Créer ou modifier des instructions de stratégie d'accès

ONTAP 9

NetApp
April 24, 2024

Sommaire

Créer ou modifier des instructions de stratégie d’accès

À propos des règles des serveurs de compartiment et de magasin d’objets

L’accès des utilisateurs et des groupes aux ressources S3 est contrôlé par des règles de compartiment et de serveur de magasin d’objets. Si vous avez un petit nombre d’utilisateurs ou de groupes, le contrôle de l’accès au niveau du compartiment est probablement suffisant, mais si vous avez de nombreux utilisateurs et groupes, il est plus facile de contrôler l’accès au niveau du serveur du magasin d’objets.

Modifier une règle de compartiment

Vous pouvez ajouter des règles d’accès à la stratégie de compartiment par défaut. L’étendue de son contrôle d’accès est le godet contenant, il est donc le plus approprié lorsqu’il y a un seul godet.

Avant de commencer

Une VM de stockage compatible avec S3 contenant un serveur S3 et un compartiment doit déjà exister.

Vous devez avoir déjà créé des utilisateurs ou des groupes avant d’accorder des autorisations.

Description de la tâche

Vous pouvez ajouter de nouvelles instructions pour les nouveaux utilisateurs et groupes ou modifier les attributs des instructions existantes. Pour plus d’options, reportez-vous à la section `vserver object-store-server bucket policy` pages de manuel.

Des autorisations d’utilisateur et de groupe peuvent être accordées lors de la création du compartiment ou lors de la création de ce dernier. Vous pouvez également modifier la capacité des compartiments et l’affectation des groupes de règles de QoS.

Depuis ONTAP 9.9.1, si vous prévoyez de prendre en charge la fonctionnalité de balisage d’objets du client AWS avec le serveur ONTAP S3, les actions sont les suivantes `GetObjectTagging`, `PutObjectTagging`, et `DeleteObjectTagging` doivent être autorisées à l’aide des règles de compartiment ou de groupe.

La procédure à suivre dépend de l’interface que vous utilisez—System Manager ou de l’interface de ligne de commandes :

System Manager

Étapes

1. Modifiez le compartiment : cliquez sur **stockage > godets**, cliquez sur le compartiment souhaité, puis sur **Modifier**. Lors de l'ajout ou de la modification d'autorisations, vous pouvez spécifier les paramètres suivants :
   - **Principal** : l'utilisateur ou le groupe auquel l'accès est accordé.
   - **Effet** : autorise ou refuse l'accès à un utilisateur ou à un groupe.
   - **Actions** : actions autorisées dans le godet pour un utilisateur ou un groupe donné.
   - **Ressources** : chemins et noms des objets dans le compartiment pour lesquels l'accès est accordé ou refusé.

     Les valeurs par défaut ***bucketname*** et ***bucketname/**** permettent d'accéder à tous les objets du compartiment. Vous pouvez également accorder l'accès à des objets uniques, par exemple ***bucketname/*_readme.txt**.

   - **Conditions** (facultatif) : expressions évaluées lors de la tentative d'accès. Par exemple, vous pouvez spécifier une liste d'adresses IP pour lesquelles l'accès sera autorisé ou refusé.

> À partir de ONTAP 9.14.1, vous pouvez spécifier des variables pour la stratégie de compartiment dans le champ **Resources**. Ces variables sont des espaces réservés qui sont remplacés par des valeurs contextuelles lors de l'évaluation de la règle. Par exemple, si `${aws:username}` est spécifié comme variable pour une stratégie, puis cette variable est remplacée par le nom d'utilisateur du contexte de la demande et l'action de stratégie peut être exécutée comme configuré pour cet utilisateur.

CLI

Étapes

1. Ajouter une déclaration à une politique de compartiment :

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

   Les paramètres suivants définissent les autorisations d'accès :

`-effect`	La déclaration peut autoriser ou refuser l'accès
`-action`	Vous pouvez spécifier `*` pour faire référence à toutes les actions ou à une liste d'une ou plusieurs des actions suivantes : `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`,`GetObjectAcl`, `ListBucketMultipartUploads`, et `ListMultipartUploadParts`.

