

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

Version 10.1.1

Dernière mise à jour : 2023-01-29

Mentions légales

Copyright © 2023 Veritas Technologies LLC. Tous droits réservés.

Veritas et le logo Veritas et NetBackup sont des marques ou des marques déposées de Veritas Technologies LLC ou de ses filiales aux États-Unis et dans d'autres pays. Les autres noms peuvent être des marques commerciales de leurs détenteurs respectifs.

Ce produit peut contenir des logiciels tiers pour lesquels Veritas est tenu de mentionner les tiers concernés ("Programmes tiers"). Certains des programmes tiers sont disponibles sous licence Open Source ou gratuite. Le contrat de licence accompagnant le logiciel ne modifie aucun des droits ou obligations que vous pouvez avoir dans le cadre de ces licences Open Source ou de logiciel gratuit. Reportez-vous au document des mentions légales tierces accompagnant ce produit Veritas ou disponible à l'adresse :

<https://www.veritas.com/about/legal/license-agreements>

Le produit décrit dans ce document est distribué dans le cadre de licences limitant son utilisation, sa copie, sa distribution et sa décompilation ou son ingénierie inverse. La reproduction de ce document, sous quelque forme que ce soit, est formellement interdite sans l'accord écrit préalable de Veritas Technologies LLC et de ses concédants de licence, le cas échéant.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET L'ENTREPRISE N'ASSUME AUCUNE RESPONSABILITÉ QUANT À UNE GARANTIE OU CONDITION D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, Y COMPRIS TOUTES GARANTIES OU CONDITIONS IMPLICITES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER OU DE RESPECT DES DROITS DE PROPRIÉTÉ INTELLECTUELLE, DANS LA MESURE OÙ CETTE CLAUSE D'EXCLUSION DE RESPONSABILITÉ RESPECTE LA LOI EN VIGUEUR. Veritas Technologies LLC NE SERA PAS RESPONSABLE DES DOMMAGES ACCESSOIRES OU INDIRECTS LIÉS À LA PRESTATION, LA PERFORMANCE OU L'UTILISATION DE CETTE DOCUMENTATION. LES INFORMATIONS CONTENUES DANS CETTE DOCUMENTATION SONT SUJETTES À MODIFICATION SANS PRÉAVIS.

Le logiciel et la documentation sous licence sont assimilables à un logiciel commercial selon les définitions de la section FAR 12.212 et soumis aux restrictions spécifiées dans les sections FAR 52.227-19, "Commercial Computer Software - Restricted Rights" et DFARS 227.7202 et "Commercial Computer Software and Commercial Computer Software Documentation" en vigueur et selon toute autre législation en vigueur, qu'ils soient fournis par Veritas en tant que services locaux ou hébergés. Toute utilisation, modification, reproduction, représentation ou divulgation du logiciel ou de la documentation sous licence par le gouvernement des États-Unis doit être réalisée exclusivement conformément aux conditions du Contrat.

Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

<http://www.veritas.com>

Support technique

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

<https://www.veritas.com/support>

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

<https://my.veritas.com>

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

Monde (sauf Japon)

CustomerCare@veritas.com

Japon

CustomerCare_Japan@veritas.com

Documentation

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

<https://sort.veritas.com/documents>

Commentaires sur la documentation

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

NB.docs@veritas.com

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

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

Veritas Services and Operations Readiness Tools (SORT)

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

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

Table des matières

Chapitre 1	Gestion et protection des biens dans le cloud	7
	À propos de la protection des biens cloud	8
	Restrictions et remarques	10
	Configuration de Snapshot Managers dans NetBackup	11
	Configurer un certificat d'autorité de certification tierce	12
	Ajout de Snapshot Manager	14
	Ajout d'un fournisseur cloud pour Snapshot Manager	15
	Association de serveurs de médias à un Snapshot Manager	19
	Découverte de biens sur Snapshot Manager	20
	Modifier un Snapshot Manager	21
	Activation ou désactivation d'un Snapshot Manager	22
	(Facultatif) Ajout de l'extension Snapshot Manager	22
	Gestion des groupes cloud intelligents	22
	Création d'un groupe cloud intelligent	23
	Suppression d'un groupe cloud intelligent	27
	Protection des biens ou des groupes cloud intelligents	27
	Personnalisation ou modification de biens cloud ou de groupes cloud intelligents	30
	Suppression de la protection de biens cloud ou de groupes intelligents	30
	Nettoyage des biens cloud	31
	Filtrage des biens cloud	32
	Prise en charge des services cloud AWS et Azure Government	34
	À propos de la protection des ressources Microsoft Azure au moyen de groupes de ressources	35
	Avant de commencer	36
	Restrictions et remarques	36
	À propos des configurations et des résultats des groupes de ressources	37
	Dépannage des autorisations de groupe de ressources	41
	À propos de l'accélérateur NetBackup pour les charges de travail cloud	42
	Fonctionnement de l'accélérateur NetBackup avec des machines virtuelles	42

Réanalyse forcée par l'accélérateur pour les machines virtuelles (attribut de planification)	43
Sauvegardes de l'accélérateur et catalogue NetBackup	44
Messages d'accélérateur dans le journal Détails du travail de sauvegarde	44
Configuration de la planification de sauvegarde pour les charges de travail cloud	45
Options de sauvegarde des charges de travail cloud	48
Réplication de snapshot	52
Configuration de la réplication de snapshot AWS	53
Utilisation d'une réplication de snapshot AWS	55
Matrice de prise en charge pour la réplication de compte	58
Protéger des applications sur le cloud avec les snapshots cohérents au niveau des applications	59
Protection des objets PaaS	61
Conditions préalables pour la protection des biens PaaS	61
Installation des utilitaires client natifs	62
Configuration du serveur de stockage pour l'accès instantané	67
Limitations et remarques	67
Découverte des biens PaaS	70
Affichage des biens PaaS	71
Gestion des informations d'authentification PaaS	72
Affichage du nom des informations d'authentification appliquées à une base de données	72
Ajout d'informations d'authentification à une base de données	72
Ajout de la protection des biens PaaS	74
Réalisation d'une sauvegarde immédiate	75
 Chapitre 2	
Récupération des biens cloud	77
Récupération des biens cloud	77
Restauration des biens cloud	85
Récupération des biens PaaS	85
Récupération de biens PaaS autres que RDS	86
Récupération d'un bien PaaS basé sur RDS	86
Récupération de biens protégés par Azure	87
Récupération d'images dupliquées à partir d'AdvancedDisk	90
 Chapitre 3	
Exécution d'une restauration granulaire	91
À propos de la restauration granulaire	91
Liste des environnements pris en charge	92

Listes des systèmes de fichiers pris en charge	93
Avant de commencer	94
Limitations et remarques	95
Restauration de fichiers et de dossiers à partir de machines virtuelles cloud	98
Restauration de volumes sur des machines virtuelles cloud	100
Dépannage	101

Chapitre 4

Résolution des problèmes liés à la protection et à la récupération des biens dans le cloud	103
Résolution des problèmes de protection de la charge de travail cloud	103
Résolution des problèmes de protection et de récupération de charge de travail PaaS	108

Gestion et protection des biens dans le cloud

Ce chapitre traite des sujets suivants :

- À propos de la protection des biens cloud
- Restrictions et remarques
- Configuration de Snapshot Managers dans NetBackup
- Gestion des groupes cloud intelligents
- Protection des biens ou des groupes cloud intelligents
- Nettoyage des biens cloud
- Filtrage des biens cloud
- Prise en charge des services cloud AWS et Azure Government
- À propos de la protection des ressources Microsoft Azure au moyen de groupes de ressources
- À propos de l'accélérateur NetBackup pour les charges de travail cloud
- Configuration de la planification de sauvegarde pour les charges de travail cloud
- Options de sauvegarde des charges de travail cloud
- Réplication de snapshot
- Configuration de la réplication de snapshot AWS
- Utilisation d'une réplication de snapshot AWS
- Matrice de prise en charge pour la réplication de compte

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

À propos de la protection des biens cloud

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

Le tableau suivant décrit les tâches correspondantes.

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

Tâche	Description
Avant de commencer, assurez-vous que vous disposez des autorisations appropriées.	<p>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.</p> <p>Consultez le Guide de l'administrateur de l'interface utilisateur Web NetBackup.</p> <p>Remarque : pour la gestion des applications hébergées, vous devez disposer des autorisations de gestion des biens et de gestion des plans de protection.</p>
Déployer Snapshot Manager	<p>Installez Snapshot Manager dans votre environnement.</p> <p>Se reporter à "Ajout de Snapshot Manager" à la page 14.</p> <p>Consultez les limites de Snapshot Manager et NetBackup.</p> <p>Se reporter à "Restrictions et remarques" à la page 10.</p>
	<p>Enregistrez le Snapshot Manager dans NetBackup.</p> <p>Consultez le <i>Guide de l'administrateur de NetBackup Snapshot Client</i>.</p>

Tâche	Description
Ajout d'une configuration	<p>Tous les fournisseurs cloud pris en charge sont affichés dans l'interface utilisateur Web.</p> <p>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.</p> <p>Se reporter à "Ajout d'un fournisseur cloud pour Snapshot Manager" à la page 15.</p> <p>Pour Amazon, vous pouvez choisir d'utiliser le rôle IAM.</p> <p>Se reporter à "Rôle IAM pour la configuration AWS" à la page 18.</p>
Découverte de biens	<p>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.</p> <p>Par défaut, la découverte de biens a lieu toutes les 2 heures et est configurable.</p> <p>Pour les applications, vous pouvez définir un intervalle de découverte compris entre 15 et 45 minutes.</p> <p>Se reporter à "Découverte de biens sur Snapshot Manager" à la page 20.</p>
Créer un plan de protection	<p>Permet de créer un plan de protection. Un plan de protection sert à planifier les fenêtres de démarrage des sauvegardes.</p> <p>Consultez le Guide de l'administrateur de l'interface utilisateur Web NetBackup.</p> <p>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 53.</p>

Tâche	Description
Choisir de protéger une machine virtuelle, une application ou un volume	<p>Pour chaque fournisseur cloud, une liste des biens découverts s'affiche. Ajoutez les biens à un plan de protection.</p> <p>Consultez le Guide de l'administrateur de l'interface utilisateur Web NetBackup.</p> <p>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 59.</p>
Récupérer les biens cloud	<ul style="list-style-type: none"> ■ Vous pouvez récupérer les biens à l'aide des points de récupération. Se reporter à "Récupération des biens cloud" à la page 77. Se reporter à "Récupération des biens cloud" à la page 77. Se reporter à "Restauration des biens cloud" à la page 85. ■ Vous pouvez également restaurer les biens à l'aide de l'utilitaire d'interface de ligne de commande <code>nbcloudrestore</code>. Remarque : N'utilisez pas l'interface de ligne de commande <code>bprestore</code> 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 103.

