Guide de sécurité et de chiffrement NetBackup™

UNIX, Windows et Linux

Version 10.0

VERITAS™

Guide de sécurité et de chiffrement NetBackup™

Dernière mise à jour : 2022-05-10

Mentions légales

Veritas Technologies Corporation
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

Informations préliminaires pour les communications sécurisées dans NetBackup

Ce chapitre traite des sujets suivants :

À propos de la communication sécurisée dans NetBackup

Ce document fournit des informations essentielles sur la communication sécurisée dans NetBackup. Il est vivement recommandé de lire ces informations avant d'effectuer une mise à niveau de NetBackup vers une version prenant en charge la communication sécurisée (version 8.1 ou ultérieure).

Les hôtes NetBackup 8.1 et versions ultérieures ne peuvent communiquer entre eux qu'en mode sécurisé.

NetBackup utilise le protocole de sécurité TLS (Transport Layer Security) pour la communication entre les hôtes. Chaque hôte doit présenter son certificat de sécurité et valider celui de l'hôte pair par rapport au certificat de l'autorité de certification (CA). Les certificats de sécurité NetBackup permettant d'authentifier des hôtes

NetBackup sont conformes à la norme pour les infrastructures à clés publiques X.509. NetBackup prend en charge deux types de certificats :

- Certificats signés par l'autorité de certification NetBackup : un serveur maître NetBackup agit en tant qu'autorité de certification et émet des certificats numériques pour les hôtes.
  Se reporter à "Présentation des certificats de sécurité dans NetBackup" à la page 294.
- Certificats signés par une autorité de certification externe : à partir de NetBackup 8.2, vous pouvez également configurer des certificats signés par une autorité de certification externe (ou certificats externes) sur les hôtes NetBackup.
  Se reporter à "A propos de la prise en charge d'une autorité de certification externe dans NetBackup" à la page 437.

Selon la configuration de NetBackup, un hôte exige l'un de ces types de certificats ou les deux pour la communication avec d'autres hôtes.

À partir de la version 8.3, les autorités de certification NetBackup présentant les puissances de clé suivantes sont prises en charge : 2 048 bits, 4 096 bits, 8 192 bits et 16 384 bits.

Vous pouvez choisir de déployer un certificat sur un hôte pendant l'installation de NetBackup. Si, pour une quelconque raison, un certificat ne peut pas être déployé sur un hôte pendant l'installation, la communication avec d'autres hôtes est impossible. Dans ce cas, vous devez déployer manuellement un certificat NetBackup sur l'hôte à l'aide de la commande `nbcertcmd` pour démarrer la communication entre les hôtes après l'installation.

Vous pouvez également configurer des certificats signés par une autorité de certification externe.

Les nœuds suivants de la **console d'administration NetBackup** fournissent des paramètres de communication sécurisée : **Gestion des hôtes** et **Paramètres de sécurité globaux**.

Les commandes suivantes fournissent des options permettant de gérer le déploiement de certificats et d'autres paramètres de sécurité : `nbhostmgmt`, `nbhostidentity`, `nbcertcmd` et `nbseccmd`.

Si votre environnement inclut des hôtes NetBackup 8.0 ou version antérieure, vous pouvez autoriser la communication non sécurisée avec ces hôtes.

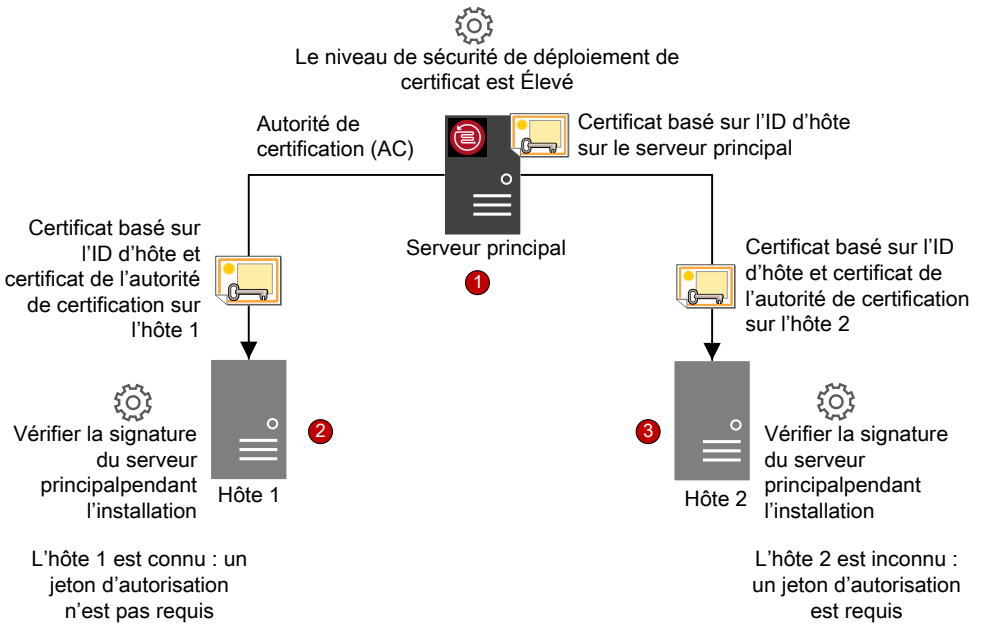
Se reporter à "Communication des hôtes NetBackup 8.1 ou version ultérieure avec les hôtes NetBackup 8.0 et versions antérieures" à la page 38.

Remarque : un certificat basée sur le nom d'hôte est requis dans les cas suivants :

- Les hôtes NetBackup Access Control ou NBAC requièrent des certificats basés sur le nom d'hôte.
- Les opérations d'audit amélioré requièrent que les hôtes disposent de certificats basés sur le nom d'hôte.
- L'utilisation de NetBackup CloudStore Service Container nécessite que le certificat basé sur le nom d'hôte soit installé sur le serveur de médias.

Déploiement de certificats signés par l'autorité de certification NetBackup (ou de certificats basés sur l'ID d'hôte) pendant l'installation

Le schéma ci-dessous présente le déploiement de certificats signés par l'autorité de certification NetBackup pendant l'installation :



Le déploiement de certificats NetBackup se déroule comme suit :

1. Un certificat NetBackup est déployé automatiquement sur le serveur maître NetBackup pendant l'installation. Le serveur maître est l'autorité de certification NetBackup.

2. Un certificat NetBackup est déployé sur l'hôte 1 pendant l'installation après vérification de la signature de l'autorité de certification fournie par l'assistant d'installation ou le script.

   Aucun jeton d'autorisation n'est nécessaire, car le niveau de sécurité du déploiement de certificats sur le serveur maître est élevé et l'hôte 1 est connu du serveur maître.

   Remarque : une signature est utilisée pour authentifier l'autorité de certification du serveur maître avant son ajout au magasin d'approbation d'un hôte. L'administrateur du serveur maître communique la signature de l'autorité de certification aux administrateurs d'hôtes par courrier électronique ou dans un fichier, ou la publie sur un site Web.

   Remarque : Un jeton d'autorisation est utilisé comme mécanisme pour autoriser la demande de certificat d'un hôte qui est envoyée au serveur maître NetBackup. Un jeton d'autorisation est confidentiel, et seul l'administrateur du serveur maître peut le créer. L'administrateur du serveur maître l'envoie ensuite à l'administrateur de l'hôte sur lequel vous souhaitez déployer un certificat. Un jeton de renouvellement est un jeton d'autorisation spécial utilisé pour redéployer un certificat sur un hôte pour lequel un certificat a été précédemment émis.

   Si vous avez continué l'installation de NetBackup sans confirmer la signature du serveur maître, vous devez exécuter des étapes manuelles pour que les sauvegardes et restaurations aient lieu.

   https://www.veritas.com/support/en_US/article.000127129

3. Un certificat NetBackup est déployé sur l'hôte 2 pendant l'installation après vérification de la signature du serveur maître. Un jeton d'autorisation est requis, car le niveau de sécurité du déploiement de certificats sur le serveur maître est élevé et le serveur maître ne connaît pas l'hôte 2.

Fonctionnement de la communication sécurisée avec les nœuds d'un cluster d'un serveur maître

Si vous disposez d'un serveur maître en cluster, consultez les scénarios suivants sur le déploiement de certificat :

- Dans le cas d'une nouvelle installation NetBackup le certificat sur un nœud actif est déployé automatiquement. Vous devez déployer manuellement les certificats sur tous les nœuds inactifs.

- En cas de reprise après incident, les certificats des nœuds actifs et inactifs ne sont pas restaurés. Après avoir installé NetBackup en mode de reprise après incident, vous devez déployer manuellement les certificats sur tous les nœuds en utilisant un jeton de renouvellement.
- Dans le cas d'une mise à niveau, les nœuds actifs ou inactifs peuvent déjà disposer d'un certificat. Vous pouvez vérifier si un nœud de cluster possède un certificat en affichant les informations de certificat à l'aide de la commande `nbcertcmd -listCertDetails`.

Remarque : Si vous avez configuré NetBackup Access Control (NBAC) ou l'audit amélioré (EA) sur un nœud d'un cluster de serveur maître, vous devez également déployer manuellement les certificats basés sur le nom d'hôte sur tous les nœuds.

Dans une configuration en cluster, le même nom virtuel est utilisé sur plusieurs nœuds de cluster. Par conséquent, le nom virtuel doit être mappé avec tous les nœuds de cluster associés.

À propos des clients NetBackup installés sur les nœuds d'une application en cluster

Consultez les scénarios suivants sur la communication sécurisée avec les clients NetBackup installés sur les nœuds d'une application en cluster :

- Pour que la communication aboutisse, vous devez mettre à niveau tous les nœuds de cluster simultanément.
- Vérifiez que le nom virtuel est mappé à tous les nœuds de cluster afin d'éviter les échecs de sauvegarde après un basculement. Veritas recommande de surveiller l'onglet **Gestion de la sécurité > Gestion des hôtes > Mappages à approuver** pour identifier les conflits détectés et approuver les mappages requis.

Déploiement de certificats NetBackup sur les hôtes pendant les mises à niveau

Lorsque vous procédez à une mise à niveau de NetBackup, NetBackup déploie des certificats NetBackup avant la mise à niveau. Si les certificats ne peuvent pas être déployés, vous pouvez arrêter la mise à niveau. Le script de mise à niveau conserve la configuration NetBackup existante que vous pouvez utiliser.

Si vous avez mis à niveau NetBackup de la version 8.0 vers la version 8.1 ou une version ultérieure, il est possible que des certificats NetBackup soient déjà présents

sur les hôtes. Dans ce cas, les certificats ne sont pas déployés pendant la mise à niveau.

Les certificats ne sont pas déployés pendant la mise à niveau si celle-ci est effectuée à l'aide d'un utilitaire (qui télécharge et installe les mises à jour de sécurité et les correctifs logiciels). Vous devez déployer les certificats manuellement.

Quand un jeton d'autorisation est requis lors du déploiement de certificats

Les informations de cette section s'appliquent uniquement aux certificats signés par l'autorité de certification NetBackup. Les certificats signés par une autorité de certification externe ne requièrent pas de jeton d'autorisation.

Le paramètre de niveau de sécurité détermine si un jeton d'autorisation est requis pour déployer un certificat. Vous pouvez changer le niveau de sécurité sur le serveur maître en fonction de vos besoins. Utilisez l'onglet **Gestion de la sécurité > Paramètres de sécurité globale > Communication sécurisée** dans la **console d'administration NetBackup**.

Les valeurs suivantes sont disponibles : La valeur par défaut est Élevé(e).

- **Moyen** : la signature du serveur maître doit être confirmée pendant le déploiement du certificat. Aucun jeton d'autorisation n'est requis.
- **Élevé** : la signature du serveur maître doit être confirmée pendant le déploiement du certificat. Aucun jeton d'autorisation n'est requis si l'hôte est connu du serveur maître.
- **Très élevé(e)** : la signature du serveur maître doit être vérifiée pendant le déploiement du certificat. Un jeton d'autorisation est requis pour chaque hôte.

Remarque : dans certaines situations, le déploiement de certificats nécessite toujours un jeton, notamment pour les clients qui se trouvent dans une zone démilitarisée ou pour la réémission d'un certificat.

Se reporter à "À propos des niveaux de sécurité de déploiement de certificats NetBackup" à la page 334.

Pourquoi il faut associer les noms d'hôte (ou adresses IP) aux ID d'hôte

Les hôtes peuvent être référencés par plusieurs noms.

C'est le cas par exemple lorsqu'il existe plusieurs interfaces réseau ou que les hôtes sont référencés à la fois par des noms courts et par des noms de domaine complets.

Pour que la communication sécurisée aboutisse dans NetBackup 8.1 ou version ultérieure, vous devez mapper tous les noms d'hôte associés à l'ID d'hôte correspondant. Le nom de client d'un hôte configuré par NetBackup (ou nom principal) est automatiquement mappé à son ID d'hôte lors du déploiement du certificat. D'autres noms d'hôte sont découverts pendant la communication et peuvent être mappés automatiquement à l'ID d'hôte correspondant ou apparaître dans la liste **Mappages à approuver**. Procédez à cette configuration dans les propriétés **Gestion des hôtes** sur le serveur maître.

Se reporter à "Ajout de mappages d'ID d'hôte vers le nom d'hôte" à la page 299.

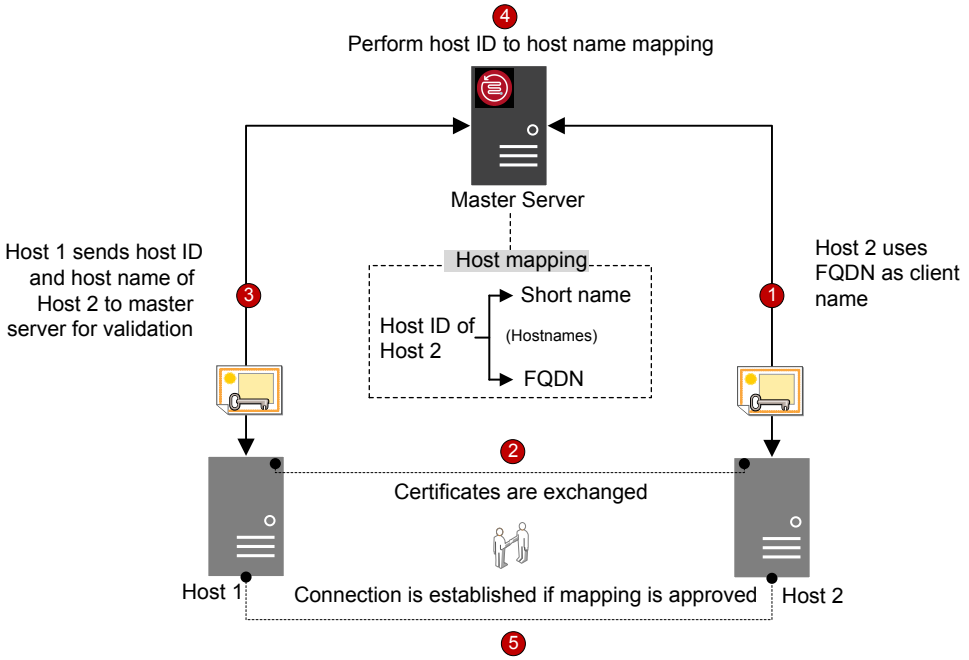
Exemples de configurations comportant plusieurs noms d'hôte :

- Si vous utilisez plusieurs interfaces réseau, un hôte dispose d'un nom d'hôte public et d'un nom d'hôte privé.
- Un hôte peut avoir un nom court et un nom de domaine complet (FQDN).
- Un hôte peut être associé à son adresse IP.
- Pour un système de fichiers ou une base de données en cluster, un hôte est associé à son nom de nœud et au nom virtuel du cluster.

Tenez compte des éléments suivants :

- Les agents Exchange, SharePoint et SQL Server requièrent également la configuration des informations d'hôte dans les propriétés d'hôte **Mappage de restauration d'application distribué** sur le serveur maître.
- Pour les environnements hautement disponibles, l'agent SQL Server n'exige plus de seconde politique contenant les noms de nœud de cluster ou les noms de nœuds AG. Vous devez également définir les autorisations des restaurations redirigées pour les nœuds de cluster ou les nœuds AG. Pour que les sauvegardes et les restaurations d'un cluster SQL Server ou d'un groupe de disponibilité aboutissent, il suffit de configurer les mappages dans les propriétés de **Gestion des hôtes** et les propriétés d'hôte **Mappage de restauration d'application distribuée**.

Le schéma suivant ci-dessous présente le processus de mappage d'un ID d'hôte à un nom d'hôte :



Le mappage d'un ID d'hôte à un nom d'hôte se déroule comme suit :

1. Le nom de domaine complet de l'hôte 2 est mappé à son ID d'hôte lors du déploiement du certificat.
2. L'hôte 1 lance une connexion sécurisée avec l'hôte 2 en utilisant le nom court. Les deux hôtes échangent leurs certificats NetBackup lors de la négociation TLS.
3. L'hôte 1 envoie l'ID d'hôte et le nom court de l'hôte 2 au serveur maître pour validation.
4. Le serveur maître recherche l'ID d'hôte et le nom court dans sa base de données. Comme le nom d'hôte court fourni n'est pas encore mappé à l'ID de l'hôte 2, l'une des opérations suivantes est exécutée :
   - Si l'option **Mapper automatiquement l'ID d'hôte aux noms d'hôte** est sélectionnée dans la **console d'administration NetBackup** et que le nom court n'est pas déjà associé à un autre ID d'hôte, le nom court découvert est associé automatiquement à l'ID de l'hôte 2, et l'hôte 1 est invité à continuer la connexion.

- Si l'option **Mapper automatiquement l'ID d'hôte aux noms d'hôte** n'est pas sélectionnée ou si le nom court est déjà mappé à un autre ID d'hôte, le mappage découvert est ajouté à la liste des approbations en attente et l'hôte 1 est invité à abandonner la connexion. Le mappage doit être approuvé manuellement pour que les connexions à l'hôte 2 utilisant le même nom court aboutissent.

5. La connexion est établie entre les hôtes si le mappage est approuvé. Si le mappage n'est pas approuvé, la connexion est abandonnée.

Réinitialisation des attributs d'hôte ou de l'état de la communication d'hôte

L'option **Réinitialiser les attributs de l'hôte** supprime les propriétés d'hôte et les informations sur les mappages d'ID d'hôte à un nom d'hôte. Le nom d'hôte principal et le certificat NetBackup ne sont pas supprimés.

La réinitialisation des attributs d'hôte est utile dans les cas suivants :

- Si vous avez rétrogradé un hôte vers la version 8.0 ou une version antérieure pour activer la communication non sécurisée (ou antérieure).
- Si vous rencontrez des problèmes de communication d'hôte et que vous voulez supprimer les informations d'hôte.

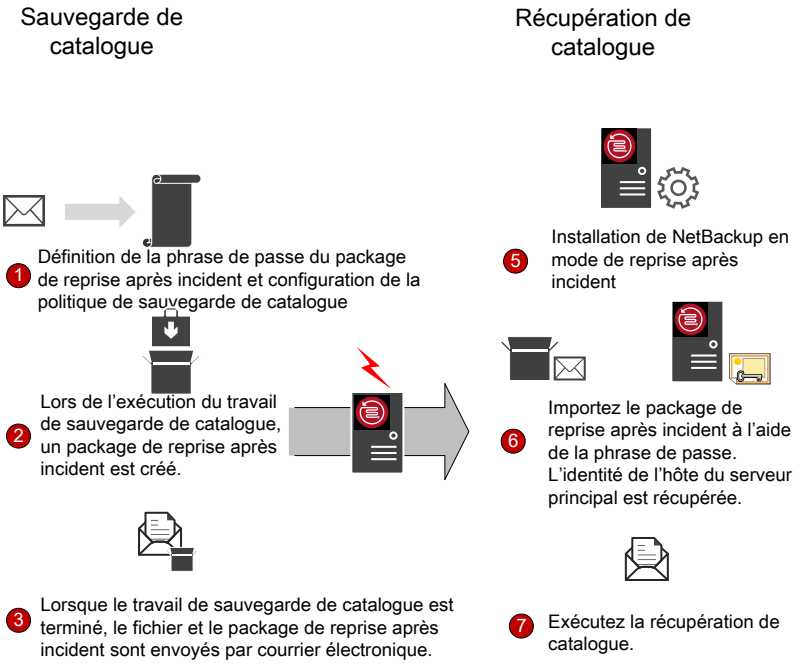
Se reporter à "Réinitialisation des attributs d'hôte NetBackup" à la page 310.

Modifications apportées à la récupération de catalogue

Dans NetBackup 8.1 ou version ultérieure, vous devez récupérer l'identité d'hôte du serveur maître lorsque vous restaurez NetBackup après un incident. L'identité d'hôte comprend les informations de certificat, les paramètres de sécurité et d'autres informations.

L'identité d'hôte antérieure étant en place, le serveur maître peut communiquer avec le serveur de médias et les clients dans la nouvelle instance de NetBackup. Un package de reprise après incident contenant l'identité d'hôte du serveur maître est créé à chaque sauvegarde de catalogue. Puisqu'il contient des données sensibles, telles que les certificats de sécurité et les paramètres de sécurité, le package de reprise après incident est chiffré à l'aide une phrase de passe.

Le schéma ci-dessous présente le workflow de la récupération de catalogue.



1. Définissez une phrase de passe pour le package de reprise après incident, puis configurez une politique de sauvegarde de catalogue. Les sauvegardes de catalogue utilisent la phrase de passe configurée lors de l'exécution de la politique.

Remarque : à partir de NetBackup 9.0, vous pouvez également définir des contraintes de phrase de passe à l'aide de l'option de commande `nbseccmd -setpassphraseconstraints`.

Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

Si vous ne définissez pas de contraintes de phrase de passe à l'aide de la commande, les contraintes par défaut s'appliquent, à savoir entre 8 et 1 024 caractères.

Pour définir une phrase de passe, utilisez l'onglet **Gestion de la sécurité > Paramètres de sécurité globaux > Reprise après incident** dans la **console d'administration NetBackup**.

Si vous modifiez la phrase de passe, la phrase de passe des packages de reprise après incident qui ont été créés auparavant n'est pas modifiée. Seules

les phrases de passe des packages de reprise après incident qui sont créés par la suite sont modifiées.

Pour récupérer d'anciens catalogues, vous devez utiliser la phrase de passe correspondante.

Attention : vous devez définir la phrase de passe avant de configurer la politique de sauvegarde de catalogue. Si la phrase de passe n'est pas définie, les sauvegardes de catalogue échouent. Si la politique de sauvegarde du catalogue est mise à niveau à partir d'une version antérieure à la 8.1, les sauvegardes échouent jusqu'à ce que la phrase de passe soit définie.

---

2. Un package de reprise après incident est créé à chaque sauvegarde de catalogue.

   Pour vérifier la phrase de passe après la sauvegarde de catalogue, exécutez la commande suivante :

   ```
   nbhostidentity -testpassphrase -infile dr_package_location
   ```

3. Les packages de reprise après incident sont enregistrés avec les fichiers de reprise après incident et envoyés par courrier électronique au destinataire que vous avez spécifié lors de la configuration de la politique.
4. Un incident se produit.
5. Après un incident, vous devez installer NetBackup sur le serveur maître en mode de reprise après incident. Ce processus vous invite à spécifier le chemin du package de reprise après incident et la phrase de passe.
6. Si la phrase de passe fournie est correcte, l'identité d'hôte du serveur maître est récupérée. Vous devez fournir la phrase de passe correspondant au package de reprise après incident que vous souhaitez récupérer.

   Si vous avez perdu la phrase de passe, vous devez déployer des certificats de sécurité sur tous les hôtes NetBackup manuellement.

   Pour plus d'informations, consultez l'article suivant :

   http://www.veritas.com/docs/000125933
7. Vous devez procéder à la récupération de catalogue immédiatement après avoir récupéré l'identité d'hôte pour éviter toute perte d'informations spécifiques aux activités de certificat qui peuvent avoir été exécutées après la restauration de l'identité d'hôte. Utilisez le fichier de reprise après incident (DR) approprié et récupérez le catalogue requis.

La phrase de passe n'est pas récupérée pendant la restauration de l'identité d'hôte (ou du package de reprise après incident) ni pendant la récupération de catalogue. Vous devez la redéfinir dans la nouvelle instance de NetBackup.

Remarque : pour restaurer l'identité d'hôte après l'installation normale de NetBackup (lorsque le mode de reprise après incident n'est pas sélectionné), vous pouvez utiliser la commande `nbhostidentity`.

Pour restaurer l'identité d'hôte de l'appliance NetBackup, vous devez utiliser la commande `nbhostidentity` après l'installation normale.

Modifications apportées à Auto Image Replication

Pour utiliser NetBackup Auto Image Replication (AIR) avec des communications sécurisées, vous devez établir une relation de confiance entre les serveurs maîtres source et cible.

Après avoir mis à niveau les serveurs maîtres source et cible vers la version 8.1 ou une version ultérieure, vous devez mettre à jour la relation de confiance sur les deux serveurs maîtres.

