Guide de l’administrateur cloud sur l’interface utilisateur Web NetBackup™

Version 10.3

VERITAS™

Dernière mise à jour : 2023-12-28

Mentions légales

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

Support technique

Le support technique entretient globalement les centres de support. Tous les services de support sont fournis conformément à votre contrat de support et aux politiques de support technique en vigueur dans l'entreprise. Pour plus d'informations sur les offres de support et comment contacter le support technique, rendez-vous sur notre site web :

https://www.veritas.com/support

Vous pouvez gérer les informations de votre compte Veritas à l'adresse URL suivante :

https://my.veritas.com

Si vous avez des questions concernant un contrat de support existant, envoyez un message électronique à l'équipe d'administration du contrat de support de votre région :

Monde (sauf Japon)	CustomerCare@veritas.com
Japon	CustomerCare_Japan@veritas.com

Documentation

Assurez-vous que vous utilisez la version actuelle de la documentation. Chaque document affiche la date de la dernière mise à jour sur la page 2. La documentation la plus récente est disponible sur le site web de Veritas :

https://sort.veritas.com/documents

Commentaires sur la documentation

Vos commentaires sont importants pour nous. Suggérez des améliorations ou rapportez des erreurs ou des omissions dans la documentation. Indiquez le titre et la version du document, le titre du chapitre et le titre de la section du texte que vous souhaitez commenter. Envoyez le commentaire à :

NB.docs@veritas.com

Vous pouvez également voir des informations sur la documentation ou poser une question sur le site de la communauté Veritas :

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) est un site Web qui fournit des informations et des outils permettant d'automatiser et de simplifier certaines tâches administratives chronophages. Selon le produit, SORT vous aide à préparer les installations et les mises à jour, à identifier les risques dans vos data centers et à améliorer l'efficacité opérationnelle. Pour voir quels services et quels outils SORT fournit pour votre produit, consultez la fiche de données :

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Table des matières

Chapitre 1

Gestion et protection des biens dans le cloud

Ce chapitre traite des sujets suivants :

- Protéger des applications sur le cloud avec les snapshots cohérents au niveau des applications
- Protection des biens PaaS

À propos de la protection des biens cloud

NetBackup permet désormais de protéger vos charges de travail dans le cloud. La structure de protection des données cloud s'appuie sur l'infrastructure Snapshot Manager pour accélérer l'évolutivité des fournisseurs cloud. À partir de NetBackup version 8.3, Snapshot Manager peut protéger des biens dans les clouds AWS, Azure, Azure Stack Hub et GCP.

Le tableau suivant décrit les tâches correspondantes.

Tableau 1-1 Configuration de la protection pour les biens cloud

Tâche	Description
Avant de commencer, assurez-vous que vous disposez des autorisations appropriées.	Pour gérer et protéger les biens cloud dans l'interface utilisateur web, vous devez posséder le rôle d'administrateur de charge de travail ou des autorisations similaires. L'administrateur de sécurité NetBackup peut gérer vos autorisations de rôle au niveau de chaque bien, du compte ou de l'abonnement, ou encore au niveau d'un fournisseur cloud. Consultez le Guide de l'administrateur de l'interface utilisateur Web NetBackup. **Remarque :** pour la gestion des applications hébergées, vous devez disposer des autorisations de gestion des biens et de gestion des plans de protection.
Déployer Snapshot Manager	Installez Snapshot Manager dans votre environnement. Se reporter à "Ajout de Snapshot Manager" à la page 12. Consultez les limites de Snapshot Manager et NetBackup. Se reporter à "Restrictions et remarques" à la page 10.
	Enregistrez le Snapshot Manager dans NetBackup. Consultez le *Guide de l'administrateur de NetBackup Snapshot Client*.

Tâche	Description
Ajout d'une configuration	Tous les fournisseurs cloud pris en charge sont affichés dans l'interface utilisateur Web. Vous devez ajouter le compte cloud (configurer le plug-in cloud) pour le fournisseur cloud dont vous avez besoin. Vous pouvez créer plusieurs configurations pour chaque fournisseur. Se reporter à "Ajout d'un fournisseur cloud pour Snapshot Manager" à la page 13. Pour Amazon, vous pouvez choisir d'utiliser le rôle IAM. Se reporter à "Rôle IAM pour la configuration AWS" à la page 16.
Découverte de biens	NetBackup récupère les biens cloud appartenant aux comptes cloud qui sont configurés dans NetBackup. Les biens sont renseignés dans la base de données de biens de NetBackup. Par défaut, la découverte de biens a lieu toutes les 2 heures et est configurable. Pour les applications, vous pouvez définir un intervalle de découverte compris entre 15 et 45 minutes. Se reporter à "Découverte de biens sur Snapshot Manager" à la page 17.
Créer un plan de protection	Permet de créer un plan de protection. Un plan de protection sert à planifier les fenêtres de démarrage des sauvegardes. Consultez le Guide de l'administrateur de l'interface utilisateur Web NetBackup. Vous pouvez également configurer le plan de protection pour la réplication de snapshot. Se reporter à "Configuration de la réplication de snapshot AWS" à la page 51.

Tâche	Description
Choisir de protéger une machine virtuelle, une application ou un volume	Pour chaque fournisseur cloud, une liste des biens découverts s'affiche. Ajoutez les biens à un plan de protection. Consultez le Guide de l'administrateur de l'interface utilisateur Web NetBackup. Vous pouvez également choisir de protéger l'application à l'aide de snapshots cohérents au niveau de l'application. Se reporter à "Protéger des applications sur le cloud avec les snapshots cohérents au niveau des applications" à la page 58.
Récupérer les biens cloud	■ Vous pouvez récupérer les biens à l'aide des points de récupération. Se reporter à "Récupération des biens cloud" à la page 92. Se reporter à "Récupération des biens cloud" à la page 92. Se reporter à "Restauration des biens cloud " à la page 101. ■ Vous pouvez également restaurer les biens à l'aide de l'utilitaire d'interface de ligne de commande `nbcloudrestore`. **Remarque :** N'utilisez pas l'interface de ligne de commande `bprestore` pour les restaurations. Consultez le Guide de référence des commandes NetBackup.
Dépannage	Se reporter à "Résolution des problèmes de protection de la charge de travail cloud" à la page 131.

Restrictions et remarques

Tenez compte de ce qui suit pour la protection des charges de travail dans le cloud

- La suppression de l'entrée d'hôte Snapshot Manager et des plug-ins qui y sont associés n'est pas prise en charge dans NetBackup.
  Si vous supprimez des plug-ins qui sont configurés dans NetBackup, vous ne pourrez pas récupérer les images Snapshot Manager associées à ces plug-ins.
- Consultez le *Guide d'installation et de mise à niveau de NetBackup Snapshot Manager* pour plus d'informations sur les fonctions de Snapshot Manager.

- Si vous disposez d'une installation précédente de Snapshot Manager, Veritas recommande de mettre à niveau le serveur Snapshot Manager au lieu de procéder à une réinstallation.
  Si vous réinstallez le serveur Snapshot Manager, vous devez reconfigurer le Snapshot Manager et suivre l'intégralité de la procédure de protection.
- Par défaut, Snapshot Manager est configuré sur le port 443.
- Une fois le serveur Snapshot Manager ajouté, l'ordinateur hôte tente d'utiliser l'adresse IPv6 pour découvrir des biens dans le cloud. Si l'adresse IPV6 se trouve sur l'hôte, l'application est configurée pour l'utiliser. Si aucune adresse IPv6 n'est trouvée, l'adresse IPv4 est utilisée.
- L'audit amélioré n'est pas pris en charge pour Snapshot Manager. Par conséquent, lorsque vous ajoutez ou mettez à jour un Snapshot Manager en tant qu'utilisateur non racine, mais avec des droits administrateur NetBackup, l'utilisateur est affiché comme utilisateur racine lors de l'audit.
- Si vous déployez Snapshot Manager à l'aide du modèle CloudFormation, vous devez utiliser l'adresse IP privée (et non publique) pour enregistrer l'agent sur hôte avec le nœud Snapshot Manager à l'aide de la commande.

Remarque : Veritas recommande d'activer l'espace d'échange sur les serveurs principaux NetBackup utilisés pour exécuter des travaux de sauvegarde à partir d'un snapshot pour des groupes de biens cloud. La taille de l'espace d'échange doit être au moins 1,5 fois supérieure à celle de la mémoire système. S'il est impossible d'activer l'espace d'échange, il est recommandé de disposer de systèmes dotés d'une mémoire plus importante.

Configurer Snapshot Manager dans NetBackup

Vous pouvez ajouter un Snapshot Manager à l'aide de l'interface utilisateur Web NetBackup. À partir de la version 8.3, le Snapshot Manager peut découvrir des biens cloud sur Amazon Web Services et Microsoft Azure Government (États-Unis).

Tenez compte des points importants suivants :

- Vous pouvez associer plusieurs Snapshot Manager à un serveur principal NetBackup, mais vous ne pouvez associer qu'un seul Snapshot Manager à un serveur principal NetBackup.
- Vous pouvez associer plusieurs serveurs de médias à un Snapshot Manager. Seuls les serveurs de médias associés à votre serveur principal NetBackup peuvent être associés à un Snapshot Manager.

- Vous pouvez désormais gérer Snapshot Manager et contrôler la découverte des biens à partir de l'interface utilisateur Web NetBackup, de l'API REST et de l'interface de ligne de commande sans utiliser les interfaces Snapshot Manager.
- Les travaux de sauvegarde à partir d'un snapshot utilisent les serveurs associés au stockage de média NetBackup plutôt que les serveurs de médias associés à Snapshot Manager. Les serveurs associés au stockage de média NetBackup doivent être connectés au Snapshot Manager pour faciliter toutes les opérations liées à Snapshot Manager.

Le tableau suivant décrit les tâches sous-jacentes.

Tableau 1-2 Configuration de Snapshot Manager

Tâche	Description
Ajout d'un Snapshot Manager	Se reporter à "Ajout de Snapshot Manager" à la page 12.
Ajouter des fournisseurs cloud	Pour découvrir des biens sur le Snapshot Manager, vous devez ajouter les fournisseurs cloud. Se reporter à "Ajout d'un fournisseur cloud pour Snapshot Manager" à la page 13.
Découverte de biens sur Snapshot Manager	Vous pouvez découvrir des biens sur le Snapshot Manager.Se reporter à "Découverte de biens sur Snapshot Manager" à la page 17.
Associer des serveurs de médias	Pour décharger des snapshots et des workflows de restauration sur un serveur de médias, vous devez associer ce dernier au Snapshot Manager.Se reporter à "Association de serveurs de médias à un Snapshot Manager" à la page 17.

Ajout de Snapshot Manager

Vous pouvez ajouter Snapshot Manager à l'aide de l'interface utilisateur Web NetBackup.

Remarque : pour effectuer des sauvegardes à partir d'un snapshot, vous devez disposer d'une connectivité bidirectionnelle entre les serveurs Snapshot Manager et NetBackup.

Pour ajouter Snapshot Manager

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Snapshot Manager**.
3. Cliquez sur **Ajouter**.
4. Dans le champ **Snapshot Manager**, entrez l'une des informations suivantes :
   - Nom d'hôte ou adresse IP du Snapshot Manager.
     Le nom d'hôte ou l'adresse IP doit correspondre à celui spécifié lors de la configuration de Snapshot Manager, pendant l'installation de Snapshot Manager.
   - Si le serveur DNS est configuré, entrez le nom de domaine complet du Snapshot Manager.
5. Dans le champ **Port**, entrez le numéro de port du Snapshot Manager.

   La valeur par défaut est 443.
6. Cliquez sur **Enregistrer**.

Ajout d'un fournisseur cloud pour Snapshot Manager

Vous pouvez protéger les biens sur les fournisseurs cloud Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure et Microsoft Azure Stack Hub. À partir de la version 9.0, le Snapshot Manager peut découvrir les charges de travail cloud Amazon Web Services et Microsoft Azure Government (États-Unis).

Pour ajouter un fournisseur cloud pour Snapshot Manager

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Fournisseurs** ou sur **Ajouter** dans la section du fournisseur cloud pour lequel vous souhaitez ajouter une configuration.
3. Saisissez une valeur dans le champ **Nom de configuration**, dans le volet **Ajouter une configuration** .
4. Sélectionnez le serveur **Snapshot Manager** préféré.

5 Entrez les informations requises.

Fournisseur cloud	Paramètre	Description
Microsoft Azure	Type d'informations d'authentification : **principal de service d'application**	
	ID du locataire	L'ID du répertoire Azure Active Directory dans lequel vous avez créé l'application.
	ID du client	ID de l'application.
	Secret key	Clé secrète de l'application.
	Type d'informations d'authentification : **System managed identity**	Activez l'identité gérée par le système sur l'hôte Snapshot Manager dans Azure. **Remarque :** Assignez un rôle à l'identité gérée par le système.
	Type d'informations d'authentification : **identité gérée par l'utilisateur**	
	ID du client	ID de l'identité gérée par l'utilisateur connectée à l'hôte Snapshot Manager.
	Les paramètres suivants s'appliquent à tous les types d'informations d'authentification ci-dessus	
	Regions	Une ou plusieurs régions pour la découverte de biens cloud. **Remarque :** Si vous configurez un cloud gouvernemental, sélectionnez US Gov Arizona, US Gov Texas US ou Gov Virginia.
	Préfixe du groupe de ressources	Chaîne à laquelle vous souhaitez ajouter toutes les ressources d'un groupe de ressources.
	Protéger les biens même si des groupes de ressources préfixés sont introuvables	La case à cocher détermine si les biens sont protégés même s'ils ne sont associés à aucun groupe de ressources.

Fournisseur cloud	Paramètre	Description
Microsoft Azure Stack Hub	*Avec AAD :* **URL du terminal client du gestionnaire de ressources Azure Stack Hub**	URL du terminal client au format suivant, qui permet à Snapshot Manager de se connecter à vos ressources Azure. `https://management.<location>.<FQDN>`
	ID du locataire	L'ID du répertoire Azure Active Directory dans lequel vous avez créé l'application.
	ID du client	ID de l'application.
	Clé secrète	Clé secrète de l'application.
	URL de la ressource d'authentification (facultatif)	URL à laquelle le jeton d'authentification est envoyé.
	À l'aide d'ADFS : **URL du terminal client du gestionnaire de ressources Azure Stack Hub**	URL du terminal client au format suivant, qui permet à Snapshot Manager de se connecter à vos ressources Azure. `https://management.<location>.<FQDN>`
	ID du locataire	L'ID du répertoire Azure Active Directory dans lequel vous avez créé l'application.
	ID du client	ID de l'application.
	Clé secrète	Clé secrète de l'application.
	URL de la ressource d'authentification (facultatif)	URL à laquelle le jeton d'authentification est envoyé.
Amazon AWS **Remarque :** si le Snapshot Manager est configuré avec IAM Config, les options **Clé d'accès** et **Clé secrète** ne sont pas disponibles.	**Clé d'accès**	ID de la clé d'accès. Lorsque cet ID est spécifié avec la clé d'accès secrète, il autorise Snapshot Manager à interagir avec les API AWS.
	Clé secrète	Clé secrète de l'application.
	Régions	Une ou plusieurs régions AWS où découvrir les biens cloud. **Remarque :** Si vous configurez un cloud gouvernemental, sélectionnez us-gov-east-1 ou us-gov-west-1.

Fournisseur cloud	Paramètre	Description
Google Cloud Platform	**ID du projet**	ID du projet à partir duquel les ressources sont gérées. Répertorié comme `project_id` dans le fichier JSON.
	Adresse électronique du client	Adresse électronique de l'ID client. Répertoriée comme `client_email` dans le fichier JSON.
	Clé privée	La clé privée. Répertoriée comme `private_key` dans le fichier JSON. **Remarque :** Vous devez entrer cette clé sans guillemets. N'entrez pas d'espace ni de retour à la ligne au début ou à la fin de la clé.
	Régions	Liste des régions dans lesquelles le fournisseur opère.

6 Entrez les détails de connexion et d'authentification dans le volet **Ajouter une configuration**.

7 Cliquez sur **Enregistrer**.

Les biens sur les fournisseurs cloud sont découverts automatiquement.

Rôle IAM pour la configuration AWS

Si le Snapshot Manager est déployé dans le cloud, vous pouvez configurer AWS pour qu'il utilise le rôle IAM pour l'authentification.

Se reporter à "Ajout d'un fournisseur cloud pour Snapshot Manager" à la page 13.

Avant de poursuivre, assurez-vous que le rôle IAM est configuré dans AWS. Consultez le *Guide d'installation et de mise à niveau de NetBackup Snapshot Manager* pour plus de détails.

Les implémentations suivantes du rôle IAM sont prises en charge :

- Compte source : les biens cloud à protéger se trouvent dans le même compte AWS que Snapshot Manager. Par conséquent, le compte AWS cloud reconnaît le nom du rôle et l'ID du compte AWS ; vous n'avez qu'à sélectionner la région.
- Compte croisé : les biens cloud à protéger se trouvent dans un autre compte AWS que Snapshot Manager. Vous devez donc entrer les informations relatives

au compte et au nom de rôle cibles, ainsi que la région, pour que Snapshot Manager puisse accéder à ces biens.

Vous devez établir une relation de confiance entre les comptes source et cible. Par exemple, s'il s'agit du rôle ARN pour le rôle à utiliser pour configurer le plug-in :

arn:aws:iam::935923755:rôle/TEST_IAM_ROLE

Ainsi, pour configurer le plug-in, fournissez la dernière partie de l'ARN, le nom : *TEST_IAM_ROLE*

Pour plus de détails, consultez les informations portant sur l'*accès aux comptes AWS à l'aide des rôles IAM* dans la documentation d'*Amazon Web Services*.

Association de serveurs de médias à un Snapshot Manager

Vous pouvez utiliser un serveur de médias pour décharger les snapshots et restaurer des travaux de votre cloud. Pour activer cette fonctionnalité, vous devez associer au moins un serveur de médias à un Snapshot Manager. Les serveurs de médias doivent être dans un état actif pour exécuter les travaux de snapshot ou de restauration. Le serveur de médias associé au Snapshot Manager doit également être associé à votre serveur principal NetBackup. Cependant, les travaux de découverte s'exécutent uniquement sur le serveur maître NetBackup.

Pour associer des serveurs de médias à un Snapshot Manager

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Snapshot Manager**.
3. Dans le menu situé en regard du Snapshot Manager, cliquez sur **Paramètres avancés**.
4. Dans l'onglet **Serveur de médias**, sélectionnez le ou les serveurs de médias à associer au Snapshot Manager.
5. Cliquez sur **Enregistrer**.

Découverte de biens sur Snapshot Manager

Après la configuration de vos fournisseurs cloud avec un Snapshot Manager, la découverte automatique de biens dans le cloud se déclenche. Lors des découvertes périodiques, NetBackup extrait les données des biens de Snapshot Manager toutes les deux heures, tandis que Snapshot Manager extrait ces données des configurations des fournisseurs cloud toutes les heures. Si vous désactivez un Snapshot Manager, les biens associés à ce serveur ne sont plus protégés ni synchronisés avec NetBackup.

Si nécessaire, vous pouvez également lancer manuellement la découverte de biens cloud à l'aide de l'option *Découvrir* pour des configurations de fournisseurs cloud spécifiques ou bien lancer une découverte sur un Snapshot Manager pour récupérer les données de biens disponibles sur le Snapshot Manager.

Après la première découverte complète, NetBackup effectue une découverte incrémentielle périodique des biens pour le Snapshot Manager configuré. Il détecte uniquement les changements (ajouts, suppressions ou modifications de biens) qui se sont produits entre la dernière découverte et la découverte actuelle.

Remarque : Pour la découverte incrémentielle précise, assurez-vous que l'heure est définie correctement sur le serveur principal NetBackup et le Snapshot Manager, selon les fuseaux horaires correspondant à leur localisation, afin d'éviter tout problème lors de la découverte.

La procédure suivante explique comment effectuer la découverte au niveau de Snapshot Manager, qui ne découvre pas les biens cloud au sens strict, mais récupère seulement les données spécifiques à partir de Snapshot Manager.

Pour découvrir des biens sur Snapshot Manager

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Snapshot Manager**.
3. Dans le menu situé en regard de Snapshot Manager, cliquez sur **Découvrir**.

La procédure suivante décrit comment effectuer la découverte au niveau de la configuration, ce qui déclenche une découverte approfondie des biens et récupère l'état des biens à un point dans le temps, tout en détectant les ajouts, les modifications ou les suppressions de biens dans le cloud.

Pour découvrir des biens appartenant à une configuration de fournisseur cloud

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Snapshot Manager**.
3. Cliquez sur l'adresse IP ou le nom d'hôte du Snapshot Manager dont vous souhaitez afficher les fournisseurs cloud.
4. Cliquez sur l'onglet du fournisseur dont vous souhaitez afficher les configurations.
5. Dans le menu près du nom de configuration, cliquez sur **Découvrir**.

Remarque : Si la première opération de découverte des configurations de fournisseur cloud prend plus de 30 minutes, elle expire. Cependant, l'opération suivante se poursuit, ce qui entraîne la synchronisation des biens NetBackup avec les biens Snapshot Manager.

Modification de la fréquence de découverte automatique pour Snapshot Manager

Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option de découverte automatique. Par exemple :

`CLOUD_AUTODISCOVERY_INTERVAL` **= nombre de secondes**

Pour plus d'informations, consultez le guide de l'administrateur NetBackup, volume I.http://www.veritas.com/docs/DOC5332

Activation ou désactivation d'un Snapshot Manager

Selon vos préférences, vous pouvez activer ou désactiver un Snapshot Manager. Si vous désactivez un Snapshot Manager, vous ne pouvez pas découvrir de biens ou assigner de plans de protection.

Pour activer ou désactiver un Snapshot Manager

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Snapshot Manager**.
3. En fonction de l'état du Snapshot Manager, sélectionnez **Activer** ou **Désactiver**.

Remarque : une fois que le serveur Snapshot Manager est désactivé, il n'assure plus la protection des biens qui lui sont associés. Dans ce cas, désabonnez les biens des plans de protection ou annulez toutes les opérations SLP en attente pour ne pas faire échouer les travaux pendant la période de désactivation.

(Facultatif) Ajout de l'extension Snapshot Manager

L'extension Snapshot Manager permet de faire évoluer la capacité de l'hôte Snapshot Manager à traiter simultanément un grand nombre de requêtes sur le serveur Snapshot Manager à sa capacité maximale. Vous pouvez installer une ou plusieurs extensions Snapshot Manager sur site ou dans le cloud, selon vos besoins, pour exécuter les travaux sans surcharger l'hôte. Une extension permet d'augmenter la capacité de traitement de l'hôte Snapshot Manager.

L'extension Snapshot Manager peut avoir une configuration identique ou supérieure à celle de l'hôte Snapshot Manager.

Environnements d'extension Snapshot Manager pris en charge :

- Extension basée sur une machine virtuelle pour une utilisation sur site
- Extension basée sur le cloud avec cluster Kubernetes géré

Consultez le chapitre *Déploiement d'extensions Snapshot Manager* de la dernière version du Guide d'installation et de mise à niveau de NetBackup Snapshot Manager.

Gestion des groupes cloud intelligents

Vous pouvez créer et protéger un groupe dynamique de biens en définissant des groupes de biens cloud intelligents à partir d'un ensemble de filtres appelés « requêtes ». NetBackup sélectionne les machines virtuelles cloud, les applications ou les volumes en fonction de ces requêtes et les ajoute au groupe. Un groupe intelligent reflète automatiquement les modifications apportées dans l'environnement des biens, ce qui vous évite d'avoir à vérifier manuellement la liste des biens du groupe lorsque des biens sont ajoutés ou supprimés dans l'environnement.

Lorsque vous appliquez un plan de protection à un groupe de biens cloud intelligent, tous les biens qui correspondent à la requête sont automatiquement protégés si l'environnement de biens est changé par la suite.

Remarque : Vous ne pouvez créer, mettre à jour ou supprimer des groupes intelligents que si votre rôle dispose des autorisations RBAC nécessaires pour les biens cloud à gérer. L'administrateur de sécurité NetBackup peut vous accorder l'accès au type de bien (machine virtuelle, PaaS, application, volume, réseau) associé à un compte ou à un abonnement spécifique, ou à un niveau de fournisseur cloud. Consultez le *Guide de l'administrateur de l'interface utilisateur Web NetBackup*.

Création d'un groupe cloud intelligent

Pour créer un groupe cloud intelligent

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Groupes intelligents**, puis cliquez sur **+ Ajouter**.
3. Entrez un nom et une description pour le groupe.

4 Sélectionnez le fournisseur cloud, l'ID de compte et la région.

Remarque : Si aucune région n'est spécifiée, le groupe cloud intelligent protège tous les biens de la région.

5 Sélectionnez le **type de bien**.

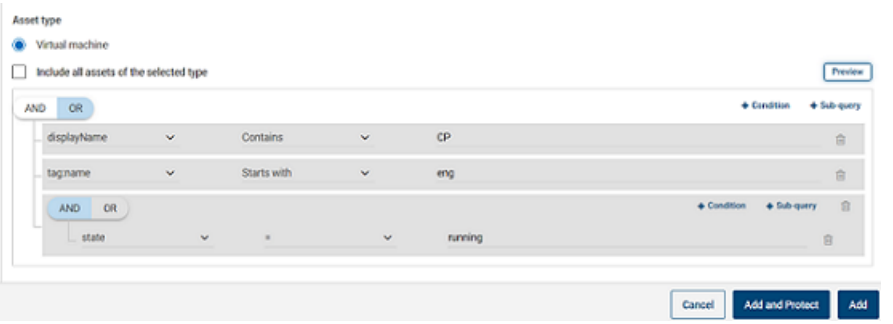
6 Ensuite, effectuez l'une des opérations suivantes :

- Sélectionnez **Inclure tous les biens du type sélectionné**.
  Cette option utilise une requête par défaut pour sélectionner tous les biens à sauvegarder lorsque le plan de protection s'exécute.
- Pour sélectionner uniquement les biens qui répondent à des conditions spécifiques, créez votre propre requête : cliquez sur **Ajouter une condition**.

7 Pour ajouter une condition, utilisez les listes déroulantes afin de sélectionner un mot-clé et un opérateur, puis entrez une valeur.

Se reporter à la section intitulée « Options de requête pour la création de groupes cloud intelligents » à la page 23.

Pour modifier l'effet de la requête, cliquez sur **+ Condition** et sur **ET** ou **OU**, puis sélectionnez le mot-clé, l'opérateur et la valeur à utiliser dans la condition. Par exemple :



Cet exemple utilise **ET** pour restreindre la portée de la requête : il sélectionne seulement les machines virtuelles dont le nom affiché contient `cp` avec une étiquette nommée `eng` et `en cours d'exécution`.

Remarque : Le caractère spécial « < » n'est pas pris en charge dans le nom d'étiquette. S'il est présent, la création du groupe de biens échouera.

Remarque : Limitation connue de NetBackup : si vous créez une requête avec des noms de biens et d'étiquettes (référencés par votre fournisseur cloud) contenant des espaces ou des caractères spéciaux tels que `(,), &, \, /, ", [, ], {, }`, vous ne pourrez plus modifier la requête pour modifier les paramètres. Cela ne vous empêche pas de créer le groupe intelligent et d'y appliquer le plan de protection. Seule la fonctionnalité de modification de requête est concernée par cette limitation.

Pour éviter ce problème, assurez-vous que les noms d'étiquette ne contiennent pas les caractères spéciaux indiqués plus haut et créez une nouvelle requête pour les nouveaux noms d'étiquette.

Vous pouvez également ajouter des sous-requêtes à une condition. Cliquez sur **+ Sous-requête**, puis sur **ET** ou **OU**, puis sélectionnez le mot-clé, l'opérateur et la valeur pour la condition de sous-requête.

8 Pour tester la requête, cliquez sur **Aperçu**.

Le processus de sélection par requête est dynamique. Les modifications apportées dans l'environnement virtuel peuvent avoir une incidence sur les biens sélectionnés par la requête lors de l'exécution du plan de protection. Par conséquent, les biens que la requête sélectionne ultérieurement, lors de l'exécution du plan de protection, peuvent différer de ceux qui figurent dans l'aperçu.

Remarque : Lorsque vous utilisez des requêtes dans les **groupes intelligents**, l'interface utilisateur Web NetBackup risque de ne pas renvoyer la liste exacte des biens correspondant à la requête si la condition indiquée comporte des caractères n'appartenant pas à l'alphabet latin.

L'utilisation de la condition de filtre `not equals` sur l'un des attributs renvoie les biens, y compris ceux qui n'ont aucune valeur (null) pour l'attribut. Pour les attributs à valeurs multiples, par exemple `tag`, seuls les biens qui correspondent au moins à l'une des valeurs de l'attribut sont renvoyés.

Remarque : Lorsque vous cliquez sur **Aperçu** ou que vous enregistrez le groupe, les options de requête sont traitées comme étant sensibles à la casse quand les biens sont sélectionnés pour le groupe. Dans la section **Machines virtuelles**, si vous cliquez sur une machine virtuelle qui n'a pas été sélectionnée pour le groupe, le champ **Groupes intelligents** affiche `Aucun`.

---

9 Pour enregistrer le groupe sans l'ajouter à un plan de protection, cliquez sur **Ajouter**.

Pour enregistrer le groupe et lui appliquer un plan de protection, cliquez sur **Ajouter et protéger**. Sélectionnez le plan et cliquez sur **Protéger**.

Options de requête pour la création de groupes cloud intelligents

---

Remarque : Les valeurs d'attribut peuvent ne pas correspondre exactement aux valeurs affichées sur le portail du fournisseur cloud. Vous pouvez consulter la page de détails du bien ou la réponse de l'API du fournisseur cloud d'un bien individuel.

Tableau 1-3 Mots-clés de requête

Mot-clé	Description (toutes les valeurs sont sensibles à la casse)
`displayName`	Nom affiché du bien.
`state`	Par exemple : en cours d'exécution, arrêté, etc.
`tag`	Étiquette assignée au bien pour la catégorisation.
`instanceType` / `machineType` / `vmSize`	Type d'instance/de machine du bien ou taille de la machine virtuelle, selon la sélection du fournisseur cloud. Par exemple, t2.large, t3.large ou b2ms, d2sv3

Tableau 1-4 Opérateurs de requête

Opérateur	Description
`Starts with`	Renvoie une correspondance lorsque la valeur apparaît au début d'une chaîne.
`Ends with`	Renvoie une correspondance lorsque la valeur apparaît à la fin d'une chaîne.
`Contains`	Recherche la valeur que vous entrez, où qu'elle apparaisse dans la chaîne.
=	Renvoie uniquement les correspondances exactes avec la valeur que vous entrez.
!=	Renvoie toute valeur différente de celle que vous entrez.

Remarque : Une fois le groupe intelligent créé, vous ne pouvez plus modifier la sélection du fournisseur cloud, mais vous pouvez modifier le nom et la description, ainsi que la requête, selon les besoins.

