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

Version 10.0

VERITAS™

Dernière mise à jour : 2022-04-27

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

Présentation de l'interface utilisateur Web de NetBackup

Chapitre 2

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
- Découverte des biens PaaS

À propos de la protection des biens cloud

NetBackup permet désormais de protéger vos charges de travail dans le cloud. L'infrastructure de protection des données cloud s'appuie sur l'infrastructure CloudPoint pour obtenir une prolifération plus rapide des fournisseurs cloud. À partir de la version 8.3, CloudPoint peut protéger des biens cloud dans les environnements AWS, Azure, Azure Stack Hub et GCP.

Le tableau suivant décrit les tâches correspondantes.

Tableau 2-1 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 CloudPoint	Installez CloudPoint dans votre environnement. Se reporter à "Ajouter un serveur CloudPoint" à la page 15. Prenez connaissance des limitations de CloudPoint et de NetBackup. Se reporter à "Restrictions et remarques" à la page 11.
Configurer le serveur CloudPoint en utilisant la console d'administration NetBackup	Enregistrez le serveur CloudPoint dans NetBackup. Consultez le *Guide de l'administrateur de NetBackup Snapshot Client*.

Tâche	Description
Ajouter 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 un serveur CloudPoint" à la page 16. Pour Amazon, vous pouvez choisir d'utiliser le rôle IAM. Se reporter à "Rôle IAM pour la configuration AWS" à la page 19.
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. Dans le cas des applications, vous pouvez appliquer l'intervalle de découverte compris entre 15 et 45 minutes. Se reporter à "Découvrir des biens sur le serveur CloudPoint" à la page 20.
Création d'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 50.

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 57.
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 61. Se reporter à "Restauration des biens cloud " à la page 68. ■ 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 85.

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 CloudPoint et des plug-ins qui y sont associés n'est pas prise en charge dans NetBackup.
  Si vous supprimez les plug-ins qui sont configurés dans NetBackup, vous ne pouvez pas récupérer toutes les images CloudPoint associées à ce plug-in.
- Consultez le *Guide d'installation et de mise à niveau de Veritas CloudPoint* pour plus d'informations sur les fonctions de CloudPoint.
- Si vous disposez d'une installation précédente de CloudPoint, Veritas recommande de mettre le serveur CloudPoint à niveau et non de le réinstaller.

Si vous réinstallez le serveur CloudPoint, vous devrez le reconfigurer et réaliser l'intégralité de la procédure relative à la protection.

- Par défaut, CloudPoint est configuré sur le port 443.
- Après l'ajout du serveur CloudPoint, l'ordinateur hôte tente d'utiliser l'adresse IPv6 pour découvrir les biens sur 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 le serveur CloudPoint. Par conséquent, lorsque vous ajoutez ou mettez à jour un serveur CloudPoint, avec des droits NetBackup autres que ceux des utilisateurs racine, mais de niveau administrateur, l'utilisateur est affiché comme utilisateur racine lors de l'audit.
- Si vous déployez CloudPoint à l'aide du modèle CloudFormation, lorsque vous enregistrez l'agent sur l'hôte avec le nœud CloudPoint à l'aide de la commande, l'adresse IP utilisée doit être privée et non pas publique.

Configurer le serveur CloudPoint dans NetBackup

Vous pouvez ajouter un serveur CloudPoint à l'aide de l'interface utilisateur Web NetBackup. À partir de la version 8.3, le serveur CloudPoint 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 serveurs CloudPoint à un serveur principal NetBackup. Cependant, vous ne pouvez associer qu'un seul serveur CloudPoint à un serveur maître NetBackup.
- Vous pouvez associer plusieurs serveurs de médias à un serveur CloudPoint. Seuls les serveurs de médias liés à votre serveur principal NetBackup peuvent être liés à un serveur CloudPoint.
- Vous pouvez maintenant gérer CloudPoint et contrôler la découverte des biens à partir de NetBackup WebUI, de l'API REST et de CLI sans interaction avec les interfaces CloudPoint.
- Les sauvegardes à partir de travaux de snapshot utilisent les serveurs associés au stockage de média NetBackup plutôt que ceux associés à CloudPoint. Les serveurs associés au stockage de média NetBackup doivent être connectés au serveur CloudPoint pour faciliter toutes les opérations liées à CloudPoint.

Le tableau suivant décrit les tâches sous-jacentes.

Tableau 2-2 Configuration de serveurs CloudPoint

Tâche	Description
Ajout d'un serveur CloudPoint	Pour ajouter le serveur CloudPoint dans NetBackup, vous devez ajouter les informations d'authentification et valider le certificat du serveur CloudPoint. Se reporter à "Ajouter un serveur CloudPoint" à la page 15.
Ajout de fournisseurs cloud	Pour découvrir des biens sur le serveur CloudPoint, vous devez ajouter les fournisseurs cloud. Se reporter à "Ajout d'un fournisseur cloud pour un serveur CloudPoint" à la page 16.
Découverte de biens sur le serveur CloudPoint	Vous pouvez découvrir des biens sur le serveur CloudPoint.Se reporter à "Découvrir des biens sur le serveur CloudPoint" à la page 20.
Association de serveurs de médias	Pour décharger des snapshots et des workflows de restauration sur un serveur de médias, vous devez associer ce dernier au serveur CloudPoint.Se reporter à "Associer des serveurs de médias à un serveur CloudPoint" à la page 20.

Configurer un certificat d'autorité de certification tierce

Vous pouvez utiliser un certificat auto-signé ou provenant d'une autorité tierce pour valider votre serveur CloudPoint.

Tenez compte des points suivants :

- Pour Windows, vous pouvez donner un certificat en tant que chemin d'accès au fichier, ou installer le certificat tiers dans les autorités de certification racine approuvées.
- Pour basculer d'un certificat auto-signé à un certificat provenant d'une autorité tierce pour un serveur CloudPoint déjà ajouté, mettez à jour la commande `tpconfig` ou modifiez l'API du serveur CloudPoint, ou encore utilisez l'interface utilisateur Web de NetBackup.

