Référence

NetApp Backup and Recovery

NetApp
November 04, 2025

Sommaire

Référence

Stratégies dans SnapCenter comparées à celles de NetApp Backup and Recovery

Il existe certaines différences entre les stratégies utilisées dans SnapCenter et celles utilisées dans NetApp Backup and Recovery qui peuvent avoir un impact sur ce que vous voyez après l'importation de ressources et de stratégies depuis SnapCenter.

Niveaux de planification

SnapCenter utilise les niveaux de planification suivants :

- **Horaire** : Plusieurs heures et minutes avec n'importe quelle heure (0-23) et n'importe quelle minute (0-60).
- **Quotidien** : Option permettant de répéter tous les nombres de jours définis, par exemple, tous les 3 jours.
- **Hebdomadaire** : du dimanche au lundi, avec la possibilité d'effectuer un instantané le jour 1 de la semaine ou sur plusieurs jours de la semaine.
- **Mensuel** : de janvier à décembre, avec la possibilité de jouer un ou plusieurs jours spécifiques chaque mois, par exemple le 7.

NetApp Backup and Recovery utilise les niveaux de planification suivants, qui sont légèrement différents :

- **Toutes les heures** : effectue des instantanés uniquement à des intervalles de 15 minutes, par exemple, des intervalles d'une heure ou de 15 minutes inférieurs à 60.
- **Quotidien** : Heures de la journée (0-23) avec heure de début par exemple à 10h00 avec une option pour effectuer toutes les heures.
- **Hebdomadaire** : Jour de la semaine (du dimanche au lundi) avec possibilité de jouer sur 1 jour ou plusieurs jours. C'est la même chose que SnapCenter.
- **Mensuel** : Dates du mois (0-30) avec une heure de début à plusieurs dates du mois.
- **Annuel** : Mensuel. Cela correspond au mensuel de SnapCenter.

Plusieurs politiques dans SnapCenter avec le même niveau de planification

Vous pouvez attribuer plusieurs politiques avec le même niveau de planification à une ressource dans SnapCenter. Cependant, NetApp Backup and Recovery ne prend pas en charge plusieurs stratégies sur une ressource qui utilise le même niveau de planification.

Exemple : Si vous utilisez trois stratégies (pour les données, le journal et le journal des snapshots) dans SnapCenter, après la migration depuis SnapCenter, NetApp Backup and Recovery utilise une seule stratégie au lieu des trois.

Horaires quotidiens SnapCenter importés

NetApp Backup and Recovery ajuste les planifications SnapCenter comme suit :

- Si la planification SnapCenter est définie sur une durée inférieure ou égale à 7 jours, NetApp Backup and Recovery définit la planification sur une durée hebdomadaire. Certains instantanés sont ignorés au cours de la semaine.

Exemple : Si vous disposez d'une stratégie quotidienne SnapCenter avec un intervalle répétitif tous les 3 jours à partir du lundi, NetApp Backup and Recovery définit la planification sur une base hebdomadaire le lundi, le jeudi et le dimanche. Certains jours seront sautés car ce n'est pas exactement tous les 3 jours.

- Si la planification SnapCenter est définie sur une durée supérieure à 7 jours, NetApp Backup and Recovery définit la planification sur mensuelle. Certains instantanés seront ignorés au cours du mois.

  Exemple : Si vous disposez d'une stratégie quotidienne SnapCenter avec un intervalle répétitif tous les 10 jours à partir du 2 du mois, NetApp Backup and Recovery, après la migration, définit la planification sur une base mensuelle les 2, 12 et 22 du mois. NetApp Backup and Recovery saute quelques jours au cours du mois prochain.

Horaires horaires SnapCenter importés

Les politiques horaires SnapCenter avec des intervalles répétitifs supérieurs à une heure sont converties en politique quotidienne dans NetApp Backup and Recovery.

Toute politique horaire avec des intervalles répétitifs qui ne sont pas un facteur de 24 (par exemple 5, 7, etc.) ignorera certains instantanés dans une journée.

Exemple : Si vous disposez d'une stratégie horaire SnapCenter avec un intervalle répétitif toutes les 5 heures à partir de 1 h 00 du matin, NetApp Backup and Recovery (après la migration) définira la planification sur quotidienne avec des intervalles de 5 heures à 1 h 00, 6 h 00, 11 h 00, 16 h 00 et 21 h 00. Certaines heures seront ignorées, après 21h00, il devrait être 2h00 du matin pour se répéter toutes les 5 heures, mais ce sera toujours 1h00 du matin.

