Offrez un accès client S3 aux données NAS

ONTAP 9

NetApp
April 24, 2024

Sommaire

Offrez un accès client S3 aux données NAS 1
Présentation multiprotocole S3 1
Exigences de données NAS pour l’accès des clients S3 3
Activez l’accès au protocole S3 aux données NAS 4
Créez un compartiment NAS S3 6
Activez les utilisateurs client S3 7

Offrez un accès client S3 aux données NAS

Présentation multiprotocole S3

Depuis ONTAP 9.12.1, vous pouvez activer les clients exécutant le protocole S3 pour accéder aux données qui sont servies aux clients qui utilisent les protocoles NFS et SMB sans nouveau formatage. Ainsi, les données NAS peuvent continuer à être servies aux clients NAS, tout en présentant les données d'objet aux clients S3 qui exécutent des applications S3 (par exemple, le data mining et l'intelligence artificielle).

La fonctionnalité multiprotocole S3 répond à deux cas d'utilisation :

1. Accès aux données NAS existantes à l'aide de clients S3

   Si vos données existantes ont été créées à l'aide de clients NAS classiques (NFS ou SMB) et sont situées sur des volumes NAS (volumes FlexVol ou FlexGroup), vous pouvez désormais utiliser les outils d'analytique des clients S3 pour accéder à ces données.

2. Stockage back-end pour les clients modernes capables d'exécuter des E/S avec les protocoles NAS et S3

   Vous pouvez désormais fournir un accès intégré pour des applications telles que Spark et Kafka qui peuvent lire et écrire les mêmes données à l'aide des protocoles NAS et S3.

Fonctionnement du protocole multiprotocole S3

ONTAP multiprotocole permet de présenter le même jeu de données que la hiérarchie de fichiers ou qu'en tant qu'objets dans un compartiment. Pour ce faire, ONTAP crée des « compartiments NAS S3 » qui permettent aux clients S3 de créer, lire, supprimer et énumérer des fichiers dans le stockage NAS à l'aide de requêtes d'objets S3. Ce mappage est conforme à la configuration de sécurité NAS, en observant les autorisations d'accès aux fichiers et aux répertoires ainsi qu'en écrivant dans la piste d'audit de sécurité si nécessaire.

Ce mappage est effectué en présentant une hiérarchie de répertoires NAS spécifiée comme un compartiment S3. Chaque fichier de la hiérarchie de répertoires est représenté comme un objet S3 dont le nom est relatif à partir du répertoire mappé vers le bas, avec des limites de répertoire représentées par le caractère de barre oblique ('/').

Les utilisateurs standard de ONTAP-defined S3 peuvent accéder à ce stockage, conformément aux règles de compartiment définies pour le compartiment correspondant au répertoire NAS. Pour que cela soit possible, des mappages doivent être définis entre les utilisateurs S3 et SMB/NFS. Les informations d'identification de l'utilisateur SMB/NFS seront utilisées pour la vérification des autorisations NAS et incluses dans tous les enregistrements d'audit résultant de ces accès.

Lorsqu'un fichier est créé par des clients SMB ou NFS, il est immédiatement placé dans un répertoire, et donc visible aux clients, avant l'écriture des données. Les clients S3 s'attendent à une sémantique différente, où le nouvel objet n'est pas visible dans le namespace tant que toutes ses données n'ont pas été écrites. Le mappage de S3 sur le stockage NAS crée des fichiers avec la sémantique S3, afin de rendre les fichiers invisibles en externe jusqu'à la fin de la commande de création S3.

Protection des données par compartiments NAS S3

Les « compartiments » NAS S3 sont simplement des mappages des données NAS pour les clients S3, ils ne

sont pas des compartiments S3 standard. Par conséquent, il n'est pas nécessaire de protéger les compartiments NAS S3 à l'aide de la fonctionnalité NetApp S3 SnapMirror. À la place, vous pouvez protéger les volumes contenant des compartiments NAS S3 à l'aide de la réplication asynchrone de volume SnapMirror. SnapMirror synchrone et la reprise d'activité SVM ne sont pas pris en charge.