Pour configurer le certificat d'une autorité de certification tierce

1. Générez le certificat tiers et la clé privée pour votre serveur CloudPoint.
2. Exécutez le script /cloudpoint/scripts/cp_certificate_management.sh pour charger le certificat, la clé et le magasin d'approbation sur le serveur CloudPoint.
3. Dans NetBackup, créez un fichier de certificat et ajoutez le certificat de l'autorité de certification racine et de toutes les autorités de certification intermédiaires dans le fichier PEM.
4. Dans le fichier `bp.conf`, à l'emplacement `/cloudpoint/openv/netbackup/`, créez les entrées suivantes :
   - ECA_TRUST_STORE_PATH = /cloudpoint/eca/trusted/cacerts.pem
   - (Facultatif) VIRTUALIZATION_CRL_CHECK = CHAIN
   - (Facultatif) ECA_CRL_PATH =/cloudpoint/eca/crl/

   Remarque : Les certificats d'autorité de certification et les listes de révocation des certificats doivent être présents sous `/cloudpoint/eca/trusted/cacerts.pem` pour le magasin d'approbation et `/cloudpoint/eca/crl` pour la liste de révocation.

   - L'option ECA_CRL_PATH spécifie le chemin d'accès au répertoire où se trouvent les listes de révocation des certifications (CRL) de l'autorité de certification externe. Tous les fichiers dans ECA_CRL_PATH doivent être au format DER, PEM ou P7B.
   - L'option VIRTUALIZATION_CRL_CHECK est requise uniquement si vous voulez vérifier l'état de révocation du certificat. Par défaut, l'option VIRTUALIZATION_CRL_CHECK est désactivée.
   - Vous pouvez désactiver la valeur de l'option VIRTUALIZATION_CRL_CHECK ou la définir sur LEAF ou CHAIN. LEAF : le staut de révocation du certificat feuille est validé à l'aide de la liste de révocation des certificats. CHAIN : le statut de révocation de tous les certificats de la chaîne de certificats est validé à l'aide de la liste de révocation des certificats.

Remarque : Vous devez charger les certificats dans l'ordre suivant : Feuille > Intermédiaire > Racine. Si les certificats ne sont pas chargés dans le bon ordre, CloudPoint risque de ne pas fonctionner.

5 Ajoutez le serveur CloudPoint à NetBackup ou exécutez la commande `tpconfig` pour mettre à jour le certificat d'un serveur CloudPoint déjà ajouté à NetBackup.

Ajouter un serveur CloudPoint

Vous pouvez ajouter un serveur CloudPoint à l'aide de l'interface utilisateur Web NetBackup. Vous devez fournir les informations d'authentification du serveur CloudPoint et valider le certificat.

Remarque : Pour réaliser des sauvegardes à partir de snapshots, vous devez disposer d'une connectivité bidirectionnelle entre CloudPoint et les serveurs NetBackup

Pour ajouter un serveur CloudPoint

1 Dans la partie gauche, cliquez sur **Cloud**.

2 Cliquez sur l'onglet **Serveur CloudPoint**.

3 Cliquez sur **Ajouter**.

4 Dans le champ **Serveur CloudPoint** , entrez l'une des valeurs suivantes :

- Le nom d'hôte ou l'adresse IP du serveur CloudPoint.
  Le nom d'hôte ou l'adresse IP doivent être identiques à ceux que vous avez fournis au moment de la configuration CloudPoint pendant l'installation CloudPoint.
- Si le serveur DNS est configuré, entrez le nom de domaine complet du serveur CloudPoint.

5 Dans le champ **Port**, entrez le numéro de port du serveur CloudPoint.

La valeur par défaut est 443.

6 Cliquez sur **Valider**.

7 Dans la boîte de dialogue **Valider le certificat**, cliquez sur **Accepter**.

8 Entrez les informations d'authentification du serveur CloudPoint qui ont été fournies au moment de son installation.

9 Cliquez sur **Enregistrer**.

Remarque : Si le niveau de sécurité NetBackup est défini sur TRÈS ÉLEVÉ, un champ supplémentaire **Jeton** s'affiche et vous pouvez y spécifier un jeton d'hôte standard. Cela est requis pour la génération de certificats NetBackup sur CloudPoint. Vous devrez peut-être demander les autorisations de sécurité supplémentaires requises pour générer le jeton auprès de l'administrateur de sécurité ou d'un administrateur de sauvegarde.

Ajout d'un fournisseur cloud pour un serveur CloudPoint

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 serveur CloudPoint peut découvrir les charges de travail cloud Amazon Web Services (AWS) et celles de la version de Microsoft Azure Government pour les États-Unis.

Pour ajouter un fournisseur cloud pour un serveur CloudPoint

1. Dans la partie gauche, cliquez sur **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 CloudPoint** voulu.

5 Entrez les informations requises.

Fournisseur cloud	Paramètre	Description
Microsoft Azure	**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.
	Régions	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.
	Avec AAD : **URL du terminal client du gestionnaire de ressources Azure Stack Hub**	URL du terminal client au format suivant, qui permet à CloudPoint de se connecter à vos ressources Azure. `https://management.<emplacement>.<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 CloudPoint de se connecter à vos ressources Azure. `https://management.<emplacement>.<FQDN>`

Fournisseur cloud	Paramètre	Description
	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 serveur CloudPoint est configuré avec IAM Config, les options **Clé d'accès** et **Clé secrète** ne sont pas disponibles.	**Clé d'accès**	L'ID de la clé d'accès, une fois spécifiée avec la clé d'accès secrète, autorise CloudPoint 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.
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.
	Zones	Une liste des zones 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 serveur CloudPoint est déployé dans le cloud, il est possible de configurer AWS pour utiliser le rôle IAM pour l'authentification.

Se reporter à "Ajout d'un fournisseur cloud pour un serveur CloudPoint" à la page 16.

