Configurer

ONTAP 9

NetApp
April 13, 2024

Sommaire

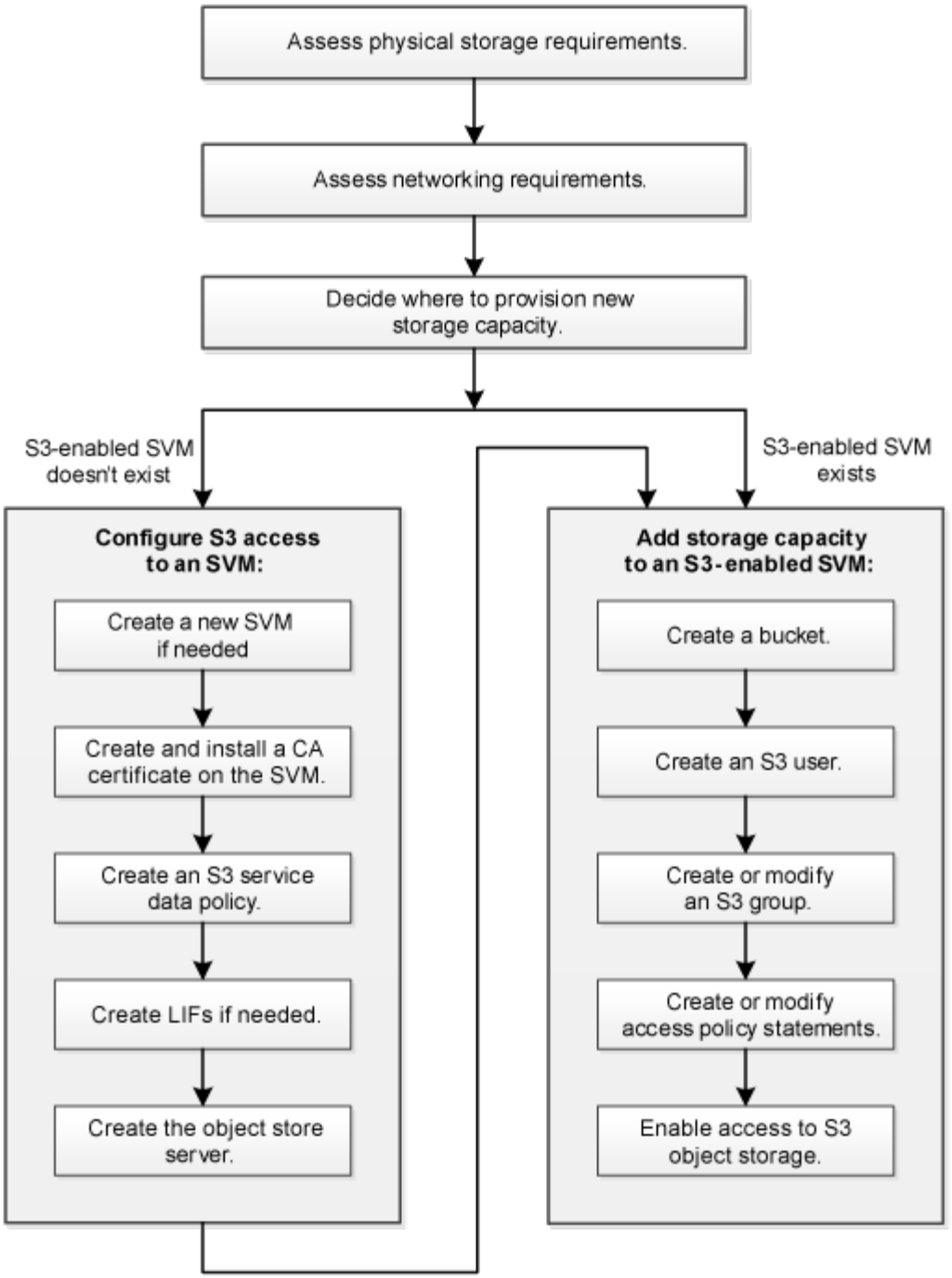
Configurer

À propos du processus de configuration S3

Workflow de configuration S3

La configuration de S3 implique d'évaluer les exigences en matière de stockage physique et de réseau, puis de choisir un workflow spécifique à votre objectif : configurer l'accès S3 pour un SVM nouveau ou existant, ou ajouter un compartiment et des utilisateurs à une SVM existante déjà entièrement configurée pour l'accès S3.

Lorsque vous configurez l'accès S3 à une nouvelle machine virtuelle de stockage à l'aide de System Manager, vous êtes invité à saisir des informations de certificat et de mise en réseau, et la machine virtuelle de stockage et le serveur de stockage objet S3 sont créés en une seule opération.



Évaluer les besoins en matière de stockage physique

Avant de provisionner le stockage S3 pour les clients, vous devez vérifier que l'espace est suffisant dans les agrégats existants pour le nouveau magasin d'objets. Si ce n'est pas le cas, vous pouvez ajouter des disques à des agrégats existants ou créer de nouveaux agrégats du type et de l'emplacement souhaités.

Description de la tâche

Lorsque vous créez un compartiment S3 dans un SVM compatible avec S3, un volume FlexGroup est automatiquement créé pour prendre en charge le compartiment. Vous pouvez laisser ONTAP Select les agrégats sous-jacents et les composants FlexGroup automatiquement (par défaut) ou sélectionner les

agrégats sous-jacents et les composants FlexGroup vous-même.

Si vous décidez de spécifier les agrégats et les composants FlexGroup, par exemple si vous avez des exigences de performances spécifiques pour les disques sous-jacents, vous devez vous assurer que la configuration de votre agrégat respecte les meilleures pratiques en matière de provisionnement d'un volume FlexGroup. En savoir plus :

- "Gestion des volumes FlexGroup"
- "Rapport technique NetApp 4571-a : meilleures pratiques relatives au volume NetApp ONTAP FlexGroup"

Si vous accédez aux compartiments à partir de Cloud Volumes ONTAP, il est fortement recommandé de sélectionner manuellement les agrégats sous-jacents pour vérifier qu'ils n'utilisent qu'un seul nœud. L'utilisation d'agrégats des deux nœuds peut avoir un impact sur les performances, car les nœuds se trouvent dans des zones de disponibilité séparées géographiquement et sont donc sujets aux problèmes de latence. Découvrez "Création de compartiments pour Cloud Volumes ONTAP".

Vous pouvez utiliser le serveur ONTAP S3 pour créer un Tier de capacité FabricPool local, à savoir dans le même cluster que le Tier de performance. Cela peut être utile, par exemple, si des disques SSD sont connectés à une paire haute disponibilité et que vous souhaitez hiérarchiser les données froide_ sur des disques HDD d'une autre paire haute disponibilité. Dans ce cas d'utilisation, le serveur S3 et le compartiment contenant le Tier de capacité locale doivent donc se trouver dans une paire HA différente de celle du Tier de performance. Le Tiering local n'est pas pris en charge sur les clusters à un ou deux nœuds.

Étapes

1. Afficher l'espace disponible dans les agrégats existants :

   ```
   storage aggregate show
   ```

   Si un agrégat dispose d'un espace suffisant ou si l'emplacement du nœud requis, enregistrez son nom pour votre configuration S3.

   ```
   cluster-1::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                            normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                            normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                            normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                            normal
   6 entries were displayed.
   ```

2. En l'absence d'agrégats disposant d'espace suffisant ou d'emplacement de nœud requis, ajoutez des disques à un agrégat existant en utilisant le `storage aggregate add-disks` ou créez un nouvel

agrégat à l'aide de `storage aggregate create` commande.

Évaluer les exigences de mise en réseau

Avant de fournir du stockage S3 aux clients, vous devez vérifier que le réseau est correctement configuré pour répondre aux exigences de provisionnement S3.

Avant de commencer

Les objets de réseau de cluster suivants doivent être configurés :

- Ports physiques et logiques
- Les domaines de diffusion
- Sous-réseaux (le cas échéant)
- IPspaces (selon les besoins, en plus de l'IPspace par défaut)
- Failover Groups (si nécessaire, en plus du groupe de basculement par défaut pour chaque broadcast domain)
- Pare-feu externes

Description de la tâche

Pour les tiers de capacité FabricPool distante (cloud) et les clients S3 distants, vous devez utiliser un SVM de données et configurer des LIF de données. Pour les niveaux cloud FabricPool, vous devez également configurer les LIF intercluster ; le peering de cluster n'est pas nécessaire.

Pour les niveaux de capacité FabricPool locaux, il est nécessaire d'utiliser la SVM système (appelée « Cluster »), mais il existe deux options de configuration de LIF :

- Vous pouvez utiliser les LIFs de cluster.

  Avec cette option, aucune autre configuration LIF n'est requise, mais le trafic sur les LIFs du cluster sera augmenté. En outre, le niveau local ne sera pas accessible aux autres clusters.

- Vous pouvez utiliser des LIF data et intercluster.

  Une configuration supplémentaire est nécessaire, notamment l'activation des LIF pour le protocole S3, mais le Tier local sera également accessible en tant que Tier cloud FabricPool distant vers d'autres clusters.

Étapes

1. Afficher les ports physiques et virtuels disponibles :

   ```
   network port show
   ```

   - Dans la mesure du possible, vous devez utiliser le port avec la vitesse la plus élevée pour le réseau de données.
   - Tous les composants du réseau de données doivent avoir le même paramètre MTU pour optimiser les performances.

2. Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, vérifiez que le sous-réseau existe et dispose des adresses suffisantes :

   ```
   network subnet show
   ```

Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Les sous-réseaux sont créés à l'aide du `network subnet create` commande.

3. Affichez les IPspaces disponibles :

   ```
   network ipspace show
   ```

   Vous pouvez utiliser l'IPspace par défaut ou un IPspace personnalisé.

4. Si vous souhaitez utiliser des adresses IPv6, vérifiez que l'IPv6 est activé sur le cluster :

   ```
   network options ipv6 show
   ```

   Si nécessaire, vous pouvez activer IPv6 en utilisant le `network options ipv6 modify` commande.

Choisissez où provisionner la capacité de stockage S3

Avant de créer un nouveau compartiment S3, vous devez décider de le placer dans un SVM nouveau ou existant. Cette décision détermine votre flux de travail.

Choix

- Si vous souhaitez provisionner un compartiment dans un nouveau SVM ou un SVM qui n'est pas activé pour S3, effectuez les étapes suivantes.

  "Création d'un SVM pour S3"

  "Création d'un compartiment pour S3"

  Bien que S3 puisse coexister dans un SVM avec NFS et SMB, il est possible de créer un nouveau SVM si l'un des cas suivants est vrai :

  - Vous activez S3 pour la première fois sur un cluster.
  - Un cluster contient des SVM dans lesquels vous ne souhaitez pas activer la prise en charge de S3.
  - Un ou plusieurs SVM compatibles S3 sont mis en cluster et un autre serveur S3 doit avoir des caractéristiques de performance différentes. Après l'activation du protocole S3 sur le SVM, procéder au provisionnement d'un compartiment.
- Pour provisionner le compartiment initial ou un compartiment supplémentaire sur un SVM compatible S3, effectuez la procédure ci-dessous.

  "Création d'un compartiment pour S3"

Configurez l'accès S3 à un SVM

Création d'un SVM pour S3

Bien que S3 puisse coexister avec d'autres protocoles dans un SVM, il peut être nécessaire de créer un nouveau SVM afin d'isoler le namespace et les workloads.

Description de la tâche

Si vous fournit uniquement le stockage objet S3 à partir d'un SVM, le serveur S3 ne nécessite aucune

configuration DNS. Toutefois, il peut être nécessaire de configurer le DNS sur le SVM si d'autres protocoles sont utilisés.

Lorsque vous configurez l'accès S3 à une nouvelle machine virtuelle de stockage à l'aide de System Manager, vous êtes invité à saisir des informations de certificat et de mise en réseau, et la machine virtuelle de stockage et le serveur de stockage objet S3 sont créés en une seule opération.

Exemple 1. Étapes

System Manager

Vous devez préparer à saisir 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.

Vous devez être prêt à saisir des adresses IP pour les données de rôle d'interface.

Si vous utilisez un certificat signé par une autorité de certification externe, vous serez invité à le saisir au cours de cette procédure ; vous avez également la possibilité d'utiliser un certificat généré par le système.

1. Activez S3 sur une VM de stockage.

   a. Ajouter une nouvelle machine virtuelle de stockage : cliquez sur **stockage > machines virtuelles de stockage**, puis sur **Ajouter**.

      S'il s'agit d'un nouveau système sans machines virtuelles de stockage existantes : cliquez sur **Tableau de bord > configurer les protocoles**.

   Si vous ajoutez un serveur S3 à une machine virtuelle de stockage existante : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez une machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez sur Sous **S3**.

   a. Cliquez sur **Activer S3**, puis entrez le nom du serveur 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. Vérifiez que la licence S3 est disponible sur votre cluster :

   ```
   system license show -package s3
   ```

   Si ce n'est pas le cas, contactez votre représentant commercial.

2. Création d'un SVM :

```
vserver create -vserver <svm_name> -subtype default -rootvolume
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security
-style unix -language C.UTF-8 -data-services <data-s3-server>
-ipspace <ipspace_name>
```

- Utilisez le paramètre UNIX pour le `-rootvolume-security-style` option.
- Utilisez le paramètre par défaut C.UTF-8 `-language` option.
- Le `ipspace` le paramètre est facultatif.

3. Vérifier la configuration et le statut du nouveau SVM :

```
vserver show -vserver <svm_name>
```

Le `Vserver Operational State` le champ doit afficher `running` état. S'il affiche le `initializing` État, cela signifie qu'une opération intermédiaire telle que la création du volume root a échoué, et vous devez supprimer la SVM et la recréer.

Exemples

La commande suivante crée un SVM pour l'accès aux données dans l'IPspace ipspaceA :

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services _data-s3-server_ -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

La commande suivante montre qu'un SVM a été créé avec un volume root de 1 Go, il a été démarré automatiquement et qu'il est en `running` état. Le volume root dispose d'une export policy par défaut qui n'inclut aucune règle et qui ne précise donc pas l'exportation du volume root au moment de sa création. Par défaut, le compte utilisateur vsadmin est créé et est dans le `locked` état. Le rôle vsadmin est attribué au compte utilisateur par défaut vsadmin.

```
cluster-1::> vserver show -vserver svm1.example.com
                                    Vserver: svm1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                    Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

Créer et installer un certificat d’autorité de certification sur le SVM

Un certificat d’autorité de certification (CA) est nécessaire pour activer le trafic HTTPS des clients S3 vers le SVM compatible avec S3.

Description de la tâche

Bien qu’il soit possible de configurer un serveur S3 pour utiliser uniquement le protocole HTTP, et bien qu’il soit possible de configurer des clients sans exigence de certificat d’autorité de certification, il est recommandé de sécuriser le trafic HTTPS vers des serveurs ONTAP S3 avec un certificat d’autorité de certification.

Un certificat CA n’est pas nécessaire pour une utilisation de hiérarchisation locale, où le trafic IP transite uniquement par les LIFs de cluster.

Les instructions de cette procédure créent et installent un certificat auto-signé ONTAP. Les certificats CA de fournisseurs tiers sont également pris en charge ; consultez la documentation relative à l’authentification de l’administrateur pour plus d’informations.

"Authentification de l’administrateur et RBAC"

Voir la `security certificate` pages de manuel pour les options de configuration supplémentaires.

Étapes

1. Créer un certificat numérique auto-signé :

   `security certificate create -vserver` *`svm_name`* `-type root-ca -common-name` *`ca_cert_name`*

   Le `-type root-ca` Option crée et installe un certificat numérique auto-signé pour signer d'autres certificats en agissant comme autorité de certification (CA).

   Le `-common-name` Option crée le nom de l'autorité de certification du SVM et sera utilisé lors de la génération du nom complet du certificat.

   La taille du certificat par défaut est de 2048 bits.

   Exemple

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   Lorsque le nom généré du certificat est affiché, veillez à l'enregistrer pour les étapes ultérieures de cette procédure.

2. Générer une demande de signature de certificat :

   `security certificate generate-csr -common-name` *`s3_server_name`* `[additional_options]`

   Le `-common-name` Le paramètre de la demande de signature doit être le nom de serveur S3 (FQDN).

   Vous pouvez fournir l'emplacement et d'autres informations détaillées sur la SVM si nécessaire.

   Vous êtes invité à conserver une copie de votre demande de certificat et de votre clé privée pour référence ultérieure.

3. Signer la RSC à l'aide de SVM_CA pour générer le certificat du serveur S3 :

   `security certificate sign -vserver` *`svm_name`* `-ca` *`ca_cert_name`* `-ca-serial` *`ca_cert_serial_number`* `[additional_options]`

   Entrez les options de commande que vous avez utilisées aux étapes précédentes :

   - `-ca` — le nom commun de l'autorité de certification que vous avez saisi à l'étape 1.
   - `-ca-serial` — le numéro de série CA de l'étape 1. Par exemple, si le nom du certificat de l'autorité de certification est svm1_CA_159D1587CE21E9D4_svm1_ca, le numéro de série est 159D1587CE2E9D4.

     Par défaut, le certificat signé expirera dans 365 jours. Vous pouvez sélectionner une autre valeur et spécifier d'autres détails de signature.

Lorsque vous y êtes invité, copiez et entrez la chaîne de demande de certificat que vous avez enregistrée à l'étape 2.

Un certificat signé s'affiche ; enregistrez-le pour une utilisation ultérieure.

4. Installez le certificat signé sur le SVM compatible S3 :

   `security certificate install -type server -vserver svm_name`

   Lorsque vous y êtes invité, entrez le certificat et la clé privée.

   Vous avez la possibilité de saisir des certificats intermédiaires si une chaîne de certificats est souhaitée.

   Lorsque la clé privée et le certificat numérique signé par l'autorité de certification sont affichés, enregistrez-les pour référence ultérieure.

5. Obtenir le certificat de clé publique :

   `security certificate show -vserver svm_name -common-name ca_cert_name -type root-ca -instance`

   Enregistrez le certificat de clé publique pour une configuration client ultérieure.

   Exemple

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
          FQDN or Custom Common Name: svm1_ca
         Serial Number of Certificate: 159D1587CE21E9D4
               Certificate Authority: svm1_ca
                 Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
             Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
              Certificate Start Date: Thu May 09 10:58:39 2020
          Certificate Expiration Date: Fri May 08 10:58:39 2021
               Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
               State or Province Name:
                        Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                             Protocol: SSL
                      Hashing Function: SHA256
              Self-Signed Certificate: true
       Is System Internal Certificate: false
```

Création d’une règle de données de service S3

Vous pouvez créer des règles de service pour les données S3 et les services de gestion. Une règle de données de service S3 est nécessaire pour activer le trafic de données S3 sur les LIF.