`-principal`	Liste d'un ou plusieurs utilisateurs ou groupes S3. • Vous pouvez spécifier un maximum de 10 utilisateurs ou groupes. • Si un groupe S3 est spécifié, il doit être dans le formulaire `group/group_name`. • `*` peut être spécifié pour signifier l'accès public, c'est-à-dire l'accès sans clé d'accès et clé secrète. • Si aucun principal n'est spécifié, l'accès est accordé à tous les utilisateurs S3 de la VM de stockage.
`-resource`	Le compartiment et tout objet qu'il contient. Les caractères génériques `*` et `?` peut être utilisé pour former une expression régulière pour spécifier une ressource. Pour une ressource, vous pouvez spécifier des variables dans une règle. Il s'agit de variables de stratégie qui sont remplacées par les valeurs contextuelles lors de l'évaluation de la règle.

Vous pouvez éventuellement spécifier une chaîne de texte sous forme de commentaire avec l' `-sid` option.

Exemples

L'exemple suivant crée une instruction de stratégie de compartiment de serveur de magasin d'objets pour la machine virtuelle de stockage svm1.example.com et le bucket1 qui spécifie l'accès autorisé à un dossier readme pour l'utilisateur du serveur de magasin d'objets user1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

L'exemple suivant crée une instruction de stratégie de compartiment de serveur de magasin d'objets pour la VM de stockage svm1.example.com et bucket1 qui spécifie l'accès autorisé à tous les objets pour le groupe de serveurs de magasin d'objets groupe1.

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

Depuis ONTAP 9.14.1, vous pouvez spécifier des variables pour une règle de compartiment. L'exemple suivant crée une instruction de stratégie de compartiment de serveur pour la VM de stockage `svm1` et `bucket1`, et spécifie `${aws:username}` comme variable pour une ressource de stratégie. Lorsque la stratégie est évaluée, la variable de stratégie est remplacée par le nom d'utilisateur du contexte de demande et l'action de stratégie peut être exécutée comme configuré pour cet utilisateur. Par exemple, lorsque l'instruction de règle suivante est évaluée, `${aws:username}` Est remplacé par l'utilisateur effectuant l'opération S3. Si un utilisateur `user1` exécute l'opération, à laquelle l'utilisateur a accès

`bucket1` comme `bucket1/user1/*`.

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

Créer ou modifier une stratégie de serveur de magasin d'objets

Vous pouvez créer des règles qui s'appliquent à un ou plusieurs compartiments dans un magasin d'objets. Les stratégies de serveur de magasin d'objets peuvent être associées à des groupes d'utilisateurs, ce qui simplifie la gestion de l'accès aux ressources dans plusieurs compartiments.

Avant de commencer

Un SVM compatible S3 contenant un serveur S3 et un compartiment doivent déjà exister.

Description de la tâche

Vous pouvez activer les politiques d'accès au niveau du SVM en spécifiant une règle par défaut ou personnalisée dans un groupe de serveurs de stockage objet. Les stratégies ne prennent effet qu'après avoir été spécifiées dans la définition de groupe.

> Lorsque vous utilisez des stratégies de serveur de stockage objet, vous spécifiez les entités (c'est-à-dire les utilisateurs et les groupes) dans la définition de groupe, et non dans la stratégie elle-même.

Il existe trois règles par défaut en lecture seule pour l'accès aux ressources ONTAP S3 :

- Accès complet
- Aucun accès
- ReadOnlyAccess

Vous pouvez également créer de nouvelles stratégies personnalisées, ajouter de nouvelles instructions pour les nouveaux utilisateurs et groupes, ou modifier les attributs des instructions existantes. Pour plus d'options, reportez-vous à la section `vserver object-store-server policy` "référence de commande".

Depuis ONTAP 9.9.1, si vous prévoyez de prendre en charge la fonctionnalité de balisage d'objets du client AWS avec le serveur ONTAP S3, les actions sont les suivantes `GetObjectTagging`, `PutObjectTagging`, et `DeleteObjectTagging` doivent être autorisées à l'aide des règles de compartiment ou de groupe.

