# Guide de l’administrateur Nutanix AHV sur l’interface utilisateur Web NetBackup™

Version 10.4

VERITAS™

Dernière mise à jour : 2024-05-14

# Mentions légales



Veritas Technologies LLC
2625 Augustine Drive
Santa Clara, CA 95054

http://www.veritas.com

## Support technique

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

https://www.veritas.com/support

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

https://my.veritas.com

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

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

## Documentation

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

https://sort.veritas.com/documents

## Commentaires sur la documentation

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

NB.docs@veritas.com

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

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

## Veritas Services and Operations Readiness Tools (SORT)

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

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

# Table des matières

Chapitre 1

# Présentation

Ce chapitre traite des sujets suivants :



## Présentation de la configuration et de la protection des biens AHV dans l'interface utilisateur Web NetBackup

**Tableau 1-1** Procédure de configuration et de protection des biens AHV

| Étape | Action | Description |
|---|---|---|
| Étape 1 | Connectez-vous à l'interface utilisateur Web NetBackup en tant qu'administrateur de la sécurité par défaut. Puis, ajoutez l'utilisateur AHV au rôle **Administrateur AHV par défaut**. | **Remarque :** Pour effectuer les tâches d'administrateur AHV, le rôle **Administrateur AHV par défaut** dispose des autorisations minimales requises.<br><br>Consultez la page consacrée au rôle *Administrateur AHV par défaut* dans le *Guide de l'administrateur de l'interface utilisateur Web NetBackup*. |

| Étape | Action | Description |
|---|---|---|
| Étape 2 | Réalisez les configurations suivantes pour un cluster AHV :<br>■ Configurez la communication sécurisée entre le cluster AHV et l'hôte NetBackup.<br>■ (Facultatif) Configurez la communication sécurisée entre le Nutanix Prism Central et l'hôte NetBackup.<br>■ Activez iSCSI sur l'hôte NetBackup que vous souhaitez utiliser comme hôte de sauvegarde ou de restauration.<br>■ (Facultatif) Inscrivez l'hôte de sauvegarde sur la liste blanche de la console Prism Nutanix.<br>**Remarque :** Vous ne pouvez utiliser le protocole NFS sur l'hôte de sauvegarde ou de récupération Linux que si NFS est autorisé à afficher l'hôte sur la console Prism Nutanix AHV. Pour plus d'informations, cliquez ici. | Se reporter à "Configurer la communication sécurisée entre le cluster AHV ou le serveur Nutanix Prism Central et l'hôte NetBackup " à la page 16.<br>Se reporter à "Installation du package d'initiateur iSCSI sur l'hôte de sauvegarde Linux" à la page 20.<br>Se reporter à "Activation du service d'initiateur iSCSI sur l'hôte de sauvegarde Windows" à la page 19. |
| Étape 3 (Facultatif) | Configurez et gérez Nutanix Prism Central. | Se reporter à " Ajout d'un nouveau serveur Nutanix Prism Central " à la page 31. |
| Étape 4 | Configurez et gérez le cluster AHV. | Se reporter à "Conditions requises pour la configuration du cluster Nutanix AHV" à la page 21. |
| Étape 5 | Ajoutez et gérez les informations d'authentification. | Se reporter à "Ajout d'informations d'authentification relatives au cluster" à la page 47. |
| Étape 6 | Configurez un plan de protection AHV. | Consultez le *Guide de l'administrateur de l'interface utilisateur Web NetBackup*™. |
| Étape 7 | Configurez un groupe de machines virtuelles intelligent. | Se reporter à "Création d'un groupe de machines virtuelles intelligent" à la page 34. |

| Étape | Action | Description |
|---|---|---|
| Étape 8 | Protégez les machines virtuelles ou les groupes de machines virtuelles intelligents AHV. | Se reporter à "Protection des machines virtuelles ou des groupes de machines virtuelles intelligents AHV" à la page 54. |
| Étape 9 | Récupérez une machine virtuelle. | Se reporter à "Récupération d'une machine virtuelle AHV" à la page 62. |

Chapitre 2

# Gestion des clusters AHV

Ce chapitre traite des sujets suivants :

- Mise à jour du groupe de machines virtuelles intelligent
- Suppression d'un groupe de machines virtuelles intelligent
- Définition des paramètres CHAP pour iSCSI
- Ajout d'un hôte d'accès AHV
- Suppression d'un hôte d'accès AHV
- Modification des limites de ressource pour les types de ressource AHV
- Modification de la fréquence de la découverte automatique des biens AHV

# Liste de contrôle de configuration rapide pour protéger les machines virtuelles AHV

Utilisez l'interface utilisateur Web NetBackup pour protéger et récupérer les machines virtuelles qui sont créées sur la plate-forme AHV. Vous pouvez également utiliser les API et les options de ligne de commande pour protéger et récupérer les machines virtuelles.

Se reporter à "Utilisation des API et des options de ligne de commande pour gérer, protéger ou récupérer des machines virtuelles AHV" à la page 120.

Le tableau suivant décrit les étapes principales ou la liste de contrôle pour protéger les machines virtuelles AHV :

**Tableau 2-1** Configuration et protection des machines virtuelles AHV à l'aide de NetBackup

| Présentation des étapes | Description et référence |
|---|---|
| Déploiement de NetBackup pour protéger les machines virtuelles AHV | Conditions requises générales pour protéger les machines virtuelles AHV :<br>■ Serveur principal NetBackup<br>■ Serveur de médias NetBackup (recommandé)<br>■ Client NetBackup qui peut servir d'hôte de sauvegarde<br>Le système d'exploitation de l'hôte de sauvegarde doit être Linux RHEL, SUSE ou Windows. L'hôte de sauvegarde peut être un serveur de médias ou un client NetBackup, ou bien une appliance NetBackup.<br>Les appliances NetBackup, notamment les appliances Flex et Flex Scale, peuvent également être utilisées comme serveur de médias NetBackup pour jouer le rôle d'hôte de sauvegarde.<br>NetBackup s'appuie sur une architecture sans agent pour protéger les machines virtuelles AHV. La communication entre NetBackup et le cluster AHV se fait au moyen d'API Nutanix AHV. |
| Configuration d'un hôte d'accès AHV pour la sauvegarde et la récupération | Un hôte d'accès AHV joue à la fois le rôle d'hôte de sauvegarde et celui d'hôte de récupération, pendant la sauvegarde et la récupération, respectivement. L'hôte d'accès est impliqué dans les transferts de données pendant les opérations de sauvegarde et de restauration.<br>Si vous prévoyez d'utiliser un hôte de sauvegarde qui n'est pas une appliance ou un serveur de médias NetBackup, ajoutez l'hôte de sauvegarde à la liste **Hôtes d'accès AHV** de NetBackup.<br>**Remarque :** Le client NetBackup doit être installé sur tout hôte de sauvegarde qui n'est ni un serveur de médias, ni une appliance.<br>Se reporter à "Ajout d'un hôte d'accès AHV" à la page 41. |
| Activer la communication sécurisée entre NetBackup et AHV | Les sections suivantes fournissent des informations supplémentaires sur la configuration d'une communication sécurisée entre NetBackup et AHV :<br>■ Communication sécurisée<br>Se reporter à "Configurer la communication sécurisée entre le cluster AHV ou le serveur Nutanix Prism Central et l'hôte NetBackup " à la page 16.<br>■ Ports de communication<br>Se reporter à "À propos des ports utilisés par NetBackup pour communiquer avec AHV" à la page 24. |

| Présentation des étapes | Description et référence |
|---|---|
| Gestion des clusters AHV, du serveur Prism Central et des groupes de machines virtuelles intelligents | ■ Gestion des clusters AHV<br>Se reporter à "Ajout ou parcours d'un cluster AHV" à la page 25.<br>■ Gestion du serveur Prism Central<br>Se reporter à " Ajout d'un nouveau serveur Nutanix Prism Central " à la page 31.<br>■ Gestion des groupes de machines virtuelles intelligents<br>Se reporter à "Création d'un groupe de machines virtuelles intelligent" à la page 34.<br>Se reporter à "Suppression d'un groupe de machines virtuelles intelligent" à la page 40. |
| Protection des machines virtuelles AHV | ■ Conditions requises :<br>L'ajout d'un cluster AHV requiert le rôle d'administrateur AHV par défaut.<br>■ Pratiques d'excellence<br>Se reporter à "Points à savoir avant de protéger les machines virtuelles AHV" à la page 53.<br>■ Protection des machines virtuelles<br>Se reporter à "Protection des machines virtuelles ou des groupes de machines virtuelles intelligents AHV" à la page 54. |
| Transport iSCSI pour les hôtes de sauvegarde Windows | Pré-requis<br>Pour Windows 2012 ou versions ultérieures, l'initiateur de client iSCSI doit être présent sous Windows. Par défaut, le service d'initiateur iSCSI est arrêté ou désactivé sous Windows.<br>Se reporter à "Activation du service d'initiateur iSCSI sur l'hôte de sauvegarde Windows" à la page 19.<br>**Remarque :** Si l'hôte de sauvegarde ou de récupération sélectionné est Windows, assurez-vous que le service iSCSI est en cours d'exécution sur l'ordinateur Windows pour éviter l'échec des travaux de sauvegarde ou restauration. |

| Présentation des étapes | Description et référence |
|---|---|
| Transport iSCSI pour les hôtes de sauvegarde Linux | Pré-requis<br><br>L'utilisation de iSCSI nécessite que le package `scsi-initiator-utils` soit installé. Par défaut, il est installé sous RHEL/SUSE.<br><br>Se reporter à "Installation du package d'initiateur iSCSI sur l'hôte de sauvegarde Linux" à la page 20.<br><br>**Remarque :** Vous ne pouvez utiliser le protocole NFS sur l'hôte de sauvegarde ou de récupération Linux que si NFS est autorisé à afficher l'hôte sur la console Prism Nutanix AHV. Pour plus d'informations, consultez https://www.veritas.com/content/support/fr_FR/doc/127664414-132725336-0/v127698742-132725336.<br><br>Si le package `iscsi-initiator-utils` est déjà installé sur l'hôte de sauvegarde ou de récupération, assurez-vous que le daemon iSCSI est en cours d'exécution.<br><br>■ Pour vérifier l'état du daemon, exécutez la commande `systemctl status iscsid`.<br>■ Si le daemon est désactivé, exécutez la commande `systemctl enable iscsid`, puis la commande de démarrage du daemon iSCSI `systemctl start iscsid`. |

| Présentation des étapes | Description et référence |
|---|---|
| Configuration des paramètres CHAP pour la communication sécurisée iSCSI avec les clusters Nutanix AHV | CHAP à sens unique :<br>■ L'initiateur iSCSI s'authentifie auprès de la cible (AHV) à l'aide du mot de passe/secret CHAP généré aléatoirement.<br>CHAP mutuel - automatique :<br>■ Le service NetBackup CMS (Credential Management Service) génère automatiquement des informations d'authentification préfixées par AHV_ISCSI_MUTUAL_AUTO_ pour le mot de passe CHAP de l'hôte de sauvegarde/récupération. Cela permet d'assurer l'authentification mutuelle entre l'initiateur iSCSI (c'est-à-dire l'hôte de sauvegarde/récupération de NetBackup) et la cible (c'est-à-dire AHV).<br>Vous pouvez définir une période de conservation pour ces mots de passe CHAP générés automatiquement. La période de conservation par défaut pour les mots de passe CHAP générés automatiquement est de 90 jours à partir de la date de création.<br>**Remarque :**<br>La configuration par défaut est CHAP à sens unique. Pour activer l'option **CHAP mutuel** :<br>Se reporter à "Configuration des paramètres CHAP pour la communication iSCSI sécurisée avec les clusters AHV" à la page 24. |
| Définition de limites globales d'utilisation des ressources AHV | Les machines virtuelles sont automatiquement protégées dès leur création et le nombre de machines protégées simultanément peut devenir important au fil du temps. Le nombre élevé de sauvegardes simultanées peut avoir un impact sur les performances d'AHV, ainsi que sur les performances de sauvegarde.<br>Vous pouvez définir des limites globales pour optimiser la gestion des ressources AHV.<br>Se reporter à "Modification des limites de ressource pour les types de ressource AHV" à la page 42. |

| Présentation des étapes | Description et référence |
|---|---|
| Sélection automatique de l'hôte de sauvegarde NetBackup | L'option de sélection automatique de l'hôte de sauvegarde NetBackup utilise en interne l'équilibrage des charges du serveur de médias NetBackup pour allouer des travaux de snapshot/sauvegarde à des serveurs de médias disponibles et pris en charge. NetBackup évite d'envoyer des travaux aux serveurs de médias occupés.<br>**Remarque :** Les sauvegardes cohérentes au niveau application nécessitent NetBackup version 9.1 ou une version ultérieure sur le serveur de médias.<br>Pré-requis<br>■ Dans l'interface utilisateur Web NetBackup, cliquez sur **Stockage > Stockage sur disque**. Puis, cliquez sur l'onglet **Serveurs de stockage**. Ajoutez tous les serveurs de médias pris en charge pour l'équilibrage de charge.<br>■ Cliquez sur **Stockage > Unités de stockage**. Sélectionnez le *nom de l'unité de stockage*. Sous le **serveur de médias**, cliquez sur **Modifier**. Puis, sélectionnez **Permettre à NetBackup d'effectuer une sélection automatique**.<br>■ Lorsque vous créez un plan de protection AHV, sélectionnez **Automatique** pour le paramètre **Sélectionner le serveur ou l'hôte à utiliser pour les sauvegardes**. |

# Configurer la communication sécurisée entre le cluster AHV ou le serveur Nutanix Prism Central et l'hôte NetBackup

NetBackup peut désormais valider les certificats du cluster AHV et du serveur Prism Central à l'aide des certificats de leur autorité de certification racine ou intermédiaire.

Seul le format de certificat `PEM` est pris en charge pour les serveurs de virtualisation.

La procédure suivante s'applique aux serveurs de médias NetBackup faisant office d'hôtes de sauvegarde et à tous les hôtes d'accès AHV.

**Pour configurer la communication sécurisée entre le cluster AHV ou le serveur AVH Prism Central et l'hôte d'accès AHV :**

1. Utilisez la commande `openssl s_client -connect Nutanix Cluster FQDN:9440 -showcerts < /dev/null` d'un système Linux pour obtenir les certificats Nutanix.

   Pour Nutanix Prism Central, utilisez le `openssl s_client -connect Nutanix Prism Central FQDN:9440 -showcerts < /dev/null`

2. Faites défiler la page jusqu'à la fin des résultats et copiez le dernier certificat qui démarre à partir de :

   ```
   -----BEGIN CERTIFICATE-----
   <Certificate>
   -----END CERTIFICATE-----
   ```

   **Remarque :** Veillez à copier les cinq tirets avant et après les mots BEGIN et END CERTIFICATE.

3. Collez ces informations dans un fichier texte, renommez-le *nom du fichier du certificat*`.pem` et copiez-le dans le chemin d'accès de l'hôte de sauvegarde. Le chemin recommandé est :

   - Pour Linux : `/usr/openv/netbackup`.
   - Pour Windows : *lecteur installation*`\Program Files\Veritas\Netbackup`.

4. - Pour Linux : entrez le chemin d'accès au fichier PEM `ECA_TRUST_STORE_PATH=/usr/openv/netbackup/`*nom fichier certificat*`.pem` dans le fichier `bp.conf` sur l'hôte de sauvegarde.
   - Pour Windows : exécutez la commande *Install drive*`\Program Files\Veritas\Netbackup\bin\nbsetconfig`.

5. Utilisez la commande `nbsetconfig` pour configurer les options de configuration NetBackup suivantes sur l'hôte d'accès :

   Pour plus d'informations sur les options de configuration, consultez le Guide de l'administrateur NetBackup, volume I.

   Pour plus d'informations sur la prise en charge des autorités de certification externes, consultez le Guide de sécurité et de chiffrement de NetBackup.

**Tableau 2-2**

| | |
|---|---|
| ECA_TRUST_STORE_PATH | Spécifie le chemin d'accès du fichier de certificats qui contient tous les certificats de l'autorité de certification racine approuvés.<br><br>Cette option est propre aux certificats basés sur un fichier. Vous ne devez pas configurer cette option si le magasin de certificats Windows est utilisé.<br><br>Si vous avez déjà configuré cette option d'autorité de certification externe, ajoutez les certificats d'autorité de certification Nutanix AHV au magasin d'approbation de certificat externe existant.<br><br>Si vous ne l'avez pas configurée, ajoutez tous les certificats d'autorité de certification de serveur Nutanix AHV requis au magasin d'approbation et définissez l'option. |
| ECA_CRL_PATH | Spécifie le chemin d'accès au répertoire où se trouvent les listes de révocation des certificats (CRL) de l'autorité de certification externe.<br><br>Si vous avez déjà configuré cette option d'autorité de certification externe, ajoutez les listes de révocation des certifications AHV au cache de CRL.<br><br>Si vous n'avez pas configuré cette option, ajoutez d'abord toutes les listes de révocation des certifications requises au cache de CRL, puis définissez l'option. |

| | |
|---|---|
| VIRTUALIZATION_HOSTS_SECURE_CONNECT_ENABLED | Cette option a un impact sur la communication sécurisée d'AHV, de RHV et de VMware. Sans cette option, la communication sécurisée ou non sécurisée avec la charge de travail est décidée par chaque charge de travail et plug-in séparément.<br>Pour Nutanix AHV, la communication sécurisée est activée par défaut.<br>Cette option permet d'ignorer la validation du certificat de sécurité.<br>Désactivez cette option si vous souhaitez ignorer la validation du certificat de sécurité.<br>Veritas vous recommande d'activer la communication sécurisée à l'aide de l'option ECA_TRUST_STORE_PATH . |
| VIRTUALIZATION_CRL_CHECK | Permet de valider l'état de révocation du certificat du serveur de virtualisation en fonction des listes de révocation des certificats.<br>Par défaut, cette option est activée. |

# Activation du service d'initiateur iSCSI sur l'hôte de sauvegarde Windows

Effectuez l'une des opérations suivantes :

1. - Cliquez sur **Gestionnaire de serveurs > Outils > Initiateur iSCSI**.
   - Une fenêtre de message s'affiche : **Pour démarrer le service maintenant et le démarrer automatiquement à chaque redémarrage, cliquez sur le bouton Oui**. Cliquez sur **Oui** pour confirmer.
2. Vous pouvez également activer le service iSCSI à partir des outils d'administration :
   - Cliquez sur **Panneau de configuration > Outils d'administration > Services**.
   - Recherchez le service **Initiateur iSCSI Microsoft**.
   - Cliquez dessus avec le bouton droit de la souris, puis cliquez sur **Démarrer**.

**Remarque :** L'option par défaut de ce service est **Manuel**. Définissez le paramètre sur **Automatique** pour lancer automatiquement l'exécution du service lors du redémarrage.

3 Si vous prévoyez d'utiliser un réseau iSCSI segmenté Nutanix, consultez la section Se reporter à "À propos de la prise en charge du réseau iSCSI segmenté Nutanix" à la page 22. pour en savoir plus sur la configuration du réseau de l'hôte de sauvegarde.

# Installation du package d'initiateur iSCSI sur l'hôte de sauvegarde Linux

Pour installer le package d'initiateur iSCSI, utilisez les commandes yum et zypper suivantes :

- `yum install iscsi-initiator-utils" - RedHat.`
- `zypper -n install open-iscsi" - SuSE.`
- Si vous prévoyez d'utiliser un réseau iSCSI segmenté Nutanix, consultez la section Se reporter à "À propos de la prise en charge du réseau iSCSI segmenté Nutanix" à la page 22. pour en savoir plus sur la configuration du réseau de l'hôte de sauvegarde.

# Migration des clusters ajoutés depuis l'interface utilisateur graphique (GUI) ou la ligne de commande (CLI) Java dans l'interface utilisateur Web

La gestion des informations d'authentification pour la GUI/CLI JAVA est distincte de celle de l'interface utilisateur Web.

- Les clusters ajoutés au moyen de la GUI/CLI Java ne sont pas reportés dans l'interface utilisateur Web et inversement.
- S'il existe des clusters dans l'interface graphique utilisateur/interface de ligne de commande de Java, l'utilisateur doit les ajouter manuellement, de même que ses informations d'authentification, dans l'interface utilisateur Web.

**Remarque :** Si un cluster est ajouté dans l'interface utilisateur Web, puis supprimé de ll'interface graphique utilisateur/interface de ligne de commande de Java, il reste intact dans l'interface utilisateur Web et inversement.

- Si le cluster est ajouté dans l'interface utilisateur Web et que ses informations d'authentification doivent être mises à jour, il doit être mis à jour uniquement depuis l'interface utilisateur Web.
  Imaginez le scénario suivant :
  - Un cluster existe à la fois dans l'interface utilisateur Web et dans l'interface utilisateur Java.
  - Les informations d'authentification du cluster sont mises à jour dans l'interface utilisateur Web uniquement.
  - Le cluster est supprimé de l'interface utilisateur Web.

  **Impact** : les sauvegardes et les restaurations peuvent échouer dans l'interface graphique utilisateur de Java, car les informations d'authentification du cluster qui y ont été ajoutées n'ont pas été mises à jour.
  **Recommandation** : mettez à jour les informations d'authentification à partir de l'interface graphique utilisateur de Java.
- Une fois le cluster ajouté dans l'interface utilisateur Web, les sauvegardes utilisant des politiques existantes aboutissent, même si vous supprimez le cluster de la l'interface graphique utilisateur de Java. Néanmoins, les travaux de restauration ne peuvent pas être déclenchés depuis l'interface graphique utilisateur de Java dans ce scénario, car il faudrait qu'un cluster y soit présent.
- Si un cluster est ajouté depuis l'interface graphique utilisateur de Java et l'interface utilisateur Web, puis est supprimé de l'interface graphique utilisateur de Java, le cluster reste visible dans l'interface utilisateur Web et inversement.
- Si un cluster se trouve à la fois dans l'interface utilisateur Web et la GUI Java, puis que ses informations d'authentification sont mises à jour dans l'interface utilisateur Web et que ce cluster y est supprimé, la sauvegarde et les restaurations risquent d'échouer, car le cluster ajouté dans l'interface utilisateur Java n'a pas été mis à jour. Il peut être nécessaire de mettre à jour les informations d'authentification depuis l'interface utilisateur Java pour que tout fonctionne normalement.

# Conditions requises pour la configuration du cluster Nutanix AHV

Conditions requises :

**Configurez l'adresse IP des services de données iSCSI sur le cluster Nutanix AHV.**

1. Pour utiliser l'option **Utiliser l'adresse IP segmentée du service de données iSCSI** ou **Utiliser l'adresse IP des services de données iSCSI segmentés spécifiée**, le cluster AHV doit être configuré avec la fonction d'interface réseau iSCSI segmentée avec des volumes (ABS).
2. Si vous prévoyez de choisir l'option **Utiliser l'adresse IP iSCSI** lors de la configuration du cluster, **Nutanix** recommande de configurer l'adresse IP des services de données iSCSI sur Nutanix AHV.

   Accédez à la console Prism du cluster Nutanix AHV à l'adresse `https://`*`Nom de domaine complet du cluster Nutanix/IP`*`:9440`.

   Cliquez sur **Paramètres > Détails du cluster > Définir l'adresse IP des services de données iSCSI**.

---

**Remarque :** Si ce paramètre n'est pas configuré :

Pour l'hôte de sauvegarde Windows, les travaux de sauvegarde/restauration échouent.

Pour l'hôte de sauvegarde Linux, les travaux basculent vers NFS à condition que l'adresse IP des services de données iSCSI segmentés soit correctement configurée.

L'échec du travail de sauvegarde/restauration pour les hôtes de sauvegarde Windows s'affiche en tant qu'échec dans la section **Moniteur d'activité > Détails du travail**. Le basculement d'iSCSI vers NFS des hôtes de sauvegarde Linux est signalé par un avertissement dans les détails du travail.

---

# À propos de la prise en charge du réseau iSCSI segmenté Nutanix

NetBackup prend en charge la séparation du trafic de sauvegarde à l'aide d'un réseau iSCSI segmenté Nutanix. La séparation du trafic de sauvegarde est utile pour réduire la charge sur les ressources de production, en consacrant la taille adéquate de ressources pour améliorer la vitesse de sauvegarde/récupération ainsi que la sécurité. Par défaut, le trafic de sauvegarde/récupération transite sur le réseau de gestion de cluster Nutanix à l'aide de l'adresse IP des services de données iSCSI à des fins de connexion et de découverte initiales.

Pendant la configuration du cluster AHV, choisissez l'une des options suivantes pour le transport iSCSI :

- **Utiliser l'adresse IP du service de données iSCSI**
- **Utiliser l'adresse IP du service de données iSCSI segmenté**
- **Utiliser l'adresse IP du service de données iSCSI segmenté spécifiée**

Pour en savoir plus, consultez la section Se reporter à "Ajout ou parcours d'un cluster AHV" à la page 25..