Description de la tâche

Une politique de données de service S3 est requise si vous utilisez des LIF de données et des LIF intercluster. Il n’est pas nécessaire d’utiliser des LIF de cluster pour la hiérarchisation locale.

Lorsqu’une politique de services est spécifiée pour une LIF, cette règle est utilisée pour construire un rôle par défaut, une politique de basculement et une liste de protocoles de données pour la LIF.

Bien que plusieurs protocoles puissent être configurés pour les SVM et les LIF, il est recommandé de configurer S3 comme le seul protocole lors du service des données d’objet.

Étapes

1. Modifiez le paramètre de privilège sur avancé :

```
set -privilege advanced
```

2. Création d'une règle de données de service :

   ```
   network interface service-policy create -vserver svm_name -policy policy_name
   -services data-core,data-s3-server
   ```

   Le `data-core` et `data-s3-server` Les services sont les seuls requis pour activer ONTAP S3, bien que d'autres services puissent être inclus si nécessaire.

Création de LIF de données

Si vous avez créé un nouveau SVM, les LIF dédiées que vous créez pour accéder à S3 doivent être des LIF de données.

Avant de commencer

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur l'administrateur `up` état.
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.

  Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide du `network subnet create` commande.

- La politique de service LIF doit déjà exister.

Description de la tâche

- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster à l'aide de `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).
- Si vous activez la hiérarchisation distante de la capacité FabricPool (cloud), vous devez également configurer les LIF intercluster.

Étapes

1. Créer une LIF :

   ```
   network interface create -vserver svm_name -lif lif_name -service-policy
   service_policy_names -home-node node_name -home-port port_name {-address
   IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy
   data -auto-revert {true|false}
   ```

   - `-home-node` Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

     Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec le `-auto-revert` option.

   - `-home-port` Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

- Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec le `-subnet_name` option.
- Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Le `network route create` La page man contient des informations sur la création d'une route statique au sein d'un SVM.
- Pour le `-firewall-policy` utilisez la même option par défaut `data` Comme le rôle LIF.

  Vous pouvez créer et ajouter une stratégie de pare-feu personnalisée ultérieurement si vous le souhaitez.

  > Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "Configuration des politiques de pare-feu pour les LIF".

- `-auto-revert` Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `false` selon les stratégies de gestion de réseau de votre environnement.
- Le `-service-policy` spécifie la stratégie de données et de services de gestion que vous avez créée ainsi que les autres règles dont vous avez besoin.

2. Si vous souhaitez attribuer une adresse IPv6 dans `-address` option :

   a. Utilisez le `network ndp prefix show` Commande permettant d'afficher la liste des préfixes de RA apprises sur diverses interfaces.

      Le `network ndp prefix show` la commande est disponible au niveau de privilège avancé.

   b. Utiliser le format `prefix:id` Pour construire l'adresse IPv6 manuellement.

      `prefix` est le préfixe utilisé sur les différentes interfaces.

   Pour calculer le `id`, choisissez un nombre hexadécimal 64 bits aléatoire.

3. Vérifier que le LIF a été créé avec succès en utilisant le `network interface show` commande.
4. Vérifiez que l'adresse IP configurée est accessible :

Pour vérifier…	Utiliser…
Adresse IPv4	`network ping`
Adresse IPv6	`network ping6`

Exemples

La commande suivante montre comment créer une LIF de données S3 attribuée avec le `my-S3-policy` règle de service :

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

La commande suivante affiche toutes les LIFs du cluster-1. Les LIF de données datalif1 et datalif3 sont configurées avec des adresses IPv4 et le datalif4 est configuré avec une adresse IPv6 :

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

Création des LIFs intercluster pour le Tiering distant des FabricPool

Si vous activez le Tiering FabricPool à distance (cloud) à l'aide de ONTAP S3, vous devez configurer les LIF intercluster. Vous pouvez configurer les LIFs intercluster sur des ports partagés avec le réseau de données. Cela réduit le nombre de ports nécessaires pour la mise en réseau intercluster.

Avant de commencer

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur l'administrateur `up` état.
- La politique de service LIF doit déjà exister.

Description de la tâche

Les LIF intercluster ne sont pas nécessaires pour la hiérarchisation locale des pools de structure ni pour le traitement d'applications S3 externes.

Étapes

1. Lister les ports dans le cluster :

   `network port show`

   L'exemple suivant montre les ports réseau dans `cluster01`:

```
cluster01::> network port show
                                                                 Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. Création des LIFs intercluster sur le SVM système :

   `network interface create -vserver Cluster -lif` *`LIF_name`* `-service-policy default-intercluster -home-node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

   L'exemple suivant illustre la création de LIFs intercluster `cluster01_icl01` et `cluster01_icl02`:

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Vérifier que les LIFs intercluster ont été créés :

   `network interface show -service-policy default-intercluster`

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. Vérifier que les LIFs intercluster sont redondants :

   `network interface show –service-policy default-intercluster -failover`

   L'exemple suivant indique que les LIFs intercluster `cluster01_icl01` et `cluster01_icl02` sur le `e0c` le port basculera vers le `e0d` port.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

Créez le serveur de magasin d'objets S3

Le serveur de magasin d'objets ONTAP gère les données sous forme d'objets S3 au lieu du stockage de fichiers ou de blocs fourni par les serveurs NAS et SAN ONTAP.

Avant de commencer

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

Vous devez disposer d'un certificat d'autorité de certification auto-signé (créé aux étapes précédentes) ou d'un certificat signé par un fournisseur d'autorité de certification externe. Un certificat CA n'est pas nécessaire pour une utilisation de hiérarchisation locale, où le trafic IP transite uniquement par les LIFs de cluster.

Description de la tâche

Lorsqu'un serveur de magasin d'objets est créé, un utilisateur root avec UID 0 est créé. Aucune clé d'accès ou clé secrète n'est générée pour cet utilisateur root. L'administrateur ONTAP doit exécuter le `object-store-server users regenerate-keys` commande permettant de définir la clé d'accès et la clé secrète pour cet utilisateur.

> Dans le cadre de nos bonnes pratiques, ne pas utiliser cet utilisateur root. Toute application client qui utilise la clé d'accès ou la clé secrète de l'utilisateur root dispose d'un accès complet à tous les compartiments et objets du magasin d'objets.

Voir la `vserver object-store-server` pages de manuel pour des options de configuration et d'affichage supplémentaires.

Exemple 2. Étapes

System Manager

Suivez cette procédure si vous ajoutez un serveur S3 à une machine virtuelle de stockage existante. Pour ajouter un serveur S3 à une nouvelle machine virtuelle de stockage, voir "Création d'un SVM de stockage pour S3".

Vous devez être prêt à saisir des adresses IP pour les données de rôle d'interface.

1. Activez S3 sur une machine virtuelle de stockage existante.
   a. Sélectionnez la VM de stockage : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez une VM de stockage, cliquez sur **Paramètres**, puis cliquez sur Sous **S3**.
   b. Cliquez sur **Activer S3**, puis entrez le nom du serveur S3.
   c. 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.

   d. 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. Création du serveur S3 :

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

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

   - Si vous configurez une hiérarchisation locale, le nom du SVM peut être un SVM de données ou un nom de SVM système (cluster).
   - Le nom du certificat doit être le nom du certificat du serveur (certificat d'utilisateur final ou de serveur) et non le certificat de l'autorité de certification du serveur (certificat de l'autorité de certification intermédiaire ou racine).
   - HTTPS est activé par défaut sur le port 443. Vous pouvez modifier le numéro de port à l'aide du `-secure-listener-port` option.

     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 sur le port 80. Vous pouvez l'activer avec le `-is-http-enabled` ou modifiez le numéro de port avec le `-listener-port`

option.

Lorsque HTTP est activé, la requête et les réponses sont envoyées sur le réseau en texte clair.

2. Vérifier que S3 est configuré :

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

Exemple

Cette commande 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
```

Ajout de capacité de stockage à un SVM compatible S3

Créer un compartiment

Les objets S3 sont conservés dans *buckets*. Ils ne sont pas imbriqués en tant que fichiers dans un répertoire à l'intérieur d'autres répertoires.

Avant de commencer

Une VM de stockage contenant un serveur S3 doit déjà exister.

Description de la tâche

- Depuis la version ONTAP 9.14.1, le redimensionnement automatique a été activé sur les volumes FlexGroup S3 lorsque des compartiments sont créés. Cela élimine l'allocation excessive de capacité lors de la création du compartiment sur les volumes FlexGroup existants et nouveaux. Les volumes FlexGroup sont redimensionnés au minimum requis selon les instructions suivantes. La taille minimale requise correspond à la taille totale de tous les compartiments S3 d'un volume FlexGroup.
  - À partir de ONTAP 9.14.1, si un volume FlexGroup S3 est créé dans le cadre d'une nouvelle création de compartiment, le volume FlexGroup est créé avec la taille minimale requise.
  - Si un volume FlexGroup S3 a été créé avant ONTAP 9.14.1, le premier compartiment créé ou supprimé après ONTAP 9.14.1 redimensionne le volume FlexGroup à la taille minimale requise.
  - Si un volume FlexGroup S3 a été créé avant ONTAP 9.14.1 et disposait déjà de la taille minimale requise, la création ou la suppression d'un compartiment après ONTAP 9.14.1 conserve la taille du

volume FlexGroup S3.

