Contraintes relatives aux règles d'administration pour Cloud Storage

Cette page fournit des informations supplémentaires sur les contraintes liées aux règles d'administration (/resource-manager/docs/organization-policy/overview) qui s'appliquent à Cloud Storage. Utilisez des contraintes pour appliquer des comportements de bucket et d'objet dans l'ensemble d'un projet ou d'une organisation.

Contraintes Cloud Storage

Les contraintes suivantes peuvent être appliquées à une règle d'administration et concernent Cloud Storage :

Appliquer la protection contre l'accès public

Nom de l'API : `constraints/storage.publicAccessPrevention`

Lorsque vous appliquez la contrainte `publicAccessPrevention` d'une ressource, l'accès public est limité (/storage/docs/public-access-prevention#enforced) pour tous les buckets et objets, nouveaux ou existants, inclus dans cette ressource.

Notez que l'activation ou la désactivation de `publicAccessPrevention` peut prendre jusqu'à 10 minutes.

Durée de la règle de conservation en secondes

Nom de l'API : `constraints/storage.retentionPolicySeconds`

Lorsque vous appliquez la contrainte `retentionPolicySeconds`, vous spécifiez une ou plusieurs durées dans le cadre de la contrainte. Une fois définies, les règles de conservation (/storage/docs/bucket-lock) du bucket doivent inclure l'une des durées spécifiées. La contrainte `retentionPolicySeconds` est requise lors de la création d'un bucket, ou lors de l'ajout ou de la mise à jour de la durée de conservation d'un bucket préexistant. Elle n'est pas requise pour les buckets préexistants.

Si vous définissez plusieurs contraintes `retentionPolicySeconds` pour différents niveaux de

ressources, elles sont appliquées de manière hiérarchique (/resource-manager/docs/organization-policy/understanding-hierarchy#hierarchy_evaluation_rules). Pour cette raison, il est recommandé de définir le champ `inheritFromParent` sur `true`, ce qui garantit que les règles des niveaux supérieurs sont également prises en compte.

Exiger un accès uniforme au niveau du bucket

Nom de l'API : `constraints/storage.uniformBucketLevelAccess`

Lorsque vous appliquez la contrainte `uniformBucketLevelAccess`, les nouveaux buckets (/storage/docs/creating-buckets) doivent activer la fonctionnalité d'accès uniforme au niveau du bucket (/storage/docs/uniform-bucket-level-access), elle est activée pour les buckets préexistants et ne peut être désactivée. Les buckets préexistants pour lesquels l'accès uniforme au niveau du bucket est désactivé ne sont pas nécessaires à son activation.

Mode de journalisation d'audit détaillé

Nom de l'API : `constraints/gcp.detailedAuditLoggingMode`

Lorsque vous appliquez la contrainte `detailedAuditLoggingMode`, les journaux d'audit Cloud associés aux opérations Cloud Storage (/storage/docs/audit-logging) contiennent des informations détaillées sur les requêtes et les réponses. Il est recommandé d'utiliser cette contrainte conjointement avec le verrou de bucket (/storage/docs/bucket-lock) lorsque vous recherchez différentes conformités (/security/compliance/sec-us), telles que les règles SEC 17a-4(f), CFTC 1.31(c)-(d) et FINRA 4511(c).

Les informations consignées incluent les paramètres de requête, les paramètres de chemin d'accès et les paramètres du corps de la requête. Les journaux excluent certaines parties des requêtes et des réponses associées à des informations sensibles. Par exemple, les journaux excluent :

- Les identifiants, tels que `Authorization`, `X-Goog-Signature` ou `upload-id` ;
- Les informations sur la clé de chiffrement, par exemple `x-goog-encryption-key` ;
- Les données d'objet brutes.

Lorsque vous utilisez cette contrainte, tenez compte des points suivants :

- Les informations détaillées sur les requêtes et les réponses ne sont pas garanties. Dans de rares cas, des journaux vides peuvent être renvoyés.

- L'activation de `detailedAuditLoggingMode` augmente la quantité de données stockées dans les journaux d'audit, ce qui peut affecter votre facturation Cloud Logging (/stackdriver/pricing#logging-costs) pour les journaux d'accès aux données.
- L'activation ou la désactivation de `detailedAuditLoggingMode` prend jusqu'à 10 minutes.
- Les requêtes et les réponses consignées sont enregistrées dans un format générique correspondant aux noms de champ de l'API JSON.