Remarque : si la relation de confiance n'est pas rétablie sur les deux serveurs après la mise à niveau, les nouvelles politiques de cycle de vie du stockage (SLP) ne fonctionnent pas.

Vous pouvez configurer la relation de confiance à l'aide de la **console d'administration NetBackup** ou de la commande `nbseccmd -setuptrustedmaster`.

Pour plus d'informations sur les serveurs maîtres approuvés pour Auto Image Replication, consultez le Guide de déduplication NetBackup.

Fonctionnement des hôtes avec des certificats révoqués

L'administrateur du serveur maître peut révoquer des certificats NetBackup pour diverses raisons. Une liste de révocation de certificats contenant des informations sur les certificats révoqués est créée par le serveur maître et récupérée régulièrement par tous les hôtes. La fréquence de mise à jour des listes de révocation de certificats est déterminée par le niveau de sécurité du déploiement de certificat sur le serveur maître.

Les listes de révocation de certificats sont vérifiées pendant la communication entre les hôtes. Un hôte qui utilise un certificat révoqué n'est plus approuvé et la communication avec cet hôte est interrompue.

Se reporter à "À propos de la liste de révocations des certificats basés sur l'ID d'hôte" à la page 362.

Les certificats NetBackup sont-ils sauvegardés ?

Pour des raisons de sécurité, les certificats NetBackup ne sont pas inclus dans les sauvegardes. Les certificats sont automatiquement supprimés lorsque NetBackup est désinstallé. Si nécessaire, vous pouvez les sauvegarder manuellement avec les clés privées correspondantes avant de désinstaller NetBackup.

Se reporter à "Conservation des certificats basés sur l'ID d'hôte lors de la réinstallation de NetBackup sur des hôtes non maîtres" à la page 348.

Configuration de certificats externes pour le serveur maître

Vous pouvez utiliser des certificats X.509 émis par votre autorité de certification approuvée. NetBackup prend en charge les certificats basés sur un fichier et le magasin de certificats Windows en tant que sources pour les certificats externes pour les hôtes NetBackup. Il prend en charge les certificats aux formats PEM, DER et P7B.

Se reporter à "Workflow d'utilisation de certificats externes pour la communication avec l'hôte NetBackup" à la page 441.

Fonctionnement de la communication sécurisée avec les nœuds de cluster d'un serveur maître lorsque des certificats externes sont utilisés

Vous pouvez utiliser pour un serveur maître en cluster des certificats X.509 émis par votre autorité de certification approuvée.

Vous devez d'abord indiquer à votre domaine NetBackup d'utiliser les certificats signés par une autorité de certification externe en configurant le serveur Web NetBackup. Vous pouvez ensuite configurer le serveur maître en cluster NetBackup pour qu'il utilise des certificats signés par une autorité de certification externe afin d'assurer une communication sécurisée avec l'hôte.

Se reporter à "Workflow permettant l'utilisation des certificats externes pour un serveur maître en cluster" à la page 480.

Fonctionnement des listes de révocation pour les certificats externes

La liste de révocation de certificats pour une autorité de certification externe contient la liste des certificats numériques que l'autorité de certification a révoqués avant la date d'expiration planifiée et qui ne doivent plus être approuvés.

Se reporter à "À propos des listes de révocation des certifications pour l'autorité de certification externe" à la page 460.

Processus de communication lorsqu'un hôte ne peut pas se connecter directement au serveur maître

Dans une zone démilitarisée (DMZ), les clients NetBackup n'ont pas forcément la possibilité d'envoyer directement des demandes (pour le déploiement de certificat, etc.) au serveur maître. Le tunnel HTTP sur le serveur de médias est utilisé pour accepter les demandes de service Web envoyées par les hôtes clients et les transférer au serveur maître. La configuration de la tunnelisation HTTP est automatique et ne nécessite aucune intervention. La tunnelisation HTTP fonctionne uniquement avec les clients et les serveur de médias NetBackup 8.1 ou version ultérieure.

Quel que soit le niveau de sécurité de déploiement de certificats défini sur le serveur maître, vous devez utiliser un jeton d'autorisation pour déployer un certificat signé par l'autorité de certification NetBackup sur un hôte qui se trouve dans une zone démilitarisée.

Se reporter à "Communication entre un client NetBackup situé dans une zone démilitarisée et un serveur maître, via un tunnel HTTP" à la page 384.

Communication des hôtes NetBackup 8.1 ou version ultérieure avec les hôtes NetBackup 8.0 et versions antérieures

Les hôtes NetBackup 8.1 ou version ultérieure ne peuvent communiquer avec d'autres hôtes 8.1 ou version ultérieure qu'en mode sécurisé. Pour qu'un hôte 8.1

ou version ultérieure puisse communiquer avec des hôtes 8.0 ou version antérieure, vous devez autoriser la communication non sécurisée.

L'option **Activer la communication non sécurisée avec les hôtes NetBackup 8.0 et versions antérieures** est activée par défaut. Cette option est disponible dans la **console d'administration NetBackup**, dans l'onglet **Gestion de la sécurité > Paramètres de sécurité globaux > Communication sécurisée**.

Si vous désactivez l'option pour autoriser seulement la communication sécurisée, vous devez redémarrer les services NetBackup sur le serveur maître pour arrêter les communications non sécurisées et autoriser uniquement les communications sécurisées.

Pendant une communication non sécurisée, l'hôte NetBackup se connecte tout d'abord au serveur maître pour la validation d'hôte. Le serveur maître vérifie si la communication non sécurisée est activée. Si l'option est activée, la communication entre les deux hôtes est établie. Si l'option est désactivée, la communication est abandonnée.

Processus de communication avec les serveurs de médias hérités dans le cadre d'une configuration en cloud

Si l'option **Activer la communication non sécurisée avec les hôtes NetBackup 8.0 et antérieurs** est désactivée, NetBackup ne peut pas communiquer avec les serveurs de médias hérités que vous utilisez pour le stockage en cloud indépendamment de la valeur de l'option de configuration `CSSC_LEGACY_AUTH_ENABLED`.

L'option **Activer la communication non sécurisée avec les hôtes NetBackup 8.0 et antérieurs** est disponible dans la **console d'administration NetBackup**, dans l'onglet **Gestion de la sécurité > Paramètres de sécurité globale > Communication sécurisée**.

Scénarios d'échec de communication

Consultez les scénarios suivants pour résoudre les problèmes éventuels de communication entre les hôtes dans NetBackup 8.1 ou version ultérieure.

Échec pendant la communication avec les hôtes 8.0 ou antérieurs

Si la communication non sécurisée n'est pas autorisée dans NetBackup, la communication avec les hôtes 8.0 et antérieurs échoue. Pour que la communication

avec les hôtes NetBackup 8.0 et antérieurs aboutisse procédez de l'une des manières suivantes :

- Dans la **console d'administration NetBackup** de l'hôte du serveur maître, sélectionnez l'option **Gestion de la sécurité > Sécurité globale > Communication sécurisée > Activer la communication non sécurisée avec les hôtes NetBackup 8.0 et antérieurs**.
- Sur l'hôte du serveur maître, exécutez la commande `nbseccmd -setsecurityconfig -insecurecommunication on`.

Échec de la sauvegarde de catalogue

Si la phrase de passe de package de reprise après incident n'est pas définie, les sauvegardes de catalogue échouent avec le code d'état 2524. Le message d'erreur suivant s'affiche :

```
Catalog backup failed because the passphrase for the disaster recovery package is not set.
```

Pour définir une phrase de passe, utilisez l'onglet **Gestion de la sécurité > Paramètres de sécurité globale > Reprise après incident** dans la **console d'administration NetBackup**.

Prise en charge de la communication sécurisée pour d'autres hôtes dans le domaine NetBackup

Lisez cette section pour en savoir plus sur la prise en charge de la communication avec les hôtes OpsCenter et BMR (Bare Metal Restore) par NetBackup 8.1.

Communication entre un serveur maître NetBackup 8.1 ou version ultérieure et un serveur OpsCenter

Assurez-vous que les options suivantes sont configurées avant de collecter des données depuis un serveur maître NetBackup 8.1 avec un serveur OpsCenter :

- Le nom du serveur OpsCenter doit être ajouté en fonction de l'option de configuration `OPS_CENTER_SERVER_NAME` dans le fichier de configuration NetBackup (`bp.conf` sous UNIX ou clé de Registre sous Windows).
- La communication non sécurisée est activée dans NetBackup. Vérifiez l'un des points suivants :

- Dans la **console d'administration NetBackup** sur l'hôte du serveur maître, l'option **Gestion de la sécurité > Sécurité globale > Hôtes > Activer la communication non sécurisée avec les hôtes NetBackup 8.0 et versions antérieures** est sélectionnée.
- Sur l'hôte du serveur maître, l'option de ligne de commande `nbseccmd -setsecurityconfig -insecurecommunication` est définie sur « on ».

Prise en charge de la communication sécurisée pour BMR

NetBackup Bare Metal Restore (BMR) 8.1.1 et les versions ultérieures prennent en charge la communication sécurisée NetBackup. L'option **Autoriser le renouvellement de certificat automatique** active le paramètre `autoreissue` d'un hôte NetBackup, ce qui vous permet de déployer un certificat sur l'hôte sans avoir recours à un jeton de renouvellement.

Se reporter à "Autoriser ou ne pas autoriser le renouvellement de certificat automatique" à la page 312.

Pour plus d'informations sur BMR, consultez le Guide de l'administrateur NetBackup Bare Metal Restore.

Configuration des sauvegardes VMware qui protègent SQL Server et des sauvegardes avec SQL Server utilisant plusieurs cartes réseau

Dans certains environnements, vous devez configurer les informations d'hôte dans les propriétés d'hôte **Mappage de restauration d'application distribué** sur le serveur maître. Si vous disposez de plusieurs cartes d'interface réseau, vous devez mapper les hôtes dans cette propriété d'hôte (ou dans le répertoire altnames). Pour les sauvegardes VMware, si vous utilisez un identifiant de la machine virtuelle principale autre que le nom d'hôte de la machine virtuelle, vous devez mapper l'identifiant de la machine virtuelle principale au nom d'hôte du client.

Chapitre 2

Augmentation de la sécurité dans NetBackup

Ce chapitre traite des sujets suivants :

Sécurité et chiffrement NetBackup

Le chiffrement et la sécurité de NetBackup assurent la protection pour toutes les parties d'opérations de NetBackup sur des serveurs maître de NetBackup, serveurs de médias et clients liés. Les systèmes d'exploitation, sur lesquels les serveurs et les clients sont en cours d'exécution, sont également sécurisés. Les données de sauvegarde sont protégées par des procédés de chiffrement et l'enregistrement dans un centre de sauvegarde. Les données NetBackup transmises par câble sont protégées par des ports réseau dédiés et sécurisés.

Les différents niveaux et mises en place de sécurité et de chiffrement NetBackup sont inclus dans les rubriques suivantes.

Se reporter à "Niveaux de mise en place de sécurité de NetBackup" à la page 43.

Se reporter à "NetBackup Access Control (NBAC)" à la page 48.

Se reporter à "Sécurité du système d'exploitation" à la page 56.

Se reporter à "Sécurité standard de NetBackup" à la page 57.

Se reporter à "Sécurité du chiffrement côté client" à la page 58.

Se reporter à "NBAC sur le serveur maître, le serveur de médias et la sécurité d'interface utilisateur graphique" à la page 60.

Se reporter à "Sécurité complète NBAC" à la page 62.

Niveaux de mise en place de sécurité de NetBackup

La perspective d'implémentation de sécurité de NetBackup commence dans un sens très large au niveau global et devient plus détaillé au niveau de l'entreprise. La sécurité devient très spécifique au niveau de centre de données.

Tableau 2-1 explique comment des niveaux de sécurité de NetBackup peuvent être mis en application.

Tableau 2-1 Niveaux de mise en place de sécurité de NetBackup

Niveau de sécurité	Description
Niveau mondial	Indique l'accès au serveur Web et aux bandes chiffrées qui sont transportées et placées dans le centre de sauvegarde
Niveau de l'entreprise	Spécifie des utilisateurs internes et des administrateurs de la sécurité
Niveau du centre de données	Spécifie des opérations de NetBackup

Sécurité de niveau mondial

La sécurité de niveau mondial permet aux utilisateurs externes d'accéder aux serveurs Web d'entreprise avec des pare-feux et permet aux bandes chiffrées d'être transportées et protégées hors site. La sécurité de niveau mondial englobe le niveau d'entreprise et le niveau de centre de données.

Figure 2-1 Portée de sécurité de niveau mondial

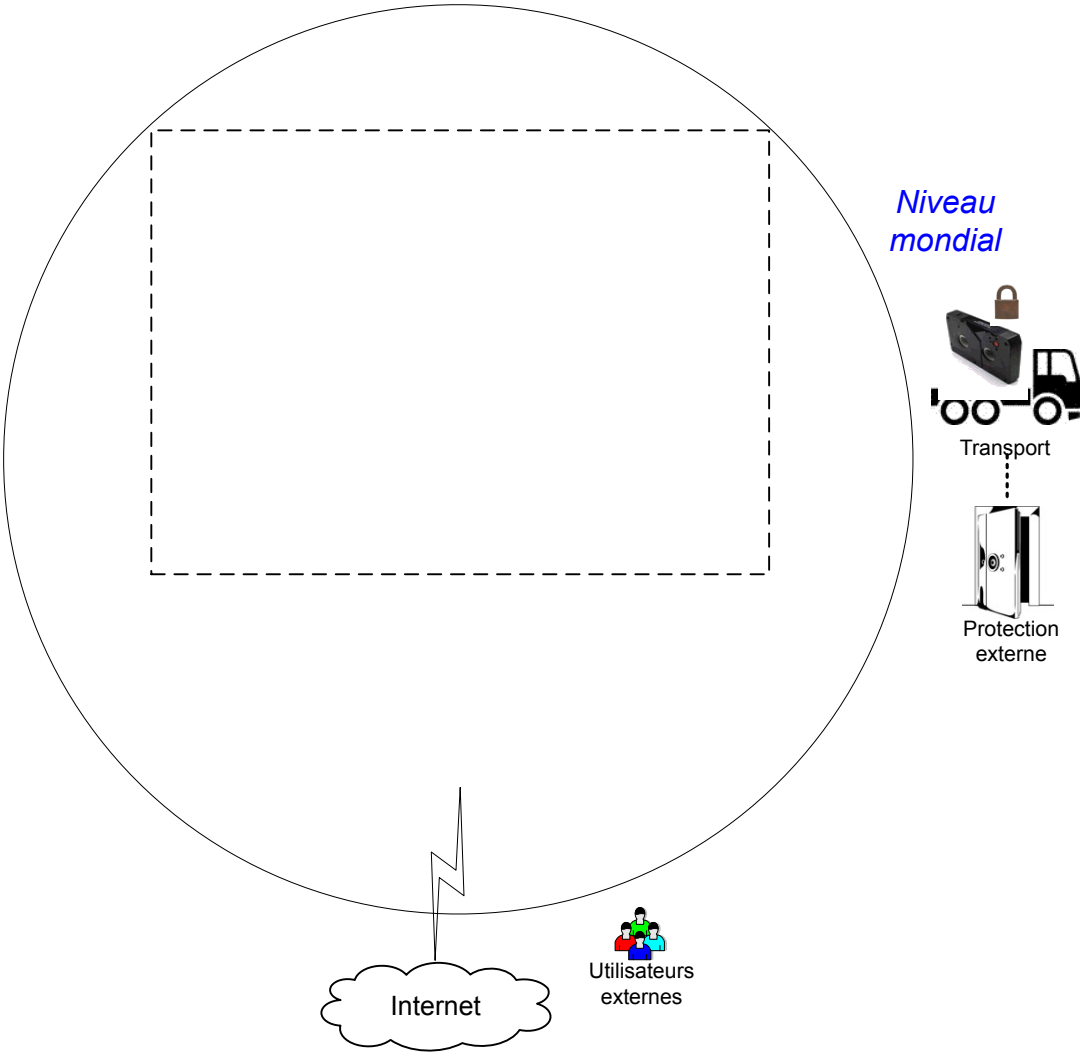


Tableau 2-2 Types de sécurité de niveau mondial

Type	Description
Utilisateurs extérieurs de niveau mondial	Spécifie que les utilisateurs externes peuvent accéder aux serveurs Web derrière des pare-feux. Les utilisateurs externes ne peuvent pas accéder ou utiliser les fonctionnalités de NetBackup depuis Internet si le pare-feu externe empêche l'accès aux ports de NetBackup.
Internet de niveau mondial	Indique un ensemble de réseaux d'ordinateurs connectés entre eux par des câbles de cuivre, des câbles de fibre optique ou par des connexions sans fil. Il est possible d'accéder aux serveurs Web d'entreprise via Internet en utilisant des ports HTTP au travers de pare-feux.
Niveau mondial WAN	Le réseau étendu (WAN) n'est pas affiché dans l'illustration de présentation de sécurité. Le WAN est une connexion haut débit dédiée, utilisée pour lier les data centers NetBackup qui sont répartis sur le plan géographique.
Transport de niveau mondial	Spécifie qu'un camion de transport peut déplacer les bandes client chiffrées hors site pour sécuriser des équipements de centre de sauvegarde.
Centre de sauvegarde de niveau mondial hors site	Spécifie que la bande chiffrée peut être sauvegardée dans des installations de stockage sécurisé autres que le centre de données actuel.

Sécurité de niveau d'entreprise

La sécurité de niveau d'entreprise contient des parties plus réelles de la mise en place de sécurité de NetBackup. Elle englobe les utilisateurs internes, les administrateurs de la sécurité et le niveau du centre de données.

Figure 2-2 Portée de sécurité de niveau d'entreprise

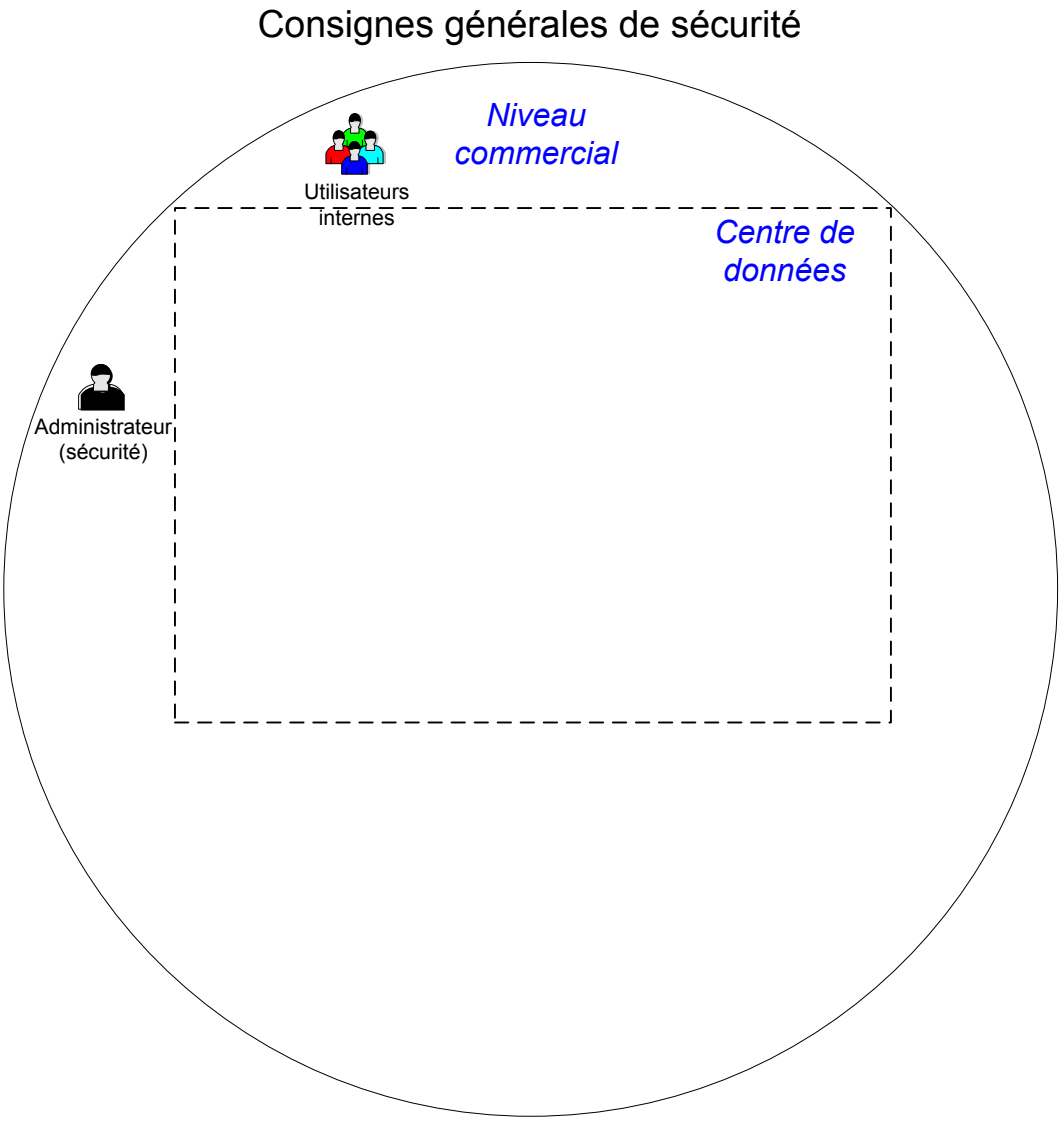


Tableau 2-3 Types de sécurité de niveau d'entreprise

Type	Description
Utilisateurs internes	Spécifie les utilisateurs qui ont des autorisations requises pour accéder et utiliser la fonctionnalité NetBackup depuis le data center. Les utilisateurs internes sont généralement une combinaison d'individus tels que des administrateurs de bases de données, des administrateurs de sauvegarde, des opérateurs et des utilisateurs système généraux.
Administrateur de sécurité	Désigne un utilisateur qui a reçu des autorisations d'administrateur requises pour accéder à et gérer la fonctionnalité de sécurité de NetBackup depuis le data center.

présentation de sécurité de Centre de données-Niveau

la sécurité de Data center-Niveau comporte le noyau de la fonctionnalité de sécurité de NetBackup. Elle peut se composer d'un groupe de travail, d'un unique data center ou d'un multi-data center.

Tableau 2-4 décrit les modèles de déploiement seuls à la sécurité de centre de données-Niveau.

Tableau 2-4 Modèles de déploiement pour la sécurité de centre de données-Niveau

Type	Description
Groupe de travail	Un groupe de travail est un petit groupe de systèmes (moins de 50) utilisés entièrement en interne avec NetBackup.
Datacenter unique	Un groupe d'hôtes moyen à grand (plus grand que 50) et peut sauvegarder des hôtes dans la zone démilitarisée (DMZ).
Centre de données multiple	Désigne un support vers un grand groupe d'hôtes (plus de50) étendu sur deux ou plusieurs régions géographiques. Ils peuvent se connecter par WAN. Cette configuration peut également inclure des hôtes dans les DMZ qui sont sauvegardés.

Se reporter à "Niveaux de mise en place de sécurité de NetBackup" à la page 43.

NetBackup Access Control (NBAC)

La fonctionnalité NetBackup Access Control (NBAC) incorpore NetBackup Product Authentication and Authorization à NetBackup et renforce la sécurité pour les serveurs maître, les serveurs de médias et les clients.

Se reporter à "Sécurité et chiffrement NetBackup" à la page 43.

Les points importants à propos de NBAC incluent :

- L'authentification et l'autorisation sont utilisées conjointement.
- NBAC utilise des identités d'authentification à partir d'une source approuvée pour identifier de manière fiable les parties impliquées. Des décisions d'accès peuvent alors être prises pour la manipulation de NetBackup en fonction de ces identités. Notez que les services de sécurité de NetBackup sont maintenant intégrés.
- NetBackup Product Authentication and Authorization se compose du courtier racine, du courtier d'authentification, du moteur d'autorisation et de l'interface utilisateur graphique.
- Oracle, Oracle Archiver, DB2, Informix, Sybase, SQL Server, SAP et EV Migrator ne sont pas pris en charge avec NBAC.
- NBAC n'est pas pris en charge sur les appliances.
- La sauvegarde de catalogue NetBackup est prise en charge avec NBAC.

Le tableau suivant décrit les composants de NetBackup qui sont utilisés dans la sécurité.

Tableau 2-5 Composants de NetBackup utilisés dans la sécurité

Composant	Description
Courtier racine	Le serveur maître NetBackup est le courtier racine dans une installation de data center. Il n'y a aucune disposition pour l'utilisation d'un autre courtier racine. La recommandation est de permettre la confiance entre les courtiers racine. Le courtier racine authentifie le courtier d'authentification. Le courtier racine n'authentifie pas les clients.
Courtier d'authentification	Authentifie le serveur maître, le serveur de médias, l'interface utilisateur graphique et les clients en établissant les informations d'authentification avec chacun d'entre eux. Le courtier d'authentification authentifie également un utilisateur lorsqu'il actionne une invite de commande. Il peut y avoir plus d'un courtier d'authentification dans une installation de data center. Le courtier d'authentification peut parfois être associé au courtier racine.