## Configuration du réseau de l'hôte de sauvegarde pour utiliser la configuration du réseau iSCSI segmenté Nutanix

- Le réseau iSCSI segmenté se trouve sur un sous-réseau différent du réseau de gestion de cluster. Par conséquent, le réseau de l'hôte de sauvegarde doit être configuré pour se connecter aux réseaux suivants :
  - Réseau de gestion de cluster AHV
  - Réseau segmenté iSCSI

  Pour cela, configurez l'hôte de sauvegarde avec deux VLAN : l'un correspondant au réseau de gestion de cluster, l'autre au réseau iSCSI segmenté qui sera dédié au trafic de sauvegarde/récupération.
- Pour obtenir de meilleures performances, utilisez le nom d'hôte/l'adresse IP correspondant au réseau segmenté comme nom d'hôte lors de l'installation/la configuration de NetBackup sur l'hôte de sauvegarde.
- Vérifiez la connectivité à l'aide de la commande suivante sur l'hôte Windows :
  - Cliquez sur **Gestionnaire de serveurs > Outils > Initiateur iSCSI**. La boîte de dialogue des **propriétés de l'initiateur iSCSI** s'ouvre alors.
  - Cliquez sur **Discovery > Discovery portal** et fournissez l'adresse IP en fonction du type de cible iSCSI configuré pour le cluster AHV.
  - DEFAULT : utilisez l'adresse IP des services de données iSCSI de la page de détails du cluster.
  - SEGMENTED : utilisez les données iSCSI segmentées de la page de détails du cluster .
  - SEGMENTED_SPECIFIC : utilisez l'adresse IP virtuelle spécifiée lors de la configuration du cluster dans NetBackup.
- Vérifiez la connectivité à l'aide de la commande suivante sur l'hôte Linux :
  - `iscsiadm -m discovery -t sendtargets -p` *`correct IP as per configured iSCSITargetType`*
  - DEFAULT : utilisez l'adresse IP des services de données iSCSI de la page de détails du cluster.

    - SEGMENTED : utilisez les données iSCSI segmentées de la page de détails du cluster .
- SEGMENTED_SPECIFIC : utilisez l'adresse IP virtuelle spécifiée lors de la configuration du cluster dans NetBackup. En cas de problème de connectivité, une erreur similaire à la suivante s'affiche : `iscsiadm : connexion <adresse IP> arrivée à expiration`.

# Configuration des paramètres CHAP pour la communication iSCSI sécurisée avec les clusters AHV

Les paramètres CHAP s'appliquent à tous les clusters AHV configurés dépendant du serveur principal actuellement sélectionné.

1. Dans la partie gauche, sélectionnez **Charges de travail > Nutanix AHV**.
2. En haut, cliquez sur **Paramètres AHV**.
3. Sélectionnez **CHAP pour iSCSI**.
4. Sélectionnez l'option CHAP appropriée.

# À propos des ports utilisés par NetBackup pour communiquer avec AHV

Le tableau suivant décrit les ports dont NetBackup a besoin pour communiquer avec AHV :

**Tableau 2-3** Ports requis par NetBackup pour communiquer avec AHV

| Port | Protocole | Emplacement | Objet |
|---|---|---|---|
| 860, 3260 | iSCSI sur TCP | *bidirectionnel | iSCSI assure l'accès au niveau des blocs aux périphériques de stockage avec `SCSI`.<br>iSCSI facilite les transferts de données, généralement sur une liaison Ethernet. |

| Port | Protocole | Emplacement | Objet |
|---|---|---|---|
| 3205 | iSCSI sur TCP | *bidirectionnel | iSNS peut émuler les services de Fabric Fibre Channel et gérer à la fois les périphériques iSCSI et Fibre Channel. Un serveur iSNS peut être utilisé comme point de configuration consolidé pour un réseau de stockage entier. |
| 111 | TCP | *bidirectionnel | Portmapper |
| 2 049 | TCP | *bidirectionnel | NFS |
| 9440 | TCP | Cluster AHV<br>Serveur AHV Prism Central | Console Prism, API REST |

*Les ports doivent être ouverts en mode bidirectionnel entre l'hôte d'accès AHV et le cluster AHV. Le port 9440 est uniquement ouvert en entrée vers le cluster AHV à partir de l'hôte d'accès AHV.

# Ajout ou parcours d'un cluster AHV

Vous pouvez ajouter et parcourir un cluster AHV et ses informations d'authentification.

**Pour ajouter un cluster AHV et ses informations d'authentification**

1. Sur la gauche, cliquez **Nutanix AHV**, puis sur l'onglet **Cluster AHV**.
2. Cliquez sur **Ajouter** pour ajouter un cluster AHV et entrez les éléments suivants :

   Se reporter à "Erreur lors de l'ajout des informations d'authentification AHV" à la page 97.

   - **Nom du cluster**

     **Remarque :** NetBackup recommande d'utiliser le nom de domaine complet pour ajouter le cluster AHV. Le nom de cluster est limité à 218 caractères.

   - **Port REST API (paramètre par défaut : 9440)**
     Ce port doit rester ouvert entre l'hôte de sauvegarde et le cluster AHV.

Se reporter à "À propos des ports utilisés par NetBackup pour communiquer avec AHV" à la page 24.

- Cochez la case **Utiliser Prism Central pour ce cluster** pour protéger les attributs de machines virtuelles associés au serveur Prism Central. Par exemple, pour capturer des attribut liés au réseau cloud privé virtuel, au projet, à la catégorie et au propriétaire de la machine virtuelle.
  Se reporter à " Ajout d'un nouveau serveur Nutanix Prism Central " à la page 31.

  **Remarque :** Le serveur Prism Central doit être ajouté dans l'environnement NetBackup avant de cocher cette case.

- Sélectionnez l'une des options suivantes dans le **transport iSCSI**.
  - **Utiliser l'adresse IP du service de données iSCSI**
    L'adresse IP des services de données iSCSI configurée sur le cluster AHV est utilisée en tant que portail de découverte de cible iSCSI et de point de connexion initial.

    **Remarque :** Cette option bascule vers NFS sur un hôte de sauvegarde Linux dans les cas suivants :

    L'adresse IP des services de données iSCSI n'est pas configurée sur le cluster AHV.

    La connexion iSCSI n'est pas établie sur l'hôte de sauvegarde.

  - **Utiliser l'adresse IP du service de données iSCSI segmenté**
    L'adresse IP des services de données iSCSI segmentés configurée sur le cluster AHV est utilisée en tant que portail de découverte de cible iSCSI et de point de connexion initial.

    **Remarque :** La validation de cluster échoue si la configuration n'est pas présente sur le cluster AHV.

    Le travail de sauvegarde/récupération échoue si la configuration n'est pas présente sur le cluster AHV ou si l'hôte de sauvegarde ne dispose pas de la configuration réseau requise.

  - **Utiliser l'adresse IP du service de données iSCSI segmenté spécifiée**

- Dans le champ **Adresse IP virtuelle**, fournissez l'adresse IP valide. Fournissez l'adresse IP virtuelle correspondant à l'interface réseau iSCSI segmentée Nutanix que vous prévoyez d'utiliser pour la sauvegarde et la récupération du trafic de données iSCSI.

L'adresse IP spécifiée est utilisée comme portail de découverte de cible iSCSI et de point de connexion initial. NetBackup effectue la validation à l'aide des API Nutanix, si l'adresse IP virtuelle provient de l'une des interfaces de services de données iSCSI segmentées configurées.

---

**Remarque :** Le travail de sauvegarde/récupération échoue si la configuration n'est pas effectuée sur le cluster AHV ou si l'hôte de sauvegarde ne dispose pas de la configuration réseau requise.

---

3 - **Sélectionnez un hôte de sauvegarde.**
Cet hôte de sauvegarde est utilisé pour la validation et la découverte.

---

**Remarque :** La validation des informations d'authentification et la découverte des machines virtuelles ne sont prises en charge qu'à partir de NetBackup 9.1.

---

- **Associez les informations d'authentification.**

  Effectuez l'une des opérations suivantes :

  - Sélectionnez des informations d'authentification existantes, consultez *Gestion des informations d'authentification* dans le Guide de l'administrateur de l'interface utilisateur Web NetBackup™.
  - Se reporter à "Ajout d'informations d'authentification relatives au cluster" à la page 47.

---

**Remarque :** Vous devez associer les informations d'authentification d'un utilisateur du cluster AHV disposant du rôle d'administrateur de cluster.

---

4 Cliquez sur **Ajouter et gérer des autorisations**.

Des validations sont effectuées pour toutes les entrées.

Sélectionnez les rôles qui doivent avoir accès à ce cluster. Consultez la page *Gestion du contrôle d'accès basé sur les rôles* dans le Guide de l'administrateur de l'interface utilisateur Web NetBackup™.

5 Pour ajouter les informations d'authentification d'un autre cluster AHV, cliquez sur **Ajouter**.

## Actions intégrées sur un cluster AHV

Vous pouvez exécuter les action intégrées suivantes sur un cluster AHV :

- **Découvrir** : découvrez manuellement les biens de machine virtuelle qui appartiennent au cluster AHV sélectionné.
- **Modifier** : modifiez les informations d'authentification du cluster AHV.
- **Supprimer** : supprimez le cluster AHV.
- **Gérer les autorisations** : ajoutez ou gérez les autorisations sur le cluster sélectionné.

## Actions en bloc sur le cluster AHV

Vous pouvez sélectionner un ou plusieurs clusters AHV et exécuter les actions en bloc suivantes :

- **Découvrir** : découvrez manuellement les biens de machine virtuelle qui appartiennent au cluster AHV sélectionné.

  **Remarque :** La découverte est déclenchée de manière séquentielle pour les clusters, l'un après l'autre.

- **Valider** :
  - Valide les informations d'authentification du cluster AHV.
  - Si vous choisissez **Utiliser l'adresse IP du service de données iSCSI segmenté**, la configuration de l'adresse IP du service de données iSCSI segmenté est vérifiée sur le cluster Nutanix.
  - Si vous sélectionnez **Utiliser l'adresse IP du service de données iSCSI segmenté spécifiée**, la configuration de l'adresse IP virtuelle spécifiée en tant qu'adresse IP du service de données iSCSI segmenté est vérifiée sur le cluster Nutanix.
- **Supprimer** : supprimez le cluster AHV.

## Parcourir un cluster AHV

Vous pouvez parcourir les clusters AHV pour localiser des machines virtuelles et des conteneurs de stockage, ainsi que leurs informations.

**Pour parcourir un cluster AHV**

1. Dans la partie gauche, cliquez sur Nutanix AHV.
2. Cliquez sur l'onglet **Cluster AHV** et lancez la recherche.

   La liste regroupe les clusters AHV auxquels vous avez accès.

   L'onglet affiche les clusters AHV auxquels vous pouvez accéder en appliquant la hiérarchie suivante :

   ```
   All
   AHV_clusters
    cluster1
     VirtualMachine
     StorageContainer
    cluster2
     VirtualMachine
     StorageContainer
   ```

   Pour localiser un cluster, vous pouvez entrer une chaîne dans le champ de recherche.
3. Cliquez sur un cluster AHV pour afficher ses informations.
4. Cliquez sur une machine virtuelle pour afficher son état de protection, ses points de récupération et son activité de restauration.
5. Cliquez sur **Ajouter la protection** pour abonner la machine virtuelle sélectionnée à un plan de protection. Vous pouvez également sélectionner les options **Sauvegarder maintenant**, **Récupérer** et **Gérer les autorisations**.

---

**Remarque :** Assurez-vous que le plan de protection pour AHV existe pour ajouter la protection à un bien.

---

6 Cliquez sur un conteneur de stockage pour afficher l'espace libre et la date et l'heure de la dernière découverte.

**Remarque :** Lorsque les données dépassent la capacité annoncée, les données supplémentaires sont affichées comme négatives. L'interface utilisateur Web NetBackup affiche un champ vide et l'API correspondante affiche la valeur -ve pour le champ d'espace disponible d'un conteneur de stockage donné.

7 Pour le conteneur de stockage, vous pouvez **gérer les autorisations**.

**Remarque : L'autorisation de gestion** est activée uniquement lorsque vous sélectionnez le conteneur de stockage.

# Suppression des clusters AHV

Utilisez cette procédure pour supprimer des clusters AHV.

**Pour supprimer un cluster AHV**

1 Dans la partie gauche, cliquez sur **Nutanix AHV**, puis sur l'onglet **Clusters AHV**.

L'onglet affiche la liste des noms des clusters AHV auxquels vous avez accès. Vous pouvez également consulter le **statut de découverte** et la **dernière tentative de découverte** pour déterminer la date de la dernière découverte des machines virtuelles et des autres objets du serveur.

2 Recherchez et sélectionnez le cluster AHV.

3 Sélectionnez **Actions > Supprimer**.

**Remarque :** Si vous supprimez un cluster, les machines virtuelles qui y sont associées ne sont plus protégées. Vous pourrez toujours récupérer les images de sauvegarde existantes, mais les sauvegardes de machines virtuelles sur ce serveur échoueront.

4 Si vous êtes sûr de vouloir supprimer le cluster AHV, cliquez sur **Supprimer**.

# Ajout d'un nouveau serveur Nutanix Prism Central

Vous pouvez ajouter et parcourir un serveur Nutanix Prism Central et ses informations d'authentification.

**Pour ajouter les informations d'authentification Nutanix Prism Central et les informations d'authentification respectives**

1. Dans la partie gauche, cliquez sur **Nutanix AHV**, puis sur l'onglet **Serveurs Prism Central**.
2. Cliquez sur **Ajouter** pour ajouter un serveur Nutanix Prism Central et entrez les éléments suivants :
   - **Nom du serveur Prism Central**
   - **Port REST API (paramètre par défaut : 9440)**
     Ce port doit rester ouvert entre l'hôte de sauvegarde et le cluster AHV.
   - **Hôte de sauvegarde**

     **Remarque :** L'hôte de sauvegarde doit utiliser au moins la version 10.1.1 de NetBackup. Le système d'exploitation doit être Linux (RHEL et SUSE) ou Windows.

   - **Associer les informations d'authentification**

     Effectuez l'une des opérations suivantes :

     - Lors de l'ajout d'informations d'authentification de serveur Prism Central pour des informations d'authentification existantes, sélectionnez la catégorie **AHV Prism Central**. Pour plus d'informations, consultez la section *Gestion informations d'authentification* du Guide de l'administrateur de l'interface utilisateur Web NetBackup.
     - Se reporter à "Ajout de nouvelles informations d'authentification pour le serveur Prism Central " à la page 32.
3. Cliquez sur **Ajouter et gérer des autorisations**.

   Des validations sont effectuées pour toutes les entrées.

   Sélectionnez les rôles qui doivent avoir accès à ce cluster. Consultez la page *Gestion du contrôle d'accès basé sur les rôles* dans le Guide de l'administrateur de l'interface utilisateur Web NetBackup™.
4. Pour ajouter les informations d'authentification d'un autre serveur AHV Prism Central, cliquez sur **Ajouter**.

### Actions intégrées sur Nutanix Prism Central

Vous pouvez exécuter les actions intégrées suivantes sur un serveur Nutanix Prism Central :

- **Valider** : permet de réaliser une validation manuelle.
- **Modifier** : permet de modifier l'hôte de sauvegarde et les informations d'authentification du serveur Nutanix Prism Central.
- **Supprimer** : permet de supprimer le serveur Nutanix Prism Central.
- **Gérer les autorisations** : permet d'ajouter ou de gérer les autorisations sur le serveur Prism Central sélectionné.

### Actions en bloc sur Nutanix Prism Central

Vous pouvez sélectionner un ou plusieurs serveurs Nutanix Prism Central et exécuter les actions en bloc suivantes :

- **Valider**
- **Supprimer**

# Ajout de nouvelles informations d'authentification pour le serveur Prism Central

1. Dans la partie gauche, cliquez sur **Nutanix AHV**, puis sur l'onglet **Nutanix Prism Central**.
2. Cliquez sur **Ajouter** pour ajouter un nouveau serveur Prism Central.
3. Sur la page **Ajouter AHV Prism Central > Associer des informations d'authentification**, cliquez sur **Ajouter de nouvelles informations d'authentification**.
4. Entrez des informations telles que le **Nom des informations d'authentification**, l'**Etiquette** et la **Description**.
5. Dans la partie **Informations d'authentification de Nutanix Prism Central** , ajoutez le **Nom d'utilisateur**, le **Mot de passe** et le **Domaine** du serveur Prism Central associé.

---

**Remarque :** Les informations d'authentification associées doivent correspondre à un utilisateur disposant du rôle d'administrateur Prism Central.

---

6 Cliquez sur **Suivant**.

Sélectionnez le rôle existant ou ajoutez un nouveau rôle pour fournir des autorisations pour les informations d'authentification.

7 Cliquez sur **Enregistrer**.

# Suppression de Nutanix Prism Central

Cette procédure permet de supprimer un ou plusieurs serveurs Nutanix Prism Central.

**Pour supprimer un serveur Nutanix Prism Central**

1 Dans la partie gauche, cliquez sur **Nutanix AHV**, puis sur l'onglet **Serveurs Prism Central**.

L'onglet affiche la liste des noms de serveurs Nutanix Prism Central auxquels vous avez accès.

2 Recherchez et sélectionnez un serveur AHV Prism Central.

3 Sélectionnez au moins un serveur Prism Central et cliquez sur **Actions > Supprimer**.

---

**Remarque :** Si vous supprimez un serveur Prism Central, toutes les machines virtuelles associées à ce serveur supprimé seront sauvegardées/récupérées sans attributs liés au réseau de cloud privé virtuel, au projet, à la catégorie et au propriétaire.

---

4 Désactivez la case à cocher **Désactivez l'option « Utiliser le serveur Prism Central pour ce cluster » pour tous les clusters associés au serveur Prism Central. Désélectionnez cette option si vous souhaitez la maintenir activée.** si nécessaire, puis cliquez sur **Supprimer**.

---

**Remarque :** Une fois le serveur Nutanix Prism Central supprimé, la découverte des biens ne sera pas déclenchée automatiquement pour les clusters de ce serveur Prism Central. Par conséquent, les machines virtuelles de ces clusters afficheront le serveur Prism Central et se projetteront sur la page de détails des machines virtuelles jusqu'à ce que la découverte de biens suivante soit déclenchée.

---

**Remarque :** Si un environnement comporte des clusters associés à ce serveur Prism Central et que la case **Utiliser le serveur Prism Central pour ce cluster** est cochée, lorsque le serveur Prism Central est supprimé en décochant la case **Désactivez l'option « Utiliser le serveur Prism Central pour ce cluster » pour tous les clusters associés au serveur Prism Central**, les travaux de sauvegarde ou de restauration suivants échouent jusqu'à l'ajout du serveur Prism Central associé.

# Création d'un groupe de machines virtuelles intelligent

Vous pouvez créer un groupe de machines virtuelles intelligent à partir d'un ensemble de filtres nommés requêtes. NetBackup sélectionne automatiquement des machines virtuelles en fonction de ces requêtes et les ajoute au groupe. Vous pouvez ensuite appliquer la protection au groupe. Un groupe intelligent reflète automatiquement les modifications apportées dans l'environnement des machines virtuelles, ce qui vous évite d'avoir à vérifier manuellement la liste des machines virtuelles du groupe.

**Remarque :** Une tâche en arrière-plan ajoute les machines virtuelles récemment découvertes et correspondant à la requête au groupe de machines virtuelles intelligent. Cette tâche en arrière-plan s'exécute 30 minutes après le démarrage du service NetBackup Web Management. Après cela, la tâche s'exécute toutes les 30 minutes.

**Pour créer un groupe de machines virtuelles intelligent**

1. Dans la partie gauche, cliquez sur **Nutanix AHV**.
2. Cliquez sur l'onglet **Groupes intelligents de VM**, puis sur **Ajouter un groupe intelligent de VM**.
3. Entrez un nom et une description pour le groupe.

   La longueur du nom affiché du groupe de machines virtuelles intelligent doit être comprise entre 1 et 256 caractères.
4. Dans le volet **Clusters**, cliquez sur **Ajouter des clusters**.

   **Remarque :** Vous ne pouvez créer un groupe que s'il existe au moins un cluster.

   - Dans la fenêtre **Ajouter des clusters**, sélectionnez les clusters à ajouter.

**Remarque :** Pour ajouter un cluster, vous devez disposer des autorisations d'affichage et de création sur ce cluster.

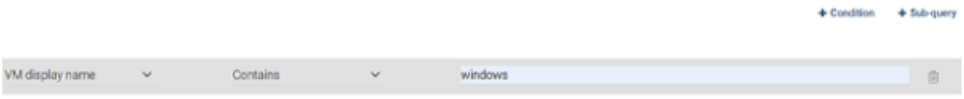
5 Effectuez l'une des opérations suivantes :

- Sélectionnez la requête par défaut : **Inclure toutes les machines virtuelles**. Lorsque le plan de protection s'exécute, toutes les machines virtuelles qui font partie des clusters AHV sont ajoutées au groupe de machines virtuelles intelligent.
- Pour créer votre propre requête : cliquez sur **Ajouter une condition**.

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

Les options sont décrites après cette procédure : Options de requête pour la création de groupes de machines virtuelles intelligents.

Voici un exemple de requête :




Dans cet exemple, la requête ajoute au groupe toute machine virtuelle dont le nom affiché contient le terme `windows`.

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 :


Dans cet exemple, nous utilisons **ET** pour limiter l'étendue de la requête : seules les machines virtuelles dont le nom affiché contient le terme `windows` et dont l'état d'alimentation est `ACTIVÉ` sont sélectionnées. Si le nom affiché d'une machine virtuelle ne contient pas `windows` et que son état d'alimentation est `ACTIVÉ`, elle n'est pas ajoutée au groupe.

Pour élargir la portée de la requête, utilisez **OU** :


Dans cet exemple, **OU** permet d'ajouter les machines virtuelles suivantes au groupe :

- Machines virtuelles dont le nom affiché contient `windows` (quel que soit leur état d'alimentation)
- Machines virtuelles dont l'état d'alimentation est `ACTIVÉ` (quel que soit leur nom affiché).

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

---

**Remarque :** Le processus de sélection par requête est dynamique. Les modifications qui ont lieu dans l'environnement virtuel peuvent avoir une incidence sur les machines virtuelles sélectionnées par la requête lors de l'exécution du plan de protection. En conséquence, les machines virtuelles que la requête sélectionne ultérieurement, lors de l'exécution du plan de protection, peuvent ne pas être identiques à celles figurant dans l'aperçu.

---

**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 machines virtuelles sont sélectionnées pour le groupe. Dans **Machines virtuelles**, si vous cliquez sur une machine virtuelle qui n'a pas été sélectionnée pour le groupe, le champ **Membre des groupes des machines virtuelles** affiche `Aucun`.

Cependant, quand vous ajoutez le groupe à un plan de protection, certaines des options de requête sont traitées comme n'étant pas sensibles à la casse lorsque la sauvegarde du plan de protection s'exécute. En conséquence, la même machine virtuelle peut maintenant être incluse dans le groupe et elle est sauvegardée.

Pour connaître le comportement relatif à la casse pour chaque option, consultez la rubrique suivante :

Options de requête pour la création de groupes de machines virtuelles intelligents

---

8 Pour enregistrer le groupe, cliquez sur **Ajouter et gérer les autorisations**.

**Remarque :** Vous pouvez modifier, protéger et gérer les autorisations pour ce groupe.

- Ajoutez un plan de protection :
  Se reporter à "Protection des machines virtuelles ou des groupes de machines virtuelles intelligents AHV" à la page 54.
- Modifiez ou mettez à jour le groupe de machines virtuelles intelligent :
  Se reporter à "Mise à jour du groupe de machines virtuelles intelligent" à la page 39.
- Attribuez des autorisations au groupe de machines virtuelles :
  Se reporter à "Attribution d'autorisations au groupe de machines virtuelles intelligent" à la page 39.