Restreindre les types d'authentification

Nom de l'API : `constraints/storage.restrictAuthTypes`

Lorsque vous appliquez la contrainte `restrictAuthTypes`, les requêtes d'accès aux ressources Cloud Storage utilisant le type d'authentification restreint échouent, quelle que soit la validité de la requête. Cette contrainte est recommandée lorsque vous devez répondre à des exigences réglementaires ou renforcer la sécurité de vos données.

Remarque : Actuellement, cette contrainte ne peut être utilisée que pour restreindre les clés HMAC (/storage/docs/authentication/hmackeys).

Les types d'authentification suivants peuvent être restreints :

- `USER_ACCOUNT_HMAC_SIGNED_REQUESTS` : restreint les requêtes signées (/storage/docs/authentication/signatures#signing-process) par des clés HMAC de compte utilisateur.
- `SERVICE_ACCOUNT_HMAC_SIGNED_REQUESTS` : restreint les requêtes signées par des clés HMAC de compte de service.
- `in:ALL_HMAC_SIGNED_REQUESTS` : restreint les requêtes signées par des clés HMAC de compte utilisateur ou de compte de service. Si vous devez répondre à des exigences de souveraineté des données, nous vous recommandons de restreindre toutes les requêtes signées HMAC.

Lorsque vous activez cette contrainte, voici ce qui se produit :

- Cloud Storage restreint l'accès aux requêtes authentifiées avec le type d'authentification restreint. Les requêtes échouent avec l'erreur `403 Forbidden`.

.

- Les entités précédemment autorisées à effectuer la requête reçoivent un message d'erreur indiquant que le type d'authentification est désactivé.
- Si les clés HMAC sont restreintes :
  - Les clés HMAC de type restreint ne peuvent plus être créées ni activées dans la ressource sur laquelle la contrainte est appliquée. Les requêtes de création ou d'activation de clés HMAC échouent avec l'erreur `403 Forbidden`.
  - Les clés HMAC existantes restent, mais ne sont plus utilisables. Elles peuvent être désactivées ou supprimées, mais ne peuvent pas être réactivées.

Lorsque vous utilisez la contrainte `restrictAuthTypes`, tenez compte des ressources existantes qui dépendent de l'authentification HMAC. Par exemple, si vous avez migré depuis Amazon Simple Storage Service (Amazon S3), votre application utilise probablement des clés HMAC pour authentifier les requêtes adressées à Cloud Storage. Vous pouvez utiliser la métrique Cloud Monitoring `storage.googleapis.com/authn/authentication_count` pour savoir combien de fois les clés HMAC ont été utilisées pour authentifier les requêtes.

Exiger l'utilisation de clés de chiffrement gérées par le client (CMEK)

Nom de l'API : `constraints/gcp.restrictNonCmekServices`

Lorsque vous appliquez la contrainte `restrictNonCmekServices`, vous définissez les services dont les ressources nécessitent l'utilisation de clés de chiffrement gérées par le client (/storage/docs/encryption/customer-managed-keys). Vous pouvez appliquer cette contrainte aux objets ou aux buckets Cloud Storage en ajoutant `storage.googleapis.com` à la liste des services limités avec la contrainte définie sur `Deny`. S'ils sont soumis à la contrainte, les objets Cloud Storage doivent être écrits à l'aide d'une clé Cloud KMS, qui est soit spécifiée dans la requête (/storage/docs/encryption/using-customer-managed-keys#add-object-key), soit définie comme clé de chiffrement par défaut (/storage/docs/encryption/using-customer-managed-keys#set-default-key) pour le bucket de destination. Une clé Cloud KMS doit être définie sur les buckets Cloud Storage en tant que clé de chiffrement par défaut.

Si vous tentez d'écrire un objet ou de créer un bucket non chiffré par une clé Cloud KMS, vous recevez le message d'erreur suivant: "Une clé de chiffrement gérée par le client (CMEK) est requise par une règle d'administration en vigueur. Définissez une CMEK par défaut sur le bucket ou spécifiez une CMEK dans votre requête."