Composant	Description
Moteur d'autorisation	Communique avec le serveur maître et le serveur de médias pour déterminer les autorisations d'un utilisateur authentifié. Ces autorisations déterminent la fonctionnalité disponible pour un serveur donné. Le moteur d'autorisation enregistre également les groupes d'utilisateurs et les autorisations. Seul un moteur d'autorisation est requis dans une installation de data center. Le moteur d'autorisation communique également sur le WAN pour autoriser d'autres serveurs de médias dans un environnement de data center multiple.
interface utilisateur graphique	Spécifie une console d'administration à distance qui reçoit les informations d'authentification des courtiers d'authentification. L'interface utilisateur graphique peut utiliser les informations d'authentification pour accéder à la fonctionnalité sur les clients, les serveurs de médias et les serveurs maîtres.
Serveur maître	Communique avec le courtier racine, le courtier d'authentification, l'interface utilisateur graphique, le moteur d'autorisation, le serveur de médias et les clients.
Administrateur NetBackup	Désigne un utilisateur qui a reçu des autorisations d'administrateur pour accéder et gérer la fonctionnalité NetBackup depuis le data center.
Serveur de médias	Communique avec le serveur maître, le courtier racine et le courtier d'authentification, le moteur d'autorisation, et les clients 1 à 6. Le serveur de médias enregistre des données non chiffrées sur bande pour le client 5 et des données chiffrées sur bande pour le client 6.
Clients	Spécifie que les clients 1 à 4 sont les types standard de NetBackup. Le client 5 est un type de serveur Web situé dans la zone démilitarisée. Le client 6 est un type de client chiffré côté client également situé dans la zone démilitarisée. Tous les types de client sont gérés par le serveur maître et leurs données peuvent être sauvegardées sur une bande par le serveur de médias. Les clients 5 et 6 communiquent avec NetBackup uniquement à l'aide de ports NetBackup via le pare-feu interne. Le client 5 reçoit également des connexions Internet en utilisant seulement des ports réservés au HTTP via le pare-feu externe.
Bandes	La sécurité des bandes dans NetBackup peut être augmentée en ajoutant ce qui suit : ■ Chiffrement côté client ■ Chiffrement des données au repos Des bandes de données décryptées et cryptées sont produites dans le data center. Les données de bande non chiffrées sont écrites pour les clients 1 à 5 et stockées sur site dans le data center. Les bandes chiffrées sont écrites pour le client 6 et sont transportées hors site dans un centre de sauvegarde pour reprise après incident.

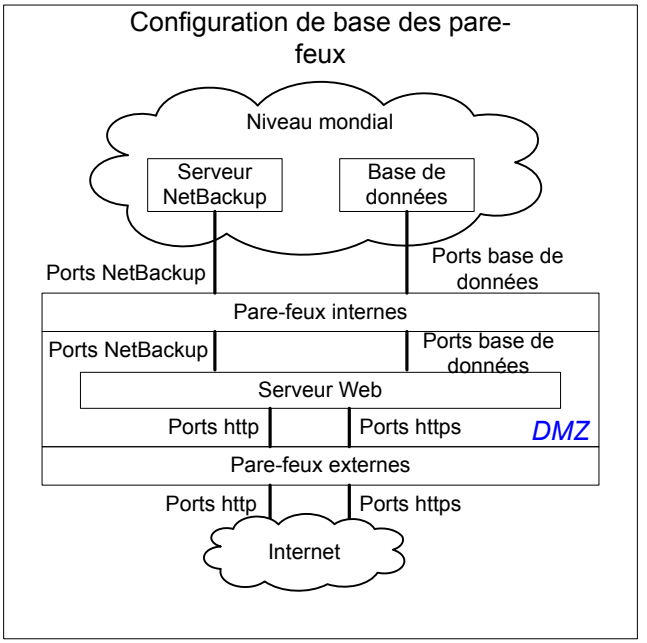
Composant	Description
Chiffrement	Spécifie que le chiffrement de NetBackup peut augmenter la sécurité en fournissant ce qui suit : ■ Une meilleure confidentialité des données ■ La perte de bande physique n'est pas aussi critique si toutes les données sont effectivement chiffrées ■ La meilleure stratégie de contrôle de risque Pour plus d'informations sur le chiffrement : Se reporter à "Questions importantes sur la sécurité du chiffrement" à la page 498.
Sécurité des données transmises par câble	Inclut la communication entre les serveurs maître, les serveurs de médias, les clients et la communication à l'aide des ports par les pare-feux et via WAN. Pour plus d'informations sur les ports, consultez le Guide de référence des ports réseau NetBackup : La part de données transmises par câble de NetBackup permet d'accroître la sécurité comme suit : ■ NetBackup Access Control (NBAC) ■ Les daemons classiques de NetBackup utilisent l'authentification lorsque NBAC est activé. ■ Les daemons de CORBA utilisent des canaux entièrement chiffrés prenant en charge la confidentialité et garantissant l'intégrité des données. ■ Pare-feux ■ Désactivation des ports inutilisés dans NetBackup et dans d'autres produits : ■ Les ports dédiés PBX et VNETD permettent d'accroitre la sécurité NetBackup. ■ Ensemble de ports centraux à surveiller et ouvrir via des pare-feux. **Remarque :** La communication entre NetBackup 8.1 et les hôtes de version ultérieure est sécurisée. Se reporter à "Communication sécurisée dans NetBackup" à la page 295.

Composant	Description
Sécurité du pare-feu	Spécifie que la prise en charge du pare-feu de NetBackup peut aider à augmenter la sécurité. Voici des points importants concernant la sécurité du pare-feu : ■ Il est recommandé d'utiliser la protection à l'aide du pare-feu et de la détection d'intrusion pour NetBackup. ■ Du point de vue de NetBackup, la protection à l'aide d'un pare-feu fait référence à la sécurité générale du réseau. Elle se concentre sur la réduction des verrous potentiels qu'un pirate peut tenter d'obtenir. Il peut être utile de vérifier un blocage éventuel des ports NFS, telnet, FTP et de messagerie. Ces éléments ne sont pas strictement nécessaires pour l'utilisation de NetBackup et peuvent constituer une "porte ouverte" aux accès indésirables. ■ Sécurisez le serveur maître autant que possible ■ Les pare-feux peuvent inclure des pare-feux internes et externes, comme suit : ■ Le pare-feu interne permet à NetBackup d'accéder au client de serveur Web n° 5 et au client chiffré n° 6 dans la zone démilitarisée. Vous ne pouvez activer que les ports NetBackup sélectionnés et les ports de certaines applications pour transmettre des données par le biais du pare-feu interne depuis et vers la zone démilitarisée. Les ports HTTP sont ouverts dans le pare-feu externe et ne sont pas autorisés à traverser le pare-feu interne. ■ Le pare-feu externe permet aux utilisateurs externes d'accéder au client de serveur Web 5 situé dans la zone démilitarisée depuis Internet par le biais des ports HTTP. Les ports NetBackup sont ouverts pour que le client de serveur Web 5 puisse communiquer via le pare-feu interne avec NetBackup. Les ports NetBackup ne peuvent pas passer par le pare-feu externe pour se connecter à Internet. Seuls les ports HTTP du client de serveur Web 5 peuvent passer par le pare-feu externe pour se connecter à Internet.

Composant	Description
Zone démilitarisée (DMZ)	Spécifie que la zone démilitarisée (DMZ) augmente la sécurité comme suit : ■ la zone démilitarisée est une zone dans laquelle le nombre de ports qui sont permis pour les hôtes spécifiques est fortement commandé ■ la zone démilitarisée se trouve entre les pare-feu externe et interne. Dans cet exemple, la zone commune est le serveur Web. Le pare-feu externe bloque tous les ports sauf les ports Web HTTP (standard) et HTTPS (sécurisés). Le pare-feu interne bloque tous les ports sauf les ports NetBackup et ports de base de données. la zone démilitarisée bloque. la zone démilitarisée bloque l'accès Internet externe vers le serveur NetBackup interne et les informations de la base de données. La zone démilitarisée fournit une zone de fonctionnement "sûre" pour le client de serveur Web 5 et pour le client chiffré 6 entre les pare-feux interne et externe. Le client de serveur Web 5 de la zone démilitarisée peut échanger des données avec NetBackup via le pare-feu interne en utilisant les ports NetBackup affectés. Le client de serveur Web 5 peut également communiquer sur Internet par le biais du pare-feu externe en utilisant uniquement des ports HTTP. Figure 2-3 affiche un exemple de pare-feux interne et externe avec la zone démilitarisée.

Le schéma suivant affiche un exemple du pare-feu interne et externe avec zone démilitarisée.

Figure 2-3 Exemples de pare-feux et de zone démilitarisée

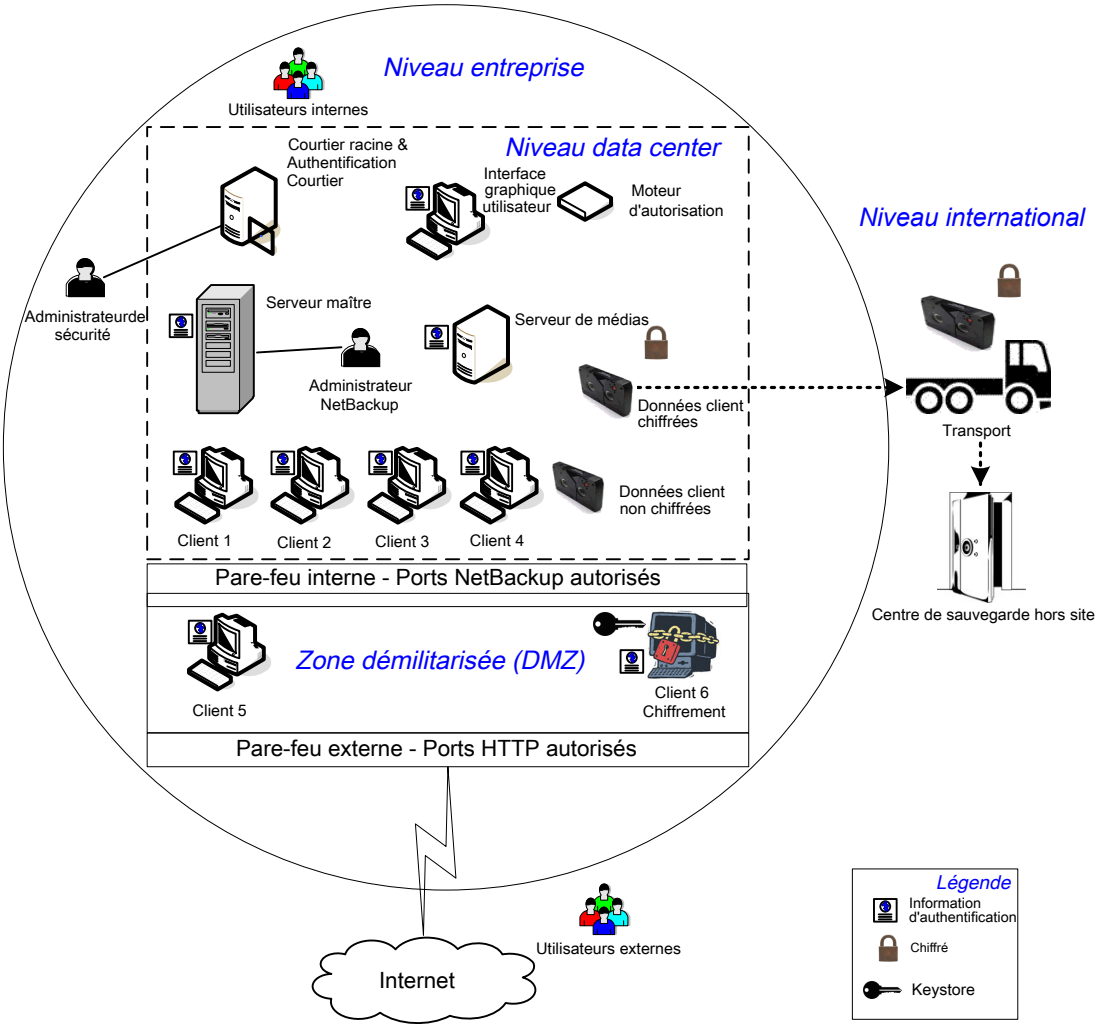


Niveaux mondial, de l'entrerprise et de data center combinés

Le modèle de niveaux mondial, de l'entreprise et de data center combinés est la zone où sont effectuées les opérations NetBackup complètes générales. Via le niveau mondial (le plus à l'extérieur), les utilisateurs externes peuvent accéder aux serveurs Web d'entreprise situés derrière des pare-feux et les bandes chiffrées sont transportées et placées en centre de sauvegarde hors-site. Les fonctions relatives aux utilisateurs internes, administrateurs de sécurité et au niveau de data center sont effectuées au niveau suivant, plus profond (niveau de l'entreprise). Au niveau le plus profond, le niveau de data center, la principale fonctionnalité de sécurité de NetBackup se produit par un groupe de travail, un unique data center ou plusieurs data centers.

Le schéma suivant affiche le modèle des niveaux combinés de monde, entreprise et data center.

Figure 2-4 Niveau combiné de monde, entreprise et data center



Types d'implémentation de sécurité NetBackup

Le tableau suivant affiche les types d'implémentation de sécurité, les caractéristiques, la complexité et les modèles de déploiement de la sécurité potentiels de NetBackup.

Tableau 2-6 Types d'implémentation de sécurité

Type d'implémentation de sécurité	Caractéristiques	Complexité	Modèles de déploiement de la sécurité
Se reporter à "Sécurité du système d'exploitation" à la page 56.	■ En fonction du système d'exploitation ■ Varie selon sur certains composants du système	Variable	Groupe de travail Data center unique Datacenter multiple
Se reporter à "Sécurité standard de NetBackup" à la page 57.	■ Gérer en tant que racine ou administrateur ■ Les données ne sont pas chiffrées	Faible	Groupe de travail avec NetBackup Datacenter unique avec NetBackup standard Datacenter multiple avec NetBackup standard
Se reporter à "Sécurité du chiffrement côté client" à la page 58.	■ Des données sont chiffrées sur le client ■ Des données chiffrées sont transmises par fil ■ Peut affecter les performances du CPU sur le client ■ Emplacement des clés	Moyen	Data center unique avec chiffrement côté client Data center multiple avec chiffrement côté client
Se reporter à "NBAC sur le serveur maître, le serveur de médias et la sécurité d'interface utilisateur graphique" à la page 60.	■ NBAC fournit l'autorisation d'accès au serveur maître et au serveur de médias. ■ Authentifie le système et les utilisateurs pour accéder au serveur maître et aux serveurs de médias.	Moyen	Data center unique avec NBAC sur les serveurs maître et de médias Data center multiple avec NetBackup Access Control sur les serveurs maîtres et de médias
Se reporter à "Sécurité complète NBAC" à la page 62.	■ NBAC fournit l'autorisation dans l'ensemble du système. ■ NBAC fournit l'authentification dans l'ensemble du système (serveurs, clients et utilisateurs)	Haut	Data center unique avec NBAC complet Datacenter multiple avec NBAC complet

Sécurité du système d'exploitation

La sécurité du système d'exploitation peut être améliorée pour les serveurs maîtres, les serveurs de médias et les clients en faisant ce qui suit :

- Installation des correctifs du système d'exploitation
  Les correctifs du système d'exploitation incluent des mises à niveau appliquées à l'OS pour qu'il continue à fonctionner au plus haut niveau de l'intégrité du système. Les mises à niveau et les correctifs doivent être maintenus au niveau spécifié par le fournisseur.
- Procédures sécurisées suivantes du pare-feu
- Employer l'administration de privilèges minimum
- Limitation des utilisateurs racines
- Application du protocole de sécurité sur le matériel IP (IPSEC)
- Désactiver les ports inutilisés des applications extérieures de revêtement
- Fourniture d'une base sécurisée sur laquelle exécuter NetBackup
- Ajouter une première ligne d'intelligence dans une enquête afin de déterminer si le système d'exploitation a été compromis
- Veiller à ce que la mise en place de la sécurité est la même pour tous les systèmes d'exploitation
- Ajout d'une interopérabilité totale entre divers systèmes utilisant NBAC dans un environnement hétérogène

Failles de sécurité dans NetBackup

Il est recommandé de mettre en place les mesures de protection suivantes pour éviter les rares instances d'une potentielle vulnérabilité de sécurité dans NetBackup :

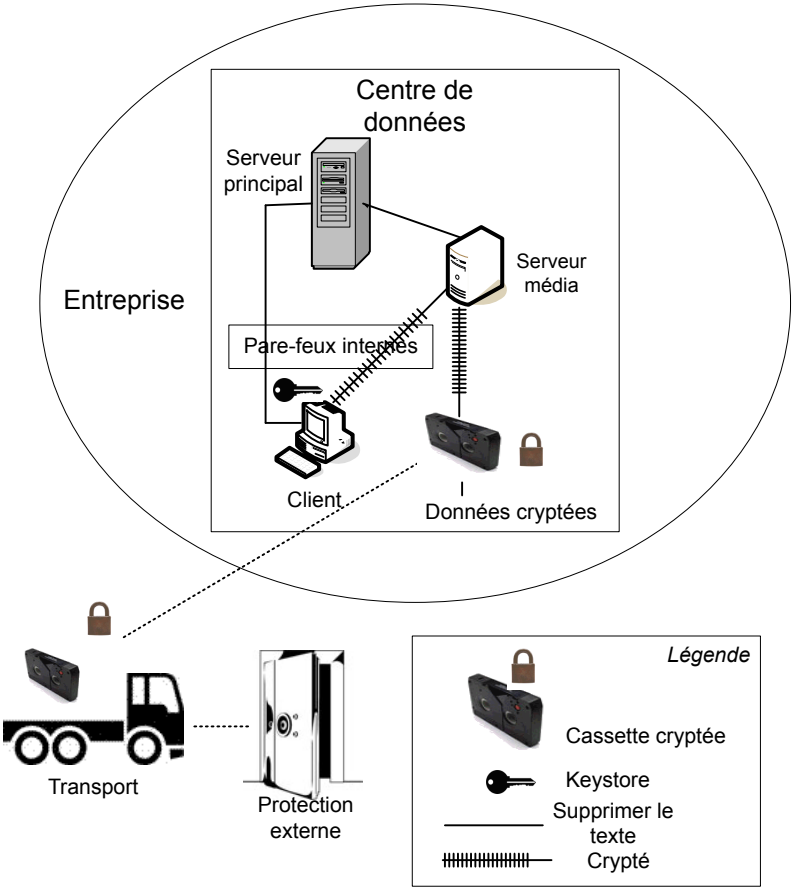
- Une mise à jour complète de NetBackup avec le prochain correctif de maintenance de NetBackup.
- Importance des mises à jour cumulées de NetBackup
- Utilisez les sites Web suivants pour plus d'informations sur les potentiels problèmes de vulnérabilité de sécurité :
  https://www.veritas.com/content/support/en_US/security.html
  https://www.veritas.com/security
- Utilisez les contacts électroniques pour les questions de failles de sécurité potentielles :
  secure@veritas.com

Sécurité standard de NetBackup

La sécurité standard de NetBackup inclut seulement la sécurité qui est offerte par le système d'exploitation et les composants matériels du data center. Les utilisateurs NetBackup autorisés gèrent au niveau racine ou administrateur. Les données du client ne sont pas chiffrées. Le serveur maître, le serveur de médias et le client sont exécutés dans un centre de données d'entreprise local. Les données non codées sont généralement stockées sur site, ce qui présente un risque relativement élevé en l'absence d'un plan de reprise après incident. Les données envoyées hors site sont susceptibles de subir une violation de la confidentialité si elles sont interceptées.

Le schéma suivant affiche un exemple de la configuration NetBackup standard.

Figure 2-5 NetBackup standard



Sécurité du chiffrement côté client

La sécurité du chiffrement côté client est utilisée pour assurer la confidentialité de données à travers les câbles aussi bien que sur bande. Ce chiffrement aide à diminuer les risques de branchement clandestin au sein d'une société. Le risque d'exposition de données est réduit car les bandes sont déplacées hors site. La clé de chiffrement se trouve sur le client. La transmission de données est chiffrée tout au long des câbles qui relient le client au serveur de médias. Le chiffrement des données par le client peut utiliser des ressources d'UC importantes.

Les types de politique de sauvegarde suivants prennent en charge l'utilisation de l'option client de chiffrement.

- AFS
- DB2
- DataStore
- DataTools-SQL-BackTrack
- Informix-On-BAR
- LOTUS_NOTES
- MS-Exchange
- MS-SharePoint
- MS-SQL-Server
- MS-Windows
- Oracle
- PureDisk-Export
- SAP
- Miroir partagé
- Standard
- Sybase

Les types de sauvegarde de politique suivants ne prennent pas en charge l'option de chiffrement client. Vous ne pouvez pas sélectionner la case à cocher de chiffrement dans l'interface des attributs de politique pour ces types de politique.

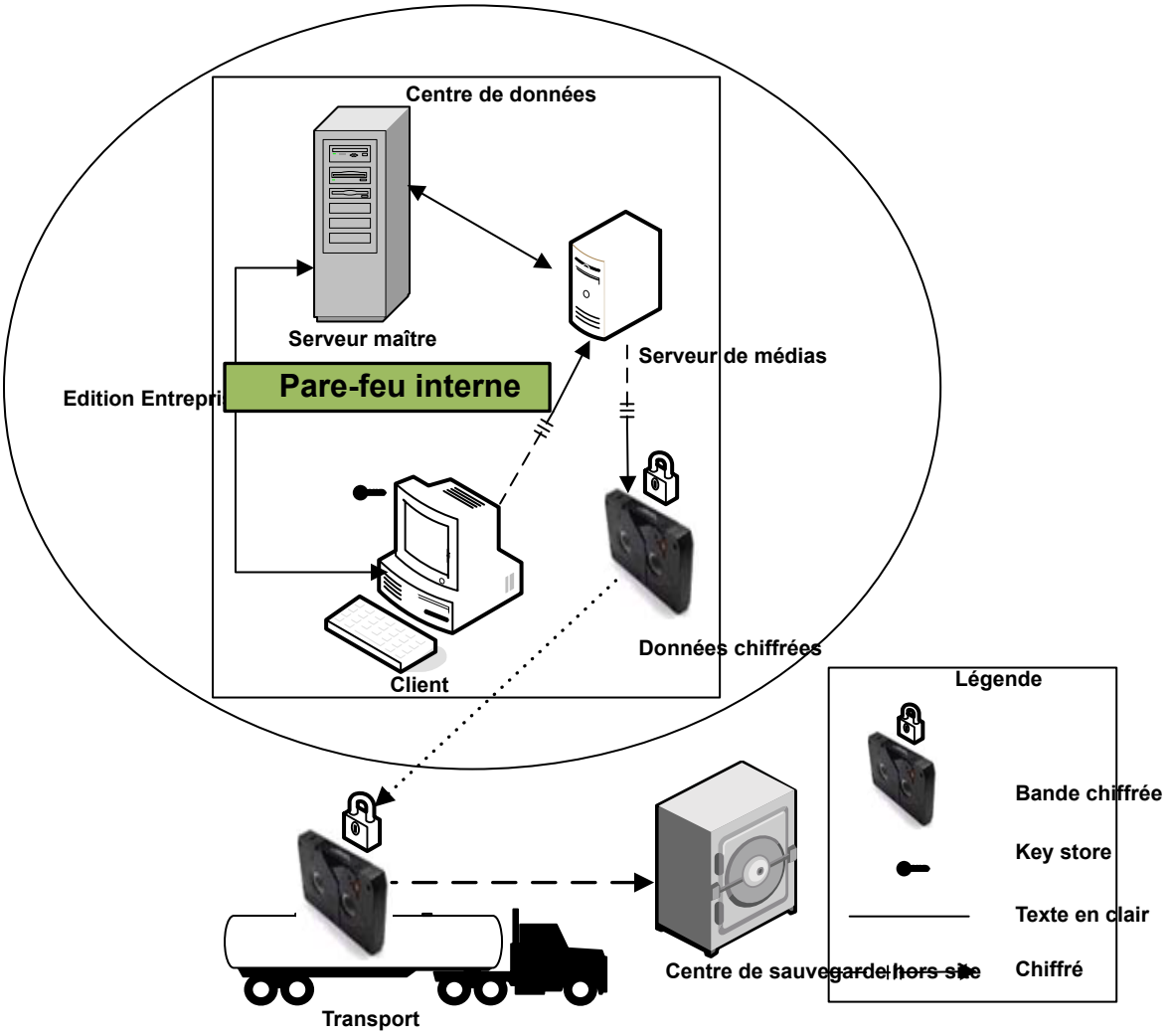
- FlashBackup
- FlashBackup-Windows
- NDMP

- NetWare
- OS/2
- Centre de sauvegarde

Notez que les clients VMS et OpenVMS ne prennent pas en charge l'option de chiffrement de client. Ces clients utilisent le type de politique standard.