## Options de requête pour la création de groupes de machines virtuelles intelligents

**Tableau 2-4** Mots-clés de requête

| Mot-clé | Description |
|---|---|
| `displayName` | Nom affiché de la machine virtuelle.<br>Sensible à la casse lors de l'exécution du plan de protection. |
| `powerState` | État d'alimentation de la machine virtuelle.<br>ACTIVÉ et DÉSACTIVÉ sont sensibles à la casse. |
| `vmUuid` | UUID de l'instance de la machine virtuelle.<br>Par exemple : `501b13c3-52de-9a06-cd9a-ecb23aa975d1`<br>N'est pas sensible à la casse lors de l'exécution du plan de protection. |
| `StorageContainerName` | Nom du conteneur de stockage.<br>Sensible à la casse lors de l'exécution du plan de protection. |

| Mot-clé | Description |
|---|---|
| `Category` | Vérifiez que les conditions suivantes sont remplies :<br>La catégorie AHV est appliquée aux machines virtuelles sur le serveur Nutanix Prism Central. Pour une recherche complète, elle doit être au format **CategoryName:Value**. |

**Tableau 2-5** Opérateurs de requête

| Opérateur | Description |
|---|---|
| `Starts with` | Renvoie une correspondance lorsque la valeur apparaît au début d'une chaîne.<br>Par exemple : si la valeur entrée est `box`, cette option trouve une correspondance avec la chaîne `box_car`, mais pas avec `flatbox`. |
| `Ends with` | Renvoie une correspondance lorsque la valeur apparaît à la fin d'une chaîne.<br>Par exemple : si la valeur entrée est `dev`, cette option trouve une correspondance avec la chaîne `01dev`, mais pas avec `01dev99` ni `devOP`. |
| `Contains` | Recherche la valeur que vous entrez, où qu'elle apparaisse dans la chaîne.<br>Par exemple : si la valeur entrée est `dev`, cette option trouve une correspondance avec les chaînes `01dev`, `01dev99`, `devOP` et `development_machine`. |
| = | Renvoie uniquement les correspondances exactes avec la valeur que vous entrez.<br>Par exemple : si la valeur entrée est `VMtest27`, trouve une correspondance avec `VMTest27` (même casse), mais pas `vmtest27`, `vmTEST27` ni `VMtest28`. |
| != | Renvoie toute valeur qui n'est pas égale à celle que vous entrez. |

# Attribution d'autorisations au groupe de machines virtuelles intelligent

Points à considérer avant d'assigner des autorisations au groupe de machines virtuelles.

- **Afficher/Mettre à jour**
  - Tous les clusters du groupe ; vous devez avoir l'autorisation AFFICHER.
  - En l'absence de l'autorisation AFFICHER sur l'un des clusters, vous ne pourrez pas prévisualiser les machines virtuelles du groupe dans l'onglet **Machines virtuelles**.
  - Le cluster pour lequel vous n'avez pas cette autorisation s'affiche avec le symbole de cadenas.
  - Le cluster supprimé est accompagné du symbole **X**.
  - Pour ajouter un cluster au groupe de machines virtuelles existant, vous devez avoir l'autorisation AFFICHER pour le cluster voulu.
  - Pour mettre à jour le groupe de machines virtuelles, vous devez avoir l'autorisation AFFICHER correspondant au cluster. Cependant, vous pouvez supprimer un cluster non existant ou un cluster sans autorisation AFFICHER.
- **Protéger**
  - Tous les clusters du groupe doivent disposer de l'autorisation PROTÉGER.
  - Pour protéger un groupe de machines virtuelles, vous devez avoir l'autorisation PROTÉGER sur tous les clusters du groupe, ainsi que sur le groupe de machines virtuelles.
  - En l'absence de l'autorisation PROTÉGER sur tous les clusters, la fonction **Sauvegarder maintenant** est désactivée.
  - L'option **Supprimer la protection** est activée indépendamment des autorisations sur les clusters. Elle dépend uniquement des autorisations portant sur le groupe de machines virtuelles.

Consultez le Guide de l'administrateur de l'interface utilisateur Web NetBackup pour plus de détails sur les autorisations de rôles.

# Mise à jour du groupe de machines virtuelles intelligent

Vous pouvez modifier un groupe de machines virtuelles intelligent.

**Pour modifier un groupe de machines virtuelles intelligent**

1. Dans la partie gauche, cliquez sur **Nutanix AHV**.
2. Cliquez sur l'onglet **Groupes intelligents de VM** et sélectionnez le groupe de machines virtuelles à modifier.
3. Dans l'onglet **Machine virtuelle**, cliquez sur **Modifier**.

   Dans le volet **Clusters**, cliquez sur **Ajouter des clusters**.

---

**Remarque :** Vous pouvez supprimer ou ajouter des groupes de machines virtuelles. Pour ajouter un groupe de machines virtuelles intelligent, consultez la section Se reporter à "Création d'un groupe de machines virtuelles intelligent" à la page 34..

---

# Suppression d'un groupe de machines virtuelles intelligent

Procédez comme suit pour supprimer un groupe de machines virtuelles intelligent.

**Pour supprimer un groupe de machines virtuelles intelligent**

1. Dans la partie gauche, cliquez sur **Nutanix AHV**.
2. Recherchez le groupe sous l'onglet **Groupes intelligents de VM**.
3. Si le groupe n'est pas protégé, cliquez sur sa case à cocher et cliquez sur **Supprimer**.
4. Si le groupe est protégé, cliquez dessus, faites défiler et cliquez sur le verrou, puis cliquez sur **Désabonner**.
5. Cliquez sur **Supprimer**.

# Définition des paramètres CHAP pour iSCSI

Les paramètres CHAP s'appliquent à tous les clusters AHV configurés dépendant du serveur principal sélectionné. La configuration par défaut est CHAP à sens unique.

---

**Remarque :** Pour l'option CHAP à sens unique, aucune action n'est requise.

---

**Pour activer l'option CHAP mutuel :**

1. Dans le volet gauche, cliquez sur **Nutanix AHV**.
2. En haut à droite, sélectionnez **Paramètres  AHV > CHAP for iSCSI** et sélectionnez l'option CHAP mutuel appropriée.

---

**Remarque :** Pour l'option CHAP mutuel, le système de gestion des informations d'authentification de NetBackup génère automatiquement les informations d'authentification avec le préfixe `AHV_ISCSI_MUTUAL_AUTO_` pour l'hôte de sauvegarde ou de récupération sélectionné. Les informations d'authentification CHAP mutuel pour iSCSI sont visibles dans l'onglet **Gestion des informations d'authentification**.

---

**Remarque :** Par défaut, les informations d'authentification générées automatiquement pour l'option CHAP mutuel ne sont pas visibles pour les utilisateurs créés par le rôle Administrateur AHV par défaut. L'administrateur de sécurité/utilisateur racine doit autoriser l'utilisateur à afficher ces informations d'authentification.

Elles sont générées automatiquement dans l'onglet **Gestion des informations d'authentification** et ne peuvent pas être modifiées ; elles peuvent seulement être supprimées. Elles sont recréées manuellement en cas de suppression manuelle lors de l'exécution du travail suivant pour lequel elles ont été générées.

---

# Ajout d'un hôte d'accès AHV

NetBackup utilise un hôte spécial appelé hôte d'accès AHV. Il s'agit d'un client NetBackup qui effectue des sauvegardes pour le compte des machines virtuelles. L'hôte d'accès est le seul hôte pourvu d'un logiciel de serveur de médias ou d'un logiciel client NetBackup. Le logiciel client NetBackup est requis sur les machines virtuelles. Cependant, l'hôte d'accès doit avoir accès au conteneur de stockage des machines virtuelles. L'hôte d'accès lit les données du conteneur de stockage et les envoie au serveur de médias par l'intermédiaire du réseau.

L'hôte d'accès AHV s'appelait précédemment « hôte de sauvegarde AHV ». L'hôte d'accès est appelé hôte de récupération lorsqu'il effectue une restauration.

---

**Remarque :** Assurez-vous que le logiciel client ou le logiciel de serveur de médias NetBackup est installé sur tous les hôtes d'accès que vous ajoutez.

---

**Pour ajouter un hôte d'accès AHV**

1. Dans le volet gauche, cliquez sur **Nutanix AHV**.
2. En haut à droite, sélectionnez **Paramètres AHV > Hôtes d'accès**.

   NetBackup répertorie tous les hôtes d'accès qui ont été ajoutés précédemment.
3. Cliquez sur **+ Ajouter**.
4. Entrez le `nom/nom de domaine complet/IP` de l'hôte d'accès et cliquez sur **Ajouter**.

# Suppression d'un hôte d'accès AHV

**Pour supprimer un hôte d'accès AHV**

1. Dans la partie gauche, cliquez sur **Nutanix AHV**.
2. Dans la partie droite, sélectionnez **Paramètres AHV > Hôtes d'accès**.

   NetBackup répertorie tous les hôtes d'accès qui ont été ajoutés précédemment.
3. Recherchez l'hôte d'accès AHV, puis cliquez sur l'icône de suppression.
4. Pour confirmer la suppression, cliquez sur **Supprimer**.

# Modification des limites de ressource pour les types de ressource AHV

Les limites des ressources Nutanix AHV contrôlent le nombre de sauvegardes simultanées qui peuvent être effectuées sur des ressources Nutanix AHV. Les paramètres s'appliquent à toutes les politiques NetBackup pour le serveur principal sélectionné.

Limites de ressource disponibles pour Nutanix AHV :

- **Travaux de sauvegarde par hôte**
- **Travaux de sauvegarde par cluster AHV**
- **Travaux de sauvegarde par conteneur de stockage**
- **Travaux de snapshots par cluster AHV**

---

**Remarque :** Pour chaque type de ressource, la valeur par défaut est 0 (aucune limite).

---

**Pour définir des limites de ressource pour les ressources Nutanix AHV**

1. Dans la partie gauche, cliquez sur **Nutanix AHV**.
2. Dans la partie supérieure droite, cliquez sur **Paramètres AHV > Limites des ressources**.

   Pour chaque type de ressource, la valeur par défaut est **0** (aucune limite).

   ---

   **Remarque :** L'option **Travaux de snapshots par cluster AHV** définit une limite pour le nombre d'opérations de snapshot simultanées par cluster. Elle s'applique uniquement à la phase de création de snapshot d'une sauvegarde. Elle ne contrôle pas le nombre de travaux de sauvegarde simultanés. Ce paramètre contrôle l'effet de plusieurs opérations de snapshot sur le cluster AHV. Pour remplacer le paramètre global de snapshot pour ce cluster AHV, ajoutez un cluster AHV spécifique.

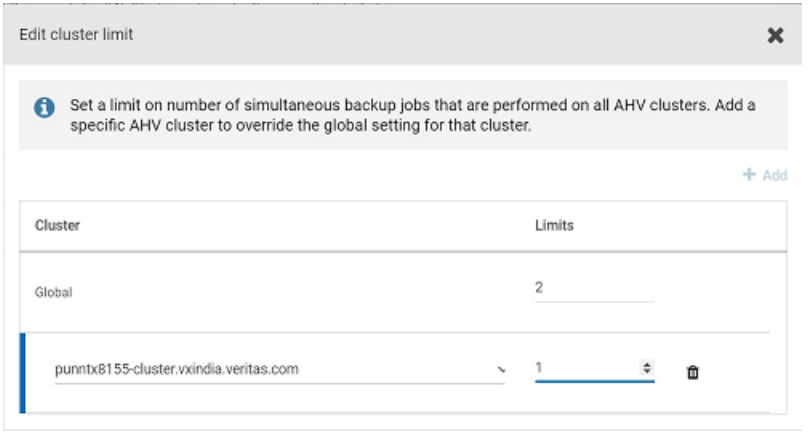
   ---

3. Recherchez la ressource AHV à modifier, puis cliquez sur **Modifier**.

**4** Sélectionnez l'une des options suivantes.

| | |
|---|---|
| Définissez une limite globale pour un type de ressource AHV. | Recherchez le paramètre **Global** et sélectionnez la valeur **Limites** que vous souhaitez appliquer.<br>Cette valeur limite le nombre de sauvegardes simultanées qui peuvent être effectuées pour le type de ressource. |
| Définissez une limite pour une ressource AHV spécifique. | Cliquez sur **Ajouter**.<br>Dans la liste, sélectionnez la ressource.<br>Sélectionnez la valeur **Limites** à appliquer.<br>Cette valeur limite le nombre de sauvegardes simultanées qui peuvent être effectuées pour la ressource sélectionnée. |

L'exemple suivant affiche une limite globale de **2** pour tous les clusters AHV et une limite de **1** pour le cluster AHV sélectionné.




**5** Cliquez sur **Enregistrer**.

La valeur **Limites** indique le nombre de sauvegardes simultanées qui peuvent être effectuées pour le type de ressource. Il s'agit de la limite globale. La valeur **Remplacer** indique le nombre de ressources dont les limites sont différentes de la limite globale.

**Remarque :** les limites de ressource définies n'entrent en vigueur qu'après l'exécution de quelques travaux.

## Réinitialisation des limites pour toutes les ressources AHV

**Pour réinitialiser les limites de toutes les ressources AHV**

- Cliquez sur **Réinitialiser les valeurs par défaut** pour éliminer tous les remplacements et rétablir les valeurs par défaut des paramètres de limite globale des ressources AHV.

## Exemple : définition des limites de ressource pour un cluster Nutanix à deux nœuds

Considérez l'exemple suivant :

- Le cluster Nutanix comporte deux nœuds.
- Chaque nœud héberge 40 machines virtuelles, soit 80 au total dans le cluster.
- La politique **Nutanix AHV** comporte 20 machines virtuelles.

Quand NetBackup se connecte à l'environnement Nutanix pour la sauvegarde, il établit une connexion par machine virtuelle. Si aucune limite de ressource n'est définie, un total de 160 travaux s'exécute en même temps (80 snapshots + 80 sauvegardes). Consultez cet article.

Nutanix recommande de ne pas établir plus de 20 connexions simultanément par CVM dans le cluster, ce qui signifie que 20 machines virtuelles par nœud sont sauvegardées en même temps. Dans notre exemple, vous pouvez appliquer une limite de 20 connexions avec les paramètres suivants :

| | |
|---|---|
| **Travaux de sauvegarde par nœud** | **20** |
| **Travaux de sauvegarde par cluster** | **40** |
| **Travaux de sauvegarde par conteneur de stockage** | Définissez les limites en fonction des caractéristiques de la technologie de stockage. |
| **Travaux de snapshots par cluster** | **10** |

Quand une sauvegarde commence, le moniteur d'activité affiche les travaux comme suit :

- Travaux de snapshot : 20
- Travaux actifs : 10 (travaux de snapshot et leurs travaux de sauvegarde)
- Travaux en file d'attente : 10
- Une fois les travaux de snapshot actifs terminés, les travaux de snapshot en file d'attente deviennent actifs à leur tour.

# Modification de la fréquence de la découverte automatique des biens AHV

La découverte automatique des biens AHV se produit à intervalles réguliers. La fréquence par défaut est de 8 heures. Procédez comme suit pour modifier la fréquence de la découverte automatique.

**Pour modifier la fréquence de la découverte automatique des biens AHV**

1. Dans la partie gauche, cliquez sur **Charges de travail > Nutanix AHV**.
2. Dans la partie droite, sélectionnez **Paramètres AHV > Découverte automatique**.
3. Sélectionnez **Fréquence > Modifier**.
4. Utilisez les flèches haut ou bas pour choisir la fréquence de découverte automatique des biens AHV par NetBackup. Ensuite, cliquez sur **Enregistrer**.

   La plage disponible est comprise entre 1 et 24 heures. Pour définir la fréquence de la découverte automatique en minutes ou en secondes, ou pour la désactiver, vous devez utiliser l'API de découverte automatique AHV.

Chapitre 3

# Gestion des informations d’authentification

Ce chapitre traite des sujets suivants :



## Gestion des informations d’authentification de cluster AHV

Cette section décrit les procédures d’ajout, de mise à jour et de validation des informations d’authentification du cluster AHV.

### Ajout d’informations d’authentification relatives au cluster

1. Sur la gauche, cliquez **Nutanix AHV**, puis sur l’onglet **Cluster AHV**.
2. Cliquez sur **Ajouter** pour ajouter un nouveau cluster.
3. Sur la page **Ajouter un cluster AHV > Associer des informations d’authentification**, cliquez sur **Ajouter de nouvelles informations d’authentification**.
4. Sur la page **Ajouter des informations d’authentification**, entrez des informations telles que le **nom des informations d’authentification**, le **nom d’utilisateur** et le **mot de passe**.

5 Cliquez sur **Suivant**.

Sélectionnez ou ajoutez des rôles afin d'octroyer des autorisations pour les informations d'authentification.

6 Cliquez sur **Enregistrer**.

---

**Remarque :** Vous pouvez **Modifier** ou **Supprimer** les informations d'authentification que vous avez ajoutées.

---

## Mise à jour et validation des informations d'authentification du cluster AHV

**Pour valider les informations d'authentification AHV**

1 Dans la partie gauche, cliquez sur **Nutanix AHV**, puis sur l'onglet **Clusters AHV**.

2
- Pour valider les informations d'authentification d'un cluster donné, localisez et sélectionnez le cluster AHV. Cliquez ensuite sur **Valider** dans la colonne **Informations d'authentification** ou dans la barre supérieure.
- Pour valider les informations d'authentification de plusieurs serveurs simultanément, localisez et sélectionnez le cluster AHV. Cliquez ensuite sur **Valider** dans la barre supérieure.

---

**Remarque :** NetBackup vérifie les informations d'authentification actuelles du cluster AHV sélectionné.

Si les informations d'authentification ne sont pas valides, NetBackup indique **Non valide** sous **Informations d'authentification**. Suivez les étapes ci-dessous pour mettre à jour les informations d'authentification du cluster AHV.

---

**Pour mettre à jour les informations d'authentification du cluster AHV**

1 Sur la gauche, cliquez **Nutanix AHV**, puis sur l'onglet **Cluster AHV**.

2 Recherchez et sélectionnez le cluster AHV.

3 Sélectionnez **Actions > Modifier**.

4 Le cas échéant, mettez à jour les informations d'authentification.

---

**Remarque :** Lorsque vous ajoutez ou mettez à jour des informations d'authentification du cluster AHV, la découverte du cluster AHV démarre automatiquement. Lorsque les informations sur l'hôte de sauvegarde sont fournies dans la requête, elles sont utilisées pour valider les informations d'authentification et procéder à la découverte. Pour la découverte, NetBackup 9.1 est la version minimale prise en charge pour un client ou serveur de médias NetBackup utilisé en tant qu'hôte de sauvegarde.

---

5 Cliquez sur **Enregistrer**.

NetBackup vérifie les informations d'authentification mises à jour pour le cluster AHV sélectionné.

# Gestion des informations d'authentification pour Nutanix Prism Central

Cette section décrit les procédures d'ajout, de mise à jour et de validation des informations d'authentification du serveur Nutanix Prism Central.

## Ajout de nouvelles informations d'authentification pour Nutanix Prism Central

1 Dans la partie gauche, cliquez sur **Nutanix AHV**, puis sur l'onglet **Serveurs Prism Central**.

2 Cliquez sur **Ajouter** pour ajouter un nouveau serveur Prism Central.

3 Sur la page **Ajouter un serveur AHV Prism Central > Associer des informations d'authentification**, cliquez sur **Ajouter de nouvelles informations d'authentification**.

4 Sur la page **Ajouter des informations d'authentification**, entrez des informations telles que le **nom des informations d'authentification**, le **nom d'utilisateur** et le **mot de passe**.

5 Cliquez sur **Suivant**.

Sélectionnez ou ajoutez des rôles afin d'octroyer des autorisations pour les informations d'authentification.

6 Cliquez sur **Enregistrer**.

---

**Remarque :** Vous pouvez **Modifier** ou **Supprimer** les informations d'authentification que vous avez ajoutées.

---

## Mise à jour et validation des informations d'authentification Nutanix Prism Central

**Pour valider les informations d'authentification du serveur Prism Central**

1 Dans la partie gauche, cliquez sur **Nutanix AHV**, puis sur l'onglet **Serveurs Prism Central**.

2
- Pour valider des informations d'authentification de serveurs Prism Central spécifiques, localisez et sélectionnez le serveur Prism Central. Cliquez ensuite sur **Valider** dans la colonne **Informations d'authentification** ou dans la barre supérieure.
- Pour valider les informations d'authentification de plusieurs serveurs simultanément, localisez et sélectionnez les serveurs Prism Central. Cliquez ensuite sur **Valider** dans la barre supérieure.

---

**Remarque :** NetBackup vérifie les informations d'authentification actuelles pour les serveurs Prism Central sélectionnés.

Si les informations d'authentification ne sont pas valides, NetBackup indique **Non valide** sous **Informations d'authentification**. Suivez la procédure suivante pour mettre à jour les informations d'authentification du serveur Prism Central.

---

**Pour mettre à jour les informations d'authentification pour le serveur Prism Central**

1 Dans la partie gauche, cliquez sur **Nutanix AHV**, puis sur l'onglet **Serveurs Prism Central**.

2 Recherchez et sélectionnez un serveur Prism Central.

3 Sélectionnez **Actions > Modifier**.

4 Le cas échéant, mettez à jour les informations d'authentification.

---

**Remarque :** L'ajout ou la mise à jour des informations d'authentification du serveur Prism Central démarre également automatiquement la découverte du serveur Prism Central. Lorsque les informations sur l'hôte de sauvegarde sont fournies dans la requête, elles sont utilisées pour valider les informations d'authentification et procéder à la découverte. Pour la découverte, NetBackup 9.1 est la version minimale prise en charge pour un client ou serveur de médias NetBackup utilisé en tant qu'hôte de sauvegarde.

---

5 Cliquez sur **Enregistrer**.

NetBackup vérifie les informations d'authentification mises à jour pour le serveur Prism Central sélectionné.

# Affichage du nom des informations d'authentification appliquées à un bien

Vous pouvez afficher les informations d'authentification nommées qui sont configurées pour un type de bien. Si les informations d'authentification ne sont pas configurées pour un bien spécifique, ce champ reste vide.

**Pour afficher les informations d'authentification des clusters Nutanix AHV**

1 Sur la gauche, sélectionnez **Charges de travail > Nutanix AHV**.

2 Dans l'onglet **Clusters AHV**, localisez la colonne **Nom des informations d'authentification**.

# Modification ou suppression d'informations d'authentification nommées

Vous pouvez modifier les propriétés d'informations d'authentification nommées ou supprimer des informations d'authentification nommées NetBackup à partir de la **gestion des informations d'authentification**.

## Modification des informations d'authentification nommées

Vous pouvez modifier des informations d'authentification nommées pour modifier les éléments suivants : étiquette des informations d'authentification, description, catégorie, détails ou autorisations. Vous ne pouvez pas modifier le nom des informations d'authentification.

**Remarque :** Assurez-vous que la catégorie d'informations d'authentification utilisée pour le **cluster AHV** est *AHV* et **Prism Central** pour *Nutanix Prism Central*.

**Pour modifier des informations d'authentification nommées**

1. Sur la gauche, cliquez sur **Gestion des informations d'authentification**.
2. Dans l'onglet **Informations d'authentification nommées**, cliquez sur les informations d'authentification à modifier.
3. Cliquez sur **Modifier** et mettez à jour les informations d'authentification.
4. Vérifiez les modifications et cliquez sur **Terminer**.

## Suppression d'informations d'authentification nommées

Vous pouvez supprimer des informations d'authentification nommées dont vous n'avez plus besoin avec NetBackup. Assurez-vous d'appliquer d'autres informations d'authentification à tous les biens qui utilisent les informations d'authentification que vous voulez supprimer. Sinon, les sauvegardes et les restaurations peuvent échouer pour ces biens.

**Pour supprimer des informations d'authentification nommées**

1. Sur la gauche, cliquez sur **Gestion des informations d'authentification**.
2. Dans l'onglet **Informations d'authentification nommées**, cliquez sur les informations d'authentification à supprimer.
3. Cliquez sur **Supprimer**.

Chapitre 4

# Protection des machines virtuelles AHV

Ce chapitre traite des sujets suivants :



## Points à savoir avant de protéger les machines virtuelles AHV

Pendant la création d'un plan de protection, certaines validations doivent être prises en considération :

- Si le type de planification est Automatique, assurez-vous que toutes les versions de NetBackup sont telles que mentionnées :

- Les planifications incrémentielles sont uniquement prises en charge pour l'hôte de sauvegarde 8.3 ou version ultérieure.
- Si vous utilisez un ordinateur Windows comme hôte de sauvegarde, assurez-vous que sa version est au moins 9.1.
- Si vous voulez utiliser l'option Activer la suspension de la machine virtuelle, assurez-vous que la version de l'hôte de sauvegarde est 9.1 ou une version ultérieure.
- Si un attribut de catégorie est défini comme filtre pour le groupe de machines virtuelles intelligent, l'hôte de sauvegarde doit disposer de la version 10.4 ou d'une version ultérieure.

- Pour protéger les attributs de machines virtuelles associés à Nutanix Prism Central, la configuration de Nutanix Prism Central est requise.

---

**Remarque :** Pour protéger les attributs de machine virtuelle associés à Nutanix Prism Central, assurez-vous que la version de l'hôte NetBackup est la version 10.1.1 ou une version ultérieure.

---

# Protection des machines virtuelles ou des groupes de machines virtuelles intelligents AHV

Procédez comme suit pour abonner des biens, qu'il s'agisse de machines virtuelles ou de groupes de machines virtuelles intelligents AHV, 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 à gérer et aux plans de protection à utiliser. Si vous devez protéger un groupe de machines virtuelles intelligent, assurez-vous que tous les clusters qui forment ce groupe disposent de l'autorisation de protection.