Avant de continuer, vérifiez les points suivants :

- Le rôle IAM est configuré dans AWS. Consultez le *Guide d'installation et de mise à niveau CloudPoint NetBackup* pour plus de détails.
- Après la mise à niveau de NetBackup et CloudPoint vers la dernière version, vous devez mettre à jour les informations d'authentification. Exécutez la commande `tpconfig -update`.

Remarque : Après la mise à niveau, les informations d'authentification sont mises à jour pour ne prendre en charge que le rôle IAM.

Les implémentations suivantes du rôle IAM sont prises en charge :

- Compte source : les biens cloud qui doivent être protégés sont dans le même compte AWS que CloudPoint. 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 qui doivent être protégés se trouvent dans un autre compte AWS que CloudPoint. Par conséquent, vous devez entrer les informations relatives au nom de rôle cible et au compte cible, ainsi qu'à la région afin que CloudPoint 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*.

Associer des serveurs de médias à un serveur CloudPoint

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 un ou plusieurs serveurs de médias à un serveur CloudPoint. 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 serveur CloudPoint doit également être associé à votre serveur maître NetBackup. Cependant, les travaux de découverte s'exécutent uniquement sur le serveur maître NetBackup.

Pour associer des serveurs de médias à un serveur CloudPoint

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

Découvrir des biens sur le serveur CloudPoint

Après avoir configuré vos fournisseurs cloud avec un serveur CloudPoint, la découverte automatique se déclenche pour rechercher les biens cloud. Lors des découvertes périodiques, NetBackup extrait les données de biens de CloudPoint toutes les deux heures, tandis que CloudPoint extrait ces données à partir des configurations de fournisseur cloud toutes les heures. Si vous désactivez un serveur CloudPoint, tous les biens associés à ce serveur ne sont plus protégés ni synchronisés avec NetBackup

Vous pouvez également lancer manuellement la découverte de biens cloud si nécessaire à l'aide de l'option *Découvrir* pour les configurations de fournisseurs cloud individuelles, ou vous pouvez déclencher une découverte sur un serveur CloudPoint pour récupérer les données de biens disponibles sur le serveur CloudPoint.

Après la première découverte complète, NetBackup effectue une découverte incrémentielle périodique des biens pour les plug-ins et serveurs CloudPoint configurés. 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 serveur CloudPoint, selon les fuseaux horaires correspondant à leur localisation, afin d'éviter tout problème lors du processus de découverte.

La procédure suivante décrit comment effectuer la découverte au niveau du serveur CloudPoint, qui ne découvre pas les biens cloud au sens strict, mais récupère seulement les données correspondant à un point dans le temps sur le serveur CloudPoint.

Pour découvrir des biens sur le serveur CloudPoint

1. Dans la partie gauche, cliquez sur **Cloud**.
2. Cliquez sur l'onglet **Serveur CloudPoint**.
3. Dans le menu situé en regard de Serveur CloudPoint, 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 **Cloud**.
2. Cliquez sur l'onglet **Serveur CloudPoint**.
3. Cliquez sur l'adresse IP ou le nom d'hôte du serveur CloudPoint 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 poursuit les synchronisations des biens NetBackup avec ceux du serveur CloudPoint.

Modification de la fréquence de découverte automatique pour les serveurs CloudPoint

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

Modifier un serveur CloudPoint

Vous pouvez mettre à jour les informations d'authentification du serveur CloudPoint. Cependant, vous ne pouvez pas en modifier le nom d'hôte, l'adresse IP ou le port.

Pour modifier un serveur CloudPoint

1. Dans la partie gauche, cliquez sur **Cloud**.
2. Cliquez sur l'onglet **Serveur CloudPoint**.
3. Dans le menu situé en regard du serveur CloudPoint, cliquez sur **Modifier**.

   Vous ne pouvez mettre à jour que les informations d'authentification du serveur CloudPoint. Vous devez valider le certificat pour pouvoir mettre à jour les informations d'authentification.
4. Mettez à jour les informations d'authentification.
5. Dans le champ **Jeton**, entrez un jeton de renouvellement pour le serveur CloudPoint.
6. Cliquez sur **Enregistrer**.

Activer ou désactiver un serveur CloudPoint

Selon vos préférences, vous pouvez activer ou désactiver un serveur CloudPoint. Si vous désactivez un serveur CloudPoint, vous ne pouvez pas découvrir les biens ou assigner des plans de protection.

Pour activer ou désactiver un serveur CloudPoint

1. Dans la partie gauche, cliquez sur **Cloud**.
2. Cliquez sur l'onglet **Serveur CloudPoint**.
3. En fonction de l'état du serveur CloudPoint, sélectionnez **Activer** ou **Désactiver**.

Remarque : Une fois le serveur CloudPoint désactivé, la protection des biens qui lui sont associés ne sera plus assurée par ce serveur. 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 d'une extension CloudPoint

L'extension CloudPoint permet de faire évoluer la capacité de l'hôte CloudPoint à traiter simultanément un grand nombre de requêtes sur le serveur CloudPoint à sa capacité maximale. Vous pouvez installer une ou plusieurs extensions CloudPoint 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 CloudPoint.

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

Environnements d'extension CloudPoint 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 CloudPoint* dans la dernière version du Guide d'installation et de mise à niveau de NetBackup CloudPoint.

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

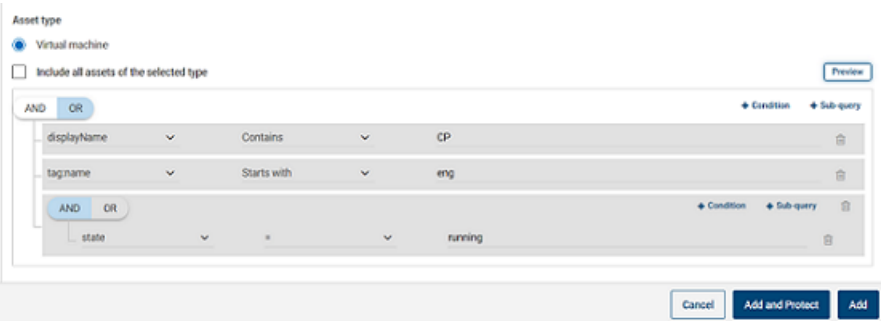
Pour créer un groupe cloud intelligent

1. Dans la partie gauche, cliquez sur **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.
5. Sélectionnez le **type de ressource**.
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 26.