Le schéma suivant affiche un exemple de la configuration du chiffrement côté client.

Figure 2-6 Chiffrement côté client



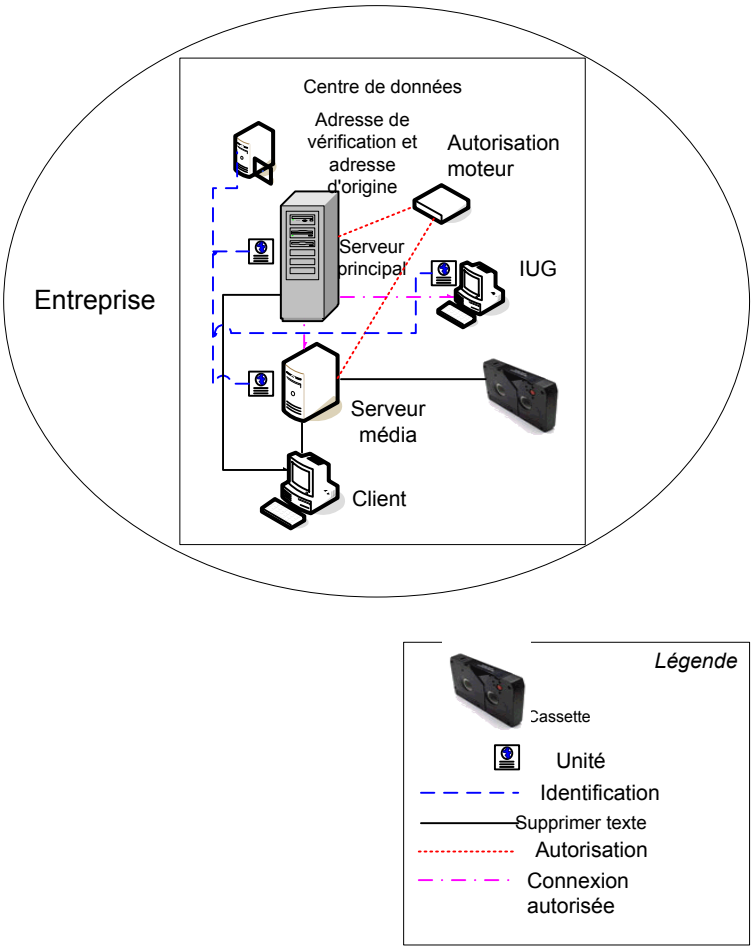
NBAC sur le serveur maître, le serveur de médias et la sécurité d'interface utilisateur graphique

Le courtier fournit les informations d'authentification au serveur maître, au serveur de médias et à l'interface utilisateur graphique. Le courtier fournit les informations d'authentification au serveur maître, au serveur de médias et à l'interface utilisateur

graphique. Cet exemple du data center utilise NetBackup Access Control sur le serveur maître et les serveurs de médias pour limiter l'accès aux parties de NetBackup. L'administration non-racine de NetBackup peut également être réalisée à l'aide de cet exemple. NBAC est configuré pour l'utilisation entre les serveurs et les interfaces utilisateur graphiques. Les utilisateurs non-root peuvent ouvrir une session sur NetBackup à l'aide du système d'exploitation. Utilisez le mot de passe UNIX ou le domaine local Windows pour gérer NetBackup. Les référentiels d'utilisateurs (NIS/NIS+ ou Active Directory) peuvent également être utilisés pour gérer NetBackup. En outre, NBAC peut être utilisé pour limiter le niveau d'accès à NetBackup de certains utilisateurs. Par exemple, vous pouvez isoler le contrôle opérationnel quotidien de la configuration environnementale (ajout de nouvelles politiques, robots, par exemple).

Le schéma suivant affiche un exemple NBAC sur la configuration de serveur maître et de serveurs de médias.

Figure 2-7 NBAC sur le serveur maître et le serveur de médias



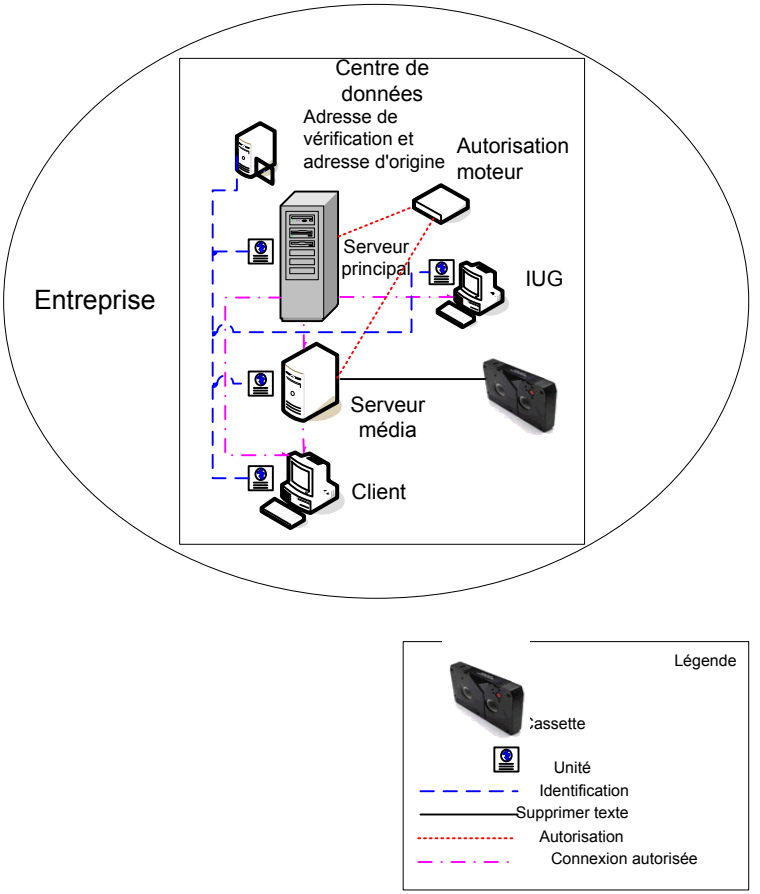
Sécurité complète NBAC

La méthode de sécurité complète NBAC utilise le courtier d'authentification pour fournir les informations d'authentification au serveur maître, au serveur de médias et au client. Cet environnement est très semblable au serveur maître NBAC, au serveur de médias et au modèle d'interface utilisateur graphique. La différence principale réside dans le fait que tous les hôtes faisant partie de l'environnement NetBackup sont identifiés de manière sécurisée à l'aide d'informations d'authentification. Par ailleurs, les administrateurs autres que racine ont la capacité de gérer les clients NetBackup basés sur les niveaux configurables de l'accès.

Notez que les identités des utilisateurs peuvent se trouver dans des référentiels globaux tels que l'annuaire Active Directory sous Windows ou NIS sous UNIX. Les identités peuvent également se trouver dans des référentiels locaux (mot de passe UNIX, domaine Windows local) sur ces hôtes prenant en charge un courtier d'authentification.

Le schéma suivant affiche un exemple de configuration terminée de NBAC.

Figure 2-8 NBAC complet



Chapitre 3

Modèles de déploiement de la sécurité

Ce chapitre traite des sujets suivants :

Groupes de travail

Un groupe de travail est un petit groupe de systèmes (moins de 50) qui est utilisé en interne avec NetBackup.

Un exemple de groupe de travail est affiché comme suit :

- Se reporter à "Groupe de travail avec NetBackup" à la page 65.

Data centers uniques

Un data center unique contient un groupe d'hôtes de grande taille (supérieure à 50).

Des exemples de data centers uniques sont indiqués dans la liste suivante :

- Se reporter à "Data center unique avec logiciel NetBackup standard" à la page 69.
- Se reporter à "Data center unique avec chiffrement côté client" à la page 72.
- Se reporter à "Data center unique avec NetBackup Access Control sur les serveurs maîtres et de médias" à la page 74.
- Se reporter à "Data center unique avec transport NetBackup Access Control" à la page 78.

Data centers multiples

Un data center multiple contient un groupe d'hôtes de taille moyenne à grande (plus de 50). Ces hôtes peuvent couvrir deux zones géographiques ou plus et être connectés à un réseau étendu (WAN).

Des exemples de data centers multiples sont indiqués dans la liste suivante :

- Se reporter à "Data center multiple avec NetBackup standard" à la page 82.
- Se reporter à "Centre de données multiple avec chiffrement côté client" à la page 86.
- Se reporter à "Data center multiple avec NetBackup Access Control sur les serveurs maîtres et de médias" à la page 92.
- Se reporter à "Data center multiple avec NBAC complet" à la page 98.

Groupe de travail avec NetBackup

Un groupe de travail avec NetBackup est classé en tant que petit groupe de systèmes (moins de 50). Le groupe de travail est utilisé avec NetBackup en interne. Cette configuration n'a généralement pas de service de dénomination unifié tel que NIS ou Active Directory. Elle peut ne pas avoir un service de dénomination d'hôte de référence tel que DNS ou WINS. L'on retrouve typiquement cette configuration

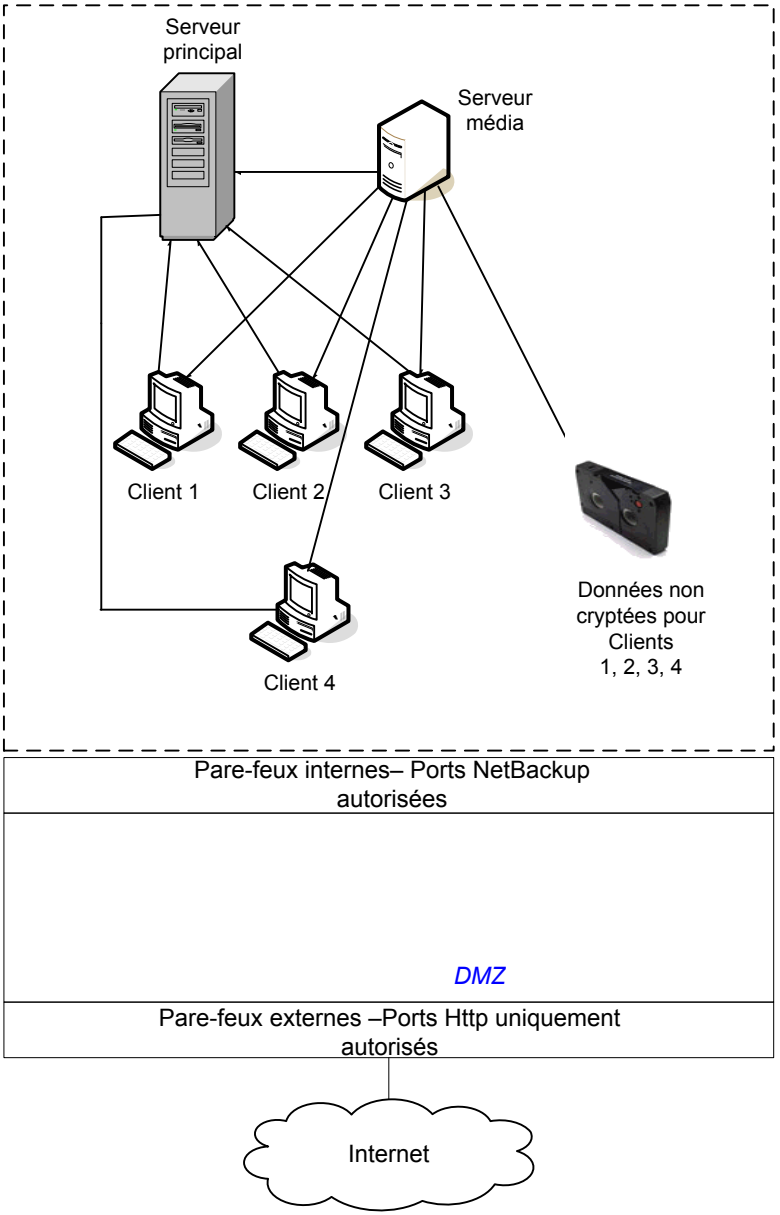
dans les laboratoires de test de grandes sociétés ou comme environnements dans de petites sociétés.

Le groupe de travail avec NetBackup présente les caractéristiques suivantes :

- Très peu de serveurs NetBackup
- Environnements informatiques de taille réduite
- Pas de matériel communiquant avec l'extérieur

présente un exemple de groupe de travail avec NetBackup.

Figure 3-1 Groupe de travail avec NetBackup



Le tableau suivant décrit les composants de NetBackup qui sont utilisés avec le groupe de travail.

Tableau 3-1 Composants de NetBackup utilisés avec le groupe de travail

Composant	Description
Serveur maître	Communique avec le serveur de médias et les clients 1, 2, 3 et 4.
Serveur de médias	Le serveur de médias communique avec le serveur maître et les clients 1, 2, 3 et 4. Il gère l'enregistrement des données déchiffrées pour enregistrer sur bande pour les clients 1, 2, 3 et 4.
Bande	La bande contient les données de sauvegarde non chiffrées des clients 1, 2, 3 et 4.
Clients	Les clients 1, 2, 3 et 4 sont les clients NetBackup standard gérés par le serveur maître. Leurs données non chiffrées sont sauvegardées sur bande par le serveur de médias.
Pare-feu interne	Permet à NetBackup d'avoir accès aux clients dans la zone démilitarisée. Vous ne pouvez activer que les ports NetBackup sélectionnés et les ports de certaines applications pour transmettre des données depuis et vers la zone démilitarisée. Les ports HTTP qui sont ouverts dans le pare-feu externe ne sont pas autorisés à passer par le pare-feu interne depuis Internet. Le pare-feu interne n'est pas utilisé avec le modèle de déploiement de groupe de travail. Dans cet exemple, aucun client n'accède au pare-feu interne. Par conséquent, les ports de NetBackup ne doivent pas être ouverts par son biais. **Remarque :** Dans cet exemple il n'existe aucun client au delà du pare-feu interne. Ainsi les ports de NetBackup ne doivent pas être ouverts par l'intermédiaire du pare-feu interne.
Zone démilitarisée (DMZ)	Fournit une zone d'opérations "sécurisée" pour les clients NetBackup existant entre le pare-feu interne et le pare-feu externe. Les clients opérant éventuellement dans la zone démilitarisée incluent des clients NetBackup de serveur Web utilisant les clients NetBackup standard ou les clients NetBackup chiffrés. Les clients de la zone démilitarisée peuvent communiquer avec NetBackup par le biais du pare-feu interne à l'aide des ports NetBackup spécifiés. Les clients NetBackup de serveur Web peuvent recevoir des connexions du pare-feu externe vers Internet en utilisant les ports HTTP normaux. La zone démilitarisée n'est pas accessible pour les clients du modèle de déploiement du groupe de travail.
Pare-feu externe	Le pare-feu externe permet aux utilisateurs externes d'accéder aux clients NetBackup de serveur Web situés dans la zone démilitarisée à partir d'Internet, généralement par les ports HTTP. Les ports NetBackup s'ouvrent pour que les clients qui ne sont pas autorisés à passer par le pare-feu externe puissent communiquer par l'intermédiaire du pare-feu interne vers Internet.
Internet	Spécifie un ensemble de réseaux d'ordinateurs connectés entre eux par des câbles de cuivre, des câbles de fibre optique ou par des connexions sans fil. Les clients n'utilisent pas Internet dans le modèle de déploiement de groupe de travail. **Attention :** Les clients ne doivent jamais placer des clients NetBackup en dehors de la zone démilitarisée et directement sur Internet. Un pare-feu externe doit être utilisé pour bloquer en permanence l'accès aux ports de NetBackup à partir de l'extérieur.

Data center unique avec logiciel NetBackup standard

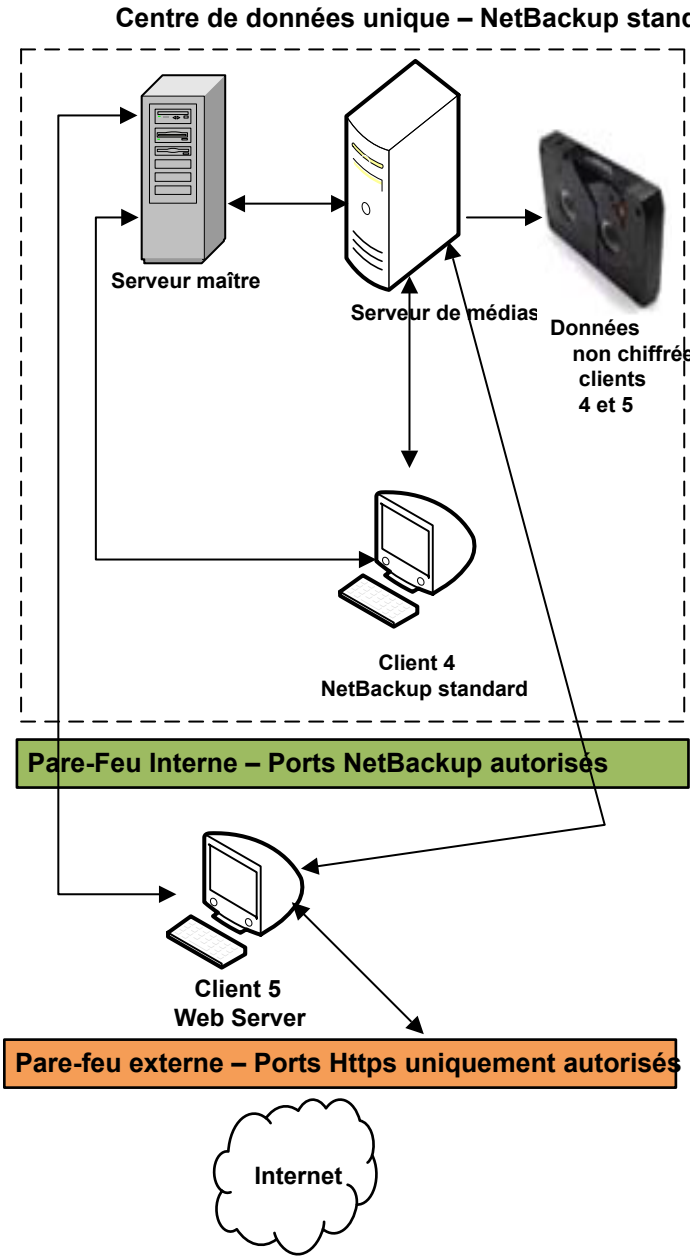
Un data center unique avec NetBackup standard est défini comme support au grand groupe d'hôtes (supérieur à 50). Il inclut les hôtes qui sont internes seulement et ceux qui se développent par la zone démilitarisée à l'Internet. Cette configuration centralise généralement le service d'appelation des hôtes (tels que DNS ou WINS). Il compte également un service de nommage centralisé des utilisateurs (service NIS, Network Information Services ou annuaire Active Directory).

Le data center unique avec NetBackup standard inclut :

- Hôtes interfacés avec l'extérieur
- Les services de nommage centralisés existent en général
- Taille supérieure à 50 hôtes
- Très facile à configurer et ne requiert qu'une connaissance générale de NetBackup
- Configuration généralement utilisée pour les clients NetBackup
- N'assume aucune crainte de l'interception passive de données sur le câble pendant l'exécution de la sauvegarde

présente un exemple de datacenter unique avec logiciel NetBackup standard.

Figure 3-2 Data center unique avec logiciel NetBackup standard



Le tableau suivant décrit les composants de NetBackup qui sont utilisés pour un data center unique avec NetBackup standard.

Tableau 3-2 Composants NetBackup pour data center unique avec NetBackup standard

Composant	Description
Serveur maître	Communique avec le serveur de médias, le client 4 de NetBackup standard et le client 5 de NetBackup serveur Web dans la zone démilitarisée.
Serveur de médias	Communique avec le serveur maître, le client 4 de NetBackup standard et le client 5 de NetBackup serveur Web dans la zone démilitarisée. Le serveur de médias gère l'écriture sur bande de données non chiffrées pour les clients 4 et 5.
Bande	Contient les données de sauvegarde décryptées qui sont enregistrées pour les clients 4 et 5.
Clients	Spécifie que le client 4 est un type de NetBackup standard et le client 5 est un type de serveur Web. Le serveur maître gère les deux clients et le serveur de médias sauvegarde leurs données non codées sur bande. Le client 4 existe dans le data center Le client 5 existe dans la zone démilitarisée. Le client 5 communique vers NetBackup à l'aide des ports réservés à NetBackup via le pare-feu interne. Le client 5 reçoit des connexions Internet en utilisant des ports réservés au HTTP via le pare-feu externe. Notez que tout le trafic de consultation de NetBackup est envoyé non chiffré, par câble.
Pare-feu interne	Permet à NetBackup d'accéder au client 5 de NetBackup serveur Web dans la zone démilitarisée. Vous ne pouvez activer que les ports NetBackup sélectionnés et les ports de certaines applications pour transmettre des données depuis et vers la zone démilitarisée. Les ports HTTP qui sont ouverts dans le pare-feu externe ne peuvent pas passer par le pare-feu interne d'Internet.
Zone démilitarisée (DMZ)	Fournit une zone d'opérations "sécurisée" pour le client 5 de NetBackup serveur Web qui existe entre le pare-feu interne et le pare-feu externe. Le client 5 de la zone démilitarisée peut communiquer avec NetBackup par le pare-feu interne à l'aide des ports de NetBackup indiqués. Le client 5 de serveur Web peut communiquer sur Internet via le pare-feu externe en utilisant des ports HTTP.
Pare-feu externe	Permet aux utilisateurs externes d'accéder au client 5 de serveur Web situé dans la zone démilitarisée depuis les ports Internet sur HTTP. Les ports NetBackup sont ouverts pour le client 5 afin qu'il communique par le pare-feu interne. **Attention :** Les ports NetBackup ne sont pas autorisés à passer par le pare-feu externe pour se connecter à Internet. Seuls les ports HTTP vers le client 5 sont ouverts dans le pare-feu externe pour se connecter à Internet.

Composant	Description
Internet	Internet est un ensemble de réseaux d'ordinateurs connectés entre eux par des câbles de cuivre, des câbles de fibre optique ou par des connexions sans fil. Le client 5 de serveur Web peut recevoir des connexions sur Internet par le biais du pare-feu externe en utilisant des ports HTTP.

Data center unique avec chiffrement côté client

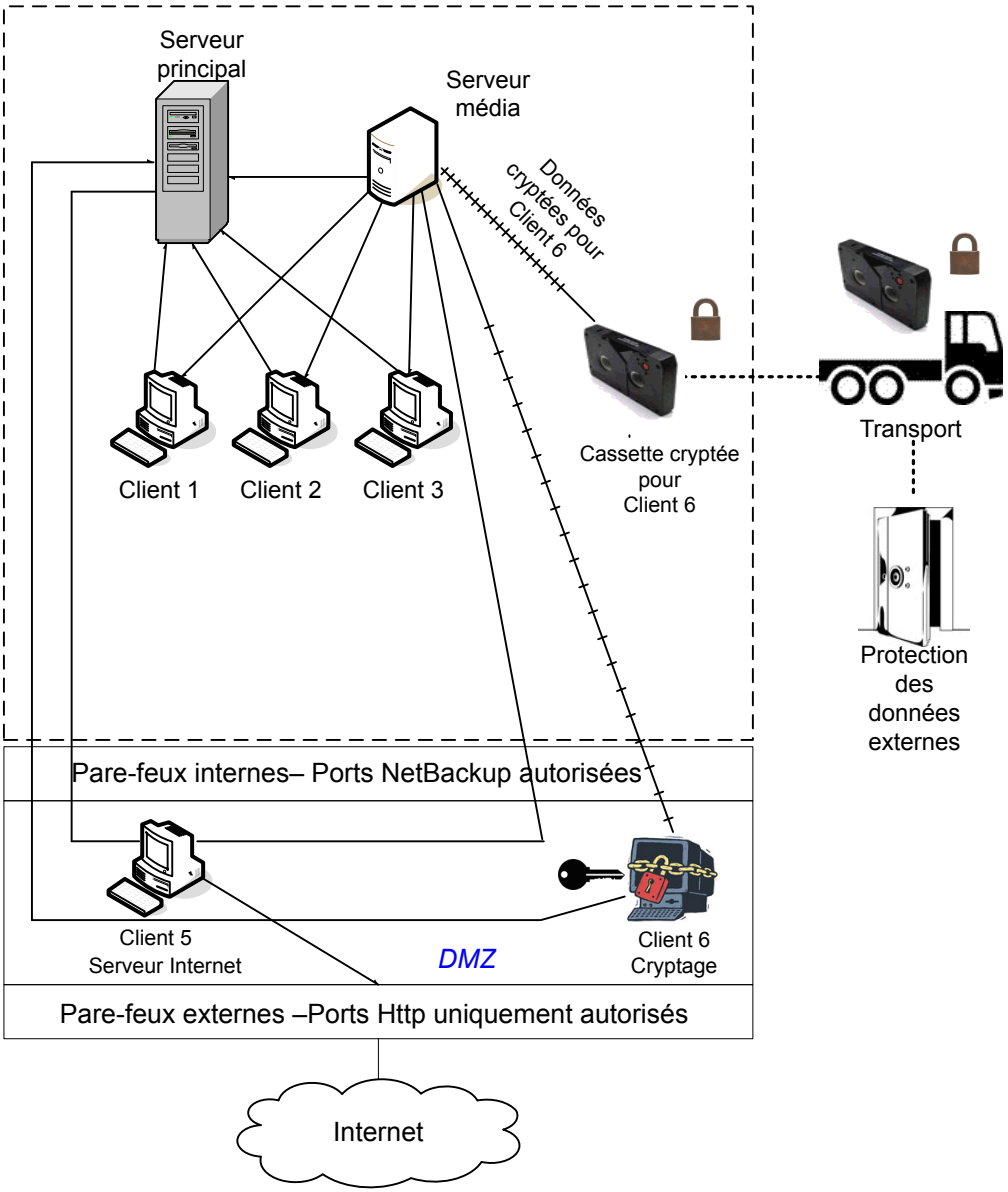
Cet exemple de data center unique avec chiffrement côté client utilise le chiffrement côté client pour garantir la confidentialité des données transmises par fil et enregistrées sur bande. Le chiffrement côté client atténue les risques de branchement de clandestin de fil passif au sein de l'entreprise. Le risque de divulgation de données est réduit car les bandes sont déplacées hors site. Ce modèle de data center assure un support à un grand nombre (supérieur à 50) d'hôtes gérés. Les clients du data center ainsi que la DMZ peuvent utiliser des services d'attribution de nom centralisés pour les hôtes et identités d'utilisateur.