- Les niveaux de service de stockage sont des groupes de règles prédéfinies de qualité de service (QoS) adaptative, avec des niveaux par défaut *Value*, *performance* et *Extreme*. Au lieu d'un des niveaux de service de stockage par défaut, vous pouvez également définir un groupe de règles de QoS personnalisé et le appliquer à un compartiment. Pour plus d'informations sur les définitions de service de stockage, reportez-vous à la section "Définitions des services de stockage". Pour plus d'informations sur la gestion des performances, reportez-vous à la section "Gestion des performances". Depuis ONTAP 9.8, lorsque vous provisionnez le stockage, la QoS est activée par défaut. Vous pouvez désactiver QoS ou choisir une règle de QoS personnalisée lors du processus de provisionnement ou ultérieurement.
- Si vous configurez la hiérarchisation de la capacité locale, vous créez des compartiments et des utilisateurs dans une VM de stockage des données, et non dans la VM de stockage du système où se trouve le serveur S3.
- Pour l'accès client à distance, vous devez configurer des compartiments dans une VM de stockage compatible S3. Si vous créez un compartiment dans une machine virtuelle de stockage non compatible S3, il sera uniquement disponible pour le Tiering local.
- À partir de ONTAP 9.14.1, vous pouvez "Créez un compartiment sur un agrégat en miroir ou sans miroir dans une configuration MetroCluster".
- Pour l'interface de ligne de commandes, lorsque vous créez un compartiment, deux options de provisionnement sont disponibles :
  - Laissez ONTAP Select les agrégats sous-jacents et les composants FlexGroup (par défaut)
    - ONTAP crée et configure un volume FlexGroup pour le premier compartiment en sélectionnant automatiquement les agrégats. Il sélectionne automatiquement le niveau de service le plus élevé disponible pour votre plateforme, ou vous pouvez spécifier le niveau de service de stockage. Tout compartiment supplémentaire que vous ajoutez ultérieurement dans la VM de stockage aura le même volume FlexGroup sous-jacent.
    - Vous pouvez également indiquer si le compartiment sera utilisé pour le Tiering, dans ce cas, ONTAP tente de sélectionner un support économique avec des performances optimales pour les données hiérarchisées.
  - Vous sélectionnez les agrégats sous-jacents et les composants FlexGroup (nécessite des options de commande avec privilèges avancés) : vous pouvez sélectionner manuellement les agrégats sur lesquels le compartiment et le volume FlexGroup contenant doivent être créés, puis spécifier le nombre de composants sur chaque agrégat. Lors de l'ajout de compartiments supplémentaires :
    - Si vous spécifiez les agrégats et les composants pour un nouveau compartiment, un nouveau FlexGroup est créé pour ce nouveau compartiment.
    - Si vous ne spécifiez pas d'agrégats ni de composants pour un nouveau compartiment, le nouveau compartiment est ajouté à un FlexGroup existant. Voir Gestion des volumes FlexGroup pour en savoir plus.

      Lorsque vous spécifiez des agrégats et des composants lors de la création d'un compartiment, aucun groupe de règles de QoS, n'est appliqué par défaut ou personnalisé. Vous pouvez le faire plus tard avec le `vserver object-store-server bucket modify` commande.

  Voir "vserver object-store-server bucket modify" pour en savoir plus.

Remarque : si vous utilisez des compartiments à partir de Cloud Volumes ONTAP, vous devez utiliser la procédure CLI. Il est fortement recommandé de sélectionner manuellement les agrégats sous-jacents pour s'assurer qu'ils n'utilisent qu'un seul nœud. L'utilisation d'agrégats des deux nœuds peut avoir un impact sur les performances, car les nœuds se trouvent dans des zones de disponibilité séparées géographiquement et sont donc sujets aux problèmes de latence.

Créez des compartiments S3 avec l'interface de ligne de commandes de ONTAP

1. Si vous prévoyez de sélectionner vous-même les agrégats et les composants FlexGroup, définissez le niveau de privilège sur Avancé (sinon, le niveau de privilège admin est suffisant) : `set -privilege advanced`
2. Création d'un compartiment :

   `vserver object-store-server bucket create -vserver` *`svm_name`* `-bucket` *`bucket_name`* `[-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

   Le nom de la VM de stockage peut être soit une VM de stockage de données, soit `Cluster` (Nom de la machine virtuelle de stockage du système) si vous configurez la hiérarchisation locale.

   Si vous n'indiquez aucune option, ONTAP crée un compartiment de 800 Go avec un niveau de service défini sur le niveau le plus élevé disponible pour votre système.

   Si vous souhaitez que ONTAP crée un compartiment en fonction de la performance ou de l'utilisation, choisissez l'une des options suivantes :

   - niveau de service

     Incluez le `-storage-service-level` option avec l'une des valeurs suivantes : `value`, `performance`, ou `extreme`.

   - tiering

     Incluez le `-used-as-capacity-tier true` option.

     Pour spécifier les agrégats sur lesquels créer le volume FlexGroup sous-jacent, utilisez les options suivantes :

   - Le `-aggr-list` Le paramètre spécifie la liste des agrégats à utiliser pour les composants de volume FlexGroup.

     Chaque entrée de la liste crée un composant sur l'agrégat spécifié. Vous pouvez spécifier un agrégat plusieurs fois afin d'avoir plusieurs composants créés sur l'agrégat.

   Pour assurer des performances prévisibles sur l'ensemble du volume FlexGroup, tous les agrégats doivent utiliser les mêmes configurations de type de disque et de groupe RAID.

   - Le `-aggr-list-multiplier` le paramètre spécifie le nombre de fois pour effectuer l'itération sur les agrégats répertoriés avec le `-aggr-list` Paramètre lors de la création d'un volume FlexGroup.

     La valeur par défaut du `-aggr-list-multiplier` le paramètre est 4.

3. Ajout d'une « policy group » QoS le cas échéant :

   `vserver object-store-server bucket modify -bucket` *`bucket_name`* `-qos-policy -group` *`qos_policy_group`*

4. Vérification de la création de compartiment :

   `vserver object-store-server bucket show [-instance]`

Exemple

L'exemple suivant illustre la création d'un compartiment pour la machine virtuelle de stockage `vs1` de taille `1TB` et spécifier l'agrégat :

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

Création de compartiments S3 avec System Manager

1. Ajoutez un nouveau compartiment à une machine virtuelle de stockage compatible S3.
   a. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**.
   b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.
      - Si vous cliquez sur **Enregistrer** à ce stade, un compartiment est créé avec les paramètres par défaut suivants :
        - L'accès au compartiment n'est accordé à aucun utilisateur, sauf si des règles de groupes sont déjà en vigueur.

          Vous ne devez pas utiliser l'utilisateur root S3 pour gérer le stockage objet ONTAP et partager ses autorisations, car il dispose d'un accès illimité au magasin d'objets. Créez plutôt un utilisateur ou un groupe avec les privilèges d'administration que vous attribuez.

        - Niveau de qualité de service (performance) le plus élevé disponible pour votre système
      - Cliquez sur **Enregistrer** pour créer un compartiment avec ces valeurs par défaut.

Configurer des autorisations et restrictions supplémentaires

Vous pouvez cliquer sur **plus d'options** pour configurer les paramètres de verrouillage d'objet, les autorisations utilisateur et le niveau de performances lorsque vous configurez le compartiment, ou vous pouvez modifier ces paramètres ultérieurement.

Si vous prévoyez d'utiliser le stockage d'objets S3 pour le Tiering FabricPool, choisissez **use pour le Tiering** (utilisez des supports à faible coût avec des performances optimales pour les données hiérarchisées) plutôt que un niveau de service de performance.

Si vous souhaitez activer la gestion des versions de vos objets pour une récupération ultérieure, sélectionnez **Activer la gestion des versions**. La gestion des versions est activée par défaut si vous activez le verrouillage des objets sur le compartiment. Pour plus d'informations sur la gestion des versions d'objet, reportez-vous à la section "Gestion des versions dans des compartiments S3 pour Amazon".