Suppression d'un groupe cloud intelligent

Pour supprimer un groupe cloud intelligent

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Recherchez le groupe dans l'onglet **Groupes intelligents**.
3. Si le groupe n'est pas protégé, sélectionnez-le et cliquez sur **Supprimer**.
4. Si le groupe est protégé, cliquez dessus, faites défiler la fenêtre vers le bas et cliquez sur **Supprimer la protection**.
5. Sélectionnez ensuite ce groupe dans l'onglet **Groupes intelligents**, puis cliquez sur **Supprimer**.

Protection des biens ou des groupes cloud intelligents

Vous pouvez créer des plans de protection ciblant le fournisseur de vos charges de travail cloud. Vous pouvez ensuite abonner les biens associés au fournisseur cloud à un plan de protection spécifique à ce fournisseur.

Remarque : si vous aviez précédemment appliqué un plan de protection aux biens de différents fournisseurs cloud, il est automatiquement converti au nouveau format spécifique au fournisseur. Cette conversion s'effectue après une mise à niveau vers NetBackup 9.1. Par exemple, si les biens Google Cloud et AWS Cloud étaient abonnés à un plan de protection, ce dernier est divisé en deux plans distincts, un pour chaque fournisseur.

section Se reporter à la section intitulée « Conversion des plans de protection après une mise à niveau vers NetBackup 9.1 » à la page 26..

Procédez comme suit pour abonner une machine virtuelle, une application ou un groupe cloud intelligent à un plan de protection. Lorsque vous abonnez un bien à un plan de protection, vous lui assignez des paramètres de sauvegarde prédéfinis.

Remarque : Le rôle RBAC qui vous est assigné doit vous permettre d'accéder aux biens que vous voulez gérer et aux plans de protection que vous voulez utiliser.

Pour protéger un bien cloud ou un groupe intelligent

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Dans l'onglet **Machines virtuelles**, **Applications**, **Volumes** ou **Groupes intelligents**, cochez la case du bien ou du groupe de biens, puis cliquez sur **Ajouter la protection**.
3. Sélectionnez un plan de protection, puis cliquez sur **Suivant**.
4. Vous pouvez définir les paramètres suivants :
   - **Planifications et conservation**
   - **Options de stockage**
     Pour plus d'informations sur les options de stockage de l'interface utilisateur Web, consultez la section *Configuration du stockage* du Guide de l'administrateur de l'interface utilisateur Web NetBackup.
   - **Options de sauvegarde**
5. Cliquez sur **Protéger**.

Option Sauvegarder maintenant pour une protection immédiate

Outre les plans de protection planifiés, vous pouvez utiliser l'option **Sauvegarder maintenant** pour sauvegarder immédiatement un bien et le protéger contre toute circonstance imprévue.

1. Sélectionnez un bien cloud ou un groupe intelligent et cliquez sur **Sauvegarder maintenant**.
2. Sélectionnez ensuite le plan de protection à appliquer. Seuls les plans de protection s'appliquant au fournisseur cloud du bien s'affichent.
3. Cliquez sur **Démarrer la sauvegarde**.

   Un travail de sauvegarde est déclenché. Vous pouvez en effectuer le suivi sur la page **Moniteur d'activité**.

Pour plus d'informations, consultez le Guide de l'administrateur de l'interface utilisateur Web NetBackup.

Conversion des plans de protection après une mise à niveau vers NetBackup 9.1

Notez les points suivants en ce qui concerne la conversion automatique des plans de protection plus anciens au nouveau format.

- La conversion des plans de protection démarre une fois la migration des biens terminée (après la mise à niveau vers NetBackup 9.1).

- Les anciens plans de protection auxquels aucun bien n'est abonné ne sont pas convertis au nouveau format. Vous pouvez les supprimer manuellement.
- **Avant ou pendant la conversion**
  - Tous les biens sont désabonnés de l'ancien plan de protection et abonnés au plan de protection converti.
  - Aucun nouveau bien ne peut être abonné à l'ancien plan de protection.
  - L'opération **Sauvegarder maintenant** échoue pour l'ancien plan.
  - Vous ne pourrez pas personnaliser ou modifier l'ancien plan de protection.
- **Après une conversion réussie**
  - Si l'ancien plan de protection a été utilisé pour protéger les biens d'un seul fournisseur cloud, le nouveau plan conserve le même nom et le même abonnement de biens lors de la conversion.
  - Si l'ancien plan de protection était utilisé pour protéger les biens de plusieurs fournisseurs cloud, son nom est conservé. Le nom du plan de protection est mis à jour afin de maintenir l'abonnement de biens pour tous les fournisseurs cloud lors de la conversion.
    Pour les autres fournisseurs cloud qui faisaient partie de l'ancien plan, de nouveaux plans de protection sont créés lors de la conversion et seuls les biens appartenant aux différents fournisseurs sont abonnés. Les nouveaux plans sont nommés selon le format suivant `<nom_ancien_plan>_<fournisseur_cloud>`.
  - Vous pouvez donc constater une augmentation du nombre de plans dans le menu *Plans de protection* de l'interface utilisateur Web.
  - Les messages de confirmation s'affichent dans les notifications comme suit :
    Le plan de protection <protectionPlanName> a été créé pendant la conversion vers le nouveau format.
    Le plan de protection <protectionPlanName> a été converti vers le nouveau format.
    Vous pouvez ensuite gérer et appliquer les plans de protection convertis comme d'habitude.

Scénarios de défaillance

Consultez les références suivantes pour savoir comment les scénarios de défaillance sont gérés pendant ou après la conversion des plans de protection. Vérifiez également les notifications des alertes de défaillance éventuelles et prenez les mesures nécessaires.

- Certains biens peuvent ne pas avoir été désabonnés de l'ancien plan de protection. Dans ce cas, la conversion continue avec les biens désabonnés. Le

processus de conversion des biens qui a échoué est relancé toutes les quatre heures.

- Après la conversion, certains biens peuvent ne pas avoir été abonnés automatiquement au nouveau plan. Dans ce cas, vous devez abonner manuellement ces biens au plan de protection converti.
- Des problèmes peuvent se produire lors de l'assignation des autorisations d'accès requises au nouveau plan de protection converti. Dans ce cas, vous devez assigner manuellement les autorisations d'accès.

Personnalisation ou modification de biens cloud ou de groupes cloud intelligents

Vous pouvez modifier certains paramètres d'un plan de protection, notamment les fenêtres de sauvegarde de planifications et d'autres options.

Pour personnaliser ou modifier le plan de protection d'un bien cloud

1. À gauche, cliquez sur **Charges de travail > Cloud**.
2. Dans l'onglet **Machines virtuelles**, **Applications**, **Volumes** ou **Groupes intelligents**, cliquez sur le bien dont vous souhaitez personnaliser la protection.
3. Cliquez sur **Protection personnalisée > Continuer**.
4. Vous pouvez définir les paramètres suivants :
   - **Planifications et conservation**
     Changez la fenêtre de démarrage de la sauvegarde.
   - **Options de sauvegarde**
     Activez/désactivez les snapshots régionaux pour les biens Google Cloud ou spécifiez/modifiez le groupe de ressources de destination de snapshot pour les biens Azure et Azure Stack Hub.

Suppression de la protection de biens cloud ou de groupes intelligents

Vous pouvez désabonner un bien cloud d'un plan de protection. Quand le bien est désabonné, les sauvegardes ne sont plus effectuées.

Pour supprimer la protection d'un bien cloud

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Dans l'onglet **Machines virtuelles**, **Applications**, **Volumes** ou **Groupes intelligents**, cliquez sur le bien dont vous souhaitez supprimer la protection.
3. Cliquez sur **Supprimer la protection > Oui**.

Nettoyage des biens cloud

Les biens cloud sont nettoyés automatiquement pendant le cycle de nettoyage ou manuellement selon les critères suivants :

- Aucun plan de protection n'est actif pour le bien cloud.
- Le bien n'a pas été découvert au cours des 30 derniers jours (âge du nettoyage).
- Il n'existe aucun point de récupération.
- Le bien est marqué pour suppression (il est supprimé sur Snapshot Manager).

L'utilisateur peut améliorer les critères de nettoyage de biens cloud en mettant à jour l'âge du nettoyage et en appliquant des critères de filtre spécifiques pour les biens via le fichier `bp.conf`. Les paramètres suivants doivent être configurés dans le fichier `bp.conf` :

- CLOUD.CLEANUP_AGE_MINUTES
- CLOUD.CLEANUP_FILTER

Par exemple,

```
/usr/openv/netbackup/bin/nbsetconfig

nbsetconfig> CLOUD.CLEANUP_AGE_MINUTES = 180

nbsetconfig> CLOUD.CLEANUP_FILTER = provider eq 'aws'

nbsetconfig>
```

L'utilisateur peut également exécuter manuellement la requête POST à l'aide de la requête `cleanup-assets` avec le corps de demande suivant, puis exécuter une requête GET avec l'ID de requête obtenu de la réponse POST, comme décrit dans l'exemple suivant :

```
{
    "data":{
    "type":"query",
    "attributes":{
        "queryName":"cleanup-assets",
        "workloads":["cloud"],
        "parameters": {
            "cleanup_age_minutes": 180
        },
        "filter": "provider eq 'aws'"
      }
    }
}
```

Filtrage des biens cloud

L'utilisateur peut définir un filtre personnalisé à partir d'attributs, afin de répertorier les biens dans l'onglet Machines virtuelles, Applications, PaaS ou Volumes.

Pour créer un filtre

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Dans l'onglet Machines virtuelles, Applications, PaaS ou Volumes, cliquez sur l'icône **Filtre** dans la partie supérieure droite de l'écran.

   L'option **Créer un filtre** s'affiche.
3. Cliquez sur l'option **Créer un filtre** pour définir un filtre personnalisé à partir d'attributs, afin de répertorier les biens dans l'onglet Machines virtuelles, Applications, PaaS ou Volumes.
4. Pour créer un filtre, entrez les informations nécessaires pour les paramètres suivants :

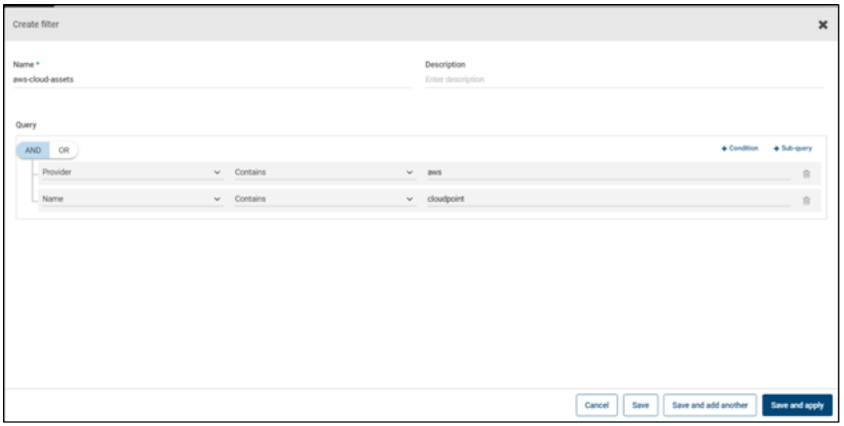
Paramètre	Description
Nom	Nom du filtre.
Description	Décrivez le filtre.
Requête	Pour sélectionner uniquement les biens qui répondent à des conditions spécifiques, créez votre propre requête.

5 Pour sélectionner uniquement les biens qui répondent à des conditions spécifiques, créez votre propre requête : cliquez sur **+ Condition**.

6 Pour ajouter une condition, utilisez les listes déroulantes afin de sélectionner un mot-clé et un opérateur, puis entrez une valeur.

Se reporter à la section intitulée « Options de requête pour la création de groupes cloud intelligents » à la page 23.

Pour modifier l'effet de la requête, cliquez sur **+ Condition** et sur **ET** ou **OU**, puis sélectionnez le mot-clé, l'opérateur et la valeur à utiliser dans la condition. Par exemple :



Cet exemple utilise **AND** pour restreindre la portée de la requête : il sélectionne seulement les biens dont le nom affiché contient `aws` et qui ont également un **Nom** comme `CloudPoint`, et dont l'état est `en cours d'exécution`.

Vous pouvez également ajouter des sous-requêtes à une condition. Cliquez sur **+ Sous-requête**, puis sur **ET** ou **OU**, puis sélectionnez le mot-clé, l'opérateur et la valeur pour la condition de sous-requête.

Options de requête pour créer un filtre

Remarque : Les valeurs d'attribut peuvent ne pas correspondre exactement aux valeurs affichées sur le portail du fournisseur cloud. Vous pouvez consulter la page de détails du bien ou la réponse de l'API du fournisseur cloud d'un bien individuel.

Tableau 1-5 Mots-clés de requête

Mot-clé	Description (toutes les valeurs sont sensibles à la casse)
`Server type`	Type du serveur.
`Instance ID`	Identifiant de l'instance du bien, selon la sélection du fournisseur cloud.
`Instance name`	Nom de l'instance du bien, selon la sélection du fournisseur cloud.
`Name`	Nom affiché du bien.
`Provider`	Nom du fournisseur cloud du bien.
`Region`	Nom de la région du fournisseur cloud du bien.
ID de configuration	ID de configuration du bien.
Service de base de données	Service de base de données du bien
Supprimé	Bien supprimé.
Type d'entité	Type d'entité du bien.
Domaine de service	Domaine de service du bien.
Snapshot Manager	Instance de Snapshot Manager auprès de laquelle le bien est enregistré.

Tableau 1-6 Opérateurs de requête

Opérateur	Description
`Starts with`	Renvoie une correspondance lorsque la valeur apparaît au début d'une chaîne.
`Ends with`	Renvoie une correspondance lorsque la valeur apparaît à la fin d'une chaîne.
`Contains`	Recherche la valeur que vous entrez, où qu'elle apparaisse dans la chaîne.
=	Renvoie uniquement les correspondances exactes avec la valeur que vous entrez.
!=	Renvoie toute valeur qui n'est pas égale à celle que vous entrez.

Prise en charge des services cloud AWS et Azure Government

À partir de la version 8.3, le Snapshot Manager peut découvrir les charges de travail cloud Amazon Web Services et Microsoft Azure Government (États-Unis). Une fois le Snapshot Manager ajouté à NetBackup, vous pouvez protéger les charges de travail avec NetBackup. NetBackup répond aux exigences réglementaires, notamment avec la prise en charge d'IPv6 pour le déploiement de Snapshot Manager sur les charges de travail AWS et Azure Government (États-Unis).

Après avoir configuré les services cloud AWS ou Azure Government (États-Unis), le service d'agent AWS et Azure est créé pour découvrir les biens cloud correspondant à la région visée. Les biens découverts s'affichent dans NetBackup. Actuellement, seules les charges de travail des régions sélectionnées et du terminal mappé sont découvertes et protégées. Vous ne pouvez pas utiliser une combinaison de clouds publics et gouvernementaux pour un même hôte Snapshot Manager.

Une erreur peut se produire si vous mettez à jour un plug-in cloud lorsque les opérations du plug-in sont en cours.

Snapshot Manager prend en charge les régions suivantes de GovCloud (États-Unis) :

Fournisseur cloud	Régions GovCloud (États-Unis)
Amazon Web Services	■ us-gov-east-1 ■ us-gov-west-1
Microsoft Azure	■ US Gov Arizona ■ US Gov Texas ■ US Gov Virginia

Remarque : les biens PaaS ne prennent pas en charge Government Cloud.

Pour plus d'informations sur la configuration d'AWS et de Microsoft Azure, consultez la section Se reporter à "Ajout d'un fournisseur cloud pour Snapshot Manager" à la page 13.

À propos de la protection des ressources Microsoft Azure au moyen de groupes de ressources

NetBackup permet de définir la destination des snapshots de groupes de ressources pairs pour tout groupe de ressources contenant des machines virtuelles et des volumes protégés.

Toutes les ressources de Microsoft Azure sont associées à un groupe de ressources. Lorsqu'un snapshot est créé, il est associé à un groupe de ressources. En outre, chaque groupe de ressources est associé à une région. Voir ci-dessous :

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/manage-resource-groups-portal

Snapshot Manager crée un snapshot qu'il place dans le groupe de ressources auquel appartient la ressource, y compris dans les conditions suivantes :

- Si vous ne fournissez pas de préfixe pour un groupe de ressources
- Les groupes de ressources pairs ne sont pas créés
- Vous autorisez la création des snapshots

Vous pouvez changer les paramètres, afin de placer les snapshots dans un groupe de ressources autre que celui qui est associé à la ressource. Cependant, tenez compte des points importants suivants :

- Le groupe de ressources pair doit appartenir à la même région que le groupe de ressources de la ressource.
- Si aucun groupe de ressources pair n'est trouvé, les configurations déterminent si la création de snapshots réussit ou échoue.

Pour activer cette fonction, vous devez créer des groupes de ressources pairs. Snapshot Manager ajoute alors le préfixe du groupe de ressources associé à la ressource. Lorsqu'un snapshot est créé, le nom du groupe de ressources pair est dérivé en fonction du préfixe et du groupe de ressources auquel la ressource est associée.

Remarque : Vous pouvez désormais associer directement un snapshot à un groupe de ressources pair existant lors de la création d'un plan de protection. Cependant, la fonction de définition d'un groupe de ressources pair en spécifiant un préfixe, qui est décrite dans cette section, reste valide.

Pour la procédure complète, consultez les informations sur la création de plans de protection dans le *guide de l'administrateur de l'interface utilisateur Web NetBackup*.

Avant de commencer

- Les groupes de ressources pairs doivent être accessibles par les ressources protégées à l'aide du groupe de ressources.
- Les régions d'une configuration de plugin ne doivent pas chevaucher une autre configuration si un préfixe est spécifié.

Restrictions et remarques

- Seuls les caractères alphanumériques, les points, les signes soulignés ou les parenthèses sont autorisés dans les noms de groupe de ressources.
- La longueur du préfixe doit être inférieure à 89 caractères.
- Vous ne pouvez pas utiliser des caractères qui ne sont pas autorisés par la configuration Azure pour les conventions de nommage de groupes de ressources.

À propos des configurations et des résultats des groupes de ressources

Le tableau suivant répertorie les scénarios de configuration des machines virtuelles et des groupes de ressources, de configuration des ressources et en indique le résultat.

Tableau 1-7 Configurations et résultats

Préfixe du groupe de ressources	Case à cocher Protéger les biens même si des groupes de ressources préfixés sont introuvables	Résultat
Non spécifié	Pas sélectionné	NetBackup associe les snapshots récemment créés au groupe de ressources de la ressource.

Préfixe du groupe de ressources	Case à cocher Protéger les biens même si des groupes de ressources préfixés sont introuvables	Résultat
Spécifié	Pas sélectionné	NetBackup crée des snapshots et les associe au groupe de ressources pair si les conditions suivantes sont remplies : ■ Le groupe de ressources pair est créé. ■ Le groupe de ressources pair doit appartenir à la même région que le groupe de ressources. Si les conditions ne sont pas remplies, les travaux de snapshot échouent.
Spécifié	Sélectionné	NetBackup crée des snapshots et les associe au groupe de ressources pair si les conditions suivantes sont remplies : ■ Le groupe de ressources pair est créé. ■ Le groupe de ressources pair doit appartenir à la même région que le groupe de ressources. Si un groupe de ressources pair n'est pas créé ou se trouve dans une région différente, le nouveau snapshot est associé au groupe de ressources de la ressource protégée.==

Exemples de configurations de groupe de ressources

Le tableau suivant répertorie les exemples de configurations de groupe de ressources.

Tableau 1-8 Exemples de configurations

Conditions	Configurations	Résultat
■ Le système d'exploitation et tous les disques appartiennent au même groupe de ressources. ■ Le groupe de ressources pair est nommé correctement. ■ La ressource paire se trouve dans la même région que le groupe de ressources de la ressource.	■ La valeur du préfixe du groupe de ressources est fournie. ■ La case à cocher **Protéger les biens même si des groupes de ressources préfixés sont introuvables** est sélectionnée.	Les snapshots sont créés dans le groupe de ressources pair.
■ Le système d'exploitation et tous les disques appartiennent à des groupes de ressources différents. ■ Les groupes de ressources pairs sont nommés correctement. ■ Les ressources paires sont dans la même région que les groupes de ressources des ressources.	■ La valeur du préfixe du groupe de ressources est fournie. ■ La case à cocher **Protéger les biens même si des groupes de ressources préfixés sont introuvables** est sélectionnée.	Les snapshots sont créés dans le groupe de ressources pair.
■ Le système d'exploitation et tous les disques appartiennent au même groupe de ressources. ■ Le groupe de ressources pair est créé dans une région différente de celle du groupe de ressources de la ressource.	■ La valeur du préfixe du groupe de ressources est fournie. ■ La case à cocher **Protéger les biens même si des groupes de ressources préfixés sont introuvables** est sélectionnée.	Les snapshots sont créés dans le groupe de ressources d'origine, et non pas dans le groupe de ressources pair.

Conditions	Configurations	Résultat
■ Le système d'exploitation et tous les disques appartiennent au même groupe de ressources. ■ Le groupe de ressources pair n'est pas créé.	■ La valeur du préfixe du groupe de ressources est fournie. ■ La case à cocher **Protéger les biens même si des groupes de ressources préfixés sont introuvables** est sélectionnée.	Les snapshots sont créés dans le groupe de ressources d'origine, et non pas dans le groupe de ressources pair.
■ Le système d'exploitation et tous les disques appartiennent à des groupes de ressources différents, RG1 et RG2. ■ Les groupes de ressources pairs RG1 sont nommés correctement et situés dans la même région que les ressources. ■ Le groupe de ressources pair RG2 n'est pas créé.	■ La valeur du préfixe du groupe de ressources est fournie. ■ La case à cocher **Protéger les biens même si des groupes de ressources préfixés sont introuvables** est sélectionnée.	Les snapshots sont créés dans le groupe de ressources pairs de RG1 et le groupe de ressources d'origine RG2.
■ Le système d'exploitation et tous les disques appartiennent au même groupe de ressources. ■ Les groupes de ressources pairs sont nommés correctement. ■ Le groupe de ressources pair est situé dans une région différente de celle du groupe de ressources des ressources.	■ La valeur du préfixe du groupe de ressources est fournie. ■ La case à cocher **Protéger les biens même si des groupes de ressources préfixés sont introuvables** n'est pas sélectionnée.	Les snapshots ne sont pas créés et le travail échoue.

Conditions	Configurations	Résultat
■ Le système d'exploitation et tous les disques appartiennent au même groupe de ressources. ■ Le groupe de ressources pair n'est pas créé.	■ La valeur du préfixe du groupe de ressources est fournie. ■ La case à cocher **Protéger les biens même si des groupes de ressources préfixés sont introuvables** n'est pas sélectionnée.	Les snapshots ne sont pas créés et le travail échoue.
■ Le système d'exploitation et tous les disques appartiennent à des groupes de ressources différents, RG1 et RG2. ■ Les groupes de ressources pairs de RG1 et de RG2, à savoir snapRG1 et snapRG2 sont dans des régions différentes. ■ Le groupe de ressources pair snapRG1 doit appartenir à la même région que le groupe de ressources RG1. ■ Le groupe de ressources pair snapRG2 doit appartenir à la même région que le groupe de ressources RG2.	■ La valeur du préfixe du groupe de ressources est fournie. ■ La case à cocher **Protéger les biens même si des groupes de ressources préfixés sont introuvables** n'est pas sélectionnée.	Les snapshots ne sont pas créés et le travail échoue.

Dépannage des autorisations de groupe de ressources

Si les autorisations appropriées ne sont pas assignées au groupe de ressources, la création de snapshot échoue pour les ressources Azure associées aux groupes de ressources.

Solution de contournement :

Pour résoudre ce problème, procédez comme suit :

1. Accédez à https://portal.azure.com/#blade/HubsExtension/BrowseResourceGroups.

2. Cliquez sur le groupe de ressources à utiliser dans le snapshot.
3. Cliquez sur **Contrôle d'accès (IAM)**.
4. Cliquez sur **Ajouter un rôle**.
5. Sélectionnez **Role as Owner** et **Assign Access to as User**, puis sélectionnez l'**application (créée pour Snapshot Manager pour les appels d'API)**.
6. Enregistrez et relancez la sauvegarde.

À propos de l'accélérateur NetBackup pour les charges de travail cloud

L'accélérateur NetBackup réduit le temps de sauvegarde des sauvegardes cloud. NetBackup utilise des snapshots de référence pour identifier les modifications qui ont été apportées au sein d'une machine virtuelle. Seuls les blocs de données modifiés sont envoyés au serveur de médias NetBackup, afin de réduire significativement les temps d'E/S et de sauvegarde. Le serveur de médias combine les nouvelles données avec les données de sauvegarde précédentes et produit une image NetBackup complète traditionnelle incluant les fichiers de machine virtuelle complets.

NetBackup prend en charge la sauvegarde de l'accélérateur pour les charges de travail AWS, Azure et Azure Stack.

Remarque : L'accélérateur est particulièrement approprié pour les données de machine virtuelle ne comportant pas de taux élevé de modification.

L'accélérateur présente les avantages suivants :

- Effectue les sauvegardes complètes plus vite que les sauvegardes traditionnelles. Crée un flux de sauvegarde compact qui utilise moins de bande passante réseau entre l'hôte de sauvegarde et le serveur. L'accélérateur envoie seulement les blocs de données modifiés pour la sauvegarde. NetBackup crée alors une image NetBackup traditionnelle complète incluant les données de blocs modifiées.
- Les sauvegardes de l'accélérateur prennent en charge la technologie de récupération granulaire (GRT).
- Réduit les E/S sur le Snapshot Manager.
- Réduit la charge d'UC sur le Snapshot Manager.

Fonctionnement de l'accélérateur NetBackup avec des machines virtuelles

Pour les sauvegardes Azure et Azure Stack, l'accélérateur est activé lorsque vous sélectionnez un type de stockage pris en charge par l'accélérateur, comme MSDP, OpenStorage, CloudStorage et MSDP-C (Azure et AWS).

L'accélérateur NetBackup crée le flux et l'image de sauvegarde pour chaque machine virtuelle comme suit :

- Si la machine virtuelle n'a aucune sauvegarde précédente, NetBackup effectue une sauvegarde complète.
- Lors de la prochaine sauvegarde, NetBackup identifie les données ayant été modifiées depuis la sauvegarde précédente. Seuls les blocs modifiés et les informations d'en-tête sont inclus dans la sauvegarde pour créer une sauvegarde de machine virtuelle complète. Les blocs modifiés sont identifiés en comparant le snapshot de référence précédent et le snapshot actuel. Si vous sélectionnez l'option **Conserver la sauvegarde uniquement** ou **Lancer la sauvegarde si le snapshot est sur le point d'expirer** dans le plan de protection, le snapshot est conservé pour l'accélérateur jusqu'à ce que la sauvegarde suivante soit terminée.
- L'hôte de sauvegarde envoie au serveur de médias un flux de sauvegarde TAR qui comprend ce qui suit : les blocs modifiés de la machine virtuelle, ainsi que l'ID et les zones de stockage de la sauvegarde précédente (décalage et taille de bloc) des blocs inchangés.
- Le serveur de médias lit les blocs modifiés de la machine virtuelle, l'ID de sauvegarde et les informations relatives aux zones de stockage des blocs inchangés. A partir de l'ID de sauvegarde et des zones de stockage, le serveur de médias localise le reste des données de la machine virtuelle dans les sauvegardes existantes.
- Le serveur de médias indique au serveur de stockage de créer une nouvelle image complète qui comprend ce qui suit : les blocs nouvellement modifiés et les blocs inchangés existants qui résident sur le serveur de stockage. Le serveur de stockage peut ne pas enregistrer les blocs existants mais plutôt les lier à l'image.
- Microsoft Azure n'autorise pas plus de 200 snapshots incrémentiels ultérieurs. Si vous sélectionnez l'option **Conserver le snapshot avec la sauvegarde** dans le plan de protection et spécifiez une période de conservation pour le snapshot qui entraîne plus de 200 snapshots incrémentiels, les sauvegardes complètes sont exécutées à la place de l'accélérateur. Il est donc recommandé d'utiliser une période raisonnable de conservation des snapshots pour profiter des avantages de l'accélérateur.

- Si la configuration d'une machine virtuelle change, par exemple, si un nouveau disque est ajouté à une machine virtuelle entre deux sauvegardes d'accélérateur, une sauvegarde complète est réalisée pour ce disque et une sauvegarde de l'accélérateur est réalisée pour les disques existants.

Réanalyse forcée par l'accélérateur pour les machines virtuelles (attribut de planification)

L'option Nouvelle analyse forcée par l'accélérateur aide à éviter les problèmes d'images de sauvegarde endommagées en exécutant manuellement la commande ForcedRescan. Quand l'option Nouvelle analyse forcée par l'accélérateur est utilisée, toutes les données sur la machine virtuelle sont sauvegardées. Cette sauvegarde est semblable à la première sauvegarde d'accélérateur pour une politique. Pour le travail de nouvelle analyse forcée, le pourcentage d'optimisation de l'accélérateur est de 0. La durée de la sauvegarde est semblable à celle d'une sauvegarde complète non accélérateur.

La fonction de nouvelle analyse forcée améliore la sécurité et établit une baseline pour la sauvegarde avec accélérateur suivante. Cette fonction vous protège contre les dommages potentiels, par exemple en cas d'échec de la vérification de la somme de contrôle sur les données, dans la zone intermédiaire.

Recommandations d'utilisation d'une nouvelle analyse forcée :

- Ne déclenchez pas une nouvelle analyse forcée pour les machines virtuelles arrêtées.
- Si la mémoire de l'emplacement de stockage est saturée, une notification s'affiche dans l'interface utilisateur. Ne lancez la nouvelle analyse forcée que si la mémoire disponible à l'emplacement de stockage est suffisante.

NetBackup crée une planification nommée « ForcedRescan » pour chaque machine virtuelle protégée. Pour déclencher manuellement la sauvegarde avec la nouvelle analyse forcée, exécutez la commande suivante depuis l'invite de commande ou le terminal Linux :

```
bpbackup -i -p <policy_name> -s ForcedRescan
```

Par exemple, `bpbackup -i -p msdp_10mins_FRS+5d990ab5-f791-474f-885a-ae0c30f31c98 -s ForcedRescan`

Vous pouvez obtenir le nom de la politique à partir de l'interface utilisateur Web du plan de protection approprié.

Sauvegardes de l'accélérateur et catalogue NetBackup

Le fait d'utiliser l'accélérateur n'affecte pas la taille du catalogue NetBackup. Une sauvegarde complète avec l'accélérateur génère la même taille de catalogue qu'une sauvegarde complète des mêmes données sans l'accélérateur. Il en va de même pour les sauvegardes incrémentielles : le fait d'utiliser l'accélérateur ne requiert pas plus d'espace de catalogue qu'une sauvegarde sans l'accélérateur.