À partir de ONTAP 9.14.1, les compartiments NAS S3 sont pris en charge dans les agrégats en miroir et sans miroir pour les configurations MetroCluster IP et FC.

Découvrez "Réplication asynchrone SnapMirror".

Audit des compartiments NAS S3

Les compartiments NAS S3 ne sont pas des compartiments S3 classiques. L'audit S3 ne peut donc pas être configuré pour l'audit de l'accès. En savoir plus sur "Audit S3".

Cependant, les fichiers et les répertoires NAS mappés dans des compartiments NAS S3 peuvent être audités pour les événements d'accès à l'aide de procédures d'audit ONTAP conventionnelles. Les opérations S3 peuvent ainsi déclencher des événements d'audit NAS, à l'exception de ce qui suit :

- Si l'accès client S3 est refusé par la configuration de la règle S3 (groupe ou règle de compartiment), l'audit NAS pour l'événement n'est pas lancé. En effet, les autorisations S3 sont vérifiées avant la vérification des audits des SVM.
- Si le fichier cible d'une requête GET S3 est de taille 0, le contenu 0 est renvoyé à la demande GET et l'accès en lecture n'est pas consigné.
- Si le fichier cible d'une requête GET S3 se trouve dans un dossier pour lequel l'utilisateur n'a pas d'autorisation « traverse », la tentative d'accès échoue et l'événement n'est pas enregistré.

Découvrez "Audit des événements NAS sur les SVM".

Interopérabilité S3 et NAS

Sauf mention contraire, les compartiments NAS ONTAP S3 prennent en charge les fonctionnalités NAS standard et S3.

La fonctionnalité NAS n'est pas prise en charge par les compartiments NAS S3

Un niveau de capacité FabricPool

Les compartiments NAS S3 ne peuvent pas être configurés en tant que Tier de capacité pour FabricPool.

La fonctionnalité S3 n'est pas prise en charge par les compartiments NAS S3

Métadonnées d'utilisateur AWS

- Les paires de valeurs-clés reçues dans le cadre des métadonnées S3 ne sont pas stockées sur le disque avec les données d'objet dans la version actuelle.
- Les en-têtes de demande avec le préfixe "x-amz-META" sont ignorés.

Balises AWS

- Sur les demandes d'initialisation D'objet PUT et multipart, les en-têtes avec le préfixe "x-amz-tagging" sont ignorés.
- Les demandes de mise à jour des balises sur un fichier existant (c'est-à-dire une requête PUT, GET et Delete avec la chaîne de requête ?tagging) sont rejetées par une erreur.

Gestion des versions

Il n’est pas possible de spécifier la gestion des versions dans la configuration du mappage des compartiments.

- Les demandes qui incluent des spécifications de version non nulles (versionID=xyz query-string) reçoivent des réponses d’erreur.
- Les demandes visant à affecter l’état de gestion des versions d’un compartiment sont rejetées avec des erreurs.

Opérations en plusieurs parties

Les opérations suivantes ne sont pas prises en charge :

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- ListMultipartUpload

Exigences de données NAS pour l’accès des clients S3

Il est important de comprendre qu’il existe des incompatibilités inhérentes lors du mappage des fichiers NAS et des répertoires pour l’accès S3. Il peut être nécessaire d’ajuster la hiérarchie des fichiers NAS avant de les transférer à l’aide de compartiments NAS S3.

Un compartiment NAS S3 fournit un accès S3 à un répertoire NAS en effectuant le mappage de ce répertoire à l’aide de la syntaxe du compartiment S3, et les fichiers de l’arborescence sont considérés comme des objets. Les noms d’objet sont les chemins d’accès délimités par des barres obliques des fichiers par rapport au répertoire spécifié dans la configuration du compartiment S3.

