Créer ou modifier des instructions de stratégie d'accès

ONTAP 9

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/s3-config/create-modify-bucket-policy-statements-task.html on February 13, 2026. Always check docs.netapp.com for the latest.

Sommaire

Créer ou modifier des instructions de stratégie d'accès . . . 1
- Découvrez les règles du serveur de stockage objet et du compartiment ONTAP S3 . . . 1
- Ajoutez des règles d'accès à la politique de compartiment ONTAP S3 par défaut . . . 1
- Création ou modification d'une règle de serveur de magasin d'objets ONTAP S3 . . . 4
- Configurez les services d'annuaire externes pour l'accès ONTAP S3 . . . 6
  - Configurez l'accès S3 pour LDAP . . . 7
  - Utilisez le mode de liaison rapide LDAP pour l'authentification . . . 8
  - Configurer l'accès S3 pour les serveurs Active Directory ou SMB . . . 9
- Activez les utilisateurs LDAP ou du domaine pour générer leurs propres clés d'accès ONTAP S3 . . . 10
  - Configurer les utilisateurs pour la génération de clés d'accès . . . 11
  - En tant qu'utilisateur S3 ou LDAP, générez vos propres clés d'accès . . . 14

Créer ou modifier des instructions de stratégie d'accès

Découvrez les règles du serveur de stockage objet et du compartiment ONTAP S3

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.

Ajoutez des règles d'accès à la politique de compartiment ONTAP S3 par défaut

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 en savoir plus, `vserver object-store-server bucket policy` consultez le "Référence de commande ONTAP".

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}/*##
```

Création ou modification d'une règle de serveur de magasin d'objets ONTAP S3

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 en savoir plus, `vserver object-store-server policy` consultez le "Référence de commande ONTAP".

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 machine virtuelle de stockage : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la machine virtuelle de stockage, cliquez sur **Paramètres**, puis 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.

Pour en savoir plus sur les commandes décrites dans cette procédure"Référence de commande ONTAP", reportez-vous à la .

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

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 "En savoir plus sur l'utilisation des services de noms LDAP sur les SVM ONTAP NFS"la section .

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 des certificats d'autorité de certification racine auto-signés sur la SVM".
5. Un client LDAP est configuré avec TLS activé sur le SVM. Voir "Créer des configurations de client LDAP pour l'accès NFS ONTAP" et "Associez les configurations client LDAP aux SVM NFS ONTAP pour plus d'informations".

Configurez l'accès S3 pour LDAP

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 en savoir plus sur la commande `vserver services name-service ns-switch modify`, consultez la référence de commande ONTAP.

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 en savoir plus sur la commande `vserver services name-service ns-switch modify`, consultez la référence de commande ONTAP.

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 au format suivant : exemple `"NTAPFASTBIND"` : `"NTAPFASTBIND" + base64-encode(user-name:password)` + base64-encode(ldapuser:password), ce qui en résulte `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.

Identifiants Base64

La configuration par défaut de ONTAP S3 exclut HTTP et utilise exclusivement HTTPS et une connexion TLS (transport Layer Security). ONTAP peut générer des certificats auto-signés, mais il est recommandé d'utiliser les certificats d'une autorité de certification tierce. Lorsque vous utilisez des certificats d'autorité de certification, vous créez une relation de confiance entre les applications clientes et le serveur de magasin d'objets ONTAP.

Sachez que les informations d'identification codées à l'aide de Base64 sont facilement décodées. L'utilisation du protocole HTTPS empêche les informations d'identification codées d'être capturées par les renifleurs de paquets MAN-in-the-middle.

N'utilisez pas le mode de liaison rapide LDAP pour l'authentification lors de la création d'URL pré-signées. L'authentification est basée exclusivement sur la clé d'accès Base64 incluse dans l'URL présignée. Le nom d'utilisateur et le mot de passe seront divulgués à toute personne qui décochera la clé d'accès Base64.

La méthode d'authentification est nsswitch et LDAP est activé exemple

```
$curl -siku <user>:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>", "name":<user>,"key_time_to_live":"PT6H3M"}
```

Orienter l'API vers la LIF de cluster management, et non vers la LIF de données du SVM. Si vous souhaitez autoriser les utilisateurs à générer leurs propres clés, vous devez ajouter des autorisations HTTP à leur rôle pour utiliser curl. Cette autorisation vient en complément des autorisations de l'API S3.

Configurer l'accès S3 pour les serveurs Active Directory ou SMB

Si le groupe nasgroup spécifié dans l'instruction de stratégie de compartiment ou si les utilisateurs qui font partie du groupe nasgroup n'ont pas d'UID et de GID définis, les recherches échouent lorsque ces attributs ne sont pas trouvés. Active Directory utilise SID et non UID. Si les entrées SID ne peuvent pas être mappées à l'UID, les données nécessaires doivent être transférées à ONTAP.

Pour ce faire, utiliser "vserver active-directory create" afin que le SVM puisse s'authentifier auprès d'Active Directory et obtenir les informations nécessaires sur les utilisateurs et les groupes.

Vous pouvez également utiliser "création d'un vserver cifs" pour créer un serveur SMB dans un domaine Active Directory.

Si vous utilisez des noms de domaine différents pour les serveurs de noms et les magasins d'objets, des échecs de recherche peuvent survenir. Pour éviter ces échecs, NetApp recommande d'utiliser des domaines de confiance pour l'autorisation des ressources au format UPN : `nasgroup/group@trusted_domain.com` Les domaines de confiance sont ceux ajoutés à la liste des domaines de confiance du serveur SMB. Découvrez comment "ajouter, supprimer et modifier les domaines de confiance préférés" dans la liste des serveurs SMB.

Générez des clés lorsque la méthode d'authentification est domaine et que les domaines de confiance sont configurés dans Active Directory

Utilisez le `s3/services/<svm_uuid>/users` noeud final avec les utilisateurs spécifiés au format UPN. Exemple :

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user@fqdn>,"key_time_to_live":"PT6H3M"}
```

Orienter l'API vers la LIF de cluster management, et non vers la LIF de données du SVM. Si vous souhaitez autoriser les utilisateurs à générer leurs propres clés, vous devez ajouter des autorisations HTTP à leur rôle pour utiliser curl. Cette autorisation vient en complément des autorisations de l'API S3.