Messages d'accélérateur dans le journal Détails du travail de sauvegarde

Quand une machine virtuelle est d'abord sauvegardé, l'accélérateur n'est pas utilisé pour cette sauvegarde. Les messages suivants apparaissent dans le journal des détails du travail :

```
Jul 21, 2021 1:55:52 PM - Info bpbrm (pid=78332) accelerator enabled
Jul 21, 2021 1:55:53 PM - Info bpbrm (pid=78332) There is no
complete backup image match with track journal, a regular full
backup will be performed.

..

Jul 21, 2021 1:56:11 PM - Info bpbkar (pid=1301) accelerator sent
402666496 bytes out of 402664960 bytes to server, optimization 0.0%
```

Quand les sauvegardes ultérieures de la machine virtuelle utilisent l'accélérateur, les messages suivants apparaissent dans le journal des détails du travail :

```
Jul 21, 2021 2:01:33 PM - Info bpbrm (pid=79788) accelerator enabled

..

Jul 21, 2021 2:02:00 PM - Info bpbkar (pid=1350) accelerator
sent 1196032 bytes out of 402664960 bytes to server, optimization 99.7%
```

Ce message est une trace clé pour l'accélérateur. Dans cet exemple, l'accélérateur réussit à réduire les données de sauvegarde de 99.7 %.

Configuration de la planification de sauvegarde pour les charges de travail cloud

Vous pouvez ajouter une planification de sauvegarde dans l’onglet Attributs de la boîte de dialogue Ajouter une planification de sauvegarde lors de la création d’un

plan de protection pour les charges de travail cloud Azure, Azure Stack, AWS et GCP.

Consultez la section *Gestion des plans de protection* du *Guide de l'administrateur de l'interface utilisateur Web NetBackup* pour plus d'informations sur la création d'un plan de protection.

Pour ajouter une planification de sauvegarde à une charge de travail cloud

1. Sur la gauche, cliquez sur **Protection** > **Plans de protection**, puis sur **Ajouter**.
2. Dans **Propriétés de base**, entrez un **nom** et une **description**, puis sélectionnez **cloud** dans la liste déroulante **charge de travail**.
3. Sélectionnez un **fournisseur cloud** dans la liste déroulante et cliquez sur **Suivant**. Dans **Planifications**, cliquez sur **Ajouter une planification**.

   Dans l'onglet **Ajouter une planification de sauvegarde**, vous pouvez configurer les options de conservation de la sauvegarde et du snapshot.
4. (Pour les biens Azure SQL Server, GCP SQL Server et les biens PaaS SQL Managed Instance uniquement) Si vous avez sélectionné **Protéger les biens PaaS uniquement** pour le plan de protection, définissez l'option **Type de sauvegarde** sur **Sauvegarde incrémentielle** ou sur **Complète**. Pour les sauvegardes incrémentielles, NetBackup effectue une première sauvegarde complète et toutes les sauvegardes ultérieures capturent uniquement les modifications incrémentielles de la base de données. Cette fonction améliore considérablement les performances de sauvegarde. En cas de modification de schéma, le système passe d'une sauvegarde incrémentielle à une sauvegarde complète et cette modification est enregistrée dans le moniteur d'activité.

   Dans une politique, définissez une période de conservation plus longue pour les sauvegardes complètes que pour les sauvegardes incrémentielles. Une restauration complète requiert la sauvegarde complète précédente plus toutes les sauvegardes incrémentielles ultérieures. Si la sauvegarde complète arrive à expiration avant les sauvegardes incrémentielles, vous ne pourrez peut-être pas restaurer tous les fichiers. Se reporter à "À propos des sauvegardes incrémentielles pour les charges de travail PaaS" à la page 72.
5. Dans la liste déroulante **Récurrence**, spécifiez la fréquence de la sauvegarde.
6. Dans la section Options de snapshot et de sauvegarde, exécutez l'une des actions suivantes :

   - Sélectionnez l'option **Conserver le snapshot et la sauvegarde** pour conserver à la fois le snapshot et la sauvegarde. Spécifiez la période de conservation pour le snapshot et la sauvegarde à l'aide des listes déroulantes **Conserver le snapshot pendant** et **Conserver la sauvegarde**

pendant. Sélectionnez **Complet** dans la liste déroulante **Type de sauvegarde**. Sélectionnez l'option **Lancer la sauvegarde uniquement si le snapshot est sur le point d'expirer** pour démarrer le travail de sauvegarde juste avant que le snapshot conservé n'expire.

- Sélectionnez l'option **Conserver le snapshot uniquement** pour ne conserver que le snapshot. Spécifiez la période de conservation du snapshot à l'aide de la liste déroulante **Conserver le snapshot pendant**.
  - (Facultatif) Si vous avez sélectionné Amazon AWS comme fournisseur et que vous avez choisi de conserver le snapshot en sélectionnant l'une des deux options ci-dessus, vous pouvez configurer la réplication de snapshot à ce stade. Pour plus d'informations sur la réplication de snapshot cloud, consultez Se reporter à "Configuration de la réplication de snapshot AWS" à la page 51.
  - Sélectionnez **Activer la réplication de snapshot**.
  - Dans le tableau, sélectionnez **Région**, **Compte AWS** et **Période de conservation** pour les snapshots répliqués.

    Remarque : Le nombre de copies de réplication que vous configurez s'affiche dans la colonne **Répliques de snapshot** de la table **Planifications et conservation** de l'onglet **Planifications**.

- Sélectionnez l'option **Conserver la sauvegarde uniquement** pour ne conserver que la sauvegarde. Le snapshot expire immédiatement après la sauvegarde. Spécifiez la période de conservation de la sauvegarde à l'aide de la liste déroulante **Conserver la sauvegarde pendant**. Sélectionnez **Complet** dans la liste déroulante **Type de sauvegarde**.

7 Poursuivez la création de la planification dans l'onglet **Fenêtre de démarrage**, comme décrit dans la section *Gestion des plans de protection* du *Guide de l'administrateur de l'interface utilisateur Web NetBackup*.

Disponibilité de la restauration granulaire pour différentes options de sauvegarde

La disponibilité de la récupération granulaire pour les fichiers ou les dossiers dépend des différentes options de sauvegarde que vous sélectionnez pour la charge de travail.

- Si vous sélectionnez l'option **Conserver le snapshot et la sauvegarde**, la restauration granulaire est disponible.
- Si vous sélectionnez l'option **Conserver le snapshot uniquement**, la restauration granulaire est disponible.

- Si vous sélectionnez l'option **Conserver la sauvegarde uniquement**, la restauration granulaire est disponible.

Indexation pendant les travaux de sauvegarde et de snapshot

- NetBackup effectue l'indexation basée sur VxMS (Veritas Mapping Service) à partir du snapshot, et l'indexation intégrée pendant la sauvegarde à partir des travaux de snapshot. Il peut indexer des fichiers indépendamment de la région et de l'emplacement du Snapshot Manager. L'indexation reposant sur VxMS est actuellement prise en charge pour les clouds GCP, AWS, Azure et Azure Stack Hub.
- L'indexation est effectuée pendant les travaux de sauvegarde ou de snapshot, mais vous ne pouvez exécuter la récupération de fichiers ou de dossiers spécifiques qu'à partir de la copie du snapshot et de la sauvegarde à l'aide de l'option **Activer la récupération granulaire pour les fichiers et les dossiers**.
- Une fois le snapshot des biens de machine virtuelle créé, le travail « Indexer à partir du snapshot » est déclenché pour chacun des biens. Vous pouvez consulter les détails du travail d'indexation dans le **Moniteur d'activité**.
- Les journaux de débogage VxMS et du connecteur cloud sont disponibles dans le dossier */cloudpoint/openv/dm/datamover.<datamover-id>/netbackup/logs* du Snapshot Manager.
- Pour indexer des fichiers et des dossiers avec le même chemin de montage que celui mentionné dans `/etc/fstab`, le fichier `/etc/fstab` sur les serveurs Linux doit comporter des entrées basées sur le système de fichiers UUID et non des chemins d'accès de périphériques. Les chemins d'accès de périphériques peuvent changer selon l'ordre dans lequel Linux découvre les périphériques lors du démarrage du système.

Remarque : Si la machine virtuelle n'est pas connectée, la sauvegarde de la machine virtuelle continue et le travail de sauvegarde est marqué comme partiellement réussi. Dans ce cas, vous ne pouvez pas restaurer des fichiers ou des dossiers individuels, car l'indexation n'est pas disponible lorsque la machine virtuelle n'est pas connectée.

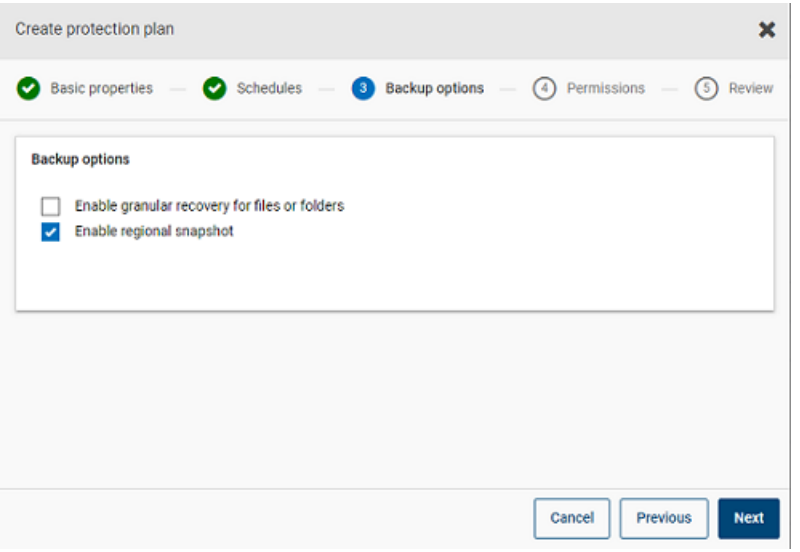
Options de sauvegarde des charges de travail cloud

Remarque : dans le cas d'une machine virtuelle connectée, une tentative de création de snapshot cohérent au niveau du système de fichiers est effectuée. Si la machine virtuelle connectée est arrêtée par la suite, l'application passe à l'état d'erreur et un snapshot de blocage cohérent est créé à la place d'un snapshot cohérent au niveau du système de fichiers. Vous pouvez consulter le moniteur des travaux et les journaux si un snapshot de blocage cohérent ou un snapshot cohérent au niveau du système de fichiers est créé.

Snapshots régionaux pour Google Cloud

Vous pouvez activer les snapshots régionaux pour les charges de travail Google Cloud lors de la création d'un plan de protection.

Si l'option de snapshot régional est activée, le snapshot sera créé dans la même région que le bien. Sinon, le snapshot sera créé à un emplacement occupant plusieurs régions.



Groupe de ressources de destination de snapshot pour Azure et Azure Stack Hub

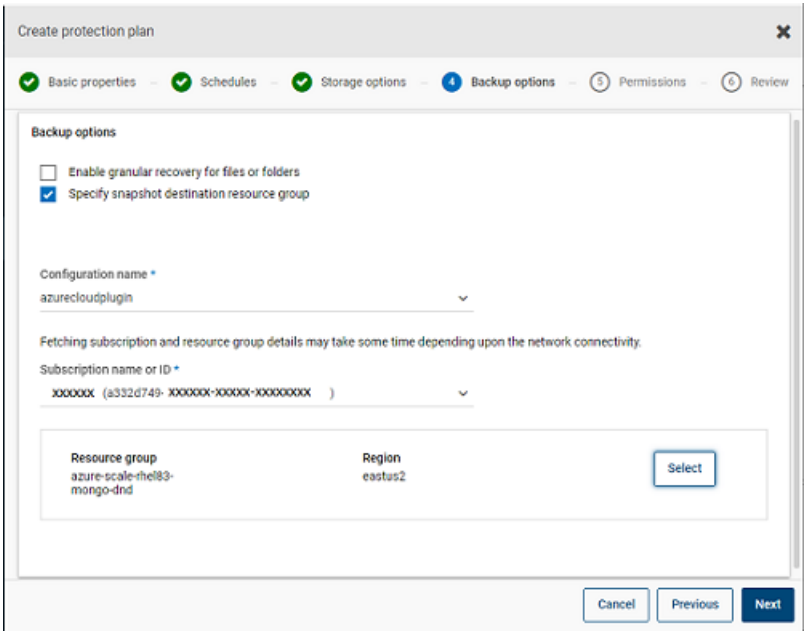
Vous pouvez spécifier un groupe de ressources pair de destination de snapshot lors de la création du plan de protection pour Azure ou Azure Stack Hub. Il reste

possible de définir un groupe de ressources pair en spécifiant un préfixe, mais vous pouvez désormais associer directement un snapshot à un groupe de ressources pair existant lors de la création d'un plan de protection.

Si vous avez sélectionné Microsoft Azure ou Azure Stack Hub comme fournisseur cloud lors de la création d'un plan de protection, vous pouvez sélectionner **Spécifier le groupe de ressources de destination du snapshot** pour associer des snapshots à un groupe de ressources pair particulier dans la même région que le bien. Sélectionnez ensuite une configuration, un abonnement et un groupe de ressources pour la destination de snapshot.

Le snapshot est stocké dans l'un des groupes de ressources cibles en appliquant les préférences suivantes :

- Un groupe de ressources de destination spécifié dans le plan de protection
- Un groupe de ressources préfixé et spécifié dans la configuration de plug-in (pour Azure uniquement)
- Un groupe de ressources dans lequel le bien existe, si aucune destination ou aucun groupe de ressources préfixé n'est spécifié dans NetBackup



Exclusion des disques sélectionnés de la sauvegarde

Vous pouvez configurer un plan de protection de façon à exclure certains disques de la sauvegarde et du snapshot qui s’appliquent à tous les fournisseurs cloud pris

en charge, y compris GCP. Vous évitez ainsi les images redondantes des disques qui n'ont pas besoin d'être sauvegardés et accélérez les sauvegardes en réduisant le volume de données à traiter.

Si vous créez un plan de protection pour les clouds AWS, Azure, Azure Stack Hub ou GCP, vous pouvez sélectionner l'option **Exclure les disques sélectionnés des sauvegardes** et spécifier les disques à ne pas inclure dans l'image de sauvegarde. Vous pouvez choisir d'exclure tous les disques qui ne sont pas des disques de démarrage ou les disques qui ont des balises spécifiques associées dans le compte de fournisseur cloud correspondant.

Remarque : Un plan de protection dont l'option d'exclusion de disque est activée peut être appliqué uniquement aux biens de type machine virtuelle cloud et aux groupes intelligents de machines virtuelles.

Lors de la restauration des machines virtuelles depuis l'onglet Points de récupération, reportez-vous à la colonne **Inclut des disques** pour afficher la liste de disques qui sont inclus ou exclus dans l'image de sauvegarde.

Pour la procédure complète, consultez la section sur la création d'un plan de protection dans le *guide de l'administrateur de l'interface utilisateur Web NetBackup*.

Remarques :

- Dans le cas de LVM, si des disques sont partiellement exclus, le système peut ne pas démarrer correctement.
- Lorsqu'un système de fichiers non pris en charge est configuré sur un disque et que l'utilisateur souhaite exclure ce disque du snapshot, un snapshot de blocage cohérent est créé.
- Si l'utilisateur souhaite exclure ce disque, l'indicateur **nofail** doit être associé au disque de données avant la prise d'un snapshot dans le fichier `/etc/fstab`. Cette opération est requise si l'utilisateur redémarre l'instance sans ce volume

(par exemple, après avoir déplacé le volume vers une autre instance). L'option de montage **nofail** permet à l'instance de démarrer même en cas d'erreur lors du montage du volume. Pour plus d'informations, consultez l'exemple d'entrée suivant dans le fichier `/etc/fstab` :

Par exemple, **UUID=aebf131c-6957-451e-8d34-ec978d9581ae /data xfs defaults,nofail 0 2**

- L'utilisateur doit s'assurer que les biens sont découverts correctement une fois que leurs étiquettes ont été modifiées par le fournisseur cloud. Une fois que l'exécution de la politique est planifiée pour un bien, les disques sont exclus en fonction des données découvertes uniquement. Si l'utilisateur connecte une étiquette alors que le snapshot est en cours, cette **étiquette** ne sera pas prise en compte dans l'exclusion. L'étiquette sera prise en compte lors du cycle de protection suivant une fois la découverte terminée.
- Dans le cas d'un système d'exploitation dont les paramètres régionaux ne sont pas définis sur l'anglais, si l'utilisateur opte pour l'exclusion basée sur une étiquette dans le plan de protection et si l'étiquette de disque comporte un caractère non anglais, l'exclusion de disque fonctionnera comme prévu. Cependant, dans certains cas, les étiquettes comportant un caractère non anglais ne sont pas correctement capturées dans les journaux job(try) et les journaux d'audit, bien qu'aucune fonctionnalité ne soit affectée, car l'exclusion de disque est correctement prise en compte.

Réplication de snapshot

La réplication d'un snapshot consiste à enregistrer une copie du snapshot à un autre emplacement. Dans AWS, cet emplacement peut être :

- une région différente dans le même compte.
- la même région dans un compte différent.
- une région différente dans un compte différent.

Par exemple, si les biens d'un administrateur cloud AWS se trouvent dans la région X, les snapshots de ces biens seront également enregistrés dans la région X. Pour une sécurité accrue, vous pouvez également répliquer les snapshots dans la région Y dans le même compte ou la région X/Y dans un compte différent. Dans la terminologie NBU Snapshot Manager, l'emplacement d'origine (X) est la source de réplication, et l'emplacement vers lequel les snapshots sont répliqués (Y) est l'emplacement de réplication.

La réplication s'effectue en trois étapes. Ce mécanisme est effectué en interne et l'ensemble du processus est totalement transparent pour l'utilisateur.

- Ne partagez le snapshot que si vous effectuez une réplication sur un compte croisé. Pour plus d'informations, consultez la section Partager un instantané de la documentation AWS.
- Copiez le snapshot. Pour plus d'informations, consultez la section CopySnapshot de la documentation AWS.
- N'annulez le partage du snapshot que si vous effectuez une réplication sur un compte croisé.

Configuration de la réplication de snapshot AWS

Conditions requises pour la réplication de snapshots

- **Réplication de snapshots non chiffrés**
  Assurez-vous que les comptes/régions sources et cibles sont configurés à l'aide du fournisseur cloud AWS dans NetBackup Snapshot Manager. Aucune autre condition n'est requise pour la réplication de snapshots non chiffrés.
- **Réplication de snapshots chiffrés à l'aide d'AWS KMS**
  Assurez-vous que les comptes/régions sources et cibles sont configurés à l'aide du fournisseur cloud AWS dans NetBackup Snapshot Manager.
  En outre, pour répliquer des snapshots chiffrés sur un compte croisé, la clé de chiffrement CMK de l'emplacement d'origine doit être partagée avec le compte cible. (Cette clé KMS partagée est implicitement utilisée lors de la copie du snapshot vers le compte cible et le snapshot copié peut être répliqué à l'aide d'une clé différente).
  Les emplacements source et cible doivent disposer d'une clé de chiffrement (clé KMS) du même nom, c'est-à-dire qu'ils doivent disposer du même alias de clé (AWS).
  Si la clé de chiffrement portant le même nom n'est pas présente sur la cible, le snapshot répliqué est chiffré à l'aide de la clé KMS par défaut dans l'emplacement cible.
- **Autorisations de réplication sur un compte croisé**
  Pour la réplication sur un compte croisé, l'utilisateur ou le rôle AWS IAM associé au compte AWS de la région source du snapshot (compte AWS source) doit disposer des autorisations suivantes :
  - `ModifySnapshotAttribute` et `CopySnapshot` sur l'instance EC2.
  - `DescribeKey` et `ReEncrypt` sur la clé KMS utilisée pour le chiffrement du snapshot d'origine.

Pour la réplication sur un compte croisé, l'utilisateur ou le rôle AWS IAM associé au compte AWS de la région cible du snapshot (compte AWS cible) doit disposer des autorisations suivantes :

- `CreateGrant`, `DescribeKey` et `Decrypt` sur la clé KMS utilisée pour le chiffrement du snapshot d'origine.
- `CreateGrant`, `Encrypt`, `Decrypt`, `DescribeKey` et `GenerateDataKeyWithoutPlainText` sur la clé de chiffrement KMS utilisée lors de l'exécution de l'opération `CopySnapshot` sur le snapshot d'origine.

Vous pouvez choisir de répliquer des snapshots de biens cloud AWS de l'emplacement principal vers un emplacement secondaire ou distant. Les Snapshot Managers prennent en charge la réplication entre régions et entre comptes. La réplication de snapshot vous permet d'effectuer les actions suivantes :

- Conserver une copie des biens cloud à un emplacement différent pour la conservation à long terme et les exigences d'audit.
- Récupérer des biens cloud des copies répliquées à partir d'une autre région en cas de panne de la région.
- Récupérer des biens cloud des copies répliquées à partir d'un autre compte dans le cas où le compte utilisateur est compromis.

Configuration

Consultez les informations suivantes pour configurer la réplication de snapshot :

- Vous pouvez configurer la réplication de snapshot quand vous créez un plan de protection. Consultez le Guide de l'administrateur de l'interface utilisateur Web NetBackup™.
- Pour la réplication entre comptes, vous devez établir une relation de confiance entre les comptes source et cible. Pour plus de détails, consultez les informations de la section *Comptes AWS croisés à l'aide des rôles IAM* dans la documentation relative à *Amazon Web Services*.

Remarques

Tenez compte des éléments suivants lorsque vous configurez la réplication de snapshot cloud :

- Même si plusieurs planifications sont configurées, la région de destination de réplication configurée est appliquée à toutes les planifications.
- La réplication de snapshot cloud est prise en charge uniquement pour les fournisseurs cloud Amazon.

Critères de protection de bien

Tenez compte des points suivants avant d'ajouter des biens cloud à un plan de protection configuré pour la réplication de snapshot cloud :

- Les biens doivent être ajoutés à un plan de protection qui réplique des snapshots sur une région différente.
  Par exemple, les biens résidant dans la région « aws_account_1-us-east-1 » ne peuvent pas être abonnés à un plan de protection répliquant sur la même région « aws_account_1-us-east-1 ».
- Les biens peuvent être répliqués sur un autre compte dans la même région.
  Par exemple, les biens résidant dans la région « aws_account_1-us-east-1 » peuvent être abonnés à un plan de protection répliquant sur la même région, mais sur un autre compte « aws_account_2-us-east-1 ».
- Les biens découverts par un Snapshot Manager doivent être répliqués vers la région découverte par ce Snapshot Manager.
  Par exemple, les biens découverts par le Snapshot Manager ‘CP1’ ne peuvent pas être abonnés à un plan de protection qui effectue la réplication vers une région découverte par le Snapshot Manager ‘CP2’.
- Seuls les biens Amazon peuvent être abonnés à un plan de protection configuré pour la réplication de snapshot cloud.

Gérer les réplications de snapshot simultanées

Pour de meilleures performances, vous pouvez régler le nombre de réplications de snapshot simultanées. Amazon présente des limites différentes pour chaque type de bien afin d'effectuer des réplications de snapshot simultanées sur une région de destination unique. Par exemple, RDS a une limite de 5, EBS a une limite de 5 et EC2 a une limite de 50. Pour plus de détails, consultez les informations de la section *Snapshot de copie* dans la documentation relative à *Amazon Web Services*.

Dans NetBackup, cette limite est définie à l'aide du paramètre suivant dans le fichier `bp.conf` :

```
MAX_CLOUD_SNAPSHOT_REPLICATION_JOBS_PER_DESTINATION
```

La valeur par défaut est 5.

Utilisation d'une réplication de snapshot AWS

Cette section explique comment créer des répliques de snapshots à l'aide de la fonction de réplication de snapshot AWS et restaurer les snapshots répliqués chaque fois que nécessaire. Sauf indication contraire, consultez le *Guide d’installation et de mise à niveau de NetBackup Snapshot Manager* et le *Guide de*

l'administrateur de l'interface utilisateur Web NetBackup pour en savoir plus sur ces étapes.

Création de réplications de snapshot

Cette section décrit comment configurer la région source pour créer des répliques de snapshots dans la région cible.

Pour créer des répliques

1. Ajoutez Snapshot Manager (CP1) dans l'interface utilisateur Web.

   Se reporter à "Ajout de Snapshot Manager" à la page 12.

2. Ajoutez le plug-in AWS des régions source et cible pour la réplication.
3. Créez un plan de protection et sélectionnez **Région** et **Compte**.

   Se reporter à "Configuration de la planification de sauvegarde pour les charges de travail cloud" à la page 43.

4. Connectez et configurez une machine virtuelle invitée cohérente au niveau application à l'aide de l'agent OnHost.
5. Lancez la sauvegarde par snapshot et répliquez les snapshots à l'aide du plan de protection.
6. Vérifiez les points de récupération pour la copie de snapshot et de réplique.

Restauration à partir des répliques de snapshots dans la région cible

Si la région source échoue, vous pouvez restaurer les machines virtuelles appartenant à cette région, à partir de la région cible où vous avez pris les répliques de snapshot. La région source étant défaillante, vous devez d'abord restaurer les machines virtuelles dans la région cible.

Remarque : Vous ne pouvez pas restaurer de fichiers ou de dossiers individuels à partir d'une réplique découverte par un autre Snapshot Manager dans une région ayant basculé.

Restauration dans la région cible

1. Désactivez le serveur CP1 dans la région source à partir de l'interface utilisateur Web.

   Se reporter à "Activation ou désactivation d'un Snapshot Manager" à la page 19.

2. Enregistrez un nouveau Snapshot Manager (CP2) dans la région cible à partir de l'interface utilisateur Web.

3 Ajoutez le plug-in AWS pour la région et le compte cibles uniquement. Laissez la découverte se terminer.

4 Pour restaurer des machines virtuelles :

- Connectez-vous à l'interface utilisateur Web NetBackup.
- Dans la partie gauche, cliquez sur **Charges de travail > Cloud**. Dans l'onglet **Machines virtuelles**, cliquez sur l'ordinateur que vous souhaitez récupérer.
- Cliquez sur l'onglet **Points de récupération**. Dans la liste d'images, cliquez sur **Restaurer** en regard de l'image de **réplique** requise, puis cliquez sur **Restaurer la machine virtuelle**.
- Pour modifier le nom d'affichage de la machine virtuelle, entrez un nouveau nom.
- Sélectionnez un sous-réseau (chemin d'accès au sous-réseau avec VPC). Se reporter à "Récupération des biens cloud" à la page 92.

5 Ajoutez le groupe de sécurité approprié aux machines virtuelles restaurées pour activer l'accès à distance.

6 Désinstallez et réinstallez l'agent Snapshot Manager des machines virtuelles restaurées, puis enregistrez les agents Snapshot Manager auprès du nouveau serveur CP2.

7 Exécutez une découverte approfondie à partir de la console du fournisseur AWS.

8 Créez un plan de protection pour protéger les machines virtuelles restaurées. Lancez une sauvegarde par snapshot.

Restauration vers la région source à partir de la région cible

Vous pouvez restaurer les machines virtuelles de la région cible vers la région source, une fois que la région source est de nouveau en ligne.

Restauration vers la région source

1 Modifiez le plug-in AWS pour CP2 et ajoutez la région source.

2 Créez un plan de protection pour créer une réplique de snapshot dans la région source.

3 Lancez une sauvegarde par snapshot et répliquez-la.

4 Désactivez le serveur CP2 dans l'interface utilisateur Web. Se reporter à "Activation ou désactivation d'un Snapshot Manager" à la page 19.

5 Activez le serveur CP1 et lancez la découverte détaillée à partir de la console du fournisseur AWS.

6 Effectuez une restauration complète des machines virtuelles à partir de la région cible.

7 Ajoutez le groupe de sécurité approprié pour activer l'accès à distance aux machines virtuelles restaurées.

8 Désinstallez et réinstallez les agents Snapshot Manager sur les machines virtuelles restaurées. Puis, inscrivez les agents Snapshot Manager auprès du serveur CP1.

9 Exécutez une découverte détaillée à partir de la console AWS.

10 Utilisez le plan de protection existant pour protéger les nouvelles machines virtuelles restaurées.

Matrice de prise en charge pour la réplication de compte

Tableau 1-9 Matrice de prise en charge pour la réplication sur un même compte

Types de biens	Bien source (région X)	Snapshot source (région X)	Snapshot répliqué (région Y)
Volume EBS, instance EC2 et RDS/Aurora	Non chiffré	Non chiffré	Non chiffré
	Disques connectés chiffrés à l'aide de la clé AWS KMS par défaut	Disques connectés chiffrés à l'aide de la clé AWS KMS par défaut	Disques connectés chiffrés à l'aide de la clé AWS KMS par défaut
	Chiffré à l'aide d'une clé CMK AWS KMS (avec Alias ABC)	Chiffré à l'aide d'une clé CMK AWS KMS (Alias ABC)	Chiffré à l'aide d'une clé CMK AWS KMS nommée si présente (liste d'alias) ou chiffré à l'aide de la clé AWS KMS par défaut.

Tableau 1-10 Matrice de prise en charge pour la réplication sur un compte différent dans une même région

Types de biens	Bien source (compte A, région X)	Snapshot source (compte A, région X)	Snapshot répliqué (compte B, région Y)
Volume EBS, instance EC2 et RDS/Aurora	Non chiffré	Non chiffré	Non chiffré
	Chiffré à l'aide de la clé AWS KMS par défaut	Chiffré à l'aide de la clé AWS KMS par défaut	Non pris en charge
	Chiffré à l'aide d'une clé CMK AWS KMS (avec Alias ABC)	Chiffré à l'aide d'une clé CMK AWS KMS (avec Alias ABC)	Chiffré à l'aide d'une clé CMK AWS KMS nommée si présente (avec Alias ABC) ou chiffré à l'aide de la clé AWS KMS par défaut.

Tableau 1-11 Matrice de prise en charge pour la réplication sur un compte différent dans une région différente

Types de biens	Bien source (compte A, région X)	Snapshot source (compte A, région X)	Snapshot répliqué (compte B, région Y)
Volume EBS et instance EC2	Non chiffré	Non chiffré	Non chiffré
	Chiffré à l'aide de la clé AWS KMS par défaut	Chiffré à l'aide de la clé AWS KMS par défaut	Non pris en charge
	Chiffré à l'aide d'une clé CMK AWS KMS (avec Alias ABC)	Chiffré à l'aide d'une clé CMK AWS KMS (avec Alias ABC)	Chiffré à l'aide d'une clé CMK AWS KMS nommée si présente (avec Alias ABC) ou chiffré à l'aide de la clé AWS KMS par défaut.