La procédure à suivre dépend de l'interface que vous utilisez—System Manager ou de l'interface de ligne de commandes :

System Manager

Utilisez System Manager pour créer ou modifier une stratégie de serveur de magasin d'objets

Étapes

1. Modifiez la VM de stockage : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la VM de stockage, puis sur **Paramètres** et enfin sur Sous S3.
2. Ajouter un utilisateur : cliquez sur **Policies**, puis sur **Ajouter**.
   a. Entrez un nom de stratégie et sélectionnez-le dans une liste de groupes.
   b. Sélectionnez une stratégie par défaut existante ou ajoutez-en une nouvelle.

      Lors de l'ajout ou de la modification d'une stratégie de groupe, vous pouvez spécifier les paramètres suivants :

      - Groupe : groupes auxquels l'accès est accordé.
      - Effet : autorise ou refuse l'accès à un ou plusieurs groupes.
      - Actions : actions autorisées dans un ou plusieurs compartiments pour un groupe donné.
      - Ressources : chemins et noms d'objets dans un ou plusieurs compartiments pour lesquels l'accès est accordé ou refusé. Par exemple :
        - ***** Permet l'accès à tous les compartiments de la machine virtuelle de stockage.
        - **bucketname** et **bucketname/*** permettent d'accéder à tous les objets d'un compartiment spécifique.
        - **bucketname/readme.txt** donne accès à un objet dans un compartiment spécifique.
   c. Si vous le souhaitez, ajoutez des instructions aux stratégies existantes.

CLI

Utilisez l'interface de ligne de commande pour créer ou modifier une stratégie de serveur de stockage d'objets

Étapes

1. Créer une stratégie de serveur de stockage objet :

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. Créer une instruction pour la règle :

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   Les paramètres suivants définissent les autorisations d'accès :

`-effect`	La déclaration peut autoriser ou refuser l'accès

`-action`	Vous pouvez spécifier `*` pour faire référence à toutes les actions ou à une liste d'une ou plusieurs des actions suivantes : `GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads`, et `ListMultipartUploadParts`.
`-resource`	Le compartiment et tout objet qu'il contient. Les caractères génériques `*` et `?` peut être utilisé pour former une expression régulière pour spécifier une ressource.

Vous pouvez éventuellement spécifier une chaîne de texte sous forme de commentaire avec l' `-sid` option.

Par défaut, de nouvelles instructions sont ajoutées à la fin de la liste des instructions, qui sont traitées dans l'ordre. Lorsque vous ajoutez ou modifiez des instructions ultérieurement, vous avez la possibilité de modifier les instructions `-index` paramètre permettant de modifier l'ordre de traitement.

Configurez l'accès S3 pour les services d'annuaire externes

Depuis ONTAP 9.14.1, les services pour les répertoires externes ont été intégrés au stockage objet ONTAP S3. Cette intégration simplifie la gestion des utilisateurs et des accès via des services d'annuaire externes.

Vous pouvez fournir des groupes d'utilisateurs appartenant à un service d'annuaire externe ayant accès à votre environnement de stockage objet ONTAP. Le protocole LDAP (Lightweight Directory Access Protocol) est une interface permettant de communiquer avec des services d'annuaire, tels qu'Active Directory, qui fournit une base de données et des services de gestion des identités et des accès (IAM). Pour y accéder, vous devez configurer les groupes LDAP dans votre environnement ONTAP S3. Une fois l'accès configuré, les membres du groupe disposent des autorisations nécessaires pour les compartiments ONTAP S3. Pour plus d'informations sur LDAP, reportez-vous à la section "Présentation de l'utilisation de LDAP".

Vous pouvez également configurer des groupes d'utilisateurs Active Directory en mode de liaison rapide, de sorte que les informations d'identification des utilisateurs puissent être validées et que les applications S3 tierces et open source puissent être authentifiées via des connexions LDAP.

Avant de commencer

Avant de configurer les groupes LDAP et d'activer le mode de liaison rapide pour l'accès aux groupes, vérifiez les points suivants :

1. Une VM de stockage compatible S3 contenant un serveur S3 a été créée. Voir "Création d'un SVM pour S3".
2. Un compartiment a été créé dans cette VM de stockage. Voir "Créer un compartiment".
3. DNS est configuré sur la machine virtuelle de stockage. Voir "Configurez les services DNS".
4. Un certificat d'autorité de certification racine (CA) auto-signé du serveur LDAP est installé sur la machine

virtuelle de stockage. Voir "Installer le certificat d'autorité de certification racine auto-signé sur le SVM".