Restrictions et remarques

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

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

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

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

Configuration de Snapshot Managers dans NetBackup

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

Tenez compte des points importants suivants :

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

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

Le tableau suivant décrit les tâches sous-jacentes.

Tableau 1-2 Configuration des Snapshot Manager

Tâche	Description
Ajout de Snapshot Manager	Pour ajouter Snapshot Manager dans NetBackup, vous devez ajouter les informations d'authentification et valider le certificat du Snapshot Manager. Se reporter à "Ajout de Snapshot Manager" à la page 14.
Ajouter des fournisseurs cloud	Pour découvrir des biens sur le Snapshot Manager, vous devez ajouter les fournisseurs cloud. Se reporter à "Ajout d'un fournisseur cloud pour Snapshot Manager" à la page 15.
Découverte de biens sur Snapshot Manager	Vous pouvez découvrir des biens sur le Snapshot Manager.Se reporter à "Découverte de biens sur Snapshot Manager" à la page 20.
Associer des serveurs de médias	Pour télécharger des snapshots et des workflows de restauration sur un serveur de médias, vous devez associer ce dernier au Snapshot Manager.Se reporter à "Association de serveurs de médias à un Snapshot Manager" à la page 19.

Configurer un certificat d'autorité de certification tierce

Vous pouvez utiliser un certificat auto-signé ou un certificat tiers pour valider votre Snapshot Manager.

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 passer d'un certificat auto-signé à un certificat tiers pour un Snapshot Manager déjà ajouté, mettez à jour la commande `tpconfig`, modifiez l'API du Snapshot Manager ou utilisez l'interface utilisateur Web NetBackup.

Pour configurer le certificat d'une autorité de certification tierce

- 1 Générez le certificat tiers et la clé privée pour votre Snapshot Manager.
- 2 Exécutez le script `/cloudpoint/scripts/cp_certificate_management.sh` pour charger le certificat, la clé et le magasin d'approbation sur le Snapshot Manager.
- 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/openssl/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 statut 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, Snapshot Manager risque de ne pas fonctionner.

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

Ajout de Snapshot Manager

Vous pouvez ajouter Snapshot Manager à l'aide de l'interface utilisateur Web NetBackup. Vous devez fournir les informations d'authentification Snapshot Manager et valider le certificat.

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

Pour ajouter Snapshot Manager

- 1 Dans la partie gauche, cliquez sur **Cloud**.
- 2 Cliquez sur l'onglet **Snapshot Manager**.
- 3 Cliquez sur **Ajouter**.
- 4 Dans le champ **Snapshot Manager**, entrez l'une des informations suivantes :
 - Nom d'hôte ou adresse IP du Snapshot Manager.
Le nom d'hôte ou l'adresse IP doit correspondre à celui spécifié lors de la configuration de Snapshot Manager, pendant l'installation de Snapshot Manager.
 - Si le serveur DNS est configuré, entrez le nom de domaine complet du Snapshot Manager.
- 5 Dans le champ **Port**, entrez le numéro de port du Snapshot Manager.
La valeur par défaut est 443.
- 6 Cliquez sur **Valider**.
- 7 Dans la boîte de dialogue **Valider le certificat**, cliquez sur **Accepter**.
- 8 Entrez les informations d'authentification Snapshot Manager spécifiées lors de l'installation de Snapshot Manager.
- 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. Ce jeton est requis pour la génération de certificats NetBackup sur Snapshot Manager. 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 Snapshot Manager

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

Pour ajouter un fournisseur cloud pour Snapshot Manager

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

5 Entrez les informations requises.

Fournisseur cloud	Paramètre	Description
Microsoft Azure	Type d'informations d'authentification :	principal de service d'application
	ID du locataire	L'ID du répertoire Azure Active Directory dans lequel vous avez créé l'application.
	ID du client	ID de l'application.
	Clé secrète	Clé secrète de l'application.
	Type d'informations d'authentification : System managed identity	Activez l'identité gérée par le système sur l'hôte Snapshot Manager dans Azure. Remarque : Assignez un rôle à l'identité gérée par le système.
	Type d'informations d'authentification :	identité gérée par l'utilisateur
	ID du client	ID de l'identité gérée par l'utilisateur connectée à l'hôte Snapshot Manager.
	<i>Les paramètres suivants s'appliquent à tous les types d'informations d'authentification ci-dessus</i>	
	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.

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

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

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

7 Cliquez sur **Enregistrer**.

Les biens sur les fournisseurs cloud sont découverts automatiquement.

Rôle IAM pour la configuration AWS

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

Se reporter à "[Ajout d'un fournisseur cloud pour Snapshot Manager](#)" à la page 15.

Avant de continuer, vérifiez les points suivants :

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

```
tpconfig -update -snapshot_manager <snapshot manager host>
-snapshot_manager_user_id <snapshot manager user ID>
-manage_workload <workload type> -security_token <security token>
```

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

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

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

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

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

Association de serveurs de médias à un Snapshot Manager

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

Pour associer des serveurs de médias à un Snapshot Manager

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

Découverte de biens sur Snapshot Manager

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

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

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

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

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

Pour découvrir des biens sur Snapshot Manager

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

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

Pour découvrir des biens appartenant à une configuration de fournisseur cloud

- 1 Dans la partie gauche, cliquez sur **Cloud**.
- 2 Cliquez sur l'onglet **Snapshot Manager**.

- 3 Cliquez sur l'adresse IP ou le nom d'hôte du Snapshot Manager dont vous souhaitez afficher les fournisseurs cloud.
- 4 Cliquez sur l'onglet du fournisseur dont vous souhaitez afficher les configurations.
- 5 Dans le menu près du nom de configuration, cliquez sur **Découvrir**.

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

Modification de la fréquence de découverte automatique pour Snapshot Manager

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

`CLOUD_AUTODISCOVERY_INTERVAL` = **nombre de secondes**

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

Modifier un Snapshot Manager

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

Pour modifier un Snapshot Manager

- 1 Dans la partie gauche, cliquez sur **Cloud**.
- 2 Cliquez sur l'onglet **Snapshot Manager**.
- 3 Dans le menu situé en regard du Snapshot Manager, cliquez sur **Modifier**.
 Vous pouvez uniquement modifier les informations d'authentification de Snapshot Manager. 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 Snapshot Manager.
- 6 Cliquez sur **Enregistrer**.

Activation ou désactivation d'un Snapshot Manager

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

Pour activer ou désactiver un Snapshot Manager

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

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

(Facultatif) Ajout de l'extension Snapshot Manager

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

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

Environnements d'extension Snapshot Manager pris en charge :

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

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

Gestion des groupes cloud intelligents

Vous pouvez créer et protéger un groupe dynamique de biens en définissant des groupes de biens cloud intelligents à partir d'un ensemble de filtres appelés « requêtes ». NetBackup sélectionne les machines virtuelles cloud, les applications ou les volumes en fonction de ces requêtes et les ajoute au groupe. Un groupe

intelligent reflète automatiquement les modifications apportées dans l'environnement des biens, ce qui vous évite d'avoir à vérifier manuellement la liste des biens du groupe lorsque des biens sont ajoutés ou supprimés dans l'environnement.

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

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

Création d'un groupe cloud intelligent

Pour créer un groupe cloud intelligent

- 1 Dans la partie gauche, cliquez sur **Cloud**.
- 2 Cliquez sur l'onglet **Groupes intelligents**, puis cliquez sur **+ Ajouter**.
- 3 Entrez un nom et une description pour le groupe.
- 4 Sélectionnez le fournisseur cloud, l'ID de compte et la région.

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

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

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

Se reporter à [la section intitulée « Options de requête pour la création de groupes cloud intelligents »](#) à la page 25.

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 :

The screenshot shows a query builder interface. At the top, 'Asset type' is set to 'Virtual machine' with a radio button. Below it, there's a checkbox 'Include all assets of the selected type'. The main area is a table with columns for 'AND/OR', 'Field', 'Operator', and 'Value'. The first row has 'displayName', 'Contains', and 'CP'. The second row has 'tagname', 'Starts with', and 'eng'. The third row has 'state', '=', and 'running'. There are buttons for '+ Condition' and '+ Sub-query' on the right. At the bottom, there are buttons for 'Cancel', 'Add and Protect', and 'Add'.

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 (référéncés par votre fournisseur cloud) contenant des espaces ou des caractères spéciaux tels que (,), &, \, /, ", [,], {, }, vous ne pourrez plus modifier la requête pour modifier les paramètres. Cela ne vous empêche pas de créer le groupe intelligent et d'y appliquer le plan de protection. Seule la fonctionnalité de modification de requête est concernée par cette limitation.