Le data center unique avec le chiffrement côté client présente les caractéristiques suivantes :

- Utile pour protéger les données hors site
- Les données du client sont chiffrées pour empêcher l'interception passive des données transmises par le câble
- La gestion des clés est décentralisée vers les clients
- L'option de chiffrement NetBackup initiale
- Le processeur du client est utilisé pour exécuter le chiffrement
- Vous devez disposer de la clé pour récupérer les données. Une clé perdue est synonyme de perte de données.
- Utile pour analyser des bandes hors site et/ou lorsque la confidentialité est nécessaire sur le câble

Figure 3-3 présente un exemple de data center unique avec chiffrement côté client.

Figure 3-3 Data center unique avec chiffrement côté client



Le tableau suivant décrit les composants NetBackup qui sont utilisées pour un seul data center avec chiffrement côté client.

Tableau 3-3 Composants NetBackup d'un data center unique avec chiffrement côté client

Composant	Description
Zone démilitarisée (DMZ)	Fournit une zone d'opérations "sécurisée" pour le client 5 de serveur Web et le client chiffré 6. Ces clients existent entre le pare-feu interne et le pare-feu externe. Le client 5 de serveur Web et le client chiffré 6 de la zone démilitarisée peuvent communiquer avec NetBackup via le pare-feu interne en utilisant les ports NetBackup affectés. Le client 5 de serveur Web et le client chiffré 6 peuvent échanger des données sur Internet par le biais du pare-feu externe en utilisant des ports HTTP. Le client chiffré 6 dans la zone démilitarisée peut communiquer avec NetBackup par le biais du pare-feu interne à l'aide des ports NetBackup affectés.
Pare-feu externe	Il permet aux utilisateurs externes d'accéder au client 5 de serveur Web et au client chiffré 6. Ces clients sont accessibles dans la zone démilitarisée via Internet, par le biais des ports HTTP. Les ports de NetBackup sont ouverts pour le client 5 de serveur Web et le client chiffré 6 pour communiquer via le pare-feu interne. Les ports NetBackup ne sont cependant pas autorisés à passer par le pare-feu externe pour se connecter à Internet. Seuls les ports HTTP du client 5 de serveur Web peuvent passer par le pare-feu externe pour se connecter à Internet. Le pare-feu externe limite les clients 5 et 6 de la communication bidirectionnelle par Internet.
Internet	Internet est un ensemble de réseaux d'ordinateurs connectés entre eux par des câbles de cuivre, des câbles de fibre optique ou par des connexions sans fil. Le client 5 de serveur Web peut communiquer via Internet à l'aide de ports HTTP à travers le pare-feu externe.

Data center unique avec NetBackup Access Control sur les serveurs maîtres et de médias

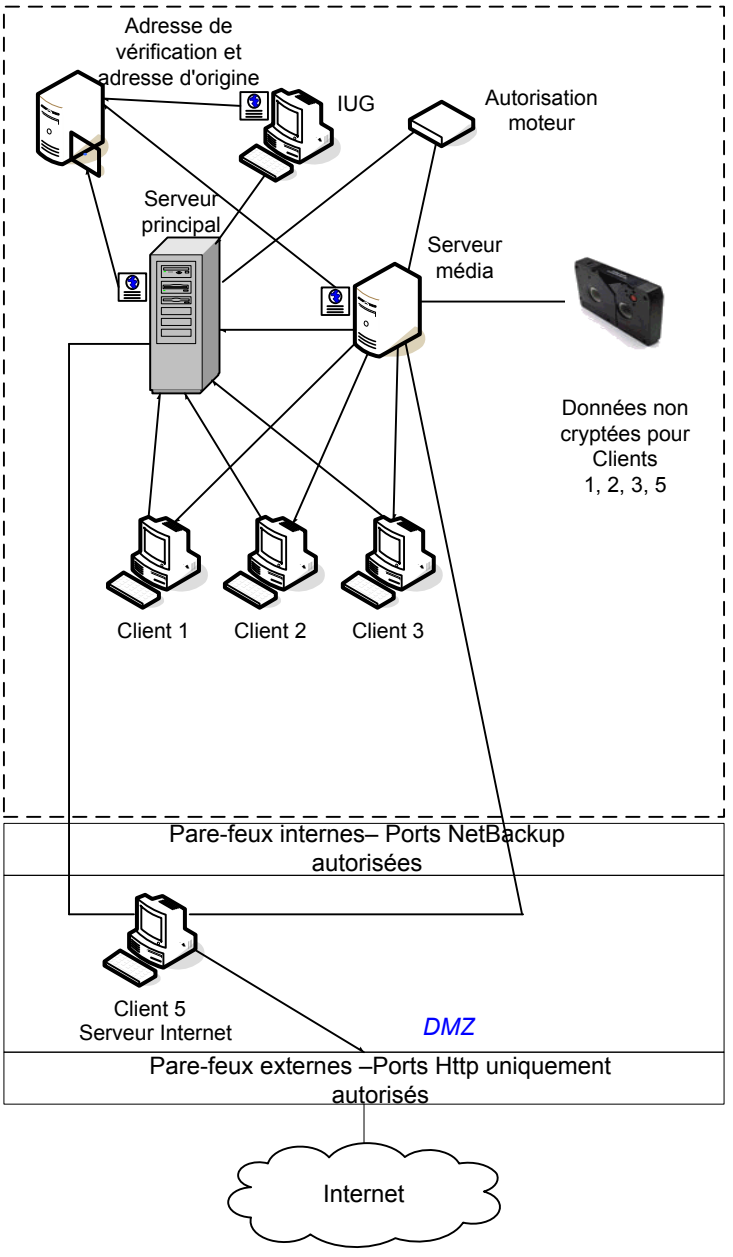
L'exemple du data center unique avec NBAC sur des serveurs maîtres et des serveurs de médias utilise NetBackup Access Control sur les serveurs maîtres et les serveurs de médias. Cette configuration limite l'accès à certaines parties de NetBackup et fournit l'administration autre que racine de NetBackup. NBAC est configuré pour s'exécuter entre les serveurs et les interfaces graphiques utilisateur. Les utilisateurs autres que racine peuvent se connecter à NetBackup avec le système d'exploitation (mot de passe UNIX ou domaine local Windows) ou les référentiels d'utilisateur globaux (NIS/NIS+ ou Active Directory) pour gérer NetBackup. En outre, NBAC peut être utilisé pour limiter le niveau d'accès de certains utilisateurs à NetBackup. Par exemple, vous pouvez isoler le contrôle opérationnel quotidien de la configuration de l'environnement (ajout de nouvelles politiques, robots, etc.).

Le data center unique avec NBAC sur les serveurs maîtres et de médias inclut les éléments suivants :

- Gestion des utilisateurs autres que racine
- Gestion d'UNIX avec un ID d'utilisateur Windows
- Gestion de Windows avec un compte UNIX
- Isolement et limitation des actions des utilisateurs
- La racine ou l'administrateur ou les hôtes client peuvent encore faire des sauvegardes et des restaurations du client local
- Peut être combiné avec d'autres options de sécurité
- Tous les serveurs doivent avoir la version requise NetBackup

Figure 3-4 affiche un exemple de data center unique avec NBAC sur les serveurs maîtres et de médias.

Figure 3-4 Data center unique avec NetBackup Access Control sur les serveurs maîtres et de médias



Le tableau suivant décrit les composants de NetBackup qui sont utilisés pour un data center unique avec NBAC sur les serveurs maîtres et de médias.

Tableau 3-4 Composants NetBackup du data center unique avec NBAC sur les serveurs maîtres et de médias

Composant	Description
Serveur maître	Communique avec le serveur de médias, le courtier racine et le courtier d'authentification. Il communique également avec le moteur d'autorisation, les clients 1, 2, 3 et le client 5, le serveur Web, dans la zone démilitarisée. Le serveur maître communique avec et reçoit des informations d'authentification du courtier d'authentification. Lorsqu'une interface de ligne de commande ou une interface graphique utilisateur accède à un daemon situé sur un serveur maître, des informations d'authentification sont échangées pour identifier l'utilisateur. Le moteur d'autorisation est ensuite contacté pour vérifier les droits d'accès aux fonctions des daemons.
Serveur de médias	Communique avec le serveur maître, clients 1, 2, 3 et client 5, serveur Web, dans la zone démilitarisée. Le serveur de médias communique également avec le moteur d'autorisation et reçoit des informations d'authentification du courtier d'authentification. Le serveur de médias permet l'écriture sur bande de données non chiffrées pour les clients 1, 2, 3 et 5. Lorsqu'une interface de ligne de commande ou une interface graphique utilisateur accède à un daemon situé sur un serveur de médias, des informations d'authentification sont échangées pour identifier l'utilisateur. Le moteur d'autorisation est ensuite contacté pour vérifier les droits d'accès aux fonctions des daemons.
Interface graphique utilisateur (GUI)	Cette interface graphique utilisateur de la console d'administration à distance reçoit des informations d'authentification du courtier d'authentification. L'interface graphique utilisateur utilise ces informations d'authentification pour accéder aux fonctions des serveurs de médias et serveurs maîtres.
Courtier racine	Authentifie le courtier d'authentification mais pas les clients. Dans l'exemple suivant, le courtier racine et le courtier d'authentification sont affichés comme même composant.
Courtier d'authentification	Authentifie le serveur maître, le serveur de médias et l'interface graphique utilisateur en établissant les informations d'authentification avec chacun. Si une invite de commande est utilisée, le courtier d'authentification authentifie également un utilisateur.
Moteur d'autorisation	Communique avec le serveur maître et le serveur de médias pour déterminer les autorisations d'un utilisateur authentifié. Ces autorisations déterminent les fonctionnalités disponibles pour l'utilisateur. Il stocke également les groupes d'utilisateurs et les autorisations. Un seul moteur d'autorisation est nécessaire. **Remarque :** Le moteur d'autorisation se trouve sur le serveur maître en tant que processus de daemon. Il est affiché dans le schéma en tant qu'image distincte à titre d'exemple uniquement.
Bande	La bande contient les données de sauvegarde non chiffrées des clients 1, 2, 3 et 5.

Composant	Description
Clients	Les clients 1, 2 et 3 sont des types de NetBackup standard et le client 5 est un type de serveur Web. Les deux types sont gérés par le serveur maître et leurs données non chiffrées sont sauvegardées sur bande par le serveur de médias. Les clients 1, 2 et 3 existent dans le data center. Le client 5 existe dans la zone démilitarisée. Le client 5 communique vers NetBackup à l'aide des ports réservés à NetBackup via le pare-feu interne. Le client 5 reçoit des connexions Internet en utilisant des ports réservés au HTTP via le pare-feu externe.
Pare-feu interne	Permet à NetBackup d'accéder au client 5 de serveur Web dans la zone démilitarisée. Vous ne pouvez activer que les ports NetBackup sélectionnés et les ports de certaines applications pour transmettre des données depuis et vers la zone démilitarisée. Des ports HTTP sont ouverts dans le pare-feu externe et ne sont pas autorisés à passer par le pare-feu interne.
Zone démilitarisée (DMZ)	Fournit une zone d'opérations "sécurisée" pour le client 5 de serveur Web qui existe entre le pare-feu interne et le pare-feu externe. Le client 5 de serveur Web de la zone démilitarisée peut échanger des données avec NetBackup via le pare-feu interne en utilisant les ports NetBackup affectés. Le client 5 de serveur Web peut communiquer sur Internet via le pare-feu externe en utilisant des ports HTTP.
Pare-feu externe	Permet aux utilisateurs externes d'accéder au client 5 de serveur Web situé dans la zone démilitarisée depuis les ports Internet sur HTTP. Les ports NetBackup sont ouverts pour le client 5 afin qu'il communique par le pare-feu interne. Les ports NetBackup ne sont pas autorisés à passer par le pare-feu externe pour se connecter à Internet. Seuls les ports HTTP du client 5 peuvent passer par le pare-feu externe pour se connecter à Internet.
Internet	Internet est un ensemble de réseaux d'ordinateurs connectés entre eux par des câbles de cuivre, des câbles de fibre optique ou par des connexions sans fil. Le client 5 peut communiquer par Internet en utilisant des ports HTTP via le pare-feu externe.

Data center unique avec transport NetBackup Access Control

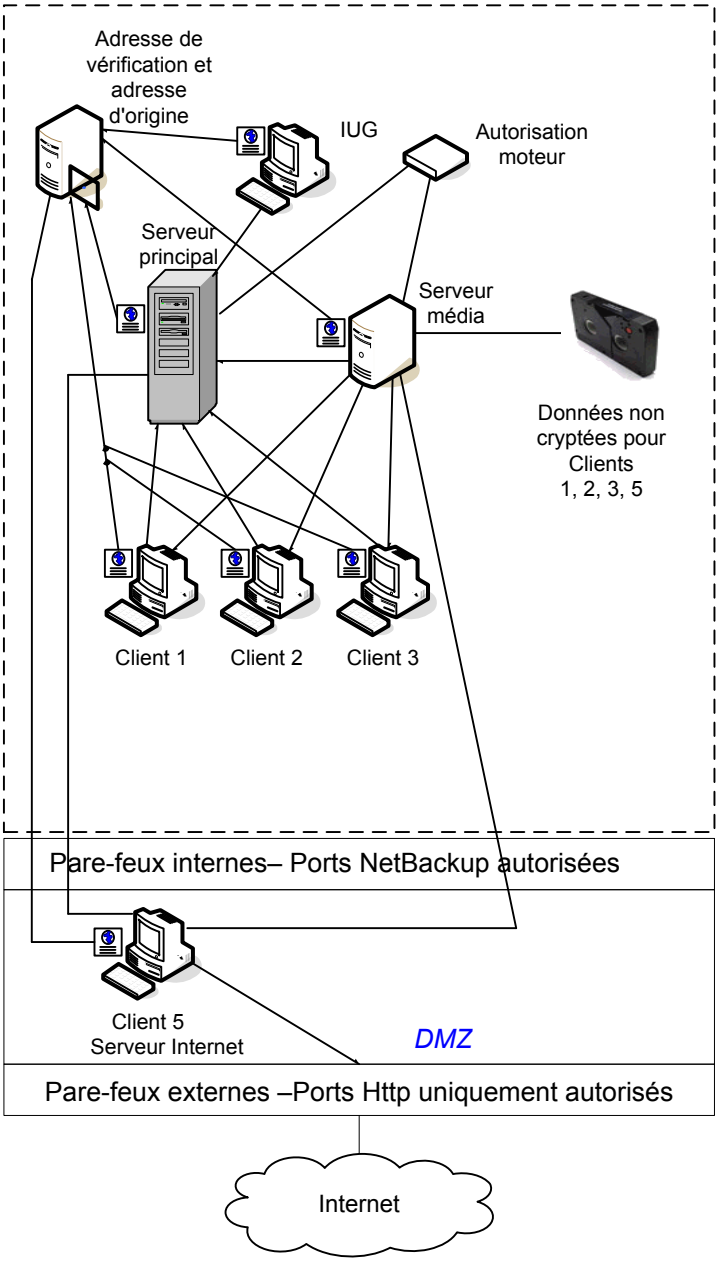
Le data center unique avec l'environnement de NBAC complet est très semblable au data center unique avec le serveur maître et de médias de NBAC. Les différences principales sont que tous les hôtes qui participent à l'environnement de NetBackup sont identifiés de manière fiable avec les informations d'authentification. Les administrateurs non racine peuvent également gérer les clients NetBackup basés sur les niveaux d'accès configurables. Notez que les identités des utilisateurs peuvent se trouver dans des référentiels globaux tels que l'annuaire Active Directory sous Windows ou NIS sous UNIX. Les identités peuvent également se trouver dans des référentiels locaux (mot de passe UNIX, domaine Windows local) sur ces hôtes prenant en charge un courtier d'authentification.

Le data center unique avec NBAC complet inclut ce qui suit :

- Semblable aux détails pour le data center unique avec le serveur maître et le serveur de médias de NBAC, excepté la racine ou l'administrateur sur le client
- Pour les systèmes client, vous pouvez configurer les utilisateurs qui ne sont ni utilisateur racine, ni administrateur pour qu'ils puissent effectuer des sauvegardes et restaurations locales (configuration par défaut)
- L'environnement facilite la connexion de tous les hôtes autorisés faisant partie de NetBackup
- Tous les hôtes doivent avoir la version requise NetBackup

Figure 3-5 affiche un exemple d'un unique data center avec NBAC complet.

Figure 3-5 Data center unique avec transport NetBackup Access Control



Le tableau suivant décrit les composants de NetBackup qui sont utilisés avec un data center unique avec NBAC complet.

Tableau 3-5 Composants de NetBackup pour data center unique avec NBAC complet

Composant	Description
Serveur maître	Communique avec le serveur de médias, le courtier racine et le courtier d'authentification. Il communique également avec le moteur d'autorisation, les clients 1, 2, 3 et le client 5, le serveur Web, dans la zone démilitarisée. Le serveur maître communique envoie davantage de données avec le courtier d'authentification qui lui envoie des informations d'authentification. Lorsqu'une interface de ligne de commande ou une interface graphique utilisateur accède à un daemon situé sur un serveur maître, des informations d'authentification sont échangées pour identifier l'utilisateur. Le moteur d'autorisation est contacté pour vérifier les droits d'accès aux fonctions des daemons.
Serveur de médias	Communique avec le serveur maître, clients 1, 2, 3 et client 5, serveur Web, dans la zone démilitarisée. Le serveur de médias communique également avec le moteur d'autorisation et reçoit des informations d'authentification du courtier d'authentification. Le serveur de médias permet l'écriture sur bande de données non chiffrées pour les clients 1, 2, 3 et 5. Lorsqu'une interface de ligne de commande ou une interface graphique utilisateur accède à un daemon situé sur un serveur de médias, des informations d'authentification sont échangées pour identifier l'utilisateur. Le moteur d'autorisation est contacté pour vérifier les droits d'accès aux fonctions des daemons.
Interface graphique utilisateur (GUI)	Cette interface graphique utilisateur de la console d'administration à distance reçoit des informations d'authentification du courtier d'authentification. L'interface graphique utilisateur utilise ces informations d'authentification pour accéder aux fonctions des serveurs de médias et serveurs maîtres.
Courtier racine	Authentifie le courtier d'authentification mais pas les clients. Figure 3-5, affiche le courtier racine et le courtier d'authentification comme même composant.
Courtier d'authentification	Authentifie le serveur maître, le serveur de médias, l'interface graphique utilisateur, les clients et les utilisateurs en établissant les informations d'authentification avec chacun.
Moteur d'autorisation	Communique avec le serveur maître et le serveur de médias pour déterminer les autorisations d'un utilisateur authentifié. Il stocke également les groupes d'utilisateurs et les autorisations. Un seul moteur d'autorisation est nécessaire. **Remarque :** Le moteur d'autorisation se trouve sur le serveur maître en tant que processus de daemon. Il est affiché dans le schéma en tant qu'image distincte à titre d'exemple uniquement.
Bande	La bande contient les données de sauvegarde non chiffrées des clients 1, 2, 3 et 5.

Composant	Description
Clients	Les clients 1, 2 et 3 sont des types de NetBackup standard et le client 5 est un type de serveur Web. Lors de la réception des informations d'authentification du courtier d'authentification, les clients 1, 2, 3 et 5 sont authentifiés dans le domaine NetBackup Product Authentication Service. Le serveur standard et les types de serveur Web sont gérés par le serveur maître et ont leurs données non chiffrées sauvegardées sur bande par le serveur de médias. Les clients 1, 2 et 3 existent dans le data center. Le client 5 existe dans la zone démilitarisée. Le client 5 communique vers NetBackup à l'aide des ports réservés à NetBackup via le pare-feu interne. Le client 5 reçoit des connexions Internet en utilisant des ports réservés au HTTP via le pare-feu externe.
Pare-feu interne	Permet à NetBackup d'accéder au client 5 de serveur Web dans la zone démilitarisée. Vous ne pouvez activer que les ports NetBackup sélectionnés et les ports de certaines applications pour transmettre des données depuis et vers la zone démilitarisée. Des ports HTTP sont ouverts dans le pare-feu externe et ne sont pas autorisés à passer par le pare-feu interne.
Zone démilitarisée (DMZ)	Fournit une zone d'opérations "sécurisée" pour le client 5 de serveur Web qui existe entre le pare-feu interne et le pare-feu externe. Le client 5 de serveur Web de la zone démilitarisée peut échanger des données avec NetBackup via le pare-feu interne en utilisant les ports NetBackup affectés. Le client 5 de serveur Web peut communiquer sur Internet via le pare-feu externe en utilisant des ports HTTP.
Pare-feu externe	Permet aux utilisateurs externes d'accéder au client 5 de serveur Web situé dans la zone démilitarisée depuis les ports Internet sur HTTP. Les ports NetBackup sont ouverts pour le client 5 afin qu'il communique par le pare-feu interne. Les ports NetBackup ne sont pas autorisés à passer par le pare-feu externe pour se connecter à Internet. Seuls les ports HTTP du client 5 peuvent passer par le pare-feu externe pour se connecter à Internet.
Internet	Internet est un ensemble de réseaux d'ordinateurs connectés entre eux par des câbles de cuivre, des câbles de fibre optique ou par des connexions sans fil. Le client 5 peut communiquer par Internet en utilisant des ports HTTP via le pare-feu externe.

Data center multiple avec NetBackup standard

Un data center unique avec NetBackup standard est défini comme support pour un grand groupe d'hôtes (plus de 50). Ces hôtes peuvent couvrir deux ou plusieurs régions géographiques et être connectés à un réseau étendu (WAN). Dans l'exemple suivant, un data center se trouve à Londres et l'autre se trouve à Tokyo. Les deux data centers sont connectés par une connexion WAN dédiée.