5. Un client LDAP est configuré avec TLS activé sur le SVM. Voir "Créez une configuration client LDAP" et "Associez la configuration client LDAP aux SVM pour plus d'informations".

Configurez l'accès S3 pour les services d'annuaire externes

1. Préciser LDAP comme *NAME service database* du SVM pour le groupe et password pour LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

   Pour plus d'informations sur cette commande, reportez-vous au "vserver services name-service ns-switch modify" commande.

2. Créez une instruction de stratégie de compartiment de magasin d'objets avec `principal` Sélectionnez le groupe LDAP auquel vous souhaitez accorder l'accès :

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

   Exemple : l'exemple suivant crée une instruction de politique de compartiment pour `buck1`. La stratégie autorise l'accès au groupe LDAP `group1` à la ressource (compartiment et ses objets) `buck1`.

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. Vérifiez qu'un utilisateur du groupe LDAP `group1` Est capable d'effectuer des opérations S3 à partir du client S3.

Utilisez le mode de liaison rapide LDAP pour l'authentification

1. Préciser LDAP comme *NAME service database* du SVM pour le groupe et password pour LDAP:

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

Pour plus d'informations sur cette commande, reportez-vous au "vserver services name-service ns-switch modify" commande.

2. Assurez-vous qu'un utilisateur LDAP accédant au compartiment S3 dispose des autorisations définies dans les règles de compartiment. Pour plus d'informations, voir "Modifier une règle de compartiment".
3. Vérifiez qu'un utilisateur du groupe LDAP peut effectuer les opérations suivantes :
   a. Configurez la clé d'accès sur le client S3 dans le format suivant :
      `"NTAPFASTBIND" + base64-encode(user-name:password)`
      Exemple : `"NTAPFASTBIND"` + base64-encode(ldapuser:password), qui résulte en `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`

      > Le client S3 peut vous inviter à saisir une clé secrète. En l'absence d'une clé secrète, vous pouvez saisir un mot de passe d'au moins 16 caractères.

   b. Effectuez des opérations S3 de base à partir du client S3 pour lequel l'utilisateur dispose des autorisations nécessaires.

Activez les utilisateurs LDAP ou du domaine pour générer leurs propres clés d'accès S3

À partir de ONTAP 9.14.1, en tant qu'administrateur ONTAP, vous pouvez créer des rôles personnalisés et les attribuer à des groupes locaux ou de domaine ou à des groupes LDAP (Lightweight Directory Access Protocol), de sorte que les utilisateurs appartenant à ces groupes puissent générer leur propre accès et leurs propres clés secrètes pour l'accès client S3.

Vous devez effectuer quelques étapes de configuration sur votre machine virtuelle de stockage, afin que le rôle personnalisé puisse être créé et attribué à l'utilisateur qui appelle l'API pour la génération de la clé d'accès.

Avant de commencer

Vérifiez les points suivants :

1. Une VM de stockage compatible S3 contenant un serveur S3 a été créée. Voir "Création d'un SVM pour S3".
2. Un compartiment a été créé dans cette VM de stockage. Voir "Créer un compartiment".
3. DNS est configuré sur la machine virtuelle de stockage. Voir "Configurez les services DNS".
4. Un certificat d'autorité de certification racine (CA) auto-signé du serveur LDAP est installé sur la machine virtuelle de stockage. Voir "Installer le certificat d'autorité de certification racine auto-signé sur le SVM".
5. Un client LDAP est configuré avec TLS activé sur la VM de stockage. Voir "Créez une configuration client LDAP" et .

6. Associer la configuration client au Vserver. Voir "Associer la configuration client LDAP aux SVM" et "création du ldap nom-service des services vserver".
7. Si vous utilisez une VM de stockage de données, créez une interface réseau de gestion (LIF) et sur la VM, ainsi qu'une politique de service pour la LIF. Voir la "création d'interface réseau" et "création de la stratégie de service de l'interface réseau" commandes.