Ce mappage impose une certaine exigence lorsque les fichiers et les répertoires sont gérés à l’aide de compartiments NAS S3 :

- Les noms S3 sont limités à 1024 octets. Les fichiers dont les chemins d’accès sont plus longs ne sont donc pas accessibles via S3.
- Les noms de fichiers et de répertoires sont limités à 255 caractères, de sorte qu’un nom d’objet ne peut pas comporter plus de 255 caractères consécutifs non-slash ('/')
- Un chemin SMB délimité par des caractères de barre oblique inverse («\') apparaîtra à s3 comme un nom d’objet contenant des caractères de barre oblique («/ »).
- Certaines paires de noms d’objets S3 légaux ne peuvent pas coexister dans l’arborescence de répertoires NAS mappée. Par exemple, les noms d’objet S3 légal “part1/part2” et “part1/part2/part3” correspondent à des fichiers qui ne peuvent pas exister simultanément dans l’arborescence du répertoire NAS, “part1/part2” étant un fichier du premier nom et un répertoire de l’autre.
  - Si “part1/part2” est un fichier existant, la création S3 de “part1/part2/part3” échouera.
  - Si “part1/part2/part3” est un fichier existant, la création ou la suppression S3 de “part1/part2” échouera.
  - La création d’objet S3 correspondant au nom d’un objet existant remplace l’objet existant (dans des compartiments sans version). La gestion est assurée dans le NAS, mais la correspondance est obligatoire. Les exemples ci-dessus ne peuvent pas entraîner la suppression de l’objet existant car les noms entrent en collision et ne correspondent pas.

Alors qu'un magasin d'objets est conçu pour prendre en charge un grand nombre de noms arbitraires, une structure d'annuaire NAS peut rencontrer des problèmes de performance si un très grand nombre de noms sont placés dans un répertoire. En particulier, les noms sans barre oblique ('/') dans ces caractères seront tous placés dans le répertoire racine du mappage NAS. Les applications qui utilisent de manière intensive les noms qui ne sont pas « compatibles avec le NAS » seraient mieux hébergées dans un compartiment de magasin d'objets réel plutôt que dans un mappage NAS.

Activez l'accès au protocole S3 aux données NAS

L'activation de l'accès au protocole S3 consiste à s'assurer qu'un SVM compatible avec NAS répond aux mêmes exigences qu'un serveur compatible S3, notamment l'ajout d'un serveur de magasin d'objets et la vérification des exigences en matière de réseau et d'authentification.

Pour les nouvelles installations ONTAP, il est recommandé d'activer l'accès par le protocole S3 à un SVM après sa configuration afin d'assurer le service des données NAS aux clients. Pour en savoir plus sur la configuration du protocole NAS, voir :

- "Configuration NFS"
- "Configuration SMB"

Avant de commencer

Les éléments suivants doivent être configurés avant d'activer le protocole S3 :

- Le protocole S3 et les protocoles NAS souhaités (NFS, SMB ou les deux) sont sous licence.
- Un SVM est configuré pour les protocoles NAS souhaités.
- Les serveurs NFS et/ou SMB existent.
- DNS et tous les autres services requis sont configurés.
- Les données NAS sont exportées ou partagées vers les systèmes clients.

Description de la tâche

Un certificat d'autorité de certification (CA) est nécessaire pour activer le trafic HTTPS des clients S3 vers le SVM compatible avec S3. Les certificats CA provenant de trois sources peuvent être utilisés :

- Nouveau certificat auto-signé ONTAP sur le SVM.
- Certificat ONTAP signé automatiquement sur le SVM.
- Un certificat tiers.

Vous pouvez utiliser les mêmes LIF de données pour le compartiment S3/NAS que pour le service des données NAS. Si des adresses IP spécifiques sont requises, reportez-vous à la section "Création de LIF de données". Une règle de données de service S3 est nécessaire pour activer le trafic de données S3 sur les LIF. Vous pouvez modifier la règle de service existante de la SVM afin d'inclure S3.