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

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

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

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

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

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

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

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

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

Options de requête pour la création de groupes cloud intelligents

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

Tableau 1-3 Mots-clés de requête

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

Tableau 1-4 Opérateurs de requête

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

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

Suppression d'un groupe cloud intelligent

Pour supprimer un groupe cloud intelligent

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

Protection des biens ou des groupes cloud intelligents

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

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

section Se reporter à [la section intitulée « Conversion des plans de protection après une mise à niveau vers NetBackup 9.1 »](#) à la page 28..

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**
Pour plus d'informations sur les options de stockage de l'interface utilisateur Web, consultez la section *Configuration du stockage* du [Guide de l'administrateur de l'interface utilisateur Web NetBackup](#).
 - **Options de sauvegarde**
- 5 Cliquez sur **Protéger**.

Option Sauvegarder maintenant pour une protection immédiate

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

1. Sélectionnez un bien cloud ou un groupe intelligent et cliquez sur **Sauvegarder maintenant**.
2. Sélectionnez ensuite le plan de protection à appliquer. Seuls les plans de protection s'appliquant au fournisseur cloud du bien s'affichent.
3. Cliquez sur **Démarrer la sauvegarde**.
Un travail de sauvegarde est déclenché. Vous pouvez en effectuer le suivi sur la page **Moniteur d'activité**.

Pour plus d'informations, consultez le [Guide de l'administrateur de l'interface utilisateur Web NetBackup](#).

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

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

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

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

Scénarios de défaillance

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

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

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

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

Personnalisation ou modification de biens cloud ou de groupes cloud intelligents

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

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

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

Suppression de la protection de biens cloud ou de groupes intelligents

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

Pour supprimer la protection d'un bien cloud

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

Nettoyage des biens cloud

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

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

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

- `CLOUD.CLEANUP_AGE_MINUTES`
- `CLOUD.CLEANUP_FILTER`

Par exemple,

```
/usr/openv/netbackup/bin/nbsetconfig  
nbsetconfig> CLOUD.CLEANUP_AGE_MINUTES = 180  
nbsetconfig> CLOUD.CLEANUP_FILTER = "provider eq 'aws'"  
nbsetconfig>
```

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

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

Filtrage des biens cloud

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

Pour créer un filtre

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

L'option **Créer un filtre** s'affiche.

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

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

- 5 Pour sélectionner uniquement les biens qui répondent à des conditions spécifiques, créez votre propre requête : cliquez sur **+ Condition**.
- 6 Pour ajouter une condition, utilisez les listes déroulantes afin de sélectionner un mot-clé et un opérateur, puis entrez une valeur.

Se reporter à [la section intitulée « Options de requête pour la création de groupes cloud intelligents »](#) à la page 25.

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 :

The screenshot shows a 'Create filter' window. At the top, there's a 'Name' field containing 'aws-cloud-assets' and a 'Description' field with the placeholder 'Enter description'. Below this is a 'Query' section. It features a toggle switch between 'AND' (which is selected) and 'OR'. Underneath, there are two conditions, each with a dropdown for the field name, a dropdown for the operator, and a text input for the value. The first condition is 'Provider' contains 'aws'. The second condition is 'Name' contains 'cloudpoint'. At the bottom right of the query section, there are links '+ Condition' and '+ Sub-query'. At the very bottom of the window are four buttons: 'Cancel', 'Save', 'Save and add another', and 'Save and apply'.

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

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

Options de requête pour créer un filtre

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

Tableau 1-5 Mots-clés de requête

Mot-clé	Description (toutes les valeurs sont sensibles à la casse)
Server type	Type du serveur.
Instance ID	Identifiant de l'instance du bien, selon la sélection du fournisseur cloud.
Instance name	Nom de l'instance du bien, selon la sélection du fournisseur cloud.
Name	Nom affiché du bien.
Provider	Nom du fournisseur cloud du bien.
Region	Nom de la région du fournisseur cloud du bien.

Tableau 1-6 Opérateurs de requête

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

Prise en charge des services cloud AWS et Azure Government

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

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

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

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

Fournisseur cloud	Régions GovCloud (États-Unis)
Amazon Web Services	<ul style="list-style-type: none"> ■ us-gov-east-1 ■ us-gov-west-1
Microsoft Azure	<ul style="list-style-type: none"> ■ US Gov Arizona ■ US Gov Texas ■ US Gov Virginia

Pour plus d'informations sur la configuration d'AWS et de Microsoft Azure, consultez la section Se reporter à "[Ajout d'un fournisseur cloud pour Snapshot Manager](#)" à la page 15.

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

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

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

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

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

- Si vous ne fournissez pas de préfixe pour un groupe de ressources

- Les groupes de ressources pairs ne sont pas créés
- Vous autorisez la création des snapshots

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

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

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

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

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

Avant de commencer

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

Restrictions et remarques

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

À propos des configurations et des résultats des groupes de ressources

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

Tableau 1-7 Configurations et résultats

Préfixe du groupe de ressources	Case à cocher Protéger les biens même si des groupes de ressources préfixés sont introuvables	Résultat
Non spécifié	Pas sélectionné	NetBackup associe les snapshots récemment créés au groupe de ressources de la ressource.
Spécifié	Pas sélectionné	<p>NetBackup crée des snapshots et les associe au groupe de ressources pair si les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> ■ Le groupe de ressources pair est créé. ■ Le groupe de ressources pair doit appartenir à la même région que le groupe de ressources. <p>Si les conditions ne sont pas remplies, les travaux de snapshot échouent.</p>

Préfixe du groupe de ressources	Case à cocher Protéger les biens même si des groupes de ressources préfixés sont introuvables	Résultat
Spécifié	Sélectionné	<p>NetBackup crée des snapshots et les associe au groupe de ressources pair si les conditions suivantes sont remplies :</p> <ul style="list-style-type: none"> ■ Le groupe de ressources pair est créé. ■ Le groupe de ressources pair doit appartenir à la même région que le groupe de ressources. <p>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.==</p>

Exemples de configurations de groupe de ressources

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

Tableau 1-8 Exemples de configurations

Conditions	Configurations	Résultat
<ul style="list-style-type: none"> ■ 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. 	<ul style="list-style-type: none"> ■ 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. 	<p>Les snapshots sont créés dans le groupe de ressources pair.</p>

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

Conditions	Configurations	Résultat
<ul style="list-style-type: none"> ■ 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. 	<ul style="list-style-type: none"> ■ 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.
<ul style="list-style-type: none"> ■ 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. 	<ul style="list-style-type: none"> ■ 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.
<ul style="list-style-type: none"> ■ Le système d'exploitation et tous les disques appartiennent au même groupe de ressources. ■ Le groupe de ressources pair n'est pas créé. 	<ul style="list-style-type: none"> ■ 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.

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

Conditions	Configurations	Résultat
<ul style="list-style-type: none"> ■ 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. 	<ul style="list-style-type: none"> ■ 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.
<ul style="list-style-type: none"> ■ 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. 	<ul style="list-style-type: none"> ■ 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.
<ul style="list-style-type: none"> ■ Le système d'exploitation et tous les disques appartiennent au même groupe de ressources. ■ Le groupe de ressources pair n'est pas créé. 	<ul style="list-style-type: none"> ■ 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
<ul style="list-style-type: none"> ■ 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. 	<ul style="list-style-type: none"> ■ La valeur du préfixe du groupe de ressources est fournie. ■ La case à cocher Protéger les biens même si des groupes de ressources préfixés sont introuvables n'est pas sélectionnée. 	Les snapshots ne sont pas créés et le travail échoue.

Dépannage des autorisations de groupe de ressources

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

Solution de contournement :

Pour résoudre ce problème, procédez comme suit :

1. Accédez à <https://portal.azure.com/#blade/HubsExtension/BrowseResourceGroups>.
2. Cliquez sur le groupe de ressources à utiliser dans le snapshot.
3. Cliquez sur **Contrôle d'accès (IAM)**.
4. Cliquez sur **Ajouter un rôle**.
5. Sélectionnez **Role as Owner** et **Assign Access to as User**, puis sélectionnez l'**application (créée pour Snapshot Manager pour les appels d'API)**.
6. Enregistrez et relancez la sauvegarde.

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

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

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

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

L'accélérateur présente les avantages suivants :

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

Fonctionnement de l'accélérateur NetBackup avec des machines virtuelles

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

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

- Si la machine virtuelle n'a aucune sauvegarde précédente, NetBackup effectue une sauvegarde complète.

- Lors de la prochaine sauvegarde, NetBackup identifie les données ayant été modifiées depuis la sauvegarde précédente. Seuls les blocs modifiés et les informations d'en-tête sont inclus dans la sauvegarde pour créer une sauvegarde de machine virtuelle complète. Les blocs modifiés sont identifiés en comparant le snapshot de référence précédent et le snapshot actuel. Si vous sélectionnez l'option **Conserver la sauvegarde uniquement** ou **Lancer la sauvegarde si le snapshot est sur le point d'expirer** dans le plan de protection, le snapshot est conservé pour l'accélérateur jusqu'à ce que la sauvegarde suivante soit terminée.
- L'hôte de sauvegarde envoie au serveur de médias un flux de sauvegarde TAR qui comprend ce qui suit : les blocs modifiés de la machine virtuelle, ainsi que l'ID et les zones de stockage de la sauvegarde précédente (décalage et taille de bloc) des blocs inchangés.
- Le serveur de médias lit les blocs modifiés de la machine virtuelle, l'ID de sauvegarde et les informations relatives aux zones de stockage des blocs inchangés. À 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 :

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

Par exemple, `bpbbackup -i -p`

```
msdp_10mins_FRS+5d990ab5-f791-474f-885a-ae0c30f31c98 -s ForcedRescan
```

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

Sauvegardes de l'accélérateur et catalogue NetBackup

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

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

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

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

..

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

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

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

..