À partir de la version 9.14.1, le verrouillage des objets est pris en charge par les compartiments S3. Le verrouillage des objets S3 nécessite une licence SnapLock standard. Cette licence est incluse avec "ONTAP One". Avant ONTAP One, la licence SnapLock était incluse dans le bundle sécurité et conformité. Le bundle sécurité et conformité n'est plus proposé, mais reste valide. Bien qu'ils ne soient pas encore requis, les clients existants peuvent choisir de le faire "Passez à ONTAP One". Si vous activez le verrouillage d'objet sur un compartiment, vous devez "Vérifiez qu'une licence SnapLock est installée". Si aucune licence SnapLock n'est installée, vous devez le faire "installer" avant de pouvoir activer le verrouillage des objets. Une fois que vous avez vérifié que la licence SnapLock est installée, pour protéger les objets de votre compartiment contre la suppression ou l'écrasement, sélectionnez **Activer le verrouillage d'objet**. Le verrouillage peut être activé sur

l'ensemble des versions d'objets ou sur des versions spécifiques, et uniquement lorsque l'horloge de conformité SnapLock est initialisée pour les nœuds de cluster. Voici la procédure à suivre :

1. Si l'horloge de conformité SnapLock n'est pas initialisée sur un nœud du cluster, le bouton **initialiser horloge de conformité SnapLock** apparaît. Cliquez sur **initialiser horloge de conformité SnapLock** pour initialiser l'horloge de conformité SnapLock sur les nœuds du cluster.
2. Sélectionnez le mode **Governance** pour activer un verrouillage basé sur le temps qui autorise les autorisations *Write Once, Read Many (WORM)* sur les objets. Même en mode *Governance*, les objets peuvent être supprimés par les utilisateurs administrateurs disposant d'autorisations spécifiques.
3. Sélectionnez le mode **conformité** si vous souhaitez affecter des règles plus strictes de suppression et de mise à jour des objets. Dans ce mode de verrouillage d'objet, les objets ne peuvent être expirés qu'à la fin de la période de conservation spécifiée. À moins qu'une période de conservation ne soit spécifiée, les objets restent verrouillés indéfiniment.
4. Spécifiez la durée de conservation du verrou en jours ou en années si vous souhaitez que le verrouillage soit effectif pendant une certaine période.

> Le verrouillage s'applique aux compartiments S3 avec et sans version. Le verrouillage d'objet ne s'applique pas aux objets NAS.

Vous pouvez configurer les paramètres de protection et d'autorisation, ainsi que le niveau de service de performances du compartiment.

> Vous devez avoir déjà créé un utilisateur et des groupes avant de configurer les autorisations.

Pour plus d'informations, reportez-vous à la section "Créer un miroir pour le nouveau godet".

Vérifier l'accès au godet

Sur les applications client S3 (ONTAP S3 ou une application tierce externe), vous pouvez vérifier votre accès au nouveau compartiment en saisissant les informations suivantes :

- Certificat CA de serveur S3.
- La clé d'accès et la clé secrète de l'utilisateur.
- Nom de domaine complet du serveur S3 et nom de compartiment.

Créez un compartiment sur un agrégat en miroir ou sans miroir dans une configuration MetroCluster

À partir de ONTAP 9.14.1, vous pouvez provisionner un compartiment sur un agrégat en miroir ou sans miroir dans des configurations MetroCluster FC et IP.

Description de la tâche

- Par défaut, les compartiments sont provisionnés sur les agrégats en miroir.
- Les mêmes instructions de provisionnement que celles de la section "Créer un compartiment" S'applique à la création d'un compartiment dans un environnement MetroCluster.
- Les fonctionnalités de stockage objet S3 suivantes sont **non** prises en charge dans les environnements MetroCluster :
  - SnapMirror S3

- Gestion du cycle de vie des compartiments S3
- Verrouillage d'objet S3 en mode **Compliance**

  Le verrouillage d'objet S3 en mode **gouvernance** est pris en charge.

- Tiering FabricPool local

Avant de commencer

Un SVM contenant un serveur S3 doit déjà exister.

Processus de création de compartiments

CLI

1. Si vous prévoyez de sélectionner vous-même les agrégats et les composants FlexGroup, définissez le niveau de privilège sur Avancé (sinon, le niveau de privilège admin est suffisant) : `set -privilege advanced`
2. Création d'un compartiment :

   `vserver object-store-server bucket create -vserver <svm_name> -bucket <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates true/false]`

   Réglez le `-use-mirrored-aggregates` option à `true` ou `false` selon que vous souhaitez utiliser un agrégat en miroir ou sans miroir.

   Par défaut, le `-use-mirrored-aggregates` l'option est définie sur `true`.

   - Le nom du SVM doit être un SVM de données.
   - Si vous n'indiquez aucune option, ONTAP crée un compartiment de 800 Go avec un niveau de service défini sur le niveau le plus élevé disponible pour votre système.
   - Si vous souhaitez que ONTAP crée un compartiment en fonction de la performance ou de l'utilisation, choisissez l'une des options suivantes :
     - niveau de service

       Incluez le `-storage-service-level` option avec l'une des valeurs suivantes : `value`, `performance`, ou `extreme`.

     - tiering

       Incluez le `-used-as-capacity-tier true` option.
   - Pour spécifier les agrégats sur lesquels créer le volume FlexGroup sous-jacent, utilisez les options suivantes :
     - Le `-aggr-list` Le paramètre spécifie la liste des agrégats à utiliser pour les composants de volume FlexGroup.

       Chaque entrée de la liste crée un composant sur l'agrégat spécifié. Vous pouvez spécifier un agrégat plusieurs fois afin d'avoir plusieurs composants créés sur l'agrégat.

   Pour assurer des performances prévisibles sur l'ensemble du volume FlexGroup, tous les agrégats doivent utiliser les mêmes configurations de type de disque et de groupe RAID.

   - Le `-aggr-list-multiplier` le paramètre spécifie le nombre de fois pour effectuer l'itération sur les agrégats répertoriés avec le `-aggr-list` Paramètre lors de la création d'un volume FlexGroup.

     La valeur par défaut du `-aggr-list-multiplier` le paramètre est 4.
3. Ajout d'une « policy group » QoS le cas échéant :

   `vserver object-store-server bucket modify -bucket *bucket_name* -qos-policy-group *qos_policy_group*`

4. Vérification de la création de compartiment :

```
vserver object-store-server bucket show [-instance]
```

Exemple

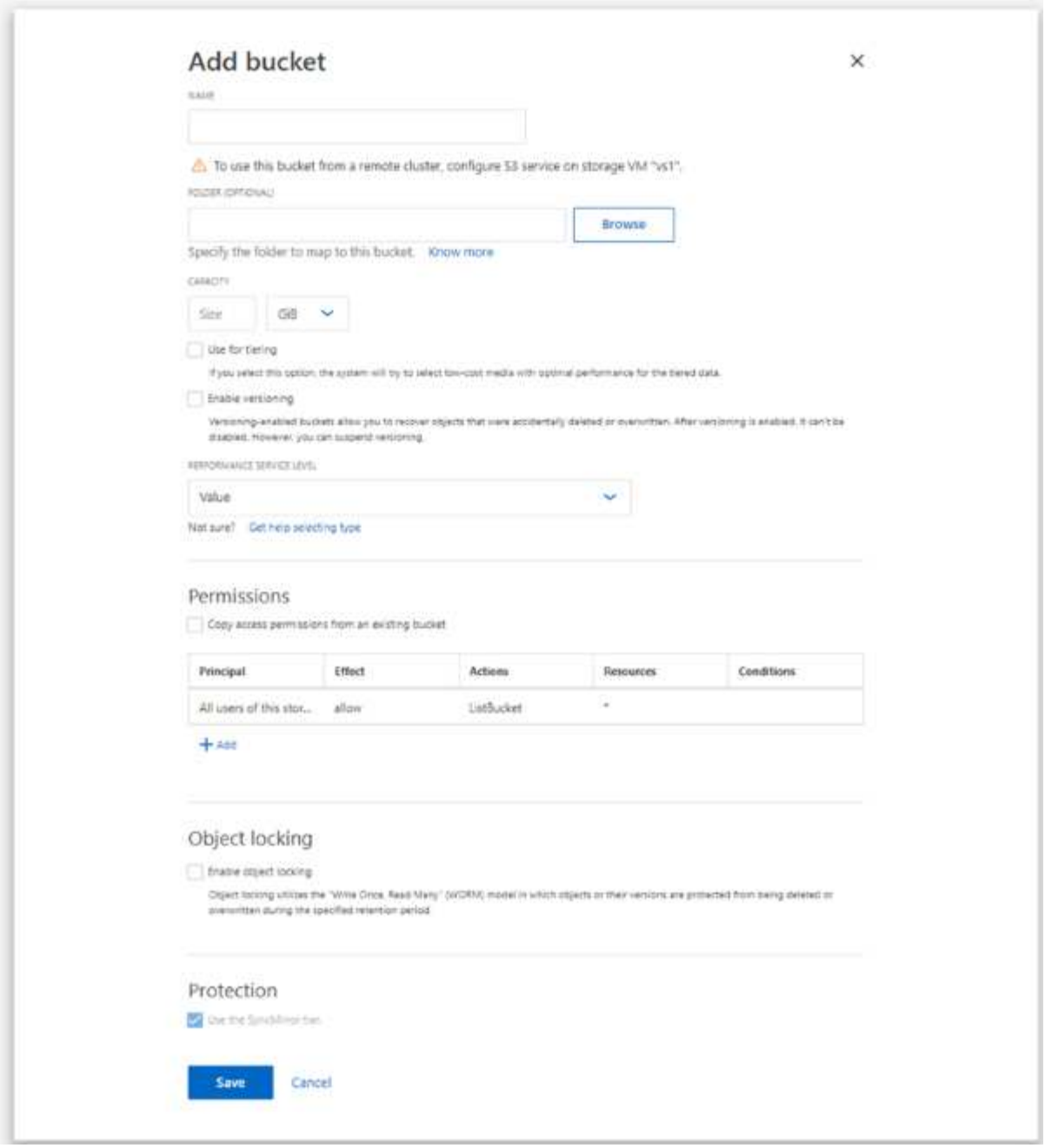
L'exemple suivant illustre la création d'un compartiment pour le SVM vs1 de 1 To sur un agrégat en miroir :

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

System Manager

1. Ajoutez un nouveau compartiment à une machine virtuelle de stockage compatible S3.
   a. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**.
   b. Entrez un nom, sélectionnez la machine virtuelle de stockage, puis entrez une taille.