Configurer les utilisateurs pour la génération de clés d'accès

1. Spécifiez LDAP comme *name service database* de la machine virtuelle de stockage pour le groupe et le mot de passe pour LDAP :

   ```
   ns-switch modify -vserver <vserver-name> -database group -sources
   files,ldap
   ns-switch modify -vserver <vserver-name> -database passwd -sources
   files,ldap
   ```

   Pour plus d'informations sur cette commande, reportez-vous au "vserver services name-service ns-switch modify" commande.

2. Créez un rôle personnalisé en accédant au terminal de l'API REST de l'utilisateur S3 :
   `security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
   Dans cet exemple, le `s3-role` Le rôle est généré pour les utilisateurs de la VM de stockage `svm-1`, auquel tous les droits d'accès, lecture, création et mise à jour sont accordés.

   ```
   security login rest-role create -vserver svm-1 -role s3role -api
   "/api/protocols/s3/services/*/users" -access all
   ```

   Pour plus d'informations sur cette commande, reportez-vous au "sécurité login rest-role créer" commande.

3. Créez un groupe d'utilisateurs LDAP avec la commande Security login et ajoutez le nouveau rôle personnalisé pour accéder au point final de l'API REST de l'utilisateur S3. Pour plus d'informations sur cette commande, reportez-vous au "création d'une connexion de sécurité" commande.

   ```
   security login create -user-or-group-name <ldap-group-name> -application
   http -authentication-method nsswitch -role <custom-role-name> -is-ns
   -switch-group yes
   ```

   Dans cet exemple, le groupe LDAP `ldap-group-1` est créé dans `svm-1`, et le rôle personnalisé `s3role` Est ajouté pour accéder au noeud final de l'API, ainsi que pour activer l'accès LDAP en mode de liaison rapide.

   ```
   security login create -user-or-group-name ldap-group-1 -application http
   -authentication-method nsswitch -role s3role -is-ns-switch-group yes
   -second-authentication-method none -vserver svm-1 -is-ldap-fastbind yes
   ```

Pour plus d'informations, voir "Utilisez LDAP FAST bind pour l'authentification nsswitch".

L'ajout du rôle personnalisé au domaine ou au groupe LDAP permet aux utilisateurs de ce groupe d'avoir un accès limité à ONTAP `/api/protocols/s3/services/{svm.uuid}/users` point final. En appelant l'API, les utilisateurs du domaine ou du groupe LDAP peuvent générer leurs propres clés d'accès et secrètes pour accéder au client S3. Ils peuvent générer les clés pour eux-mêmes et non pour les autres utilisateurs.

En tant qu'utilisateur S3 ou LDAP, générez vos propres clés d'accès

À partir de ONTAP 9.14.1, vous pouvez générer vos propres clés d'accès et vos clés secrètes pour accéder aux clients S3, si votre administrateur vous a accordé le rôle de génération de vos propres clés. Vous ne pouvez générer les clés que vous-même à l'aide du terminal d'API REST ONTAP suivant.

Méthode HTTP et noeud final

Cet appel d'API REST utilise la méthode et le point de terminaison suivants. Pour plus d'informations sur les autres méthodes de ce noeud final, reportez-vous à la référence "Documentation de l'API".

Méthode HTTP	Chemin
POST	/api/protocoles/s3/services/{svm.uuid}/utilisateurs

Exemple de boucle

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"_name_"}'
```

Exemple de sortie JSON


```
{
  "records": [
    {
      "access_key":
"Pz3SB54G2B_6dsXQPrA5HrTPcf478qoAW6_Xx6qyqZ948AgZ_7YfCf_9nO87YoZmskxx3cq41
U2JAH2M3_fs321B4rkzS3a_oC5_8u7D8j_45N8OsBCBPWGD_1d_ccfq",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user-1",
      "secret_key":
"A20_tDhC_cux2C2BmtL45bXB_a_Q65c_96FsAcOdo14Az8V31jBKDTc0uCL62Bh559gPB8s9r
rn0868QrF38_1dsV2u1_9H2tSf3qQ5xp9NT259C6z_GiZQ883Qn63X1"
    }
  ],
  "num_records": "1"
}
```