Types de biens	Bien source (compte A, région X)	Snapshot source (compte A, région X)	Snapshot répliqué (compte B, région Y)
RDS	Non chiffré	Non chiffré	Non chiffré
	Chiffré à l'aide de la clé AWS KMS par défaut	Chiffré à l'aide de la clé AWS KMS par défaut	Non pris en charge
	Chiffré à l'aide de la clé AWS KMS par défaut	Chiffré à l'aide de la clé AWS KMS par défaut	Non pris en charge
Aurora	Non chiffré	Non chiffré	Non pris en charge
	Chiffré à l'aide de la clé AWS KMS par défaut	Chiffré à l'aide de la clé AWS KMS par défaut	Non pris en charge
	Chiffré à l'aide de la clé AWS KMS par défaut	Chiffré à l'aide de la clé AWS KMS par défaut	Non pris en charge

Protéger des applications sur le cloud avec les snapshots cohérents au niveau des applications

Vous pouvez prendre des snapshots cohérents au niveau application (à un moment précis) des applications déployées sur des machines virtuelles dans le cloud. Cela vous permet d'assurer la récupération des applications à un moment précis.

Vous pouvez effectuer des restaurations à l'emplacement d'origine et à un autre emplacement pour ces charges de travail.

Pour la restauration à un autre emplacement, considérez ce qui suit :

- Pour les autres emplacements de restauration des charges de travail MS SQL, l'hôte cible doit être découvert, mais l'application ne doit pas être connectée ou configurée.
- Pour les autres emplacements de restauration des charges de travail Oracle, l'hôte cible doit être découvert, mais l'application ne doit pas être connectée ou configurée.

Avant de commencer

Assurez-vous que la base de données est préparée pour les snapshots. Pour plus de détails, consultez les remarques relatives à la configuration des plug-ins dans la documentation de Veritas Snapshot Manager.

Pour configurer des applications pour la récupération spécifique

1. Connectez-vous à la machine virtuelle qui héberge les applications.
   - Après avoir découvert les biens cloud, accédez à l'onglet **Machines virtuelles**.
   - Sélectionnez la machine virtuelle qui héberge l'application. Dans le coin supérieur droit, cliquez sur **Gérer les informations d'authentification**.
   - Entrez les informations d'authentification. Si les informations d'authentification de la machine virtuelle ne sont pas configurées, vous devez les configurer. Consultez le chapitre *Gestion des informations d'authentification* du *Guide de l'administrateur de l'interface utilisateur Web*.
   - Une fois que les machines virtuelles sont connectées, leur état devient **Connecté**.
2. Sélectionnez la machine virtuelle qui héberge l'application. En haut à droite, cliquez sur **Configurer l'application**.
3. Une fois le processus terminé, l'état de l'application passe à Configuré.
4. Les applications sont affichées sous l'onglet **Applications** à l'issue de la découverte suivante.
5. Appliquez le plan de protection. Consultez le *Guide de l'administrateur de l'interface utilisateur Web NetBackup*.

Pour modifier ou mettre à jour les informations d'authentification des machines virtuelles

1. Accédez à l'onglet **Machines virtuelles**.
2. Sélectionnez les machines virtuelles pour lesquelles vous voulez mettre à jour les informations d'authentification. Dans le coin supérieur droit, cliquez sur **Gérer les informations d'authentification**.
3. Mettez à jour les informations d'authentification.

Pour modifier ou mettre à jour la configuration de l'application

1. Accédez à l'onglet **Applications**.
2. Sélectionnez l'application à mettre à jour. Dans le coin supérieur droit, cliquez sur **Modifier la configuration**
3. Mettez à jour les informations d'authentification et cliquez sur **Configurer**.

Protection des biens PaaS

Vous pouvez gérer les biens PaaS une fois ces derniers découverts par NetBackup. Ces biens s'affichent dans les onglets **PaaS** et **Applications**, dans la section de la charge de travail cloud. L'onglet **Applications** affiche les biens RDS, tandis que l'onglet **PaaS** affiche les biens autres que RDS. Vous pouvez afficher, protéger et récupérer des biens PaaS à partir de ces deux onglets.

Conditions préalables pour la protection des biens PaaS

NetBackup permet de découvrir, protéger et restaurer plusieurs types de biens PaaS sur différentes plates-formes cloud. Cette section présente les plates-formes et les bases de données prises en charge.

Fournisseurs cloud pris en charge

NetBackup vous permet de protéger des biens PaaS avec les fournisseurs cloud suivants :

- Microsoft Azure
- AWS
- GCP

Bases de données prises en charge pour différents fournisseurs

Le tableau suivant répertorie les bases de données prises en charge pour chaque fournisseur cloud.

Tableau 1-12 Bases de données prises en charge par PaaS

Fournisseurs	Bases de données prises en charge
Microsoft Azure	PostgreSQL, SQL Managed Instance, SQL, MariaDB, Azure Cosmos DB for NoSQL, Azure Cosmos DB for MongoDB et MySQL **Les composants suivants ne sont pas pris en charge :** Azure SQL : pool Elastic Azure SQL Managed Instance - Azure Arc Azure Cosmos DB for MongoDB vCore Azure PostgreSQL : groupe de serveurs Hyperscale (Citus) et PostgreSQL Hyperscale avec Azure Arc

Fournisseurs	Bases de données prises en charge
AWS	RDS SQL, RDS PostgreSQL, RDS MySQL, RDS MariaDB, RDS Aurora MySQL, RDS Aurora PostgreSQL, Amazon RDS for Oracle, Amazon Redshift et DynamoDB
GCP	Cloud SQL for PostgreSQL, Cloud SQL for SQL Server et Cloud SQL for MySQL

Plates-formes prises en charge

Cette section présente les plates-formes prises en charge pour les serveurs principaux et de médias.

Tableau 1-13 Plates-formes prises en charge pour PaaS

Serveur NetBackup	Plate-forme prise en charge
Serveur principal	RHEL, SUSE et Windows
Serveur de médias	RHEL
Serveur de stockage	Partage universel sur le stockage de blocs MSDP sous-jacent ou l'unité de stockage cloud MSDP

Autorisations requises pour le fournisseur cloud

Les informations d'authentification que vous utilisez pour ajouter les fournisseurs cloud doivent disposer de toutes les autorisations et privilèges requis, comme indiqué dans le *Guide d'installation et de mise à niveau de NetBackup Snapshot Manager*.

Ports pris en charge

Voici les ports pris en charge pour différentes bases de données PaaS.

Tableau 1-14 Ports pris en charge pour PaaS

Charge de travail PaaS de la base de données	Ports pris en charge
Azure SQL Server	1433
Instance gérée par Azure SQL	1433
Azure MySQL	3306
Azure PostgreSQL	5432

Charge de travail PaaS de la base de données	Ports pris en charge
Azure MariaDB	3306
GCP PostgreSQL	5432
GCP MySQL	3306
AWS DynamoDB	N/A
AWS RDS PostgreSQL	5432
AWS RDS MySQL	3306
AWS MariaDB	3306
AWS RDS AuroraDB Postgres	5432
AWS RDS AuroraDB MySQL	3306
AWS RDS SQL Server	1433
Amazon RDS for Oracle	1521
Azure Cosmos DB for NoSQL	443
Azure Cosmos DB for MongoDB	10255
Port GCP SQL Server	1433
Amazon Redshift	5439

Activation de la consignation binaire pour les bases de données MySQL

- Pour AWS, consultez la page https://aws.amazon.com/premiumsupport/knowledge-center/rds-mysql-functions/
- Pour Azure, définissez la valeur du paramètre `log_bin_trust_function_creators` sur 1, comme décrit sur la page suivante : https://learn.microsoft.com/fr-fr/azure/mysql/single-server/how-to-server-parameters
- Pour GCP, procédez comme suit :
  - Ouvrez l'instance et cliquez sur **Modifier**.

- Faites défiler jusqu'à la section **Indicateurs**.
- Pour définir un indicateur, cliquez sur **Ajouter un élément**, sélectionnez l'indicateur **log_bin_trust_function_creators** dans le menu déroulant et définissez sa valeur sur « on ».
- Cliquez sur **Enregistrer** pour enregistrer les modifications. Vous pouvez confirmer les modifications sous **Indicateurs** dans la page **Vue d'ensemble**.

Installation des utilitaires client natifs

Si vous utilisez une configuration BYO (Build-Your-Own), vous devez installer les utilitaires client natifs dans votre environnement NetBackup pour que votre charge de travail PaaS fonctionne.

Pour les déploiements NetBackup dans AKS (Azure Kubernetes Services) ou EKS (Elastic Kubernetes Services), les utilitaires client natifs sont fournis dans le package du serveur de médias NetBackup, du serveur principal et de l'image de conteneur système de déplacement des données. Aucune installation manuelle n'est requise pour eux.

Assurez-vous que les paramètres réseau, tels que le pare-feu, le groupe de sécurité et la configuration DNS sont correctement définis pour permettre l'accès aux bases de données du fournisseur cloud.

Remarque : Si l'un de ces packages est déjà installé sur le ou les serveurs de médias, supprimez-le pour éviter tout conflit avec les dernières versions des packages que vous installez.

Installation de l'utilitaire client MySQL

Remarque : La version recommandée de l'utilitaire client MySQL est 8.0.34.

Emplacement de téléchargement de RPM	https://downloads.mysql.com/archives/community/

Pour procéder à l'installation, exécutez les commandes suivantes sur le terminal :

1. `rpm -ivh mysql-community-common-<version_no>.x86_64.rpm`
2. `rpm -ivh mysql-community-client-plugins- <version_no>.x86_64.rpm`

3 `rpm -ivh mysql-community-libs- <version_no>.x86_64.rpm`

4 `rpm -ivh mysql-community-client- <version_no>.x86_64.rpm`

Remarque : Évitez d'utiliser la version 8.0.32 de l'utilitaire client MySQL, car elle contient un bogue signalé par MySQL.

Installation de l'utilitaire client sqlpackage

Remarque : Il est recommandé d'installer la version 19.2 (build 162.0.52) de l'utilitaire client `sqlpackage`.

Emplacements de téléchargement
https://docs.microsoft.com/fr-fr/sql/tools/
/sqlpackage-download?view=sql-server-ver15

https://packages.microsoft.com/rhel/7/prod/msodbcsql17-17.9.1.1-1.x86_64.rpm

https://packages.microsoft.com/rhel/7/
prod/unixODBC-2.3.7-1.rh.x86_64.rpm

Pour procéder à l'installation, exécutez les commandes suivantes sur le terminal :

1 `cd ~`

2 `mkdir sqlpackage`

3 `unzip ~/Downloads/sqlpackage-linux-<version string>.zip -d ~/sqlpackage`

4 `echo "export PATH=\"\$PATH:$HOME/sqlpackage\""> ~/.bashrc`

5 `chmod a+x ~/sqlpackage/sqlpackage`

6 `source ~/.bashrc`

Remarque : Vérifiez que `sqlpackage` a été ajouté comme variable de chemin d'accès par défaut. Si l'erreur indiquant que `sqlpackage` est introuvable persiste, redémarrez les services NetBackup sur le serveur de médias.

---

7 `sqlpackage`

8 `rpm -ivh unixODBC-2.3.7-1.rh.x86_64.rpm`

9 `rpm -ivh msodbcsql17-17.10.2.1-1.x86_64.rpm`

Les utilisateurs de RHEL 9 effectuent les étapes supplémentaires suivantes :

1. Téléchargez Microsoft.NETCore.App.Runtime.linux-x64 en cliquant sur le lien :

   https://www.nuget.org/api/v2/package/Microsoft.NETCore.App.Runtime.linux-x64/6.0.10

   Recherchez le fichier :
   `microsoft.netcore.app.runtime.linux-x64.6.0.10.nupkg`.
2. Extrayez le fichier à l'aide d'un outil de décompression tel que 7zip.
3. Accédez à :

   microsoft.netcore.app.runtime.linux-x64.6.0.10.nupkg\runtimes\linux-x64\lib\net6.0\
4. Copiez le fichier `System.Security.Cryptography.X509Certificates.dll` dans le dossier `~/sqlpackage` créé à l'étape 2 de la tâche d'installation de l'utilitaire client *sqlpackage*.

Si vous connectez le serveur de médias 10.1 en tant que serveur de médias externe avec la version 10.1.1 de NetBackup, effectuez les étapes suivantes sur le serveur de médias 10.1.

Pour une configuration BYO NetBackup :

- Exécutez la commande suivante :
  `mkdir -p <backup and restore ushare export path>`
- Vérifiez la valeur de `Defaultvers` de NFS dans le fichier `/etc/nfsmount.conf`.
  - Si la valeur de `Defaultvers` est `nfs3`, montez le chemin d'accès ushare de sauvegarde et de restauration avec l'option `nolock`. Par exemple : `mount <ushare mount path> <ushare export path> -o nolock`
  - Si la valeur de `Defaultvers` est `nfs4`, montez le chemin d'accès ushare de sauvegarde et de restauration sans l'option `nolock`.

Pour une instance de NetBackup déployée dans des environnements AKS et EKS :

- Exécutez la commande suivante :
  `mkdir -p <backup and restore ushare export path>`
- Vérifiez la valeur de `Defaultvers` de NFS dans le fichier `/etc/nfsmount.conf`.
  - Si la valeur de `Defaultvers` est `nfs3`, montez le chemin d'accès ushare de sauvegarde et de restauration avec l'option `nolock`. Par exemple : `mount <ushare mount path> <ushare export path> -o nolock`
  - Si la valeur de `Defaultvers` est `nfs4`, montez le chemin d'accès ushare de sauvegarde et de restauration de version v4 sans l'option `nolock`.

Installation de l'utilitaire client PostgresSQL

Il est recommandé d'utiliser la version 15.3 de l'utilitaire client PostgresSQL.

Emplacements de téléchargement		
	RHEL 7	https://download.postgresql.org/pub/repos/yum/15/redhat/rhel-7-x86_64/
	RHEL 8	https://download.postgresql.org/pub/repos/yum/15/redhat/rhel-8-x86_64/
	RHEL 9	https://download.postgresql.org/pub/repos/yum/15/redhat/rhel-9-x86_64/

Pour procéder à l'installation, exécutez les commandes suivantes sur le terminal :

1. `rpm -ivh postgresql15-libs-15.3-1PGDG.rhel7.x86_64.rpm`
2. `rpm -ivh postgresql15-15.3-1PGDG.rhel7.x86_64.rpm`

> **Remarque :** Le `package de compression lz4` et `libicu` sont requis par `postgresql15-15.3-1PGDG.rhel8.x86_64.rpm` sur RHEL 8 et 9.

Installation de l'utilitaire client MongoDB

La version recommandée de l'utilitaire client MongoDB est 100.7.3.

Emplacements de téléchargement		
	RHEL 7	https://fastdl.mongodb.org/tools/db/mongodb-database-tools-rhel70-x86_64-100.7.3.rpm
	RHEL 8	https://fastdl.mongodb.org/tools/db/mongodb-database-tools-rhel80-x86_64-100.7.3.rpm
	RHEL 9	https://fastdl.mongodb.org/tools/db/mongodb-database-tools-rhel90-x86_64-100.7.3.rpm

Pour procéder à l'installation, exécutez les commandes suivantes sur le terminal :

```
rpm -ivh mongodb-database-tools-rhel70-x86_64-100.7.3.rpm
```

Installation de l'utilitaire client Amazon RDS for Oracle

La version 21.11.0.0.0-1.el8 est recommandée pour l'utilitaire client Amazon RDS for Oracle.

Emplacements de téléchargement		
	instantclient-basic	https://download.oracle.com/otn_software/linux/instantclient/2111000/oracle-instantclient-basic-21.11.0.0.0-1.el8.x86_64.rpm
	instantclient-odbc	https://download.oracle.com/otn_software/linux/instantclient/2111000/oracle-instantclient-odbc-21.11.0.0.0-1.el8.x86_64.rpm

Pour procéder à l'installation, exécutez les commandes suivantes sur le terminal :

1. `c. yum install unixODBC`
2. `rpm -ivh oracle-instantclient-basic-21.10.0.0.0-1.el8.x86_64.rpm`
3. `d. rpm -ivh oracle-instantclient-odbc-21.10.0.0.0-1.el8.x86_64.rpm`

Installation de l'utilitaire EFS et configuration des autorisations

Pour installer l'utilitaire EFS

1. Consultez la page suivante de la documentation AWS :

   https://docs.aws.amazon.com/efs/latest/ug/installing-amazon-efs-utils.html#https://docs.aws.amazon.com/fr_fr/efs/latest/ug/installing-amazon-efs-utils.html

2. Consultez la section *Pour créer et installer amazon-efs-utils en tant que package RPM pour Amazon Linux, Amazon Linux 2 et les distributions Linux autres qu'openSUSE ou SLES*.
3. Installez la version 5 de `stunnel`.
4. Remplacez la région de `/etc/amazon/efs/efs-utils.conf` par la région de votre instance RDS.

Configuration d'EFS et du chemin de montage de restauration sur AWS

Avant de pouvoir effectuer des opérations de sauvegarde ou de restauration, vous devez configurer Amazon Elastic File System (EFS). Pour la restauration, vous devez également configurer le chemin de montage EFS.

- Pour configurer EFS, consultez l'article de base de connaissances suivant : https://www.veritas.com/support/en_US/article.100059038
- Pour configurer le chemin de montage pour la restauration, consultez l'article de base de connaissances suivant : https://www.veritas.com/support/en_US/article.100059039

Configuration des autorisations AWS pour NetBackup

NetBackup requiert des autorisations pour effectuer des sauvegardes et des restaurations dans AWS. Pour configurer les autorisations, créez un rôle AWS IAM et assignez-lui les autorisations requises par NetBackup. Pour plus d'informations sur la création d'un rôle IAM, consultez le lien suivant dans la documentation AWS :

https://docs.aws.amazon.com/iam/index.html

Autorisations requises :

```
efsdescribemounttarget:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "elasticfilesystem:DescribeMountTargets",
                "elasticfilesystem:DescribeFileSystems",
            ],
            "Resource": [
                "arn:aws:elasticfilesystem:*:*:access-point/*",
                "arn:aws:elasticfilesystem:*:*:file-system/*"
            ]
        }
    ]
}

rdsdescribeoptiongroup
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "rds:DescribeOptionGroupOptions",
            "Resource": "arn:aws:rds:*:*:og:*"
        }
    ]
}

AmazonRDSReadOnlyAccess:(AWS Managed)
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "rds:Describe*",
                "rds:ListTagsForResource",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeAvailabilityZones",
```

```
                "ec2:DescribeInternetGateways",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeVpcs"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:ListMetrics",
                "cloudwatch:GetMetricData",
                "logs:DescribeLogStreams",
                "logs:GetLogEvents",
                "devops-guru:GetResourceCollection"
            ],
            "Resource": "*"
        },
        {
            "Action": [
                "devops-guru:SearchInsights",
                "devops-guru:ListAnomaliesForInsight"
            ],
            "Effect": "Allow",
            "Resource": "*",
            "Condition": {
                "ForAllValues:StringEquals": {
                    "devops-guru:ServiceNames": [
                        "RDS"
                    ]
                },
                "Null": {
                    "devops-guru:ServiceNames": "false"
                }
            }
        }
    ]
}
```

Configuration du serveur de stockage pour l'accès instantané

La configuration suivante est requise pour que votre serveur de stockage puisse prendre en charge l'accès aux instances.

1. Assurez-vous que NFS et NGINX sont installés.
2. La version de NGINX doit être identique à celle de la version officielle de RHEL correspondante. Vous devez l'installer à partir de la source Yum RHEL correspondante (EPEL).
3. Vérifiez que les packages `policycoreutils` et `policycoreutils-python` sont installés à partir de la même source Yum RHEL (serveur RHEL). Exécutez les commandes suivantes :
   - `semanage port -a -t http_port_t -p tcp 10087`
   - `setsebool -P httpd_can_network_connect 1`
4. Assurez-vous qu'aucun point de montage direct n'est créé pour le dossier `/mnt` du serveur de stockage. Montez uniquement les points de montage sur leurs sous-dossiers.
5. Activez l'autorisation `logrotate` dans `selinux` à l'aide de la commande suivante :

   ```
   semanage permissive -a logrotate_t
   ```

Configuration du stockage pour différents déploiements

Cette section décrit la procédure de configuration du stockage pour différents déploiements NetBackup.

Pour les déploiements cloud MSDP

Les cibles de stockage MSDP utilisent les serveurs de médias. L'utilitaire client natif doit être installé sur le serveur de médias qui doit disposer d'une connectivité à la charge de travail PaaS.

Pour le stockage de volume cloud MSDP, NetBackup protège les biens PaaS via le conteneur de système de déplacement des données (DMC), à l'aide de l'accélérateur de partage universel.

L'accélérateur de partage universel requiert au minimum 500 Go d'espace de stockage, en tant que stockage persistant pour stocker les métadonnées temporaires dans le DMC. Ce chemin d'accès au stockage doit être identique à celui utilisé dans le serveur de stockage MSDP.

Déploiements Kubernetes

Tenez compte des points suivants :

- Créez les revendications de volume persistant à l'aide des classes de stockage basées sur disque et de suppression de politique et connectez-vous au conteneur à l'emplacement du stockage.
- Il est recommandé d'utiliser la classe de stockage par défaut avec la taille par défaut de 600 Gio. Pour modifier la classe de stockage ou la taille du stockage, vous devez mettre à jour le mappage de configuration `pdconf` du déploiement Kubernetes, comme suit :

```
STORAGE_CLASS=<disk based storage class>
STORAGE_SIZE=<pv size>
```

Déploiements BYO basés sur une machine virtuelle

Tenez compte des points suivants :

- Montez un nouveau disque avec un stockage de 600 Go dans NetBackup Snapshot Manager, à l'emplacement suivant `:/stockage_système_déplacement_données`.
- Chaque conteneur de système de déplacement des données crée un répertoire à l'emplacement du disque monté et crée un lien symbolique comme chemin d'accès au stockage. Ce chemin d'accès apparaît dans le conteneur du système de déplacement des données comme chemin d'accès au stockage. Il est identique au chemin d'accès du stockage MSDP utilisé pour le stockage temporaire des opérations de l'accélérateur de partage universel.

Si vous n'avez pas suffisamment d'espace de stockage disponible lors du déploiement, vous pouvez modifier les conditions requises pour stockage. Procédez comme suit :

1. Accédez à `/cloudpoint/openv/netbackup/vpfs_override_parameters.json`.
2. Mettez à jour le paramètre `CloudCacheSize` avec la taille de stockage disponible en Go.

```
{
"DataTransferManagementOptions": {
"CloudCacheSize": 200
}
}
```

À propos des sauvegardes incrémentielles pour les charges de travail PaaS

NetBackup prend en charge la sauvegarde incrémentielle différentielle pour les charges de travail Azure SQL Server, Azure SQL Managed Instance et GCP SQL Server. Les sauvegardes incrémentielles réduisent considérablement la fenêtre de sauvegarde dans NetBackup. Avec cette méthode, NetBackup sauvegarde uniquement les données modifiées depuis la dernière sauvegarde complète.

La sauvegarde incrémentielle différentielle est compatible uniquement avec les charges de travail pour lesquelles la fonction de capture des données modifiées sur Azure SQL Server, GCP SQL Server et Azure SQL Managed Instance est activée.

Recommandations concernant l'utilisation des sauvegardes incrémentielles pour les charges de travail PaaS :

- Dans une politique, définissez une période de conservation plus longue pour les sauvegardes complètes que pour les sauvegardes incrémentielles. Une restauration complète requiert la sauvegarde complète précédente plus toutes les sauvegardes incrémentielles ultérieures. Si la sauvegarde complète arrive à expiration avant les sauvegardes incrémentielles, vous ne pourrez peut-être pas restaurer tous les fichiers.
- Utilisez un stockage pour les sauvegardes complètes et incrémentielles.
- Ne créez pas de copie à long terme pour les sauvegardes incrémentielles.
- Ne faites pas expirer des images de sauvegarde incrémentielle aléatoires. Leur expiration peut entraîner une incohérence au niveau de l'application en raison de la perte de données. NetBackup utilise la sauvegarde complète précédente et toutes les sauvegardes incrémentielles suivantes.
- Lors de la duplication, assurez-vous que les copies de sauvegarde complète et incrémentielle sont dupliquées sur le stockage cible. L'absence d'une image complète ou incrémentielle précédente peut entraîner une perte de données.
- Lors de l'importation, assurez-vous que les copies de sauvegarde complète et incrémentielle sont importées. L'absence d'une image complète ou incrémentielle précédente peut entraîner une défaillance.

Limitations et remarques

Tenez compte de ce qui suit pour la protection des charges de travail dans le cloud.

Pour toutes les bases de données

- Les déploiements de NetBackup sous Flex Appliance et Flex Scale ne sont pas compatibles avec les charges de travail PaaS.

- Prend en charge uniquement les ports par défaut pour toutes les bases de données de différents fournisseurs. Les instances de charge de travail configurées avec des ports personnalisés ne sont pas prises en charge.
- Les noms de base de données contenant les caractères « # » et « / » ne sont pas pris en charge pour les opérations de sauvegarde et de restauration. En outre, le nom de base de données doit respecter les conventions de nommage suggérées par les fournisseurs de cloud.
- Le point-virgule (« ; ») n'est pas pris en charge dans les mots de passe de serveur ou de base de données.
- La sauvegarde et la restauration d'une base de données contenant des caractères ASCII non codés sur 7 bits ne sont pas prises en charge pour un serveur principal fonctionnant sous Windows et disposant d'un serveur de médias doté d'une version antérieure à 10.1.1.
- Vous pouvez dupliquer l'image de sauvegarde PaaS sur un serveur de stockage pris en charge. Mais avant de lancer une restauration, vous devez dupliquer l'image sur un serveur MSDP pour lequel le partage universel est activé. Se reporter à "Récupération d'images dupliquées à partir d'AdvancedDisk" à la page 107.
- NetBackup 10.3 permet de sauvegarder et de restaurer les bases de données PaaS Azure prises en charge avec l'authentification de base de données basée sur l'identité gérée. Cette opération n'est pas prise en charge pour le serveur Azure Database for MariaDB. Cette fonction nécessite au moins un serveur de médias 10.2 ou de version ultérieure.
- Pour que l'authentification de la base de données Azure fonctionne sur tous les serveurs de médias, il est recommandé d'utiliser l'identité gérée attribuée par l'utilisateur. Un utilisateur de base de données doté d'une identité gérée attribuée par le système, associée au serveur de médias ou au groupe de machines virtuelles identiques (AKS/EKS), ne peut se servir d'aucun autre serveur de médias ou média appartenant à un autre groupe de machines virtuelles identiques (AKS/EKS).
- L'identité gérée Azure n'est pas prise en charge pour les abonnements à plusieurs locataires.

Pour PostgreSQL

- La restauration des privilèges de sécurité n'est pas prise en charge.
- Lors de la restauration, vous pouvez utiliser les options `-no-owner` et `-no-privileges`. Après la restauration, les métadonnées capturées lors de la sauvegarde sont affichées sous le propriétaire/la liste de contrôle d'accès dans l'activité de restauration du journal de progression sur l'interface utilisateur Web.

- La restauration n'échoue pas si le propriétaire ou le rôle n'existe pas à l'emplacement de destination.
- Après la restauration, le rôle de la base de données est associé selon les informations d'authentification fournies dans NetBackup par rapport à l'instance de destination.
- Les utilisateurs doivent modifier l'appartenance des bases de données après la restauration.
- La sauvegarde et la restauration ne sont pas prises en charge si seule la connexion SSL (Secure Sockets Layer) s'applique au niveau du serveur pour la charge de travail PostgreSQL sur GCP.
- La restauration de base de données Azure Postgres d'un serveur unique vers un serveur flexible, ou inversement, n'est pas prise en charge en raison des limitations du fournisseur cloud.
- Le workflow de restauration ne prend pas en charge les caractères suivants dans les noms de base de données : `, @, \, [,], !, #, %, ^, ., ,, &, *, (,), <, >, ?, /, |, }, {, ~, :, ', ", ;, +, = et -.
- Le nom d'utilisateur en majuscules n'est pas pris en charge pour les nouveaux utilisateurs ajoutés après la création du serveur PostgreSQL.

Pour AWS DynamoDB

- La restauration sur un autre client n'est pas prise en charge pour la région et le compte.
- La restauration d'images importées à partir d'un autre serveur principal est uniquement prise en charge avec l'API REST NetBackup.

Pour AWS RDS SQL

- Seules les éditions Express et Web d'AWS RDS SQL sont prises en charge.
- Concernant la validation des informations d'authentification, IAM n'est pas pris en charge pour AWS RDS SQL. Vous pouvez utiliser la méthode avec nom d'utilisateur et mot de passe.
- Seul le type de gestion des données **Amazon RDS** est pris en charge. Le type de gestion des données **RDS Custom** n'est pas pris en charge pour les éditions d'instance AWS RDS SQL.
- Les bases de données qui utilisent le chiffrement transparent des données (TDE) sont sauvegardées avec le chiffrement MSDP. Cela permet de restaurer votre base de données dans d'autres scénarios, tels que la perte de la clé de chiffrement TDE, une panne de la région cloud, une reprise après incident sur un autre cloud, etc.

Pour MySQL

- L'opération de restauration requiert des privilèges de superutilisateur si le fichier de vidage contient l'instruction CREATE DEFINER pour les sauvegardes effectuées sur une version antérieure à la 10.2.
- Les sauvegardes effectuées sur la version 10.3 ou une version ultérieure ne peuvent pas être restaurées à l'aide d'une version antérieure à la 10.2.
- La sauvegarde et la restauration ne sont pas prises en charge si seule la connexion SSL s'applique au niveau du serveur pour la charge de travail MySQL sur GCP.
- Vous pouvez restaurer la base de données MySQL vers une autre instance dotée d'une version de MySQL différente de celle de l'instance de sauvegarde, selon la compatibilité de version de MySQL.

Pour GCP SQL Server

- La sauvegarde et la restauration de bases de données en lecture seule ne sont pas prises en charge.
- Les informations d'authentification du fournisseur sont validées pour la sauvegarde complète et la restauration, non comme informations d'authentification de base de données.
- La sauvegarde et la restauration de bases de données en mode utilisateur unique ne sont pas prises en charge.
- Lorsqu'une opération est en cours, les travaux suivants sont placés dans la file d'attente. Si l'exécution du travail en cours prend du temps, les travaux présents dans la file d'attente peuvent expirer et échouer.

Pour des sauvegardes incrémentielles à l'aide de GCP SQL Server

- Suite à une modification apportée à la DML, les sauvegardes incrémentielles peuvent échouer lorsqu'une table est renommée après l'activation de la capture des données modifiées dans la table. Pour contourner ce problème, vous devez modifier manuellement tous les objets qui référencent la table renommée. Par exemple, si vous renommez une table qui est référencée dans un déclencheur, vous devez modifier ce déclencheur pour qu'il contienne le nouveau nom de la table. Pour répertorier les dépendances dans la table avant de la renommer, consultez la documentation Azure.
- La sauvegarde et la restauration de bases de données contenant des données binaires ou d'images ne sont pas prises en charge. L'insertion en bloc sur Cloud SQL Server requiert une autorisation sysadmin non fournie par GCP.