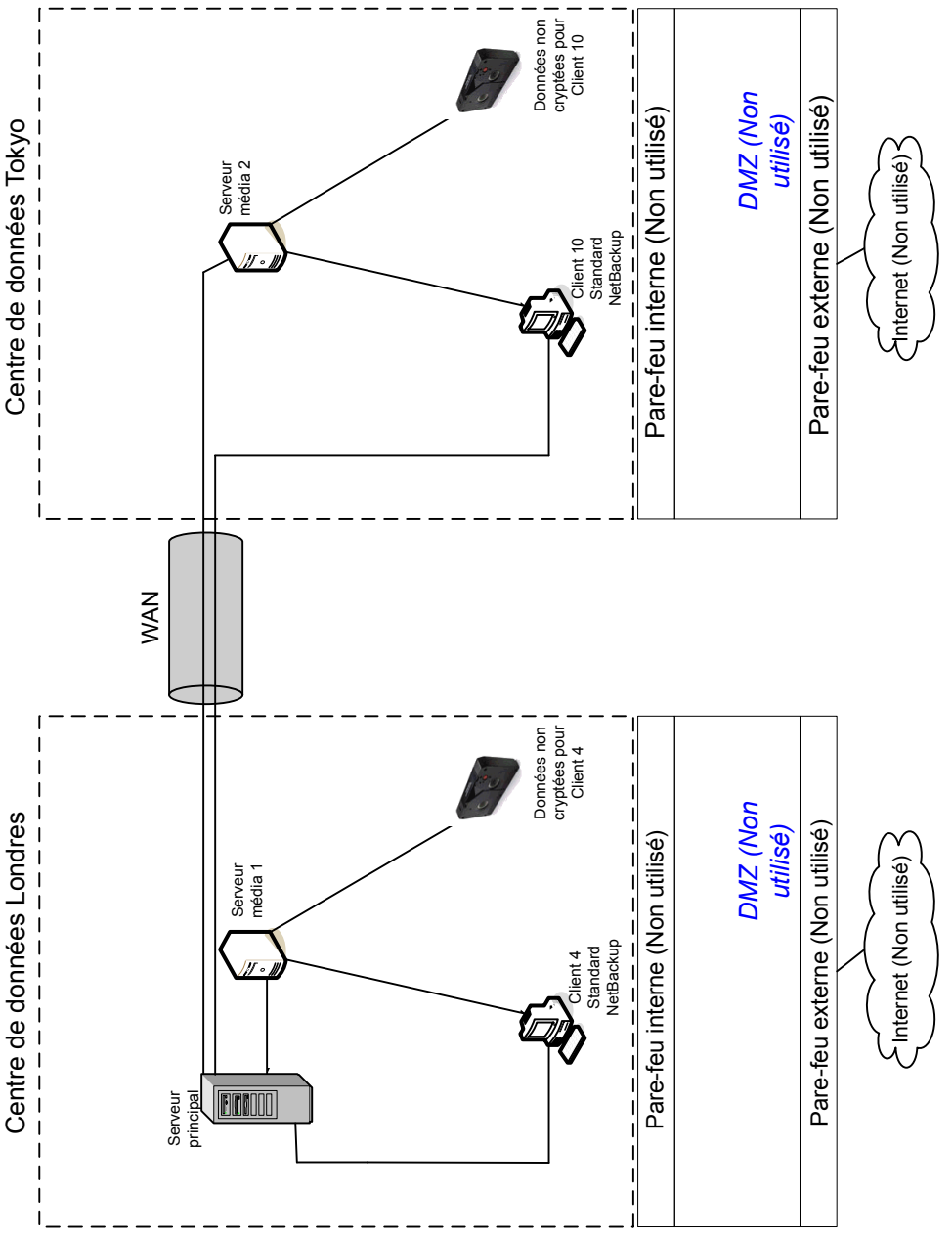
Un data center multiple inclut les hôtes qui sont internes seulement et ceux qui s'étendent sur Internet via la zone démilitarisée. Cette configuration centralise généralement le service d'appelation des hôtes (tels que DNS ou WINS). Il compte également un service de nommage centralisé des utilisateurs (service NIS, Network Information Services ou annuaire Active Directory).

Le data center multiple avec NetBackup standard inclut :

- NetBackup couvre deux régions géographiques ou plus par le biais d'un réseau étendu (WAN)
- Les services de nommage centralisés existent en général
- Taille supérieure à 50 hôtes
- Très facile à configurer et ne requiert qu'une connaissance générale de NetBackup
- N'assume aucune crainte de l'interception passive de données sur le câble pendant l'exécution de la sauvegarde

présente un exemple de datacenter multiple avec NetBackup standard.

Figure 3-6 Data center multiple avec NetBackup standard



Le tableau suivant décrit les composants de NetBackup qui sont utilisés avec un data center multiple qui a mis en application NetBackup standard.

Tableau 3-6 Composants de NetBackup pour un data center multiple avec NetBackup standard mis en application

Composant	Description
Datacenter de Londres	Le data center de Londres contient le serveur maître, le serveur de médias 1, le client 4 NetBackup standard et la bande de données non chiffrées pour le client 4. Le data center de Londres se connecte au data center de Tokyo par une connexion WAN dédiée.
Datacenter de Tokyo	Le data center de Tokyo contient le serveur de médias 2, le client 10 NetBackup standard et la bande de données non chiffrées pour le client 10. Le data center de Tokyo se connecte au data center de Londres par une connexion WAN dédiée.
Réseau étendu (WAN)	Spécifie le lien WAN dédié qui connecte le data center de Londres au data center de Tokyo. Le réseau étendu fournit une connectivité entre le serveur maître et le serveur de médias 2 et le client 10.
Serveur maître	Spécifie qu'il se trouve à Londres et communique avec le serveur de médias 1 à Londres. Le serveur maître communique également par le WAN avec le serveur de médias 2 à Tokyo. Le serveur maître communique avec le client NetBackup standard 4 à Londres et le client 10 par le WAN à Tokyo.
Serveurs de médias	Spécifie que le data center multiple peut avoir deux serveurs de médias. Un serveur de médias est à Londres et l'autre est à Tokyo. Le serveur de médias 1 à Londres communique avec le serveur de médias et le client 4 NetBackup également à Londres. Le serveur de médias 1 effectue l'écriture des données non chiffrées sur bande pour le client 4 à Londres. Le serveur de médias 2 à Tokyo communique avec le serveur maître à Londres et le client 10 NetBackup standard à Tokyo. Le serveur de médias 2 effectue l'écriture des données non chiffrées sur bande pour le client 10 à Tokyo.
Bandes	Spécifie que des bandes sont produites dans les data centers de Londres et de Tokyo. La bande de Londres contient les données de sauvegarde déchiffrées écrites pour le client 4. La bande de Tokyo contient les données de sauvegarde déchiffrées écrites pour le client 10.
Clients	Spécifie que les clients se trouvent dans les data centers de Londres et de Tokyo. Les clients 4 et 10 sont de type NetBackup standard. Les deux clients peuvent être gérés par le serveur maître qui se trouve à Londres. Leurs données déchiffrées sont sauvegardées sur bande par le serveur de médias. Les données déchiffrées sont enregistrées sur bande du client 4 à Londres et la bande du client 10 à Tokyo. Notez que tout le trafic de NetBackup pour la consultation du client 10 est envoyé non chiffré par le câble (WAN) de Tokyo à Londres.

Composant	Description
Pare-feux internes	Les pare-feux internes ne sont pas utilisés au data center de Londres ou de Tokyo avec NetBackup standard.
Zones démilitarisées (DMZ)	Les zones démilitarisées ne sont pas utilisés au data center de Londres ou de Tokyo avec NetBackup standard.
Pare-feux externes	Les pare-feux externes ne sont pas utilisés au data center de Londres ou de Tokyo avec NetBackup standard.
Internet	Internet n'est pas utilisé au data center de Londres ou de Tokyo avec NetBackup standard.

Centre de données multiple avec chiffrement côté client

Un centre de données multiple avec l'option de chiffrement côté client est défini comme un support pour un grand groupe d'hôtes (plus de 50). Ces hôtes peuvent couvrir deux ou plusieurs zones géographiques et être connectés à un réseau étendu (WAN). Dans l'exemple suivant, un centre de données se trouve à Londres et l'autre se trouve à Tokyo. Les deux centres de données sont connectés par une connexion WAN dédiée.

L'exemple du centre de données multiple peut utiliser le chiffrement côté client afin d'assurer la confidentialité des données à travers le câble et sur bande. Ce chiffrement aide à diminuer les risques de branchement clandestin au sein d'une société. Le risque d'exposition des données commes des bandes est déplacé hors site. Ce modèle de centre de données assure un support à un grand nombre (supérieur à 50) d'hôtes gérés. Les clients à l'intérieur du data center aussi bien que du DMZ, peuvent avoir la possibilité de bénéficier de services de dénomination centralisés pour des hôtes et des identités d'utilisateur.

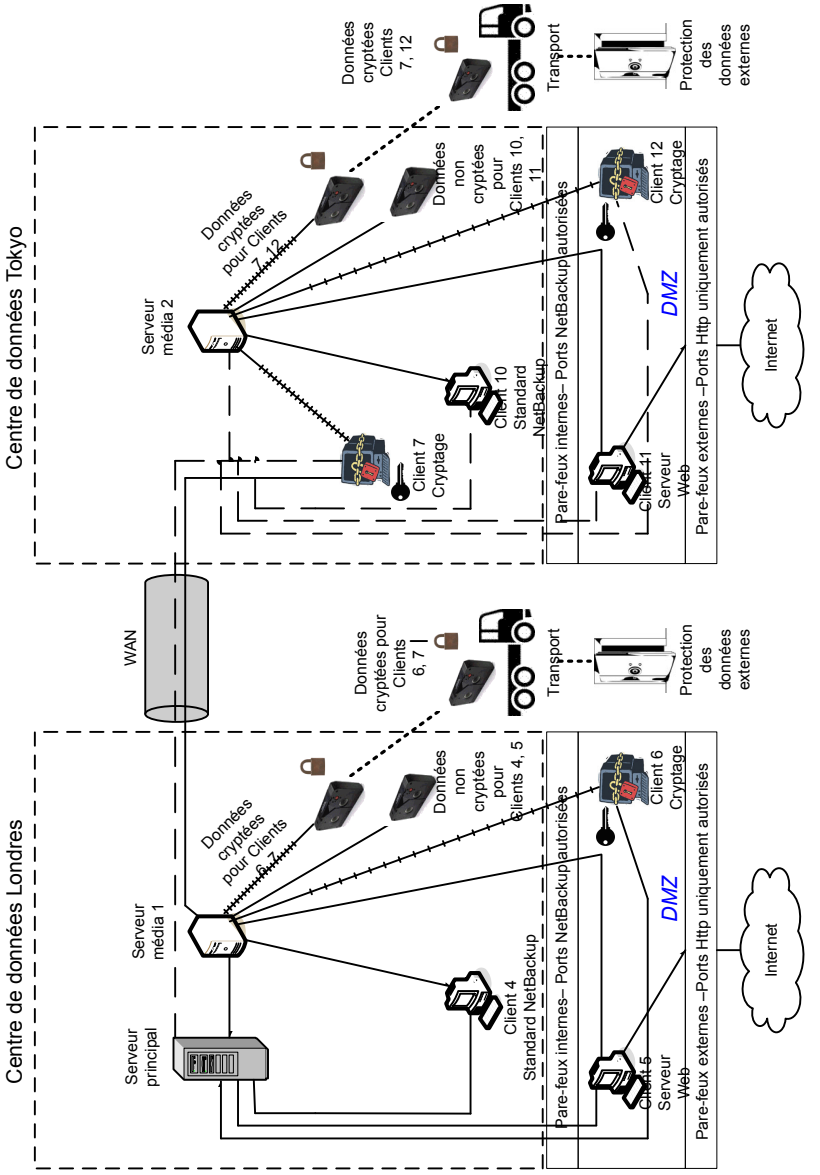
Le centre de données unique avec le chiffrement côté client inclut :

- NetBackup couvre deux régions géographiques ou plus par le biais d'un réseau étendu (WAN)
- Utile pour protéger les données hors site
- Les données du client sont chiffrées pour empêcher l'interception passive des données transmises par le câble
- La gestion des clés est décentralisée vers les clients
- L'option de chiffrement NetBackup initiale
- Le processeur du client est utilisé pour exécuter le chiffrement

- Vous devez disposer de la clé pour récupérer les données. Une clé perdue est synonyme de perte de données.
- Utile quand vous devez analyser des bandes hors site ou si vous avez besoin de confidentialité sur le câble.

Figure 3-7 présente un exemple de centre de données multiple avec chiffrement côté client.

Figure 3-7 Data center multiple avec chiffrement côté client



Le tableau suivant décrit les composants de NetBackup qui sont utilisés pour un data center multiple avec chiffrement côté client.

Tableau 3-7 Composants de NetBackup pour un data center multiple avec le chiffrement côté client mis en application

Composant	Description
Centre de données de Londres	Le centre de données de Londres contient le serveur maître, le serveur de médias 1 et les clients 4, 5 et 6. Il contient également la bande de données chiffrées pour les clients 6 et 7 et la bande de données déchiffrée pour les clients 4 et 5. Le centre de données de Londres se connecte au centre de données de Tokyo par une connexion WAN dédiée.
Centre de données de Tokyo	Le centre de données de Tokyo contient le serveur de médias 2 et les clients 7, 10, 11 et 12. Il contient également la bande de données chiffrées pour les clients 7 et 12 et la bande de données déchiffrée pour les clients 10 et 11. Le centre de données de Tokyo se connecte au centre de données de Londres par une connexion WAN dédiée.
Réseau étendu (WAN)	Spécifie le lien WAN dédié qui connecte le centre de données de Londres au centre de données de Tokyo. Le WAN fournit la connectivité entre le serveur maître de Londres et le serveur maître 2 avec les clients 7, 10, 11 et 12 à Tokyo. Le WAN fournit également la connectivité entre le serveur de médias 1 à Londres et le client 7 à Londres.
Serveur maître	Le serveur maître se trouve dans le centre de données de Londres et communique avec le serveur de médias 1 et les clients 4, 5 et 6. Le serveur maître utilise également le WAN pour communiquer avec le serveur de médias 2 et les clients 7, 10, 11 et 12 à Tokyo.
Serveurs de médias	Précise que ce centre de données multiple utilise deux serveurs de médias. Le serveur de médias 1 est situé dans le centre de données de Londres et le serveur de médias 2 est situé dans le centre de données de Tokyo. A Londres, le serveur de médias 1 communique avec le serveur maître et les clients 4, 5 et 6. Le serveur de médias 1 communique également avec le client 7 à Tokyo. Le serveur de médias 1 enregistre des données non chiffrées sur bande pour les clients 4 et 5. Le serveur de médias 1 enregistre des données chiffrées sur bande pour les clients 6 et 7. Notez que le client 7 se trouve à Tokyo mais sa sauvegarde sur bande se trouve à Londres. La bande chiffrée pour les clients 6 et 7 est transportée hors site vers un centre de sauvegarde à Londres. A Tokyo, le serveur de médias 2 communique avec le serveur maître à Londres par le WAN et les clients 7, 10, 11 et 12 à Tokyo. Le serveur de médias 2 enregistre des données non chiffrées sur bande pour les clients 10 et 11. Le serveur de médias 2 enregistre également des données chiffrées sur bande pour les clients 7 and 12. Notez que même si le client 7 se trouve à Tokyo et soit sauvegardé à Londres, le client 7 est également sauvegardé à Tokyo. La bande chiffrée pour les clients 7 et 12 est transportée hors site vers un centre de sauvegarde à Tokyo.
Chiffrement côté client	Le chiffrement côté client (non affiché dans le schéma) assure la confidentialité des données sur l'ensemble de la connexion, ainsi que sur les bandes.

Composant	Description
Bandes	Des bandes de données déchiffrées et chiffrées sont produites au centre de données de Londres et au centre de données de Tokyo. La bande chiffrée contient les données de sauvegarde chiffrées côté client. A Londres, la bande déchiffrée est écrite pour les clients 4 et 5 et stockées sur site dans le centre de données de Londres. La bande chiffrée est enregistrée pour les clients 6 et 7. La bande chiffrée est transportée hors site vers un centre de sauvegarde à Londres pour la protection de reprise après incident. A Tokyo, la bande chiffrée est écrite pour les clients 10 et 11 et est stockée hors site dans le centre de données de Tokyo. La bande chiffrée est enregistrée pour les clients 7 et 12. Notez que même si le client 7 se trouve à Tokyo et qu'il est sauvegardé à Tokyo, le client 7 est également sauvegardé à Londres. La bande chiffrée est transportée hors site vers un centre de sauvegarde à Tokyo pour la protection de reprise après incident. **Remarque :** Pour déchiffrer les données, les clés utilisées pour le chiffrement de données doivent être disponibles.
Transports	Précise que le centre de données multiple utilise deux transports. Un transport se trouve à Londres et l'autre à Tokyo. A Londres, le camion de transport déplace la bande chiffrée des clients 6 et 7 hors site vers un centre de sauvegarde sécurisé hors site situé à Tokyo. A Tokyo, le camion de transport déplace la bande chiffrée des clients 7 et 12 hors site vers un centre de sauvegarde sécurisé hors site situé à Tokyo. Une copie de sauvegarde du client n° 7 se trouve à la fois dans le centre de sauvegarde de Londres et de Tokyo. **Remarque :** Dans le cas peu probable d'une perte de bande pendant le transport, le gestionnaire du centre de données a potentiellement réduit le risque de violation des données. L'infraction est réduite par l'utiliser du chiffrement des données côté client.
Centres de sauvegarde hors site	Précise que le centre de données multiple utilise deux centres de sauvegarde hors site. Un centre de sauvegarde se trouve à Londres et l'autre à Tokyo. Les deux centres de sauvegarde fournissent des installations de stockage de bande chiffrés sécurisés hors site à des emplacements différents de ceux des centres de données. **Remarque :** Sauvegarder les bandes chiffrées dans des emplacements distincts des centres de données favorise une bonne protection lors de récupérations d'urgence.

Composant	Description
Clients	Spécifie que les clients se trouvent dans les centres de données de Londres et de Tokyo. A Londres, le client 4 est un type de NetBackup standard. Le client 5 est un type de serveur Web situé dans la zone démilitarisée. Le client 6 est un type de client chiffré côté client également situé dans la zone démilitarisée. Tous les types de client peuvent être gérés par le serveur maître et ont leurs données sauvegardées sur bande via le serveur maître 1. Les clients 5 et 6 communiquent au NetBackup en utilisant seulement des ports NetBackup par le pare-feu interne. Le client 6 reçoit des connexions Internet à l'aide des ports réservés au HTTP via le pare-feu externe. A Tokyo, le client 7 est un client chiffré côté client mais en dehors de la zone démilitarisée. Le client 10 est un type de NetBackup standard. Le client 11 est un type de serveur Web situé dans la zone démilitarisée. Le client 12 est un type de client chiffré côté client également situé dans la zone démilitarisée. Tous les types de client peuvent être gérés par le serveur maître à Londres. Les données du client 7 sont sauvegardées sur bande par le serveur de médias 1 et 2. Les clients 10, 11 et 12 sont sauvegardés sur bande par le serveur de médias 2. Les clients 11 et 12 communiquent à NetBackup en utilisant seulement les ports de NetBackup par le pare-feu interne. Le client 12 reçoit des connexions Internet à l'aide des ports réservés au HTTP via le pare-feu externe.
Pare-feux internes	Spécifie que le centre de données multiple peut utiliser les deux pare-feux internes. Un pare-feu interne se trouve à Londres et l'autre à Tokyo. A Londres, le pare-feu interne permet à NetBackup d'accéder au serveur Web 5 et au client chiffré 6 côté client se trouvant dans la zone démilitarisée. A Tokyo, le pare-feu interne permet à NetBackup d'accéder au serveur Web 11 et au client chiffré 11 côté client dans la zone démilitarisée. Vous ne pouvez activer que les ports NetBackup sélectionnés et les ports de certaines applications pour transmettre des données depuis et vers la zone démilitarisée. Des ports HTTP sont ouverts dans le pare-feu externe et ne sont pas autorisés à passer par le pare-feu interne.
Zones démilitarisées (DMZ)	Précise que le centre de données multiple utilise deux zones démilitarisées. Une zone démilitarisée se trouve à Londres et l'autre à Tokyo. A Londres, la zone démilitarisée fournit une zone d'action "sécurisée" pour le serveur Web 5 et le client chiffré 6 côté client. Ce client existe entre le pare-feu interne et externe. Le client 5 de serveur Web et le client chiffré côté client 6 dans la zone démilitarisée peuvent communiquer vers NetBackup. Les deux clients communiquent par le pare-feu interne à l'aide des ports de NetBackup désignés. Le client 5 de serveur Web peut également communiquer sur Internet par le biais du pare-feu externe en utilisant uniquement des ports HTTP. A Tokyo, la zone démilitarisée fournit une zone d'opérations "sécurisée" pour le serveur Web 11 et le client chiffré 12 côté client. Le client 12 existe entre le pare-feu interne et externe. Le client 11 de serveur Web de la zone démilitarisée peut échanger des données avec NetBackup via le pare-feu interne à l'aide des ports NetBackup affectés. Le client 11 de serveur Web peut également communiquer sur Internet par le biais du pare-feu externe en utilisant uniquement des ports HTTP.

Composant	Description
Pare-feux externes	Spécifie que le centre de données multiple peut utiliser les deux pare-feux externes. Un pare-feu externe se trouve à Londres et l'autre à Tokyo. A Londres, le pare-feu externe permet aux utilisateurs externes d'accéder au client 5 de serveur Web situé dans la zone démilitarisée depuis Internet en passant par des ports HTTPS. Les ports NetBackup sont ouverts afin que le client 5 de serveur Web puisse communiquer avec NetBackup à travers le pare-feu interne. Les ports NetBackup ne peuvent pas passer par le pare-feu externe pour se connecter à Internet. Seuls les ports HTTP du client 5 de serveur Web peuvent passer par le pare-feu externe pour se connecter à Internet. Vous ne pouvez pas accéder au client 6 chiffré côté client depuis Internet. A Tokyo le pare-feu externe permet aux utilisateurs externes d'accéder au client 11 de serveur Web situé dans la zone démilitarisée depuis Internet en passant par des ports HTTPS. Les ports NetBackup sont ouverts pour que le client 11 de serveur Web puisse communiquer via le pare-feu interne avec NetBackup. Les ports NetBackup ne peuvent pas passer par le pare-feu externe pour se connecter à Internet. Seuls les ports HTTP du client 11 de serveur Web peuvent passer par le pare-feu externe pour se connecter à Internet. Vous ne pouvez pas accéder au client 12 chiffré côté client depuis Internet.
Internet	Spécifie qu'il existe un seul Internet mais deux connexions Internet dans cet exemple de centre de données multiple. Une connexion Internet se trouve à Londres et l'autre à Tokyo. Internet est un ensemble de réseaux d'ordinateurs connectés entre eux par des câbles de cuivre, des câbles de fibre optique ou par des connexions sans fil. A Londres, le client 5 de serveur Web peut envoyer et recevoir des données sur Internet à l'aide des ports HTTP et en passant par le pare-feu externe. A Tokyo, le client 11 de serveur Web peut envoyer et recevoir des données sur Internet à l'aide des ports HTTP et en passant par le pare-feu externe.

Data center multiple avec NetBackup Access Control sur les serveurs maîtres et de médias

Un exemple de data center multiple avec NBAC sur le serveur maître et le serveur de médias est défini comme un support pour un grand groupe d'hôtes (plus de 50). Ces hôtes peuvent couvrir deux ou plusieurs régions géographiques et être connectés à un réseau étendu (WAN). Dans l'exemple suivant, un data center se trouve à Londres et l'autre se trouve à Tokyo. Les deux data centers sont connectés par une connexion WAN dédiée.

Cet exemple de data center utilise NetBackup Access Control sur les serveurs maîtres et les serveurs de médias. Le data center limite l'accès à certaines parties de NetBackup et peut utiliser l'administration non racine de NetBackup. Dans cet environnement, NBAC est configuré pour être utilisé entre les serveurs et les interfaces graphiques utilisateur. Les utilisateurs autres que racine peuvent se connecter à NetBackup en utilisant le système d'exploitation (mot de passe UNIX

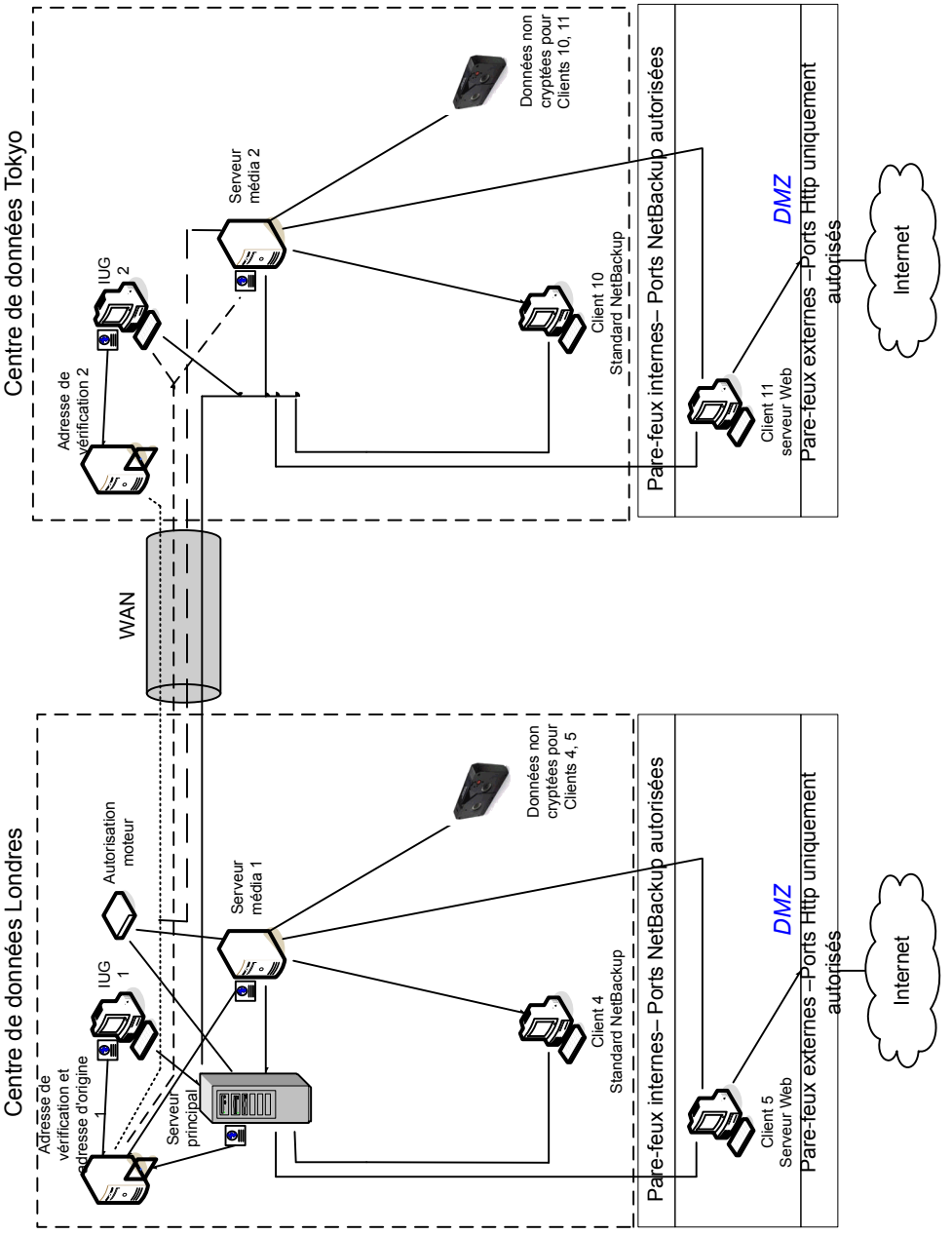
ou domaine local Windows). Il est également possible d'utiliser des référentiels d'utilisateur globaux (NIS/NIS+ ou Active Directory) pour gérer NetBackup. En outre, NBAC peut être utilisé pour limiter le niveau d'accès à NetBackup de certains utilisateurs. Par exemple, vous pouvez isoler le contrôle opérationnel quotidien de la configuration de l'environnement (ajout de nouvelles politiques, robots, par exemple).