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

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

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

Vous pouvez ajouter une planification de sauvegarde dans l'onglet Attributs de la boîte de dialogue Ajouter une planification de sauvegarde lors de la création d'un plan de protection pour les charges de travail cloud Azure, Azure Stack, AWS et GCP.

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

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

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

- 3 Sélectionnez un **fournisseur cloud** dans la liste déroulante et cliquez sur **Suivant**. Dans **Planifications**, cliquez sur **Ajouter une planification**.
 Dans l'onglet **Ajouter une planification de sauvegarde**, vous pouvez configurer les options de conservation de la sauvegarde et du snapshot.
- 4 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 53.
- Sélectionnez **Activer la réplication de snapshot**.
- Dans le tableau, sélectionnez **Région**, **Compte AWS** et **Période de conservation** pour les snapshots répliqués.

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

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

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 Snapshot Manager. L'indexation reposant sur VxMS est actuellement prise en charge pour les clouds GCP, AWS, Azure et Azure Stack Hub.
- L'indexation a lieu pendant les travaux de sauvegarde ou de snapshot réels, mais vous ne pouvez exécuter la récupération de fichiers ou de dossiers individuels uniquement qu'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 du connecteur cloud sont disponibles dans le dossier `/cloudpoint/openv/dm/datamover.<datamover-id>/netbackup/logs` du Snapshot Manager.

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

Options de sauvegarde des charges de travail cloud

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

Snapshots régionaux pour Google Cloud

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

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

Create protection plan

Basic properties — Schedules — **3 Backup options** — 4 Permissions — 5 Review

Backup options

☐ Enable granular recovery for files or folders

☒ Enable regional snapshot

Cancel Previous Next

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

Create protection plan

Basic properties — Schedules — Storage options — **4 Backup options** — 5 Permissions — 6 Review

Backup options

☐ Enable granular recovery for files or folders
☒ Specify snapshot destination resource group

Configuration name *
 azurecloudplugin

Fetching subscription and resource group details may take some time depending upon the network connectivity.

Subscription name or ID *
 xxxxxxxx (a332d749-xxxxxx-xxxxxx-xxxxxx-xxxxxx)

Resource group	Region	
azure-scale-rhel83-mongo-dnd	eastus2	Select

Cancel Previous Next

Exclusion des disques sélectionnés de la sauvegarde

Vous pouvez configurer un plan de protection de façon à exclure certains disques de la sauvegarde et du snapshot qui s'appliquent à tous les fournisseurs cloud pris en charge, y compris GCP. Vous évitez ainsi les images redondantes des disques qui n'ont pas besoin d'être sauvegardés et accélérez les sauvegardes en réduisant le volume de données à traiter.

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



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

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

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

Remarques :

- Dans le cas de LVM, si des disques sont partiellement exclus, le système peut ne pas démarrer correctement.
- Lorsqu'un système de fichiers non pris en charge est configuré sur un disque et que l'utilisateur souhaite exclure ce disque du snapshot, un snapshot de blocage cohérent est créé.
- Si l'utilisateur souhaite exclure ce disque, l'indicateur **nofail** doit être associé au disque de données avant la prise d'un snapshot dans le fichier `/etc/fstab`. Cette opération est requise si l'utilisateur redémarre l'instance sans ce volume (par exemple, après avoir déplacé le volume vers une autre instance). L'option de montage **nofail** permet à l'instance de démarrer même en cas d'erreur lors du montage du volume. Pour plus d'informations, consultez l'exemple d'entrée suivant dans le fichier `/etc/fstab` :
Par exemple, **UUID=aebf131c-6957-451e-8d34-ec978d9581ae /data xfs defaults,nofail 0 2**
- L'utilisateur doit s'assurer que les biens sont découverts correctement une fois que leurs étiquettes ont été modifiées par le fournisseur cloud. Une fois que l'exécution de la politique est planifiée pour un bien, les disques sont exclus en fonction des données découvertes uniquement. Si l'utilisateur connecte une

étiquette alors que le snapshot est en cours, cette **étiquette** ne sera pas prise en compte dans l'exclusion. L'étiquette sera prise en compte lors du cycle de protection suivant une fois la découverte terminée.

- Dans le cas d'un système d'exploitation dont les paramètres régionaux ne sont pas définis sur l'anglais, si l'utilisateur opte pour l'exclusion basée sur une étiquette dans le plan de protection et si l'étiquette de disque comporte un caractère non anglais, l'exclusion de disque fonctionnera comme prévu. Cependant, dans certains cas, les étiquettes comportant un caractère non anglais ne sont pas correctement capturées dans les journaux job(try) et les journaux d'audit, bien qu'aucune fonctionnalité ne soit affectée, car l'exclusion de disque est correctement prise en compte.

Réplication de snapshot

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

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

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

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

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

Configuration de la réplication de snapshot AWS

Conditions requises pour la réplication de snapshots

■ Réplication de snapshots non chiffrés

Assurez-vous que les comptes/régions sources et cibles sont configurés à l'aide du fournisseur cloud AWS dans NetBackup Snapshot Manager. Aucune autre condition n'est requise pour la réplication de snapshots non chiffrés.

■ Réplication de snapshots chiffrés à l'aide d'AWS KMS

Assurez-vous que les comptes/régions sources et cibles sont configurés à l'aide du fournisseur cloud AWS dans NetBackup Snapshot Manager.

En outre, pour répliquer des snapshots chiffrés sur un compte croisé, la clé de chiffrement CMK de l'emplacement d'origine doit être partagée avec le compte cible. (Cette clé KMS partagée est implicitement utilisée lors de la copie du snapshot vers le compte cible et le snapshot copié peut être répliqué à l'aide d'une clé différente).

Les emplacements source et cible doivent disposer d'une clé de chiffrement (clé KMS) du même nom, c'est-à-dire qu'ils doivent disposer du même alias de clé (AWS).

Si la clé de chiffrement portant le même nom n'est pas présente sur la cible, le snapshot répliqué est chiffré à l'aide de la clé KMS par défaut dans l'emplacement cible.

■ Autorisations de réplication sur un compte croisé

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

- `ModifySnapshotAttribute` et `CopySnapshot` sur l'instance EC2.
- `DescribeKey` et `ReEncrypt` sur la clé KMS utilisée pour le chiffrement du snapshot d'origine.

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

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

Vous pouvez choisir de répliquer des snapshots de biens cloud AWS de l'emplacement principal vers un emplacement secondaire ou distant. Les Snapshot

Managers prennent en charge la réplication entre régions et entre comptes. La réplication de snapshot vous permet d'effectuer les actions suivantes :

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

Configuration

Consultez les informations suivantes pour configurer la réplication de snapshot :

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

Remarques

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

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

Critères de protection de bien

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

- Les biens doivent être ajoutés à un plan de protection qui réplique des snapshots sur une région différente.
Par exemple, les biens résidant dans la région « aws_account_1-us-east-1 » ne peuvent pas être abonnés à un plan de protection répliquant sur la même région « aws_account_1-us-east-1 ».
- Les biens peuvent être répliqués sur un autre compte dans la même région.
Par exemple, les biens résidant dans la région « aws_account_1-us-east-1 » peuvent être abonnés à un plan de protection répliquant sur la même région, mais sur un autre compte « aws_account_2-us-east-1 ».

- Les biens découverts par un Snapshot Manager doivent être répliqués vers la région découverte par ce Snapshot Manager.
Par exemple, les biens découverts par le Snapshot Manager 'CP1' ne peuvent pas être abonnés à un plan de protection qui effectue la réplication vers une région découverte par le Snapshot Manager 'CP2'.
- Seuls les biens Amazon peuvent être abonnés à un plan de protection configuré pour la réplication de snapshot cloud.

Gérer les réplications de snapshot simultanées

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

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

```
MAX_CLOUD_SNAPSHOT_REPLICATION_JOBS_PER_DESTINATION
```

La valeur par défaut est 5.

Utilisation d'une réplication de snapshot AWS

Cette section explique comment créer des répliques de snapshots à l'aide de la fonction de réplication de snapshot AWS et restaurer les snapshots répliqués chaque fois que nécessaire. Sauf indication contraire, consultez le *Guide d'installation et de mise à niveau de NetBackup™ Snapshot Manager* et le *Guide de l'administrateur de l'interface utilisateur Web NetBackup* pour en savoir plus sur ces étapes.

Création de réplications de snapshot

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

Pour créer des répliques

- 1 Ajoutez Snapshot Manager (CP1) dans l'interface utilisateur Web. Se reporter à ["Ajout de Snapshot Manager"](#) à la page 14.
- 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 45.

- 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 de fichiers ou de dossiers individuels à partir d'une réplique découverte par un autre Snapshot Manager dans une région ayant basculé.

Restauration dans la région cible

- 1 Désactivez le serveur CP1 dans la région source à partir de l'interface utilisateur Web. Se reporter à ["Activation ou désactivation d'un Snapshot Manager"](#) à la page 22.
- 2 Enregistrez un nouveau Snapshot Manager (CP2) dans la région cible à partir de l'interface utilisateur Web.
- 3 Ajoutez le plug-in AWS pour la région et le compte cibles uniquement. Laissez la découverte se terminer.
- 4 Pour restaurer des machines virtuelles :
 - 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 77.

- 5 Ajoutez le groupe de sécurité approprié aux machines virtuelles restaurées pour activer l'accès à distance.
- 6 Désinstallez et réinstallez l'agent Snapshot Manager des machines virtuelles restaurées, puis enregistrez les agents Snapshot Manager auprès du nouveau serveur CP2.
- 7 Exécutez une découverte approfondie à partir de la console du fournisseur AWS.
- 8 Créez un plan de protection pour protéger les machines virtuelles restaurées. 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 ["Activation ou désactivation d'un Snapshot Manager"](#) 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 Snapshot Manager des machines virtuelles restaurées, puis enregistrez les agents Snapshot Manager auprès du serveur CP1.
- 9 Exécutez une découverte détaillée à partir de la console AWS.
- 10 Utilisez le plan de protection existant pour protéger les nouvelles machines virtuelles restaurées.