---

**Pour protéger les machines virtuelles ou les groupes de machines virtuelles AHV**

1. Dans le volet gauche, cliquez sur **Nutanix AHV**.
2. Dans l'onglet **Machines virtuelles** ou **Groupes intelligents de VM**, cochez les cases des machines virtuelles ou des groupes de machines virtuelles, 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**
  Changez la fenêtre de démarrage de la sauvegarde.
- **Options de sauvegarde**
  Sélectionnez le serveur ou l'hôte à utiliser pour les sauvegardes.

---

**Remarque :** Si l'option **Automatique** est sélectionnée ici et que ce plan de protection est utilisé pour protéger des groupes intelligents de machines virtuelles pour lesquels une catégorie est définie comme filtre, assurez-vous de disposer au moins d'un serveur de médias doté de la version 10.4 ou d'une version ultérieure associé à l'unité de stockage.

---

- **Options avancées**
  Activez la suspension de la machine virtuelle pour le plan de protection.

5 Cliquez sur **Protéger**.

Les résultats de vos choix apparaissent dans **Machines virtuelles** ou **Groupes de machines virtuelles intelligents**.

# Protection des machines virtuelles AHV dans un VPC

NetBackup 10.2 permet de protéger les machines virtuelles hébergées sur un réseau privé virtuel sur le serveur Nutanix Prism Central. NetBackup protège également les attributs suivants des machines virtuelles à l'aide du serveur Nutanix Prism Central configuré.

- **Projet** : ensemble d'utilisateurs ayant un ensemble commun de conditions requises ou une structure et une fonction communes. Les projets permettent d'effectuer des regroupements logiques de rôles d'utilisateur pour gérer l'utilisation des ressources.
- **Catégories associées** : une catégorie est un regroupement d'entités qui forme une paire valeur-clé. En règle générale, les nouvelles entités sont attribuées à une catégorie en fonction de certains critères. Les politiques peuvent ensuite être associées aux entités auxquelles une valeur de catégorie spécifique est attribuée (regroupement par catégorie) .
- **Attributs de réseau VPC** : adresses IP principales et secondaires attribuées aux machines virtuelles dans un VPC.

- **Propriétaire du projet** : utilisateur/propriétaire du projet sur lequel CALM est déployé conjointement dans le serveur Nutanix Prism Central.

**Pour protéger des machines virtuelles sur un VPC**

1 Configurez Nutanix Prism Central.

---

**Remarque :** Pour un cluster configuré, NetBackup utilise Nutanix Prism Central pour protéger des attributs supplémentaires de la machine virtuelle uniquement si la case **Utiliser Prism Central** est cochée.

---

Se reporter à " Ajout d'un nouveau serveur Nutanix Prism Central " à la page 31.

2 Cochez la case **Utiliser Prism Central** pour ajouter tous les clusters Nutanix AHV dans NetBackup.

Se reporter à "Ajout ou parcours d'un cluster AHV" à la page 25.

3 Pour obtenir des informations complètes sur la protection des machines virtuelles, consultez la section suivante :

Se reporter à "Protection des machines virtuelles ou des groupes de machines virtuelles intelligents AHV" à la page 54.

---

**Remarque :** Si vous définissez l'option Sélectionner le serveur ou l'hôte à utiliser pour les sauvegardes sur **Automatique** dans un plan de protection et si l'unité de stockage est associée à un serveur de médias doté d'une version de NetBackup antérieure à la 10.2, le travail de sauvegarde risque d'utiliser l'ancien serveur de médias comme hôte de sauvegarde.

Dans ce cas, le travail de sauvegarde s'exécute sans protéger les attributs Nutanix Prism Central.

---

# Personnaliser les paramètres de protection pour un bien AHV

Vous pouvez modifier certains paramètres d'un plan de protection, notamment les planifications.

**Pour personnaliser les paramètres de protection pour un bien AHV**

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

2 Effectuez l'une des opérations suivantes :

- Modification des paramètres pour une machine virtuelle

Dans l'onglet **Machines virtuelles**, cliquez sur la machine virtuelle à modifier.

- Modification des paramètres pour un groupe de machines virtuelles intelligent
  Dans l'onglet **Groupes intelligents de VM**, cliquez sur le groupe à modifier.

3. Cliquez sur **Protection personnalisée > Continuer**.
4. Vous pouvez modifier les paramètres suivants :
   - Fenêtre de démarrage de la restauration
     Se reporter à "Planifications et conservation" à la page 57.
   - **Options de sauvegarde**
     Se reporter à "Options de sauvegarde" à la page 57.
5. Cliquez sur **Protéger**.

# Planifications et conservation

- Fenêtre de démarrage.
  - Définissez la fenêtre de démarrage d'une sauvegarde.

# Options de sauvegarde

L'utilisateur peut définir les paramètres suivants pour s'abonner à un plan de protection.

1 Sélectionnez le serveur ou l'hôte en tant qu'hôte d'accès à utiliser pour les sauvegardes.

Hôte qui exécute les sauvegardes pour le compte des machines virtuelles. Les utilisateurs peuvent choisir l'option Automatique pour laisser NetBackup sélectionner le serveur de médias en fonction de l'unité de stockage. L'utilisateur peut également sélectionner un autre hôte dans la liste. Ces hôtes sont d'autres serveurs de médias dans l'environnement ou des hôtes configurés en tant qu'hôtes d'accès.

---

**Remarque :** Pendant la sauvegarde d'une machine virtuelle avec une version d'hôte de sauvegarde antérieure à 9.1, si la machine virtuelle ayant le même UUID existe dans un cluster différent. La colonne d'état **Dernière sauvegarde correcte** pour cette machine virtuelle n'est pas mise à jour. Cependant, la sauvegarde de la machine virtuelle est correcte et vous pouvez afficher des points de récupération et procéder à la récupération.

---

2 **Options avancées**

Pour l'activation, Se reporter à "Conditions requises pour activer la suspension de machine virtuelle" à la page 58.

- **Activer la suspension de la machine virtuelle**
- **Activer les snapshots non suspendus en cas d'échec des snapshots suspendus**

Par défaut, les E/S de la machine virtuelle sont suspendues avant que NetBackup ne crée le snapshot. Dans la majorité des cas, vous devez utiliser ce paramètre par défaut. Si l'activité des fichiers n'est pas suspendue, la cohérence des données dans le snapshot ne peut pas être garantie. Si vous désactivez la mise en veille, vous devez analyser les données de sauvegarde par souci de cohérence.

# Conditions requises pour activer la suspension de machine virtuelle

- Par défaut, la fonction NGT (Nutanix Guest Tools) est désactivée pour les machines virtuelles s'exécutant dans un cluster Nutanix. Nutanix recommande d'installer NGT et, dans certains cas, de prévoir des scripts pre-freeze et post-thaw sur la machine virtuelle si vous devez créer des snapshots cohérents au niveau de l'application pour activer la suspension de la machine virtuelle.

**Remarque :** Les sauvegardes cohérentes au niveau application nécessitent la version 9.1 ou une version ultérieure du serveur de médias NetBackup.

- Pour installer NGT et ajouter des scripts, consultez cette page.

# Suppression de la protection de machines virtuelles ou de groupes intelligents de machines virtuelles

Vous pouvez désabonner des machines virtuelles ou des groupes de machines virtuelles intelligents d'un plan de protection. Quand le bien est désabonné, les sauvegardes ne sont plus effectuées.

**Remarque :** Lorsque vous désabonnez un bien d'un plan de protection, il est possible que le bien affiche **Politique classique** dans la colonne **Protégé par** de l'interface utilisateur Web. Cela peut se produire lorsqu'un bien est abonné à un plan de protection et qu'une sauvegarde est exécutée pour ce bien. Le bien est alors désabonné du plan de protection, mais dispose toujours d'une image de sauvegarde valide. L'interface utilisateur Web affiche la **Politique classique**, mais il se peut qu'il n'existe aucune politique active protégeant le bien.

**Pour supprimer la protection de machines virtuelles ou de groupes de machines virtuelles intelligents**

1. Dans la partie gauche, cliquez sur **Nutanix AHV**.
2. Dans l'onglet **Machines virtuelles** ou **Groupes intelligents de VM**, sélectionnez la machine virtuelle ou le groupe de machines virtuelles intelligent.
3. Cliquez sur **Supprimer la protection > Oui**.

   Dans la section **Machines virtuelles** ou **Groupe de VM intelligentes**, le bien apparaît désormais comme **Non protégé**.

# Affichage de l'état de protection des machines virtuelles ou des groupes de machines virtuelles intelligents

Vous pouvez afficher les plans de protections utilisés pour protéger les machines virtuelles ou les groupes intelligents de machines virtuelles.

**Pour afficher l'état de protection des machines virtuelles ou des groupes de machines virtuelles intelligents**

1. Dans la partie gauche, cliquez sur **Nutanix AHV**.
2. Dans l'onglet **Machines virtuelles** ou **Groupes intelligents de VM**, sélectionnez la machine virtuelle ou le groupe de machines virtuelles intelligent.

   L'onglet **Protection** affiche les informations relatives aux plans d'abonnement du bien.

   ---

   **Remarque :** Si le bien a été sauvegardé alors que son état indique le contraire, consultez la section Se reporter à "Erreurs d'état d'une machine virtuelle nouvellement découverte" à la page 98..

   ---

3. Si le bien n'est pas protégé, cliquez sur **Ajouter la protection** pour sélectionner un plan de protection.

   Se reporter à "Protection des machines virtuelles ou des groupes de machines virtuelles intelligents AHV" à la page 54.

Chapitre 5

# Récupération des machines virtuelles AHV

Ce chapitre traite des sujets suivants :

# Points à considérer avant de récupérer les machines virtuelles AHV

Assurez-vous que l'hôte de récupération ou de sauvegarde peut communiquer avec le cluster AHV et le serveur Prism Central (s'il est installé) via le port 9440.

# À propos de la vérification de pré-récupération

La vérification de pré-récupération vérifie les points suivants :

- Utilisation de caractères pris en charge et de la longueur dans le nom affiché.
- Existence d'une machine virtuelle portant le même nom affiché.
- Connectivité avec le serveur AHV et validation des informations d'authentification AHV.
- Disponibilité du cluster AHV.
- Espace disponible avec le conteneur de stockage.

# Récupération d'une machine virtuelle AHV

Vous pouvez récupérer une machine virtuelle à son emplacement de sauvegarde d'origine ou à un autre emplacement. Vous pouvez choisir de la récupérer à partir de la copie par défaut de l'image de sauvegarde ou d'une autre copie, s'il en existe une. La copie par défaut est également connue comme la copie principale.

**Pour récupérer une machine virtuelle**

1. Dans la partie gauche, cliquez sur **Nutanix AHV**.
2. Recherchez la machine virtuelle et cliquez dessus.
3. Cliquez sur l'onglet **Points de récupération**. Dans la vue de calendrier à gauche, cliquez sur la date à laquelle la sauvegarde a été réalisée (indiquée par un point vert).

   Les images disponibles sont répertoriées sur des lignes et sont accompagnées d'un horodatage de sauvegarde.
4. Sur l'image à récupérer, sélectionnez l'une des options de récupération d'image suivantes :

   - **Récupérer**
     Permet d'effectuer une récupération à partir de la copie par défaut de l'image de sauvegarde.

- **Récupération à partir de la copie par défaut**
  Permet d'effectuer une récupération à partir de la copie par défaut de l'image de sauvegarde. Cette option s'affiche si plusieurs copies existent.
- **nn copies**
  Effectue une récupération à partir de la copie par défaut ou d'une copie différente de l'image de sauvegarde. NetBackup permet de réaliser jusqu'à 10 copies de la même image de sauvegarde. Toutes les copies disponibles sont affichées quand vous sélectionnez cette option. Pour chaque copie, le **nom de stockage**, le **serveur de stockage** et le **type de serveur de stockage** s'affichent. Cliquez sur **Récupérer** pour la copie à récupérer.

**5** Vérifiez les valeurs **Restaurer vers** dans **Cible de la récupération**.

Les valeurs par défaut proviennent de l'image de sauvegarde de la machine virtuelle.

- Pour récupérer les données à un autre emplacement, modifiez le cluster par défaut dans l'option **Restaurer**. Cliquez ensuite sur **Suivant**.

---

**Remarque :** Vous devez avoir les autorisations **Afficher** et **Afficher la cible de restauration** sur le conteneur de stockage ou le cluster pour inclure le conteneur de stockage prévu dans la liste déroulante cible.

---

**6** Vérifiez ou modifiez les valeurs des **options de récupération**.

| | |
|---|---|
| **Autoriser le remplacement de la machine virtuelle existante** | Supprime toute machine virtuelle qui possède le même nom affiché et qui existe à l'emplacement. Cette machine virtuelle doit être supprimée avant le début de la récupération. Sinon, la récupération échoue. |
| **Mettre sous tension après récupération** | Met automatiquement la machine virtuelle sous tension lorsque la récupération est terminée. |
| **Hôte de récupération** | Indiquez l'hôte à utiliser pour la récupération. Par défaut, l'hôte de récupération est celui qui a réalisé la sauvegarde. |
| **Créer un nouvel ID de machine virtuelle pour remplacer l'existant** | Créez un nouvel ID de machine virtuelle, différent de la valeur définie lors de la sauvegarde.<br>**Remarque :** L'ID de la machine virtuelle correspond à son UUID. |
| **Restaurer la machine virtuelle à partir d'un snapshot** | Permet de restaurer la machine virtuelle à partir d'un snapshot.<br>**Remarque :** Si aucun snapshot n'est disponible, la machine virtuelle est restaurée à partir de l'image de sauvegarde. |

7 Vérifiez ou modifiez les options **avancées**.

| | |
|---|---|
| **Supprimer des interfaces réseau** | Supprimez les interfaces réseau définies pour la machine virtuelle lors de la sauvegarde. |
| **Conserver l'adresse MAC** | Conservez l'adresse MAC définie pour la machine virtuelle lors de la sauvegarde. |

8 Cliquez sur **Suivant** pour exécuter la **Vue d'ensemble de la récupération**.

Cette option permet d'exécuter la vérification de pré-récupération avec les valeurs fournies sur les pages Cible de la récupération et Options de récupération. Vérifie la connectivité et l'existence d'un cluster AHV et de conteneurs de stockage. Détermine si le conteneur de stockage a de l'espace disponible et vérifie les autres spécifications.

Se reporter à "Vérifications de pré-récupération pour Nutanix AHV" à la page 87.

9 Cliquez sur **Lancer la récupération**.

10 Cliquez sur l'onglet **Restaurer l'activité** pour surveiller la progression d'un travail. Sélectionnez un travail spécifique pour en afficher les informations.

# Récupération d'une machine virtuelle AHV dans un VPC

La récupération des machines virtuelles sur un VPC est soumise à certaines limitations répertoriées ci-dessous :

- Les restaurations sur un autre client aboutissent si la case **Supprimer des interfaces réseau** est cochée. Cependant, des attributs tels que le projet, la catégorie, les informations sur le propriétaire et les informations liées au VPC ne sont pas restaurés.
- Si un réseau était configuré sur la machine virtuelle lors du déclenchement de la sauvegarde et que l'utilisateur tente d'effectuer une autre restauration avec cette image de sauvegarde sans cocher la case **Supprimer des interfaces réseau**, l'opération de restauration échoue.
- Si une machine virtuelle comporte un projet lors de la sauvegarde, mais n'existe plus lors du déclenchement de la restauration, le travail de restauration échoue.
- Si la catégorie d'une machine était configurée lors de la sauvegarde, mais n'existait pas lors de la restauration, le travail de restauration échoue.
- Si l'utilisateur de la machine virtuelle n'est pas présent dans le serveur Nutanix Prism Central ou dans le projet lors de la restauration, l'opération échoue.

- Seules les adresses IP de type ASSIGNED sont prises en compte pour la restauration. Le type d'adresse IP LEARNED est ignoré et l'utilisateur doit configurer l'IP manuellement après la restauration.
- Si la machine virtuelle comporte une carte réseau avec un port de répartition activé, cette option est ignorée après la restauration. Vous devez ajouter et configurer manuellement la répartition sur la carte réseau avec l'interface de ligne de commande Nutanix.
- Une machine virtuelle est restaurée avec les informations de projet, de catégorie et de propriétaire et d'autres attributs relatifs au VPC si la restauration a été effectuée à l'emplacement d'origine.
- Un comportement non défini est observé lors d'une tentative de sauvegarde/restauration des machines virtuelles d'un cluster qui ont été déplacées d'un serveur Prism Central à un autre.
- Un hôte de sauvegarde doté de la version 10.2 ou d'une version ultérieure est requis pour la sauvegarde/restauration du projet, de la catégorie et d'autres attributs relatifs au cloud privé virtuel (VPC). Si un hôte de sauvegarde doté d'une version antérieure à la 10.2 est utilisé, la sauvegarde/restauration se termine sans capture des attributs relatifs au VPC en l'absence de machine virtuelle dans l'environnement VPC. Si une machine virtuelle est présente dans l'environnement VPC et si la restauration est déclenchée à l'aide d'un hôte de sauvegarde doté d'une version antérieure à la 10.2, la restauration peut échouer.

# À propos de la restauration sans agent des fichiers et des dossiers Nutanix AHV

NetBackup 9.1 et les versions ultérieures prennent en charge la restauration sans agent des fichiers et des dossiers Nutanix AHV. Il permet de restaurer des fichiers ou dossiers spécifiques sur l'hôte cible de votre choix. L'hôte cible peut être une machine virtuelle hébergée sur AHV ou d'autres hyperviseurs, voire un ordinateur physique sur lequel le client NetBackup n'est pas installé. Cette restauration utilise le package VxUpdate de la plate-forme d'hôte cible voulue et déploie l'outil de récupération NetBackup sur l'hôte cible. La restauration sans agent de fichiers et de dossiers nettoie l'outil de récupération et l'emplacement intermédiaire une fois le processus de restauration terminé. Le processus de récupération utilise un hôte NetBackup comme hôte de récupération pour assurer la connectivité réseau avec l'hôte cible. Cet hôte de récupération peut être un serveur ou un client NetBackup.

Vue d'ensemble du processus de restauration des fichiers et des dossiers

1. Le serveur principal NetBackup reçoit l'entrée de l'interface utilisateur Web NetBackup ou de l'API de récupération sans agent. L'utilisateur spécifie les

fichiers ou dossiers à restaurer, ainsi que les informations d'authentification de l'hôte cible. Les informations d'authentification requises sont :

- Windows : l'utilisateur doit appartenir au groupe local d'administrateurs si UAC est désactivé. Si UAC est activé, l'utilisateur doit être un utilisateur de domaine ajouté au groupe local d'administrateurs.
- Linux : l'utilisateur doit être un utilisateur racine ou un sudoer disposant de toutes les autorisations.

2. Le serveur principal envoie les données demandées à l'hôte de récupération.
3. L'hôte de récupération confirme qu'il dispose du package de reprise VxUpdate nécessaire pour effectuer la restauration. S'il n'est pas disponible, l'hôte de récupération télécharge le package requis à partir du serveur principal qui utilise VxUpdate.
4. L'hôte de récupération copie l'outil de récupération du package VxUpdate sur l'hôte cible. La récupération s'exécute sous Linux et l'hôte cible utilise le protocole SSH pour l'opération de récupération. La récupération s'exécute sous Windows et l'hôte cible utilise les protocoles WMI et SMB pour l'opération de récupération.
5. Le fichier de flux de données contenant les fichiers ou les dossiers à restaurer est copié à l'emplacement intermédiaire sur un hôte de récupération.
6. Le fichier créé sur l'emplacement intermédiaire de l'hôte de récupération est copié à un emplacement intermédiaire sur un hôte cible.
7. L'outil de récupération est appelé et les fichiers ou dossiers sélectionnés sont récupérés avec les listes de contrôle d'accès (ACL) et les détails de métadonnées.
8. NetBackup effectue le nettoyage nécessaire, que l'opération de restauration ait réussi ou échoué. Tous les fichiers temporaires stockés à l'emplacement intermédiaire sur les hôtes cible et de récupération sont supprimés. En cas d'échec, des preuves sont collectées sur l'hôte cible et transférées sur l'hôte de récupération avec la configuration par défaut.
9. NetBackup prend en charge les plates-formes suivantes pour le système d'exploitation de l'hôte cible en préparation pour la restauration de fichiers sans agent :
   - Windows
   - Red Hat Enterprise Linux (RHEL)
   - SUSE Linux (SLES)
   - Ubuntu

Pour la prise en charge des versions de système d'exploitation de l'hôte cible, consultez la section `Client NetBackup` de la Liste de compatibilité logicielle de NetBackup 8.1 et versions ultérieures.

# Conditions requises pour la récupération sans agent de fichiers et de dossiers

Vous ne pouvez récupérer des fichiers ou des dossiers que si la machine virtuelle AHV source est en cours d'exécution sur le système d'exploitation spécifié, tel que Red Hat Linux, SuSE Linux ou Windows. En outre, le système de fichiers doit être compatible pour permettre la création de mappages de système de fichiers à partir de la sauvegarde de machine virtuelle sans agent complète. Pour plus d'informations sur la compatibilité AHV, consultez la section Prise en charge des environnements virtuels NetBackup.

---

**Remarque :** Si vous devez pouvoir restaurer des fichiers et dossiers individuels pour un système d'exploitation non pris en charge, protégez ces machines virtuelles avec le type de politique standard NetBackup.