Conservation des journaux à partir des politiques SnapCenter

Si vous disposez d'une ressource dans SnapCenter avec plusieurs stratégies, NetApp Backup and Recovery utilise l'ordre de priorité suivant pour attribuer la valeur de conservation des journaux :

- Pour les stratégies « Sauvegarde complète avec sauvegarde du journal » et « Journal uniquement » dans SnapCenter, NetApp Backup and Recovery utilise la valeur de rétention de la stratégie Journal uniquement.
- Pour les stratégies « Sauvegarde complète avec journal uniquement » et « Complète et journal » dans SnapCenter, NetApp Backup and Recovery utilise la valeur de rétention du journal uniquement.
- Pour « Sauvegarde complète et journal » plus « Sauvegarde complète » dans SnapCenter, NetApp Backup and Recovery utilise la valeur de rétention « Sauvegarde complète et journal ».
- Si vous ne disposez que d'une sauvegarde complète dans SnapCenter, NetApp Backup and Recovery n'active pas la sauvegarde du journal.

Conservation des sauvegardes des journaux

SnapCenter prend en charge plusieurs valeurs de rétention pour les stratégies sur une ressource. NetApp Backup and Recovery ne prend en charge qu'une seule valeur de rétention par ressource.

Nombre de rétentions à partir des politiques SnapCenter

Si vous disposez d'une ressource avec une protection secondaire activée dans SnapCenter avec plusieurs volumes sources, plusieurs volumes de destination et plusieurs relations SnapMirror , NetApp Backup and Recovery utilise uniquement le nombre de rétention de la première stratégie.

Exemple : Si vous disposez d'une stratégie SnapCenter avec un nombre de rétention de 5 et d'une autre stratégie avec un nombre de rétention de 10, NetApp Backup and Recovery utilise le nombre de rétention de 5.

Étiquettes SnapMirror à partir des politiques SnapCenter

SnapCenter conserve les étiquettes SnapMirror pour chaque politique après la migration, même si le niveau change.

Exemple : Une politique horaire de SnapCenter peut changer en quotidienne dans NetApp Backup and Recovery. Cependant, les étiquettes SnapMirror restent les mêmes après la migration.

Rôles de gestion des identités et des accès (IAM) de NetApp Backup and Recovery

NetApp Backup and Recovery utilise la gestion des identités et des accès (IAM) pour gérer l'accès de chaque utilisateur à des fonctionnalités et actions spécifiques.

Pour en savoir plus sur les rôles IAM spécifiques à NetApp Backup and Recovery, reportez-vous à "Rôles de NetApp Backup and Recovery dans la NetApp Console" .

Restaurer les données de configuration de NetApp Backup and Recovery sur un site sombre

Lorsque vous utilisez NetApp Backup and Recovery sur un site sans accès Internet, appelé *mode privé*, les données de configuration de NetApp Backup and Recovery sont sauvegardées dans le compartiment StorageGRID ou ONTAP S3 où vos sauvegardes sont stockées. Si vous rencontrez un problème avec le système hôte de l'agent de console, vous pouvez déployer un nouvel agent de console et restaurer les données critiques de NetApp Backup and Recovery .

Cette procédure s'applique uniquement aux données de volume ONTAP .

Lorsque vous utilisez NetApp Backup and Recovery dans un environnement SaaS avec l'agent de console déployé chez votre fournisseur de cloud ou sur votre propre hôte connecté à Internet, le système sauvegarde et protège toutes les données de configuration importantes dans le cloud. Si vous rencontrez un problème avec l'agent de console, créez un nouvel agent de console et ajoutez vos systèmes. Les détails de la sauvegarde sont automatiquement restaurés.

Il existe deux types de données sauvegardées :

- Base de données de NetApp Backup and Recovery : contient une liste de tous les volumes, fichiers de sauvegarde, politiques de sauvegarde et informations de configuration.
- Fichiers de catalogue indexés - contiennent des index détaillés utilisés pour la fonctionnalité de recherche et de restauration qui rendent vos recherches très rapides et efficaces lorsque vous recherchez des données de volume que vous souhaitez restaurer.

Ces données sont sauvegardées une fois par jour à minuit et un maximum de 7 copies de chaque fichier sont conservées. Si l'agent de console gère plusieurs systèmes ONTAP sur site, les fichiers de NetApp Backup and

Recovery sont stockés dans le compartiment du système qui a été activé en premier.

Aucune donnée de volume n'est jamais incluse dans la base de données NetApp Backup and Recovery ou dans les fichiers de catalogue indexés.