Matrice de prise en charge pour la réplication de compte

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

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

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

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

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

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

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

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

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

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

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

Avant de commencer

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

Pour configurer des applications pour la récupération spécifique

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

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

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

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

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

Protection des objets PaaS

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

Conditions préalables pour la protection des biens PaaS

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

Fournisseurs cloud pris en charge

NetBackup prend en charge les fournisseurs cloud suivants :

- Microsoft Azure
- AWS
- GCP

Bases de données prises en charge pour différents fournisseurs

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

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

Fournisseurs	Bases de données prises en charge
Microsoft Azure	PostgreSQL, instance gérée par SQL, SQL, MariaDB et MySQL. Les composants suivants ne sont pas pris en charge : Azure SQL : pool Elastic Instance gérée par Azure SQL - Azure Arc Azure PostgreSQL : groupe de serveurs Hyperscale (Citus) et Hyperscale PostgreSQL compatible Azure Arc
AWS	RDS SQL, RDS PostgreSQL, RDS MySQL, RDS MariaDB, RDS Aurora MySQL, RDS Aurora PostgreSQL et DynamoDB.
GCP	Cloud SQL for PostgreSQL et Cloud SQL for MySQL

Plates-formes prises en charge

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

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

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

Installation des utilitaires client natifs

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

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

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

Installation de l'utilitaire client MySQL

Remarque : La version recommandée de l'utilitaire client MySQL est 8.0.25.

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

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

```
1 rpm -ivh mysql-community-common-<version_no>.x86_64.rpm
2 rpm -ivh mysql-community-client-plugins- <version_no>.x86_64.rpm
3 rpm -ivh mysql-community-libs- <version_no>.x86_64.rpm
4 rpm -ivh mysql-community-libs-compat- <version_no>.x86_64.rpm
5 rpm -ivh mysql-community-client- <version_no>.x86_64.rpm
```

Remarque : L'utilitaire client MySQL version 8.0.27 peut présenter un problème de connectivité.

Dans NetBackup déployé dans des environnements AKS et EKS, effectuez les étapes suivantes pour que la sauvegarde et la restauration de la base de données MySQL fonctionnent :

- 1 Créez la structure de dossiers comme indiqué. Conservez tous les noms de dossier en minuscules.

```
nbshared
└─ mysql
```

Videz le fichier `mysql` 4 rpm dans le dossier `mysql` :

```
nbshared
└─ mysql
    ├── mysql-community-client-8.0.25-1.el7.x86_64.rpm
    ├── mysql-community-client-plugins-8.0.25-1.el7.x86_64.rpm
    ├── mysql-community-common-8.0.25-1.el7.x86_64.rpm
    └── mysql-community-libs-8.0.25-1.el7.x86_64.rpm
```

- 2 Copiez le dossier `nbshared` dans : `pod principal >kubectl cp <chemin>/nbshared <espace de noms netbackup>/<nom de pod principal>:/mnt/nbdata/nbshared`

Par exemple : `kubectl cp nbshared nb-namespace/nbu-primary-0:/mnt/nbdata/nbshared`

- 3 Vérifiez si le contenu `nbshared` est copié correctement sur le pod principal. Pour cela, exécutez :

```
kubectl exec -it pod/nbu-primary-0 -c nbu-primary -n nb-namespace
-- ls -ltr /mnt/nbdata/nbshared drwxr-xr-x. 2 root root 228 Sep
13 01:42 mysql
```

- 4 À l'aide de la même commande, vérifiez si le dossier `mysql` contient les fichiers RPM requis.

Installation de l'utilitaire client *sqlpackage*

Remarque : La version recommandée pour l'utilitaire client `sqlpackage` est 19.2 (numéro : 16.0.6296.0).

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

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

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

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

- 1 `cd ~`
- 2 `mkdir sqlpackage`
- 3 `unzip ~/Downloads/sqlpackage-linux-<version string>.zip -d ~/sqlpackage`
- 4 `echo "export PATH=\"\$PATH:\$HOME/sqlpackage\""> ~/.bashrc`
- 5 `chmod a+x ~/sqlpackage/sqlpackage`
- 6 `source ~/.bashrc`

Remarque : Vérifiez que `sqlpackage` a été ajouté comme variable de chemin d'accès par défaut.

- 7 `sqlpackage`
- 8 `rpm -ivh unixODBC-2.3.7-1.rh.x86_64.rpm`
- 9 `rpm -ivh msodbcsql17-17.9.1.1-1.x86_64.rpm`

Les utilisateurs de RHEL 9 effectuent les étapes supplémentaires suivantes :

- 1 Téléchargez Microsoft.NETCore.App.Runtime.linux-x64 en cliquant sur le lien :
<https://www.nuget.org/api/v2/package/Microsoft.NETCore.App.Runtime.linux-x64/6.0.10>
Recherchez le fichier :
`microsoft.netcore.app.runtime.linux-x64.6.0.10.nupkg.`
- 2 Extrayez le fichier à l'aide d'un outil de décompression tel que 7zip.

3 Accédez à :

microsoft.netcore.app.runtime.linux-x64.6.0.10.nupkg\runtimes\linux-x64\lib\net6.0\

4 Copiez le fichier `System.Security.Cryptography.X509Certificates.dll` dans le dossier `/sqlpackage` créé à l'étape 2 de la tâche d'installation de l'utilitaire client *sqlpackage*.

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

Pour une configuration BYO NetBackup :

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

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

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

Installation de l'utilitaire client Postgres

Remarque : La version recommandée de l'utilitaire client Postgres est 14.3.

Environnement de test	RHEL 7	https://download.postgresql.org/pub/repos/yum/14/redhat/rhel-7-x86_64/
	RHEL 8	https://download.postgresql.org/pub/repos/yum/14/redhat/rhel-8-x86_64/
	RHEL 9	https://download.postgresql.org/pub/repos/yum/14/redhat/rhel-9-x86_64/

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

- 1 `rpm -ivh postgresql14-libs-14.3-1PGDG.rhel7.x86_64.rpm`
- 2 `rpm -ivh postgresql14-14.3-1PGDG.rhel7.x86_64.rpm`

Remarque : Le package de compression `lz4` et `libc` sont requis par `postgresql14-14.3-1PGDG.rhel8.x86_64.rpm` sur RHEL 8 et 9.

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

Configuration du serveur de stockage pour l'accès instantané

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

- 1 Assurez-vous que NFS et NGINX sont installés.
- 2 La version de NGINX doit être identique à celle de la version officielle de RHEL correspondante. Vous devez l'installer à partir de la source Yum RHEL correspondante (EPEL).
- 3 Vérifiez que les packages `polycoreutils` et `polycoreutils-python` sont installés à partir de la même source Yum RHEL (serveur RHEL). Exécutez les commandes suivantes :

- `semanage port -a -t http_port_t -p tcp 10087`
- `setsebool -P httpd_can_network_connect 1`

- 4 Assurez-vous qu'aucun point de montage direct n'est créé pour le dossier `/mnt` du serveur de stockage. Montez uniquement les points de montage sur leurs sous-dossiers.
- 5 Activez l'autorisation `logrotate` dans `selinux` à l'aide de la commande suivante :

```
semanage permissive -a logrotate_t
```

Limitations et remarques

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

Pour toutes les bases de données

- Les déploiements NetBackup sous Flex Appliance et Flex Scale ne sont pas compatibles avec les charges de travail PaaS.
- Prend en charge uniquement les ports par défaut pour les bases de données de différents fournisseurs. Les instances de charge de travail configurées avec des ports personnalisés ne sont pas prises en charge.
- Les noms de base de données contenant les caractères « # » et « / » ne sont pas pris en charge pour les opérations de sauvegarde et de restauration. En outre, le nom de base de données doit respecter les conventions de nommage suggérées par les fournisseurs de cloud.
- La sauvegarde et la restauration d'une base de données avec des caractères multi-octets ou non latins ne sont pas prises en charge pour un serveur principal fonctionnant sous Windows et un serveur de médias dont le niveau de version est inférieur à 10.1.1.
- Vous pouvez dupliquer l'image de sauvegarde PaaS sur un serveur de stockage pris en charge. Mais avant de lancer une restauration, vous devez dupliquer l'image sur un serveur MSDP avec partage universel activé. Se reporter à ["Récupération d'images dupliquées à partir d'AdvancedDisk"](#) à la page 90.

Pour PostgreSQL

- La restauration des privilèges de sécurité n'est pas prise en charge.
- Pendant la restauration, nous utilisons les options `--no-owner` et `--no-privileges`, et lors de la phase de post-restauration, nous affichons les détails des métadonnées capturées au moment de la sauvegarde en tant que propriétaire/liste de contrôle d'accès dans l'activité de restauration du journal de progression de l'interface utilisateur Web.
- La restauration n'échoue pas si le propriétaire/rôle n'existe pas sur l'emplacement.
- Après la restauration, le rôle de la base de données est associé selon les informations d'authentification fournies dans NetBackup par rapport à l'instance de destination.
- Les utilisateurs doivent modifier l'appartenance des bases de données après la restauration.
- La sauvegarde et la restauration ne sont pas prises en charge si seule la connexion SSL (Secure Sockets Layer) s'applique au niveau du serveur pour la charge de travail PostgreSQL sur GCP.

- La restauration de base de données Azure Postgres d'un serveur unique vers un serveur flexible, ou inversement, n'est pas prise en charge en raison des limitations du fournisseur cloud.
- Les caractères suivants ne sont pas pris en charge dans le nom de base de données dans le workflow de restauration : &, (,), <, >, \, |, /, ;, `, ' et ".
- Le nom d'utilisateur en majuscules n'est pas pris en charge pour les nouveaux utilisateurs ajoutés après la création du serveur PostgreSQL.