Le data center multiple avec NBAC sur les serveurs maîtres et de médias inclut les éléments suivants :

- NetBackup couvre deux régions géographiques ou plus par le biais d'un réseau étendu (WAN)
- Gérer comme utilisateurs autres que racine.
- Gérer UNIX avec un ID d'utilisateur Windows.
- Gérer Windows avec un compte UNIX.
- Isoler et limiter les actions d'utilisateurs spécifiques.
- La racine ou l'administrateur ou les hôtes client peuvent encore faire des sauvegardes et des restaurations du client local
- Peut être combiné avec d'autres options de sécurité
- Tous les serveurs doivent correspondre à la version NetBackup 7.7. ou ultérieure.

Figure 3-8 affiche un exemple de data center multiples avec NBAC sur les serveurs maîtres et les serveurs de médias.

Figure 3-8 Data center multiple avec NBAC sur les serveurs maître et les serveurs de médias



Le tableau suivant décrit les composants de NetBackup qui sont utilisés pour un data center multiple avec NBAC sur les serveurs maîtres et de médias.

Tableau 3-8 Composants de NetBackup utilisés pour un data center multiple avec NBAC sur les serveurs maître et de médias

Composant	Description
Data center de Londres	Le data center de Londres contient le courtier racine, le courtier d'authentification 1, l'interface graphique utilisateur 1, le moteur d'autorisation, le serveur maître, le serveur de médias 1 et les clients 4 et 5. Le data center de Londres contient également la bande de données déchiffrée pour les clients 4 et 5. Le data center de Londres se connecte au data center de Tokyo par une connexion WAN dédiée.
Data center de Tokyo	Le data center de Tokyo contient le courtier d'authentification 2, l'interface graphique utilisateur 2, le serveur de médias 2 et les clients 10 et 11. Le data center de Tokyo contient également la bande de données déchiffrée pour les clients 10 et 11. Le data center de Tokyo se connecte au data center de Londres par une connexion WAN dédiée.
Réseau étendu (WAN)	Spécifie le lien WAN dédié qui connecte le data center de Londres au data center de Tokyo. Le WAN fournit la connectivité entre le courtier racine et le courtier d'authentification 1 et le courtier d'authentification 2. De plus, le WAN fournit la connectivité entre le courtier racine et le courtier d'authentification 1 et l'interface graphique utilisateur 2 avec le serveur de médias 2. Le WAN connecte également le moteur d'autorisation au serveur de médias 2. Enfin, le WAN connecte le serveur maître avec l'interface graphique utilisateur 2, le serveur de médias 2 et les clients 10 et 11.
Serveur maître	Le serveur maître, situé dans le data center de Londres, communique avec le courtier racine et le courtier d'authentification 1. Il communique également avec l'interface graphique utilisateur 1, le moteur d'autorisation et le serveur de médias 1. Le serveur maître communique avec les clients 4 et 5 à Londres. Le serveur maître communique également avec l'interface graphique utilisateur 2, le serveur de médias 2 et les clients 10 et 11 à Tokyo.
Serveurs de médias	Précise que dans cet exemple de data center multiple, il existe deux serveurs de médias. Le serveur de médias 1 est situé dans le data center de Londres et le serveur de médias 2 est situé dans le data center de Tokyo. A Londres, le serveur de médias 1 communique avec le serveur maître, le courtier racine et le courtier d'authentification 1, le moteur d'autorisation et les clients 4 et 5. Le serveur de médias 1 enregistre des données non chiffrées sur bande pour les clients 4 et 5. A Tokyo, le serveur de médias 2 communique avec le serveur maître et le moteur d'autorisation à Londres par le WAN. Le serveur de médias 2 communique également avec l'interface graphique utilisateur 2 et les clients 10 et 11 à Tokyo. Le serveur de médias n° 2 enregistre des données non chiffrées sur bande pour les clients n° 10 et n° 11.

Composant	Description
Interfaces graphiques utilisateur	Précise que dans cet exemple de data center multiple, il existe deux interfaces graphiques utilisateur. L'interface graphique utilisateur 1 se trouve à Londres et l'interface graphique utilisateur 2 se trouve à Tokyo. Les interfaces graphiques utilisateur des consoles d'administration à distance reçoivent les informations d'authentification des courtiers. Les interfaces graphiques utilisateur utilisent ces informations d'authentification pour accéder aux fonctions des serveurs de médias et serveurs maîtres. A Londres, l'interface graphique utilisateur 1 reçoit des informations d'authentification du courtier d'authentification 1.L'interface graphique utilisateur 1 a accès aux fonctionnalités du serveur maître et des serveurs de médias 1 et 2. A Tokyo, l'interface graphique utilisateur 2 reçoit des informations d'authentification du courtier d'authentification 2. L'interface graphique utilisateur 2 a accès aux fonctionnalités du serveur maître et des serveurs de médias 1 et 2.
Courtier racine	Précise que dans une installation de data center multiple, un seul courtier racine est requis. Le courtier racine peut parfois être associé au courtier d'authentification. Dans l'exemple suivant, le courtier racine et le courtier d'authentification sont affichés comme même composant et se trouvent dans le data center de Londres. A Londres, le courtier racine authentifie le courtier d'authentification 1 également situé à Londres et le courtier d'authentification 2 à Tokyo. Le courtier racine n'authentifie pas les clients.
Courtiers d'authentification	Spécifie qu'il peut y avoir plus d'un courtier d'authentification dans une installation de data center multiple. Le courtier d'authentification peut parfois être associé au courtier racine. Dans l'installation de ce data center, deux courtiers d'authentification sont utilisés. Le courtier d'authentification authentifie le serveur maître, le serveur de médias et l'interface graphique utilisateur en établissant des informations d'authentification pour chacun d'entre eux. Le courtier d'authentification authentifie également un utilisateur avec une invite de commande. A Londres, le courtier d'authentification 1 authentifie des informations d'authentification avec le serveur maître, le serveur de médias 1 et l'interface graphique utilisateur 1. Les serveurs NetBackup et les clients à Tokyo et à Londres authentifient le courtier d'authentification 1 à Londres. L'interface graphique utilisateur 1 authentifie le courtier d'authentification 1 à Londres. L'interface graphique utilisateur 2 authentifie le courtier d'authentification 2 à Tokyo.
Moteur d'autorisation	Précise que dans une installation de data center multiple, un seul moteur d'autorisation est requis. Le moteur d'autorisation communique avec le serveur maître et le serveur de médias pour vérifier les autorisations d'un utilisateur authentifié. Ces autorisations déterminent les fonctionnalités disponibles pour l'utilisateur. Le moteur d'autorisation enregistre également les groupes d'utilisateurs et les autorisations. Le moteur d'autorisation réside à Londres et communique avec le serveur maître et le serveur de médias 1. Le moteur d'autorisation communique également via le réseau étendu WAN pour autoriser l'accès au serveur de médias 2 à Tokyo. **Remarque :** Le moteur d'autorisation se trouve sur le serveur maître en tant que processus de daemon. Il est affiché dans le schéma en tant qu'image distincte à titre d'exemple uniquement.

Composant	Description
Bandes	Des bandes de données déchiffrées sont produites au data center de Londres et au data center de Tokyo. A Londres, la bande déchiffrée est écrite pour les clients 4 et 5 et stockées sur site dans le data center de Londres. A Tokyo, la bande chiffrée est écrite pour les clients 10 et 11 et est stockée hors site dans le data center de Tokyo.
Clients	Spécifie que les clients se trouvent dans les data centers de Londres et de Tokyo. A Londres, le client 4 est un type de NetBackup standard. Le client 5 est un type de serveur Web situé dans la zone démilitarisée. Tous les types de client peuvent être gérés par le serveur maître et faire sauvegarder leurs données sur bande par le client 5 du serveur de médias 1. Le client 5 communique avec NetBackup à l'aide des ports NetBackup uniquement via le pare-feu interne. Le client 5 reçoit également des connexions Internet en utilisant seulement des ports réservés au HTTP via le pare-feu externe. A Tokyo, le client 10 est un type de NetBackup standard. Le client 11 est un type de serveur Web situé dans la zone démilitarisée. Tous les types de client peuvent être gérés par le serveur maître et faire sauvegarder leurs données sur bande par le client 11 du serveur de médias 2. Le client 5 communique avec NetBackup à l'aide des ports NetBackup uniquement via le pare-feu interne. Le client 11 reçoit également des connexions Internet en utilisant des ports réservés au HTTP via le pare-feu externe
Pare-feux internes	Précise que dans cet exemple de data center multiple, il existe deux pare-feux internes. Un pare-feu interne se trouve à Londres et l'autre à Tokyo. A Londres, le pare-feu interne permet à NetBackup d'accéder au client 5 de serveur Web se trouvant dans la zone démilitarisée. A Londres, le pare-feu interne permet à NetBackup d'accéder au client 11 de serveur Web se trouvant dans la zone démilitarisée. Vous ne pouvez activer que les ports NetBackup sélectionnés et les ports de certaines applications pour transmettre des données par le biais du pare-feu interne depuis et vers la zone démilitarisée. Des ports HTTP sont ouverts dans le pare-feu externe et ne sont pas autorisés à passer par le pare-feu interne.
Zones démilitarisées (DMZ)	Précise que dans cet exemple de data center multiple, il existe deux zones démilitarisées. Une zone démilitarisée se trouve à Londres et l'autre à Tokyo. A Londres, la zone démilitarisée fournit une zone d'opérations "sécurisée" pour le client 5 de serveur Web entre le pare-feu interne et le pare-feu externe. Le client 5 de serveur Web et le client chiffré 6 côté client de la zone démilitarisée peuvent communiquer avec NetBackup via le pare-feu interne en utilisant les ports NetBackup affectés. Le client 5 de serveur Web peut également communiquer sur Internet par le biais du pare-feu externe en utilisant uniquement des ports HTTP. A Tokyo, la zone démilitarisée fournit une zone d'opérations "sécurisée" pour le client 11 de serveur Web entre le pare-feu interne et le pare-feu externe. Le client 11 de serveur Web de la zone démilitarisée peut échanger des données avec NetBackup via le pare-feu interne à l'aide des ports NetBackup affectés. Le client 11 de serveur Web peut également communiquer sur Internet par le biais du pare-feu externe en utilisant uniquement des ports HTTP.

Composant	Description
Pare-feux externes	Précise que dans cet exemple de data center multiple, il existe deux pare-feux externes. Un pare-feu externe se trouve à Londres et l'autre à Tokyo. A Londres, le pare-feu externe permet aux utilisateurs externes d'accéder au client 5 de serveur Web situé dans la zone démilitarisée depuis Internet en passant par des ports HTTP. Les ports NetBackup sont ouverts pour que le client 5 de serveur Web puisse communiquer via le pare-feu interne avec NetBackup. Les ports NetBackup ne peuvent pas passer par le pare-feu externe pour se connecter à Internet. Seuls les ports HTTP du client 5 de serveur Web peuvent passer par le pare-feu externe pour se connecter à Internet. A Tokyo le pare-feu externe permet aux utilisateurs externes d'accéder au client 11 de serveur Web situé dans la zone démilitarisée depuis Internet en passant par des ports HTTPS. Les ports NetBackup sont ouverts pour que le client 11 de serveur Web puisse communiquer via le pare-feu interne avec NetBackup. Les ports NetBackup ne peuvent pas passer par le pare-feu externe pour se connecter à Internet. Seuls les ports HTTP du client 11 de serveur Web peuvent passer par le pare-feu externe pour se connecter à Internet.
Internet	Spécifie qu'il existe un seul Internet mais deux connexions Internet dans cet exemple de data center multiple. Une connexion Internet se trouve à Londres et l'autre à Tokyo. Internet est un ensemble de réseaux d'ordinateurs connectés entre eux par des câbles de cuivre, des câbles de fibre optique ou par des connexions sans fil. A Londres, le client 5 de serveur Web peut envoyer et recevoir des données sur Internet à l'aide des ports HTTP et en passant par le pare-feu externe. A Tokyo, le client 11 de serveur Web peut envoyer et recevoir des données sur Internet à l'aide des ports HTTP et en passant par le pare-feu externe.

Data center multiple avec NBAC complet

L'exemple d'un data center multiple avec NBAC complet est défini comme un support ppur un grand groupe d'hôtes (plus de 50) qui couvre deux régions géographiques ou plus et peuvent être connectées par un réseau étendu (WAN). Dans cet exemple, un data center est à Londres et l'autre data center est à Tokyo. Les deux data centers sont connectés par une connexion WAN dédiée.

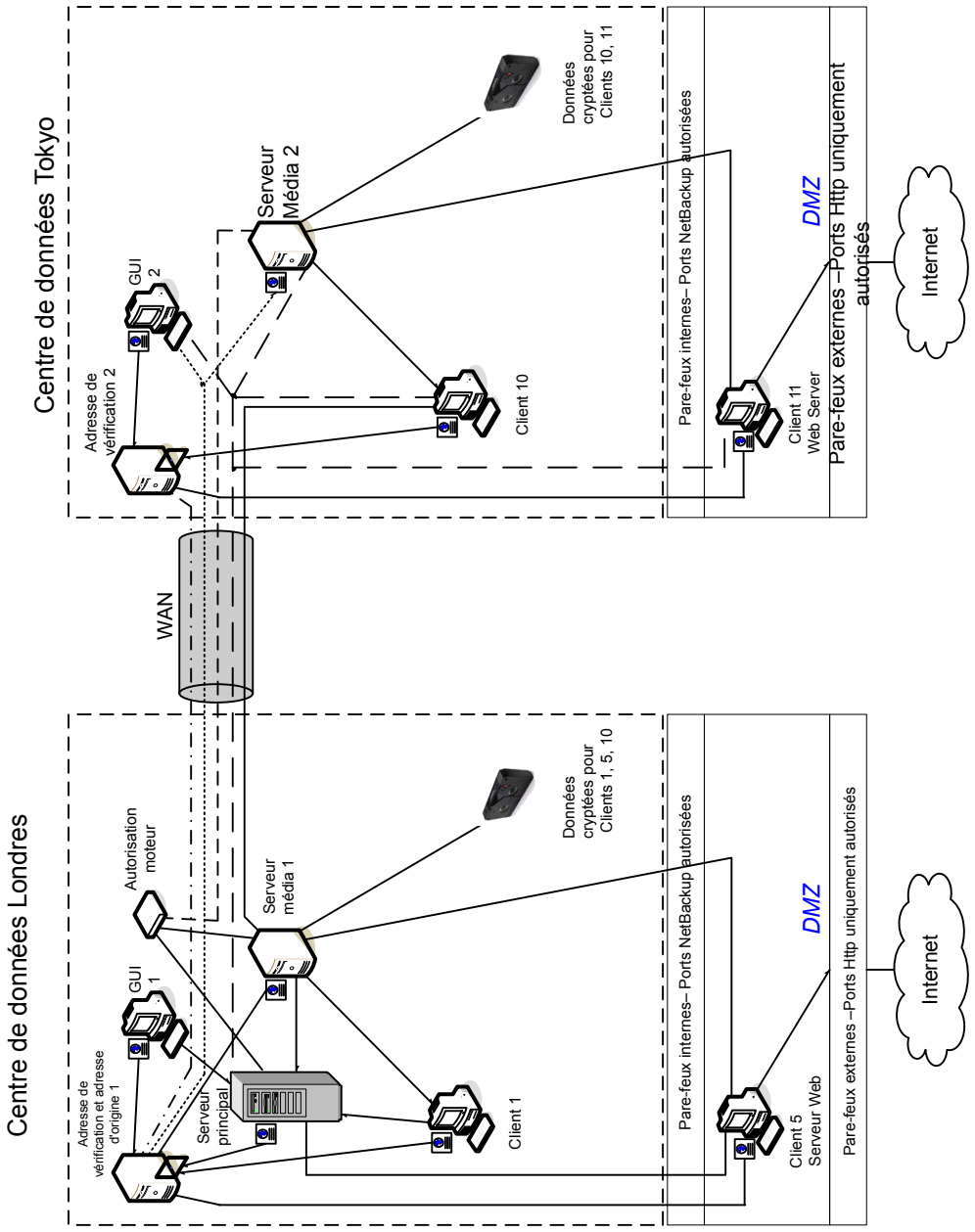
Cet environnement est très semblable au data center multiple avec le serveur maître et le serveur de médias de NBAC. Les principales différences sont que tous les hôtes participant à l'environnement de NetBackup sont identifiés de manière fiable avec les informations d'authentification et des administrateurs non racine peuvent gérer les clients NetBackup en fonction des niveaux d'accès configurables. Les identités des utilisateurs peuvent se trouver dans des référentiels globaux tels que l'annuaire Active Directory sous Windows ou NIS sous UNIX. Les identités peuvent également se trouver dans des référentiels en local (mot de passe UNIX, domaine Windows local) sur ces hôtes prenant en charge un courtier d'authentification.

Le data center multiple avec NBAC complet inclut ce qui suit :

- NetBackup couvre deux régions géographiques ou plus par le biais d'un réseau étendu (WAN)
- Semblable aux détails pour le data center multiple avec le serveur maître et le serveur de médias de NBAC, excepté la racine ou l'administrateur sur le client L'administration non racine des clients et des serveurs est permise dans cette configuration.
- Pour les systèmes client, vous pouvez configurer les utilisateurs qui ne sont ni utilisateur racine, ni administrateur pour qu'ils puissent effectuer des sauvegardes et restaurations locales (configuration par défaut)
- L'environnement facilite la connexion de tous les hôtes autorisés faisant partie de NetBackup
- Exige que tous les hôtes utilisent NetBackup version 7.7. ou ultérieure.

Figure 3-9 affiche un exemple d'un data center multiple avec NBAC complet.

Figure 3-9 Data center multiple avec NBAC complet



Le tableau suivant décrit les composants de NetBackup qui sont utilisés pour un data center multiple avec NBAC complet mis en application.

Tableau 3-9 Composants de NetBackup utilisés pour un data center multiple avec NBAC complet mis en application

Composant	Description
Data center de Londres	Le data center de Londres contient le courtier racine, le courtier d'authentification 1, l'interface graphique utilisateur 1, le moteur d'autorisation, le serveur maître, le serveur de médias 1 et les clients 1 et 5. Le data center de Londres contient également la bande de données déchiffrée pour les clients 1, 5 et 10. Le data center de Londres se connecte au data center de Tokyo par une connexion WAN dédiée.
Data center de Tokyo	Le data center de Tokyo contient le courtier d'authentification 2, l'interface graphique utilisateur 2, le serveur de médias 2 et les clients 10 et 11. Le data center de Tokyo contient également la bande de données déchiffrée pour les clients 10 et 11. Le data center de Tokyo se connecte au data center de Londres par une connexion WAN dédiée.
Réseau étendu (WAN)	Spécifie le lien WAN dédié qui connecte le data center de Londres au data center de Tokyo. Le WAN fournit la connectivité entre le courtier racine et le courtier d'authentification 1 et le courtier d'authentification 2. De plus, le WAN fournit la connectivité entre le courtier racine et le courtier d'authentification 1 et l'interface graphique utilisateur 2 avec le serveur de médias 2. Le WAN connecte le serveur maître à l'interface graphique utilisateur 2, le serveur de médias 2 et les clients 10 et 11. Enfin, le WAN connecte le serveur de médias 1 au client 10.
Serveur maître	Le serveur maître, situé dans le data center de Londres, communique avec le courtier racine et le courtier d'authentification 1. Il communique également avec l'interface graphique utilisateur 1, le moteur d'autorisation et le serveur de médias 1. Le serveur maître communique aussi avec l'interface graphique utilisateur 2 et le serveur de médias 2 et les clients 10 et 11 à Tokyo.
Serveurs de médias	Précise que dans cet exemple de data center multiple, il existe deux serveurs de médias. Le serveur de médias 1 est situé dans le data center de Londres et le serveur de médias 2 est situé dans le data center de Tokyo. A Londres, le serveur de médias 1 communique avec le serveur maître, le courtier racine et le courtier d'authentification 1, le moteur d'autorisation et les clients 1, 5 et 10. Le serveur de médias 1 enregistre des données non chiffrées sur bande pour les clients 1, 5 et 10. A Tokyo, le serveur de médias n° 2 échange des données avec le serveur maître, le courtier racine, le courtier d'authentification n° 1 et le moteur d'autorisation à Londres par le biais du réseau étendu. Le serveur de médias 2 communique également avec l'interface graphique utilisateur 2 et les clients 10 et 11 à Tokyo. Le serveur de médias n° 2 enregistre des données non chiffrées sur bande pour les clients n° 10 et n° 11.

Composant	Description
Interfaces graphiques utilisateur	Précise que dans cet exemple de data center multiple, il existe deux interfaces graphiques utilisateur. L'interface graphique utilisateur 1 se trouve à Londres et l'interface graphique utilisateur 2 se trouve à Tokyo. Les interfaces graphiques utilisateur des consoles d'administration à distance reçoivent les informations d'authentification des courtiers. Les interfaces graphiques utilisateur utilisent ces informations d'authentification pour accéder aux fonctions des serveurs de médias et serveurs maîtres. A Londres, l'interface graphique utilisateur 1 reçoit des informations d'authentification du courtier d'authentification 1.L'interface graphique utilisateur 1 a accès aux fonctionnalités du serveur maître et des serveurs de médias 1 et 2. A Tokyo, l'interface graphique utilisateur 2 reçoit des informations d'authentification du courtier d'authentification 2. L'interface graphique utilisateur 2 a accès aux fonctionnalités du serveur maître et des serveurs de médias 1 et 2.
Courtier racine	Précise que dans une installation de data center multiple, un seul courtier racine est requis. Le courtier racine peut parfois être associé au courtier d'authentification. Dans l'exemple suivant, le courtier racine et le courtier d'authentification sont affichés comme même composant et se trouvent dans le data center de Londres. A Londres, le courtier d'authentifcation authentifie le courtier d'authentification 1, également à Londres, et le courtier d'authentification 2 à Tokyo. Le courtier racine n'authentifie pas les clients.
Courtiers d'authentification	Spécifie qu'il peut y avoir plus d'un courtier d'authentification dans une installation de data center. Le courtier d'authentification peut parfois être associé au courtier racine. Dans l'installation de ce data center, deux courtiers d'authentification sont utilisés. Le courtier d'authentification authentifie le serveur maître, le serveur de médias, l'interface graphique utilisateur et les clients en établissant des informations d'authentification pour chacun d'entre eux. Le courtier d'authentification authentifie également un utilisateur via une invite de commande. A Londres, le courtier d'authentification 1 authentifie des informations d'authentification avec le serveur maître, le serveur de médias 1, l'interface graphique utilisateur 1 et les clients 1 et 5. Tous les serveurs et clients NetBackup à Tokyo et à Londres s'authentifient auprès du courtier d'authentification 1 à Londres. L'interface graphique utilisateur 1 authentifie le courtier d'authentification 1 à Londres. L'interface graphique utilisateur 2 authentifie le courtier d'authentification 2 à Tokyo.
Moteur d'autorisation	Un seul moteur d'autorisation est requis dans une installation de data center. Le moteur d'autorisation communique avec le serveur maître et le serveur de médias pour vérifier les autorisations d'un utilisateur authentifié. Ces autorisations déterminent les fonctionnalités disponibles pour l'utilisateur. Le moteur d'autorisation enregistre également les groupes d'utilisateurs et les autorisations. Le moteur d'autorisation réside à Londres et communique avec le serveur maître et le serveur de médias 1. Le moteur d'autorisation communique également via le réseau étendu WAN pour autoriser l'accès au serveur de médias 2 à Tokyo. **Remarque :** Le moteur d'autorisation se trouve sur le serveur maître en tant que processus de daemon. Il est affiché dans le schéma en tant qu'image distincte à titre d'exemple uniquement.