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 **AND** ou **OR**, 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. En conséquence, les biens que la requête sélectionne ultérieurement, lors de l'exécution du plan de protection, peuvent ne pas être identiques à 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`, les biens qui ne correspondent pas au moins à l'une des valeurs de l'attribut ne sont pas 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. Sous **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 externe. Vous pouvez consulter la page de détails du bien ou la réponse de l'API du fournisseur cloud d'un bien individuel.

Tableau 2-3 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 2-4 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 qui n'est pas égale à 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 **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. Les biens ainsi associés à un fournisseur cloud peuvent être abonnés à un plan de protection qui lui est propre.

Remarque : Si vous aviez précédemment appliqué un plan de protection aux biens de différents fournisseurs cloud, il sera automatiquement converti au nouveau format propre au fournisseur après la mise à niveau vers NetBackup 9.1. Par exemple, si vous avez abonné les biens Google Cloud et AWS Cloud à un plan de protection, ce plan de protection sera divisé et converti en deux plans distincts, un pour chaque fournisseur.

Se reporter à la section intitulée « Conversion des plans de protection après la mise à niveau vers NetBackup 9.1 » à la page 29..

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 **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**

- **Options de sauvegarde**

5 Cliquez sur **Protéger**.

Option « Sauvegarder maintenant » pour la 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 la 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 lorsque la migration des biens est terminée après la mise à niveau vers NetBackup 9.1.
- Les anciens plans de protection sans biens abonnés ne seront 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 a été utilisé pour protéger les biens de plusieurs fournisseurs cloud, le nom de l'ancien plan de protection est conservé, mais est mis à jour pour conserver l'abonnement de biens pour l'un de ces 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>`.
- Par conséquent, il est possible que davantage de plans figurent 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 <nomPlanProtection> a été créé pendant la conversion vers le nouveau format.* »
  « *Le plan de protection <nomPlanProtection> a été converti au 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. Ensuite, la tentative de conversion des biens qui n'ont pas été désabonnés reprend 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 **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 (le bien est supprimé du serveur CloudPoint).