Restaurer les données de NetApp Backup and Recovery vers un nouvel agent de console

Si votre agent de console sur site cesse de fonctionner, vous devrez installer un nouvel agent de console, puis restaurer les données de NetApp Backup and Recovery sur le nouvel agent de console.

Vous devrez effectuer les tâches suivantes pour remettre votre système NetApp Backup and Recovery en état de fonctionnement :

- Installer un nouvel agent de console
- Restaurer la base de données de NetApp Backup and Recovery
- Restaurer les fichiers du catalogue indexé
- Redécouvrez tous vos systèmes ONTAP et StorageGRID sur site sur l'interface utilisateur de la NetApp Console

Après avoir vérifié que votre système fonctionne, créez de nouveaux fichiers de sauvegarde.

Ce dont vous aurez besoin

Vous devrez accéder aux sauvegardes de base de données et d'index les plus récentes à partir du compartiment StorageGRID ou ONTAP S3 où vos fichiers de sauvegarde sont stockés :

- Fichier de base de données MySQL de NetApp Backup and Recovery

  Ce fichier se trouve à l'emplacement suivant dans le bucket `netapp-backup-<GUID>/mysql_backup/` , et il s'appelle `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- Fichier zip de sauvegarde du catalogue indexé

  Ce fichier se trouve à l'emplacement suivant dans le bucket `netapp-backup-<GUID>/catalog_backup/` , et il s'appelle `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

Installer un nouvel agent de console sur un nouvel hôte Linux local

Lors de l'installation d'un nouvel agent de console, téléchargez la même version du logiciel que l'agent d'origine. Les modifications apportées à la base de données NetApp Backup and Recovery peuvent empêcher les nouvelles versions du logiciel de fonctionner avec les anciennes sauvegardes de base de données. Tu peux "mettre à niveau le logiciel de l'agent de la console vers la version la plus récente après la restauration de la base de données de sauvegarde" .

1. "Installer l'agent de console sur un nouvel hôte Linux local"
2. Connectez-vous à la console à l'aide des informations d'identification de l'utilisateur administrateur que vous venez de créer.

Restaurer la base de données de NetApp Backup and Recovery

1. Copiez la sauvegarde MySQL de l'emplacement de sauvegarde vers le nouvel hôte de l'agent de console. Nous utiliserons le nom de fichier d'exemple « CBS_DB_Backup_23_05_2023.sql » ci-dessous.
2. Copiez la sauvegarde dans le conteneur Docker MySQL à l'aide de l'une des commandes suivantes, selon que vous utilisez un conteneur Docker ou Podman :

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Accédez au shell du conteneur MySQL à l'aide de l'une des commandes suivantes, selon que vous utilisez un conteneur Docker ou Podman :

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. Dans le shell du conteneur, déployez « env ».
5. Vous aurez besoin du mot de passe de la base de données MySQL, copiez donc la valeur de la clé « MYSQL_ROOT_PASSWORD ».
6. Restaurez la base de données MySQL de NetApp Backup and Recovery à l'aide de la commande suivante :

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. Vérifiez que la base de données MySQL de NetApp Backup and Recovery a été restaurée correctement à l'aide des commandes SQL suivantes :

```
mysql -u root -p cloud_backup
```

8. Entrez le mot de passe.

```
mysql> show tables;
mysql> select * from volume;
```

9. Vérifiez que les volumes affichés correspondent bien à ceux de votre environnement d'origine.

Restaurer les fichiers du catalogue indexé

1. Copiez le fichier zip de sauvegarde du catalogue indexé (nous utiliserons le nom de fichier d'exemple « Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip ») de l'emplacement de sauvegarde vers le nouvel hôte de l'agent de console dans le dossier « /opt/application/netapp/cbs ».
2. Décompressez le fichier « Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip » à l'aide de la commande suivante :

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. Exécutez la commande **ls** pour vous assurer que le dossier « catalogdb1 » a été créé avec les sous-dossiers « changes » et « snapshots » en dessous.

Découvrez vos clusters ONTAP et vos systèmes StorageGRID

1. "Découvrez tous les systèmes ONTAP sur site"qui étaient disponibles dans votre environnement précédent. Cela inclut le système ONTAP que vous avez utilisé comme serveur S3.
2. "Découvrez vos systèmes StorageGRID".

Configurer les détails de l'environnement StorageGRID

Ajoutez les détails du système StorageGRID associé à vos systèmes ONTAP tels qu'ils ont été configurés lors de la configuration de l'agent de console d'origine à l'aide de l' "API de la NetApp Console" .