---

**Tableau 5-1** Conditions requises pour la récupération de fichiers et de dossiers

| Présentation des étapes | Description et référence |
|---|---|
| **Restauration basée sur un agent** | ■ La restauration avec agent s'effectue si un client ou serveur NetBackup est installé sur l'hôte cible.<br>■ Pour ce client ou serveur, la version de NetBackup doit être au minimum 8.1 pour Windows et 8.2 pour Linux.<br>**Remarque :** Si vous sélectionnez Linux version 8.1 ou une version antérieure, les options de restauration sans agent s'affichent.<br>■ Vous devez spécifier le nom d'hôte configuré NetBackup sur l'hôte cible pour la restauration avec agent.<br>■ Si l'utilisateur NetBackup connecté dispose d'autorisations suffisantes, il peut parcourir la liste d'hôtes NetBackup et en sélectionner un pour restaurer des fichiers ou des dossiers. Si l'utilisateur connecté ne dispose pas d'autorisations RBAC suffisantes, l'hôte cible doit être spécifié manuellement.<br>■ Vous devez spécifier le nom d'hôte NetBackup configuré ou son adresse IP sur l'hôte cible pour la restauration avec agent.<br>Si la machine virtuelle AHV source s'exécute sur une plate-forme Linux, vous pouvez restaurer les fichiers ou les dossiers sur l'hôte cible de votre choix sur n'importe quelle plate-forme Linux prise en charge.<br>**Remarque :** Si NetBackup n'est plus installé sur l'hôte cible, vous pouvez toujours lancer la restauration avec agent, mais elle échouera. |
| **Restauration sans agent** | La restauration sans agent s'effectue si aucun client ou serveur NetBackup n'est installé sur l'hôte cible.<br>■ Vous devez spécifier le nom de domaine complet ou l'adresse IP de l'hôte cible.<br>■ NetBackup détecte si l'hôte est une machine non-NetBackup dans la configuration NetBackup et les options de restauration sans agent s'affichent.<br>**Remarque :** Les adresses IPv4 et IPv6 sont toutes deux prises en charge. Dans IPv6, le format CIDR standard n'est pas pris en charge. |

| Présentation des étapes | Description et référence |
| --- | --- |
| **Hôte cible** | ■ L'hôte cible désigne l'hôte sur lequel les fichiers ou les dossiers d'une sauvegarde de machine virtuelle AHV doivent être restaurés. Le nom d'hôte doit reprendre le format de nom de domaine complet ou d'adresse IP.<br>■ Vous pouvez restaurer les fichiers ou les dossiers sur n'importe quel hôte cible déployé sur AHV, sur d'autres hyperviseurs ou même sur un hôte physique.<br>**Remarque :** Assurez-vous que l'hôte cible est accessible depuis l'hôte de récupération.<br>■ Les plates-formes d'hôte source et cible doivent être homogènes. Les fichiers d'hôte de source Windows peuvent être restaurés sur un hôte cible Windows, tandis que les fichiers de machine virtuelle source Linux peuvent être restaurés sur un hôte cible Linux.<br>■ Par défaut, le répertoire intermédiaire de l'hôte cible est le répertoire d'origine de l'utilisateur. Vous pouvez spécifier un emplacement intermédiaire personnalisé.<br>Conditions requises :<br>■ NetBackup ne crée pas d'emplacement intermédiaire de l'hôte cible, car cet emplacement doit avoir été créé au préalable et inclure des autorisations d'écriture et d'exécution.<br>■ L'emplacement intermédiaire de l'hôte cible doit disposer d'assez d'espace pour l'opération de restauration. Cela inclut la taille du fichier de restauration, le package de restauration NetBackup (environ 150 Mo pour Windows et environ 100 Mo pour Linux) et l'espace dédié aux journaux des opérations NetBackup.<br>**Remarque :** Si le chemin d'accès de l'emplacement intermédiaire se trouve sur un lecteur système, ce dernier doit disposer de suffisamment d'espace pour les autres processus en cours d'exécution. |

| Présentation des étapes | Description et référence |
| --- | --- |
| **Hôte cible Linux** | ■ La machine cible sans agent doit être en cours d'exécution sur les plates-formes de système d'exploitation prises en charge. Pour plus d'informations sur la compatibilité AHV, consultez la section Prise en charge des environnements virtuels NetBackup.<br>■ L'utilitaire TAR doit être présent sur le chemin d'accès par défaut sur l'hôte cible et le chemin d'accès est ajouté à la variable de chemin d'accès du système.<br>■ NetBackup prend en charge le nom d'hôte au format ASCII uniquement. Si le nom d'hôte n'est pas au format ASCII, vous pouvez spécifier l'hôte cible à l'aide de son adresse IP.<br>■ Le nombre maximum de connexions SSH à l'hôte cible est configurable et la valeur par défaut est 10.<br>■ Le port SSH doit être ouvert entre l'hôte de récupération et l'hôte cible. Si un pare-feu est configuré, le port SSH doit figurer dans la liste d'exceptions du pare-feu.<br>■ Pour procéder à la restauration sur le chemin d'accès réseau de l'hôte cible, fournissez les autorisations d'exportation nécessaires. Par exemple, `rw,sync,no_root_squash`. |

| Présentation des étapes | Description et référence |
| --- | --- |
| **Conditions de connexion SSH** | ■ La restauration sans agent sur l'hôte cible Linux s'effectue au moyen du service SSH. Il doit être en cours d'exécution sur l'hôte cible.<br>■ Le délai de communication SSH sur l'hôte cible doit être supérieur à 5 minutes.<br>■ Lorsque vous communiquez avec l'hôte cible à l'aide de SSH, NetBackup utilise le chiffrement `aes256-ctr`.<br>■ La version de SSH doit être 1.2 ou une version ultérieure.<br>■ L'utilisation d'un port SSH personnalisé est prise en charge.<br>**Remarque :** Le port SSH par défaut est 22.<br>■ Ce qui suit est pris en charge :<br>■ Algorithmes d'échange de clés :<br>■ `diffie_helman_group_exchange_sha256`<br>■ `ecdh_sha2_nistp256`<br>■ `cdh_sha2_nistp384`<br>■ `ecdh_sha2_nistp521`<br>■ `diffie_helman_group14_sha1`<br>■ Clé d'hôte<br>■ `ssh-rsa`<br>■ `ssh-dss`<br>■ `ecdsa-sha2-nistp256`<br>■ `ecdsa-sha2-nistp384`<br>■ `ecdsa-sha2-nistp521`<br>■ Méthode de hachage<br>■ `sha256 Hex encoded` |

| Présentation des étapes | Description et référence |
|---|---|
| **Restauration d'utilisateur SUDO** | ■ L'utilisateur sudo doit déjà exister sur l'hôte cible Linux.<br>■ Assurez-vous que l'utilisateur non-racine est déjà configuré dans le fichier sudoers.<br>Exemple :<br>■ `<sudo-username> ALL = (ALL)`<br>■ `<sudo-username> ALL = (ALL) NOPASSWD`<br>■ Il doit y avoir une entrée unique configurée pour l'utilisateur non racine dans le fichier sudoers.<br>■ L'utilisateur sudo (Linux) doit posséder l'emplacement intermédiaire personnalisé et disposer des autorisations de lecture, d'écriture et d'exécution.<br>Vous pouvez utiliser la clé privée SSH au lieu du mot de passe.<br>Se reporter à "Signature de clé SSH" à la page 79. |

| Présentation des étapes | Description et référence |
| --- | --- |
| **Hôte cible Windows** | |

| Présentation des étapes | Description et référence |
| --- | --- |
| | ■ La machine cible sans agent doit être en cours d'exécution sur les plates-formes de système d'exploitation prises en charge. Pour plus d'informations sur la compatibilité AHV, consultez la section Prise en charge des environnements virtuels NetBackup.<br>■ WMI doit être configuré et accessible entre l'hôte de récupération et l'hôte cible. Pour les conditions requises concernant WMI et SMB, consultez https://www.veritas.com/support/fr_FR/article.100040135.<br>■ Accepte le nom d'hôte au format ASCII. Pour le nom d'hôte Unicode, utilisez l'adresse IP au lieu du nom d'hôte.<br>■ Les services suivants doivent être en cours d'exécution sur vos hôtes Windows :<br>■ DCOM<br>■ RPC<br>■ WMI<br>■ Partage de fichiers et d'imprimantes<br>■ Par défaut, le **partage administratif** est activé sur l'hôte. S'il est désactivé, dans GPO, l'utilisateur doit activer le partage administratif sur le lecteur d'emplacement intermédiaire ou le lecteur sur lequel l'emplacement intermédiaire se trouve.<br>**Remarque :** Par défaut, les administrateurs sont autorisés à accéder à WMI et DCOM. En cas de problème au niveau des autorisations DCOM et WMI, reportez-vous à la *documentation Microsoft*.<br>■ Utilisateur ou groupe utilisé pour assigner des autorisations DCOM et WMI :<br>Procédez de l'une des deux façons suivantes pour assigner des autorisations **DCOM** et **WMI** :<br>■ L'utilisateur doit faire partie du groupe d'administrateurs et vous pouvez assigner les autorisations au groupe d'administrateurs.<br>■ Assignez les autorisations à l'utilisateur en question.<br>■ Prend en charge les environnements UAC et non UAC :<br>■ L'administrateur intégré et l'utilisateur de domaine, qui ont été ajoutés au groupe local d'administrateurs de l'hôte cible, disposent des |

| Présentation des étapes | Description et référence |
| --- | --- |
| | autorisations requises pour effectuer la restauration sans agent.<br><br>**Remarque :** Restrictions distantes UAC : pour l'utilisateur local du groupe d'administrateurs, il est recommandé d'utiliser la restauration avec agent. Toutefois, l'utilisateur peut toujours effectuer une restauration sans agent en désactivant le filtrage UAC.<br><br>Pour désactiver les restrictions distantes UAC, voir ici |

| Présentation des étapes | Description et référence |
| --- | --- |
| | ■ **Conditions requises pour l'emplacement** intermédiaire :<br>■ L'emplacement par défaut est le répertoire d'origine de l'utilisateur, mais si un chemin d'accès personnalisé est spécifié, l'utilisateur doit y avoir accès.<br>■ Il doit s'agir d'un chemin absolu.<br>**Remarque :** Les liens symboliques, liens physiques, chemins d'accès réseau, etc. ne sont pas pris en charge.<br>■ L'espace doit être suffisant pour l'opération de restauration. Cela inclut :<br>■ La taille du fichier de restauration.<br>■ Le package de restauration NetBackup (environ 150 Mo).<br>■ L'espace dédié aux journaux des opérations NetBackup. Les conditions requises varient selon le niveau de détail du fichier journal.<br>**Remarque :** Si le chemin d'accès se trouve sur le lecteur système, il doit comporter suffisamment d'espace pour les autres processus en cours d'exécution.<br>■ Le nombre de caractères du chemin d'accès est limité à 260. Cependant, NetBackup nécessite environ 110 caractères pour la formation de l'emplacement temporaire. Par conséquent, choisissez un chemin d'accès comportant moins de 150 caractères.<br>■ Si l'emplacement intermédiaire et l'emplacement de restauration se trouvent sur le même lecteur, prévoyez le double de l'espace de restauration par précaution.<br>■ L'exécution parallèle de plusieurs travaux de restauration du même utilisateur est prise en charge. Cependant, si des dossiers de destination identiques sont spécifiés, l'état des données restaurées risque de ne plus être cohérent. |

| Présentation des étapes | Description et référence |
| --- | --- |
| **Conditions requises pour WMI et SMB** | ■ La restauration sans agent sur l'hôte cible Windows repose sur les protocoles WMI (Windows Management Instrumentation) et SMB (Server Message Block).<br>■ Assurez-vous que les ports WMI et SMB sont ouverts dans les paramètres de votre pare-feu.<br>■ Port DCOM par défaut : 135<br>■ Port SMB par défaut : 445<br>■ Ports dynamiques : 49152-65535<br>**Remarque :** Votre environnement peut également inclure un port fixe statique.<br>■ Chiffrez le transfert de données sur SMB en activant le chiffrement SMB. Consultez la *documentation Microsoft* pour plus de détails.<br>■ Prend en charge la version SMB 3.0. Si votre hôte a une version plus ancienne, vous pouvez la désactiver. Reportez-vous aux directives de Microsoft. |

| Présentation des étapes | Description et référence |
|---|---|
| **Hôte de récupération** | L'hôte de récupération est un hôte qui est installé sur le client/serveur de médias NetBackup et qui sert à communiquer avec l'hôte cible spécifié.<br>■ La version de NetBackup sur l'hôte de récupération doit être 9.1 ou une version ultérieure et doit disposer d'une connectivité avec l'hôte cible.<br>■ Tout hôte de récupération Linux doit disposer d'une connectivité SSH avec l'hôte cible Linux . De même, tout hôte de récupération Windows doit disposer d'une connectivité WMI et SMB avec l'hôte cible Windows.<br>■ L'hôte de récupération doit être une plate-forme homogène. Tout hôte de récupération Windows doit pouvoir restaurer les fichiers issus d'une machine virtuelle Windows AHV sur un hôte Windows cible. De même, tout hôte de récupération Linux doit pouvoir restaurer un fichier issu d'une machine virtuelle Linux AHV sur un hôte Linux cible.<br>**Remarque :** Pour restaurer des fichiers sur l'hôte cible Ubuntu, utilisez RHEL ou SUSE comme hôte de récupération.<br>■ Seuls les hôtes de récupération incluant le serveur ou client NetBackup 9.1 sont pris en charge.<br>■ Chemin d'accès réseau comme emplacement intermédiaire sur l'hôte de récupération, dans la mesure où les autorisations d'exportation sont correctes. Par exemple, `rw,sync,no_root_squash`.<br>■ L'emplacement intermédiaire par défaut sur l'hôte de récupération est :<br>■ Pour Linux : `/{chemin-installation}/openv/var/tmp/staging`<br>■ Pour Windows : `{chemin-installation}\NetBackup\Temp\staging`<br>■ L'emplacement intermédiaire par défaut peut être modifié à l'aide de `bpsetconfig`.<br>■ Exécutez `<NetBackup path>/bin/admincmd/bpsetconfig`.<br>■ Définissez `AGENTLESS_RHOST_STAGING_PATH = <Path>`.. |

| Présentation des étapes | Description et référence |
|---|---|
| **Autre** | ■ Assurez-vous que la valeur « `PasswordAuthentication` définie dans le fichier « /etc/ssh/sshd_config » pour l'hôte cible SUSE est `Yes` ». Redémarrez ensuite le service « ssh ».<br>**Remarque :** Par défaut, la valeur `passwordAuthentication` définie pour les hôtes cibles SUSE est `No`. |

# Signature de clé SSH

**Pour obtenir l'empreinte digitale de clé SSH de l'hôte cible Linux :**

1. Utilisez la commande suivante sur l'hôte cible RHEL ou SUSE OS pour obtenir la clé `SHA256-based RSA`.

```
cat /etc/ssh/ssh_host_rsa_key.pub |awk '{print $2}' |base64 -d |sha256sum |
awk '{print $1}'
```

**Remarque :** La sortie des commandes correspond à la clé RSA. De même, modifiez le chemin d'accès à la clé publique, exécutez cette commande pour obtenir la signature de clé SSH ecdsa ou DSS configurée sur l'hôte cible.

- Exemple de clé RSA :

```
cat /etc/ssh/ssh_host_rsa_key.pub |awk '{print $2}'|base64 -d |
sha256sum |awk '{print $1}'
```

- Sortie de commande :

```
b2352722053ac9f40bc1XXXXXXXXXXXXXXXXXXXXXXXXXX419fa241ba9431fd6b9
```

2. Copiez la signature RSA. Vous pouvez fournir cette signature de clé SSH lorsque vous ajoutez les informations de l'hôte cible. Vous pouvez également vérifier la signature de clé SSH affichée en cliquant sur **Récupérer la signature de clé SSH** sur la page **Hôte de récupération**.

**Pour générer la clé privée SSH :**

1. Exécutez les commandes suivantes sur l'hôte cible Linux :

- `ssh-keygen -t rsa`

- `-t option supports "ecdsa | rsa | dss"`

2 Vous devez ajouter/préfixer la clé publique de l'hôte cible dans le fichier cible `vm ~/.ssh/authorized_keys`.

# Récupération de fichiers et de dossiers avec la restauration sans agent Nutanix AHV

**Pour récupérer des fichiers et des dossiers avec la restauration sans agent Nutanix AHV**

1 Assurez-vous que l'hôte cible est sous tension et dispose d'une connectivité réseau à l'hôte de récupération qui est utilisé par le processus de restauration.

2 Dans le volet gauche, cliquez sur **Nutanix AHV**.

3 Localisez et sélectionnez la machine virtuelle AHV qui contient les fichiers et les dossiers à restaurer.

Cette machine virtuelle est appelée « machine virtuelle source ».

4 Cliquez sur l'onglet **Points de récupération**. Dans la vue de calendrier, sélectionnez la date de la sauvegarde.

5 Les images disponibles sont répertoriées sur des lignes et sont accompagnées d'un horodatage de sauvegarde.

6 Sur l'image à récupérer, cliquez sur **Récupérer > Restaurer les fichiers et les dossiers**.

7 Dans le volet **Sélectionner les fichiers**, spécifiez les fichiers et dossiers à récupérer, puis cliquez sur **Suivant**. Ces fichiers ou dossiers sont désormais appelés fichiers ou dossiers sources.

8 Cliquez sur **Suivant**.

9 Sur la page **Cible de la récupération**, procédez comme suit :

- Entrez l'IP/le nom d'hôte manuellement.
- Si nécessaire, entrez l'emplacement intermédiaire sur l'hôte cible.
- Sélectionnez l'option de restauration de fichier voulue.
- Sélectionnez l'hôte correct de récupération.
- Ajoutez des informations d'authentification correctes en fonction du type de système d'exploitation.

Se reporter à "Options de la cible de récupération" à la page 82.

**10** Sur la page **Options de récupération**, sélectionnez l'une des options suivantes :

- **Ajouter la chaîne aux noms de fichier** : ajoute la chaîne spécifiée aux noms de fichier cible, avant toute extension de fichier. Cette valeur s'applique uniquement aux fichiers.
- **Remplacer les fichiers existants** : remplace les fichiers ou les dossiers s'ils existent à l'emplacement de destination sous le même nom.
- **Restaurer les répertoires sans croiser les points de montage**
- **Créer de nouveaux fichiers pour les liens physiques**
- **Renommer les cibles pour les liens virtuels**

---

**Remarque :** Les options **Créer de nouveaux fichiers pour les liens physiques** et **Renommer les cibles pour les liens virtuels** sont activées uniquement pour tout restaurer dans un autre répertoire.

---

**11** Cliquez sur **Suivant**.

**12** Sur la page **Vérification** : la page Vérification affiche l'état de la vérification de pré-récupération. NetBackup effectue la validation de pré-récupération pour confirmer si le travail de restauration s'exécutera correctement au moyen des entrées que vous avez fournies.

Se reporter à "Vérifications de pré-récupération pour Nutanix AHV" à la page 87.

- Si la pré-récupération échoue, les causes probables de la défaillance s'affichent. Cliquez sur le bouton **Modifier** de l'entrée à corriger.
- Si la pré-récupération est réussie, cliquez sur **Démarrer la récupération**.

# Options de la cible de récupération

**Tableau 5-2** Options de la cible de récupération

| Présentation des étapes | Description et référence |
|---|---|
| **Hôte cible** | ■ Le champ Hôte cible est pré-rempli avec le nom d'hôte/l'adresse IP de la machine virtuelle AHV source stocké lors de la dernière découverte réussie du cluster AHV correspondant à la machine virtuelle.<br>**Avertissement :** La restauration avec agent est effectuée si le client NetBackup est installé et configuré avec le nom d'hôte ou l'adresse IP fournie.<br>■ Si vous devez effectuer la restauration sur un autre client NetBackup, cliquez sur Rechercher et sélectionnez le client requis dans la liste.<br>**Remarque :** Veillez à sélectionner des clients utilisant des plates-formes homogènes.<br>■ Si l'option de recherche n'est pas disponible, entrez manuellement l'hôte cible.<br>■ Si vous souhaitez effectuer la restauration sur un hôte sur lequel le client NetBackup n'est pas installé, saisissez le nom de domaine complet ou l'adresse IP de cet hôte sur l'hôte cible. Les options de **restauration sans agent** s'affichent. |

| Présentation des étapes | Description et référence |
|---|---|
| **Options de restauration sans agent** | ■ **Modifier l'emplacement intermédiaire sur l'hôte cible** : si vous voulez fournir un emplacement intermédiaire différent de la valeur par défaut, entrez le chemin d'accès voulu. Le chemin d'accès de l'emplacement intermédiaire ne doit comporter que des caractères ASCII.<br>**Remarque :** L'emplacement intermédiaire par défaut correspond au répertoire d'origine de l'utilisateur.<br>■ **Options de restauration de fichier** : selon vos besoins, sélectionnez l'une des options appropriées de restauration de fichiers ci-dessous :<br>■ **Tout restaurer dans le répertoire d'origine**<br>■ **Tout restaurer dans un autre répertoire** Indiquez le chemin d'accès d'un répertoire différent dans lequel effectuer la restauration.<br>■ **Aplatir la structure de répertoires existante** Sélectionnez cette option pour tout restaurer dans un répertoire unique sans créer de sous-dossiers lorsque des fichiers sont sélectionnés dans des répertoires différents. |

| Présentation des étapes | Description et référence |
|---|---|
| **Hôte de récupération** | ■ Le champ **Hôte de récupération** est pré-rempli avec l'hôte de sauvegarde qui a été utilisé pendant l'opération de sauvegarde de la machine virtuelle AHV sélectionnée.<br><br>**Remarque :** Le champ **Hôte de récupération** est vide si la machine virtuelle sélectionnée et la plate-forme de l'hôte de sauvegarde ne sont pas homogènes.<br><br>**Remarque :** Pour restaurer des fichiers sur l'hôte cible Ubuntu, utilisez RHEL ou SUSE comme hôte de récupération.<br><br>■ Cliquez sur Rechercher pour sélectionner un autre hôte de récupération. La liste des serveurs de médias compatibles s'affiche. Pour sélectionner un client compatible avec NetBackup comme hôte de récupération, cliquez sur **Serveurs de médias > Clients**.<br>■ Si l'option de recherche n'est pas disponible, entrez manuellement l'hôte de récupération.<br><br>**Remarque :** L'hôte de récupération doit utiliser une plate-forme homogène par rapport à la machine virtuelle et le serveur ou le client NetBackup 9.1 ou version ultérieure doit être installé.<br><br>■ Dans un environnement Flex Scale, si tous les serveurs de médias ne sont pas répertoriés dans l'onglet de serveur de médias, l'utilisateur doit disposer d'une autorisation d'affichage sur le serveur de médias ou peut manuellement saisir le serveur de médias pour continuer.<br>■ Si vous avez déjà effectué une restauration sur le même hôte cible, l'hôte de récupération reprend automatiquement l'hôte de récupération utilisé précédemment en fonction des autorisations prédéfinies assignées à l'utilisateur qui exécutait cette restauration. |

| Présentation des étapes | Description et référence |
| --- | --- |
| **Connectivité SSH Linux** | |

| Présentation des étapes | Description et référence |
|---|---|
| | Pour la machine virtuelle Linux source sélectionnée, les options suivantes s'affichent pour la connectivité SSH :<br>■ **Port SSH de l'hôte cible** Spécifiez le port SSH de l'hôte cible. La valeur par défaut est 22.<br>Si vous avez déjà effectué une restauration sur le même hôte cible, le port SSH est pré-rempli avec la valeur utilisée précédemment en fonction des autorisations assignées à l'utilisateur qui exécutait cette restauration.<br>■ **Signature de clé SSH de l'hôte cible** Pour authentifier l'hôte cible, fournissez la signature de clé SSH au format hexadécimal.<br>■ Vous pouvez saisir manuellement la signature de clé SSH de l'hôte cible ou cliquer sur **Récupérer la signature de clé SSH**.<br>■ **Récupérer la signature de clé SSH** : si l'option Récupérer la signature de clé SSH n'est pas disponible, vous devez fournir cette signature manuellement. Se reporter à "Signature de clé SSH" à la page 79.<br>■ Si vous avez déjà effectué une restauration sur le même hôte cible, la signature de clé SSH est pré-remplie avec la valeur utilisée précédemment en fonction des autorisations assignées à l'utilisateur qui exécutait cette restauration. Vous pouvez ignorer la valeur pré-remplie pour rétablir la confiance.<br>■ **Récupérer la signature de clé SSH**<br>■ Affiche la liste des signatures de clé SSH, ainsi que les types de clés NetBackup pris en charge et configurés sur l'hôte cible.<br>■ Sélectionnez l'une des signatures répertoriées et cliquez sur **OK**. NetBackup établit la confiance avec l'hôte cible en appliquant la signature sélectionnée.<br>■ **Informations d'authentification de l'hôte cible**<br>■ **Nom d'utilisateur** Spécifiez le nom d'utilisateur de l'hôte cible. Il doit s'agir d'un utilisateur sudoer racine ou non racine.<br>**Utilisateur sudoer** Se reporter à "Conditions requises pour la récupération sans agent de fichiers et de dossiers" à la page 67. |

| Présentation des étapes | Description et référence |
|---|---|
| | ■ **Fournir le mot de passe** Sélectionnez cette option pour choisir l'authentification basée sur mot de passe.<br>■ **Mot de passe** Spécifiez le mot de passe de l'hôte cible pour l'utilisateur indiqué.<br>■ **Fournir une clé privée SSH** Sélectionnez cette option pour choisir l'authentification basée sur une clé privée SSH. Se reporter à "Signature de clé SSH" à la page 79.<br>■ **Clé privée SSH** Spécifiez une clé SSH privée.<br>■ **Phrase de passe de la clé** Si une clé privée SSH est créée à partir d'une phrase de passe, spécifiez la phrase de passe de la clé. |
| **Connectivité WMI Windows** | ■ **Nom d'utilisateur** Spécifiez le nom d'utilisateur de l'hôte cible. Cet utilisateur peut faire partie d'un domaine ou être un utilisateur local et doit faire partie du groupe d'administrateurs local. Les formats **nom_utilisateur_local** et **domaine\nom_utilisateur** sont pris en charge pour le nom d'utilisateur.<br>■ **Mot de passe** Spécifiez le mot de passe de l'hôte cible pour l'utilisateur indiqué. |

# Vérifications de pré-récupération pour Nutanix AHV

**Tableau 5-3** Vérifications de pré-récupération pour Nutanix AHV

| Validation | Description et référence | Source d'entrée |
|---|---|---|
| Espace sur l'hôte de récupération | Vérifie l'espace requis sur l'emplacement intermédiaire de l'hôte de récupération. | Hôte de récupération |
| Connectivité de l'hôte cible | Permet de vérifier si l'hôte cible est accessible depuis l'hôte de récupération. | Hôte cible et port de l'hôte cible |

| Validation | Description et référence | Source d'entrée |
|---|---|---|
| Informations d'authentification de l'hôte cible | Vérifie si les informations d'authentification fournies pour l'hôte cible sont valides. | Informations d'authentification de l'hôte cible |
| Emplacement intermédiaire de l'hôte cible sur un disque local | Permet de déterminer si l'emplacement intermédiaire de l'hôte cible n'est pas un chemin d'accès réseau. | Emplacement intermédiaire de l'hôte cible |
| Espace de l'emplacement intermédiaire de l'hôte cible | Permet de vérifier si l'espace requis est disponible sur l'emplacement intermédiaire de l'hôte cible.<br>**Remarque :** L'espace requis est fonction de la taille totale du fichier sélectionné et de la taille requise pour le package de restauration NetBackup, ainsi que de l'espace requis pour les journaux et d'autres fichiers. | Emplacement intermédiaire de l'hôte cible |
| Autorisations de l'emplacement intermédiaire de l'hôte cible | Permet de vérifier si l'utilisateur fourni est propriétaire et dispose d'autorisations RBAC sur l'emplacement intermédiaire de l'hôte cible. | Emplacement intermédiaire de l'hôte cible |
| Chemin d'accès de l'emplacement intermédiaire par défaut de l'hôte cible | Permet de vérifier si les caractères du chemin d'accès de l'emplacement intermédiaire de l'hôte cible fourni sont valides. NetBackup prend uniquement en charge les caractères ASCII pour le chemin d'accès de l'emplacement intermédiaire de l'hôte cible. | Emplacement intermédiaire de l'hôte cible |
| Système d'exploitation de l'hôte cible | Permet de vérifier si le système d'exploitation de l'hôte cible est pris en charge. | Général |

| Validation | Description et référence | Source d'entrée |
|---|---|---|
| Package VxUpdate | Permet de vérifier si le package VxUpdate requis est disponible sur le serveur principal. | Général |
| **Vérifications propres à l'hôte cible Linux** | | |
| Signature de clé SSH de l'hôte cible | Permet de vérifier si la signature de clé SSH de l'hôte cible est valide et permet d'établir la confiance avec l'hôte cible depuis l'hôte de récupération. | Signature de clé SSH de l'hôte cible |
| Existence de tar sur l'hôte cible | Vérifie si `tar` est disponible sur l'hôte cible. | Hôte cible |

# À propos de la restauration basée sur un agent des fichiers et des dossiers Nutanix-AHV

NetBackup 9.1 et les versions ultérieures prennent en charge la restauration basée sur un agent de fichiers et de dossiers Nutanix-AHV individuels La restauration basée sur un agent permet de restaurer des fichiers Nutanix-AHV individuels sur un hôte comportant un client NetBackup. L'hôte cible basé sur un agent peut être une machine virtuelle hébergée sur AHV ou d'autres hyperviseurs, voire un ordinateur physique sur lequel le client NetBackup est installé.