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'"
      }
    }
}
```

Prise en charge des services cloud AWS et Azure Government

À partir de la version 8.3, le serveur CloudPoint peut découvrir les charges de travail cloud Amazon Web Services (AWS) et celles de la version de Microsoft Azure Government pour les États-Unis. Une fois le serveur CloudPoint ajouté à NetBackup, vous pouvez protéger les charges de travail avec NetBackup. NetBackup remplit toutes les conditions réglementaires, notamment avec la prise en charge d'IPv6, pour le déploiement de CloudPoint pour 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. Pour un même hôte CloudPoint, vous ne pouvez pas utiliser une combinaison de clouds publics et gouvernementaux.

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

CloudPoint 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

Pour plus d'informations sur la configuration d'AWS et de Microsoft Azure, voir Se reporter à "Ajout d'un fournisseur cloud pour un serveur CloudPoint" à la page 16.

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/fr-fr/azure/azure-resource-manager/management/manage-resource-groups-portal

CloudPoint crée un snapshot et le place dans le groupe de ressources auquel la ressource appartient, 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. CloudPoint 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 2-5 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.
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.

Préfixe du groupe de ressources	Case à cocher Protéger les biens même si des groupes de ressources préfixés sont introuvables	Résultat
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 2-6 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.

Conditions	Configurations	Résultat
■ 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.
■ 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.

Conditions	Configurations	Résultat
■ 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.
■ 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.

Conditions	Configurations	Résultat
■ 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 **Rôle propriétaire**, **Attribuer l'accès comme utilisateur** et sélectionnez l'**Application (créée pour CloudPoint pour effectuer des 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 l'E/S sur le serveur CloudPoint.
- Réduit la charge du processeur sur le serveur CloudPoint.

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, tout en créant un plan de protection pour les charges de travail cloud Azure, Azure Stack et AWS.

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 Dans la liste déroulante **Récurrence**, spécifiez la fréquence de la sauvegarde.

5 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 50.
  - 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 est affiché dans la colonne **Répliques de snapshot** du tableau **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**.

Remarque : Comme NetBackup ne prend en charge la restauration granulaire qu'à partir du snapshot, si vous sélectionnez l'option **Conserver la sauvegarde uniquement** , les options de récupération granulaire ne fonctionnent pas. De même, la fonction de réplication de snapshot AWS ne fonctionne pas si vous cochez **Conserver uniquement la sauvegarde**.

6 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 n'est pas disponible.

Indexation pendant les travaux de sauvegarde et de snapshot

- NetBackup effectue l'indexation reposant 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 serveur CloudPoint. L'indexation reposant sur VxMS est actuellement prise en charge pour les clouds AWS, Azure et Azure Stack Hub.
- L'indexation est effectuée pendant les travaux de sauvegarde ou de snapshot réels, mais vous pouvez exécuter la récupération de fichiers ou de dossiers individuels uniquement à partir de la copie de snapshot 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 de débogage du connecteur cloud sont disponibles dans le dossier */cloudpoint/openv/dm/datamover.<datamover-id>/netbackup/logs* du serveur CloudPoint.

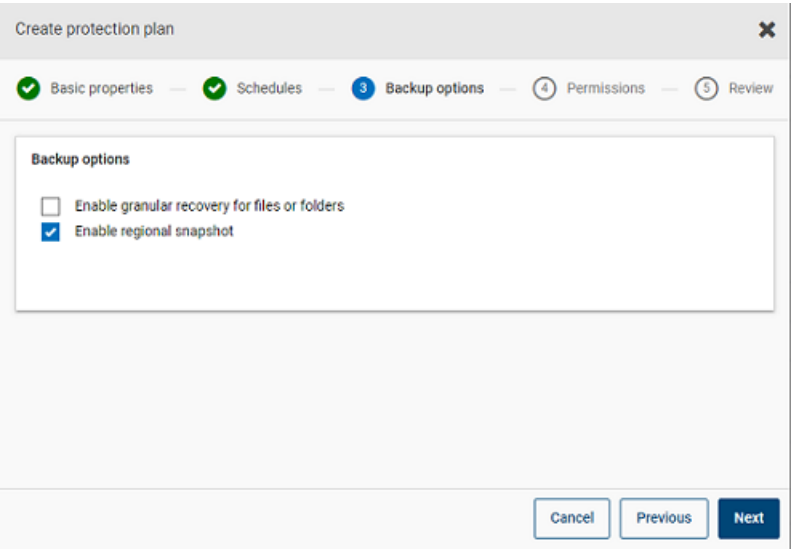
Remarque : Si la machine virtuelle n'est pas connectée, la sauvegarde de la machine virtuelle continue et le travail de sauvegarde est marqué comme partiellement réussi. Dans ce cas, vous ne pouvez pas restaurer des fichiers ou des dossiers individuels, car l'indexation n'est pas disponible lorsque la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

Options de sauvegarde des charges de travail cloud

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

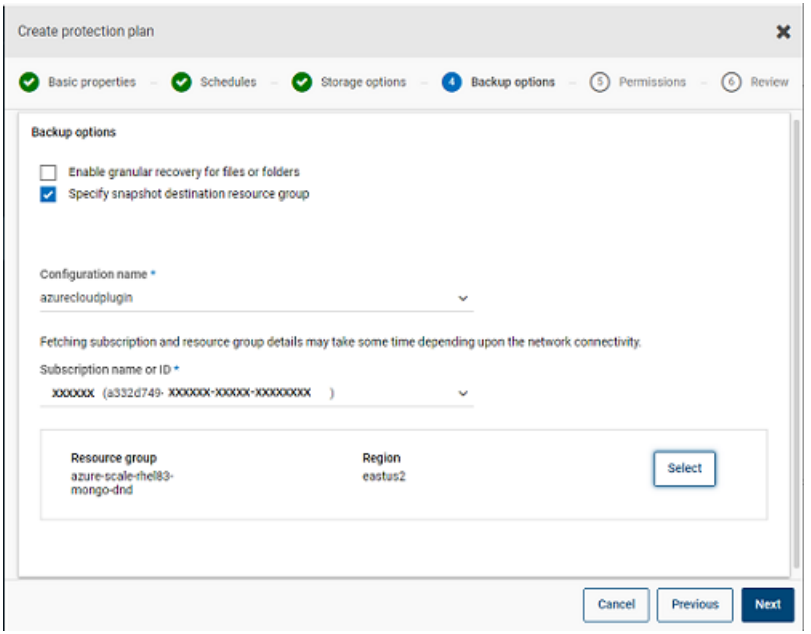
Vous pouvez spécifier un groupe de ressources pair de destination de snapshot lors de la création du plan de protection pour Azure ou Azure Stack Hub. Il reste possible de définir un groupe de ressources pair en spécifiant un préfixe, mais vous

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, le snapshot reste un snapshot de blocage cohérent même si le disque contenant le système de fichiers non pris en charge est exclu.
- 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 CloudPoint NetBackup, 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 Share a snapshot de la documentation AWS.
- Copiez le snapshot. Pour plus d'informations, consultez la section opySnapshot 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 CloudPoint. 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 CloudPoint.
  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 serveurs CloudPoint prennent en charge la réplication entre régions et entre comptes. Grâce à la réplication de snapshot, vous pouvez 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 serveur CloudPoint doivent être répliqués sur la région découverte par ce serveur CloudPoint.
  Par exemple, les biens découverts par le serveur CloudPoint « CP1 » ne peuvent pas être abonnés à un plan de protection assurant la réplication dans une région découverte par le serveur CloudPoint « 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. Consultez le *Guide d'installation et de mise à niveau de NetBackup™ CloudPoint* et le *Guide de l'administrateur de l'interface utilisateur Web NetBackup* pour en savoir plus sur ces étapes, sauf indication contraire.

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 le serveur CloudPoint (CP1) dans l'interface utilisateur Web. Se reporter à "Ajouter un serveur CloudPoint" à la page 15.
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. Déclenchez 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. Étant donné que la région source est défaillante, vous devez d'abord restaurer les machines virtuelles dans la région cible.

Remarque : Vous ne pouvez pas restaurer des fichiers ou des dossiers spécifiques à partir d'une réplique découverte par un autre serveur CloudPoint 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 "Activer ou désactiver un serveur CloudPoint" à la page 22.
2. Enregistrez un nouveau CloudPoint cible (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 la console NetBackup.

- Dans la partie gauche, cliquez sur **Cloud**, dans la section **Charges de travail**. Dans l'onglet **Machines virtuelles**, cliquez sur la machine 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 61.

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