Lorsque vous créez le serveur objet S3, vous devez préparer le nom du serveur S3 en tant que nom de domaine complet (FQDN) que les clients utiliseront pour l'accès S3. Le FQDN du serveur S3 ne doit pas commencer par un nom de compartiment.

System Manager

1. Activez S3 sur une machine virtuelle de stockage avec les protocoles NAS configurés.
   a. Cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez une machine virtuelle de stockage prête pour le NAS, cliquez sur Paramètres, puis sur ⚙ Sous S3.
   b. Sélectionnez le type de certificat. Que vous sélectionniez un certificat généré par le système ou l'un de vos propres certificats, il sera nécessaire d'accéder au client.
   c. Saisissez les interfaces réseau.
2. Si vous avez sélectionné le certificat généré par le système, les informations de certificat s'affichent lorsque la création de la nouvelle machine virtuelle de stockage est confirmée. Cliquez sur **Download** et enregistrez-le pour accéder au client.
   - La clé secrète ne s'affiche plus.
   - Si vous avez besoin de nouveau des informations de certificat : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.

CLI

1. Vérifier que le protocole S3 est autorisé sur la SVM :
   `vserver show -fields allowed-protocols`
2. Enregistrer le certificat de clé publique pour ce SVM.
   Si vous avez besoin d'un nouveau certificat auto-signé ONTAP, reportez-vous à la section "Créer et installer un certificat d'autorité de certification sur le SVM".
3. Mettre à jour la stratégie de données de service
   a. Afficher la politique de données de service pour la SVM
   `network interface service-policy show -vserver svm_name`
   b. Ajoutez le `data-core` et `data-s3-server services` s'ils ne sont pas présents.
   `network interface service-policy add-service -vserver svm_name -policy policy_name -services data-core,data-s3-server`
4. Vérifier que les LIF de données du SVM répondent à vos exigences :
   `network interface show -vserver svm_name`
5. Création du serveur S3 :
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

Vous pouvez spécifier des options supplémentaires lors de la création du serveur S3 ou à tout moment ultérieurement.

- HTTPS est activé par défaut sur le port 443. Vous pouvez modifier le numéro de port à l'aide de l'option -Secure-Listener-port.
  Lorsque HTTPS est activé, des certificats CA sont requis pour une intégration correcte avec SSL/TLS.
- HTTP est désactivé par défaut ; lorsqu'il est activé, le serveur écoute le port 80. Vous pouvez l'activer avec l'option -is-http-enabled ou modifier le numéro de port avec l'option -port d'écoute.
  Lorsque HTTP est activé, toutes les demandes et réponses sont envoyées en clair sur le réseau.
  1. Vérifiez que S3 est configuré comme vous le souhaitez :

```
vserver object-store-server show
```