      Par défaut, le compartiment est provisionné sur un agrégat en miroir. Si vous souhaitez créer un compartiment sur un agrégat sans miroir, sélectionnez **plus d'options** et décochez la case **utiliser le niveau SyncMirror** sous **protection**, comme illustré dans l'image suivante :



- Si vous cliquez sur **Enregistrer** à ce stade, un compartiment est créé avec les paramètres par défaut suivants :
  - L'accès au compartiment n'est accordé à aucun utilisateur, sauf si des règles de groupes sont déjà en vigueur.

> Vous ne devez pas utiliser l'utilisateur root S3 pour gérer le stockage objet ONTAP et partager ses autorisations, car il dispose d'un accès illimité au magasin d'objets. Créez plutôt un utilisateur ou un groupe avec les privilèges d'administration que vous attribuez.

  - Niveau de qualité de service (performance) le plus élevé disponible pour votre système
- Vous pouvez cliquer sur **plus d'options** pour configurer les autorisations utilisateur et le niveau de performances lorsque vous configurez le compartiment, ou vous pouvez modifier ces paramètres ultérieurement.

- Vous devez avoir déjà créé des utilisateurs et des groupes avant d'utiliser **plus d'options** pour configurer leurs autorisations.
- Si vous prévoyez d'utiliser le stockage d'objets S3 pour le Tiering FabricPool, choisissez **use pour le Tiering** (utilisez des supports à faible coût avec des performances optimales pour les données hiérarchisées) plutôt que un niveau de service de performance.

2. Pour les applications client S3, un autre système ONTAP ou une application tierce externe, vérifiez l'accès au nouveau compartiment en saisissant les éléments suivants :
   - Certificat CA de serveur S3.
   - Clé d'accès et clé secrète de l'utilisateur.
   - Nom de domaine complet du serveur S3 et nom de compartiment.

Créez une règle de gestion du cycle de vie des compartiments

À partir de ONTAP 9.13.1, vous pouvez créer des règles de gestion du cycle de vie pour gérer les cycles de vie des objets dans vos compartiments S3. Vous pouvez définir des règles de suppression pour des objets spécifiques d'un compartiment et, par le biais de ces règles, ces objets de compartiment expirent. Cela vous permet de respecter les exigences de conservation et de gérer efficacement l'ensemble du stockage objet S3.

Si le verrouillage des objets est activé pour vos objets de compartiment, les règles de gestion du cycle de vie pour l'expiration des objets ne seront pas appliquées aux objets verrouillés. Pour plus d'informations sur le verrouillage des objets, reportez-vous à la section "Créer un compartiment".

Avant de commencer

Un SVM compatible S3 contenant un serveur S3 et un compartiment doivent déjà exister. Voir "Création d'un SVM pour S3" pour en savoir plus.

Description de la tâche

Lors de la création de vos règles de gestion du cycle de vie, vous pouvez appliquer les actions de suppression suivantes à vos objets de compartiment :

- Suppression des versions actuelles - cette action expire les objets identifiés par la règle. Si la gestion des versions est activée sur le compartiment, S3 rend tous les objets expirés indisponibles. Si la gestion des versions n'est pas activée, cette règle supprime définitivement les objets. L'action CLI est `Expiration`.
- Suppression de versions non actuelles - cette action indique quand S3 peut supprimer définitivement des objets non actuels. L'action CLI est `NoncurrentVersionExpiration`.
- Suppression des marqueurs de suppression expirés - cette action supprime les marqueurs de suppression d'objet expirés. Dans les compartiments avec gestion des versions, les objets avec des marqueurs de suppression deviennent les versions actuelles des objets. Les objets ne sont pas supprimés et aucune action ne peut être effectuée sur eux. Ces objets deviennent expirés lorsqu'aucune version n'est associée à ces objets. L'action CLI est `Expiration`.
- Suppression des téléchargements partitionnés incomplets : cette action définit une durée maximale (en jours) pendant laquelle vous souhaitez autoriser les téléchargements partitionnés à rester en cours. Après quoi, ils sont supprimés. L'action CLI est `AbortIncompleteMultipartUpload`.

La procédure à suivre dépend de l'interface que vous utilisez. Avec ONTAP 9.13,1, vous devez utiliser

l'interface de ligne de commandes. Depuis ONTAP 9.14.1, vous pouvez également utiliser System Manager.

Gérez les règles de gestion du cycle de vie avec l'interface de ligne de commande

À partir de ONTAP 9.13.1, vous pouvez utiliser l'interface de ligne de commandes ONTAP pour créer des règles de gestion du cycle de vie et faire expirer les objets de vos compartiments S3.

Avant de commencer

Pour l'interface de ligne de commandes, vous devez définir les champs requis pour chaque type d'action d'expiration lors de la création d'une règle de gestion du cycle de vie des compartiments. Ces champs peuvent être modifiés après la création initiale. Le tableau suivant affiche les champs uniques pour chaque type d'action.

Type d'action	Champs uniques
NonCurrentVersionExpiation	• `-non-curr-days` - Nombre de jours après lesquels les versions non actuelles seront supprimées • `-new-non-curr-versions` - Nombre de dernières versions non actuelles à conserver
Expiration	• `-obj-age-days` - Nombre de jours depuis la création, après lesquels la version actuelle des objets peut être supprimée • `-obj-exp-date` - Date précise à laquelle les objets doivent expirer • `-expired-obj-del-markers` - Nettoyage des marqueurs de suppression d'objet
AbortIncompleMultipartUpload	• `-after-initiation-days` - Nombre de jours d'initiation, après quoi le téléchargement peut être abandonné

Pour que la règle de gestion du cycle de vie des compartiments ne s'applique qu'à un sous-ensemble d'objets spécifique, les administrateurs doivent définir chaque filtre lors de la création de la règle. Si ces filtres ne sont pas définis lors de la création de la règle, la règle s'applique à tous les objets du compartiment.

Tous les filtres peuvent être modifiés après la création initiale *sauf* pour les éléments suivants :

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

Étapes

1. Utilisez le `vserver object-store-server bucket lifecycle-management-rule create` commande contenant les champs requis pour votre type d'action d'expiration pour créer votre règle de gestion du cycle de vie des compartiments.

Exemple

La commande suivante crée une règle de gestion du cycle de vie des compartiments NonCurrentVersionExexpiration :

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

Exemple

La commande suivante crée une règle de gestion du cycle de vie des compartiments d'expiration :

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

Exemple

La commande suivante crée une règle de gestion du cycle de vie des compartiments AbortIncompletteMultipartUpload :

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

Gérez les règles de gestion du cycle de vie avec System Manager

Depuis ONTAP 9.14.1, vous pouvez faire expirer les objets S3 à l'aide de System Manager. Vous pouvez ajouter, modifier et supprimer des règles de gestion du cycle de vie pour vos objets S3. En outre, vous pouvez importer une règle de cycle de vie créée pour un compartiment et l'utiliser pour les objets d'un autre compartiment. Vous pouvez désactiver une règle active et l'activer ultérieurement.

Ajoutez une règle de gestion du cycle de vie

1. Cliquez sur **stockage > compartiments**.
2. Sélectionnez le compartiment pour lequel vous souhaitez spécifier la règle d'expiration.
3. Cliquez sur le bouton ⋮ Et sélectionnez **gérer les règles de cycle de vie**.
4. Cliquez sur **Ajouter > règle de cycle de vie**.

5. Sur la page Ajouter une règle de cycle de vie, ajoutez le nom de la règle.
6. Définissez la portée de la règle, que vous souhaitiez qu'elle s'applique à tous les objets du compartiment ou à des objets spécifiques. Si vous souhaitez spécifier des objets, ajoutez au moins l'un des critères de filtre suivants :
   a. Préfixe : spécifiez le préfixe des noms de clés d'objet auxquels la règle doit s'appliquer. Il s'agit généralement du chemin ou du dossier de l'objet. Vous pouvez entrer un préfixe par règle. À moins qu'un préfixe valide ne soit fourni, la règle s'applique à tous les objets d'un compartiment.
   b. Balises : spécifiez jusqu'à trois paires de clés et de valeurs (balises) pour les objets auxquels la règle doit s'appliquer. Seules les clés valides sont utilisées pour le filtrage. La valeur est facultative. Cependant, si vous ajoutez des valeurs, assurez-vous d'ajouter uniquement des valeurs valides pour les clés correspondantes.
   c. Taille : vous pouvez limiter la portée entre la taille minimale et la taille maximale des objets. Vous pouvez entrer l'une ou l'autre des valeurs ou les deux. L'unité par défaut est MIB.
7. Spécifiez l'action :
   a. **Expire la version actuelle des objets** : définissez une règle pour rendre tous les objets actuels définitivement indisponibles après un nombre de jours spécifique depuis leur création ou à une date spécifique. Cette option n'est pas disponible si l'option **Supprimer les marqueurs de suppression d'objet expiré** est sélectionnée.
   b. **Supprimer définitivement les versions non actuelles** : Indiquez le nombre de jours après lesquels la version devient non actuelle, puis peut être supprimée, et le nombre de versions à conserver.
   c. **Supprimer les marqueurs de suppression d'objets expirés** : sélectionnez cette action pour supprimer des objets avec des marqueurs de suppression expirés, c'est-à-dire supprimer des marqueurs sans objet courant associé.