6 Désinstallez et réinstallez l'agent CloudPoint des machines virtuelles restaurées, puis enregistrez les agents CloudPoint sur le 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. Déclenchez 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 Déclenchez une sauvegarde et une réplication par snapshot.

4 Désactivez le serveur CP2 dans l'interface utilisateur Web. Se reporter à "Activer ou désactiver un serveur CloudPoint" à la page 22.

5 Activez le serveur CP1 et déclenchez 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 CloudPoint des machines virtuelles restaurées, puis enregistrez les agents CloudPoint sur le 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 2-7 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 2-8 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 2-9 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 MongoDB et 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 CloudPoint.

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**.

Découverte des biens PaaS

NetBackup permet de découvrir et de restaurer des biens de base de données Azure SQL et des biens de base de données gérées Azure SQL 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 : Vous ne pouvez pas ajouter de biens PaaS à des plans de protection NetBackup.

Pour découvrir des biens PaaS

1. Ajoutez un serveur CloudPoint. Se reporter à "Ajouter un serveur CloudPoint" à la page 15.
2. Ajoutez Microsoft Azure en tant que fournisseur. Se reporter à "Ajout d'un fournisseur cloud pour un serveur CloudPoint" à la page 16.
3. Exécutez une découverte. Se reporter à "Découvrir des biens sur le serveur CloudPoint" à la page 20.

Une fois la découverte terminée, vous pouvez trouver les biens découverts de base de données Azure SQL et les biens de base de données gérées Azure SQL dans l'onglet **PaaS** de la charge de travail **cloud**.

Remarque : Lorsque vous créez et supprimez des biens PaaS du même nom par intervalles et si le bien PaaS est supprimé après découverte, l'interface utilisateur Web affiche d'anciennes données jusqu'à ce que la découverte périodique suivante s'exécute.

Chapitre 3

Surveillance de NetBackup

Chapitre 4

Récupération des biens dans le cloud

Ce chapitre traite des sujets suivants :

Récupération des biens cloud

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

Lors de la restauration des 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 les machines virtuelles dans une autre configuration, dans une région différente, avec un abonnement différent et restaurer des machines virtuelles ou des disques dans un groupe de ressources différent.

À propos de la vérification de pré-récupération 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 serveur CloudPoint et validation des informations d'authentification cloud.

À propos de la vérification de pré-récupération pour les biens PaaS

Lors de la vérification de pré-récupération pour les biens PaaS, les points suivants sont vérifiés :

- Un nom d'affichage valide de la base de données SQL Azure. Une autre base de données avec le même nom d'affichage ne doit pas exister.
- Un point de restauration valide dans Azure. Le point de restauration doit être une heure postérieure ou égale au point de récupération le plus ancien et antérieure ou égale à l'heure actuelle.
- Une instance gérée valide dans Azure. L'instance gérée spécifiée doit exister. Si l'instance gérée existe, seul le nom affiché de la base de données SQL est validé sous cette instance. Applicable uniquement aux points de récupération des bases de données gérées Azure SQL.

Paramètres pris en charge pour la restauration des 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 4-1 Paramètres pris en charge pour les copies de snapshot et de sauvegarde Azure et Azure Stack

Paramètres	Copie de snapshot		Copie de sauvegarde		
	Azure	Azure Stack	Azure	Azure Stack	AWS

Modifier le nom affiché de la machine virtuelle	O	O	O	O	O
Modifier l'état d'alimentation de la machine virtuelle	O	O	O	O	O
Supprimer les associations d'étiquettes	O	O	O	O	O
Restaurer sur un autre réseau	O	O	O	O	O
ID de l'abonnement			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	O
Modifier le groupe de ressources pour les disques	O	O	O	O	

Tableau 4-2 Paramètres pris en charge par les copies de snapshot AWS et GCP

Paramètres	**AWS**	**GCP**
Modifier le nom affiché de la machine virtuelle	O	O

Modifier l'état d'alimentation de la machine virtuelle	O	O
Supprimer les associations d'étiquettes	O	O
Restaurer sur un autre réseau	O	O

Récupération des machines virtuelles

Pour récupérer une machine virtuelle

1. Dans la partie gauche, cliquez sur **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**.

8 Cliquez sur **Suivant**.

9 Dans la page Options de récupération :

- Si vous restaurez une copie de sauvegarde dans une autre région, sélectionnez une **région**. 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.
- Si vous restaurez une copie de snapshot, cliquez sur l'icône de recherche dans **Configuration du réseau** et sélectionnez un réseau cible pour la récupération. La liste affiche les réseaux disponibles dans cette région.

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.

---

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 **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 **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.

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 Google Cloud Platform avec des volumes 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 de l'interface utilisateur Web NetBackup)	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 cohérent au niveau panne (dans l'onglet *Machines virtuelles* sous Charges de travail cloud de l'interface utilisateur Web NetBackup)	Pendant la restauration d'une telle machine virtuelle à son emplacement d'origine ou à un autre emplacement, un disque « en lecture seule » sera restauré 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 de l'interface utilisateur Web NetBackup)	Même si un disque en lecture seule peut être connecté à plusieurs machines virtuelles, il sera découvert sous une seule machine virtuelle.
	
	Dans le cas d'une machine virtuelle Windows, le snapshot échouera avec une erreur VSS, semblable à ce qui suit :
	
	`Failure: flexsnap.GenericError: Failed to take snapshot(error: Failed to create VSS snapshot of the selected volumes.)"`
	
	Dans le cas d'une machine virtuelle Linux, le snapshot peut être réussi ou non pour une machine virtuelle sous laquelle le disque est découvert, mais il échouera pour d'autres 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-west2-b-7534340043132122994'] but no other entity produces said requirements\n MissingDependencies`
	
	Dans le cas ci-dessus, si un snapshot est réussi pour une machine virtuelle Linux, un disque « en lecture seule » sera restauré en mode « Lecture/écriture ».

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 le volet gauche, cliquez sur **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

NetBackup permet de restaurer des biens de base de données Azure SQL et des biens de base de données gérée Azure SQL 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 **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 à un moment donné**, cliquez sur **Restaurer**.
5. Sélectionnez une date et une heure sous **Point de restauration (UTC)**. Vous pouvez sélectionner n'importe quel point de restauration situé entre le point de restauration 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, selon le fuseau horaire UTC.