Générez des clés lorsque la méthode d'authentification est domaine et qu'il n'y a pas de domaines de confiance

Cette action est possible lorsque LDAP est désactivé ou lorsque des utilisateurs non POSIX n'ont pas configuré UID et GID. Exemple :

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn]>,"key_time_to_live":"PT6H3M"}
```

Orienter l'API vers la LIF de cluster management, et non vers la LIF de données du SVM. Si vous souhaitez autoriser les utilisateurs à générer leurs propres clés, vous devez ajouter des autorisations HTTP à leur rôle pour utiliser curl. Cette autorisation vient en complément des autorisations de l'API S3. Il vous suffit d'ajouter la valeur de domaine facultative (@fqdn) à un nom d'utilisateur s'il n'y a pas de domaines de confiance.

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

Si LDAP est désactivé, vous pouvez "configurer des services d'annuaire externes pour l'accès ONTAP S3" pour permettre aux utilisateurs de générer des clés 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 des certificats d'autorité de certification racine auto-signés sur la SVM".
5. Un client LDAP est configuré avec TLS activé sur la VM de stockage. Voir "Créer des configurations de client LDAP pour l'accès NFS ONTAP".
6. Associer la configuration client au Vserver. Voir "Associer les configurations client LDAP aux SVM ONTAP NFS". Pour en savoir plus, `vserver services name-service ldap create` consultez le "Référence de commande ONTAP".
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. Pour en savoir plus sur `network interface create` et `network interface service-policy create` dans le "Référence de commande ONTAP".

Configurer les utilisateurs pour la génération de clés d’accès

Exemple 1. Étapes

Utilisateurs LDAP

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 en savoir plus, `vserver services name-service ns-switch modify` consultez le "Référence de commande ONTAP".

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 en savoir plus, `security login rest-role create` consultez le "Référence de commande ONTAP".

3. Créez un groupe d'utilisateurs LDAP avec le `security login` commandez et ajoutez le nouveau rôle personnalisé pour accéder au point de terminaison de l'API REST de l'utilisateur S3. En savoir plus sur `security login create` dans le "Référence de commande ONTAP" .

```
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 "Utiliser la liaison rapide LDAP pour l'authentification nsswitch pour les SVM NFS ONTAP".

Pour en savoir plus, `security login create` consultez le "Référence de commande ONTAP".

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

Utilisateurs du domaine

1. Créez un rôle personnalisé avec accès au point de terminaison 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 sur la machine virtuelle de stockage `svm-1` , auquel tous les droits d'accès, de lecture, de création et de mise à jour sont accordés.

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

Pour en savoir plus, `security login rest-role create` consultez le "Référence de commande ONTAP".

1. Créez un groupe d'utilisateurs de domaine avec le `security login` commandez et ajoutez le nouveau rôle personnalisé pour accéder au point de terminaison de l'API REST de l'utilisateur S3. En savoir plus sur `security login create` dans le "Référence de commande ONTAP" .

   ```
   security login create -vserver <vserver-name> -user-or-group-name domain\<group-name> -application http -authentication-method domain -role <custom-role-name>
   ```

   Dans cet exemple, le groupe de domaines `domain\group1` est créé en `svm-1` , et le rôle personnalisé `s3role` est ajouté pour accéder au point de terminaison de l'API.

   ```
   security login create -user-or-group-name domain\group1 -application http -authentication-method domain -role s3role -vserver svm-1
   ```

   Pour en savoir plus, `security login create` consultez le "Référence de commande ONTAP".

L'ajout du rôle personnalisé au groupe de domaine permet aux utilisateurs de ce groupe un accès limité à ONTAP `/api/protocols/s3/services/{svm.uuid}/users` Point de terminaison. En invoquant l'API, les utilisateurs du groupe de domaine peuvent générer leurs propres clés d'accès et clés secrètes pour accéder au client S3. Ils peuvent générer ces clés uniquement 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.

Créer un utilisateur S3 et générer des clés

Cet appel d'API REST utilise la méthode et le point de terminaison suivants. Pour plus d'informations sur ce point de terminaison, consultez la référence. "Documentation de l'API" .

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

Pour les utilisateurs de domaine, utilisez le format suivant pour le nom d'utilisateur S3 : `user@fqdn` , où `fqdn` est le nom de domaine complet du domaine.

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":"user1@example.com"}'
```

Exemple de sortie JSON

```
{
  "records": [
    {
      "access_key": "4KX07KF7ML8YNWY01JWG",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

Régénérer les clés pour un utilisateur S3

Si un utilisateur S3 existe déjà, vous pouvez régénérer ses clés d'accès et secrètes. Cet appel d'API REST utilise la méthode et le point de terminaison suivants.

Méthode HTTP	Chemin
CORRECTIF	/api/protocols/s3/services/{svm.uuid}/users/{name}

Exemple de boucle

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

Exemple de sortie JSON

```
{
  "records": [
    {
      "access_key": "DX12U609DMRVD8U30Z1M",
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.