Pour AWS DynamoDB

- Pour AWS DynamoDB, vous devez créer un compartiment S3 portant le nom `netbackup-<idcompte>`. NetBackup utilise ce compartiment comme emplacement intermédiaire pour les opérations de sauvegarde.
- Les autres restaurations pour la région et le compte ne sont pas prises en charge.
- La restauration d'images importées à partir d'un autre serveur principal est uniquement prise en charge à l'aide de l'API REST NetBackup.

Pour AWS RDS SQL

-
- Seules les éditions Express et Web d'AWS RDS SQL sont prises en charge.
- Concernant la validation des informations d'authentification, IAM n'est pas pris en charge pour AWS RDS SQL. Vous pouvez utiliser la méthode avec nom d'utilisateur et mot de passe.
- Seul le type de gestion des données **Amazon RDS** est pris en charge. Le type de gestion des données **RDS Custom** n'est pas pris en charge pour les éditions d'instance AWS RDS SQL.

Pour MySQL

- L'opération de restauration requiert des privilèges de superutilisateur si le fichier de vidage contient l'instruction CREATE DEFINER.
- La sauvegarde et la restauration ne sont pas prises en charge si seule la connexion SSL s'applique au niveau du serveur pour la charge de travail MySQL sur GCP.

Pour l'instance gérée par Azure SQL et SQL

- La machine virtuelle Azure utilisée comme serveur de médias doit appartenir au même réseau virtuel (Vnet) que celui d'une instance gérée par Azure. Autrement, si le serveur de médias et l'instance gérée par SQL sont dans un

Vnet différent, les deux réseaux virtuels doivent être configurés comme pairs pour accéder à l'instance de base de données.

- Échec de la sauvegarde lorsqu'un Readlock est placé sur la base de données ou le groupe de ressources.
- La sauvegarde est partiellement réussie lorsqu'un Deletelock est placé sur la base de données ou le groupe de ressources. L'entrée obsolète tempdb n'est pas supprimée du portail cloud Azure. Vous devez la supprimer manuellement.

Découverte des biens PaaS

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

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

Pour découvrir des biens PaaS :

- 1 Ajoutez Snapshot Manager. Se reporter à ["Ajout de Snapshot Manager"](#) à la page 14.
- 2 Ajoutez Microsoft Azure, GCP ou AWS en tant que fournisseur. Se reporter à ["Ajout d'un fournisseur cloud pour Snapshot Manager"](#) à la page 15.
- 3 Exécutez une découverte. Se reporter à ["Découverte de biens sur Snapshot Manager"](#) à la page 20.

Une fois la découverte terminée, vous pouvez trouver tous les biens Azure PostgreSQL, SQL Managed Instance, SQL, MySQL et GCP Cloud SQL for PostgreSQL, Cloud SQL for MySQL ou AWS Oracle dans l'onglet **PaaS**, dans la charge de travail **Cloud**.

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

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

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

Affichage des biens PaaS

Pour afficher les biens PaaS :

- 1 Dans la partie gauche, cliquez sur **Cloud**, dans la section **Charges de travail**.
- 2 Dans l'onglet **PaaS**, seuls les biens qui sont disponibles pour vous s'affichent. Les biens RDS s'affichent dans l'onglet **Applications**.

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

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

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

Gestion des informations d'authentification PaaS

Vous pouvez ajouter des informations d'authentification à une base de données figurant dans les onglets **PaaS** et **Applications** sous la section de la charge de travail **cloud**. Vous pouvez ajouter, modifier ou supprimer les informations d'authentification PaaS depuis la console centrale **Gestion des informations d'authentification** de NetBackup.

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

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

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

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

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

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

Pour ajouter ou modifier des informations d'authentification

- 1 Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
Dans l'onglet **PaaS**, seuls les biens auxquels vous avez accès s'affichent. Les biens RDS s'affichent dans l'onglet **Applications**.
- 2 Sélectionnez la base de données dans le tableau, puis cliquez sur **Gérer les informations d'authentification**.
- 3 Sélectionnez un **Hôte de validation**. L'hôte de validation doit être le serveur de médias RHEL assurant la connectivité avec la charge de travail PaaS.

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

- Pour sélectionner les informations d'authentification existantes du compte, sélectionnez l'option **Sélectionner parmi les informations**

d'authentification existantes, sélectionnez les informations d'authentification requises dans le tableau ci-dessous et cliquez sur **Suivant**.

- Pour ajouter de nouvelles informations d'authentification au compte, sélectionnez **Ajouter des informations d'authentification** et cliquez sur **Suivant**. Entrez le **Nom des informations d'authentification**, la **Balise** et une **Description** pour les nouvelles informations d'authentification. Dans la section **Informations d'authentification du service** :
 - Sélectionnez **Authentification de base de données IAM** pour les biens Amazon RDS uniquement et spécifiez le **Nom d'utilisateur de la base de données**.
Se reporter à ["Création d'un nom d'utilisateur de base de données IAM"](#) à la page 74.

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

- Sélectionnez **Authentification par mot de passe** et spécifiez le nom d'utilisateur et le mot de passe du serveur de base de données. Cliquez sur **Suivant**.
- Ajoutez un rôle pour lequel vous souhaitez autoriser l'accès aux informations d'authentification. Pour ajouter de nouvelles autorisations à un rôle :
 - Cliquez sur **Ajouter**.
 - Sélectionnez un rôle.
 - Sélectionnez les autorisations que vous souhaitez accorder au rôle sur la base de ses informations d'authentification.
 - Cliquez sur **Enregistrer**.

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

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

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

Pour créer un nom d'utilisateur IAM :

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

Ajout de la protection des biens PaaS

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

Pour protéger des biens PaaS

- 1 Dans la partie gauche, cliquez sur **Charges de travail > Cloud**.
- 2 Pour protéger les biens PostgreSQL RDS AWS ou MySQL RDS, cliquez sur l'onglet **Applications**. Pour les autres biens PaaS, cliquez sur l'onglet **PaaS**.

- 3 Vérifiez si le bien à protéger dispose d'informations d'authentification.
Se reporter à ["Affichage du nom des informations d'authentification appliquées à une base de données"](#) à la page 72.
Si la colonne **Nom des informations d'authentification** est vide, vous devez assigner des informations d'authentification au bien.
Se reporter à ["Ajout d'informations d'authentification à une base de données"](#) à la page 72.
- 4 Pour protéger un bien, sélectionnez le bien, puis cliquez sur **Ajouter la protection**.
Un bien doit disposer d'informations d'authentification pour la plupart des opérations. Par exemple, vous souhaitez assigner le bien à un plan de protection ou effectuer une sauvegarde immédiatement.
- 5 Sélectionnez un plan de protection, puis cliquez sur **Suivant**.
- 6 Vérifiez les paramètres de configuration et cliquez sur **Protéger**.

Réalisation d'une sauvegarde immédiate

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

Pour effectuer une sauvegarde immédiate

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

Pour sauvegarder les biens AWS RDS PostgreSQL ou RDS MySQL, cliquez sur l'onglet **Applications**. Pour les autres biens PaaS, cliquez sur l'onglet **PaaS**.

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

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

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

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

Récupération des biens cloud

Ce chapitre traite des sujets suivants :

- [Récupération des biens cloud](#)
- [Restauration des biens cloud](#)
- [Récupération des biens PaaS](#)

Récupération des biens cloud

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

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

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

À propos de la vérification de prérécupération pour les machines virtuelles

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

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

Paramètres pris en charge pour la restauration de biens cloud

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

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

Paramètres	Copie de snapshot			Copie de sauvegarde		
	Azure	Azure Stack	GCP et AWS	Azure	Azure Stack	GCP et AWS
Modifier le nom affiché de la machine virtuelle	O	O	O	O	O	O
Modifier l'état d'alimentation de la machine virtuelle	O	O	O	O	O	O

Supprimer les associations d'étiquettes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Restaurer sur un autre réseau	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
ID de l'abonnement				<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Modifier le groupe de ressources	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	
Modifier la région de la machine virtuelle				<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Modifier la configuration du fournisseur				<input type="radio"/>	<input type="radio"/>	
Modifier le groupe de ressources pour les disques	<input type="radio"/>	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>	
Zone	<input type="radio"/>		<input type="radio"/>	<input type="radio"/>		<input type="radio"/>
Groupe de sécurité/Règle de pare-feu/Groupe de sécurité réseau	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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 :

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

Dans la section **Avancé** :

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

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

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

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

- 11** Cliquez sur **Lancer la récupération**.

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

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

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

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

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

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

- 1** Dans la partie gauche, cliquez sur **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 GCP avec des volumes en lecture seule.

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

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

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

Les biens PaaS sont répertoriés sous la charge de travail **Cloud**. Vous pouvez restaurer des biens AWS RDS PostgreSQL, RDS MySQL et RDS SQL Server à partir de l'onglet **Applications**, et tous les autres biens PaaS à partir de l'onglet **PaaS**. Le workflow de récupération des biens Azure varie selon que ces biens sont protégés par NetBackup ou par Azure.

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

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

séparées par des virgules. Par exemple : MEDIA_SERVER_POD_CIDR=10.0.0.0/8, 10.0.0.0/16

Récupération de biens PaaS autres que RDS

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

Pour restaurer des biens PaaS autres que RDS

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

Les points de récupération disponibles s'affichent dans le tableau.

- 3 Cliquez sur **Récupérer** dans la ligne de l'image que vous voulez récupérer.
- 4 Le champ **Nom** affiche le nom d'origine du bien par défaut. Vous pouvez modifier le nom dans ce champ. Il est possible que ce nom ne puisse plus être modifié par la suite.
- 5 (Facultatif) Dans le champ **Instance cible**, l'instance source du bien est sélectionnée par défaut. Pour effectuer la restauration dans une autre instance, sélectionnez l'instance requise. Cliquez sur **Lancer la récupération**.