      Cette option devient indisponible lorsque vous sélectionnez l'option **expire la version actuelle des objets** qui supprime automatiquement tous les objets après la période de rétention. Cette option devient également indisponible lorsque des balises d'objet sont utilisées pour le filtrage.

   d. **Supprimer les téléchargements partiaux incomplets** : définit le nombre de jours après lesquels les téléchargements partiaux incomplets doivent être supprimés. Si les téléchargements partitionnés en cours échouent dans la période de conservation spécifiée, vous pouvez supprimer les téléchargements partitionnés incomplets. Cette option devient indisponible lorsque des balises d'objet sont utilisées pour le filtrage.
   e. Cliquez sur **Enregistrer**.

Importer une règle de cycle de vie

1. Cliquez sur **stockage > compartiments**.
2. Sélectionnez le compartiment pour lequel vous souhaitez importer la règle d'expiration.
3. Cliquez sur le bouton ⋮ Et sélectionnez **gérer les règles de cycle de vie**.
4. Cliquez sur **Ajouter > Importer une règle**.
5. Sélectionnez le compartiment à partir duquel vous souhaitez importer la règle. Les règles de gestion du cycle de vie définies pour le compartiment sélectionné s'affichent.
6. Sélectionnez la règle à importer. Vous avez la possibilité de sélectionner une règle à la fois, la sélection par défaut étant la première règle.
7. Cliquez sur **Importer**.

Modifier, supprimer ou désactiver une règle

Vous pouvez uniquement modifier les actions de gestion du cycle de vie associées à la règle. Si la règle a été filtrée avec des balises d'objet, les options **Supprimer les marqueurs de suppression d'objet expirés** et **Supprimer les téléchargements partitionnés incomplets** ne sont pas disponibles.

Lorsque vous supprimez une règle, celle-ci ne s'applique plus aux objets précédemment associés.

1. Cliquez sur **stockage > compartiments**.
2. Sélectionnez le compartiment pour lequel vous souhaitez modifier, supprimer ou désactiver la règle de gestion du cycle de vie.
3. Cliquez sur le bouton ⋮ Et sélectionnez **gérer les règles de cycle de vie**.
4. Sélectionnez la règle requise. Vous pouvez modifier et désactiver une règle à la fois. Vous pouvez supprimer plusieurs règles à la fois.
5. Sélectionnez **Modifier**, **Supprimer** ou **Désactiver** et terminez la procédure.

Créez un utilisateur S3

Une autorisation utilisateur est requise sur tous les magasins d'objets ONTAP pour limiter la connectivité aux clients autorisés.

Avant de commencer.

Une VM de stockage compatible avec S3 doit déjà exister.

Description de la tâche

Un utilisateur S3 peut se voir accorder l'accès à n'importe quel compartiment d'une VM de stockage. Lorsque vous créez un utilisateur S3, une clé d'accès et une clé secrète sont également générées pour l'utilisateur. Ils doivent être partagés avec l'utilisateur avec le nom de domaine complet du magasin d'objets et du nom du compartiment. Les clés d'un utilisateur S3 peuvent être affichées à l'aide du `vserver object-store-server user show` commande.

Vous pouvez accorder des autorisations d'accès spécifiques aux utilisateurs S3 dans une stratégie de compartiment ou une stratégie de serveur d'objets.

> ⓘ Lorsque vous créez un nouveau serveur de magasin d'objets, ONTAP crée un utilisateur root (UID 0), qui est un utilisateur privilégié ayant accès à tous les compartiments. Au lieu d'administrer ONTAP S3 en tant qu'utilisateur root, NetApp recommande la création d'un rôle d'utilisateur admin avec des privilèges spécifiques.

CLI

1. Création d'un utilisateur S3 :
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - L'ajout d'un commentaire est facultatif.
   - À partir de ONTAP 9.14.1, vous pouvez définir la période pendant laquelle la clé sera valide dans le `-key-time-to-live` paramètre. Vous pouvez ajouter la période de conservation dans ce format pour indiquer la période après laquelle la clé d'accès expire :
     `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
     Par exemple, si vous souhaitez entrer une période de conservation d'un jour, de deux heures, de trois minutes et de quatre secondes, entrez la valeur comme `P1DT2H3M4S`. Sauf indication contraire, la clé est valide pour une durée indéterminée.

     L'exemple ci-dessous crée un utilisateur avec un nom `sm_user1` Sur la machine virtuelle de stockage `vs0`, avec une période de conservation des clés d'une semaine.

   ```
   vserver object-store-server user create -vserver vs0 -user sm_user1
   -key-time-to-live P1W
   ```

2. Veillez à enregistrer la clé d'accès et la clé secrète. Elles seront requises pour l'accès à partir des clients S3.

System Manager

1. Cliquez sur **stockage > machines virtuelles de stockage**. Sélectionnez la VM de stockage à laquelle vous devez ajouter un utilisateur, sélectionnez **Paramètres**, puis cliquez sur Sous S3.
2. Pour ajouter un utilisateur, cliquez sur **utilisateurs > Ajouter**.
3. Entrez un nom pour l'utilisateur.
4. À partir de ONTAP 9.14.1, vous pouvez spécifier la période de conservation des clés d'accès créées pour l'utilisateur. Vous pouvez spécifier la période de conservation en jours, heures, minutes ou secondes, après laquelle les clés expirent automatiquement. Par défaut, la valeur est définie sur `0` cela indique que la clé est indéfiniment valide.
5. Cliquez sur **Enregistrer**. L'utilisateur est créé et une clé d'accès et une clé secrète sont générées pour l'utilisateur.
6. Téléchargez ou enregistrez la clé d'accès et la clé secrète. Elles seront requises pour l'accès à partir des clients S3.

Étapes suivantes

- Création ou modification de groupes S3

Création ou modification de groupes S3

Vous pouvez simplifier l'accès au compartiment en créant des groupes d'utilisateurs avec les autorisations d'accès appropriées.

Avant de commencer

Les utilisateurs S3 d'un SVM compatible avec S3 doivent déjà exister.

Description de la tâche

Les utilisateurs d'un groupe S3 peuvent accéder à n'importe quel compartiment d'une SVM, mais pas dans plusieurs SVM. Les autorisations d'accès aux groupes peuvent être configurées de deux façons :

- Au niveau du godet

  Une fois que vous avez créé un groupe d'utilisateurs S3, vous spécifiez les autorisations de groupe dans les instructions de règles de compartiment et elles ne s'appliquent qu'à ce compartiment.

- Au niveau de la SVM

  Après la création d'un groupe d'utilisateurs S3, vous spécifiez les noms des règles de serveur d'objets dans la définition de groupe. Ces stratégies déterminent les compartiments et l'accès des membres du groupe.

System Manager

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 groupe : sélectionnez **groupes**, puis **Ajouter**.
3. Entrez un nom de groupe et sélectionnez-le dans une liste d'utilisateurs.
4. Vous pouvez sélectionner une stratégie de groupe existante ou en ajouter une maintenant, ou vous pouvez ajouter une ultérieurement.

CLI

1. Création d'un groupe S3 :
   `vserver object-store-server group create -vserver` *`svm_name`* `-name` *`group_name`* `-users` *`user_name`*`\(s\)` `[-policies` *`policy_names`*`] [-comment` *`text`*`\]`
   Le `-policies` l'option peut être omise dans les configurations avec un seul compartiment dans un magasin d'objets ; le nom du groupe peut être ajouté à la politique de compartiment.
   Le `-policies` vous pouvez l'ajouter ultérieurement avec le `vserver object-store-server group modify` commande après la création de règles de serveur de stockage objet

Régénérer les clés et modifier leur période de conservation

Les clés d'accès et les clés secrètes sont automatiquement générées lors de la création de l'utilisateur pour l'activation de l'accès client S3. Vous pouvez régénérer des clés pour un utilisateur si une clé est périmée ou compromise.

Pour plus d'informations sur la génération de clés d'accès, reportez-vous à la section "Créez un utilisateur S3".

CLI

1. Régénérer les clés d'accès et les clés secrètes pour un utilisateur en exécutant `vserver object-store-server user regenerate-keys` commande.
2. Par défaut, les clés générées sont valides indéfiniment. À partir de 9.14.1, vous pouvez modifier leur période de conservation, après laquelle les clés expirent automatiquement. Vous pouvez ajouter la période de conservation au format suivant :
   `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
   Par exemple, si vous souhaitez entrer une période de conservation d'un jour, de deux heures, de trois minutes et de quatre secondes, entrez la valeur comme `P1DT2H3M4S`.