# Conditions requises pour la récupération basée sur agent de fichiers et de dossiers

- Vous pouvez effectuer une récupération des dossiers et des fichiers individuels à partir d'une image de machine virtuelle AHV source sauvegardée. Le système d'exploitation invité et le système de fichiers doivent être compatibles pour créer des mappages de système de fichiers.
  Consultez la *liste de compatibilité logicielle Nutanix AHV afin de connaître les systèmes d'exploitation invités et les systèmes de fichiers pris en charge pour les restaurations de fichiers individuels*.
  Prise en charge de NetBackup <versions> dans les environnements virtuels
- Vous pouvez récupérer les fichiers individuels à partir d'une sauvegarde de machine virtuelle AHV source. Le serveur principal NetBackup, le serveur de

médias et le serveur de sauvegarde doivent disposer de NetBackup 9.1 ou version ultérieure.

- Une restauration avec agent s'effectue si un client ou serveur NetBackup est installé sur l'hôte cible. Le client ou l'hôte cible doit disposer de NetBackup 8.1 ou version ultérieure pour Windows, ou de la version 8.2 ou version ultérieure pour Linux.

  **Remarque :** Si vous sélectionnez Linux version 8.1 ou une version antérieure, les options de restauration sans agent s'affichent.

  Vous devez spécifier le nom d'hôte ou l'adresse IP configurée par NetBackup sur l'hôte cible pour effectuer la restauration avec agent.

- Un utilisateur disposant des autorisations RBAC nécessaires pour afficher les hôtes NetBackup peut naviguer et sélectionner l'hôte NetBackup pour une restauration de fichiers ou de dossiers.
  Un utilisateur sans autorisations RBAC nécessaires doit spécifier manuellement le nom d'hôte ou l'adresse IP NetBackup configuré pour l'hôte cible.

- Vous trouverez ci-dessous les autorisations RBAC minimales requises pour qu'un utilisateur puisse effectuer une restauration avec agent de fichiers et de dossiers.

**Tableau 5-4** Autorisations pour tous les biens AHV

| Opération | Description | Opérations requises supplémentaires | Opérations supplémentaires facultatives |
|---|---|---|---|
| Restauration granulaire | Permet de restaurer des fichiers ou des dossiers à partir d'un bien AHV.<br>Cette autorisation est requise sur la machine virtuelle source. | Global > Gestion de NetBackup > Images de sauvegarde NetBackup > Afficher<br>Global > Gestion de NetBackup > Images de sauvegarde NetBackup > Afficher le contenu<br>Global > Gestion de NetBackup > Hôtes NetBackup > Afficher<br>Biens > Biens > Restaurer des fichiers à l'aide du client | Biens > Biens > Écraser les fichiers et les dossiers |

**Tableau 5-5** Autorisations pour tous les biens AHV

| Opération | Description | Opérations requises supplémentaires | Opérations supplémentaires facultatives |
|---|---|---|---|
| Restauration granulaire | Permet de restaurer des fichiers ou des dossiers à partir d'un bien AHV.<br>Cette autorisation est requise sur la machine virtuelle source. | Global > Gestion de NetBackup > Images de sauvegarde NetBackup > Afficher<br>Global > Gestion de NetBackup > Images de sauvegarde NetBackup > Afficher le contenu<br>Global > Gestion de NetBackup > Hôtes NetBackup > Afficher<br>Biens > Biens > Restaurer des fichiers à l'aide du client | Biens > Biens > Écraser les fichiers et les dossiers |

# Récupération de fichiers et de dossiers avec la restauration avec agent Nutanix AHV

1. Assurez-vous que l'hôte cible est sous tension et dispose d'une connectivité réseau à l'hôte de récupération qui est utilisé par le processus de restauration.
2. Dans la partie gauche, cliquez sur **Nutanix AHV**.
3. Localisez et sélectionnez la machine virtuelle AHV qui contient les fichiers et les dossiers à restaurer.

   Cette machine virtuelle sera désormais appelée « machine virtuelle source ».
4. Cliquez sur l'onglet **Points de récupération**. Dans la vue de calendrier, sélectionnez la date de la sauvegarde.

   Les images disponibles sont répertoriées sur des lignes et sont accompagnées d'un horodatage de sauvegarde.
5. Sur l'image à récupérer, cliquez sur **Récupérer > Restaurer les fichiers et les dossiers**.

6 Dans le volet **Sélectionner les fichiers**, spécifiez les fichiers et les dossiers à récupérer, puis cliquez sur **Suivant**. Ces fichiers ou dossiers sont désormais appelés fichiers ou dossiers sources.

7 Sur la page **Cible de la récupération**, procédez comme suit :

- Sélectionnez l'hôte cible.
  - L'hôte cible spécifié doit être un nom de domaine complet ou une adresse IP. Si vous êtes autorisé à afficher les hôtes, cliquez sur l'icône de recherche pour afficher les hôtes sur lequel le client NetBackup est déjà présent et sélectionnez l'hôte requis.

    **Remarque :** La liste déroulante inclut uniquement NetBackup 8.1 ou version ultérieure.

- Sélectionnez l'option de restauration de fichier voulue.

Se reporter à "Options de la cible de récupération" à la page 82.

8 Sur la page **Options de récupération**, sélectionnez l'une des options suivantes :

- **Ajouter la chaîne aux noms de fichier :** ajoute la chaîne spécifiée aux noms de fichier cible, avant toute extension de fichier. Cette valeur s'applique uniquement aux fichiers.
- **Remplacer les fichiers existants** : remplace les fichiers ou les dossiers s'ils existent à l'emplacement de destination sous le même nom.
- **Restaurer les répertoires sans croiser les points de montage**
  Pour ignorer les systèmes de fichiers montés dans les répertoires sélectionnés. Désactivez cette case à cocher pour restaurer les systèmes de fichiers montés dans les répertoires sélectionnés
- **Créer de nouveaux fichiers pour les liens physiques**
- **Renommer les cibles pour les liens virtuels**

  **Remarque :** Les options **Créer de nouveaux fichiers pour les liens physiques** et **Renommer les cibles pour les liens virtuels** sont activées uniquement pour tout restaurer dans un autre répertoire.

9 Cliquez sur **Suivant**.

10 Sur la page **Vérification** : vérifiez toutes les options précédemment sélectionnées.

11 Cliquez sur **Lancer la récupération**.

# Limitations

- L'opération de récupération multiplate-forme des fichiers n'est pas prise en charge. Vous ne pouvez restaurer les fichiers Windows que sur les systèmes d'exploitation invités Windows, et les fichiers Linux que sur les systèmes d'exploitation invités Linux pris en charge. En d'autres termes, l'hôte de restauration doit utiliser la même plate-forme que les fichiers à restaurer.
- Au cours d'un processus de récupération, NetBackup recrée les liens entre un lien physique et son fichier d'origine. Dans ce cas seulement, le fichier de lien et son fichier cible doivent être restaurés par le même travail.

  **Remarque :** Si les deux fichiers sont restaurés individuellement par des travaux de restauration distincts, ils le sont en tant que fichiers distincts et le lien n'est pas rétabli.

- Pour les machines virtuelles à double démarrage, NetBackup ne prend pas en charge la récupération de fichiers ou dossiers individuels.
- Pour en savoir plus sur la prise en charge et les limitations de la plate-forme client et du système de fichiers, consultez la page https://www.veritas.com/content/support/en_US/doc/NB_70_80_VE (en anglais).
- Les options **Aplatir la structure de répertoires existante** et **Ajouter la chaîne aux noms de fichier** s'appliquent seulement aux fichiers. Elles ne sont pas disponibles pour les répertoires.
- Si vous sélectionnez les options **Aplatir la structure de répertoires existante** et **Remplacer les fichiers existants**, vous risquez d'effectuer une restauration incorrecte si elle contient plusieurs fichiers du même nom.

  **Remarque :** Le dernier fichier restauré est disponible lorsque la restauration est terminée.

- Si vous sélectionnez l'option **Aplatir la structure de répertoires existante** sans sélectionner l'option **Remplacer les fichiers existants**, la restauration aboutit, mais le premier fichier restauré est également présent à l'issue de la restauration. Pour éviter cela, ne sélectionnez pas l'option **Aplatir la structure**

**de répertoires existante** lors de la restauration de plusieurs fichiers portant le même nom.

- Si une sauvegarde et une restauration se produisent simultanément sur la même machine virtuelle, l'un de ces travaux, voire les deux, peut avoir des résultats inattendus.

  **Remarque :** Si une sauvegarde ou une restauration se ferme avec un code d'état NetBackup différent de zéro, il est possible que plusieurs travaux s'exécutent simultanément sur la même machine virtuelle.

- Si les données de restauration sélectionnées contiennent des fichiers masqués tels que `.bashrc` ou `.bash_history`, l'option de restauration **Ajouter la chaîne aux noms de fichier** n'est pas prise en charge.
- Les restaurations sans agent Nutanix ne peuvent être utilisées que pour la restauration de fichiers et de dossiers.
- Le travail de restauration échoue si NetBackup ne dispose pas des privilèges suffisants pour le répertoire intermédiaire ou si l'espace de ce répertoire est insuffisant.

  **Remarque :** Veritas déconseille d'effectuer des restaurations Nutanix AHV sans agent si un client NetBackup existe déjà sur la machine virtuelle cible. Dans ce cas, l'administrateur NetBackup doit utiliser la restauration avec agent.

- Sur l'hôte cible Windows, l'utilisation d'un lecteur mappé comme destination de restauration n'est pas prise en charge.
- NetBackup ne prend pas en charge la communication avec les hôtes cible Windows utilisant `openSSH`. Dans ce cas, le travail de restauration échoue.
- NetBackup prend uniquement en charge les caractères ASCII pour le chemin d'accès de l'emplacement intermédiaire de l'hôte cible.
- NetBackup prend uniquement en charge l'authentification de type NTLM pour l'hôte cible Windows.
- Les images AHV qui ont été restaurées avec une version antérieure à 9.1 ne peuvent pas être restaurées à partir de l'interface utilisateur Web. Pour restaurer ces images, l'utilisateur doit utiliser la Console d'administration NetBackup.
- Les images de sauvegarde AHV sont disponibles sur l'interface utilisateur Web, même si la sauvegarde a été réalisée depuis la Console d'administration

NetBackup, à condition que l'hôte de sauvegarde dispose au moins de NetBackup version 9.1.

À propos des images de sauvegarde sur l'interface utilisateur Web :

- Si la découverte de biens se déroule normalement, et une fois la sauvegarde réalisée à partir de la Console d'administration NetBackup, les images de sauvegarde deviennent disponibles sur l'interface utilisateur Web.
- Si le serveur principal et l'hôte de sauvegarde sont mis à niveau vers la version 9.1, la sauvegarde est réalisée depuis la Console d'administration NetBackup. Puis, si vous configurez l'interface utilisateur Web, vous devez procéder à la découverte des biens pour consulter les images de sauvegarde.
- Si le serveur principal est mis à niveau vers la version 9.1 (avec une version de l'hôte de sauvegarde inférieure à 9.1 et une sauvegarde effectuée à partir de la Console d'administration NetBackup, alors vous ne pourrez pas afficher les images de sauvegarde si vous configurez l'interface utilisateur Web, même après la découverte de biens.

Chapitre 6

# Dépannage des opérations AHV

Ce chapitre traite des sujets suivants :



## Astuces de dépannage de NetBackup pour AHV

Pour plus d'informations sur le dépannage de AHV, vérifiez les détails suivants :

- En cas d'échec des travaux de découverte :
  - Vérifiez la section **Informations concernant le travail** du travail en question dans le moniteur d'activité.
  - Vérifiez le journal `ncfnbcs`.
- Pour les échecs de travail de snapshot :
  - Vérifiez la section **Informations concernant le travail** du travail en question dans le moniteur d'activité.
  - Vérifiez le journal `bpfis`.
  - Pour les erreurs liées à AHV, cochez **Alertes** sur la console Prism AHV.

- Pour les échecs de travail de sauvegarde :
  - Vérifiez la section **Informations concernant le travail** du travail en question dans le moniteur d'activité.
  - Vérifiez les journaux `bpbkar` et `VxMS`.
  - Pour les erreurs liées à un snapshot AHV, cochez **Alertes** sur la console Prism AHV.
- Pour les échecs de travail de restauration :
  - Le travail de restauration échoue avec l'erreur 2822 (erreur de restauration de la politique de l'hyperviseur)
  - Vérifiez la section **Informations concernant le travail** du travail en question dans le moniteur d'activité.
  - Vérifiez les journaux `bprd`, `bpVMutil`, `Vélums` ou `ncfnbrestore`.
  - Pour les erreurs liées à AHV, cochez **Alertes** sur la console Prism AHV.

# Erreur lors de l'ajout des informations d'authentification AHV

**Tableau 6-1** Erreur lors de l'ajout des informations d'authentification AHV

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| La découverte des machines virtuelles et les validations des informations d'authentification sont prises en charge à partir de NetBackup 9.1. Le serveur/l'hôte de sauvegarde sélectionné dispose de NetBackup 8.3. | Mettez à niveau le serveur/l'hôte de sauvegarde ou sélectionnez un autre serveur/hôte de sauvegarde disposant de la version requise de NetBackup. |

# Erreur lors de la phase de découverte de machines virtuelles AHV

Le tableau suivant décrit les problèmes qui peuvent se produire quand vous découvrez des machines virtuelles AHV.

**Tableau 6-2** Erreur lors de la phase de découverte des machines virtuelles AHV

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Les biens AHV ne sont pas découverts après l'ajout des informations d'authentification correctes du cluster AHV. L'opération de découverte des machines virtuelles échoue. | Exécutez maintenant la découverte et relancez la sauvegarde. La longueur maximale autorisée pour le nom du cluster AHV est de 255 caractères. Cependant, si la saisie dépasse 95 caractères, la découverte des biens échoue.<br>Solution de contournement :<br>■ Assurez-vous que le nom du cluster AHV ne dépasse pas 95 caractères. |
| Le travail de découverte échoue avec l'erreur 200. Le planificateur n'a trouvé aucune sauvegarde ni aucun client pour le déploiement de NetBackup. | Assurez-vous que la requête spécifiée dans la politique ou le groupe de machines virtuelles intelligent est correcte. Les machines virtuelles à protéger ont été ajoutées récemment au cluster AHV ou la configuration de machine virtuelle a changé et la découverte automatique ou immédiate n'a pas été déclenchée.<br>■ La découverte du bien ne fonctionne pas si les informations d'authentification du cluster AHV sont ajoutées à l'aide de `tpconfig`.<br>Solution de contournement :<br>Dans l'interface utilisateur Web NetBackup, cliquez sur **Découvrir** pour le cluster AHV spécifié.<br>Vous devez ajouter les informations d'authentification du cluster AHV depuis l'API ou l'interface utilisateur Web NetBackup. |

# Erreurs d'état d'une machine virtuelle nouvellement découverte

Le tableau suivant décrit les problèmes qui peuvent se produire quand vous découvrez des machines virtuelles AHV.

**Tableau 6-3** Erreur d'état d'une machine virtuelle nouvellement découverte

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| L'état de dernière sauvegarde réussie de la machine virtuelle indique qu'elle n'a pas été sauvegardée. | Dans l'interface utilisateur Web NetBackup, l'état de dernière sauvegarde réussie d'une machine virtuelle nouvellement découverte n'indique pas que la machine virtuelle a été sauvegardée.<br><br>Dans certains cas, par exemple, dans celui d'un groupe de machines virtuelles intelligent, une nouvelle machine virtuelle est sauvegardée en fonction de la requête fournie avant sa découverte, comme dans le scénario suivant :<br><br>■ Par défaut, la détection automatique survient toutes les 8 heures.<br>■ Une nouvelle machine virtuelle est ajoutée à l'environnement.<br>■ Un travail de sauvegarde aboutit avant la fin de la découverte.<br>Par exemple, un travail de sauvegarde qui utilise les politiques existantes où la nouvelle machine virtuelle est incluse dans le cadre des critères de sélection de la sauvegarde.<br>■ Dans l'interface utilisateur Web NetBackup, l'état de la dernière sauvegarde réussie de la machine virtuelle n'a pas été mis à jour, ce qui indique que la machine virtuelle n'a pas été sauvegardée.<br><br>Solution de contournement :<br><br>■ Si vous rencontrez un problème semblable, vous pouvez toujours parcourir les points de récupération et les récupérer.<br>Cependant, ce n'est qu'une fois que la découverte est déclenchée sur le cluster et qu'une autre sauvegarde de la machine virtuelle s'est terminée correctement après la découverte, que l'état de la dernière sauvegarde correcte est mis à jour. |

# Erreur lors de la sauvegarde des machines virtuelles AHV

Le tableau suivant décrit les problèmes qui peuvent se produire lorsque vous sauvegardez des machines virtuelles AHV :