Les informations suivantes s'appliquent aux installations en mode privé à partir de NetApp Console 3.9.xx. Pour les versions plus anciennes, utilisez la procédure suivante : "Sauvegarde Cloud DarkSite : sauvegarde et restauration de MySQL et du catalogue indexé" .

Vous devrez effectuer ces étapes pour chaque système qui sauvegarde des données sur StorageGRID.

1. Extrayez le jeton d'autorisation à l'aide de l'API oauth/token suivante.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

   Alors que l'adresse IP, le nom d'utilisateur et les mots de passe sont des valeurs personnalisées, le nom du compte ne l'est pas. Le nom du compte est toujours « account-DARKSITE1 ». De plus, le nom d'utilisateur doit utiliser un nom au format e-mail.

   Cette API renverra une réponse comme celle-ci. Vous pouvez récupérer le jeton d'autorisation comme indiqué ci-dessous.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```


2. Extrayez l'ID système et l'ID X-Agent à l'aide de l'API tenancy/external/resource.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

Cette API renverra une réponse comme celle-ci. La valeur sous « resourceIdentifier » désigne l'*ID de l'environnement de travail* et la valeur sous « agentId » désigne *x-agent-id*.


```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```


3. Mettez à jour la base de données NetApp Backup and Recovery avec les détails du système StorageGRID associé aux systèmes. Assurez-vous de saisir le nom de domaine complet du StorageGRID, ainsi que la clé d'accès et la clé de stockage comme indiqué ci-dessous :

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

Vérifier les paramètres de NetApp Backup and Recovery

1. Sélectionnez chaque système ONTAP et cliquez sur **Afficher les sauvegardes** à côté du service de sauvegarde et de récupération dans le panneau de droite.

   Vous devriez voir toutes les sauvegardes créées pour vos volumes.

2. Depuis le tableau de bord de restauration, sous la section Rechercher et restaurer, cliquez sur **Paramètres d'indexation**.

   Assurez-vous que les systèmes sur lesquels le catalogage indexé était précédemment activé restent activés.

3. À partir de la page Rechercher et restaurer, exécutez quelques recherches de catalogue pour confirmer que la restauration du catalogue indexé a été effectuée avec succès.

Niveaux de stockage d'archives AWS pris en charge avec NetApp Backup and Recovery

NetApp Backup and Recovery prend en charge deux classes de stockage d'archivage S3 et la plupart des régions.

Pour basculer vers et depuis les versions de l'interface utilisateur NetApp Backup and Recovery , reportez-vous à"Passer à l'interface utilisateur précédente de NetApp Backup and Recovery" .

Classes de stockage d'archivage S3 prises en charge pour NetApp Backup and Recovery

Lorsque les fichiers de sauvegarde sont initialement créés, ils sont stockés dans le stockage S3 *Standard*. Ce niveau est optimisé pour stocker des données rarement consultées, mais qui vous permet également d'y accéder immédiatement. Après 30 jours, les sauvegardes passent à la classe de stockage S3 *Standard-Infrequent Access* pour réduire les coûts.

Si vos clusters sources exécutent ONTAP 9.10.1 ou une version ultérieure, vous pouvez choisir de hiérarchiser les sauvegardes vers le stockage *S3 Glacier* ou *S3 Glacier Deep Archive* après un certain nombre de jours (généralement plus de 30 jours) pour une optimisation supplémentaire des coûts. Vous pouvez définir cette valeur sur « 0 » ou sur 1 à 999 jours. Si vous le définissez sur « 0 » jours, vous ne pourrez pas le modifier ultérieurement sur 1 à 999 jours.

Les données de ces niveaux ne sont pas accessibles immédiatement en cas de besoin et nécessiteront un coût de récupération plus élevé. Vous devez donc tenir compte de la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Consultez la section sur cette page concernant la restauration des données à partir du stockage d'archives.

- Si vous ne sélectionnez aucun niveau d'archivage dans votre première politique de sauvegarde lors de l'activation de NetApp Backup and Recovery, *S3 Glacier* sera votre seule option d'archivage pour les politiques futures.
- Si vous sélectionnez *S3 Glacier* dans votre première politique de sauvegarde, vous pouvez alors passer au niveau *S3 Glacier Deep Archive* pour les futures politiques de sauvegarde de ce cluster.
- Si vous sélectionnez *S3 Glacier Deep Archive* dans votre première politique de sauvegarde, ce niveau sera le seul niveau d'archivage disponible pour les futures politiques de sauvegarde pour ce cluster.