- Lors de la duplication de sauvegardes incrémentielles sur différents serveurs de stockage, NetBackup génère différents numéros de copie pour le même point de récupération. Si vous tentez de restaurer une copie incrémentielle ne contenant aucune sauvegarde complète ou incrémentielle, l'opération risque d'échouer.
- Si vous disposez de plusieurs serveurs de médias, les sauvegardes incrémentielles peuvent s'exécuter uniquement avec la version 10.3 ou une version ultérieure.
- Les bases de données système et le schéma de la capture des données modifiées sont sauvegardés et restaurés sur la base de données cible.
- Vous devez définir une période de conservation de la capture des données modifiées supérieure à la période de planification de la fréquence des sauvegardes incrémentielles.
- Les sauvegardes incrémentielles des bases de données comportant plusieurs tables peuvent être plus longues, car l'activation de la capture des données modifiées pour plusieurs tables prend plus de temps.
- Les sauvegardes incrémentielles ne sont pas prises en charge pour les éditions Web et Express des bases de données.
- Toute tentative d'activation de la capture des données modifiées échoue si la base de données contient déjà un schéma personnalisé ou une capture des données modifiées nommée par un utilisateur.
- Pour assurer la cohérence au niveau application, NetBackup utilise la sauvegarde complète précédente et toutes les sauvegardes incrémentielles suivantes.Si une image de sauvegarde quelconque est expirée, cela peut entraîner une incohérence au niveau application en raison de la perte de données.
- La capture des données modifiées requiert les éditions Standard ou Enterprise de SQL Server. Si une base de données est connectée ou restaurée avec l'option KEEP_CDC vers une édition différente de Standard ou Enterprise, la sauvegarde échoue. Le message d'erreur 932 s'affiche alors.

Pour Azure SQL et SQL Managed Instance

- La machine virtuelle Azure utilisée comme serveur de médias doit appartenir au même réseau virtuel (Vnet) que celui d'une instance gérée par Azure. Autrement, si le serveur de médias et l'instance gérée par SQL sont dans un Vnet différent, les deux réseaux virtuels doivent être configurés comme pairs pour accéder à l'instance de base de données.
- Échec de la sauvegarde lorsqu'un Readlock est placé sur la base de données ou le groupe de ressources.

- La sauvegarde aboutit partiellement lorsqu'un verrou de suppression est appliqué à la base de données ou au groupe de ressources. L'entrée obsolète tempdb n'est pas supprimée du portail cloud Azure. Vous devez la supprimer manuellement.
- Avant de lancer la restauration d'une base de données sur un serveur Azure SQL ou sur Azure Managed Instance, vous devez attribuer le privilège d'administrateur AAD sur le serveur cible. Avant la restauration, procédez comme suit, selon le cas :
  - L'identité gérée par le système ou par l'utilisateur des serveurs de médias.
  - Le `groupe de machines virtuelles identiques` dans lequel le média NetBackup est déployé (dans le cas d'un déploiement AKS ou EKS).

Pour une sauvegarde incrémentielle Azure SQL Server et SQL Managed Instance

- Vous pouvez activer la capture des données modifiées uniquement sur les niveaux de bases de données S3 et supérieurs. Cette fonctionnalité n'est pas prise en charge pour les bases de données Azure SQL Server et SQL Managed Instance de type sous-cœur (bases de données de base, S0, S1 et S2).
- Des problèmes de sauvegarde ou de restauration peuvent se produire pour les bases de données dont la table contient des colonnes chiffrées. Pour contourner le problème, Microsoft suggère d'utiliser les commandes Publish/Extract.
- La restauration peut échouer pour les bases de données dont la table contient des données d'objet blob.
- Pour dupliquer des sauvegardes incrémentielles sur différents serveurs de stockage, NetBackup génère différents numéros de copie pour le même point de récupération. Si vous tentez de restaurer une copie incrémentielle ne contenant aucune référence antérieure à une sauvegarde complète ou incrémentielle, l'opération échoue.

  Remarque : La sauvegarde incrémentielle d'Azure SQL Server peut s'exécuter uniquement sur un serveur de médias doté de NetBackup 10.2 ou d'une version ultérieure. La sauvegarde incrémentielle d'Azure SQL Managed Instance peut s'exécuter uniquement sur un serveur de médias doté de NetBackup 10.3 ou d'une version ultérieure.

- L'ID d'utilisateur utilisé pour le service cloud doit être autorisé à activer et à désactiver la capture des données modifiées. Sans cette autorisation, vous risquez de rencontrer ce type d'erreurs :

```
3842: "Failed to enable CDC"
and
3844: "Failed to disable CDC"
```

- Toute tentative d'activation de la capture des données modifiées échoue si la base de données contient un schéma personnalisé ou un utilisateur nommé `cdc`. L'utilisation du terme `cdc` est réservée au système.
- Dans une base de données dotée d'un schéma de capture des données modifiées créé avant la première sauvegarde complète, ce schéma n'est pas sauvegardé ni restauré.
- Si vous effectuez une restauration vers une édition autre que l'édition Standard ou Enterprise, l'opération est bloquée, car la capture des données modifiées requiert l'une de ces éditions de SQL Server. Le message d'erreur 932 s'affiche.
- Évitez de sauvegarder des bases de données contenant des tables de données d'objet BLOB. Si une table contient des données d'objet BLOB, la sauvegarde peut aboutir, mais la restauration échoue.
- Le paramètre de chiffrement d'une base de données Azure SQL Server ou Azure SQL Managed Instance ne peut pas être préservé (*Is_encryption=0*) pendant une restauration.

Pour Azure Cosmos DB for MongoDB

- La découverte, la protection et la restauration ne sont pas prises en charge si le compte est configuré à l'aide du cluster vCore.
- La sauvegarde et la restauration ne sont pas prises en charge si le compte est configuré avec une clé de personnalisation.
- NetBackup ne prend pas en charge Azure Cosmos DB for MongoDB version 3.2.
- L'option **Remplacer la base de données existante** n'est pas prise en charge.
- Règles d'attribution de nom des bases de données :
  - La longueur des noms de base de données doit être comprise entre 3 et 63 caractères.
  - Les noms de base de données prennent en charge tous les caractères, excepté les suivants : #, /, ?,&, <, >, =, }, $, {,], [, ", ', ., \ .

Pour Azure Cosmos DB for NoSQL

- La sauvegarde et la restauration ne sont pas prises en charge si le compte est configuré avec une clé de personnalisation.
- La protection de Azure Cosmos DB for MongoDB version 3.2 n'est pas prise en charge.

- L'option **Remplacer la base de données existante** n'est pas prise en charge.
- Règles d'attribution de nom des bases de données :
  - La longueur des noms de base de données doit être comprise entre 3 et 63 caractères.
  - Les noms de base de données prennent en charge tous les caractères, excepté les suivants : #, /, ?,&, <, >, =, }, $, {,], [, ", ', ., \ .

Pour Amazon RDS for Oracle

- Seules les instances Oracle prises en charge par le système EFS peuvent être sauvegardées et restaurées.
- Les éditions Standard et Enterprise sont prises en charge.
- Les bases de données de conteneurs à plusieurs locataires et les répliques de lecture ne sont pas prises en charge.
- La sauvegarde et la restauration ne sont pas prises en charge pour les instances Oracle avec la fonction TDE activée.
- Seul le type de gestion des données Amazon RDS est pris en charge. Le type de gestion des données RDS Custom n'est pas pris en charge.
- Le groupe d'options associé à RDS Oracle doit présenter la même version et le même nom de moteur de base de données.
- La restauration est prise en charge vers l'emplacement intermédiaire EFS uniquement, y compris la restauration manuelle à partir de l'onglet **Base de données à accès instantané**.

Pour Amazon Redshift

- Les restaurations vers une région ou un compte différent ne sont pas prises en charge.
- NetBackup protège les bases de données de cluster AWS Redshift individuelles. La protection de l'ensemble du cluster AWS Redshift n'est pas prise en charge.
- Seules les bases de données utilisateur sont protégées. Les bases de données système ne sont pas affichées ou protégées.
- La restauration d'images importées à partir d'un autre serveur principal est prise en charge uniquement à l'aide de l'API REST NetBackup.
- Seuls les clusters Redshift sont pris en charge. Redshift sans serveur n'est pas pris en charge.
- Tous les clusters dont vous sauvegardez les bases de données doivent afficher l'état Disponible.

- Les tables dont les noms sont sensibles à la casse et contiennent des guillemets doubles ne sont pas restaurées.
- Lors de la restauration, un fichier peut manquer dans le nombre total de fichiers sauvegardés.
- Il est déconseillé de sauvegarder les bases de données dont les tables sont vides.
- NetBackup assure une protection en mode cohérence d'incident des données Redshift. Tenez compte du type d'activité et des conditions d'application avant d'effectuer des sauvegardes pour déterminer si ces opérations nécessitent la vérification ou la suspension d'une application.

Découverte des biens PaaS

NetBackup permet de découvrir, de protéger et de restaurer des biens de base de données PaaS. Vous pouvez également découvrir et restaurer une base de données Azure SQL et des biens de base de données gérés par Azure SQL qui sont sauvegardés par Microsoft Azure. Les modes de sauvegarde pris en charge sont la sauvegarde à un moment donné et la sauvegarde de conservation à long terme.

Remarque : si vous avez mis à niveau NetBackup Snapshot Manager (anciennement CloudPoint) de la version 10.0 vers la version 10.1, les biens PaaS sont marqués comme supprimés dans l'onglet **PaaS** pour tous les utilisateurs disposant de rôles personnalisés. Les biens n'indiquent aucun point de récupération et, par contre, les nouveaux biens portant le même nom sont visibles. Les anciens biens sont supprimés de l'onglet **PaaS** après le nettoyage planifié suivant des biens (la durée par défaut est de 30 jours). Pour remédier à ce problème, assignez de nouveau les autorisations de tous les nouveaux biens au rôle RBAC existant ou créez un rôle personnalisé. Pour plus d'informations, consultez le *Guide de l'administrateur de l'interface utilisateur Web de NetBackup*.

Remarque : Si vous passez la configuration du plug-in cloud Snapshot Manager du principal de service Azure à l'identité gérée par Azure, les biens PaaS précédemment découverts affichent l'état Supprimé. NetBackup Snapshot Manager supprime les biens supprimés toutes les 24 heures. Pour effectuer une sauvegarde ou une récupération avant le nettoyage planifié, contactez le support technique de Veritas.

Pour découvrir des biens PaaS :

1. Ajoutez Snapshot Manager. Se reporter à "Ajout de Snapshot Manager" à la page 12.
2. Ajoutez Microsoft Azure, GCP ou AWS en tant que fournisseur. Se reporter à "Ajout d'un fournisseur cloud pour Snapshot Manager" à la page 13.
3. Exécutez une découverte. Se reporter à "Découverte de biens sur Snapshot Manager" à la page 17.

   Une fois la découverte terminée, vous pouvez trouver les biens découverts dans l'onglet **PaaS** de la charge de travail **Cloud**.

   Tous les biens AWS RDS découverts s'affichent dans l'onglet **Applications**. Les instances RDS prennent en charge les sauvegardes basées sur des snapshots du fournisseur, ainsi que les sauvegardes gérées par NetBackup.

   NetBackup peut gérer et protéger tous les biens répertoriés dans l'onglet **PaaS**. De plus, la base de données Azure SQL et les biens de base de données gérés par Azure SQL peuvent également être sauvegardés par Microsoft Azure.

Remarque : Lorsque vous alternez la création et la suppression d'un bien PaaS portant le même nom, et que le bien PaaS est supprimé après la découverte, l'interface utilisateur Web affiche les anciennes données jusqu'à l'exécution de la découverte périodique suivante.

Affichage des biens PaaS

Pour afficher les biens PaaS :

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Dans l'onglet **PaaS**, seuls les biens auxquels vous avez accès s'affichent. Les biens RDS s'affichent dans l'onglet **Applications**.

   Vous pouvez effectuer les opérations **Ajouter une protection**, **Sauvegarder maintenant** et **Gérer les informations d'authentification** dans les biens affichés.

   Pour les biens DynamoDB et Amazon Redshift, l'option **Gérer les informations d'authentification** n'est pas disponible.

   Pour les biens supprimés, vous pouvez uniquement gérer les informations d'authentification.

Gestion des informations d'authentification PaaS

Vous pouvez ajouter des informations d'authentification à une base de données figurant dans les onglets **PaaS** et **Applications** sous la section de la charge de travail **cloud**. Vous pouvez ajouter, modifier ou supprimer les informations d'authentification PaaS depuis la console centrale **Gestion des informations d'authentification** de NetBackup. Certaines charges de travail telles DynamoDB et Amazon Redshift ne prennent pas en charge la gestion des informations d'authentification via NetBackup et utilisent les informations d'authentification du fournisseur.

Affichage du nom des informations d'authentification appliquées à une base de données

Vous pouvez afficher le nom des informations d'authentification qui sont configurées pour les bases de données dans la colonne **Nom des informations d'authentification** de l'onglet **PaaS**. Si les informations d'authentification ne sont pas configurées pour un bien spécifique, ce champ reste vide.

Pour afficher les informations d'authentification des bases de données PaaS :

1. Dans la partie gauche, sélectionnez l'onglet **Charges de travail > Cloud > PaaS**.
2. Cliquez sur **Afficher ou masquer les colonnes** au-dessus du tableau de liste de base de données.
3. Sélectionnez **Nom des informations d'authentification** pour afficher la colonne de nom des informations d'authentification.

Ajout d'informations d'authentification à une base de données

Vous pouvez ajouter ou modifier des informations d'authentification à une base de données figurant dans l'onglet **PaaS**.

Pour ajouter ou modifier des informations d'authentification

1. Dans la partie gauche, cliquez sur **Charges de travail** >**Cloud**.

   Dans l'onglet **PaaS**, seuls les biens auxquels vous avez accès s'affichent. Les biens RDS s'affichent dans l'onglet **Applications**.
2. Sélectionnez la base de données dans le tableau, puis cliquez sur **Gérer les informations d'authentification**.
3. Sélectionnez un **Hôte de validation**. L'hôte de validation doit être un serveur de médias RHEL disposant d'une connectivité à la charge de travail PaaS, ou une instance NetBackup Snapshot Manager. Si vous utilisez une instance

NetBackup Snapshot Manager, un conteneur de système de déplacement des données est ajouté à l'hôte Snapshot Manager.

Vous pouvez ajouter des informations d'authentification existantes ou en créer de nouvelles pour la base de données :

- Pour sélectionner les informations d'authentification existantes du compte, sélectionnez l'option **Sélectionner parmi les informations d'authentification existantes**, sélectionnez les informations d'authentification requises dans le tableau ci-dessous et cliquez sur **Suivant**.
- Pour ajouter de nouvelles informations d'authentification au compte, sélectionnez **Ajouter des informations d'authentification** et cliquez sur **Suivant**. Entrez le **Nom des informations d'authentification**, la **Balise** et une **Description** pour les nouvelles informations d'authentification. Dans la section **Informations d'authentification du service** :
  - Sélectionnez **Authentification de base de données basée sur les rôles (applicable pour les services de base de données pris en charge)** pour utiliser l'authentification IAM AWS, l'authentification gérée par le système Azure et l'authentification gérée par l'utilisateur.
    - Sélectionnez **Authentification de base de données IAM (applicable pour Amazon RDS uniquement)** pour les biens Amazon RDSS uniquement, et spécifiez le **Nom d'utilisateur de la base de données**.
      Se reporter à "Création d'un nom d'utilisateur de base de données IAM" à la page 85.

      Remarque : Si Snapshot Manager est déployé dans le cloud et est associé à un rôle IAM disposant de l'autorisation requise. Vous devez également déployer le serveur de médias dans le même environnement cloud et associer le même rôle IAM. Sans quoi, les travaux de sauvegarde des biens AWS échoueront.

    - Sélectionnez **Authentification d'identité gérée par le système Azure** ou **Authentification d'identité gérée par l'utilisateur Azure** selon les besoins. Entrez le nom d'utilisateur de la base de données et cliquez sur **Suivant**.
      Pour effectuer des opérations de sauvegarde et de restauration utilisant l'authentification d'identité gérée, vous devez configurer l'administrateur AAD sur les serveurs de base de données source et cible.
      Se reporter à "Création d'un nom d'utilisateur d'identité gérée par le système ou par l'utilisateur" à la page 86.

Remarque : Si Snapshot Manager est déployé dans le cloud avec une identité gérée associée disposant des autorisations requises, associez la même identité au serveur de médias. Pour les déploiements AKS et EKS, associez la même identité gérée au groupe de machines virtuelles identiques.

- Sélectionnez **Authentification par mot de passe** et spécifiez le nom d'utilisateur et le mot de passe du serveur de base de données.
  Si vous utilisez Azure Cosmos DB for NoSQL :
  - Le nom d'utilisateur est l'**URI du compte** disponible sur le portail Azure, sous **Paramètres** > **Clés** > **URI**.
  - Le mot de passe est la **clé principale** ou **secondaire** disponible sur le portail Azure, sous **Paramètres** > **Clés** > **CLÉ PRINCIPALE** ou **CLÉ SECONDAIRE**.
  - Les clés de lecture prennent en charge les sauvegardes uniquement. Il est recommandé d'utiliser des clés de lecture/écriture pour restaurer des bases de données.

  Si vous utilisez Azure Cosmos DB for MongoDB :
  - Le nom d'utilisateur correspond au nom du compte, disponible sur le portail Azure, sous **Paramètres** > **Chaînes de connexion** > **NOM_UTILISATEUR**.
  - Le mot de passe est la **clé principale** ou **secondaire** disponible sur le portail Azure, sous **Paramètres** > **Clés** > **CLÉ PRINCIPALE** ou **CLÉ SECONDAIRE**.
  - Les clés de lecture prennent en charge les sauvegardes uniquement. Il est recommandé d'utiliser des clés de lecture/écriture pour restaurer des bases de données.

  Cliquez sur **Suivant**.
- Ajoutez un rôle pour lequel vous souhaitez autoriser l'accès aux informations d'authentification. Pour ajouter de nouvelles autorisations à un rôle :
  - Cliquez sur **Ajouter**.
  - Sélectionnez un rôle.
  - Sélectionnez les autorisations que vous souhaitez accorder au rôle sur la base de ses informations d'authentification.
  - Cliquez sur **Enregistrer**.

4 Cliquez sur **Suivant** pour terminer la création des informations d'authentification.

Pour plus d'informations sur les informations d'authentification et leur modification ou suppression, consultez le *Guide de l'administrateur de l'interface utilisateur Web NetBackup*.

Création d'un nom d'utilisateur de base de données IAM

Pour créer un nom d'utilisateur IAM :

1. Activez l'authentification de base de données IAM sur l'instance de base de données RDS.
2. Créez un utilisateur de base de données à l'aide de la connexion principale (rds_iam
   - Pour MySQL, créez le nom d'utilisateur à l'aide de la connexion principale (rds_iam) :
     - mysql --protocol=tcp --host=instance_fqdn --user=admin -p --port=3306
     - CREATE USER iamuser IDENTIFIED WITH AWSAuthenticationPlugin as 'RDS';
     - GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, RELOAD, PROCESS, REFERENCES, INDEX, ALTER, SHOW DATABASES, LOCK TABLES, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, EVENT, TRIGGER ON *.* '<db_user>'@'%';
   - Pour PostgreSQL, créez l'utilisateur sous le serveur.
     - psql -h instance_fqdn -U postgres
     - CREATE USER iamuser WITH LOGIN;
     - GRANT rds_iam TO iamuser;
     - ALTER ROLE iamuser WITH LOGIN CREATEDB;
     - GRANT rds_superuser TO iamuser;
3. Associez la politique RDS au rôle IAM rattaché au serveur de médias NetBackup.

Pour plus de détails, consultez la section *Autorisations AWS requises par NetBackup Snapshot Manager* dans la dernière version du *Guide d'installation et de mise à niveau de NetBackup Snapshot Manager*.

Configuration des autorisations pour l'utilisateur de base de données

Pour MySQL

Créez un utilisateur de base de données disposant de la connexion principale et accordez les autorisations suivantes :

- mysql --protocol=tcp --host=instance_fqdn --user=admin -p --port=3306
- CREATE USER dbuser IDENTIFIED BY '<password>';
- GRANT SELECT, INSERT, UPDATE, DELETE, CREATE, DROP, RELOAD, PROCESS, REFERENCES, INDEX, ALTER, SHOW DATABASES, LOCK TABLES, CREATE VIEW, SHOW VIEW, CREATE ROUTINE, ALTER ROUTINE, EVENT, TRIGGER ON *.* TO `dbuser`@'%' WITH GRANT OPTION;

Pour PostgreSQL

Créez un utilisateur de base de données sous le serveur et accordez les autorisations suivantes :

- psql -h instance_fqdn -U postgres
- CREATE USER dbuser WITH PASSWORD '<password>' CREATEDB;
- (Pour AWS RDS PostgreSQL) GRANT rds_superuser TO dbuser;
- (Pour AZURE PostgreSQL) GRANT azure_pg_admin TO dbuser;
- (Pour GCP PostgreSQL) GRANT cloudsqlsuperuser TO dbuser;

Pour SQL Server

Créez un utilisateur de base de données sous le serveur et accordez l'autorisation suivante :

- Créez une connexion sur le serveur :
  CREATE LOGIN dbuser WITH PASSWORD='<password>'
- Créez un utilisateur pour la base de données dans le serveur :
  - CREATE USER [dbuser] FOR LOGIN [dbuser]
  - ALTER ROLE [db_owner] ADD MEMBER [dbuser]

Remarque : Aucun rôle de refus de base de données ne doit être assigné à l'utilisateur de base de données. Par exemple : db_denydatareader et db_denydatawriter.

Création d'un nom d'utilisateur d'identité gérée par le système ou par l'utilisateur

Pour Azure SQL Server et Managed Instance

Effectuez l'une des configurations suivantes :

Configurez l'utilisateur d'identité gérée comme administrateur AAD :

- Définissez l'administrateur AAD sur le serveur SQL ou sur Managed Instance.
- Accédez à Paramètres > Azure Active Directory > Définir l'administrateur. Recherchez et définissez une identité gérée attribuée par le système ou par l'utilisateur, puis enregistrez.

Remarque : Seuls les serveurs de médias configurés comme une identité gérée attribuée par le système et définie comme administrateur AAD peuvent effectuer des opérations de sauvegarde et de restauration.

Créez un utilisateur d'identité géré sur la base de données à l'aide du client SSMS :

- Pour définir l'administrateur AAD pour le serveur SQL et créer l'utilisateur, accédez à Paramètres > Administrateur Active Directory > Définir l'administrateur. Choisissez l'utilisateur Active Directory et enregistrez.
- Connectez-vous à la base de données SQL ou à la base de données gérée pour créer un utilisateur sous cette base de données.

```
CREATE USER [<managed_identity>] FROM EXTERNAL PROVIDER;
ALTER ROLE db_owner ADD MEMBER [<managed_identity>];
```

- Exécutez la commande suivante pour accorder l'autorisation de connexion à cet utilisateur sur le serveur SQL :

```
# CREATE USER [<managed_identity>] FROM EXTERNAL PROVIDER;
# ALTER ROLE loginmanager ADD MEMBER [<managed_identity>];
```

Remarque : Vous devez créer des utilisateurs pour tous les serveurs de médias qui communiquent avec la base de données à l'aide de l'identité gérée attribuée par le système.

Remarque : Pour restaurer la base de données, vous devez configurer l'utilisateur d'identité gérée comme administrateur AAD sur le serveur cible.

Pour MySQL

- Pour définir l'administrateur AAD pour le serveur MySQL et créer l'utilisateur, accédez à Paramètres > Administrateur Active Directory > Définir l'administrateur. Choisissez l'utilisateur Active Directory et enregistrez.

- Exécutez la commande suivante pour obtenir l'ID du client pour l'identité gérée à l'aide de l'interface de ligne de commande Azure :

```
# az ad sp list --display-name <managed_identity> --query [*].appId
 --out tsv
```

- Exécutez la commande suivante pour générer un jeton d'accès pour vous connecter à l'aide de l'interface de ligne de commande Azure :

```
# az account get-access-token --resource-type oss-rdbms
```

- Exécutez la commande suivante pour vous connecter à l'aide de l'utilisateur administrateur AAD et d'un jeton d'accès :

```
# mysql -h <server name> --user <user name>
--enable-cleartext-plugin --password=<token>
```

- Exécutez la commande suivante pour créer l'utilisateur d'identité gérée et lui accorder les autorisations requises :

```
# SET aad_auth_validate_oids_in_tenant = OFF;
  # CREATE AADUSER '<db_user>' IDENTIFIED BY
'<Generated_client_id>';
  # GRANT USAGE, DROP, SELECT, CREATE, SHOW VIEW, EVENT, LOCK
TABLES , ALTER, CREATE VIEW, INSERT, REFERENCES, ALTER ROUTINE,
PROCESS ON *.* TO '<db_user>'@'%'
```

Pour PostgreSQL

- Pour configurer l'administrateur AAD pour le serveur PostgreSQL et créer l'utilisateur, accédez à Paramètres > Administrateur Active Directory > Définir l'administrateur. Choisissez l'utilisateur Active Directory et enregistrez.
- Obtenez l'ID du client pour l'identité gérée :

```
 # az ad sp list --display-name <managed_identity>  --query
[*].appId --out tsv
```

- Exécutez la commande suivante pour générer le jeton d'accès requis pour vous connecter :

```
# az account get-access-token --resource-type oss-rdbms
```

- Exécutez la commande suivante pour exporter le mot de passe pour le jeton généré :

```
# export PGPASSWORD=<token>
```

- Exécutez la commande suivante pour vous connecter à l'aide de l'utilisateur administrateur AAD et d'un jeton d'accès :

```
 # psql "host=<host name> port=5432 dbname=<dbname> user=<user
name> sslmode=require"
```

- Exécutez la commande suivante pour créer l'utilisateur et lui accorder l'autorisation requise :

```
# SET aad_auth_validate_oids_in_tenant = OFF;
  # CREATE ROLE <db_user> WITH LOGIN PASSWORD '<client_id>' IN ROLE azure_
  # GRANT azure_pg_admin TO <db_user>;
  # ALTER USER smipguser CREATEDB;
  # ALTER USER smipguser Replication;
```

Remarque : Seule l'identité gérée par l'utilisateur est prise en charge pour le serveur flexible MySQL. L'identité gérée n'est pas prise en charge pour le serveur flexible PostgreSQL.

Pour Azure Cosmos DB for NoSQL

1. Connectez-vous à votre portail Azure.
2. Pour attribuer le rôle **Cosmos DB Built-in Data Contributor** à l'identité gérée, exécutez la commande suivante :

   ```
   # az cosmosdb sql role assignment create -a <Account_Name> -g
   <Resource_Group_Name> -s "/" -p <Object_ID/Principle_ID> -d
   00000000-0000-0000-0000-000000000002
   ```

   Où :

   - *Account_Name* est le nom du compte Azure Cosmos.
   - *Resource_Group_Name* est le nom du groupe de ressources du compte.
   - *Object_ID/Principle_ID* est l'objet d'identité géré ou à l'ID principal.
   - *00000000-0000-0000-0000-000000000002* est l'ID du rôle **Cosmos DB Built-in Data Contributor**.

Ajout de la protection des biens PaaS

Une fois les biens PaaS découverts, vous pouvez les protéger dans l'onglet **Applications** ou **PaaS** de la charge de travail **cloud**.

Pour protéger des biens PaaS

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Pour protéger les biens de base de données pris en charge par AWS RDS, cliquez sur l'onglet **Applications**. Pour les autres biens PaaS, cliquez sur l'onglet **PaaS**.
3. Vérifiez si le bien à protéger dispose d'informations d'authentification.

   Se reporter à "Affichage du nom des informations d'authentification appliquées à une base de données" à la page 82.

   Si la colonne **Nom des informations d'authentification** est vide, vous devez assigner des informations d'authentification au bien.

   Se reporter à "Ajout d'informations d'authentification à une base de données " à la page 82.
4. Pour protéger un bien, sélectionnez le bien, puis cliquez sur **Ajouter la protection**.

   Un bien doit disposer d'informations d'authentification pour la plupart des opérations. Par exemple, vous souhaitez assigner le bien à un plan de protection ou effectuer une sauvegarde immédiatement.
5. Sélectionnez un plan de protection, puis cliquez sur **Suivant**.
6. Vérifiez les paramètres de configuration et cliquez sur **Protéger**.

Réalisation d'une sauvegarde immédiate

Cette option permet de créer une sauvegarde ponctuelle du bien sélectionné. Cette sauvegarde n'affecte pas les sauvegardes futures ou planifiées.

Pour effectuer une sauvegarde immédiate

1. Dans la partie gauche, cliquez sur **Charges de travail** >**Cloud**.

   Pour sauvegarder les biens de base de données pris en charge par AWS RDS, cliquez sur l'onglet **Applications**. Pour les autres biens PaaS, cliquez sur l'onglet **PaaS**.

   Remarque : Vous pouvez afficher et protéger les bases de données créées par l'utilisateur. Les bases de données système ne sont ni affichées, ni protégées, car elles nécessitent le privilège de super-utilisateur accordé par le fournisseur cloud pour les opérations de sauvegarde et de restauration.

2. Sélectionnez le bien, puis cliquez sur **Ajouter la protection**.
3. Sélectionnez le plan de protection requis, puis cliquez sur **Démarrer la sauvegarde**.

   Vous pouvez afficher l'état du travail de sauvegarde dans le moniteur d'activité.

   Les agents de base de données accèdent à la base de données depuis le serveur de médias (conteneur, si NetBackup est déployé dans des environnements AKS et EKS) et effectuent le montage NFS du chemin d'accès du partage universel sur le serveur de médias (hôte de sauvegarde).

Remarque : Pour la sauvegarde incrémentielle des bases de données Azure SQL, NetBackup effectue une sauvegarde complète même si le bien est protégé par un plan de protection associé à une sauvegarde incrémentielle différentielle.

Chapitre 2

Récupération des biens cloud

Ce chapitre traite des sujets suivants :

Récupération des biens cloud

Vous pouvez restaurer des biens de machines virtuelles AWS, Azure, Azure Stack et GCP à partir d'une copie de snapshot, de réplique, de sauvegarde ou de duplication.

Lors de la restauration de machines virtuelles, NetBackup vous donne la possibilité de modifier certains paramètres de la copie de sauvegarde ou de snapshot d'origine. Cela inclut la modification du nom affiché de la machine virtuelle, la modification de ses options d'alimentation, la suppression des associations d'étiquettes pendant la restauration et la sélection d'un autre réseau pour la restauration. Vous pouvez également restaurer des machines virtuelles dans une autre configuration, une autre région ou un autre abonnement, et restaurer des machines virtuelles ou des disques dans un autre groupe de ressources.