Lorsque vous utilisez cette contrainte, tenez compte des points suivants :

- L'activation de `restrictNonCmekServices` peut entraîner des modifications importantes si vous écrivez dans un bucket sans clé Cloud KMS par défaut ou si vous excluez une clé Cloud KMS dans votre requête.
- Les buckets existants qui ne possèdent pas de clé Cloud KMS par défaut ne sont pas affectés par la contrainte. Toutefois, si vous définissez une clé Cloud KMS sur un bucket existant avec la contrainte activée, ce bucket devient soumis à la contrainte.
- Les objets existants chiffrés à l'aide de clés de chiffrement gérées par Google (/storage/docs/encryption/default-keys) ou de clés de chiffrement fournies par le client (/storage/docs/encryption/customer-supplied-keys) ne sont pas soumis à cette contrainte. Les futures réécritures de ces objets sont toutefois soumises à la contrainte.
- La prise en compte des modifications apportées à `constraints/gcp.restrictNonCmekServices` peut prendre jusqu'à 10 minutes.

Pour en savoir plus sur cette contrainte, consultez la section Règles d'administration des CMEK (/kms/docs/cmek-org-policy).

Restreindre les projets à l'aide d'une clé de chiffrement gérée par le client valide (CMEK)

Nom de l'API : `constraints/gcp.restrictCmekCryptoKeyProjects`

Lorsque vous appliquez la contrainte `restrictCmekCryptoKeyProjects`, vous définissez les projets depuis lesquels une clé Cloud KMS (/storage/docs/encryption/customer-managed-keys) peut être utilisée dans les requêtes. Lorsque vous appliquez cette contrainte :

- Toute clé Cloud KMS spécifiée dans une requête doit provenir d'un projet autorisé par la règle d'administration.
- Si vous créez un nouveau bucket, toute clé Cloud KMS que vous définissez sur le bucket doit provenir d'un projet autorisé.
- Les écritures et les mises à jour d'objets échouent pour les buckets existants disposant d'une clé Cloud KMS non valide. Vous devez remplacer la clé Cloud KMS par défaut du bucket par une clé provenant d'un projet autorisé ou supprimer ce service du bucket. Notez que vous ne pouvez pas supprimer une clé Cloud KMS d'un bucket lorsque la contrainte `restrictNonCmekServices` est activée.

Si vous essayez de spécifier une clé Cloud KMS dans une requête qui ne provient pas d'un projet autorisé, vous recevez le message d'erreur suivant : "La clé spécifiée ne peut pas être utilisée car son projet est restreint par une règle d'administration. Veuillez réessayer avec une clé de chiffrement gérée par le client (CMEK) provenant d'un projet autorisé."

Si vous tentez d'écrire des données dans un bucket à l'aide d'une clé Cloud KMS qui ne provient pas d'un projet autorisé, le message d'erreur suivant s'affiche : "Le bucket utilise une clé par défaut à partir d'un projet restreint par une règle d'administration en vigueur. Veuillez définir une clé de chiffrement gérée par le client (CMEK) autorisée comme valeur par défaut pour le bucket ou spécifier une CMEK autorisée dans votre requête."

Lorsque vous utilisez cette contrainte, tenez compte des points suivants :

- Les objets existants ne sont pas soumis à cette contrainte.
- Cette contrainte seule n'impose pas l'utilisation de clés de chiffrement gérées par le client à partir de projets autorisés. Pour imposer l'utilisation de clés de chiffrement gérées par le client à partir de projets autorisés, vous devez appliquer les contraintes `constraints/gcp.restrictNonCmekServices` et `constraints/gcp.restrictCmekCryptoKeyProjects`.
- La prise en compte des modifications apportées à `constraints/gcp.restrictCmekCryptoKeyProjects` peut prendre jusqu'à 10 minutes.

Pour en savoir plus sur cette contrainte, consultez la section Règles d'administration des CMEK (/kms/docs/cmek-org-policy).

Étapes suivantes

- Découvrez la hiérarchie des ressources (/resource-manager/docs/cloud-platform-resource-hierarchy#resource-hierarchy-detail) qui s'applique aux règles d'administration.
- Pour savoir comment utiliser les contraintes et les règles d'administration dans Google Cloud Console, consultez la page Créer et gérer des règles d'administration (/resource-manager/docs/organization-policy/creating-managing-policies).
- Pour savoir comment utiliser les contraintes et les règles d'administration dans gcloud, consultez la page Utiliser des contraintes (/resource-manager/docs/organization-policy/using-constraints).

- Consultez la documentation de référence (/resource-manager/reference/rest) sur l'API Resource Manager pour connaître les méthodes d'API pertinentes, telles que `projects.setOrgPolicy` (/resource-manager/reference/rest/v1/projects/setOrgPolicy).

Last updated 2022-08-29 UTC.