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name
   -user user -key-time-to-live 0
   ```

3. Enregistrez les clés d'accès et les clés secrètes. Elles seront requises pour l'accès à partir des clients S3.

System Manager

1. Cliquez sur **Storage > Storage VM**, puis sélectionnez la VM de stockage.
2. Dans l'onglet **Paramètres**, cliquez sur Dans la mosaïque **S3**.
3. Dans l'onglet **Users**, vérifiez qu'il n'y a pas de clé d'accès ou que la clé a expiré pour l'utilisateur.
4. Si vous devez régénérer la clé, cliquez sur En regard de l'utilisateur, cliquez sur **régénérer la clé**.
5. Par défaut, les clés générées sont valides pour une durée indéterminée. À partir de 9.14.1, vous pouvez modifier leur période de conservation, après laquelle les clés expirent automatiquement. Entrez la période de conservation en jours, heures, minutes ou secondes.
6. Cliquez sur **Enregistrer**. La clé est régénérée. Toute modification de la période de conservation des clés prend effet immédiatement.
7. Téléchargez ou enregistrez la clé d'accès et la clé secrète. Elles seront requises pour l'accès à partir des clients S3.

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"
}
```


Activez l’accès client au stockage objet S3

Activation de l’accès ONTAP S3 pour le Tiering FabricPool distant

Pour qu’ONTAP S3 puisse être utilisé comme Tier de capacité FabricPool distante (cloud), l’administrateur ONTAP S3 doit fournir des informations sur la configuration du serveur S3 à l’administrateur du cluster ONTAP distant.

Description de la tâche

Pour configurer des tiers cloud FabricPool, vous devez disposer des informations suivantes sur le serveur S3 :

- Nom du serveur (FQDN)
- nom du compartiment
- Certificat CA
- touche d’accès
- mot de passe (clé d’accès secrète)

En outre, la configuration réseau suivante est requise :

- Il doit y avoir une entrée pour le nom d’hôte du serveur ONTAP S3 distant dans le serveur DNS configuré pour le SVM d’administration, notamment le nom de domaine complet du serveur S3 et les adresses IP sur

les LIF.

- Les LIFs intercluster doivent être configurées sur le cluster local, bien que le peering de cluster n'est pas nécessaire.

Consultez la documentation d'FabricPool sur la configuration d'ONTAP S3 en tant que Tier cloud.

"Gestion des niveaux de stockage à l'aide de FabricPool"

Activez l'accès ONTAP S3 pour le Tiering FabricPool local

Pour qu'ONTAP S3 puisse être utilisé comme Tier de capacité FabricPool locale, vous devez définir un magasin d'objets en fonction du compartiment que vous avez créé, puis relier le magasin d'objets à un agrégat de Tier de performance pour créer une FabricPool.

Avant de commencer

Vous devez disposer du nom du serveur ONTAP S3 et d'un nom de compartiment, et le serveur S3 doit avoir été créé à l'aide des LIFs de cluster (avec le `-vserver Cluster` paramètre).

Description de la tâche

La configuration du magasin d'objets contient des informations sur le Tier de capacité locale, notamment les noms de compartiment et de serveur S3 et les exigences d'authentification.

Une fois créée, une configuration de magasin d'objets ne doit pas être associée à un autre magasin d'objets ou compartiment. Vous pouvez créer plusieurs compartiments pour les tiers locaux, mais il n'est pas possible de créer plusieurs magasins d'objets dans un seul compartiment.

Aucune licence FabricPool n'est requise pour un niveau de capacité locale.

Étapes

1. Créez le magasin d'objets pour le Tier de capacité locale :

   ```
   storage aggregate object-store config create -object-store-name store_name
   -ipspace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
   -name bucket_name -access-key access_key -secret-password password
   ```

   - Le `-container-name` Est le compartiment S3 que vous avez créé.
   - Le `-access-key` Paramètre autorise les requêtes vers le serveur ONTAP S3.
   - Le `-secret-password` Le paramètre (clé d'accès secrète) authentifie les requêtes vers le serveur ONTAP S3.
   - Vous pouvez définir le `-is-certificate-validation-enabled` paramètre à `false` Pour désactiver la vérification du certificat pour ONTAP S3.

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyLocalObjStore -ipspace Cluster -provider-type
   ONTAP_S3 -server s3.example.com
   -container-name bucket1 -access-key myS3key -secret-password myS3pass
   ```

2. Afficher et vérifier les informations de configuration du magasin d'objets :

   `storage aggregate object-store config show`

3. Facultatif : pour connaître le volume de données inactives d'un volume, suivez les étapes de la section "Détermination de la quantité de données inactives d'un volume grâce au reporting des données inactives".

   Vous savez combien de données inactives d'un volume peut vous aider à choisir l'agrégat à utiliser pour le Tiering FabricPool local.

4. Attacher le magasin d'objets à un agrégat :

   `storage aggregate object-store attach -aggregate` *`aggr_name`* `-object-store-name` *`store_name`*

   Vous pouvez utiliser le `allow-flexgroup` **`true`** Possibilité de connecter des agrégats contenant des composants de volume FlexGroup

   ```
   cluster1::> storage aggregate object-store attach
   -aggregate aggr1 -object-store-name MyLocalObjStore
   ```

5. Afficher les informations du magasin d'objets et vérifier que le magasin d'objets attaché est disponible :

   `storage aggregate object-store show`

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   aggr1        MyLocalObjStore      available
   ```

Activation de l'accès client à partir d'une application S3

Pour que les applications client S3 puissent accéder au serveur ONTAP S3, l'administrateur ONTAP S3 doit fournir des informations de configuration à l'utilisateur S3.

Avant de commencer

L'application client S3 doit être capable d'authentifier auprès du serveur ONTAP S3 à l'aide des versions de signature AWS suivantes :

- Signature version 4, ONTAP 9.8 et ultérieure
- Signature version 2, ONTAP 9.11.1 et ultérieure

Les autres versions de signatures ne sont pas prises en charge par ONTAP S3.

L'administrateur ONTAP S3 doit avoir créé des utilisateurs S3 et leur accorder des autorisations d'accès, en tant qu'utilisateurs individuels ou en tant que membre de groupe, dans la stratégie de compartiment ou la stratégie de serveur de stockage objet.

L’application du client S3 doit être capable de résoudre le nom du serveur ONTAP S3, ce qui requiert que l’administrateur ONTAP S3 fournit le nom du serveur S3 (FQDN) et des adresses IP pour les LIF du serveur S3.

Description de la tâche

Pour accéder à un compartiment ONTAP S3, un utilisateur de l’application client S3 saisit les informations fournies par l’administrateur ONTAP S3.

Depuis la version ONTAP 9.9.1, le serveur ONTAP S3 prend en charge les fonctionnalités de client AWS suivantes :

- métadonnées d’objet définies par l’utilisateur

  Un ensemble de paires clé-valeur peut être attribué aux objets en tant que métadonnées lors de leur création à l’aide DE PUT (ou POST). Lorsqu’une opération GET/HEAD est exécutée sur l’objet, les métadonnées définies par l’utilisateur sont renvoyées avec les métadonnées du système.

- balisage d’objets

  Un ensemble distinct de paires clé-valeur peut être attribué en tant que balises pour classer les objets. Contrairement aux métadonnées, les balises sont créées et lues avec les API REST indépendamment de l’objet. Elles sont implémentées lors de la création d’objets ou à tout moment après.

  Pour permettre aux clients d’obtenir et de mettre des informations de marquage, les actions `GetObjectTagging`, `PutObjectTagging`, et `DeleteObjectTagging` doivent être autorisées à l’aide des règles de compartiment ou de groupe.

Pour plus d’informations, consultez la documentation AWS S3.

Étapes

1. Authentifiez l’application client S3 avec le serveur ONTAP S3 en saisissant le nom du serveur S3 et le certificat de l’autorité de certification.
2. Authentifier un utilisateur sur l’application client S3 en saisissant les informations suivantes :
   - Nom du serveur S3 (FQDN) et nom du compartiment
   - clé d’accès et clé secrète de l’utilisateur

Définitions des services de stockage

ONTAP inclut des services de stockage prédéfinis mappés sur les facteurs de performance minimaux correspondants.

L’ensemble réel de services de stockage disponibles dans un cluster ou un SVM est déterminé par le type de stockage qui constitue un agrégat dans la SVM.

Le tableau ci-dessous montre comment les facteurs de performance minimale sont mappés aux services de stockage prédéfinis :

Service de stockage	IOPS attendues (SLA)	IOPS en pic (SLO)	Nombre minimal d'IOPS pour le volume	Latence estimée	Les IOPS attendues sont-elles appliquées ?
valeur	128 par To	512 par To	75	17 ms.	Sur AFF: Oui Sinon : non
performances	2048 par To	4096 par To	500	2 ms.	Oui.
extrême	6144 par To	12288 par To	1000	1 ms.	Oui.

Le tableau ci-dessous définit le niveau de service de stockage disponible pour chaque type de support ou nœud :

Support ou nœud	Niveau de service du stockage disponible
Disque	valeur
Disque de machine virtuelle	valeur
LUN FlexArray	valeur
Hybride	valeur
Flash à capacité optimisée	valeur
Disque SSD (Solid-State Drive) - non AFF	valeur
Performance optimisée Flash - SSD (AFF)	extreme, performance, value

Informations sur le copyright

Informations sur les marques commerciales