- Pour GCP : sélectionnez **Règle de pare-feu**.
- Pour Azure : sélectionnez **Groupe de sécurité réseau**.
- Pour AWS : sélectionnez **Groupe de sécurité**.

À propos de la vérification de prérécupération pour les machines virtuelles

La vérification de pré-récupération permet d'identifier les éléments susceptibles de faire échouer une restauration avant de lancer cette dernière. Lors de la vérification de pré-récupération, les points suivants sont vérifiés :

- Utilisation de caractères pris en charge et de la longueur dans le nom affiché
- Existence d'un réseau de destination
- Existence d'un groupe de ressources sélectionné pour les machines virtuelles et les disques
- Existence d'un snapshot pour la machine virtuelle source (en cas de restauration à partir d'un snapshot)
- Existence d'un emplacement intermédiaire ajouté dans le fichier `/cloudpoint/azurestack.conf` (en cas de restauration à partir d'une sauvegarde pour Azure Stack)
- Existence d'une machine virtuelle portant le même nom affiché.
- Connectivité avec le Snapshot Manager et validation des informations d'authentification cloud.
- Validité des clés de chiffrement sélectionnées.

Paramètres pris en charge pour la restauration de biens cloud

Le tableau ci-dessous récapitule les différents paramètres que vous pouvez modifier lors de la restauration de biens de différents fournisseurs cloud.

Tableau 2-1 Paramètres pris en charge pour les copies de snapshot et de sauvegarde Azure, Azure Stack, GCP et AWS

Paramètres	**Copie de snapshot**			**Copie de sauvegarde**		
	Azure	Azure Stack	GCP et AWS	Azure	Azure Stack	GCP et AWS
Modifier le nom affiché de la machine virtuelle	O	O	O	O	O	O

Modifier l'état d'alimentation de la machine virtuelle	O	O	O	O	O	O
Supprimer les associations d'étiquettes	O	O	O	O	O	O
Restaurer sur un autre réseau	O	O	O	O	O	O
ID de l'abonnement				O	O	O
Modifier le groupe de ressources	O	O		O	O	
Modifier la région de la machine virtuelle				O	O	O
Modifier la configuration du fournisseur				O	O	
Modifier le groupe de ressources pour les disques	O	O		O	O	
Zone	O		O	O		O
Groupe de sécurité/Règle de pare-feu/Groupe de sécurité réseau	O	O	O	O	O	O
Modifier le chiffrement de disque	O		O	O		O

Récupération des machines virtuelles

Pour récupérer une machine virtuelle

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Machines virtuelles**.

   Tous les biens cloud découverts s'affichent pour la catégorie correspondante.
3. Cliquez deux fois sur le bien protégé que vous voulez récupérer.
4. Cliquez sur l'onglet **Points de récupération**.

   Les images disponibles sont répertoriées dans des lignes avec un horodatage de sauvegarde pour chaque image. Dans le cas des charges de travail AWS, vous pouvez consulter des images de réplique et de sauvegarde, si elles sont disponibles.
5. Dans la colonne **Copies**, cliquez sur la copie à récupérer. Vous pouvez consulter la copie de sauvegarde, la copie de snapshot et la copie de réplique, si elles sont disponibles. Cliquez sur **Récupérer**. Si vous ne sélectionnez aucune copie à restaurer, la copie principale est sélectionnée.
6. Cliquez sur **Restaurer la machine virtuelle**.
7. Sur la page Cible de la récupération, procédez comme suit :

   Si vous restaurez une copie de sauvegarde, modifiez les valeurs de ces paramètres au cas par cas :

   - **Configuration** : pour effectuer la restauration dans une autre configuration, sélectionnez-en une dans la liste déroulante.
   - **Région** : pour effectuer la restauration dans une autre région, sélectionnez-en une dans la liste déroulante.
   - **Abonnement** : pour effectuer la restauration en utilisant un autre abonnement, sélectionnez-en un dans la liste déroulante. Pour Azure et Azure Stack uniquement.
   - **Groupe de ressources** : pour effectuer la restauration dans un autre groupe de ressources, cliquez sur l'icône de recherche, dans la boîte de dialogue **Sélectionner un groupe de ressources**, sélectionnez le groupe de ressources requis. Pour Azure et Azure Stack uniquement.
   - **Nom affiché** : pour modifier le nom affiché, entrez-en un autre dans le champ. Le nom affiché spécifié est validé lors de la vérification de pré-récupération.

Remarque : À l'exception des charges de travail AWS, les caractères spéciaux suivants ne sont pas autorisés dans le nom affiché : ` ~ ! @ # $ % ^ & * ( ) = + _ [ ] { } \\ | ; : ' \" , < > / ?."

Si vous restaurez une copie de snapshot, spécifiez uniquement le **groupe de ressources** et le **nom affiché**.

Pendant la restauration d'une machine virtuelle à partir d'une copie de snapshot ou de sauvegarde, les clés de chiffrement peuvent être sélectionnées à partir de disques spécifiques ou de tous les disques à la fois, comme suit :

- Sélectionnez le **volume** et cliquez sur l'option **Modifier la clé de chiffrement**.
- Sélectionnez le **type de chiffrement** requis.
- Sélectionnez la **clé** de chiffrement requise et cliquez sur **Enregistrer**.

8 Cliquez sur **Suivant**.

9 Dans la page Options de récupération :

- Sélectionnez une **zone** si vous souhaitez restaurer une copie de sauvegarde dans une autre zone. Pour sélectionner un réseau disponible dans cette région, cliquez sur l'icône de recherche située près de **Configuration du réseau** et sélectionnez un réseau cible pour la récupération.
  Vous pouvez également sélectionner **Groupe de sécurité/Groupe de sécurité réseau/Règle de pare-feu** pour les fournisseurs cloud AWS, Azure et GCP, respectivement.
- (*GCP uniquement*) Sélectionnez une **région** si vous souhaitez restaurer une copie de snapshot dans une autre région. Pour sélectionner un réseau disponible dans cette zone, cliquez sur l'icône de recherche située dans **Configuration du réseau** et sélectionnez un réseau cible pour la récupération. La liste répertorie les réseaux disponibles dans cette zone.
- Sélectionnez une **zone** si vous souhaitez restaurer une copie de snapshot dans une autre zone. Pour sélectionner un réseau disponible dans cette zone, cliquez sur l'icône de recherche située dans **Configuration du réseau** et sélectionnez un réseau cible pour la récupération. La liste répertorie les réseaux disponibles dans cette zone.
  Vous pouvez également sélectionner **Groupe de sécurité/Groupe de sécurité réseau/Règle de pare-feu** pour les fournisseurs cloud AWS, Azure et GCP, respectivement.

Dans la section **Avancé** :

- Pour laisser la machine virtuelle active après la récupération, sélectionnez **Mettre sous tension après la récupération**.
- Pour supprimer les balises associées au bien au moment de la sauvegarde ou de la création d'un snapshot, sélectionnez **Supprimer les associations d'étiquettes**.

Remarque : Si vous ne sélectionnez pas l'option **Supprimer les associations d'étiquettes**, aucune valeur d'étiquette de bien ne doit comporter d'espace avant et après une virgule. Après la restauration d'un bien, les espaces avant et après les virgules des valeurs d'étiquette sont supprimés. Par exemple, la valeur du nom d'étiquette :**created_on**: *Ven, 02-Avr-2021 07:54:59 PM , EDT* est convertie en : *Ven,02-Avr-2021 07:54:59 PM,EDT*. Vous pouvez modifier manuellement les valeurs d'étiquette pour rétablir les espaces.

Remarque : si vous sélectionnez **Aucun(e)** pour le paramètre Zone, la machine virtuelle ne sera placée dans aucune zone. De même, si vous sélectionnez **Aucun(e)** pour le paramètre **Groupe de sécurité réseau/Groupe de sécurité/Règle de pare-feu**, aucune règle de sécurité n'est appliquée à la machine virtuelle restaurée.

---

10 Cliquez sur **Suivant**. La vérification de pré-récupération commence. À cette étape, les paramètres de récupération sont validés et, le cas échéant, les erreurs s'affichent. Vous pouvez corriger ces dernières avant de démarrer la récupération.

11 Cliquez sur **Lancer la récupération**.

L'onglet Restaurer l'activité affiche la progression du travail.

Pour plus d'informations sur les codes d'état de récupération, consultez l'administrateur NetBackup ou le *Guide de référence des codes d'état NetBackup*, disponible ici :

http://www.veritas.com/docs/000003214

Récupération des applications et des volumes à leur emplacement d'origine

Pour GCP, si, en l'absence du disque source, vous restaurez un snapshot créé avant la mise à niveau, un disque de restauration appelé pd-standard est créé par défaut.

Pour récupérer des applications et des volumes à leur emplacement d'origine

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Applications** ou **Volumes**.

   Tous les biens cloud découverts correspondant à la catégorie s'affichent.
3. Cliquez deux fois sur le bien protégé que vous voulez récupérer.
4. Cliquez sur l'onglet **Points de récupération**. Dans la vue de calendrier, cliquez sur la date de la sauvegarde.

   Les images disponibles sont répertoriées sur des lignes et sont accompagnées d'un horodatage de sauvegarde.
5. Dans le coin supérieur droit du point de récupération de votre choix, sélectionnez **Emplacement d'origine**.
6. Cliquez sur **Lancer la récupération**.
7. Dans la partie gauche, cliquez sur **Moniteur d'activité** pour afficher l'état du travail.

Récupération des applications et des volumes à un autre emplacement

Remarques

- Pour restaurer une machine chiffrée dans AWS à un autre emplacement, les noms de la paire de clés doivent être identiques pour la région source et la région de destination. Si ce n'est pas le cas, créez une nouvelle paire de clés dans la région de destination cohérente avec la paire de clés dans la région source.

Pour récupérer des applications et des volumes à un autre emplacement

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Applications** ou **Volumes**.

   Tous les biens cloud découverts correspondant à la catégorie s'affichent.
3. Cliquez deux fois sur le bien protégé que vous voulez récupérer.
4. Cliquez sur l'onglet **Points de récupération**. Dans la vue de calendrier, cliquez sur la date de la sauvegarde.

   Les images disponibles sont répertoriées sur des lignes et sont accompagnées d'un horodatage de sauvegarde.
5. Dans le coin supérieur droit du point de récupération de votre choix, sélectionnez **Autre emplacement**.
6. Sélectionnez l'emplacement de restauration du bien cloud.

7 Cliquez sur **Lancer la récupération**.

8 Dans la partie gauche, cliquez sur **Moniteur d'activité** pour afficher l'état du travail.

Remarque : (*Applicable pour Azure Cloud*) La restauration d'application vers un autre emplacement pour une machine virtuelle compatible avec ADE n'est pas prise en charge.

Scénarios de récupération pour les machines virtuelles GCP avec des volumes en lecture seule

Le tableau suivant décrit comment NetBackup gère la restauration/récupération des machines virtuelles GCP avec des volumes en lecture seule.

Tableau 2-2 Scénarios de récupération pour les machines virtuelles GCP en lecture seule

Scénario	Gestion
Restauration d'un volume à partir du snapshot d'un disque connecté en lecture seule (à partir de l'onglet **Volumes** sous Charges de travail cloud).	Pendant la restauration, le disque est connecté en mode Lecture/écriture à l'emplacement initial ou à un autre emplacement.
Restauration d'une machine virtuelle (avec un disque en lecture seule) à partir d'un snapshot en mode cohérence d'incident (dans l'onglet **Machines virtuelles** sous Charges de travail cloud).	Lors la restauration de ce type de machine virtuelle à son emplacement d'origine ou à un autre emplacement, les disques en lecture seule sont restaurés en mode lecture/écriture.

Scénario	Gestion
Restauration d'une machine virtuelle (avec un disque en lecture seule) à partir d'un snapshot cohérent au niveau application (dans l'onglet **Machines virtuelles** sous Charges de travail cloud)	Vous pouvez connecter un disque en lecture seule à plusieurs machines virtuelles, mais NetBackup ne le découvre que sous une seule machine virtuelle. Dans le cas d'une machine virtuelle Windows, le snapshot échoue avec une erreur VSS, semblable à ce qui suit : **Échec : flexsnap. GenericError : échec de la prise du snapshot (erreur : échec de la création du snapshot VSS des volumes sélectionnés.)** Dans le cas d'une machine virtuelle Linux, le snapshot pourra être réalisé correctement pour la machine virtuelle sous laquelle le disque est découvert, ce qui ne peut pas être garanti, mais il échouera pour le reste des machines virtuelles en raison des dépendances manquantes. Exemple d'erreur : **linear_flow.Flow: create snapshot (test-win) of host linux-1(len=4)' requires ['snap_google-gcepd-us-west 2-b-7534340043 132122994'] but no other entity produces said requirements\n MissingDependencies** Dans l'exemple ci-dessus, si un snapshot se déroule correctement pour une machine virtuelle Linux, un disque en lecture seule est restauré en mode lecture/écriture.

(*GCP uniquement*) Restauration de machines virtuelles et de volumes à l'aide de la prise en charge de la suppression automatique de disque

Lorsque vous effectuez un snapshot ou une sauvegarde à partir d'un snapshot de machine virtuelle source, des informations supplémentaires sur les disques sont enregistrées. L'indicateur **autoDelete** détermine si le disque doit être supprimé lors de la suppression de la machine virtuelle. Par conséquent, si une nouvelle machine virtuelle est créée à partir d'un snapshot ou d'une sauvegarde créée à partir d'un snapshot, les disques sont définis en tant que machine virtuelle source.

Par exemple :

Machine virtuelle source :

Disque1 : **autoDelete** est défini sur true lorsque la machine virtuelle source est supprimée (et lorsque **autoDelete** est défini sur **true**, le disque est supprimé automatiquement).

Disque2 : **autoDelete** est défini sur false.

Machine virtuelle restaurée :

Disk1_suffix : **autoDelete** est défini sur true.

Disk2_suffix : **autoDelete** est défini sur false.

Restauration des biens cloud

La restauration d'un bien cloud remplace les données existantes sur le bien d'origine. Contrairement à la restauration de machine virtuelle, la restauration (rollback) ne crée pas de nouvelle copie de l'image restaurée, mais remplace les données existantes sur la source.

Remarque : Les répliques de snapshot ne prennent pas en charge la restauration (rollback). D'autre part, les charges de travail Azure Stack et GCP ne prennent pas en charge la restauration (rollback).

Pour effectuer la restauration du bien cloud

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur **Machines virtuelles**.

   Tous les biens cloud découverts sont affichés pour la catégorie correspondante.
3. Cliquez deux fois sur le bien protégé à récupérer.
4. Cliquez sur l'onglet **Points de récupération**. Les images disponibles sont répertoriées sur des lignes et sont accompagnées d'un horodatage de sauvegarde. Dans la colonne **Copies**, cliquez sur le snapshot à récupérer. Cliquez sur **Récupérer** > **Restauration**.
5. Cliquez sur **Lancer la récupération**. Les données existantes sont écrasées.
6. Dans la partie gauche, cliquez sur **Moniteur d'activité > Travaux** pour afficher l'état du travail.

Récupération des biens PaaS

Les biens PaaS sont répertoriés sous la charge de travail **Cloud**. Vous pouvez restaurer des biens Amazon RDS à partir de l'onglet **Applications**. Tous les autres biens PaaS peuvent être restaurés à partir de l'onglet **PaaS**. Le workflow de récupération des biens Azure varie selon que ces biens sont protégés par NetBackup ou par Azure.

À partir de NetBackup 10.3, vous pouvez restaurer séparément les données ou les schémas et les métadonnées de la base de données MySQL. Vous devez disposer de privilèges de superutilisateur pour la restauration de métadonnées et d'au moins un serveur de médias doté de la version 10.2 ou d'une version ultérieure.

Remarque : Pour une restauration de MySQL, si vous ne disposez pas de privilèges d'administrateur ou d'utilisateur racine, vous devez disposer des autorisations d'affichage et de restauration.

Les biens PaaS prennent en charge l'accès instantané pendant la récupération. L'accès instantané permet d'accéder plus rapidement aux données et réduit le temps de récupération global.

Avant d'effectuer la récupération avec accès instantané, ajoutez la clé `MEDIA_SERVER_POD_CIDR` au fichier `bp.conf` du serveur principal. Dans le cas d'une instance NetBackup déployée dans un environnement AKS ou EKS, définissez sa valeur sur les sous-réseaux du pod de serveur de médias, sous forme de valeurs séparées par des virgules. Par exemple : MEDIA_SERVER_POD_CIDR=10.0.0.0/8, 10.0.0.0/16

Remarque : Lors de l'affichage des travaux de restauration PaaS dans le moniteur d'activité, les informations indiquées dans les champs **Octets transférés** et **Estimation des octets restants** peuvent ne pas être exactes. Pour obtenir l'état correct, vérifiez le nombre de **Fichiers écrits** et consultez les journaux NetBackup.

Récupération de biens PaaS autres que RDS

Vous pouvez restaurer les biens PaaS autres que RDS à partir de l'onglet **PaaS**, dans la section Charge de travail cloud.

Pour restaurer des biens PaaS autres que RDS

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud** et cliquez sur l'onglet **PaaS**. Cliquez sur le nom du bien à récupérer.
2. Cliquez sur l'onglet **Points de récupération** pour les biens Azure, puis sélectionnez **Gérés par NetBackup**.

   Les points de récupération disponibles s'affichent dans le tableau.
3. Cliquez sur **Récupérer** dans la ligne de l'image que vous voulez récupérer.
4. Le champ **Nom** affiche le nom d'origine du bien par défaut. Vous pouvez modifier le nom dans ce champ. Il est possible que ce nom ne puisse plus être modifié par la suite.

5 (Facultatif) Dans le champ **Instance cible**, l'instance source du bien est sélectionnée par défaut. Pour effectuer la restauration dans une autre instance, sélectionnez l'instance requise. L'**Instance cible** n'est pas disponible pour les biens DynamoDB.

6 (Facultatif, pour les bases de données MySQL uniquement.) Sélectionnez **Restaurer les métadonnées** pour restaurer des métadonnées telles que les vues, les déclencheurs, les procédures de stockage, etc.

7 (Facultatif, pour les bases de données MySQL uniquement.) Pour les informations d'authentification de l'instance cible à utiliser pour la restauration :

- Sélectionnez **Utiliser les informations d'authentification déjà associées** pour utiliser les informations d'authentification déjà associées à l'instance, puis cliquez sur **Lancer la récupération**.
- Sélectionnez **Utiliser des informations d'authentification différentes** pour utiliser d'autres informations d'authentification existantes ou pour en créer de nouvelles.
  Se reporter à "Ajout d'informations d'authentification à une base de données " à la page 82.
  L'hôte de validation chargé de valider ces informations d'authentification doit être identique à celui utilisé lors de la sauvegarde. Si l'hôte utilisé lors de la sauvegarde n'est pas disponible pour la phase de validation des informations d'authentification de la restauration, la validation échoue.
  (Facultatif) Sélectionnez **Définir les informations d'authentification comme informations d'authentification par défaut** pour utiliser ces informations d'authentification par défaut pour le bien.

8 Cliquez sur **Lancer la récupération**.

L'onglet **Restaurer l'activité** indique l'état.

Récupération d'un bien PaaS basé sur RDS

Vous pouvez restaurer les biens PaaS basés sur RDS à partir de l'onglet **Applications**, dans la section de la charge de travail **Cloud**.

Pour restaurer les biens PaaS basés sur RDS :

1 Dans la partie gauche, cliquez sur **Charges de travail > Cloud** et cliquez sur l'onglet **Applications**. Cliquez sur le nom du bien à récupérer.

2 Cliquez sur l'onglet **Points de récupération**, dans le calendrier, sélectionnez la date pour laquelle vous voulez afficher les points de récupération.

Les points de récupération disponibles s'affichent à droite.

3 Cliquez sur **Récupérer** dans la ligne de l'image que vous voulez récupérer.

4 Dans la section **Bases de données source**, sélectionnez les bases de données que vous voulez restaurer. Cliquez sur **Ajouter une base de données**, dans la boîte de dialogue **Ajouter une base de données**, sélectionnez les bases de données requises, puis cliquez sur **Sélectionner**.

5 (Bases de données Amazon RDS for Oracle uniquement) Entrez le chemin d'accès intermédiaire dans le champ **AWS Elastic file system**. Cliquez sur **Lancer la récupération**. La base de données récupérée apparaît dans l'onglet **Bases de données à accès instantané**. Pour effectuer la récupération du bien, consultez l'article de la base de connaissances suivant :

https://www.veritas.com/support/en_US/article.100058945

Vous pouvez sélectionner un chemin de montage EFS différent pour stocker les données restaurées à un emplacement intermédiaire. Vous pouvez également sélectionner un EFS dans une région différente de celle utilisée pendant la sauvegarde.

Pour les déploiements dans le cloud, il est recommandé de placer dans la même région le système EFS et l'instance EC2 sur lesquels vous souhaitez effectuer la restauration pour obtenir de meilleures performances et éviter la latence du réseau.

6 Entrez un préfixe à ajouter aux bases de données restaurées ou utilisez le paramètre par défaut. Ce champ doit avoir une valeur.

7 (Facultatif) Dans le champ **Instance cible**, l'instance source du bien est sélectionnée par défaut. Pour effectuer la restauration dans une autre instance, sélectionnez l'instance requise.

8 (Facultatif, pour les bases de données MySQL uniquement.) Sélectionnez **Restaurer les métadonnées** pour restaurer des métadonnées telles que les vues, les déclencheurs, les procédures de stockage, etc.

9 (Facultatif, pour les bases de données MySQL uniquement.) Pour les informations d'authentification de l'instance cible à utiliser pour la restauration :

- Sélectionnez **Utiliser les informations d'authentification déjà associées** pour utiliser les informations d'authentification déjà associées à l'instance, puis cliquez sur **Lancer la récupération**.
- Sélectionnez **Utiliser des informations d'authentification différentes** pour utiliser d'autres informations d'authentification existantes ou pour en créer de nouvelles.
  Se reporter à "Ajout d'informations d'authentification à une base de données " à la page 82.
  (Facultatif) Sélectionnez **Définir les informations d'authentification comme informations d'authentification par défaut** pour utiliser ces informations d'authentification par défaut pour le bien.

- Sélectionnez un hôte de validation pour valider les informations d'authentification spécifiées.

10 Cliquez sur **Lancer la récupération**.

L'onglet **Restaurer l'activité** indique l'état.

Ces deux workflows de restauration créent implicitement un partage de montage avec accès instantané à partir du point de récupération.

Récupération de biens protégés par Azure

NetBackup permet de restaurer des bases de données Azure SQL et des biens de base de données gérés par Azure SQL qui sont sauvegardés par Microsoft Azure. Les modes de sauvegarde pris en charge sont la sauvegarde à un moment donné et la sauvegarde de conservation à long terme.

Remarque : La restauration dans un pool élastique du pool d'instances n'est pas prise en charge.

Avant de poursuivre, assurez-vous que vous avez les autorisations requises pour restaurer des biens PaaS.

Pour récupérer des biens de sauvegarde à un moment donné :

1 Dans la partie gauche, cliquez sur **Charges de travail >Cloud**.

2 Cliquez sur l'onglet **PaaS**.

Tous les biens PaaS découverts s'affichent.

3 Dans la section **Type de points de récupération**, sélectionnez **Protégé par le fournisseur**.

4 Cliquez sur **Restaurer** dans la ligne de la base de donnée Azure MySQL et du bien de base de données géré par Azure SQL protégés que vous voulez récupérer.

5 Dans l'onglet **Points de récupération**, sous **Sauvegarde à un moment donné**, cliquez sur **Restaurer**.

6 Sélectionnez une date et une heure sous **Point de restauration (UTC)**. Vous pouvez sélectionner n'importe quel point de restauration, entre le plus ancien et :

- La dernière heure de sauvegarde pour les bases de données en ligne.
- L'heure de suppression de base de données pour les bases de données supprimées.

Microsoft Azure peut arrondir l'heure sélectionnée au point de récupération disponible le plus proche, à l'aide de l'heure UTC.

La date et l'heure de restauration par défaut qui s'affichent dans l'interface utilisateur Web peuvent différer selon le bien PaaS sélectionné. Par exemple, pour les bases de données Azure SQL, la date/heure de restauration par défaut correspond à l'heure actuelle et, pour la base de données gérée par Azure SQL, la date/heure de restauration par défaut est antérieure de 6 minutes par rapport à l'heure actuelle.

7 Pour les bases de données Azure SQL, vous pouvez entrer un nom pour la base de données restaurée dans le champ **Nom de base de données**. Les noms de base de données ne peuvent pas comporter de caractères spéciaux comme < > * % & : \ / et ? ou des caractères de commande. Ne terminez pas le nom par un point ou une espace. Pour en savoir plus sur les règles de nommage des ressources Azure, consultez la page https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules#microsoftsql

Si vous n'entrez pas de nom, NetBackup attribue automatiquement un nom au format *<nomBd>_<Date heure de restauration UTC>*.

8 Vous disposez d'une option permettant d'entrer le nom de l'instance dans le champ **Instance gérée** pour les bases de données gérées avec Azure SQL. Le nom d'instance du point de récupération s'affiche par défaut. Vous pouvez également rechercher le nom de l'instance gérée à l'aide de l'option Rechercher. Vous pouvez effectuer une restauration dans la même région que celle à laquelle appartient votre abonnement.

Si la recherche ne renvoie pas l'instance gérée voulue, effectuez une découverte manuelle. En outre, vérifiez que vous disposez d'un accès RBAC à l'instance gérée.

9 Cliquez sur **Suivant**. Une fois la vérification de pré-récupération terminée, cliquez sur **Démarrer la récupération**.

Vous pouvez vérifier l'état du travail dans le moniteur d'activité.

Pour récupérer des biens de sauvegarde de conservation à long terme :

1 Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.

2 Cliquez sur l'onglet **PaaS**.

Tous les biens PaaS découverts s'affichent.

3 Cliquez sur **Restaurer** dans la ligne du bien protégé que vous voulez récupérer.

4 Dans l'onglet **Points de récupération**, sous **Sauvegarde de conservation à long terme**, cliquez sur **Restaurer** en fonction de l'image à restaurer.

5 Pour les bases de données Azure SQL, vous pouvez entrer un nom pour la base de données restaurée dans le champ **Nom de base de données**. Les noms de base de données ne peuvent pas comporter de caractères spéciaux comme < > * %& : \ / et ? ou des caractères de commande. Ne terminez pas le nom par un point ou une espace. Pour en savoir plus sur les règles de nommage des ressources Azure, consultez la page https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules#microsoftsql

Si vous n'entrez pas de nom, NetBackup assigne automatiquement un nom au format *restore_<nomBd>*.

6 Vous disposez d'une option permettant d'entrer le nom de l'instance dans le champ **Instance gérée** pour les bases de données gérées avec Azure SQL. Le nom d'instance du point de récupération s'affiche par défaut. Vous pouvez également rechercher le nom de l'instance gérée à l'aide de l'option Rechercher. Vous pouvez effectuer une restauration dans la même région que celle à laquelle appartient votre abonnement.

7 Cliquez sur **Suivant**. Une fois la vérification de pré-récupération terminée, cliquez sur **Démarrer la récupération**.

Vous pouvez vérifier l'état du travail dans le moniteur d'activité.

Remarque : Les balises du portail, ainsi que Snapshot Manager, ne sont pas restaurées. Cependant, la balise « createdby: cloudpoint » est créée lors de la restauration par NetBackup.

Remarque : Pour les travaux de récupération protégés par le fournisseur, toute défaillance intermittente entraîne l'exécution du travail de récupération jusqu'à ce que le prochain nettoyage de travail de planification s'exécute.

Récupération d'images dupliquées à partir d'AdvancedDisk

Un serveur de médias 10.1 ne peut pas lancer de restaurations PaaS à partir d'une image dupliquée si l'image réside sur un stockage AdvancedDisk ou sur un stockage cloud MSDP. Comme solution de contournement, vous pouvez effectuer les étapes suivantes :

Conditions requises :

1. Pour AdvancedDisk, le serveur de médias associé au serveur MSDP doit être doté de la version 10.1 ou d'une version ultérieure.
2. Pour le stockage en cloud MSDP, la version du serveur de médias utilisée pour la récupération doit être 10.1.1.

3. Vérifiez que la directive ushare est définie et configurée sur le serveur MSDP.
4. Créez un partage universel sur ce serveur de stockage MSDP. Assurez-vous d'ajouter le nom d'hôte/l'adresse IP du serveur de médias correspondant dans la liste d'exportation de la directive ushare.

Pour effectuer une récupération à partir d'AdvancedDisk, procédez comme suit :

1 À l'aide du catalogue dans l'interface utilisateur Web, dupliquez manuellement l'image sur un stockage MSDP. Pour plus d'informations, consultez le *Guide de l'administrateur de l'interface utilisateur Web NetBackup*.

Remarque : Pour dupliquer une image à partir d'une deuxième copie, cliquez de nouveau sur Rechercher après avoir sélectionné l'option de duplication dans la vue Catalogue.

---

2 Une fois le travail de duplication terminé, vérifiez que le nouveau point de récupération est visible pour le bien donné dans l'interface utilisateur Web.

Pour lancer un travail de restauration, Se reporter à "Récupération des biens PaaS" à la page 101.

Pour la restauration à l'aide de l'API REST, consultez la section : `récupération/charges de travail/cloud/scénarios/bien/récupération`. Consultez la documentation des API NetBackup.

Remarque : pour la récupération d'instances RDS, NetBackup n'affiche aucun message d'erreur ou d'avertissement si vous lancez l'opération à partir d'une image de sauvegarde résidant sur un stockage AdvancedDisk.

Chapitre 3

Exécution d'une restauration granulaire

Ce chapitre traite des sujets suivants :

À propos de la restauration granulaire

NetBackup permet d'effectuer une restauration granulaire des fichiers et dossiers sur des machines virtuelles cloud. Vous pouvez créer des snapshots et effectuer des opérations de sauvegarde de snapshot et de restauration, mais aussi rechercher et restaurer des fichiers et des dossiers spécifiques. Vous pouvez également restaurer des volumes à partir de machines virtuelles.

Au cours de ce processus de restauration granulaire, chaque fichier du snapshot ou de la sauvegarde est considéré comme un granule, généralement appelé restauration de fichier unique. NetBackup effectue un inventaire de tous les fichiers

d'un snapshot ou d'une sauvegarde à l'aide d'un processus d'indexation. Vous pouvez restaurer des fichiers spécifiques à partir d'un snapshot uniquement si le snapshot a été indexé par NetBackup. Vous pouvez également restaurer des fichiers spécifiques à partir d'une sauvegarde uniquement si cette sauvegarde a été indexée par NetBackup.