Exemple
La commande suivante vérifie les valeurs de configuration de tous les serveurs de stockage objet :
`cluster1::> vserver object-store-server show`

```
Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                 Secure Listener Port For HTTPS: 443
                                   HTTP Enabled: false
                                  HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

Créez un compartiment NAS S3

Un compartiment NAS S3 est un mappage entre un nom de compartiment S3 et un chemin NAS. Les compartiments NAS S3 vous permettent d'offrir un accès S3 à n'importe quelle partie d'un namespace de SVM avec des volumes et une structure de répertoires existants.

Avant de commencer

- Un serveur d'objets S3 est configuré dans une SVM contenant des données NAS.
- Les données NAS sont conformes à la "Exigences en matière d'accès client S3".

Description de la tâche

Vous pouvez configurer les compartiments NAS S3 pour spécifier tout ensemble de fichiers et de répertoires dans le répertoire racine de la SVM.

Vous pouvez également définir des règles de compartiment qui permettent ou non l'accès aux données NAS selon n'importe quelle combinaison de ces paramètres :

- Fichiers et répertoires
- Autorisations utilisateur et groupe
- Opérations S3

Il peut par exemple s'avérer nécessaire de définir des règles de compartiment distinctes pour accorder l'accès aux données en lecture seule à un grand groupe d'utilisateurs, tandis qu'un groupe limité peut effectuer des opérations sur un sous-ensemble de ces données.

Les « compartiments » NAS S3 étant des mappages et non des compartiments S3, les propriétés suivantes des compartiments S3 standard ne s'appliquent pas aux compartiments NAS S3.

- **aggr-list \ aggr-list-multiplier \ storage-service-level \ volume \ size \ exclude-aggr-list \ qos-policy-**

group
Aucun volume ou qtree n'est créé lors de la configuration des compartiments NAS S3.

- **le rôle \ est -protégé \ est -protégé-sur-ontap \ est -protégé-sur-cloud**
  Les compartiments NAS S3 ne sont pas protégés ou mis en miroir à l'aide de SnapMirror S3, mais ils utilisent la protection SnapMirror standard disponible au niveau de la granularité des volumes.
- **etat-versionnage**
  Les volumes NAS disposent généralement de la technologie Snapshot pour enregistrer différentes versions. Cependant, la gestion de version n'est pas disponible dans les compartiments NAS S3.
- **utilisation logique \ nombre-objets**
  Des statistiques équivalentes sont disponibles pour les volumes NAS via les commandes de volume.

System Manager

Ajoutez un nouveau compartiment NAS S3 sur une machine virtuelle de stockage compatible NAS.

1. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**.
2. Entrez un nom pour le compartiment NAS S3 et sélectionnez la machine virtuelle de stockage, ne saisissez pas de taille, puis cliquez sur **plus d'options**.
3. Entrez un nom de chemin d'accès valide ou cliquez sur Parcourir pour le sélectionner dans une liste de noms de chemin valides.
   Lorsque vous entrez un chemin d'accès valide, les options qui ne sont pas pertinentes pour la configuration du NAS S3 sont masquées.
4. Si vous avez déjà mappé des utilisateurs S3 aux utilisateurs NAS et aux groupes créés, vous pouvez configurer leurs autorisations, puis cliquez sur **Enregistrer**.
   Vous devez avoir déjà mappé des utilisateurs S3 à des utilisateurs NAS avant de configurer les autorisations de cette étape.

Sinon, cliquez sur **Save** pour terminer la configuration du compartiment NAS S3.

CLI

Création d'un compartiment NAS S3 dans un SVM contenant des systèmes de fichiers NAS.

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name -type nas -nas-path junction_path [-comment text]
```

Exemple :

```
cluster1::> vserver object-store-server bucket create -bucket testbucket -type
nas -path /vol1
```

Activez les utilisateurs client S3

Pour permettre aux utilisateurs clients S3 d'accéder aux données NAS, vous devez mapper les noms d'utilisateur S3 aux utilisateurs NAS correspondants, puis leur accorder la permission d'accéder aux données NAS à l'aide des politiques de service de compartiment.

Avant de commencer

Les noms d'utilisateur pour l'accès client (utilisateurs clients LINUX/UNIX, Windows et S3) doivent déjà exister.

Description de la tâche

Le mappage d'un nom d'utilisateur S3 avec un utilisateur LINUX/UNIX ou Windows correspondant permet de vérifier les autorisations sur les fichiers NAS qui doivent être honorés lors de l'accès à ces fichiers par des clients S3. Les mappages S3 vers NAS sont spécifiés en fournissant un nom d'utilisateur S3 *Pattern*, qui peut être exprimé sous la forme d'un nom unique ou d'une expression régulière POSIX, et un nom d'utilisateur LINUX/UNIX ou Windows *Replace*.

En l'absence de mappage de nom, le mappage de nom par défaut sera utilisé, où le nom d'utilisateur S3 lui-même sera utilisé comme nom d'utilisateur UNIX et nom d'utilisateur Windows. Vous pouvez modifier les mappages de noms d'utilisateur UNIX et Windows par défaut avec l' `vserver object-store-server modify` commande.

Seule la configuration locale de mappage de noms est prise en charge ; LDAP n'est pas prise en charge.