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

L'**Instance cible** n'est pas disponible pour les biens DynamoDB.

Récupération d'un bien PaaS basé sur RDS

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

Pour restaurer les biens PaaS basés sur RDS :

- 1 Dans la partie gauche, cliquez sur **Cloud**, dans la section **Charges de travail**, et cliquez sur l'onglet **Applications**. Cliquez sur le nom du bien à récupérer.
- 2 Cliquez sur l'onglet **Points de récupération**, dans le calendrier, sélectionnez la date pour laquelle vous voulez afficher les points de récupération.

Les points de récupération disponibles s'affichent à droite.

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

- 4 Dans la section **Bases de données source**, sélectionnez les bases de données que vous voulez restaurer. Cliquez sur **Ajouter une base de données**, dans la boîte de dialogue **Ajouter une base de données**, sélectionnez les bases de données requises, puis cliquez sur **Sélectionner**.
- 5 Entrez un préfixe à ajouter aux bases de données restaurées ou utilisez le paramètre par défaut. Ce champ doit avoir une valeur.
- 6 (Facultatif) Dans le champ **Instance cible**, l'instance source du bien est sélectionnée par défaut. Pour effectuer la restauration dans une autre instance, sélectionnez l'instance requise. Cliquez sur **Lancer la récupération**.

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

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

Récupération de biens protégés par Azure

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

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

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

Pour récupérer des biens de sauvegarde à un moment donné :

- 1 Dans la partie gauche, cliquez sur **Cloud**.
- 2 Cliquez sur l'onglet **PaaS**.
Tous les biens PaaS découverts s'affichent.
- 3 Dans la section **Type de points de récupération**, sélectionnez **Protégé par le fournisseur**.
- 4 Cliquez sur **Restaurer** dans la ligne de la base de donnée Azure MySQL et du bien de base de données géré par Azure SQL protégés que vous voulez récupérer.
- 5 Dans l'onglet **Points de récupération**, sous **Sauvegarde à un moment donné**, cliquez sur **Restaurer**.

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

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

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

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

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

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

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

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

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

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

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

- 1 Dans la partie gauche, cliquez sur **Cloud**.
- 2 Cliquez sur l'onglet **PaaS**.
Tous les biens PaaS découverts s'affichent.
- 3 Cliquez sur **Restaurer** dans la ligne du bien protégé que vous voulez récupérer.
- 4 Dans l'onglet **Points de récupération**, sous **Sauvegarde de conservation à long terme**, cliquez sur **Restaurer** en fonction de l'image à restaurer.
- 5 Pour les bases de données Azure SQL, vous pouvez entrer un nom pour la base de données restaurée dans le champ **Nom de base de données**. Les noms de base de données ne peuvent pas comporter de caractères spéciaux comme < > * % & : \ / et ? ou des caractères de commande. Ne terminez pas le nom par un point ou une espace. Pour en savoir plus sur les règles de nommage des ressources Azure, consultez la page <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-name-rules#microsoftsql>

Si vous n'entrez pas de nom, NetBackup assigne automatiquement un nom au format *restore_<nomBd>*.
- 6 Vous disposez d'une option permettant d'entrer le nom de l'instance dans le champ **Instance gérée** pour les bases de données gérées avec Azure SQL. Le nom d'instance du point de récupération s'affiche par défaut. Vous pouvez également rechercher le nom de l'instance gérée à l'aide de l'option Rechercher. Vous pouvez effectuer une restauration dans la même région que celle à laquelle appartient votre abonnement.
- 7 Cliquez sur **Suivant**. Une fois la vérification de pré-récupération terminée, cliquez sur **Démarrer la récupération**.

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

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

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

Récupération d'images dupliquées à partir d'AdvancedDisk

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

Conditions requises :

1. Pour AdvanceDisk, le serveur de médias associé au serveur MSDP doit avoir la version 10.1 ou une version ultérieure.
2. Pour le stockage en cloud MSDP, la version du serveur de médias utilisée pour la récupération doit être 10.1.1.
3. Vérifiez que la directive ushare est définie et configurée sur le serveur MSDP.
4. Créez un partage universel sur ce serveur de stockage MSDP. Assurez-vous d'ajouter le nom d'hôte/l'adresse IP du serveur de médias correspondant dans la liste d'exportation de la directive ushare.

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

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

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

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

Pour lancer un travail de restauration, Se reporter à "[Récupération des biens PaaS](#)" à la page 85.

Pour la restauration à l'aide de l'API REST, consultez la section :

`récupération/charges de travail/cloud/scénarios/bien/récupération.`

Consultez la documentation des API NetBackup.

Remarque : Pour la récupération d'instance RDS, NetBackup n'affiche aucun message d'erreur ou d'avertissement, si vous lancez la restauration à partir d'une image de sauvegarde résidant sur le stockage AdvanceDisk.

Exécution d'une restauration granulaire

Ce chapitre traite des sujets suivants :

- [À propos de la restauration granulaire](#)
- [Liste des environnements pris en charge](#)
- [Listes des systèmes de fichiers pris en charge](#)
- [Avant de commencer](#)
- [Limitations et remarques](#)
- [Restauration de fichiers et de dossiers à partir de machines virtuelles cloud](#)
- [Restauration de volumes sur des machines virtuelles cloud](#)
- [Dépannage](#)

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 3-1 Tâches de restauration granulaire

Tâche	Description
Connecter des machines virtuelles	Permet de connecter les machines virtuelles que vous voulez utiliser pour effectuer une restauration granulaire.
Découvrir les biens sur la machine virtuelle	Permet d'utiliser l'option Découvrir . Accédez à Cloud > Snapshot Managers > Snapshot Manager > Actions > Découvrir .
Créer un plan de protection	Permet de créer un plan de protection. Assurez-vous que la case à cocher Activer la restauration granulaire pour les fichiers ou les dossiers est sélectionnée dans les Options de sauvegarde du plan de protection.
Abonner les biens découverts au plan de protection	Ajoutez les biens sur les machines virtuelles connectées à l'étape précédente au plan de protection dont la restauration granulaire inclut l'attribut indexable.
Exécuter le plan de protection	Permet de planifier un travail de sauvegarde et une opération d'indexation ou d'utiliser l'option Sauvegarder maintenant . Le travail de sauvegarde démarre immédiatement.
Restaurer un fichier ou un dossier, 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 3-2 Versions prises en charge

Application	Version
NetBackup	10.1.1
Système d'exploitation de l'hôte de sauvegarde NetBackup	RHEL 7.x et 8.x

Application	Version
Système d'exploitation de l'hôte Snapshot Manager	<ul style="list-style-type: none">■ RHEL 7.x et versions ultérieures, RHEL 8.6■ Ubuntu 18.04 LTS et 20.04 LTS <p>Remarque : La version du système d'exploitation (Ubuntu 20.04 LTS) répertoriée dans l'interface utilisateur est la version du conteneur.</p>
Fournisseurs cloud	<ul style="list-style-type: none">■ Amazon Web Services■ Microsoft Azure■ Microsoft Azure Stack Hub■ Google Cloud Platform
Snapshot Manager ou type d'instance d'agent	<ul style="list-style-type: none">■ Amazon AWS : t2.large/t3.large■ Microsoft Azure : D2s_V3Standard■ Microsoft Azure Stack Hub : DS2_v2 Standard, DS3_v2 Standard■ Google Cloud Platform : n1.Standard2 et spécifications supérieures
Hôte de l'agent Snapshot Manager à protéger	<ul style="list-style-type: none">■ 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 : Pour Google Cloud Platform, si l'hôte de l'agent s'exécute sur une version 8.x de RHEL, Snapshot Manager doit être installé sur un hôte doté de RHEL 8.x.	<ul style="list-style-type: none">■ ext3■ ext4■ xfs	<ul style="list-style-type: none">■ GPT■ MBR■ Aucune structure (direct FS)
Windows (avec propriété de snapshot cohérent)	NTFS	<ul style="list-style-type: none">■ 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 Snapshot Manager configuré et la machine virtuelle à protéger pour laquelle la restauration granulaire est activée doivent remplir les conditions suivantes :

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

- Le plug-in cloud doit être configuré pour protéger les biens dans la région dans laquelle l'hôte Snapshot Manager 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 autre disque ne doit être explicitement associé à l'instance Snapshot Manager.
- Les systèmes de fichiers sur l'hôte doivent être pris en charge.
Se reporter à ["Listes des systèmes de fichiers pris en charge"](#) à la page 93.
- Configurez les ports 5671 et 443 pour l'hôte Snapshot Manager ouvert.
- Pour la restauration sans agent, configurez le port 22 sur les machines virtuelles indexables dans les systèmes Linux. Pour les plates-formes Windows, configurez les ports 135 et 445 et le port WMI-IN dynamique/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 de connexion pour un disque de données disponible sur l'hôte Snapshot Manager moins 1 et type d'instance. Le volume de métadonnées Snapshot Manager utilise ce point de connexion.
- Les périphériques de stockage éphémères sont ignorés lors de la création d'un snapshot. (par exemple, des volumes de stockage d'instances Amazon AWS ou des disques temporaires Microsoft Azure) Ces périphériques sont également ignorés lors de 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. Pour prendre en charge la récupération des biens LVM, vous devez redémarrer les agents plus anciens.
- La restauration granulaire (GRT) et la restauration de fichier unique (SFR) peuvent être effectuées à l'aide de l'indexation VxMS. L'indexation VxMS s'applique à tous les systèmes de fichiers Snapshot Manager pris en charge. L'indexation VxMS peut être effectuée avec les clouds Azure, Azure Stack 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.
- Snapshot Manager 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 Snapshot Manager, 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 Snapshot Manager limite le nombre d'emplacements de disque appliqués par les fournisseurs cloud. NetBackup limite à Snapshot Manager les demandes d'indexation. Pour exécuter cette demande, NetBackup récupère les fonctions de l'hôte Snapshot Manager pendant le processus de découverte de biens cloud. Ces fonctions incluent le paramètre **Nombre maximum de travaux d'indexation**. Ce paramètre permet de limiter les demandes envoyées à Snapshot Manager 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 la découverte de l'hôte Snapshot Manager, l'API de capacité récupère le nombre maximal de travaux en fonction des points de connexion 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 Snapshot Manager. Si l'hôte Snapshot Manager reçoit un nombre de demandes d'indexation supérieur à sa capacité, les demandes supplémentaires sont mises en file d'attente.