Le tableau suivant présente le flux de la restauration granulaire de volumes, de fichiers et de dossiers :

Tableau 3-1 Tâches de restauration granulaire

Tâche	Description
Connecter des machines virtuelles	Permet de connecter les machines virtuelles que vous voulez utiliser pour effectuer une restauration granulaire.
Découvrir les biens sur la machine virtuelle	Permet d'utiliser l'option **Découvrir**. Accédez à **Cloud > Snapshot Managers > *Snapshot Manager* > Actions > Découvrir**.
Créer un plan de protection	Permet de créer un plan de protection. Assurez-vous que la case à cocher **Activer la restauration granulaire pour les fichiers ou les dossiers** est sélectionnée dans les **Options de sauvegarde** du plan de protection.
Abonner les biens découverts au plan de protection	Ajoutez les biens sur les machines virtuelles connectées à l'étape précédente au plan de protection dont la restauration granulaire inclut l'attribut indexable.
Exécuter le plan de protection	Permet de planifier un travail de sauvegarde et une opération d'indexation ou d'utiliser l'option **Sauvegarder maintenant**. Le travail de sauvegarde démarre immédiatement.
■ Restaurer un fichier ou un dossier ■ Restaurer des volumes **Remarque :** la restauration de volumes n'est pas prise en charge pour la copie de sauvegarde.	Permet d'effectuer la restauration granulaire d'un fichier, d'un dossier ou d'un volume.

Liste des environnements pris en charge

Le tableau suivant répertorie les versions prises en charge.

Tableau 3-2 Versions prises en charge

Application	Version
NetBackup	10.3
Système d'exploitation de l'hôte de sauvegarde NetBackup	RHEL 7.x et 8.8
Système d'exploitation de l'hôte Snapshot Manager	■ RHEL 7.x et versions ultérieures, RHEL 8.6 ■ Ubuntu 18.04 LTS et 20.04 LTS **Remarque :** La version du système d'exploitation (Ubuntu 20.04 LTS) répertoriée dans l'interface utilisateur est la version du conteneur.
Fournisseurs cloud	■ Amazon Web Services ■ Microsoft Azure ■ Microsoft Azure Stack Hub ■ Google Cloud Platform
Snapshot Manager ou type d'instance d'agent	■ Amazon AWS : t2.large/t3.large ■ Microsoft Azure : D2s_V3Standard ■ Microsoft Azure Stack Hub : DS2_v2 Standard, DS3_v2 Standard ■ Google Cloud Platform : n1.Standard2 et spécifications supérieures
Hôte de l'agent Snapshot Manager à protéger	■ Système d'exploitation Linux : RHEL 7.x et RHEL 8.8 ■ Version du système d'exploitation Windows : 2012 R2, 2016, 2019 et 2022

Listes des systèmes de fichiers pris en charge

Le tableau suivant fournit des informations sur les systèmes de fichiers pris en charge.

Plate-forme	Système de fichiers découvert	Structures des partitions
RHEL (avec propriété de snapshot cohérent) **Remarque :** Pour Google Cloud Platform, si l'hôte de l'agent s'exécute sur une version 8.x de RHEL, Snapshot Manager doit être installé sur un hôte doté de RHEL 8.x.	■ ext3 ■ ext4 ■ xfs	■ GPT ■ MBR ■ Aucune structure (direct FS)
Windows (avec propriété de snapshot cohérent)	NTFS	■ GPT ■ MBR

Remarque : La fonctionnalité de snapshot cohérent au niveau application n'est pas prise en charge pour le système de fichiers ext2.

Remarque : La technologie GRT est autorisée indépendamment du type de système de fichiers/de partition cible (FAT, ReFS, LDM ou LVM).

Avant de commencer

Assurez-vous que les points suivants sont traités avant d'effectuer une restauration granulaire. Le Snapshot Manager configuré et la machine virtuelle à protéger pour laquelle la restauration granulaire est activée doivent remplir les conditions suivantes :

- Les conditions suivantes s'appliquent aux snapshots :
  - (Microsoft Azure et Azure Stack Hub) Même si Snapshot Manager n'est pas déployé dans le même abonnement et la même région que la machine virtuelle connectée, mais qu'une planification de sauvegarde est configurée dans le cadre du plan de protection, une restauration granulaire peut être effectuée. Pour la planification d'un plan de protection de snapshot uniquement, pour Azure et Azure Stack Hub, vous devez déployer l'hôte Snapshot Manager dans le même abonnement et la même région que les machines virtuelles.
  - Amazon AWS : l'hôte Snapshot Manager et la machine virtuelle connectée doivent se trouver sur le même compte et dans la même région.

  - Le plug-in cloud doit être configuré pour protéger les biens de la région dans laquelle l'hôte Snapshot Manager est déployé.
- L'hôte doit être connecté et présenter la configuration prise en charge requise.
- Lorsque l'hôte est connecté, ses indicateurs **fsConsistent** et **indexable** doivent être activés. L'indicateur indexable s'applique à une planification de plan de protection de snapshot uniquement.
- La case à cocher **Activer la restauration granulaire pour les fichiers et les dossiers** doit être activée pour le plan de protection.
- Hormis le disque de démarrage et le disque monté sur `/cloudpoint`, aucun autre disque ne doit être explicitement associé à l'instance Snapshot Manager.
- Les systèmes de fichiers sur l'hôte doivent être pris en charge.
  Se reporter à "Listes des systèmes de fichiers pris en charge" à la page 111.
- Configurez les ports 5671 et 443 pour l'hôte Snapshot Manager ouvert.
- Pour la restauration sans agent, configurez le port 22 sur les machines virtuelles indexables dans les systèmes Linux. Pour les plates-formes Windows, configurez les ports 135 et 445 et le port WMI-IN dynamique ou fixe sur les machines virtuelles indexables.
- Avant de procéder à une restauration de fichier unique à partir d'une sauvegarde de snapshot, tenez compte des points suivants :
  - Vous devez disposer de NetBackup et Snapshot Manager version 10.2 ou ultérieure.
  - Une restauration granulaire fonctionne uniquement si l'image de sauvegarde est restaurée à partir du serveur de stockage MSDP (version 10.3 ou ultérieure) avec l'accès instantané activé.
  - Sur l'hôte cible Windows, l'administrateur doit disposer d'une politique de connexion et de déconnexion activée pour les disques. Pour plus d'informations, consultez la page relative à la fonction AttachVirtualDisk.
  - (Windows) Pour la restauration du lien symbolique, l'agent doit être configuré à l'aide de l'accès requis. Pour ce faire, ajoutez l'utilisateur administrateur à la politique **Créer des liens symobliques** sous `Configuration de l'ordinateur\Paramètres Windows\Paramètres de sécurité\Stratégies locales\Attribution de droits utilisateur`.
  - L'option **Restauration granulaire de fichiers** doit être sélectionnée au moment de la sauvegarde.
  - La machine virtuelle cible doit avoir accès au serveur de stockage MSDP via le partage NFS/SMB.

- La cible Windows doit répondre aux conditions suivantes :
  - (Pour restaurer le contenu d'une image Windows avec la liste de contrôle d'accès) Les informations d'authentification des utilisateurs Samba doivent être stockées dans le gestionnaire d'informations d'authentification Windows pour un serveur de stockage MSDP. Ce serveur est celui qui exporte le partage à accès instantané.
    Exécutez la commande suivante sur le serveur MSDP pour générer les informations d'authentification Samba.
    `smbpasswd -a <username>`
    Ajoutez le nom DNS ou l'adresse IP du serveur MSDP. Fournissez le nom d'utilisateur de l'étape précédente et le mot de passe généré dans le gestionnaire d'informations d'authentification Windows.
    La commande `smbpasswd` échoue si le nom d'utilisateur n'est pas présent sur le serveur MSDP. Vous devez d'abord ajouter un utilisateur à l'aide de la commande `useradd <username>`.
  - (Pour restaurer le contenu d'une image Linux) Le client NFS doit être installé.

  Pour plus d'informations sur l'activation de SMB/IA sur MSDP, consultez le *Guide de déduplication NetBackup*.
  Vérifiez la configuration SMB sur le serveur MSDP à l'aide du script de prévérification suivant :
  `/usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh`

Limitations et remarques

Les limitations suivantes s'appliquent à la restauration granulaire :

- Si l'espace requis n'est pas disponible sur l'emplacement cible, l'opération de restauration échoue avant le début de l'opération de copie.
- Lorsque des snapshots sont réalisés ou indexés, les périphériques suivants sont ignorés.
  - Périphériques de stockage éphémères
    (par ex., des volumes de stockage d'instances Amazon AWS ou des disques temporaires Microsoft Azure) Ces périphériques sont également ignorés lors de l'indexation.
  - Systèmes de fichiers créés sur un disque LDM
    Ces systèmes de fichiers sont ignorés pour les snapshots d'hôte cohérents.
- La restauration sur un autre hôte (GRT et application) du bien LVM peut échouer tant que le service de l'ancien agent (préinstallé) n'est pas redémarré. Pour

prendre en charge la récupération des biens LVM, vous devez redémarrer les agents plus anciens.

- La restauration granulaire (GRT) et la restauration de fichier unique (SFR) peuvent être effectuées à l'aide de l'indexation VxMS. L'indexation VxMS s'applique à tous les systèmes de fichiers Snapshot Manager pris en charge. L'indexation VxMS est disponible pour les clouds Azure, Azure Stack et AWS, et pour GCP.
- Le snapshot cohérent avec l'hôte est pris en charge pour le système de fichiers EXT2 uniquement s'il est monté en lecture seule.
- Si des systèmes de fichiers non pris en charge sont présents sur l'hôte, celui-ci ne peut pas être ajouté au plan de protection créé pour la restauration granulaire. La case à cocher **Activer la récupération granulaire pour les fichiers ou les dossiers** est définie sur Vrai pour les plans de protection de la restauration granulaire.
- Pendant l'indexation, des erreurs de système d'exploitation peuvent se produire lors de l'analyse des fichiers, des répertoires ou d'autres entrées. Ces erreurs sont ignorées et l'opération d'indexation continue. Pour restaurer les fichiers manquants, vous devez démarrer les opérations de restauration granulaires sur le dossier parent.
- Lorsque vous créez ou montez un disque à partir de la machine virtuelle Windows, ajoutez la lettre du lecteur. Cette action garantit que l'opération d'indexation capture la bonne lettre de lecteur.
- Dans certains cas, le point de montage n'est pas visible lorsque vous recherchez des fichiers ou des dossiers sur le point de récupération. Tenez compte des raisons suivantes :
  - Le " / " (système de fichiers racine) est sur un LVM et
  - le point de montage n'est pas directement lié à « / » (système de fichiers racine).

  Dans ce cas, recherchez le point de montage dans le volet droit, puis restaurez les fichiers ou les dossiers.

  Prenons l'exemple suivant. Un disque est monté sur `/mnt1/mnt2`, où `/mnt1` est un répertoire quelconque sur « / ». (Il s'agit du système de fichiers racine figurant dans la configuration LVM.) `mnt2` est un point de montage dans `mnt1`. `mnt2` n'est pas visible dans l'arborescence du volet gauche. Cependant, vous pouvez rechercher et restaurer des fichiers et des dossiers dans le point de montage.
- Les fichiers et les dossiers peuvent être restaurés à partir de points de récupération de snapshots de machine virtuelle uniquement si les entrées du fichier `/etc/fstab` sur les serveurs Linux sont basées sur l'UUID du système de fichiers (et non sur les chemins d'accès aux périphériques). Les chemins

d'accès de périphériques peuvent changer selon l'ordre dans lequel Linux les découvre pendant le démarrage du système.

- Lors de la restauration d'applications ou de systèmes de fichiers d'une version de système d'exploitation vers une autre version de système d'exploitation, consultez le tableau de compatibilité du fournisseur du système d'exploitation et de l'application. Il est déconseillé de restaurer un système de fichiers d'une version récente vers une version antérieure.
- Un groupe d'utilisateurs ne peut pas créer un dossier de destination pour restaurer un lecteur source. En effet, le groupe d'utilisateurs ne dispose pas d'autorisation en écriture pour créer un dossier.
- La connexion sans agent ne peut pas restaurer le fichier chiffré par Windows (ou EFS) via une restauration granulaire de niveau fichier (option Restaurer les fichiers et les dossiers). Cependant, vous pouvez restaurer le fichier via une restauration de niveau volume, puis le déchiffrer.
- Les fichiers qui sont stockés sur le volume monté sur un dossier (point de jonction) peuvent être restaurés uniquement si le disque sous-jacent présente une structure de partition GPT. Si le volume est monté à l'aide d'une lettre de lecteur, les fichiers peuvent être restaurés quelle que soit la structure de partition du disque sous-jacent.

Limitations relatives à la restauration d'un seul fichier à partir d'une copie de sauvegarde

- Lorsque vous restaurez plusieurs fichiers ou dossiers, que l'hôte source est Linux et que l'hôte cible est Windows, les limitations suivantes s'appliquent :
  - Les attributs de fichier ne peuvent pas être restaurés sur un hôte Windows et seul le contenu du fichier est restauré.
  - Si les fichiers/dossiers sélectionnés pour la restauration contiennent des liens symboliques, ces derniers ne sont pas restaurés.
  - Dans le cas d'une restauration à l'emplacement d'origine, la vérification de la taille disponible est ignorée avant l'opération de copie.
- Si vous restaurez des fichiers ou des dossiers avec des hôtes source et cible Linux, les fichiers de socket et de bloc ne sont pas restaurés.
- Les fichiers et les dossiers qui résident sur un disque LDM, un disque dynamique ou un espace de stockage ne sont pas restaurés.
- En cas de redémarrage du serveur de médias ou du moteur de déduplication PureDisk et du service du daemon du système de fichiers de provisionnement

Veritas, le montage direct conservé lors de la restauration partielle est supprimé ou expire avant la fin de la période de conservation.

- Si des serveurs de médias ne sont pas mis à niveau vers la version 10.3, le serveur principal de version 10.3 est utilisé pour la connexion à NetBackup Snapshot Manager.
- Le point de jonction sous Windows après indexation utilise le format suivant : Volume {4e3f8396-490a-400a-8abf-5579cafd4c0f}
  Pour restaurer un fichier unique à partir d'une sauvegarde, sélectionnez **Tout restaurer à un autre emplacement** et activez l'option **Restauration de la liste de contrôle d'accès requise** sous les options avancées.

Notes opérationnelles pour le moniteur d'activité

Le moniteur d'activité peut présenter les comportements suivants :

- Vous ne pouvez plus développer les répertoires dans la section **Liste de fichiers** d'un travail de restauration à l'issue de celui-ci.
- Lorsque le travail de restauration démarre, le résumé du moniteur d'activité affiche le fichier actuel, à savoir la première entrée dans les éléments de restauration. Une fois le travail terminé, le résumé ne s'affiche plus.
- Les octets transférés et les octets estimés ne sont pas mis à jour et affichent 0.

Restauration de fichiers et de dossiers à partir de machines virtuelles cloud

Vous pouvez restaurer un fichier ou un dossier d'une machine virtuelle cloud.

Remarque : Pour Microsoft Azure, Google Cloud Platform et Amazon AWS, NetBackup prend en charge les snapshots et la récupération de biens cloud chiffrés à l'aide des clés fournies par le gestionnaire.

Pour restaurer un fichier ou un dossier

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Machines virtuelles**.
3. Sélectionnez la machine virtuelle qui héberge l'application. Dans le coin supérieur droit, cliquez sur **Connecter**.
4. Une fois la machine virtuelle connectée, cliquez sur **Ajouter la protection** dans le coin supérieur droit.

5. Sélectionnez un plan de protection créé pour la récupération granulaire des fichiers et des dossiers et cliquez sur **Suivant**.
6. Cliquez sur **Protéger**.
7. Pour exécuter le plan de protection, cliquez sur **Sauvegarder maintenant**.
8. Une fois qu'un snapshot et deux travaux d'indexation ou deux sauvegardes à partir du travail de snapshot des biens sont terminés, cliquez sur l'onglet **Points de récupération**.
9. Sélectionnez **Restaurer les fichiers et les dossiers** dans le menu d'actions du point de récupération de votre choix.

   Vous pouvez également restaurer des fichiers et des dossiers pour les types de copies **Snapshot** et **Sauvegarde** en cliquant sur **Récupérer**, puis en sélectionnant **Restaurer les fichiers et les dossiers** pour le type de copie en question.
10. À l'étape Ajouter un fichier, cliquez sur **Ajouter**.
11. Dans la boîte de dialogue **Ajouter des fichiers et des dossiers**, sélectionnez les fichiers que vous voulez restaurer et cliquez sur **Ajouter**.

    Vous pouvez cliquer sur les dossiers ou les lecteurs de la partie gauche pour développer et afficher les fichiers dans un dossier spécifique. Vous pouvez rechercher des fichiers en fonction de leur nom ou de leur extension.
12. Cliquez sur **Suivant**.
13. Procédez comme suit lors de l'étape Cible de la récupération :

Boîte de dialogue	Copie de snapshot	Copie de sauvegarde
Restaurer vers	**Machine virtuelle cible** : sélectionnez une machine virtuelle. La liste des machines virtuelles connectées qui disposent du même système d'exploitation que l'hôte cible d'origine s'affiche. Si vous ne sélectionnez pas de machine virtuelle, les fichiers sont restaurés sur la machine virtuelle d'origine.	■ **Fournisseur cloud** : sélectionnez le fournisseur cloud sur lequel la restauration de fichier unique doit être effectuée. ■ **Configuration** : pour effectuer la restauration vers une autre configuration, sélectionnez la configuration souhaitée dans la liste déroulante. ■ **Région** : pour effectuer la restauration vers une autre région, sélectionnez la région souhaitée dans la liste déroulante. ■ (*Pour Azure et Azure Stack uniquement*) **Abonnement** : pour effectuer la restauration vers un autre abonnement, sélectionnez l'abonnement souhaité dans la liste déroulante. ■ **Machine virtuelle cible** : sélectionnez une machine virtuelle. La liste des machines virtuelles Linux/Windows connectées/déconnectées s'affiche pour la restauration multiplateforme.
Options de la cible de restauration	■ **Tout restaurer vers l'emplacement d'origine** ■ **Tout restaurer à un autre emplacement** Vous devez indiquer un emplacement de répertoire. Vous pouvez également entrer un chemin d'accès UNC pour l'emplacement.	

La restauration de fichiers et de dossiers vers plusieurs fournisseurs cloud est prise en charge à l'aide de la restauration granulaire à partir d'une copie de sauvegarde. Les machines virtuelles source et cible utilisées pour la restauration granulaire peuvent être rattachées à différents fournisseurs cloud.

La restauration multiplateforme est prise en charge dans les cas suivants :

- NetBackup et Snapshot Manager sur un cloud, hôte cible sur un autre cloud.
- NetBackup et Snapshot Manager sur un cloud, un autre Snapshot Manager et l'hôte cible sur un autre cloud.

- NetBackup et Snapshot Manager sur un cloud, restauration AIR (Auto Image Replication) sur un autre domaine.

14 Si l'option **Tout restaurer à l'emplacement d'origine** est sélectionnée, cliquez sur **Suivant** et sélectionnez l'option préférée suivante à l'étape Options de récupération :

Boîte de dialogue	Copie de snapshot	Copie de sauvegarde
Options	■ **Ajouter la chaîne aux noms de fichier** Dans le champ **Chaîne**, entrez la chaîne à ajouter. La chaîne est ajoutée avant la dernière extension d'un fichier. ■ **Autoriser l'écrasement des fichiers existants** Vous devez disposer des autorisations appropriées.	
Options avancées	N/A	■ (*Applicable uniquement pour la restauration de Windows vers Windows*) **Restauration de la liste de contrôle d'accès requise** : cochez cette case pour restaurer la liste de contrôle d'accès (nécessite des opérations supplémentaires). ■ **Adresse IP de la passerelle NAT de l'hôte cible** : entrez l'adresse IP de la passerelle de traduction d'adresse réseau si la machine virtuelle cible se trouve derrière une passerelle réseau et n'est pas directement accessible. **Remarque :** Seuls l'adresse IP privée et le nom d'hôte sont autorisés.

15 Si l'option **Tout restaurer à un autre emplacement** est sélectionnée, spécifiez le **répertoire de restauration** et cliquez sur **Suivant**.

16 À l'étape Vérification, affichez les options sélectionnées et cliquez sur **Lancer la récupération**.

Le travail de restauration des fichiers sélectionnés est déclenché. Vous pouvez afficher les détails du travail sur le moniteur d'activité. À l'issue du travail, vous pouvez consulter le résumé des fichiers restaurés dans les détails du travail.

Remarque : L'autorisation sur les fichiers est accordée en fonction de l'UID/du GUID lors de la restauration dans des environnements non similaires (dans lesquels l'utilisateur/les groupes ne correspondent pas). Les fichiers/dossiers restaurés doivent être accessibles à des utilisateurs/groupes non prévus sur l'hôte cible. L'utilisateur doit donc modifier l'accès selon les besoins une fois les fichiers requis restaurés.

Tenez compte des points suivants :

Suivez les instructions ci-dessous lors de la restauration de liens physiques pour la restauration de fichier unique à partir d'un snapshot ou d'une sauvegarde (machine virtuelle Linux source vers machine virtuelle Linux cible) :

- Lorsque vous sélectionnez des dossiers et des fichiers dans la boîte de dialogue **Ajouter des fichiers et des dossiers**, ne sélectionnez pas d'entrées redondantes. Par exemple, si vous sélectionnez un dossier, ne sélectionnez pas également un fichier se trouvant dans ce dossier, puisqu'il est déjà sélectionné avec le dossier.
- Si toutefois des entrées redondantes sont sélectionnées, veillez à ne pas sélectionner l'option **Autoriser l'écrasement des fichiers existants** à l'étape Option de récupération. Cela entraînera l'échec de la copie du fichier de lien physique.

Restauration de volumes sur des machines virtuelles cloud

Vous pouvez restaurer un ou plusieurs volumes sur une machine virtuelle.

Pour restaurer un volume

1. Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
2. Cliquez sur l'onglet **Machines virtuelles**.
3. Sélectionnez la machine virtuelle qui héberge l'application.
4. Une fois la machine virtuelle connectée, cliquez sur **Ajouter la protection** dans le coin supérieur droit.
5. Sélectionnez un plan de protection, puis cliquez sur **Suivant**.
6. Cliquez sur **Protéger**.
7. Pour exécuter le plan de protection, cliquez sur **Sauvegarder maintenant**.
8. Pour afficher les points de récupération, cliquez sur l'onglet **Points de récupération**.

9. Dans le coin supérieur droit du point de récupération de votre choix, sélectionnez **Restaurer les volumes**.

   Vous pouvez également appliquer des filtres de date pour rechercher des points de récupération.

10. Dans la boîte de dialogue **Restaurer les volumes**, sélectionnez un ou plusieurs volumes.

11. Dans la liste **Machine virtuelle cible**, sélectionnez la machine virtuelle sur laquelle vous voulez restaurer les volumes.

    Dans le cas d'une restauration à partir d'une machine virtuelle répliquée (autre que la machine principale), la restauration à l'emplacement d'origine n'est pas prise en charge. Si vous ne sélectionnez pas de machine virtuelle, les fichiers sont restaurés sur la machine virtuelle d'origine.

12. Cliquez sur **Restaurer**.

    Le travail de restauration des volumes sélectionnés est déclenché. Vous pouvez afficher les détails du travail sur le moniteur d'activité.

Remarque : Pour restaurer le volume sur la même machine virtuelle, vous devez déconnecter le volume existant et libérer son emplacement, puis tenter d'exécuter l'opération de restauration.

Actions à effectuer après la restauration de volumes LVM

Vous pouvez effectuer différentes actions après avoir restauré des volumes LVM.

Remarque : Les restaurations de fichiers uniques (SFR), les restaurations granulaires (GRT) et les restaurations d'application s'effectuent à l'aide des agents installés. Cependant, la récupération de volume nécessite la mise en ligne des systèmes de fichiers associés après une récupération ayant abouti.

Pour effectuer des actions après la restauration de volumes

1. Exécutez la commande pour afficher tous les volumes après restauration (PV) récemment connectés à l'hôte.`PVS`

   S'il y a des doublons de PV (un avertissement s'affiche sur la commande ci-dessus), exécutez la commande.

   ```
   vgimportclone --import /dev/<Device1> /dev/<Device2> ...
   --basevgname <NewVGName>
   ```

   Sinon, découvrez les nouveaux groupes de volumes (GV) sur l'hôte. Si les nouveaux GV ne s'affichent pas, importez-les à l'aide de la commande suivante. Elle permet de découvrir les nouveaux GV au format <NomNouveauGV>.

   ```
   vgimport -a

   vgs
   ```

2. Exécutez la commande ci-dessous pour lister tous les volumes logiques (nouveaux et anciens).

   ```
   lvs <NewVGName>
   ```

3. Activez tous les VL appartenant à <NomNouveauGV> :

   ```
   lvchange --activate y /dev/mapper/<NewVGName>-<LVName1>

   lvchange --activate y /dev/mapper/<NewVGName>-<LVName2>

   lvchange --activate y /dev/mapper/<NewVGName>-<LVNameN>
   ```

4. Identifiez l'UUID et le système de fichiers d'un VL authentifié et récemment activé.

   ```
   blkid -p /dev/mapper/<NewVGName>-<LVName1>

   Output: /dev/mapper/<NewVGName>-<LVName1>:
   UUID="2a4bdc14-b5eb-4ee6-b876-ebdcb66c55d9"
   BLOCK_SIZE="4096"TYPE="xfs" USAGE="filesystem"

   blkid -p /dev/mapper/<OldVGName>-<LVName1>

   Output: /dev/mapper/<OldVGName>-<LVName1>:
   UUID="2a4bdc14-b5eb-4ee6-b876-ebdcb66c55d9"
   BLOCK_SIZE="4096"TYPE="xfs" USAGE="filesystem"
   ```

5 Si l'UUID est le même, vous devez le modifier comme suit :

Système de fichiers	Étapes
xfs	`mkdir <NewMountPoint>`
	`mount -o nouuid /dev/mapper/<NewVGName>-<LVName1> <NewMountPoint>`
	`umount <NewMountPoint>`
	`xfs_admin -U generate /dev/mapper/<NewVGName>-<LVName1>`
	`mount /dev/mapper/<NewVGName>-<LVName1> <NewMountPoint>`
ext2/ext3/ext4	`mkdir<NewMountPoint>`
	`tune2fs -U random /dev/mapper/<NewVGName>-<LVName1>`
	`mount /dev/mapper/<NewVGName>-<LVName1> <NewMountPoint>`

6 Si l'UUID est différent, exécutez la commande suivante.

```
mount /dev/mapper/<NewVGName>-<LVName1> <NewMountPoint>
```

Dépannage

Dépannage du processus de restauration de snapshot pour le cloud Microsoft Azure

Lorsque vous démarrez une deuxième opération de restauration de suite sur la même machine virtuelle, une erreur se produit pendant l'opération de restauration. Cette erreur peut provoquer les problèmes suivants :

- Les balises du disque du système d'exploitation d'origine ne sont pas copiées sur le disque de système d'exploitation qui vient d'être restauré.
- La connexion utilisateur peut échouer après la restauration de la machine virtuelle en raison d'une défaillance SSH.

Solution de contournement :

Vérifiez si le daemon SSH est en cours d'exécution sur le système. Si ce n'est pas le cas, suivez les étapes indiquées dans l'article suivant.

learn.microsoft.com/fr-fr/troubleshoot/azure/virtual-machines/troubleshoot-ssh-connection

Filtrage des fichiers et des dossiers non pris en charge

Si vous tentez de restaurer des fichiers ou des dossiers à partir d'une partition ou d'un système de fichiers non pris en charge par Snapshot Manager, le travail de restauration renvoie l'erreur suivante.

`Erreur nbcs (pid=<ID processus>) Échec de la restauration du ou des fichiers et dossiers du snapshot pour le bien <nom du bien>`

Solution de contournement :

Vous pouvez filtrer tous les fichiers ou dossiers non pris en charge par Snapshot Manager. Dans le fichier `bp.conf` sur le serveur principal, définissez l'indicateur suivant pour activer la vérification CP DISKMAP.

CP_DISKMAP_CHECK = true/yes

Réussite partielle d'une opération de sauvegarde à partir d'une restauration

L'opération de sauvegarde à partir d'une restauration aboutit partiellement lorsque le disque du répertoire cible sélectionné est plein. Les messages suivants s'affichent :

```
Dec 29, 2022 2:57:51 PM - Info nbcs (pid=2244) Granular restore(SFR) is completed
    Dec 29, 2022 2:57:51 PM - Info nbcs (pid=2244) Summary of SFR Operation - Success
files/folders count: 0 ,
    Failed files/folders count: 1 , Warning files/folders
    count: 0, Skipped files/folders count: 0
    Dec 29, 2022 2:57:51 PM - Info nbcs (pid=2244)
    Detailed restore summary report is available on recovery target host at location:
    /var/log/flexsnap/restore/granular-restore-09b4d44d
    .
    .
    Dec 29, 2022 2:57:51 PM - Warning bprd (pid=1977) Granular Restore from backup
completed with error.
    Copy the files manually from live access mount:

ip-10-239-185-241:/mnt/vpfs_shares/vmfiles/8fcc/8fcc132b-a202-49a8-b654-81ff242a718a/livemount

    Dec 29, 2022 2:57:51 PM - end Restore; elapsed time 0:01:51
    the requested operation was partially successful(1)
```

Dans le cas d'une sauvegarde à partir d'une restauration, si le montage direct est correctement créé même si une erreur autre que ASSET_NOT_FOUND a été signalée, la réussite de la création est considérée comme partielle. Si aucun

périphérique réseau ou système de fichiers n'est monté à l'emplacement cible et que le disque est plein, les détails du travail affichent les messages suivants :

```
 Jan 02, 2023 12:11:16 AM - Error nbcs (pid=13934)
187776K space required for file/folder restore while 20K is total available space on
/disk1
```

Dans ce cas, d'autres périphériques réseau ou systèmes de fichiers doivent avoir été montés à l'emplacement cible, et l'agent Snapshot Manager tient alors compte de l'espace libre sur le périphérique ou le système de fichiers. Toutefois, la tentative de copie du fichier échoue et une erreur liée à l'espace est consignée dans le rapport récapitulatif. Exemple :

```
 /var/log/flexsnap/restore/granular-restore-09b4d44d in above Job details log
```

Solution de contournement :

- Vérifiez le rapport récapitulatif à l'emplacement de l'hôte cible. Par exemple :

```
/var/log/flexsnap/restore/granular-restore-09b4d44d
[root@ip-10-239-187-148 granular-restore-09b4d44d]# cat root-error.log
Dec 29 09:27:44: ERROR - FILE: /disk1/dl380g9-149-vm15_package.zip
[Error 28] IOError: No space left on device
```

- Si l'opération de copie de fichier a échoué en raison d'un espace disque insuffisant, libérez de l'espace et copiez le fichier à partir du montage direct. Les informations sur le chemin du montage direct se trouvent dans les détails du travail, comme suit :

```
Dec 29, 2022 2:57:51 PM - Warning bprd (pid=1977) Granular Restore from backup completed
 with error.
Copy the files manually from live access mount:
ip-10-239-185-241:/mnt/vpfs_shares/vmfiles/8fcc/8fcc132b-a202-49a8-b654-81ff242a718a/livemount
```

Une récupération partielle est effectuée lorsque l'utilisateur sélectionne une machine virtuelle cible déconnectée

La récupération peut être partielle dans les cas suivants :

- La machine virtuelle cible est déconnectée (aucune connectivité via l'agent).
- Une défaillance se produit lors de la copie de fichiers ou de dossiers sur la machine virtuelle cible.
- Le contenu d'une machine virtuelle Windows est restauré sur une machine virtuelle cible Linux.