**Tableau 6-4** Erreur lors de la sauvegarde des machines virtuelles AHV

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Après une opération de sauvegarde NetBackup, le snapshot de machine virtuelle n'est pas supprimé sur le cluster AHV. | Si un disque connecté à la machine virtuelle est dans un état inactif, le cluster AHV ne supprime pas le snapshot de machine virtuelle à l'issue d'une opération de sauvegarde.<br>Solution de contournement :<br>■ Avant l'opération de sauvegarde, vérifiez que les disques connectés à la machine virtuelle sont actifs.<br>■ Pour éviter qu'un disque dont l'état est inactif soit connecté à la machine virtuelle, assurez-vous qu'aucun disque n'y est connecté pendant son exécution. |
| Le service MSiSCSI est désactivé. Activez le service MSiSCSI sur l'hôte de sauvegarde. | Activez le service MSiSCSI (Microsoft iSCSI Initiator Service) sur l'hôte de sauvegarde Windows et exécutez le travail à nouveau. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
| --- | --- |
| Impossible d’établir une connexion. Vérifiez que le service iSCSI est installé et en cours d’exécution. | |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| | ■ Pour Windows : activez le service d'initiateur iSCSI Microsoft sur l'hôte de sauvegarde.<br>**Remarque :** Une erreur est renvoyée uniquement sous Windows.<br>■ Sous Linux, cette erreur s'affiche sous la forme d'un avertissement et revient à l'utilisation du NFS pour la sauvegarde/restauration. Si vous utilisez les services de données iSCSI segmentés, la sauvegarde/restauration échoue.<br>Assurez-vous que l'hôte de sauvegarde est ajouté à l'option `Filesystem Whitelists` dans l'interface utilisateur de Nutanix pour que les sauvegardes fonctionnent avec le transport NFS.<br>Pour que Linux utilise iSCSI : installez/activez le package d'initiateur iSCSI sur l'hôte de sauvegarde et exécutez le travail de nouveau.<br>■ Vérifiez la connectivité à l'aide de la commande suivante sur un hôte Linux : `iscsiadm -m discovery -t sendtargets -p` *`correct IP as per configured iSCSITargetType`*<br>Utilisez l'adresse IP suivante en fonction de votre type de transport iSCSI :<br>■ Services de données iSCSI : utilisez l'adresse IP des services de données iSCSI de la page de détails du cluster.<br>■ Type segmenté : utilisez les données iSCSI segmentées de la page de détails du cluster SEGMENTED_SPECIFIC.<br>■ Type spécifié segmenté : utilisez l'adresse IP virtuelle spécifiée lors de la configuration du cluster dans NetBackup.<br>■ Vérifiez la connectivité à l'aide de la commande suivante sur l'hôte Windows :<br>■ Cliquez sur **Gestionnaire de serveur -> Outils -> Initiateur iSCSI**. La boîte de dialogue des **propriétés de l'initiateur iSCSI** s'ouvre.<br>■ Cliquez sur **Discovery > Discovery portal** et fournissez l'adresse IP en fonction du type de cible iSCSI configuré pour le cluster AHV.<br>■ Default : utilisez l'adresse IP des services de données iSCSI de la page de détails du cluster.<br>■ SEGMENTED : utilisez les données iSCSI segmentées |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| | de la page de détails du cluster.<br>■ SEGMENTED_SPECIFIC : utilisez l'adresse IP virtuelle spécifiée lorsque vous avez configuré le cluster dans NetBackup.<br>■ Si vous obtenez l'erreur mentionnée lorsque l'appliance Flex ou Flex Scale est utilisée comme hôte de sauvegarde/récupération :<br>■ Modifiez la configuration pour utiliser l'option par défaut qui utilise le transport NFS.<br>■ Utilisez un autre hôte de sauvegarde/récupération qui dispose de la configuration iSCSI et réseau requise.<br>■ Mettez à jour le plan de protection pour utiliser un hôte de sauvegarde spécifique.<br>■ Utilisez un hôte de sauvegarde qui dispose de la configuration iSCSI et réseau requise. |
| Échec d'authentification. Vérifiez si l'initiateur CHAP fourni est correct. | Soit la clé CHAP fournie n'est pas valide, soit le nom d'initiateur iSCSI n'est pas unique pour chaque hôte de sauvegarde/récupération. Définissez un nom d'initiateur iSCSI unique pour chaque hôte de sauvegarde/récupération. |
| Échec de l'obtention d'une adresse IP de service de données externe pour iSCSI. Exécutez à nouveau le travail après avoir défini l'adresse IP sur le cluster Nutanix : {nom_de_cluster Nutanix AHV}. | Définissez l'adresse IP du service de données externe pour iSCSI sur le cluster Nutanix AHV. Pour plus de détails, consultez Se reporter à "Conditions requises pour la configuration du cluster Nutanix AHV" à la page 21..<br>**Remarque :** Sous Linux, le travail bascule vers NFS pour la sauvegarde/restauration. |
| La version de NetBackup n'est pas prise en charge pour un ou plusieurs hôtes de sauvegarde. Utilisez NetBackup 9.1 ou une version ultérieure sur tous les hôtes de sauvegarde Linux ou Windows afin d'utiliser l'option d'hôte de sauvegarde Automatique du plan de protection Nutanix. | Cette erreur survient lorsque l'option **Automatique** est sélectionnée pour les hôtes de sauvegarde du plan de protection Nutanix. Mettez à niveau l'hôte de sauvegarde vers la version la plus récente de NetBackup. |
| Pour l'équilibrage de charge du serveur de médias NetBackup, assurez-vous que les hôtes de sauvegarde disposent du système d'exploitation<br>Red Hat Enterprise Linux,<br>SUSE Linux Enterprise Server ou Microsoft Windows. | Cette erreur survient lorsque l'option **Automatique** est sélectionnée pour les hôtes de sauvegarde du plan de protection Nutanix.<br>Pour Nutanix AHV, les serveurs de médias pris en charge sont :<br>■ Red Hat Enterprise Linux<br>■ SUSE Linux Enterprise Server<br>■ Système d'exploitation Microsoft Windows |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| La version existante de NetBackup sur le serveur de médias ne prend pas en charge la planification de sauvegarde incrémentielle. | Mettez à niveau NetBackup vers la version la plus récente sur l'hôte de sauvegarde. |
| Impossible de définir les limites de ressource pour des clusters Nutanix spécifiques | Si les clusters pour lesquels la limite de ressource est définie sont supprimés de l'environnement NetBackup, dans certains cas, l'option **+ Ajouter** est désactivée pour définir la limite de ressource.<br>Action recommandée<br>Supprimez la limite de ressources pour les clusters supprimés, puis définissez-la pour le reste des clusters. |
| Les travaux de snapshot échouent et renvoient le code d'erreur 156 avec les détails de travail suivants :<br>`Critical bpbrm (pid=30139) from client 9c5dcb07-65d2 -4761-b861-9e517edcf5b6_ <Nutanix-cluster>`<br>`abc.cbus.com FTL - Value 2 that specifies GUID is not supported for the nameuse` | Si vous créez un plan de protection en utilisant **Options de sauvegarde > Sélectionner le serveur ou l'hôte à utiliser pour les sauvegardes > Automatique** alors que l'unité de stockage sélectionnée est configurée avec des serveurs de médias, que ce soit avec NetBackup 9.1 ou des versions précédentes, et que ce plan de protection est utilisé pour sauvegarder les machines virtuelles AHV ou le groupe de machines virtuelles intelligent, le travail de snapshot risque d'échouer.<br>**Action recommandée**<br>Tous les serveurs de médias configurés dans l'unité de stockage sélectionnée doivent être mis à niveau vers la version 9.1 de NetBackup.<br>Pour éviter les échecs des travaux alors que des mises à niveau d'autres serveurs de médias sont en cours, dans la section **Protection > Personnaliser la protection > Options de sauvegarde**, sélectionnez manuellement un serveur de médias ou un hôte de sauvegarde en tant que serveur ou hôte de sauvegarde en remplacement de l'option par défaut, **Automatique**. Il est recommandé d'utiliser un serveur de médias déjà mis à niveau. Une fois la mise à niveau de tous les serveurs de médias terminée, utilisez **Protection > Restaurer les paramètres d'origine** pour rétablir la configuration d'origine. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Erreur 1<br><br>`iscsiadm: Could not login to [iface: default, target: iqn.2010-06.com.nutanix: nbubackup -2d29da9d-f964-4157-9595-f0319090bb01-tgt0, portal: xx.xx.xx.xx,3260]`<br><br>`iscsiadm: initiator reported error (24 - iSCSI login failed due to authorization failure)`<br><br>`iscsiadm: Could not log into all portals`<br><br>Erreur 2<br><br>`iscsiadm: Could not execute operation on all records: encountered iSCSI database failure`<br><br>Erreur 3<br><br>`iscsiadm: could not read session targetname: 5`<br><br>`iscsiadm: could not find session info for session28` | Ces erreurs sont visibles dans l'onglet des détails des travaux réussis pour les travaux de sauvegarde/restauration. Ces erreurs sont renvoyées après exécution de la commande `iscsiadm`. Elles sont intermittentes et peuvent se produire en raison d'une charge élevée sur le réseau iSCSI. NetBackup fait une nouvelle tentative pour corriger ces erreurs. Lorsqu'elle réussit, le travail de sauvegarde/restauration aboutit également.<br><br>**Action recommandée**<br><br>Aucune action n'est nécessaire au niveau de NetBackup. L'utilisateur peut dépanner la commande `iscsiadm` et s'assurer que l'installation/la configuration iSCSI est correcte pour éviter de telles erreurs. |
| `iscsid: Ignoring CHAP algorithm request for MD5 due to crypto lib configuration iscsid: Couldn't set CHAP algorithm list` | Consultez la page In FIPS enabled environment, NetBackup backup/restore of Nutanix AHV VMs (Virtual Machines) using iSCSI fails |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Code d'erreur : 4798<br>L'option Use Prism Central server for this cluster n'est pas sélectionnée pour le cluster AHV. | Le travail de découverte pendant la sauvegarde peut échouer avec l'erreur pour le groupe de machines virtuelles intelligent Nutanix.<br>Recherchez et corrigez les causes possibles suivantes pour le groupe de machines virtuelles intelligent :<br>■ Le groupe a été créé avec le filtre de catégorie parmi les requêtes de filtre ET<br>■ Un ou plusieurs clusters Nutanix sont actualisés après la création du groupe de machines virtuelles intelligent afin d'utiliser l'option désélectionnée **Utiliser le serveur Prism Central pour ce cluster** ; ET l'opération **Sauvegarder maintenant** est déclenchée sur ce type de groupe de machines virtuelles intelligent. |
| Message d'erreur :<br>Impossible de trouver l'instance de Prism Central pour le cluster AHV, serveur = *Détails du serveur* | Le travail de sauvegarde échoue avec l'erreur indiquée.<br>Recherchez et corrigez les causes possibles suivantes :<br>■ Dans un groupe de machines virtuelles intelligent composé d'un ou de plusieurs clusters issus du même serveur Prism Central pour lequel un filtre de catégorie est défini, lorsque la protection de groupe de machines virtuelles intelligent est déclenchée, le serveur Prism Central est supprimé ou inaccessible.<br>■ Dans un groupe de machines virtuelles intelligent composé de deux clusters ou plus issus de serveurs Prism Central différents pour lequel un filtre de catégorie est défini, lorsque la protection du groupe de machines virtuelles intelligent est déclenchée, le serveur Prism Central est supprimé ou inaccessible. |
| Message d'erreur :<br>L'abonnement à un plan de protection doit échouer en affichant une erreur.<br>Une demande d'API non valide a été détectée.<br>`error message: backupHost: Backup host with a NetBackup version earlier than 10.4 is not supported for IntelligentVM group Category filter.` | Si un filtre de catégorie est utilisé dans le groupe de machines virtuelles intelligent, l'abonnement à un plan de protection peut échouer avec l'erreur indiquée.<br>Utilisez les correctifs applicables :<br>■ Assurez-vous que l'hôte de sauvegarde indiqué dans le plan de protection est doté de NetBackup 10.4 ou d'une version ultérieure. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Le travail de sauvegarde échoue et renvoie le code d'erreur 800.<br><br>`Error nbjm(pid=113200) NetBackup status: 800, EMM status :Use NetBackup media server version 10.4 or later to protect Nutanix Intelligent VM groups with category filters.`<br><br>`.`<br><br>`Error nbpem(pid=113293) backup of client MEDIA_SERVER exited with status 800 (resource request failed).` | Description<br><br>Cette erreur se produit si vous créez un plan de protection en sélectionnant **Options de sauvegarde > Sélectionner le serveur** ou l'hôte à utiliser pour les **sauvegardes > Automatique** alors que l'unité de stockage sélectionnée est configurée avec des serveurs de médias dotés de versions de NetBackup antérieures à la 10.4. De plus, lorsque ce plan de protection est utilisé pour sauvegarder le groupe de machines virtuelles intelligent avec un attribut de catégorie comme filtre, le travail de sauvegarde échoue.<br><br>Action recommandée :<br><br>Tous les serveurs de médias configurés dans l'unité de stockage sélectionnée doivent être mis à niveau vers NetBackup 10.4. |
| Le travail de sauvegarde échoue avec les messages d'erreur suivants :<br><br>Erreur 1<br><br>`Begin Application Resolver:Resolver Discovery`<br><br>Erreur 2<br><br>`Error nbpem(pid=98395) Invalid URI.`<br><br>Erreur 3<br><br>`Error nbpem (pid=98395) backup of client falcna12c3.abcus.com exited with status 4232 Invalid Discovery Query URI).` | Description<br><br>Lorsque le groupe de machines virtuelles intelligent est abonné à un plan de protection dont l'hôte de sauvegarde est doté de la version 10.3 ou d'une version antérieure et qu'il est modifié à l'aide du filtre de catégorie.<br><br>Lorsque le travail de sauvegarde est exécuté, il échoue avec un message d'erreur, car le filtre de catégorie n'est pas connu des versions plus anciennes des hôtes de sauvegarde.<br><br>Action recommandée :<br><br>Mettez à niveau l'hôte de sauvegarde vers la version 10.4 ou une version ultérieure en personnalisant le plan de protection. Pour plus de détails Se reporter à "Personnaliser les paramètres de protection pour un bien AHV" à la page 56. |

# Erreur lors de la restauration de machines virtuelles AHV

Le tableau suivant décrit le problème qui peut se produire lorsque vous restaurez une machine virtuelle AHV.

**Tableau 6-5** Erreur lors de la restauration des machines virtuelles AHV

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Échec de la récupération de la machine virtuelle à un autre emplacement sur un serveur principal Windows. | Pour un serveur principal NetBackup Windows, assurez-vous que le fichier renommé se termine par une ligne vide. |
| Impossible de modifier le **cluster AHV** lors de la modification de l'emplacement de récupération. | Si vous ne parvenez pas à consulter la liste des clusters AHV, vous n'avez peut-être pas accès aux clusters AHV dans RBAC.<br>Contactez l'administrateur de sécurité NetBackup pour résoudre ce problème. |
| Lorsqu'une machine virtuelle utilisant le même UUID est présente dans le cluster AHV et que l'option permettant d'écraser la machine virtuelle est désactivée, la vérification de pré-récupération s'effectue correctement, mais la restauration de la machine virtuelle échoue.<br>Le message d'erreur suivant s'affiche :<br>Info `bpVMutil` (`pid=1196`) FTL : la machine virtuelle existe et l'option d'écrasement n'a pas été spécifiée ; impossible de procéder à la restauration. Terminer la restauration ; erreur de restauration de la politique de l'hyperviseur de temps écoulé. (2822) | La vérification de pré-récupération a lieu correctement, car le nom d'affichage est comparé au lieu de l'UUID pour la découverte de la machine virtuelle. Toutefois, si l'option d'écrasement n'est pas définie, le travail de restauration échoue lorsqu'une autre machine virtuelle utilise le même UUID.<br>Solution de contournement :<br>Restaurer la machine virtuelle avec un nouvel UUID.<br>**1** Démarrez le processus de récupération.<br>**2** Sur la page **Options de récupération**, cliquez sur **Avancé**.<br>**3** Activez l'option **Créer un UUID de machine virtuelle**<br>**4** Poursuivez le processus de récupération et cliquez sur **Lancer la récupération** pour lancer la restauration.<br>Écrasez la machine virtuelle dont l'UUID est identique.<br>**1** Démarrez le processus de récupération.<br>**2** Sur la page **Options de récupération**, activez l'option **Écraser la machine virtuelle existante**.<br>**3** Poursuivez le processus de récupération et cliquez sur **Lancer la récupération** pour lancer la restauration. |
| Lorsque vous tentez de récupérer une image de machine virtuelle AHV, importée à partir d'un domaine différent à l'aide de l'interface utilisateur Web, la vérification de pré-récupération échoue et un message vous indique que l'hôte de récupération correspond par défaut à l'hôte d'accès qui a été utilisé pendant la sauvegarde. | Pendant la récupération d'images de machine virtuelle AHV importées, sélectionnez l'hôte d'accès dans le domaine cible comme hôte de récupération ou sélectionnez le serveur principal cible. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Le service `MSiSCSI` est désactivé. Activez le service `MSiSCSI` sur l'hôte de récupération. | Activez le service `MSiSCSI` (Microsoft iSCSI Initiator Service) sur la récupération de sauvegarde Windows et ré-exécutez le travail. |
| Échec de la connexion à l'hôte de récupération. | L'hôte de récupération utilisé pour la restauration sans agent n'est pas accessible.<br>Action recommandée :<br>Assurez-vous que l'hôte de récupération est accessible depuis le serveur principal et qu'un média ou un client NetBackup y est installé. |
| L'hôte de récupération spécifié doit comporter NetBackup 9.1 ou une version ultérieure pour prendre en charge les restaurations sans agent. | Les restaurations sans agent de fichiers ou de dossiers requièrent un hôte de récupération comportant NetBackup 9.1 ou une version ultérieure.<br>Action recommandée :<br>Vérifiez la version de NetBackup sur l'hôte de récupération. Il doit s'agir de la version 9.1 ou d'une version ultérieure.<br>Pour les clients et serveurs NetBackup sous UNIX, consultez le fichier `/usr/openv/netbackup/bin/version`.<br>Pour les serveurs NetBackup sous Windows, consultez le fichier `chemin_installation\netbackup\version.txt`. |
| L'emplacement intermédiaire de l'hôte de récupération n'existe pas. | Le chemin d'accès de l'emplacement intermédiaire n'existe pas sur l'hôte de récupération pour la restauration sans agent.<br>Action recommandée :<br>■ Assurez-vous que le chemin d'accès par défaut ou le chemin configuré par l'utilisateur pour l'emplacement intermédiaire est valide. NetBackup utilise ce qui suit sur l'hôte de récupération ou comme emplacement intermédiaire par défaut :<br>■ Pour UNIX : `{chemininstallation}/openv/tmp/staging`.<br>■ Pour Windows : `{chemininstallation}\Netbackup\Temp\staging\`.<br>■ Assurez-vous que le chemin d'accès de l'emplacement intermédiaire existe. Dans le cas d'un emplacement intermédiaire configuré par l'utilisateur, vérifiez qu'un chemin valide est spécifié sur l'hôte de récupération dans le paramètre `bp.conf` **AGENTLESS_RHOST_STAGING_PATH = "path"**. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Image TAR introuvable dans l'emplacement intermédiaire sur l'hôte de récupération. | Aucune image TAR n'a été trouvée à l'emplacement intermédiaire sur l'hôte de récupération, alors que cela est requis pour la restauration sans agent.<br>Action recommandée :<br>Contactez le support technique de Veritas et communiquez le journal `bpVMutil` qui figure sur l'hôte de récupération. |
| Une erreur interne a provoqué l'échec de la validation de la récupération. | Une erreur interne s'est produite pendant l'exécution des validations de pré-récupération pour la restauration sans agent.<br>Action recommandée :<br>Enregistrez les journaux **bpVMutil** sur l'hôte de récupération et contactez le support technique de Veritas. |
| Espace insuffisant sur l'hôte de récupération. | L'hôte de récupération peut ne pas disposer de suffisamment d'espace pour copier les fichiers sélectionnés à l'emplacement intermédiaire de la restauration sans agent.<br>Action recommandée :<br>Assurez-vous qu'un espace libre suffisant est disponible à l'emplacement intermédiaire de l'hôte de récupération, selon la taille totale des fichiers ou dossiers sélectionnés. Ou sélectionnez un hôte de récupération différent avec suffisamment d'espace libre pour effectuer la restauration sans agent. |
| L'utilitaire TAR est absent de l'hôte cible. | L'utilitaire TAR est introuvable sur l'hôte cible requis pour la restauration sans agent.<br>Action recommandée :<br>Déployez l'utilitaire TAR, puis réessayez. |
| L'emplacement intermédiaire spécifié n'existe pas sur l'hôte cible ou l'utilisateur ne dispose pas de l'autorisation d'accès requise. | Action recommandée :<br>Assurez-vous que l'emplacement intermédiaire de l'hôte cible existe et que l'utilisateur dispose des autorisations suffisantes pour accéder à l'emplacement. |
| L'utilisateur ne dispose pas de l'autorisation requise sur l'emplacement intermédiaire de l'hôte cible. | L'utilisateur ne dispose pas de l'autorisation requise pour procéder à la restauration sur l'hôte cible.<br>Action recommandée :<br>Assurez-vous que l'emplacement intermédiaire de l'hôte cible existe et que l'utilisateur dispose des autorisations suffisantes, en lecture comme en écriture, pour accéder à cet emplacement. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| L'utilisateur ne dispose pas de privilèges racine/d'administrateur. Pour restaurer des fichiers et des dossiers, accordez à l'utilisateur des privilèges racine ou d'administrateur. | L'utilisateur ne dispose pas de l'autorisation requise pour procéder à la restauration sur l'hôte cible.<br>Action recommandée :<br>Utilisez les informations d'authentification d'un membre du groupe d'administrateurs locaux sur l'hôte cible Windows. Pour l'hôte cible Linux, utilisez les informations d'authentification du compte racine ou sudo avec TOUTES les autorisations. |
| Le partage administratif de l'hôte cible n'est pas accessible à partir de l'hôte de récupération. | Le partage administratif de l'hôte distant n'est pas accessible depuis l'hôte de récupération pour procéder à la restauration sans agent.<br>Action recommandée :<br>■ Assurez-vous que les exceptions du pare-feu sont correctement configurées.<br>■ Assurez-vous que le partage de fichiers et d'imprimantes est activé.<br>■ Assurez-vous que l'accès n'est pas bloqué par une politique GPO/de restriction logicielle ou un antivirus.<br>■ Assurez-vous que l'hôte cible est accessible, que les informations d'authentification correctes sont entrées et qu'elles disposent des autorisations nécessaires. |
| Pour la restauration sans agent de fichiers ou dossiers dans un environnement de contrôle de compte d'utilisateur (UAC), fournissez les informations d'authentification d'un utilisateur de domaine faisant partie du groupe d'administrateurs locaux sur l'hôte cible Windows. | Action recommandée :<br>Pour une restauration sans agent dans un environnement de contrôle de compte d'utilisateur (UAC), fournissez les informations d'authentification d'un utilisateur de domaine faisant partie du groupe d'administrateurs locaux sur l'hôte cible Windows. |
| Il est impossible de procéder à une restauration sans agent. | La restauration sans agent a échoué pour une raison inattendue.<br>Action recommandée :<br>Contactez le support technique de Veritas et communiquez les journaux correspondants. |
| Les systèmes d'exploitation ne correspondent pas. Vérifiez que le système d'exploitation de l'hôte de récupération correspond à celui de la machine virtuelle sauvegardée. | La restauration sans agent est possible uniquement si le système d'exploitation de l'hôte de récupération et celui de la machine virtuelle sauvegardée sont identiques.<br>Action recommandée :<br>Utilisez un autre hôte de récupération en vous assurant qu'il repose sur le même système d'exploitation que la machine virtuelle sauvegardée. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Échec de la récupération du système d'exploitation de l'image de sauvegarde. | Impossible de récupérer le système d'exploitation de l'image de sauvegarde pour effectuer une restauration sans agent. Il s'agit d'une erreur interne. |
| Le système d'exploitation de l'hôte de récupération n'est pas compatible avec le mode de communication indiqué. Vérifiez que le système d'exploitation de l'hôte de récupération et le mode de communication indiqué sont compatibles. | Le type de système d'exploitation de l'hôte de récupération et le type de communication fourni dans la demande de vérification de récupération ou de pré-récupération sans agent ne sont pas compatibles.<br>Action recommandée :<br>Assurez-vous que le type de système d'exploitation de l'hôte de récupération et le type de communication sont compatibles. Si l'hôte de récupération utilise :<br>■ Linux : le type de communication doit être `SSH` ;<br>■ Windows : le type de communication doit être `WMI`. |
| La clé privée SSH de l'hôte cible n'est pas valide. | Le champ `sshKey` de la demande de récupération sans agent ou de vérification de pré-récupération doit être valide et la valeur de la clé privée SSH de l'hôte cible doit être renseignée.<br>Action recommandée :<br>Assurez-vous que le champ `sshKey` est spécifié si l'authentification est de type `SSH_KEY`, et qu'il n'est pas vide. |
| Le système d'exploitation de l'hôte cible n'est pas pris en charge pour la restauration sans agent des fichiers ou des dossiers. | Le système d'exploitation de l'hôte cible n'est pas pris en charge, car la restauration sans agent requiert le déploiement de packages de reprise sur l'hôte cible.<br>Action recommandée :<br>SUSE Linux Enterprise Server, Microsoft Windows, Red Hat Enterprise Linux (RHEL) et Ubuntu sont les seules plateformes prises en charge.<br>Pour connaître les plates-formes prises en charge pour cette fonction, consultez la liste de compatibilité du client NetBackup (en anglais) sur URL:\nhttp://www.netbackup.com/compatibility. |
| Nom d'utilisateur ou mot de passe de l'hôte cible non valide. | Vous devez spécifier les champs de nom d'utilisateur et de mot de passe dans les informations d'authentification de la demande de vérification de pré-récupération ou de récupération sans agent.<br>Action recommandée :<br>Dans les informations d'authentification de la demande de vérification de pré-récupération et de récupération sans agent, assurez-vous que les champs de nom d'utilisateur et de mot de passe sont spécifiés, corrects et ne sont pas vides. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| L'emplacement intermédiaire de l'hôte cible contient des caractères non ASCII. | L'emplacement intermédiaire de l'hôte cible prend uniquement en charge les caractères ASCII.<br>Action recommandée :<br>Fournissez un emplacement intermédiaire personnalisé sur l'hôte cible en veillant à utiliser uniquement des caractères ACSII. |
| Le chemin d'accès spécifié n'existe pas sur le disque local. | L'emplacement intermédiaire de l'hôte cible ne doit pas utiliser le chemin d'accès réseau.<br>Action recommandée :<br>Pour l'hôte cible, spécifiez un emplacement intermédiaire personnalisé résidant sur son disque local. |
| La connexion WMI à l'hôte cible a échoué. | La connexion WMI à l'hôte cible a échoué sur l'hôte de récupération.<br>Action recommandée :<br>■ Pour se connecter aux services WMI et DCOM, l'utilisateur doit disposer de l'autorisation requise pour se connecter au service WMI distant.<br>■ Des exceptions de pare-feu sont définies pour autoriser le trafic WMI à travers le pare-feu.<br>■ L'accès n'est pas bloqué par une politique GPO/de restriction logicielle ou un antivirus.<br>■ Assurez-vous que l'hôte cible est accessible. Validez les informations d'authentification de l'hôte cible donné.<br>■ Assurez-vous que la relation de confiance de l'hôte cible avec le domaine est intacte. Si les communications s'effectuent sur plusieurs domaines, une relation de confiance bidirectionnelle doit exister entre ces différents domaines. |
| Impossible de trouver le fichier spécifié sur le serveur distant. | Impossible de trouver le fichier spécifié sur le serveur distant.<br>Action recommandée :<br>Assurez-vous que l'emplacement intermédiaire spécifié sur l'hôte cible existe ou spécifiez un autre emplacement intermédiaire valide. |
| Un fichier porte le même nom que le répertoire. | L'hôte cible comporte un fichier portant le même nom que le chemin d'accès au répertoire fourni comme emplacement intermédiaire.<br>Action recommandée :<br>Vérifiez si l'hôte distant comporte un fichier ayant le même nom et le même chemin que l'emplacement intermédiaire. Si c'est le cas, renommez ou supprimez ce fichier. ou spécifiez un autre emplacement intermédiaire. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Échec de la validation des privilèges d'administrateur pour l'utilisateur. | L'utilisateur hôte cible ne possède pas les privilèges d'administrateur requis pour exécuter la restauration sans agent des fichiers et des dossiers.<br>Action recommandée :<br>Utilisez les informations d'authentification d'un membre du groupe d'administrateurs locaux sur l'hôte cible Windows.<br>Pour l'hôte cible Linux, utilisez les informations d'authentification du compte racine ou sudo avec **TOUTES** les autorisations. |
| Échec de la connexion d'une ressource réseau à l'aide de l'API Windows. | Le partage administratif de l'hôte cible n'est pas accessible depuis l'hôte de récupération pour procéder à la restauration sans agent des fichiers ou des dossiers.<br>Action recommandée :<br>Dans le cadre de la restauration sans agent des fichiers et des dossiers, le partage administratif SMB est créé à partir de l'hôte de récupération sur l'hôte cible à partir des informations d'authentification fournies par l'utilisateur. Cette erreur se produit généralement lorsque l'hôte cible de la restauration sans agent repose sur un système d'exploitation Windows et que le partage administratif de l'hôte cible n'est pas accessible depuis l'hôte de récupération. Assurez-vous que les conditions suivantes sont réunies sur l'hôte cible.<br>■ Les exceptions du pare-feu sont configurées correctement.<br>■ Le partage de fichiers et d'imprimantes est activé.<br>■ L'accès n'est pas bloqué par une politique GPO/de restriction logicielle ou un antivirus.<br>■ L'hôte cible est accessible avec des informations d'authentification valides. |
| Impossible de récupérer le répertoire d'origine de l'utilisateur sur l'hôte cible. Spécifiez l'emplacement intermédiaire personnalisé. | L'emplacement intermédiaire par défaut de l'utilisateur (répertoire d'origine) n'a pas pu être récupéré sur l'hôte cible. L'utilisateur doit entrer un chemin d'accès d'emplacement intermédiaire personnalisé valide.<br>Action recommandée :<br>Assurez-vous que le répertoire d'origine de l'utilisateur existe ou essayez avec un emplacement intermédiaire personnalisé valide. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Échec de l'établissement d'une session SSH avec l'hôte. | Assurez-vous que tous les critères suivants sont réunis, puis réessayez.<br>■ Aes256-ctr est le chiffrement pris en charge qui est utilisé pour la communication. Assurez-vous que ce chiffrement est pris en charge à la fois sur l'hôte de récupération et sur l'hôte cible.<br>■ Assurez-vous qu'au moins l'un des protocoles HMAC (Hash-based Message Authentication Code) suivants est pris en charge à la fois sur l'hôte de récupération et sur l'hôte cible :<br>  ■ `hmac-sha2-256`<br>  ■ `hmac-sha2-512`<br>■ Assurez-vous que la clé d'hôte est générée selon l'une des méthodes suivantes :<br>  ■ `ECDSA_SHA2_NISTP256`<br>  ■ `ECDSA_SHA2_NISTP384`<br>  ■ `ECDSA_SHA2_NISTP521`<br>  ■ `SSH_RSA`<br>  ■ `SSH_DSS` |
| Échec de la vérification de la signature de la clé SSH de l'hôte. | La signature de clé SSH de l'hôte cible fournie est incorrecte.<br>Action recommandée :<br>Vérifiez la signature de clé SSH de l'hôte cible et réessayez. |
| Échec de l'authentification de l'hôte avec le nom d'utilisateur ou le mot de passe fourni. | L'authentification de l'hôte cible a échoué avec le nom d'utilisateur ou le mot de passe fourni.<br>Action recommandée :<br>Assurez-vous que le nom d'utilisateur ou le mot de passe de l'hôte cible est correct, puis réessayez. |
| Echec de l'authentification de l'hôte avec la clé SSH spécifiée. | L'authentification de l'hôte cible a échoué avec la clé SSH fournie.<br>Action recommandée :<br>Vérifiez la clé privée SSH, ainsi que la phrase de passe de la clé si elle est utilisée pour générer la clé privée SSH de l'hôte cible, puis réessayez. Assurez-vous que la clé publique correspondante est présente dans le fichier `authorized_keys`, dans le dossier `/root/.ssh` de l'hôte cible. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| La méthode de clé d'hôte de la signature de clé SSH correspondante est introuvable sur l'hôte cible. | La méthode de clé d'hôte de la signature de clé SSH spécifiée est introuvable sur l'hôte cible.<br>Action recommandée :<br>Assurez-vous que la méthode de clé d'hôte prise en charge pour la signature de clé SSH spécifiée est disponible sur l'hôte cible ou fournissez la signature SSH de la méthode de clé d'hôte qui est configurée sur l'hôte cible. |
| La restauration échoue si vous restaurez des fichiers individuels sur une machine virtuelle comportant le logiciel client NetBackup. | Lors d'une restauration de fichiers individuels sur une machine virtuelle avec le client NetBackup, assurez-vous qu'aucun pare-feu n'empêche la restauration. Si un pare-feu arrête la restauration, désactivez-le et relancez la restauration. |
| Points de montage non disponibles lors de la restauration de fichiers à partir d'une machine virtuelle Linux | Pour les machines virtuelles Linux, seuls les systèmes de fichiers `ext2`, `ext3`, `ext4` et `xfs` sont pris en charge pour la restauration de fichiers individuels.<br>Si une partition est formatée avec un autre système de fichiers, la sauvegarde s'effectue correctement, mais NetBackup ne peut pas mapper les adresses des fichiers attribuées par le système de fichiers. En conséquence, NetBackup ne peut pas restaurer individuellement des fichiers de cette partition. Seuls les fichiers qui se trouvaient sur des partitions `ext2`, `ext3`, `ext4` et `xfs` peuvent être restaurés individuellement.<br>**Remarque :** Pour restaurer des fichiers individuels à partir de leurs points de montage initiaux, la partition « / » (racine) doit être au format `ext2`, `ext3`, `ext4` ou `xfs`. Si la partition « / » (racine) est formatée avec un système de fichiers différent, tel que `ButterFS`, les points de montage ne peuvent pas être résolus. Dans ce cas, vous pouvez restaurer les fichiers `ext2`, `ext3`, `ext4` ou `xfs` depuis le niveau /dev (par exemple, /dev/sda1). Vous ne pouvez pas restaurer les fichiers depuis le niveau initial de leur point de montage. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Pour les machines virtuelles Linux dépourvues de convention de nommage des périphériques persistants, la présence de plusieurs contrôleurs de disques, comme IDE, SCSI et SATA, peut compliquer la récupération des différents fichiers. | Ce problème se produit parce que la présence de noms de périphériques non-persistants, tels que `/dev/sda et /dev/sdb`, peut générer des modifications de point de montage inattendues au redémarrage. Si la machine virtuelle comporte à la fois un disque SCSI et un disque SATA, l'interface de navigation **Restaurer les fichiers et les dossiers > Ajouter des fichiers et des dossiers** peut présenter des points de montage incorrects pour les fichiers de la machine virtuelle. Par exemple, lorsque vous parcourez les fichiers pour la restauration, les fichiers qui figurent à l'origine dans `/vol_a` sont susceptibles d'apparaître dans `/vol_b`. La restauration s'effectue correctement, mais les fichiers restaurés peuvent ne pas être dans leur répertoire d'origine.<br><br>**Action recommandée :**<br><br>Recherchez les fichiers sur la machine virtuelle et déplacez-les vers les emplacements appropriés. Pour éviter ce problème sur les machines virtuelles Linux avec plusieurs contrôleurs de disques, Veritas vous recommande d'utiliser une méthode d'attribution de nom de périphérique persistant pour le montage des systèmes de fichiers. Si la méthode de nommage persistant est en place, le montage de périphérique est cohérent et ce problème ne se présentera pas lors de la restauration de fichiers issus de sauvegardes futures. Pour nommer un périphérique persistant, vous pouvez monter les périphériques par UUID.<br><br>Voici un exemple du fichier `/etc/fstab` contenant des périphériques montés à l'aide des UUID :<br><br>■ UUID=93a21fe4-4c55-4e5a-8124-1e2e1460fece /boot ext4 defaults 1 2.<br>■ UUID=55a24fe3-4c55-4e6a-8124-1e2e1460fadf /vola ext3 defaults 0 0.<br><br>Pour trouver les UUID de périphérique, utilisez l'une des commandes suivantes :<br><br>■ `blkid`<br>■ `ls -l /dev/disk/by-uuid/` |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Pour les machines virtuelles Ubuntu sans nommage de périphérique persistant, l'interface de navigation **Restaurer les fichiers et les dossiers > Ajouter des fichiers et des dossiers** peut afficher des points de montage incorrects pour les fichiers de la machine virtuelle et la récupération de fichiers individuels risque d'échouer. | Ce problème se produit car la présence de noms de périphériques non-persistants peut générer des modifications de point de montage inattendues. Pour la machine virtuelle Ubuntu, l'interface de navigation **Restaurer les fichiers et les dossiers > Ajouter des fichiers et des dossiers** peut présenter des points de montage incorrects pour les fichiers de la machine virtuelle. Par exemple, les fichiers et les dossiers peuvent apparaître sous `/dev/ubuntu-vg/ubuntu-lv` quand vous parcourez les fichiers à restaurer et la récupération de fichiers individuels risque d'échouer.<br>**Action recommandée :**<br>Pour éviter ce problème sur les machines virtuelles Ubuntu, Veritas recommande d'utiliser une méthode de nommage de périphérique persistant pour le montage des systèmes de fichiers. Si la méthode de nommage persistant est en place, le montage de périphérique est cohérent et ce problème ne se présentera pas lors de la restauration de fichiers issus de sauvegardes futures. Pour nommer un périphérique persistant, vous pouvez monter les périphériques par UUID.<br>Voici un exemple du fichier `/etc/fstab` contenant des périphériques montés à l'aide des UUID :<br>■ UUID=93a21fe4-4c55-4e5a-8124-1e2e1460fece /boot ext4 defaults 1 2.<br>■ UUID=55a24fe3-4c55-4e6a-8124-1e2e1460fadf /vola ext3 defaults 0 0.<br>Pour trouver les UUID de périphérique, utilisez l'une des commandes suivantes :<br>■ `blkid`<br>■ `ls -l /dev/disk/by-uuid/` |
| Impossible d'effectuer la restauration avec agent si l'hôte cible choisi est Linux 8.1. | NetBackup ne prend pas en charge la restauration avec agent pour la plate-forme Linux 8.1.<br>Concernant NetBackup 8.1, la restauration avec agent est prise en charge uniquement pour la plate-forme Windows, pas pour la plate-forme Linux.<br>Action recommandée<br>Mettez à niveau l'hôte cible Linux vers la version 8.2 ou une version ultérieure pour les restaurations basées sur agent. |