- Pendant l'indexation, des erreurs de système d'exploitation peuvent se produire lors de l'analyse des fichiers, des répertoires ou d'autres entrées. Ces erreurs sont ignorées et l'opération d'indexation continue. Pour restaurer les fichiers manquants, vous devez démarrer les opérations de restauration granulaires sur le dossier parent.
- Lorsque vous créez ou montez un disque à partir de la machine virtuelle Windows, ajoutez la lettre du lecteur. Cette action garantit que l'opération d'indexation capture la bonne lettre de lecteur.
- Dans certains cas, le point de montage n'est pas visible lorsque vous recherchez des fichiers ou des dossiers supplémentaires sur le point de récupération. Tenez compte des raisons suivantes :
 - Le `" / "` (système de fichiers racine) est sur un LVM et
 - le point de montage n'est pas directement lié à `« / »` (système de fichiers racine).

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

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.

- Un groupe d'utilisateurs ne peut pas créer un dossier de destination pour restaurer un lecteur source. En effet, le groupe d'utilisateurs ne dispose pas d'autorisation en écriture pour créer un dossier.
- La connexion sans agent ne peut pas restaurer le fichier chiffré par Windows (ou EFS) via 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.
- Les fichiers stockés sur le volume montés sur le dossier (point de jonction) peuvent être restaurés uniquement si le disque sous-jacent présente une structure de partition GPT. Si le volume est monté à l'aide d'une lettre de lecteur, les fichiers peuvent être restaurés indépendamment de la structure de partition du disque sous-jacent.

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.

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

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

Solution de contournement :

Pour ignorer les fichiers ou les dossiers non pris en charge par Snapshot Manager lorsque de la restauration d'un fichier individuel, 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`

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

Ce chapitre traite des sujets suivants :

- [Résolution des problèmes de protection de la charge de travail cloud](#)
- [Résolution des problèmes de protection et de récupération de charge de travail PaaS](#)

Résolution des problèmes de protection de la charge de travail cloud

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

- [Fichiers journaux de configuration](#)
- [Fichiers journaux pour la création de snapshot](#)
- [Fichiers journaux pour les opérations de restauration](#)
- [Fichiers journaux pour la suppression du snapshot](#)

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

Pour le dépannage, consultez le [Guide de référence des codes d'état de NetBackup](#).

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

Fichiers journaux de configuration

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

Tableau 4-1 Fichiers journaux pour la configuration

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

Fichiers journaux pour la découverte de biens

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

Tableau 4-2 Fichiers journaux pour la découverte de biens

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

Fichiers journaux pour la création de snapshot

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

Tableau 4-3 Fichiers journaux pour la création de snapshot

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

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

Fichiers journaux pour les opérations de restauration

Utilisez les journaux suivants pour résoudre les problèmes de restauration.

Tableau 4-4

Processus	Journaux
nbwebservice L'opération de restauration du snapshot est déclenchée par l'API REST NetBackup.	Windows <i>chemin d'installation de NetBackup/webserver/logs</i> UNIX <i>/usr/opensv/wmc/webserver/logs</i> <i>/usr/opensv/logs/nbwebservices</i>
bprd L'API REST NetBackup communique avec bprd pour lancer la restauration	Windows <i>chemin d'installation de NetBackup/netbackup/logs</i> UNIX <i>/usr/opensv/netbackup/logs/bprd</i>
ncfnbcs Le PID nbcs d'un travail donné est disponible dans le moniteur d'activité NetBackup.	Windows <i>chemin d'installation de NetBackup/bin/vxlogview -i 366 -P id_processus_nbcs</i> UNIX <i>/usr/opensv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id</i>

Fichiers journaux pour la suppression du snapshot

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

Tableau 4-5 Fichiers journaux pour la suppression du snapshot

Processus	Journaux
bpdm La suppression ou le nettoyage du snapshot est déclenché(e) par bpdm.	Windows <i>chemin d'installation de NetBackup/netbackup/logs</i> UNIX <i>/usr/opensv/netbackup/logs/bpdm</i>

Processus	Journaux
ncfnbcs Le PID nbcs d'un travail donné est disponible dans le moniteur d'activité NetBackup.	Windows <i>chemin d'installation de NetBackup/bin/vxlogview -i 366 -P id_processus_nbcs</i> UNIX <i>/usr/opensv/netbackup/bin/vxlogview -i 366 -P nbcs_process_id</i>

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

Si vous tentez de récupérer une machine virtuelle à partir d'une copie d'image de sauvegarde, alors que votre rôle ne vous donne pas les privilèges requis pour effectuer une restauration à un autre emplacement, cette erreur se produit pendant l'opération de vérification de pré-récupération.

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

Solution de contournement

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Messages d'état obsolète du moniteur d'activité

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

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

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

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

Code d'état 233 : fin de fichier prématurée détectée

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

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

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

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

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

Error: Broken pipe (32), premature end of file encountered EXITING with status 42, network read failed

Explication : ce problème se produit lors de la sauvegarde si le nom de client utilisé est long, car le chemin d'accès au fichier de l'image de catalogue contient plus de 256 caractères. La sauvegarde échoue et le message d'erreur ci-dessus s'affiche dans le moniteur d'activité.

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

```
<16> db_error_add_to_file: cannot stat(\\?\C:\Program Files\Veritas
\NetBackup\db\images \azure-midb-1afb87487dc04ddc8faf453dccb7ca3+
nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+
testdb_bidinet02\1656000000\tmp\catstore\
BACKUPNOW+141a73e7-cdc4-4371-823a-f170447dba2d_
1656349831_FULL.f_imgUserGroupNames0): No such file or directory (2)
<16> ImageReadFilesFile::get_file_size: cannot stat(\\?\C:\Program
Files\Veritas\NetBackup\db
\images\azure-midb-1afb87487dc04ddc8faf453d
ccb7ca3+nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+testdb_
bidinet02\1656000000\tmp\catstore\BACKUPNOW+141a73e7-cdc4-4371
-823a-f170447dba2d_1656349831_FULL.f_imgUserGroupNames0): No such
```

```
file or directory (2) <16> ImageReadFilesFile::executeQuery: Cannot
copy \\?\C:\Program
Files\Veritas\NetBackup\db\images\azure-midb-1afb87487dc04ddc8fafa453dccb7
ca3+nbux-qa-bidi-rg+eastus+az-sql-mi-bidinet01+testdb_bidinet02\1
656000000\tmp\catstore\BACKUPNOW+141a73e7-cdc4-4371-823a-f170447d
ba2d_1656349831_FULLL.f_imgUserGroupNames0
```

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

Solution de contournement : renommez la base de données de sorte que le chemin d'accès au fichier ne contienne pas plus de 256 caractères.

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

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

Action recommandée : consultez les détails du moniteur d'activité pour identifier la cause possible du problème.

Code d'état 3817 : impossible de terminer l'opération de pré-sauvegarde

Explication : le message d'erreur s'affiche dans les journaux dbagentsutil comme

```
pg_dump: error: query failed: ERROR: permission denied for table
test;pg_dump: error: query was: LOCK TABLE public.test IN ACCESS
SHARE MODE;Invoked operation: PRE_BACKUP failed
```

Cela se produit lorsque vous essayez de sauvegarder une base de données qui a plusieurs tables avec différents rôles. Si les tables ont au moins un propriétaire différent du propriétaire de la base de données et qu'il n'est pas membre du rôle de propriétaire de la base de données, la sauvegarde peut échouer.

Action recommandée : vous devez disposer d'un rôle qui a accès à toutes les tables de la base de données que vous voulez sauvegarder ou restaurer.

Par exemple, imaginons que vous vouliez sauvegarder la base de données Scolaire qui contient deux tables :

- enfants, dont le propriétaire est postgres
- professeur, dont le propriétaire est adminscolaire

Créez un rôle. Par exemple, NBUBackupadmin.

Exécutez la commande suivante pour créer le rôle :

```
postgres=> CREATE USER NBUBackupadmin WITH PASSWORD '*****';
```

```
CREATE ROLE
```

Pour faire de ce nouveau rôle un membre des rôles `postgres` et `adminscolaire`, exécutez la commande suivante :

```
postgres=> GRANT postgres TO NBUBackupadmin;
```

```
GRANT ROLE
```

```
postgres=> GRANT schooladmin TO NBUBackupadmin;
```

```
GRANT ROLE
```

Remarque : Vous devez disposer d'un rôle qui est soit propriétaire, soit un membre du rôle propriétaire de la table, pour toutes les tables de la base de données.

La sauvegarde échoue et renvoie l'état 40 (connexion réseau interrompue).

Explication : les sauvegardes échouent en raison de la perte de connexion au serveur de médias.

Action recommandée : vous pouvez redémarrer le travail de sauvegarde si des points de contrôle sont activés dans la politique. Une fois le problème réseau résolu, sélectionnez le travail de sauvegarde inachevé dans l'interface utilisateur Web et cliquez sur **Reprendre**. Le travail reprend à partir du point où il a été arrêté. Si le point de contrôle n'est pas activé dans la politique, le travail s'affiche comme ayant échoué dans l'interface utilisateur Web.