La date et l'heure de restauration par défaut affichées dans l'interface utilisateur Web peuvent différer en fonction du bien PaaS sélectionné. Par exemple, pour les bases de données Azure SQL, l'heure de restauration par défaut est l'heure actuelle, et pour les bases de données gérées Azure SQL, l'heure de restauration par défaut est 6 minutes plus tôt que l'heure actuelle.

6 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 https://docs.microsoft.com/fr-fr/azure/azure-resource-manager/management/resource-name-rules#microsoftsql

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

7 Pour les bases de données gérées Azure SQL, vous pouvez entrer le nom de l'instance dans le champ **Instance gérée**. Par défaut, le nom d'instance du point de récupération s'affiche. Vous pouvez également rechercher le nom de l'instance gérée à l'aide de l'option de recherche. Vous pouvez effectuer une restauration dans la même région que celle à laquelle appartient votre abonnement.

Si vous ne pouvez pas voir l'instance gérée désirée dans les résultats de recherche, effectuez une découverte manuelle. En outre, assurez-vous que vous disposez d'un accès RBAC à l'instance gérée.

8 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 **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** à côté de l'image que vous souhaitez 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 https://docs.microsoft.com/fr-fr/azure/azure-resource-manager/management/resource-name-rules#microsoftsql

   Si vous n'entrez pas de nom, NetBackup attribue automatiquement un nom au format *<nom_base_de_données>_<heure de restauration UTC>*.
6. Pour les bases de données gérées Azure SQL, vous pouvez entrer le nom de l'instance dans le champ **Instance gérée**. Par défaut, le nom d'instance du point de récupération s'affiche. Vous pouvez également rechercher le nom de l'instance gérée à l'aide de l'option de recherche. 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 et CloudPoint 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.

Chapitre 5

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 restauration, et à la fois 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 est considéré comme un granule, généralement appelé restauration de fichier unique. NetBackup effectue un inventaire de tous les fichiers dans un snapshot 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.

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

Tableau 5-1 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 > Serveurs CloudPoint > *Serveur CloudPoint* > 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, ou restaurer des volumes	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 5-2 Versions prises en charge

Application	Version
NetBackup	10.0

Application	Version
Système d'exploitation de l'hôte de sauvegarde NetBackup	RHEL 7.x et 8
Système d'exploitation de l'hôte CloudPoint	■ RHEL 7.x et versions ultérieures, RHEL 8.4 et 8.5 ■ 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
CloudPoint 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 version ultérieure
Hôte de l'agent CloudPoint à protéger	■ Système d'exploitation Linux : RHEL 7.x et RHEL 8.2, 8.4 et 8.5 ■ 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 :** La restauration granulaire pour l'hôte de l'agent RHEL 8.3 et 8.2 est prise en charge uniquement lorsque CloudPoint est déployé sur RHEL 8.3.	■ ext3 ■ ext4 ■ xfs	■ GPT ■ MBR ■ Aucune structure (direct FS)
Windows (avec propriété de snapshot cohérent)	NTFS	■ GPT ■ MBR

Remarque : La fonctionnalité de snapshot cohérent n'est pas prise en charge pour le système de fichiers version 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 serveur CloudPoint configuré et la machine virtuelle à protéger avec l'activation de la restauration granulaire doivent remplir les conditions suivantes :

- (Microsoft Azure et Azure Stack Hub) Si CloudPoint n'est pas déployé dans le même abonnement et dans 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 CloudPoint en utilisant le même abonnement et la même région que les machines virtuelles.
- Amazon AWS : l'hôte CloudPoint et la machine virtuelle connectée doivent être dans le même compte et dans la même région.
- Google Cloud Platform : l'hôte CloudPoint et la machine virtuelle connectée doivent être dans le même projet.
- Le plug-in Cloud doit être configuré pour protéger les biens dans la région dans laquelle l'hôte CloudPoint est déployé.

- L'hôte doit être connecté et présenter la configuration prise en charge requise.
- Les indicateurs **fsConsistent** et **indexable** de l'hôte doivent être activés lorsqu'il se connecte. 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 disque supplémentaire ne doit être explicitement lié à l'instance CloudPoint.
- 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 74.
- Configurez les ports 5671 et 443 pour l'hôte CloudPoint 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/fixe sur les machines virtuelles indexables.
- Pour restaurer le volume sur la même machine virtuelle, vous devez détacher le volume existant et libérer son emplacement, puis essayer d'exécuter l'opération de restauration.

Limitations et remarques

Tenez compte des points importants suivants lors d'une opération de restauration granulaire.

- Une fois qu'un travail de restauration est terminé, vous ne pouvez plus développer les répertoires dans la section **Liste de fichiers** du travail de restauration.
- 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 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 devient vide.
- Les octets transférés et les octets estimés dans le moniteur d'activité ne sont pas mis à jour et affichent 0.
- (Applicable uniquement à GCP) Nombre de points d'attache pour les disque de données disponibles correspond au nombre total de logements de disque en fonction du type d'instance sur l'hôte CloudPoint moins 1. Le volume de métadonnées CloudPoint consomme ce point d'attache unique.

- Les périphériques de stockage éphémères, tels que les volumes de magasin d'instances d'Amazon AWS et les disques temporaires Microsoft Azure sont ignorés lors de la réalisation de snapshots. Ces périphériques sont également ignorés pour l'indexation.
- Les systèmes de fichiers créés sur des disques LDM sont ignorés lors de la création et de l'indexation de snapshots cohérents avec l'hôte.
- 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. Vous devez redémarrer les agents plus anciens afin de prendre en charge la récupération des biens LVM.
- 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 CloudPoint pris en charge. L'indexation VxMS peut être effectuée avec les clouds Azure, AzureStack et AWS. Avec GCP, elle sera effectuée sur une indexation existante reposant sur le montage.
- 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 qui est 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.
- CloudPoint communique le nombre de travaux d'indexation pouvant être exécutés sur NetBackup. NetBackup régule ensuite les requêtes. Par défaut, le nombre de travaux d'indexation est défini sur 2. Après la découverte des fonctions de l'hôte CloudPoint, cette valeur reprend le nombre d'emplacements de disque disponibles. Néanmoins, vous pouvez mettre à jour la valeur d'indexation de max_jobs=<value> dans le fichier flexsnap.conf pour remplacer cette limite.