| Message d'erreur ou cause de l'erreur | Explication et action recommandée |
|---|---|
| Échec de la création de la machine virtuelle. Impossible d'effectuer la restauration.<br>`bpVMutil`<br>`pid=3144` | Si un hôte de sauvegarde dont la version est antérieure à 10.1.1 est utilisé pour restaurer des machines virtuelles dans un environnement cloud privé virtuel (VPC), le travail de restauration échoue.<br>Action recommandée<br>Utilisez au minimum la version 10.1.1 de l'hôte de sauvegarde pour restaurer les machines virtuelles qui appartiennent à un environnement VPC. |
| Le travail de restauration à partir d'un snapshot se termine avec un état de réussite partielle. | Le travail de restauration à partir d'un snapshot se termine avec un état de réussite partielle si la configuration correcte n'est pas présente sur le cluster AHV conformément à l'option de transport iSCSI.<br>Solution de contournement<br>Vérifiez et corrigez l'erreur suivante en fonction du paramètre de transport iSCSI :<br>■ Default : l'adresse IP des services de données iSCSI est configurée.<br>■ Segmented : l'adresse IP segmentée n'est pas configurée.<br>■ Segmented_specified : l'interface iSCSI segmentée n'est pas configurée ou l'adresse IP spécifiée ne correspond à l'adresse IP virtuelle d'aucune des interfaces iSCSI segmentées configurées. |

Chapitre 7

# API et options de ligne de commande pour AHV

Ce chapitre traite des sujets suivants :

- Utilisation des API et des options de ligne de commande pour gérer, protéger ou récupérer des machines virtuelles AHV
- Options NetBackup supplémentaires pour la configuration de AHV
- Informations supplémentaires sur le fichier renommé

## Utilisation des API et des options de ligne de commande pour gérer, protéger ou récupérer des machines virtuelles AHV

Cette rubrique répertorie les API et les options de ligne de commande permettant de protéger ou de récupérer les machines virtuelles AHV. Seules les options et les variables importantes sont mentionnées dans cette rubrique.

Cette rubrique comprend les sections suivantes :

- Se reporter à la section intitulée « Ajout d'un cluster AHV » à la page 121.
- Se reporter à la section intitulée « Définition des API des paramètres CHAP pour iSCSI » à la page 121.
- Se reporter à la section intitulée « Création d'une politique de sauvegarde de machine virtuelle AHV » à la page 122.
- Se reporter à la section intitulée « Vérification de pré-récupération de la machine virtuelle AHV à l'emplacement d'origine » à la page 124.

- Se reporter à la section intitulée « Vérification de pré-récupération de la machine virtuelle AHV à un autre emplacement » à la page 125.
- Se reporter à la section intitulée « Restauration de la machine virtuelle AHV à l'emplacement d'origine » à la page 126.
- Se reporter à la section intitulée « Restauration de la machine virtuelle AHV à un autre emplacement » à la page 128.

Pour obtenir des informations détaillées sur les API et les lignes de commande, utilisez les références suivantes :

- Toutes les API NetBackup sont répertoriées à l'emplacement suivant : Services and Operations Readiness Tools (SORT) > Base de connaissances > Documents
- Pour plus d'informations sur les commandes, consultez le *Guide de référence des commandes NetBackup*.

## Ajout d'un cluster AHV

**Tableau 7-1** Ajout d'un cluster AHV

| API ou options de ligne de commande | Options et variables importantes |
|---|---|
| `POST /netbackup/asset-service/queries`<br><br>`GET /netbackup/asset-service/queries/{aqcId}` | ▪ `clusterName` est le nom du cluster AHV.<br>▪ `backuphost` est le nom d'hôte d'un client NetBackup.<br>▪ `credentialName` correspond aux informations d'authentification associées au cluster AHV.<br>**Remarque :** Les informations d'authentification doivent inclure la mention `credentialName`. |
| Commande `tpconfig` | ▪ `virtual_machine` est le nom du cluster AHV.<br>▪ `vm_type` a la valeur 9. Le chiffre 9 représente le cluster AHV. |

## Définition des API des paramètres CHAP pour iSCSI

**Tableau 7-2** Définition des API des paramètres CHAP pour iSCSI

| API ou options de ligne de commande | Options et variables importantes |
|---|---|
| `GET /netbackup/config/iscsi-settings/{workloadType}` | ▪ `workloadType` spécifie la charge de travail prise en charge.<br>▪ Permet d'obtenir les paramètres iSCSI globaux pour le type de charge de travail spécifié. |

| API ou options de ligne de commande | Options et variables importantes |
|---|---|
| `POST /netbackup/config/iscsi-settings/{workloadType}` | ■ Permet de modifier les paramètres iSCSI globaux pour le type de charge de travail spécifié.<br>■ `authType` indique le type d'authentification. Par exemple :<br>■ `ONEWAY_CHAP`<br>■ `MUTUAL_CHAP_AUTOMATIC`<br>■ `passwordRenewalIntervalDays` s'applique uniquement à l'option CHAP mutuel - automatique.<br>**Remarque :** Les valeurs valides sont 1 à 365 jours. |

## Création d'une politique de sauvegarde de machine virtuelle AHV

**Tableau 7-3** Création d'une politique de sauvegarde de machine virtuelle AHV

| API ou options de ligne de commande | Options et variables importantes |
|---|---|
| `POST /netbackup/config/policies/` | ■ `policyType` est `Hypervisor`.<br>■ `backuphost` est le nom d'hôte d'un client NetBackup qui effectue des sauvegardes pour les machines virtuelles.<br>■ Ajoutez `Add useVirtualMachine = 6` pour Nutanix AHV.<br>■ `snapshotMethodArgs` peut avoir les valeurs suivantes pour sauvegarder une machine virtuelle à l'aide de l'UUID de machine virtuelle :<br>■ Dans `backupSelections` > `selections`, utilisez l'option de filtre sous la forme `Nutanix-ahv:/?filter=uuid Equal <uuid_filter>"` pour filtrer les machines virtuelles AHV correspondant à un UUID spécifique.<br>À l'exception de `UUID`, vous pouvez utiliser les autres critères de filtre mentionnés pour les groupes de machines virtuelles intelligents. |

| API ou options de ligne de commande | Options et variables importantes |
|---|---|
| Commande `admincmd` | ■ Dans `bpplclients -add <discoveryhost> Hypervisor Hypervisor`, l'hôte de découverte de l'hyperviseur est un hôte Windows ou Linux sur liste d'autorisation.<br>■ Dans `bpplinfo`, le type de politique (`-pt`) est `Hypervisor`.<br>■ Dans `bpplinclude`, utilisez l'option de filtre sous la forme `Nutanix-ahv:/?filter=uuid Equal <uuid_filter>"` pour filtrer les machines virtuelles AHV correspondant à un UUID spécifique.<br>■ Dans `bpplinfo`<br>■ La valeur `use_virtual_machine` est de **6** pour les machines virtuelles AHV.<br>■ La valeur de `snapshot_method` est `Hypervisor_snap`. |

La création de la politique n'affecte pas les autres commandes, telles que la création de la planification ou le déclenchement de la sauvegarde. Pour plus d'informations sur les commandes, consultez le *Guide de référence des commandes NetBackup*.

## Vérification de pré-récupération de la machine virtuelle AHV à l'emplacement d'origine

**Tableau 7-4** Vérification de pré-récupération de la machine virtuelle AHV à l'emplacement d'origine

| API ou options de ligne de commande | Options et variables importantes |
|---|---|
| `POST /netbackup/recovery/workloads /nutanix-ahv/scenarios/full-vm /pre-recovery-check` | ■ `client` est l'identifiant qui a été utilisé au moment de la sauvegarde. Il peut s'agir du `displayName` ou du `UUID`.<br>■ `ahvCluster` est le nom de l'autre cluster AHV.<br>■ `recoveryHost` est le serveur qui doit être utilisé comme hôte de récupération de la machine virtuelle pour effectuer cette vérification de pré-récupération.<br>■ `vmDisks` représente un ou plusieurs disques de machine virtuelle.<br>■ `source` est le chemin d'accès source du disque de la machine virtuelle. Il doit être au format `/conteneur_stockage/uuid_disque`.<br>■ `destination` est le chemin d'accès de destination du disque de la machine virtuelle. Il doit être au format `/conteneur_stockage`.<br>■ Définissez les valeurs suivantes :<br>`powerOnAfterRecovery`<br>`overwriteExistingVm`<br>`removeNetworkInterfaces`<br>`retainVmGuid`<br>`retainNicMacAddress` |

## Vérification de pré-récupération de la machine virtuelle AHV à un autre emplacement

**Tableau 7-5** Vérification de pré-récupération de la machine virtuelle AHV à un autre emplacement

| API ou options de ligne de commande | Options et variables importantes |
|---|---|
| `POST /netbackup/recovery/workloads /nutanix-ahv/scenarios/full-vm /pre-recovery-check` | ■ `client` est l'identifiant qui a été utilisé au moment de la sauvegarde. Il peut s'agir du `displayName` ou du `UUID`.<br>■ `ahvCluster` est le nom de l'autre cluster AHV.<br>■ `recoveryHost` est le serveur qui doit être utilisé comme hôte de récupération de la machine virtuelle pour effectuer cette vérification de pré-récupération.<br>■ `vmDisks` représente un ou plusieurs disques de machine virtuelle.<br>■ `source` est le chemin d'accès source du disque de la machine virtuelle. Il doit être au format `/conteneur_stockage/uuid_disque`.<br>■ `destination` est le chemin d'accès de destination du disque de la machine virtuelle. Il doit être au format `/conteneur_stockage`.<br>■ Définissez les valeurs suivantes :<br>`powerOnAfterRecovery`<br>`overwriteExistingVm`<br>`removeNetworkInterfaces`<br>`retainVmGuid`<br>`retainNicMacAddress` |

## Restauration de la machine virtuelle AHV à l'emplacement d'origine

**Tableau 7-6** Restauration de la machine virtuelle AHV à l'emplacement d'origine

| API ou options de ligne de commande | Options et variables importantes |
|---|---|
| `POST /netbackup/recovery/workloads/ahv/scenarios/full-vm/recover` | ■ `client` est l'identifiant qui a été utilisé au moment de la sauvegarde. Il peut s'agir du `display name` ou du `UUID`.<br>■ `recoveryHost` est le serveur qui doit être utilisé comme hôte de récupération de la machine virtuelle pour effectuer cette récupération.<br>■ Définissez les valeurs suivantes :<br>`powerOnAfterRecovery`<br>`overwriteExistingVm`<br>`removeNetworkInterfaces`<br>`retainVmGuid`<br>`retainNicMacAddress` |

| API ou options de ligne de commande | Options et variables importantes |
|---|---|
| Commande `bprestore` | ■ `vmproxy` spécifie le nom ou le nom de domaine complet de l'hôte de sauvegarde.<br>■ `vmserver` est le nom du cluster AHV.<br>■ `vmpoweron` pour démarrer la machine virtuelle après sa restauration.<br>■ `vmsn` pour supprimer les interfaces réseau des machines virtuelles.<br>■ `vmid` pour conserver l'UUID d'origine de la machine virtuelle. Vous pouvez également utiliser l'option `-K` pour conserver la machine virtuelle existante portant le même UUID et ne pas l'écraser.<br>■ L'option `-R` définit le chemin d'accès au fichier renommé. Utilisez le fichier renommé pour récupérer la machine virtuelle vers un autre emplacement ou modifier la configuration de la machine virtuelle.<br><br>Exemple de fichier renommé :<br><br>`change vmname to new_vm_name`<br>`change /storage_domain_1/disk1_UUID`<br>`to /storage_domain_2/`<br>`change /storage_domain_1/disk2_UUID`<br>`to /storage_domain_2/`<br>`change cluster to new_cluster_name`<br><br>**Remarque :** Pour un hôte NetBackup Windows, vous devez ajouter une ligne vide après les entrées du fichier renommé. Consultez la section Se reporter à "Informations supplémentaires sur le fichier renommé" à la page 130. |

## Restauration de la machine virtuelle AHV à un autre emplacement

**Tableau 7-7** Restauration de la machine virtuelle AHV à un autre emplacement

| API ou options de ligne de commande | Options et variables importantes |
|---|---|
| `POST /netbackup/recovery/workloads/ahv /scenarios/full-vm/recover` | ■ `client` est l'identifiant qui a été utilisé au moment de la sauvegarde. Il peut s'agir de `displayName` ou de `UUID`.<br>■ `ahvCluster` est le nom de l'autre cluster AHV.<br>■ `recoveryHost` est le serveur qui doit être utilisé comme hôte de récupération de la machine virtuelle pour effectuer cette récupération.<br>■ `vmDisks` représente un ou plusieurs disques de machine virtuelle.<br>■ `source` est le chemin d'accès source du disque de la machine virtuelle. Il doit être au format `/conteneur_stockage/uuid_disque`.<br>■ `destination` est le chemin d'accès de destination du disque de la machine virtuelle. Il doit être au format `/conteneur_stockage`.<br>■ Définissez les valeurs suivantes :<br>`powerOnAfterRecovery`<br>`overwriteExistingVm`<br>`removeNetworkInterfaces`<br>`retainVmGuid`<br>`retainNicMacAddress` |

| API ou options de ligne de commande | Options et variables importantes |
|---|---|
| Commande `bprestore` | ■ `vmproxy` spécifie le nom ou le nom de domaine complet de l'hôte de sauvegarde.<br>■ `vmserver` est le nom du cluster AHV.<br>■ Utilisez les valeurs suivantes pour modifier la configuration de la machine virtuelle :<br>  ■ `vmpoweron` pour démarrer la machine virtuelle après sa restauration.<br>  ■ `vmsn` pour supprimer les interfaces réseau des machines virtuelles.<br>  ■ `vmid` pour conserver l'UUID d'origine de la machine virtuelle. Vous pouvez également utiliser l'option `-K` pour conserver la machine virtuelle existante portant le même UUID et ne pas l'écraser.<br>■ L'option `-R` définit le chemin d'accès au fichier renommé. Utilisez le fichier renommé pour récupérer la machine virtuelle vers un autre emplacement ou modifier la configuration de la machine virtuelle.<br>Exemple de fichier renommé :<br>`change vmname to new_vm_name`<br>`change /storage_domain_1/disk1_UUID to /storage_domain_2/`<br>`change /storage_domain_1/disk2_UUID to /storage_domain_2/`<br>`change cluster to new_cluster_name`<br>**Remarque :** Pour un hôte NetBackup Windows, vous devez ajouter une ligne vide après les entrées du fichier renommé.<br>Se reporter à "Informations supplémentaires sur le fichier renommé" à la page 130. |

# Options NetBackup supplémentaires pour la configuration de AHV

Utilisez les options de commande NetBackup suivantes pour compléter la configuration de AHV :

Option NUTANIX_AUTODISCOVERY_INTERVAL pour les serveurs NetBackup. Cette option détermine la fréquence à laquelle NetBackup analyse les clusters AHV pour découvrir des machines virtuelles à afficher dans l'interface utilisateur Web NetBackup.

NetBackup tente d'abord de procéder à la découverte automatique avec l'hôte qui a été utilisé lors de la dernière tentative de découverte réussie. Si la découverte automatique échoue avec cet hôte, NetBackup essaye à nouveau avec d'autres hôtes dans l'ordre suivant :

1. Serveur principal NetBackup
2. Hôte d'accès, client ou serveur proxy
3. Serveur de médias

**Tableau 7-8**

| Utilisation | Options et variables importantes |
|---|---|
| `POST /netbackup/asset-service/queries`<br><br>`GET /netbackup/asset-service/queries/{aqcId}` | ■ `clusterName` est le nom du cluster AHV.<br>■ `backuphost` est le nom d'hôte d'un client NetBackup.<br>■ `credentialName` correspond aux informations d'authentification associées au cluster AHV. |
| Commande `tpconfig` | ■ `virtual_machine` est le nom du cluster AHV.<br>■ `vm_type` a la valeur 9. Le chiffre 9 représente le cluster AHV. |

# Informations supplémentaires sur le fichier renommé

- Vous pouvez spécifier le conteneur de stockage cible pour tous les disques ou pour une liste spécifique de disques.
- Si vous ne spécifiez pas de conteneur de stockage cible pour l'un des disques, ce disque est restauré à l'emplacement d'origine.
- Si vous spécifiez un conteneur de stockage cible pour un disque non valide ou non existant, la restauration de la machine virtuelle échoue.
- Pour un hôte de sauvegarde Windows, vous devez ajouter une ligne vide (retour chariot) après toutes les entrées du fichier de renommage.

Créez ou modifiez le fichier rename dans le répertoire `/usr/openv/tmp` dans les scénarios suivants :

- Récupérer la machine virtuelle dans un autre conteneur

- Récupérer la machine virtuelle dans le même conteneur ou dans un autre conteneur avec un nom de machine virtuelle modifié

Si le fichier de renommage n'est pas disponible, vous devez le créer et l'enregistrer en tant que `rename.txt` sur le serveur principal NetBackup.

Pour définir l'emplacement secondaire ou modifier la configuration, ajoutez les lignes suivantes dans le fichier rename au format donné :

| Scénario | Ligne à ajouter dans le fichier rename |
|---|---|
| Modifier le nom de la machine virtuelle | `change vmname to newVMname` |
| Récupérer la machine virtuelle dans un autre conteneur AHV | `change /<original_container1>/<disk_uuid1> to /<alternate_container1>` |

## Exemple de fichier rename

Le fichier `rename.txt` suivant permet de modifier le nom de la machine virtuelle.

```
change vmname to newVMname
```

Une fois les modifications requises effectuées dans le fichier rename, vous pouvez exécuter la commande `bprestore`.