Notez que lorsque vous configurez NetApp Backup and Recovery avec ce type de règle de cycle de vie, vous ne devez configurer aucune règle de cycle de vie lors de la configuration du bucket dans votre compte AWS.

"En savoir plus sur les classes de stockage S3".

Restaurer les données à partir du stockage d'archives

Bien que le stockage des fichiers de sauvegarde plus anciens dans un stockage d'archives soit beaucoup moins coûteux que le stockage Standard ou Standard-IA, l'accès aux données d'un fichier de sauvegarde dans un stockage d'archives pour les opérations de restauration prendra plus de temps et coûtera plus cher.

Combien coûte la restauration des données d'Amazon S3 Glacier et d'Amazon S3 Glacier Deep Archive ?

Vous pouvez choisir entre 3 priorités de restauration lors de la récupération de données depuis Amazon S3 Glacier et 2 priorités de restauration lors de la récupération de données depuis Amazon S3 Glacier Deep Archive. S3 Glacier Deep Archive coûte moins cher que S3 Glacier :

Niveau d'archivage	Restaurer la priorité et le coût		
	Haut	**Standard**	**Faible**
Glacier S3	Récupération la plus rapide, coût le plus élevé	Récupération plus lente, coût moindre	Récupération la plus lente, coût le plus bas
Archives S3 Glacier Deep		Récupération plus rapide, coût plus élevé	Récupération plus lente, coût le plus bas

Chaque méthode a des frais de récupération par Go et des frais par demande différents. Pour connaître les tarifs détaillés de S3 Glacier par région AWS, visitez le "Page de tarification Amazon S3" .

Combien de temps faudra-t-il pour restaurer mes objets archivés dans Amazon S3 Glacier ?

Le temps de restauration total est composé de deux parties :

- **Temps de récupération** : Le temps nécessaire pour récupérer le fichier de sauvegarde de l'archive et le placer dans le stockage standard. C'est ce qu'on appelle parfois le temps de « réhydratation ». Le temps de récupération est différent selon la priorité de restauration que vous choisissez.

Niveau d'archivage	Restaurer la priorité et le temps de récupération		
	Haut	**Standard**	**Faible**
Glacier S3	3 à 5 minutes	3 à 5 heures	5 à 12 heures
Archives S3 Glacier Deep		12 heures	48 heures

- **Temps de restauration** : Le temps nécessaire pour restaurer les données à partir du fichier de sauvegarde dans le stockage standard. Cette fois, ce n'est pas différent de l'opération de restauration typique directement à partir du stockage standard, lorsque vous n'utilisez pas de niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Amazon S3 Glacier et S3 Glacier Deep Archive, reportez-vous à "la FAQ d'Amazon sur ces classes de stockage" .

Niveaux d'accès aux archives Azure pris en charge avec NetApp Backup and Recovery

NetApp Backup and Recovery prend en charge un niveau d'accès aux archives Azure et la plupart des régions.

Pour basculer vers et depuis les versions de l'interface utilisateur NetApp Backup and Recovery , reportez-vous à"Passer à l'interface utilisateur précédente de NetApp Backup and Recovery" .

Niveaux d'accès Azure Blob pris en charge pour NetApp Backup and Recovery

Lorsque les fichiers de sauvegarde sont initialement créés, ils sont stockés dans le niveau d'accès *Cool*. Ce niveau est optimisé pour stocker des données rarement consultées, mais auxquelles il est possible d'accéder immédiatement en cas de besoin.

Si vos clusters sources exécutent ONTAP 9.10.1 ou une version ultérieure, vous pouvez choisir de hiérarchiser

les sauvegardes du stockage *Cool* vers *Azure Archive* après un certain nombre de jours (généralement plus de 30 jours) pour une optimisation supplémentaire des coûts. Les données de ce niveau ne sont pas accessibles immédiatement en cas de besoin et nécessiteront un coût de récupération plus élevé. Vous devez donc tenir compte de la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Consultez la section sur cette page concernant la restauration des données à partir du stockage d'archives.

Notez que lorsque vous configurez NetApp Backup and Recovery avec ce type de règle de cycle de vie, vous ne devez configurer aucune règle de cycle de vie lors de la configuration du conteneur dans votre compte Azure.

"En savoir plus sur les niveaux d'accès Azure Blob".

Restaurer les données à partir du stockage d'archives

Bien que le stockage d'anciens fichiers de sauvegarde dans un stockage d'archives soit beaucoup moins coûteux que le stockage Cool, l'accès aux données d'un fichier de sauvegarde dans Azure Archive pour les opérations de restauration prendra plus de temps et coûtera plus cher.