- L'hôte CloudPoint limite le nombre d'emplacements de disque appliqués par les fournisseurs cloud. NetBackup régule les demandes d'indexation destinées à CloudPoint. Pour exécuter cette demande, pendant le processus de découverte de biens cloud, NetBackup récupère les fonctions d'hôte CloudPoint. Ces fonctions incluent le paramètre **Nombre maximum de travaux d'indexation** . Ce paramètre permet de limiter les demandes qui sont envoyées à CloudPoint et d'indexer la file d'attente des travaux dans NetBackup. Par défaut, le nombre maximal de travaux d'indexation parallèles est de 2. Mais une fois que le plug-in cloud est configuré pour détecter l'hôte CloudPoint, l'API de capacité récupère le nombre de travaux maximum en fonction des points d'attache et des ressources disponibles. Vous pouvez définir la limite en ajoutant l'entrée

`indexing max_jobs=x` dans le fichier de **configuration** de l'hôte CloudPoint. Si l'hôte CloudPoint reçoit un nombre de demandes d'indexation supérieur à sa capacité, les demandes supplémentaires sont mises en file d'attente.

- Lorsqu'une opération d'indexation est en cours, si des erreurs se produisent au niveau du système d'exploitation lors de l'analyse des fichiers, des répertoires ou d'autres entrées, les 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.
- Si un point de montage n'est pas visible dans l'arborescence du volet gauche pour permettre la navigation quand vous ajoutez des fichiers ou des dossiers depuis le point de récupération, cela peut être dû aux 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.

  Par exemple, si un disque est monté sur/mnt1/mnt2 où /mnt1 est un répertoire de « / » (le FS racine de la configuration LVM) et mnt2 un point de montage à l'intérieur de mnt1, le « mnt2 » n'est pas visible dans l'arborescence du volet gauche. Cependant, vous pouvez rechercher et restaurer des fichiers ou des dossiers dans le point de montage.
- Les fichiers et les dossiers ne peuvent être restaurés à partir de points de récupération de snapshots de machine virtuelle que si les entrées du fichier `/etc/fstab` des 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.
- Lors de la restauration d'un lecteur en tant que source vers un autre dossier comme destination, le groupe d'utilisateurs ne peut pas effectuer l'opération d'écriture sur le dossier nouvellement créé en raison d'une absence d'autorisation d'écriture.
- La connexion sans agent ne peut pas restaurer le fichier chiffré par Windows (ou EFS) via la restauration granulaire au niveau du fichier (option Restaurer

les fichiers et les dossiers). Cependant, vous pouvez restaurer le fichier via la restauration au niveau du volume, puis déchiffrer le fichier.

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 le volet gauche, cliquez sur **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. Dans le coin supérieur droit du point de récupération de votre choix, sélectionnez **Restaurer les fichiers et les dossiers**.

   Vous pouvez également appliquer des filtres de date pour rechercher des points de récupération. Dans le cas d'une réplication, cliquez sur **Récupérer**, puis sélectionnez Restaurer les fichiers et les dossiers.
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 À l'étape Cible de récupération, sélectionnez une machine virtuelle dans la liste **Machine virtuelle cible**.

Une liste contenant toutes les machines virtuelles connectées et dont le système d'exploitation est identique à celui de 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.

14 Dans les options de **restauration de fichiers**, sélectionnez l'une des options suivantes :

- **Tout restaurer dans le répertoire d'origine**
- **Tout restaurer dans un autre répertoire**
  Vous devez alors indiquer un emplacement de répertoire. Vous pouvez également entrer un chemin d'accès UNC pour l'emplacement.

15 Cliquez sur **Suivant**.

16 À l'étape Options de récupération, sélectionnez l'option de votre choix :

- **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.
- **Remplacer les fichiers existants**
  Vous devez disposer des autorisations appropriées.
- (Si vous avez sélectionné l'option **Tout restaurer dans un autre répertoire**) **Créer de nouveaux fichiers pour les liens physiques**

17 Cliquez sur **Suivant**.

18 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.

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 **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.

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 déclenchez 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, effectuez les étapes mentionnées dans la rubrique https://docs.microsoft.com/fr-fr/azure/virtual-machines/troubleshooting/troubleshoot-ssh-connection .

Filtrage des fichiers et des dossiers non pris en charge

Si vous essayez de restaurer des fichiers ou des dossiers à partir d'une partition ou d'un système de fichiers qui n'est pas pris en charge par CloudPoint, 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 :

Pour éviter de générer la liste des fichiers ou des dossiers lorsque vous effectuez une recherche en vue d'une restauration de fichier unique, ce qui n'est pas pris en charge par CloudPoint, activez la vérification CP DISKMAP en définissant l'indicateur ci-dessous dans le fichier `bp.conf` du serveur principal NetBackup.

CP_DISKMAP_CHECK = true/yes

Chapitre 6

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

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 11.

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

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

Fichiers journaux de configuration

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

Tableau 6-1 Fichiers journaux pour la configuration

Processus	Journaux
tpconfig La commande `tpconfig` permet d'enregistrer CloudPoint 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 le plug-in et le serveur CloudPoint 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 6-2 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 6-3 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 fournir un serveur de médias pour un travail donné. Pour le cloud, un serveur de médias spécifique est sélectionné dans la liste associée des serveurs de médias pour un serveur CloudPoint.	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 6-4

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
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 6-5 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

Processus	Journaux
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 récupération de charge de travail PaaS

Erreur 150 : arrêt demandé par l'administrateur

Explication : cette erreur s'affiche lorsque vous annulez manuellement un travail 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.

Messages d'état obsolètes dans le moniteur d'activité

Explication : si le service de conteneur CloudPoint redémarre brusquement, les travaux de restauration protégés par le fournisseur peuvent rester à l'état actif. Dans ce cas, vous ne pouvez pas voir l'état mis à jour sur la page de détails du moniteur d'activité.

Solution de contournement : redémarrez les conteneurs de workflow à l'aide de la commande suivante dans le serveur CloudPoint :

```
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 selon le dernier état dans le moniteur d'activité.