Une fois que les utilisateurs S3 sont mappés aux utilisateurs NAS, vous pouvez accorder des autorisations aux utilisateurs spécifiant les ressources (répertoires et fichiers) auxquelles ils ont accès et les actions qu'ils sont autorisés ou non à y effectuer.

System Manager

1. Créez des mappages de noms locaux pour les clients UNIX ou Windows (ou les deux).
   a. Cliquez sur **stockage > compartiments**, puis sélectionnez la machine virtuelle de stockage compatible S3/NAS.
   b. Sélectionnez **Paramètres**, puis cliquez sur → Dans **Name Mapping** (sous **Host Users and Groups**).
   c. Dans les mosaïques **S3 à Windows** ou **S3 à UNIX** (ou les deux), cliquez sur **Ajouter**, puis entrez les noms d'utilisateur **Pattern** (S3) et **Replacement** (NAS) souhaités.
2. Création d'une politique de compartiment pour fournir un accès client
   a. Cliquez sur **stockage > godets**, puis sur ⋮ En regard du compartiment S3 souhaité, cliquez sur **Modifier**.
   b. Cliquez sur **Ajouter** et indiquez les valeurs souhaitées.
      - **Principal** - fournir des noms d'utilisateur S3 ou utiliser la valeur par défaut (tous les utilisateurs).
      - **Effet** - sélectionnez **Autoriser** ou **refuser**.
      - **Actions** - Entrez des actions pour ces utilisateurs et ressources. L'ensemble des opérations de ressources que le serveur de magasin d'objets prend actuellement en charge pour les compartiments NAS S3 sont : GetObject, PutObject, DeleteObject, ListBucketAcl, GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBuckeLocation, GetBucketVersioning, PutBuckeVersioning et ListBuckeVersions. Les caractères génériques sont acceptés pour ce paramètre.
      - **Ressources** - Entrez les chemins de dossier ou de fichier dans lesquels les actions sont autorisées ou refusées, ou utilisez les valeurs par défaut (répertoire racine du compartiment).

CLI

1. Créez des mappages de noms locaux pour les clients UNIX ou Windows (ou les deux).
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` - numéro de priorité pour l'évaluation de la cartographie; saisissez 1 ou 2.
   - `-pattern` - Un nom d'utilisateur S3 ou une expression régulière
   - `-replacement` - un nom d'utilisateur windows ou unix

Exemples
```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1 vserver name-mapping create -direction s3-unix
-position 2 -pattern s3_user_1 -replacement unix_user_1
```

1. Création d'une politique de compartiment pour fournir un accès client
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` - indique si l'accès est autorisé ou refusé lorsqu'un utilisateur demande une action.
   - `-action <Action>, …` - spécifie les opérations de ressources qui sont autorisées ou refusées. L'ensemble des opérations de ressources que le serveur de magasin d'objets prend actuellement

en charge pour les compartiments NAS S3 sont : GetObject, PutObject, DeleteObject, ListBucketAcl, GetObjectAcl, GetObjectTagging, PutObjectTagging, DeleteObjectTagging, GetBuckeLocation, GetBucketVersioning, PutBuckeVersioning et ListBuckeVersions. Les caractères génériques sont acceptés pour ce paramètre.

- `-principal <Objectstore Principal>, …` - valide l'utilisateur demandant un accès par rapport aux utilisateurs ou aux groupes du serveur de magasin d'objets spécifiés dans ce paramètre.
  - Un groupe de serveurs de stockage d'objets est spécifié en ajoutant un groupe de préfixe/ au nom du groupe.
  - `-principal` - (le caractère de trait d'union) donne accès à tous les utilisateurs.
- `-resource <text>, …` - spécifie le compartiment, le dossier ou l'objet pour lequel les autorisations d'autorisation/de refus sont définies. Les caractères génériques sont acceptés pour ce paramètre.
- `[-sid <SID>]` - spécifie un commentaire texte facultatif pour l'instruction de stratégie de compartiment de serveur de magasin d'objets.

Exemples

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```