Combien coûte la restauration des données à partir d'Azure Archive ?

Vous pouvez choisir deux priorités de restauration lors de la récupération de données à partir d'Azure Archive :

- **Élevé** : Récupération la plus rapide, coût plus élevé
- **Standard** : Récupération plus lente, coût inférieur

Chaque méthode a des frais de récupération par Go et des frais par demande différents. Pour connaître les tarifs détaillés d'Azure Archive par région Azure, visitez le "Page de tarification Azure" .

La priorité élevée n'est pas prise en charge lors de la restauration des données d'Azure vers les systèmes StorageGRID .

Combien de temps faudra-t-il pour restaurer mes données archivées dans Azure Archive ?

Le temps de restauration se compose de deux parties :

- **Heure de récupération** : le temps nécessaire pour récupérer le fichier de sauvegarde archivé à partir d'Azure Archive et le placer dans le stockage Cool. C'est ce qu'on appelle parfois le temps de « réhydratation ». Le temps de récupération est différent selon la priorité de restauration que vous choisissez :
  - **Élevé** : < 1 heure
  - **Standard** : < 15 heures
- **Temps de restauration** : Le temps nécessaire pour restaurer les données à partir du fichier de sauvegarde dans le stockage Cool. Cette fois, ce n'est pas différent de l'opération de restauration typique directement à partir du stockage Cool - lorsque vous n'utilisez pas de niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Azure Archive, reportez-vous à "cette FAQ Azure" .

Niveaux de stockage d’archives Google pris en charge avec NetApp Backup and Recovery

NetApp Backup and Recovery prend en charge une classe de stockage d’archivage Google et la plupart des régions.

Pour basculer vers et depuis les versions de l’interface utilisateur NetApp Backup and Recovery , reportez-vous à"Passer à l’interface utilisateur précédente de NetApp Backup and Recovery" .

Classes de stockage d’archivage Google prises en charge pour NetApp Backup and Recovery

Lorsque les fichiers de sauvegarde sont initialement créés, ils sont stockés dans le stockage *Standard*. Ce niveau est optimisé pour stocker des données rarement consultées, mais qui vous permet également d’y accéder immédiatement.

Si votre cluster sur site utilise ONTAP 9.12.1 ou une version ultérieure, vous pouvez choisir de hiérarchiser les sauvegardes plus anciennes vers le stockage *Archive* dans l’interface utilisateur NetApp Backup and Recovery après un certain nombre de jours (généralement plus de 30 jours) pour une optimisation supplémentaire des coûts. Les données de ce niveau nécessiteront un coût de récupération plus élevé. Vous devez donc tenir compte de la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Consultez la section sur cette page concernant la restauration des données à partir du stockage d’archives.

Notez que lorsque vous configurez NetApp Backup and Recovery avec ce type de règle de cycle de vie, vous ne devez configurer aucune règle de cycle de vie lors de la configuration du bucket dans votre compte Google.

"En savoir plus sur les classes de stockage Google".

Restaurer les données à partir du stockage d’archives

Bien que le stockage d’anciens fichiers de sauvegarde dans le stockage d’archives soit beaucoup moins coûteux que le stockage standard, l’accès aux données d’un fichier de sauvegarde dans le stockage d’archives pour les opérations de restauration prendra un peu plus de temps et coûtera plus cher.

Combien coûte la restauration des données de Google Archive ?

Pour connaître les tarifs détaillés de Google Cloud Storage par région, visitez le "Page de tarification de Google Cloud Storage" .

Combien de temps faudra-t-il pour restaurer mes objets archivés dans Google Archive ?

Le temps de restauration total est composé de deux parties :

- **Temps de récupération** : Le temps nécessaire pour récupérer le fichier de sauvegarde de l’archive et le placer dans le stockage standard. C’est ce qu’on appelle parfois le temps de « réhydratation ». Contrairement aux solutions de stockage « les plus froides » fournies par d’autres fournisseurs de cloud, vos données sont accessibles en quelques millisecondes.
- **Temps de restauration** : Le temps nécessaire pour restaurer les données à partir du fichier de sauvegarde dans le stockage standard. Cette fois, ce n’est pas différent de l’opération de restauration typique directement à partir du stockage standard, lorsque vous n’utilisez pas de niveau d’archivage.