Notez que les autorisations d'accès à partir d'autres stratégies de groupes et de la règle 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}/*"
    }
  ]
}
```

Informations sur le copyright

Informations sur les marques commerciales