Dans ces cas de figure, l'accès instantané créé ne sera pas supprimé et sera accessible pendant les 24 heures suivantes.

Il est possible de configurer l'intervalle de conservation d'accès instantané à l'aide de la clé **CLOUD_VM_IA_RETENTION_INTERVAL_IN_HOURS** dans le fichier `bp.conf`. La valeur par défaut est 24 heures.

Solution de contournement :

L'utilisateur peut effectuer des opérations manuelles pour accéder au partage à accès instantané sur l'hôte cible, puis copier manuellement les fichiers ou les dossiers requis.

(Copie de fichiers via NFS) Pour restaurer le contenu d'une image Linux sur un hôte Linux :

- Pour monter un partage NFS sur un système Linux, installez le package du client NFS à l'aide de la commande suivante :

  ```
  $ sudo yum install nfs-utils
  ```

- Montez l'accès instantané sur l'hôte Linux cible à l'aide de la commande de montage suivante :

  ```
  # Create a directory say /mnt/restore

  $ mkdir -p /mnt/restore

  # Mount the instant access

  $ mount -t nfs <InstantAccessServer:InstantAccessPath> /mnt/restore
  ```

- Le chemin d'accès instantané peut être récupéré à partir des journaux du gestionnaire d'activité au format suivant :

  ```
  <InstantAccessServer>:/mnt/vpfs_shares/vmfiles/<id>/<InstantAccessId>/livemount
  ```

(Accès SMB) Pour restaurer le contenu d'une image Windows (avec liste de contrôle d'accès) sur un hôte cible Windows :

- Les informations d'authentification SMB du serveur de stockage MSDP de l'image de machine virtuelle source doivent être ajoutées au gestionnaire d'informations d'authentification Windows.
- Utilisez le montage direct spécifié pour accéder aux disques durs virtuels via **Moniteur d'activité > Détails du travail**.
  Les disques durs virtuels sont répertoriés dans le dossier avec le préfixe **vhd_**.
- Dans l'onglet **Action**, connectez le disque dur virtuel requis et cliquez sur **OK**.

- Sélectionnez l'option **Attribuer la lettre de lecteur suivante** pour attribuer la lettre au disque virtuel et parcourir les données, puis cliquez sur **OK**.
- Accédez au lecteur attribué à l'étape précédente et copiez les données manuellement.

(Montage direct) Pour restaurer le contenu d'une image Windows sur un hôte cible Linux :

- Linux doit disposer du package CIFS. Procurez-vous les packages à l'aide de la commande `# yum install cifs-utils`.
- Créez le répertoire de montage à l'aide de la commande `# mkdir <my_mount_dir>`.
- Montez le chemin d'accès exporté à l'aide du nom d'utilisateur et le mot de passe Samba, comme suit :

  ```
  mount -t cifs -o username=<sambauser>
  //<InstantAccessServer>/<InstantAccessPath> <my_mount_dir>
  ```

- Copiez les fichiers à l'aide de la commande suivante :

  ```
  # cp <my_mount_dir>/<file_path> <target_dir_path>
  ```

Problèmes de restauration de fichier unique à partir d'une sauvegarde de snapshot

Problème/erreur	Description	Solution de contournement
Chemin d'accès au journal à vérifier	Pour plus d'informations sur les détails de la restauration sur l'hôte cible, consultez les journaux suivants : ■ `chemin d'accès/fichier : /tmp/flexsnap-agentless-onhost.log` ■ `/var/log/flexsnap/restore/granular-restore-*`	Pour résoudre les défaillances ou exceptions qui se produisent lors de la restauration de fichier unique sur Snapshot Manager, consultez les journaux suivants sur l'hôte Snapshot Manager : `/cloudpoint/logs/flexsnap.log`
Échec de la vérification de prérécupération	Lors de la restauration de fichiers et de dossiers sur une machine virtuelle cible déconnectée, la vérification de prérécupération échoue avec l'erreur suivante : `Target VM state: Target VM <vm_name> has no agent configured` Si la récupération est lancée, l'opération de restauration réussit partiellement.	Pour que la restauration s'effectue correctement, assurez-vous que la machine virtuelle cible est connectée à l'agent configuré.

Problème/erreur	Description	Solution de contournement
Récupération partielle d'une machine virtuelle Linux source sur une machine virtuelle Windows cible (sans client NFS)	Si vous n'installez pas le client NFS sur l'ordinateur cible Windows, une restauration de fichiers et de dossiers à partir d'une machine virtuelle Linux source réussit partiellement. L'erreur suivante s'affiche : `Error nbcs (pid=42513) Invalid operation for asset: <asset_id> Warning bprd (pid=42045) Granular Restore from backup completed with error. Copy the files manually from live access mount: <livemount_path>. Note that live access mount is available only for 24 hrs.`	Installez le client NFS sur l'ordinateur cible Windows avant de procéder à la restauration d'une machine virtuelle Linux vers une machine virtuelle Windows.
Le travail de restauration échoue pour la machine virtuelle cible supprimée	Le travail de restauration échoue avec l'erreur suivante lors de la restauration de fichiers et de dossiers sur une machine virtuelle cible supprimée de l'environnement cloud : `Error nbcs (pid=44859) Target VM not found, asset_id <asset_id>`	Sélectionnez une autre machine virtuelle cible.
Échec de la création de l'accès instantané	Si l'accès instantané n'est pas activé sur le serveur de stockage MSDP, la création d'accès instantané échoue pendant le travail de restauration.	Vérifiez si l'accès instantané est pris en charge sur le serveur de médias MSDP. Exécutez le script de prévérification suivant : `/usr/openv/pdde/vpfs/bin/ia_byo_precheck.sh`
La machine virtuelle cible ne dispose d'aucun lecteur libre pour connecter au disque virtuel	Si le nombre de volumes contenant les fichiers sélectionnés est supérieur au nombre de lecteurs disponibles sur l'hôte cible, l'opération échoue.	Sélectionnez un nombre de volumes plus petit pour la restauration.
Espace insuffisant : '*\\driverMapping.json	Le mode FIPS est activé sur le serveur de médias sur lequel MSDP est configuré.	Désactivez FIPS sur le serveur de médias sur lequel MSDP est installé. Vous pouvez également ajouter les informations d'authentification Samba de l'utilisateur de domaine à la machine virtuelle cible.

Problème lié aux machines virtuelles du fournisseur cloud Azure

Si l'un des disques de la machine virtuelle n'est pas initialisé, le téléchargement ou la restauration des fichiers de la machine virtuelle à l'aide de l'accès instantané échoue avec l'erreur suivante :

```
Jan 24, 2023 11:58:47 AM - Error NBWMC (pid=3716) Internal Error:
('failed to find operation system information, please check the source
 VM', ('Failed to expose
VMDK', 1006), None)
Failed to create the instant access mount.
(4001)
```

`libguestfs` est un outil tiers utilisé par l'accès instantané pour récupérer des fichiers à partir d'une sauvegarde de machine virtuelle. Si un disque n'est pas initialisé, `libguestfs` ne peut pas récupérer les fichiers.

Solution de contournement :

Initialisez le disque et sauvegardez la machine virtuelle. Puis, réessayez de télécharger ou de restaurer les fichiers de machine virtuelle à l'aide de l'accès instantané.

Chapitre 4

Résolution des problèmes liés à la protection et à la récupération des biens dans le cloud

Ce chapitre traite des sujets suivants :

- Résolution des problèmes de protection de la charge de travail cloud
- Résolution des problèmes de protection et de récupération de charge de travail PaaS

Résolution des problèmes de protection de la charge de travail cloud

Examinez les fichiers journaux suivants pour résoudre les problèmes relatifs à la protection des biens cloud :

- Fichiers journaux de configuration
- Fichiers journaux pour la création de snapshot
- Fichiers journaux pour les opérations de restauration
- Fichiers journaux pour la suppression du snapshot

Lors du dépannage, assurez-vous que vous avez également examiné les restrictions. Se reporter à "Restrictions et remarques" à la page 10.

Pour le dépannage, consultez le Guide de référence des codes d'état de NetBackup.

Pour afficher les fichiers journaux Snapshot Manager, consultez la rubrique relative aux journaux Snapshot Manager du *Guide d'installation et de mise à niveau de NetBackup Snapshot Manager*.

Fichiers journaux de configuration

Utilisez les journaux suivants pour résoudre les problèmes de configuration du cloud.

Tableau 4-1 Fichiers journaux pour la configuration

Processus	Journaux
tpconfig La commande `tpconfig` permet d'enregistrer Snapshot Manager dans NetBackup.	Windows *chemin d'installation de NetBackup*\volmgr\debug\tpcommand UNIX /usr/openv/volmgr/debug/tpcommand
nbwebservice Les plug-ins sont configurés à l'aide de l'API REST NetBackup.	Windows *chemin d'installation de NetBackup*/webserver/logs UNIX /usr/openv/wmc/webserver/logs /usr/openv/logs/nbwebservices
nbemm nbemm stocke les informations sur Snapshot Manager et sur les plug-ins dans la base de données EMM.	Windows *chemin d'installation de NetBackup*/path/logs/nbemm UNIX /usr/openv/logs/nbemm

Fichiers journaux pour la découverte de biens

Utilisez les journaux suivants pour résoudre les problèmes de découverte des biens.

Tableau 4-2 Fichiers journaux pour la découverte de biens

Processus	Journaux
ncfnbcs Vérifie si la découverte est terminée.	Windows *chemin d'installation de NetBackup*/bin/vxlogview -o 366 UNIX /usr/openv/netbackup/bin/vxlogview -o 366
Picloud Indique les détails de l'opération de découverte.	Windows *chemin d'installation de NetBackup*/bin/vxlogview -i 497 UNIX /usr/openv/netbackup/bin/vxlogview -i 497
nbwebservice Pour obtenir des détails sur les workflows de la base de données de biens dans le cadre de l'opération de découverte. **Remarque :** Consultez les mêmes fichiers journaux pour obtenir plus de détails sur les biens ajoutés à un plan de protection.	Windows *chemin d'installation de NetBackup*/webserver/logs UNIX /usr/openv/wmc/webserver/logs /usr/openv/logs/nbwebservices

Fichiers journaux pour la création de snapshot

Utilisez les journaux suivants pour résoudre les problèmes de création de snapshots.

Tableau 4-3 Fichiers journaux pour la création de snapshot

Processus	Journaux
nbpem Le PID nbpem d'un travail donné est disponible dans le moniteur d'activité NetBackup.	Windows *chemin d'installation de NetBackup*/bin/vxlogview -o 116 UNIX /usr/openv/netbackup/bin/vxlogview -o 116

Processus	Journaux
nbjm Le PID nbjm d'un travail donné est disponible dans le moniteur d'activité NetBackup.	Windows *chemin d'installation de NetBackup*/bin/vxlogview –o 117 UNIX /usr/openv/netbackup/bin/vxlogview -o 117
nbcs Le PID nbcs d'un travail donné est disponible dans le moniteur d'activité NetBackup.	Windows *chemin d'installation de NetBackup*/bin/vxlogview –i 366 -P *id_processus_nbcs* UNIX /usr/openv/netbackup/bin/vxlogview -i 366 -P *nbcs_process_id* Les journaux nbcs sont disponibles à l'emplacement suivant : Windows *chemin d'installation de NetBackup*/logs/ncfnbcs UNIX /usr/openv/logs/ncfnbcs
nbrb nbrb doit spécifier un serveur de médias pour un travail donné. Pour le cloud, un serveur de médias spécifique est sélectionné dans la liste associée de serveurs de médias pour un Snapshot Manager.	Windows *chemin d'installation de NetBackup*/bin/vxlogview –o 118 UNIX /usr/openv/netbackup/bin/vxlogview -i 118

Fichiers journaux pour les opérations de restauration

Utilisez les journaux suivants pour résoudre les problèmes de restauration.

Tableau 4-4

Processus	Journaux
nbwebservice L'opération de restauration du snapshot est déclenchée par l'API REST NetBackup.	Windows *chemin d'installation de NetBackup*/webserver/logs UNIX /usr/openv/wmc/webserver/logs /usr/openv/logs/nbwebservices

Processus	Journaux
bprd L'API REST NetBackup communique avec bprd pour lancer la restauration.	Windows *chemin d'installation de NetBackup*/netbackup/logs UNIX /usr/openv/netbackup/logs/bprd
ncfnbcs Le PID nbcs d'un travail donné est disponible dans le moniteur d'activité NetBackup.	Windows *chemin d'installation de NetBackup*/bin/vxlogview -i 366 -P *id_processus_nbcs* UNIX /usr/openv/netbackup/bin/vxlogview -i 366 -P *nbcs_process_id*

Fichiers journaux pour la suppression du snapshot

Utilisez les journaux suivants pour résoudre les problèmes de suppression de snapshots.

Tableau 4-5 Fichiers journaux pour la suppression du snapshot

Processus	Journaux
bpdm La suppression ou le nettoyage du snapshot est déclenché(e) par bpdm.	Windows *chemin d'installation de NetBackup*/netbackup/logs UNIX /usr/openv/netbackup/logs/bpdm
ncfnbcs Le PID nbcs d'un travail donné est disponible dans le moniteur d'activité NetBackup.	Windows *chemin d'installation de NetBackup*/bin/vxlogview -i 366 -P *id_processus_nbcs* UNIX /usr/openv/netbackup/bin/vxlogview -i 366 -P *nbcs_process_id*

Échec de la vérification de pré-récupération avec une erreur d'accès refusé lors de la restauration à un autre emplacement

Si vous tentez de récupérer une machine virtuelle à partir d'une copie d'image de sauvegarde, alors que votre rôle ne vous donne pas les privilèges requis pour

effectuer une restauration à un autre emplacement, cette erreur se produit pendant l'opération de vérification de pré-récupération.

Cela peut se produire lorsque vos privilèges sont limités à la récupération à l'emplacement d'origine et que vous essayez d'effectuer une récupération à un autre emplacement.

Solution de contournement

- Lors de la restauration à l'emplacement d'origine, ne modifiez aucun champ pré-rempli dans la page de pré-récupération.
- Si vous voulez effectuer une récupération à un autre emplacement, assurez-vous que vous disposez des privilèges requis.

Résolution des problèmes de protection et de récupération de charge de travail PaaS

La sauvegarde échoue avec l'erreur 3808 - Cannot check if the database exists (Impossible de vérifier si la base de données existe).

Le message suivant s'affiche dans le moniteur d'activité :

AuthorizationFailed -Message: The client '<clientId> '<objetId>' does not have authorization to perform action 'Microsoft.Sql/servers/databases/read' over scope '<resoourceId>' or the scope is invalid. Si l'accès a été récemment accordé, actualisez vos informations d'authentification.

Explication : cette erreur se produit lorsque le gestionnaire de snapshots et NetBackup sont déployés dans AKS et :

- Le pool de nœuds de pod de serveur de médias est un pool de nœuds différent du pool de nœuds du gestionnaire de snapshots.
- L'identité gérée est activée dans le groupe de machines virtuelles identiques du gestionnaire de snapshots.

Solution de contournement : effectuez l'une des opérations suivantes :

- Dans le serveur de médias utilisé pour la sauvegarde et la restauration, activez l'option Identité gérée dans le groupe identique. Assignez également l'autorisation requise au rôle associé à cette identité gérée.
- Créez une unité de stockage sur le serveur MSDP et utilisez uniquement les serveurs de médias pour lesquels la fonction Identité gérée est activée lors de la configuration du groupe identique.

La sauvegarde échoue lorsque le verrouillage en lecture seule est appliqué à la base de données ou au groupe de ressources. Elle est partiellement réussie lorsque l'option de suppression du verrouillage est appliquée.

Explication: ce problème se produit si l'attribut de verrouillage en lecture seule ou de suppression du verrouillage est appliqué à la base de données ou au groupe de ressources.

Solution de contournement : avant d'effectuer une sauvegarde ou une restauration, supprimez tous les attributs de verrouillage en lecture seule et de suppression du verrouillage existants de la base de données ou du groupe de ressources.

Code d'état 150 : arrêt demandé par l'administrateur

Explication : cette erreur s'affiche lorsque vous annulez manuellement un travail de sauvegarde ou de restauration à partir du moniteur d'activité et qu'une base de données est créée sur le portail pendant l'opération de restauration partielle.

Solution de contournement : nettoyez manuellement la base de données sur le portail du fournisseur et l'emplacement intermédiaire temporaire à l'emplacement de montage du partage universel sous un répertoire spécifique créé avec le nom de la base de données.

Messages d'état obsolète du moniteur d'activité

Explication : si le service de conteneur Snapshot Manager redémarre brusquement, les travaux de restauration protégés par le fournisseur peuvent rester actifs, et l'état mis à jour ne s'affichera pas sur la page de détails du moniteur d'activité.

Solution de contournement : redémarrez les conteneurs du workflow à l'aide de la commande suivante dans le Snapshot Manager :

```
docker restart flexsnap-workflow-system-0-min
flexsnap-workflow-general-0-min
```

Après le redémarrage des conteneurs, les travaux de restauration sont mis à jour en fonction du dernier état connu du moniteur d'activité.

Code d'état 233 : fin de fichier prématurée détectée

Explication : cette erreur s'affiche si le nom de client utilisé pour la sauvegarde contient plus de 255 caractères.

Le message d'erreur suivant est également ajouté aux journaux `bpdbm` :

```
db_error_add_to_file: Length of client is too long. Got 278, but
limit is 255. read_next_image: db_IMAGEreceive() failed: text exceeded
allowed length (225)
```

Remarque : Ce problème survient lorsque le serveur principal exécute RHEL.

Solution de contournement : renommez la base de données de sorte que le nom du client ne contienne pas plus de 255 caractères.

Erreur : Canal interrompu (32), fin de fichier prématurée TERMINÉ avec l'état 42, échec de lecture du réseau

Ou,

État 174 : Media Manager : une erreur système est survenue

Explication : ce problème se produit lors de la sauvegarde si la longueur du préfixe de la politique défini lors de la création du plan de protection dépasse la limite autorisée. Dans ce cas, le chemin d'accès au fichier de l'image de catalogue contient plus de 256 caractères, la sauvegarde échoue donc et le message d'erreur ci-dessus s'affiche dans le moniteur d'activité.

Le message d'erreur suivant est également ajouté aux journaux `bpdbm` :

```
<16> db_error_add_to_file: cannot stat(\\?\C:\Program Files\Veritas
\NetBackup\db\images \azure-midb-1afb87487dc04ddc8fafe453dccb7ca3+
nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+
testdb_bidinet02\1656000000\tmp\catstore\
BACKUPNOW+141a73e7-cdc4-4371-823a-f170447dba2d_
1656349831_FULL.f_imgUserGroupNames0): No such file or directory (2)
<16> ImageReadFilesFile::get_file_size: cannot stat(\\?\C:\Program
Files\Veritas\NetBackup\db
\images\azure-midb-1afb87487dc04ddc8fafe453d
ccb7ca3+nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+testdb_
bidinet02\1656000000\tmp\catstore\BACKUPNOW+141a73e7-cdc4-4371
-823a-f170447dba2d_1656349831_FULL.f_imgUserGroupNames0): No such
file or directory (2) <16> ImageReadFilesFile::executeQuery: Cannot
copy \\?\C:\Program
Files\Veritas\NetBackup\db\images\azure-midb-1afb87487dc04ddc8fafe453dccb7
ca3+nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+testdb_bidinet02\1
656000000\tmp\catstore\BACKUPNOW+141a73e7-cdc4-4371-823a-f170447d
ba2d_1656349831_FULL.f_imgUserGroupNames0
```

Remarque : Ce problème survient lorsque le serveur principal exécute Windows.

Solution de contournement : dans le plan de protection, utilisez un nom de préfixe de politique comprenant moins de 10 caractères, de sorte que le chemin d'accès complet du catalogue comprenne moins de 256 caractères.

Code d'état 3801 : impossible de terminer l'opération demandée.

Explication : NetBackup n'est pas en mesure d'exécuter correctement l'opération demandée.

Action recommandée : consultez les détails du moniteur d'activité pour identifier les causes possibles de la défaillance.

Code d'état 3817 : impossible de terminer l'opération de présauvegarde

Explication : le message d'erreur s'affiche dans les journaux `dbagentsutil` comme `pg_dump: error: query failed: ERROR: permission denied for table test;pg_dump: error: query was: LOCK TABLE public.test IN ACCESS SHARE MODE;Invoked operation: PRE_BACKUP failed`

Cela se produit lorsque vous essayez de sauvegarder une base de données qui a plusieurs tables avec différents rôles. La sauvegarde peut échouer si au moins un propriétaire des tables est différent du propriétaire de la base de données et que cette personne n'est pas membre du rôle de propriétaire de la base de données.

Action recommandée : vous devez disposer d'un rôle qui a accès à toutes les tables de la base de données que vous voulez sauvegarder ou restaurer.

Par exemple, imaginons que vous vouliez sauvegarder la base de données `Scolaire` qui contient deux tables :

- `enfants`, dont le propriétaire est `postgres`
- `professeur`, dont le propriétaire est `adminscolaire`

Créez un rôle. Par exemple, `NBUbackupadmin`.

Exécutez la commande suivante pour créer le rôle :

```
postgres=> CREATE USER NBUbackupadmin WITH PASSWORD '***********';

CREATE ROLE
```

Pour faire de ce nouveau rôle un membre des rôles `postgres` et `adminscolaire`, exécutez la commande suivante :

```
postgres=> GRANT postgres TO NBUbackupadmin;

GRANT ROLE

postgres=> GRANT schooladmin TO NBUbackupadmin;
```

```
GRANT ROLE
```

Remarque : Vous devez disposer d'un rôle qui est soit propriétaire, soit un membre du rôle de propriétaire de la table, pour toutes les tables de la base de données.

La sauvegarde échoue et renvoie l'état 40 (connexion réseau interrompue).

Explication : les sauvegardes échouent en raison de la perte de connexion au serveur de médias.

Action recommandée : vous pouvez redémarrer le travail de sauvegarde si des points de contrôle sont activés dans la politique. Une fois le problème réseau résolu, sélectionnez le travail de sauvegarde inachevé dans l'interface utilisateur Web et cliquez sur **Reprendre**. Le travail reprend à partir du point où il a été arrêté. Si le point de contrôle n'est pas activé dans la politique, le travail s'affiche comme ayant échoué dans l'interface utilisateur Web.

Le travail de sauvegarde échoue avec l'erreur "Echec de la sauvegarde de la base de données".

Explication : les détails du travail contiennent des informations supplémentaires : authentification ManagedIdentityCredential non disponible. L'identité demandée n'est pas assignée à cette ressource. Aucune identité gérée n'est associée au serveur de médias alloué.

Action recommandée : si vous utilisez l'identité gérée par le système ou par l'utilisateur pour les services PaaS SQL Azure et Managed Instance, appliquez le même ensemble d'autorisations/de règles aux serveurs de médias et à Snapshot Manager. Si vous utilisez une identité gérée par l'utilisateur, associez la même identité gérée par l'utilisateur aux serveurs de médias et à Snapshot Manager.

Code d'erreur 3842 : Le type de sauvegarde demandé pour le bien PaaS correspondant n'est pas pris en charge.

La sauvegarde incrémentielle différentielle est prise en charge uniquement pour Azure SQL Server et Azure SQL Managed Instance. Cette erreur se produit lorsque vous sélectionnez un type de sauvegarde non pris en charge.

Code d'erreur 3843 ou 3844 : Echec de l'activation ou de la désactivation de la capture des données modifiées.

Cette erreur se produit lorsque vous n'êtes pas autorisé à activer ou désactiver la capture des données modifiées.

Explication : accordez à NetBackup les autorisations nécessaires pour activer ou désactiver la capture des données modifiées dans votre environnement Azure.

Remarque : N'activez pas la capture des données modifiées manuellement. Accordez à NetBackup les autorisations nécessaires pour activer ou désactiver la capture des données modifiées.

Erreur : Restauration client - EXIT STATUS 5 : échec de la récupération des fichiers demandés Erreur de restauration de politique cloud (2824)

Erreur : ERR - Echec de la restauration de la base de données [<db_name>] nommée [<db_name>]. ERR - Echec de l'ouverture du fichier ". Numéro d'erreur = 12 : restauration client - EXIT STATUS 5 : échec de la récupération des fichiers demandés

Explication : cette erreur se produit lors de la restauration si l'image de sauvegarde a été générée sur un média 10.2 et que la restauration est effectuée vers un serveur de médias plus ancien (version antérieure à la 10.2).

Solution de contournement : mettez à niveau le média de restauration vers la version 10.2 et supprimez l'ancien média du stockage.

La mise à l'échelle automatique n'est pas activée pour la table AWS DynamoDB après une restauration à partir d'une image de sauvegarde avec l'option de mise à l'échelle automatique activée.

Explication : actuellement, la réponse de l'API AWS ne s'affiche pas si la mise à l'échelle automatique est activée pour une table. Ainsi, pendant la sauvegarde, ces métadonnées ne sont pas capturées dans NetBackup et, par conséquent, la mise à l'échelle automatique n'est pas activée pour la table restaurée.

Solution de contournement : activez manuellement la propriété de mise à l'échelle automatique de la table DynamoDB restaurée dans le portail AWS.

Sauvegardes incrémentielles Azure SQL MI compatibles avec la capture des données modifiées : l'abandon d'une base de données compatible avec la capture des données modifiées entraîne une sauvegarde complète sans modifications de schéma, au lieu d'une sauvegarde incrémentielle.

Explication : Azure SQL MI met à jour les détails de la base de données compatible avec la capture des données modifiées dans la table `cdc_jobs` du schéma `msdb`. Lorsque la base de données est abandonnée, son entrée `cdc_jobs` doit être supprimée. Parfois, cette entrée n'est pas supprimée de la table `de cdc_jobs`. De

ce fait, lorsqu'une nouvelle base de données est créée avec le même `db_id` qui existe déjà dans la table `de cdc_jobs`, le problème se produit.

Solution de contournement : lorsque vous abandonnez une base de données, vérifiez l'entrée correspondante dans la table `cdc_jobs` du schéma `msdb`. Si l'entrée y est présente, supprimez-la manuellement.

Dépannage des problèmes Amazon Redshift

Si la chaîne de requête est supérieure à 100 Ko, la restauration échoue pour Amazon Redshift.

Explication :

Il s'agit d'une limitation connue d'AWS. La taille maximale de l'instruction de requête est de 100 Ko. Consultez la documentation AWS pour plus de détails :

https://docs.aws.amazon.com/redshift/latest/mgmt/data-api.html

Après une restauration de base de données Redshift, si le nombre de procédures, de vues et de fonctions stockées n'est pas identique à celui de la base de données source.

Solution de contournement :

Procédez comme suit :

1. Montez le chemin d'accès à l'accès instantané à l'aide de l'API suivante :

   `netbackup/recovery/workloads/cloud/paas/instant-access-mounts`

2. Accédez au chemin de montage dans le serveur de médias.
3. Assurez-vous que la hiérarchie du répertoire du chemin de montage est la suivante :

   ~~Répertoire_cluster/Répertoire_bases_données/Répertoire_bases_données/Répertoire_schéma/Répertoire_table~~

4. Dans le `Répertoire_schéma/`, recherchez les fichiers `StoredProcedures.json, Views.json` et `Functions.json`. Chacun de ces fichiers contient une ou plusieurs instructions SQL que vous pouvez exécuter dans Amazon Redshift Query Editor-2.

   Exécutez manuellement ces instructions SQL.

botocore.exceptions.ClientError : une erreur s'est produite (InvalidSignatureException) lors de l'appel de l'opération ListDatabases

Explication :

Si l'heure système à laquelle vous exécutez les API AWS Redshift n'est pas correcte, vous obtenez cette erreur. Ce message apparaît dans les journaux :

```
Signature expired: 20230226T181919Z is now earlier than
20230226T181921Z (20230226T182421Z - 5 min.)"
```

Solution de contournement :

Exécutez la commande `ntpdate` pour corriger l'heure système.

Les travaux de sauvegarde ou de restauration échouent avec l'erreur « NoCredentialsError: informations d'authentification introuvables ».

Explication :

Cette erreur apparaît lorsque la région n'est pas spécifiée. Vous pouvez consulter l'erreur suivante dans les journaux `dbagentsutil`. Les journaux `dbagentsutil` se trouvent à l'emplacement suivant :

```
/usr/openv/netbackup/logs/
```

Solution de contournement :

Procédez comme suit :

1. Téléchargez l'interface de ligne de commande AWS sur le serveur de médias sur lequel`dbagent` est en cours d'exécution.
2. Exécutez la commande suivante :

   ```
   aws configure
   ```

3. Entrez le nom de région pour EC2 lorsque vous y êtes invité. Ne spécifiez pas les valeurs des autres paramètres.

Sauvegarde et restauration bloquées pour les bases de données Redshift

Explication :

Cette erreur apparaît lorsque l'instance NetBackup Snapshot Manager qui exécute la découverte n'a pas accès au cluster Redshift. Vous pouvez voir l'erreur suivante dans les journaux flexsnap :

```
Connect timeout on endpoint URL:
"https://redshift.us-east-2.amazonaws.com/
```

Solution de contournement :

Sans autorisation d'accès, Snapshot Manager requiert que les règles de trafic entrant soient configurées pour l'instance Snapshot Manager dans le groupe de sécurité du « terminal client VPC du service Redshift ».

Dans le portail AWS, sélectionnez un cluster. Cliquez sur Propriétés, sur Paramètres réseau et de sécurité, sur l'objet de cloud privé virtuel, puis sur Terminaux client. Recherchez « redshift-endpoint » dans le champ de recherche, cliquez sur l'ID de terminal client VPC, puis cliquez sur l'onglet Groupes de sécurité. Cliquez sur l'ID du groupe de sécurité, puis sur Modifier les règles de trafic entrant, et ajoutez ce qui suit pour les serveurs de médias.

```
Type : HTTPS

Protocol : TCP

Port range : 443

Source : 10.177.77.210/32
```

* Ici, la source se rapporte à l'instance de serveur de médias.

Exécutez à nouveau la découverte à partir de l'interface utilisateur Web NetBackup.