Composant	Description
Bandes	Spécifie que les bandes de données déchiffrées sont produites dans les data centers de Londres et de Tokyo. A Londres, la bande déchiffrée est enregistrée pour les clients 1, 5 et 10 et stockée sur site dans le data center de Londres. A Tokyo, la bande chiffrée est écrite pour les clients 10 et 11 et est stockée hors site dans le data center de Tokyo. Notez que même si le client 10 se trouve à Tokyo et qu'il sauvegardé à Tokyo, le client 10 est également sauvegardé à Londres.
Clients	Spécifie que les clients se trouvent dans les data centers de Londres et de Tokyo. A Londres, le client 1 est un type de NetBackup standard. Le client 5 est un type de serveur Web situé dans la zone démilitarisée. Tous les types de client peuvent être gérés par le serveur maître et faire sauvegarder leurs données sur bande par le client 5 du serveur de médias 1. Le client 5 communique avec NetBackup à l'aide des ports NetBackup uniquement via le pare-feu interne. Le client 5 reçoit également des connexions Internet en utilisant seulement des ports réservés au HTTP via le pare-feu externe. A Tokyo, le client 10 est un type de NetBackup standard. Le client 11 est un type de serveur Web situé dans la zone démilitarisée. Tous les types de client peuvent être gérés par le serveur maître et faire sauvegarder leurs données sur bande par le client 11 du serveur de médias 2. Le client 5 communique avec NetBackup à l'aide des ports NetBackup uniquement via le pare-feu interne. Le client 11 reçoit également des connexions Internet en utilisant des ports réservés au HTTP via le pare-feu externe
Pare-feux internes	Spécifie qu'il peut y avoir deux pare-feux internes dans cet exemple de data center multiple. Un pare-feu interne se trouve à Londres et l'autre à Tokyo. A Londres, le pare-feu interne permet à NetBackup d'accéder au client 5 de serveur Web se trouvant dans la zone démilitarisée. A Londres, le pare-feu interne permet à NetBackup d'accéder au client 11 de serveur Web se trouvant dans la zone démilitarisée. Vous ne pouvez activer que les ports NetBackup sélectionnés et les ports de certaines applications pour transmettre des données par le biais du pare-feu interne depuis et vers la zone démilitarisée. Des ports HTTP sont ouverts dans le pare-feu externe et ne sont pas autorisés à passer par le pare-feu interne.

Composant	Description
Zones démilitarisées (DMZ)	Spécifie qu'il peut y avoir deux zones démilitarisées dans cet exemple de data center multiple. Une zone démilitarisée se trouve à Londres et l'autre à Tokyo. A Londres, la zone démilitarisée fournit une zone d'opérations "sécurisée" pour le client 5 de serveur Web entre le pare-feu interne et le pare-feu externe. Le client 5 de serveur Web de la zone démilitarisée peut échanger des données avec NetBackup via le pare-feu interne en utilisant les ports NetBackup affectés. Le client 5 de serveur Web peut également communiquer sur Internet par le biais du pare-feu externe en utilisant uniquement des ports HTTP. A Tokyo, la zone démilitarisée fournit une zone d'opérations "sécurisée" pour le client 11 de serveur Web entre le pare-feu interne et le pare-feu externe. Le client 11 de serveur Web de la zone démilitarisée peut échanger des données avec NetBackup via le pare-feu interne à l'aide des ports NetBackup affectés. Le client 11 de serveur Web peut également communiquer sur Internet par le biais du pare-feu externe en utilisant uniquement des ports HTTP.
Pare-feux externes	Spécifie qu'il peut y avoir deux pare-feux internes dans cet exemple de data center multiple. Un pare-feu externe se trouve à Londres et l'autre à Tokyo. A Londres, le pare-feu externe permet aux utilisateurs externes d'accéder au client 5 de serveur Web situé dans la zone démilitarisée depuis Internet en passant par des ports HTTP. Les ports NetBackup sont ouverts pour que le client 5 de serveur Web puisse communiquer via le pare-feu interne avec NetBackup. Les ports NetBackup ne peuvent pas passer par le pare-feu externe pour se connecter à Internet. Seuls les ports HTTP du client 5 de serveur Web peuvent passer par le pare-feu externe pour se connecter à Internet. A Tokyo le pare-feu externe permet aux utilisateurs externes d'accéder au client 11 de serveur Web situé dans la zone démilitarisée depuis Internet en passant par des ports HTTPS. Les ports NetBackup sont ouverts pour que le client 11 de serveur Web puisse communiquer via le pare-feu interne avec NetBackup. Les ports NetBackup ne peuvent pas passer par le pare-feu externe pour se connecter à Internet. Seuls les ports HTTP du client 11 de serveur Web peuvent passer par le pare-feu externe pour se connecter à Internet.
Internet	Spécifie qu'il ne peut y avoir qu'un seul Internet mais deux connexions Internet dans cet exemple de data center multiple. Une connexion Internet se trouve à Londres et l'autre à Tokyo. Internet est un ensemble de réseaux d'ordinateurs connectés entre eux par des câbles de cuivre, des câbles de fibre optique ou par des connexions sans fil. A Londres, le client 5 de serveur Web peut envoyer et recevoir des données sur Internet à l'aide des ports HTTP et en passant par le pare-feu externe. A Tokyo, le client 11 de serveur Web peut envoyer et recevoir des données sur Internet à l'aide des ports HTTP et en passant par le pare-feu externe.

Chapitre 4

Audit des opérations NetBackup

Ce chapitre traite des sujets suivants :

À propos de l'audit de NetBackup

L'audit est activé par défaut sur les nouvelles installations. L'audit de NetBackup peut être configuré directement sur un serveur maître NetBackup ou à l'aide d'OpsCenter. Pour plus de détails, consultez le *Guide de l'administrateur NetBackupOpsCenter*.

L'audit des opérations de NetBackup présente les avantages suivants :

- En exploitant les journaux d'audit, les utilisateurs peuvent obtenir une idée globale de l'administration en analysant les changements inattendus dans un environnement NetBackup.
- Conformité réglementaire.
  L'enregistrement est conforme aux directives telles que celles définies par le SOX (Sarbanes-Oxley Act).
- Méthode permettant aux clients d'appliquer les politiques internes de gestion des changements.
- Aide pour le support de NetBackup lors du processus de résolution des problèmes pour les clients.

NetBackup Audit Manager

Le gestionnaire d'audit NetBackup (`nbaudit`) s'exécute sur le serveur maître et les enregistrements d'audit sont mis à jour dans la base de données EMM (Enterprise Media Manager).

L'administrateur peut rechercher les informations suivantes :

- Quand une action s'est produite
- Actions ayant échoué dans certaines situations
- Les actions exécutées par un utilisateur spécifique
- Les actions qui ont été exécutées dans une zone de contenu spécifique
- Modifications de la configuration d'audit

Tenez compte des points suivants :

- L'enregistrement d'audit tronque toutes les entrées qui incluent plus de 4 096 caractères. (Par exemple, le nom de la politique.)
- L'enregistrement d'audit tronque les ID d'image de restauration de plus de 1 024 caractères.

Actions auditées par NetBackup

NetBackup enregistre les actions suivantes lancées par l'utilisateur.

Actions du moniteur d'activité	Annuler, interrompre, reprendre, redémarrer ou supprimer n'importe quel type de travail crée un enregistrement d'audit.
Alertes et notifications par e-mail	Si aucune alerte ou notification par e-mail ne peut être envoyée pour les paramètres de configuration NetBackup. Par exemple, la configuration du serveur SMTP et la liste des codes d'état exclus des alertes.

Anomalies	Quand un utilisateur signale une anomalie comme un faux positif, l'action est auditée et consignée pour cet utilisateur.
Actions sur les biens	La suppression d'un bien, tel qu'un serveur vCenter, lors du processus de nettoyage des biens est auditée et consignée. La création, la modification et la suppression d'un groupe de biens, ainsi que toute action effectuée sur un groupe de biens pour lequel un utilisateur ne dispose pas des autorisations nécessaires sont auditées et consignées.
Échec de l'autorisation	L'échec de l'autorisation est audité lorsque vous utilisez l'interface utilisateur web NetBackup, les API NetBackup ou l'audit amélioré. Se reporter à "À propos de l'audit amélioré" à la page 195.
Informations de catalogue	Ces informations sont les suivantes : ■ Vérification et expiration d'images. ■ Lisez les demandes envoyées pour les données d'utilisation frontale.
Gestion des certificats	Création, révocation, renouvellement et déploiement de certificats NetBackup et défaillances de certificats NetBackup spécifiques.
Échecs de vérification de certificat (CVF)	Tentatives de connexion ayant échoué impliquant des erreurs de handshake SSL, des certificats révoqués ou des échecs de validation de nom d'hôte. Pour les échecs de validation de certificat (CVF) qui impliquent des liaisons handshake SSL et des certificats révoqués, l'horodatage indique quand l'enregistrement d'audit est publié sur le serveur maître Un enregistrement d'audit de CVF est un groupe d'événements CVF sur une période de temps. Les détails de l'enregistrement indiquent les heures de début et de fin de la période ainsi que le nombre total de CVF qui se sont produits pendant cette période.
Pools de disques et actions de pools de volume	Ajout, suppression ou mise à jour de pools de disques ou de volumes.
Opérations de mise en suspens	Création, modification et suppression d'opérations de mise en suspens.
Base de données hôte	Opérations NetBackup liées à la base de données hôte.
Tentatives de connexion	Toute tentative de connexion ayant abouti ou échoué pour la console d'administration de NetBackup, l'interface utilisateur web de NetBackup ou les API NetBackup.
Actions Politiques	Ajout, suppression ou mise à jour d'attributs de politique, de clients, de planifications et de listes de sélection de sauvegarde.

Actions utilisateur de restauration et de navigation sur les images	Toutes les opérations de restauration et de navigation sur le contenu des images (`bplist`) qu'un utilisateur effectue sont auditées avec l'identité de l'utilisateur. Pour définir un intervalle pour ajouter périodiquement les enregistrements d'audit des opérations de recherche d'images (`bplist`) du cache à la base de données NetBackup, utilisez l'option de configuration `DATAACCESS_AUDIT_INTERVAL_HOURS`. La définition de cette option de configuration empêche l'augmentation exponentielle de la taille de la base de données NetBackup en raison des enregistrements d'audit `bplist`. Consultez le Guide de l'administrateur NetBackup, volume I. Pour ajouter tous les enregistrements d'audit `bplist` du cache à la base de données NetBackup, exécutez la commande suivante sur le serveur maître : `nbcertcmd -postAudit -dataAccess`
Configuration de la sécurité	Informations relatives aux modifications apportées aux paramètres de configuration de sécurité.
Démarrage d'un travail de restauration	NetBackup n'effectue pas d'audit quand d'autres types de travaux commencent. Par exemple, NetBackup n'effectue pas d'audit quand un travail de sauvegarde commence.
Démarrage et arrêt du gestionnaire d'audit NetBackup (`nbaudit`).	Le démarrage et l'arrêt du gestionnaire `nbaudit` font toujours l'objet d'un audit, même si l'audit est désactivé.
Actions de politique de cycle de vie du stockage	Les tentatives de création, de modification ou de suppression d'une politique de cycle de vie du stockage (SLP) sont auditées et consignées. Cependant, l'activation et l'interruption d'une SLP à l'aide de la commande `nbstlutil` ne sont pas auditées. Ces opérations ne sont auditées que lorsqu'elles sont lancées à partir d'une API ou de l'interface utilisateur graphique NetBackup.
Actions de serveurs de stockage	Ajout, suppression ou mise à jour de serveurs de stockage.
Actions d'unités de stockage	Ajouter, supprimer ou mettre à jour les unités de stockage. **Remarque :** Les actions liées aux politiques de cycle de vie du stockage ne sont pas auditées.
Gestion de jeton	Création, suppression et nettoyage de jetons et défaillances d'émission de jeton spécifiques.
Gestion des utilisateurs	Ajout et suppression d'utilisateurs d'audit amélioré dans le mode correspondant.

Action de l'utilisateur qui ne parvient pas à créer un enregistrement d'audit	Si l'audit est activé mais que l'utilisateur ne parvient pas à créer un enregistrement d'audit, l'échec du service d'audit est enregistré dans le journal `nbaudit`. Le code d'état 108 NetBackup est renvoyé (`Action succeeded but auditing failed`). La console d'administration NetBackup ne renvoie pas de code d'état de sortie 108 lorsque l'audit échoue.

Actions pour lesquelles NetBackup n'effectue pas d'audit

Les actions suivantes ne sont pas enregistrées et ne s'affichent pas dans le rapport d'audit :

Toute action qui a échoué.	NetBackup consigne les actions en échec dans les journaux d'erreurs NetBackup. Les actions qui ont échoué ne s'affichent pas dans les rapports d'audit parce qu'elles ne contribuent pas à modifier l'état du système NetBackup.
Effet d'un changement de configuration	Les résultats d'une modification apportée à la configuration de NetBackup ne sont pas contrôlés. Par exemple, la création d'une politique est enregistrée dans le rapport d'audit, mais les travaux qui résultent de cette création ne le sont pas.
L'état d'achèvement d'un travail de restauration lancé manuellement	Tandis que l'acte de lancer un travail de restauration est audité, l'état d'achèvement du travail ne l'est pas, ni celui de n'importe quel autre type de travail, qu'il soit lancé manuellement ou pas. L'état d'achèvement est affiché dans le moniteur d'activité.
Actions lancées en interne	NetBackup-des actions internes lancées ne sont pas auditées. Par exemple les actions comme la suppression planifiée d'images expirées, les sauvegardes planifiées ou le nettoyage périodique de base de données d'images ne sont pas enregistrées.
Opérations de restauration	Certaines opérations sont exécutées en plusieurs étapes. Par exemple, la création d'un serveur de stockage MSDP se déroule en plusieurs étapes. Chaque étape correctement exécutée est auditée. L'échec de l'une des étapes produit une restauration ou, autrement dit, les étapes correctement exécutées peuvent avoir besoin d'être annulées. L'enregistrement d'audit ne contient pas les détails des opérations de restauration.
Actions de propriétés d'hôte	Les modifications apportées à l'aide des commandes `bpsetconfig` ou `nbsetconfig`, ou la propriété équivalente dans les propriétés d'hôte, ne sont pas auditées. Les modifications apportées directement au fichier `bp.conf` ou au registre ne sont pas auditées.

Affichage des paramètres d'audit actuels

Pour afficher la configuration actuelle d'audit, exécutez la commande `nbemmcmd` sur un serveur maître NetBackup ou affichez les paramètres à l'aide d'OpsCenter.

Pour des instructions sur l'utilisation d'OpsCenter pour configurer l'audit, consultez le Guide de l'administrateur NetBackup OpsCenter.

Pour afficher les paramètres actuels d'audit

1. Connectez-vous au serveur maître.
2. Ouvrez le répertoire suivant :

   Windows : *`install_path`*`\NetBackup\bin\admincmd\nbauditreport`

   UNIX : `/usr/openv/netbackup/bin/admincmd`
3. Exécutez la commande suivante :

   `nbemmcmd -listsettings -machinename` *`masterserver`*

   Où *`masterserver`* correspond au serveur maître concerné.
4. Les paramètres de configuration suivants apparaissent :

   - `AUDIT="ENABLED"`
     Indique que l'audit est activé.
   - `AUDIT="DISABLED"`
     Indique que l'audit est désactivé.
   - `AUDIT_RETENTION_PERIOD="90"`
     Indique que si l'audit est activé, les enregistrements sont conservés pendant cette durée (en jours) avant d'être supprimés. La période de conservation d'audit par défaut est de 90 jours. Une valeur de `0` (zéro) indique que les enregistrements ne sont jamais supprimés.

Événements d'audit

Les événements relatifs aux paramètres de sécurité suivants sont audités dans la **console d'administration NetBackup** :

- Certificat
- Connexion
- Hôte
- Connexion

- Configuration de la sécurité
- Jeton

Se reporter à "Affichage du rapport d'audit détaillé NetBackup" à la page 116.

Affichage des événements d'audit

NetBackup enregistre un certain nombre d'événements qui se produisent alors que vous travaillez avec le produit. Par exemple, un certificat de sécurité est émis sur un hôte, un jeton d'autorisation est supprimé, la connexion entre des hôtes est établie, etc.

Se reporter à "Affichage des détails des événements d'audit" à la page 112.

Se reporter à "Boîte de dialogue Détails des événements d'audit" à la page 113.

Se reporter à "Affichage de l'état des événements d'audit" à la page 114.

Pour afficher des événements d'audit

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** > **Événements de sécurité**.
2. Dans le volet des détails, cliquez sur l'onglet **Événements d'audit**.

   Se reporter à "Onglet Événements d'audit" à la page 111.

Onglet Événements d'audit

L'onglet Événements d'audit affiche des événements NetBackup en fonction des catégories d'audit que vous sélectionnez. NetBackup enregistre un certain nombre d'événements qui se produisent alors que vous travaillez avec le produit. Par exemple, un certificat de sécurité est émis sur un hôte, un jeton d'autorisation est supprimé, la connexion entre des hôtes est établie, etc.

Les informations suivantes sont affichées sur l'onglet :

Sélectionner la date/l'heure	Sélectionnez la plage de dates : les dates **From** et **To** pour lesquelles vous souhaitez afficher des événements d'audit. Vous pouvez également sélectionner la case à cocher **Heure actuelle** au lieu de sélectionner **À la date**. Les événements d'audit qui se sont produits entre la date spécifiée et l'heure actuelle sont affichés.
Sélectionner les catégories d'audit	Sélectionnez les catégories d'audit telles que Certificat, Connexion, Hôte, etc. pour afficher les événements respectifs dans le volet de rapport. Vous pouvez également sélectionner la case à cocher **Tous/Tout** pour sélectionner simultanément toutes les catégories d'audit.

Afficher l'état	Cliquez sur le lien pour ouvrir la fenêtre contextuelle **État des catégories d'audit sélectionnées**. La fenêtre contextuelle affiche les événements d'audit récupérés par catégories sélectionnées. Se reporter à "Affichage de l'état des événements d'audit" à la page 114.
Paramètres par défaut	Cliquez sur le bouton pour définir les paramètres par défaut pour la date et les catégories d'audit.
Extraire les événements d'audit	Cliquez sur le bouton pour afficher des événements d'audit en fonction des catégories sélectionnées. Pour afficher des informations supplémentaires sur un événement spécifique, sélectionnez ce dernier dans le tableau du volet de rapport et cliquez deux fois dessus. La boîte de dialogue **Détails** s'ouvre. Se reporter à "Boîte de dialogue Détails des événements d'audit" à la page 113. Initialement, l'onglet **Événements d'audit** affiche les événements d'audit pour toutes les catégories enregistrées jusqu'à présent. Vous pouvez sélectionner les catégories d'audit requises puis cliquer sur le bouton **Extraire les événements d'audit** (ou actualiser l'écran) pour extraire les événements récents pour les catégories sélectionnées.
Date	Date et heure auxquelles l'événement d'audit a été enregistré.
Utilisateur	Utilisateur qui a déclenché l'événement.
Catégorie	Catégorie d'audit, par exemple Certificat (CERT), Connexion (LOGIN), Configuration de sécurité (SEC_CONFIG) ou Jeton (TOKEN).
Action	Action effectuée par l'utilisateur, par exemple CREATE (créer un certificat) ou MODIFY (modifier une configuration de sécurité)
Description	Détails sur l'événement et l'action de l'utilisateur.

Affichage des détails des événements d'audit

Cette section fournit la procédure permettant d'afficher les détails des événements d'audit NetBackup.

Se reporter à "Onglet Événements d'audit" à la page 111.

Se reporter à "Affichage des événements d'audit" à la page 111.

Pour afficher les détails des événements d'audit

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** > **Événements de sécurité**.
2. Dans le volet des détails, cliquez sur l'onglet **Événements d'audit**.
3. Dans le volet de rapport, dans le tableau, cliquez deux fois sur l'événement d'audit dont vous voulez afficher les détails. La boîte de dialogue **Détails** s'affiche.

   Se reporter à "Boîte de dialogue Détails des événements d'audit" à la page 113.

Boîte de dialogue Détails des événements d'audit

La boîte de dialogue **Détails** affiche les informations spécifiques à l'événement d'audit que vous avez sélectionné sous l'onglet **Événements d'audit**.

Se reporter à "Onglet Événements d'audit" à la page 111.

La boîte de dialogue affiche les détails suivants :

Description	Description de l'événement d'audit que vous avez sélectionné.
Utilisateur	Utilisateur qui a déclenché l'événement.
Date	Date et heure auxquelles l'événement d'audit a été enregistré.
Catégorie	Catégorie d'audit, par exemple Certificat (CERT), Connexion (LOGIN), Configuration de sécurité (SEC_CONFIG) ou Jeton (TOKEN).
Action	Action effectuée par l'utilisateur, par exemple CREATE (créer un certificat) ou MODIFY (modifier une configuration de sécurité)
Raison	Motif de l'événement d'audit.

Remarque : S'il existe des enregistrements dans la catégorie CONNECTION, veillez à consulter les informations de l'enregistrement. Pour certains enregistrements dans cette catégorie, le champ **Date** qui s'affiche dans la boîte de dialogue indique quand l'enregistrement d'audit a été publié sur le serveur maître. Il n'indique pas nécessairement quand un événement s'est produit. Ce type d'enregistrement d'audit (par exemple, un enregistrement d'erreur de vérification de certificat (CVF)) représente un groupe d'événements qui se sont produits pendant une période. Les informations d'enregistrement d'audit fournissent **l'heure de début de l'événement** et l' **heure de fin de l'événement** de la période, ainsi que le **nombre d'événements** (le nombre total d'événements qui se sont produits pendant cette période).

Les informations de piste d'audit suivantes des événements figurent dans la boîte de dialogue :

Attribut	Attribut de l'événement d'audit associé. Par exemple : si un mappage de d'ID d'hôte vers le nom d'hôte est modifié, dans les détails du journal d'audit, les attributs suivants sont affichés : isApproved, isAddedManually, ApprovalState
Ancienne valeur	Ancienne valeur de l'attribut qui est associé à l'événement d'audit.
Nouvelle valeur	Nouvelle valeur de l'attribut.

Affichage de l'état des événements d'audit

Cette section indique la procédure à suivre pour afficher l'état des événements d'audit que vous voulez récupérer et afficher.

Se reporter à "Onglet Événements d'audit" à la page 111.

Se reporter à "Affichage des événements d'audit" à la page 111.

Pour afficher l'état des événements d'audit

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** > **Événements de sécurité**.
2. Dans le volet des détails, cliquez sur l'onglet **Événements d'audit**.
3. Sous l'onglet **Événements d'audit**, cliquez sur le lien **Afficher l'état** . La fenêtre contextuelle **État des catégories d'audit sélectionnées** s'affiche avec les informations suivantes :

Catégorie	Catégorie d'audit, par exemple certificat, connexion, hôte et ainsi de suite.
Etat	État des événements récupérées et affichés par catégorie d'audit. Par exemple : 10 événements d'audit sont récupérés. **Remarque :** L'onglet **Événements d'audit** affiche le nombre maximal de 10 000 événements par catégorie d'audit. Si le nombre d'enregistrements dépasse la limite maximale autorisée pour une date et une heure données, la fenêtre contextuelle **État des catégories d'audit sélectionnées** affiche le message de données tronquées. Pour afficher les enregistrements précédents, modifiez le filtre **Afficher la date/l'heure** sous l'onglet **Événements d'audit** ou utilisez la commande `nbauditreport`. Pour plus d'informations sur la commande `nbauditreport`, consultez le *Guide de référence des commandes NetBackup*.

Dépannage des problèmes d'audit liés à l'onglet Historique d'accès

L'onglet **Console d'administration NetBackup** > **Gestion de la sécurité** > **Événements de sécurité** > **Historique d'accès** affiche les détails concernant les activités de connexion que l'utilisateur actuel a exécutées.

Le champ **Accessible à partir de** sous l'onglet **Historique d'accès** affiche le composant que l'utilisateur a utilisé pour la connexion : **Console d'administration NetBackup** ou **API NetBackup**.

NetBackup nécessite que le service `bprd` soit en cours d'exécution pour afficher les détails d'audit des utilisateurs qui sont connectés à l'aide de la **console d'administration NetBackup**.

Si vous constatez que les enregistrements d'audit requis ne figurent pas dans l'onglet **Historique d'accès**, assurez-vous que le service `bprd` est en cours d'exécution sur le serveur maître.

Période de conservation d'audit et sauvegardes de catalogue des enregistrements d'audit

Les enregistrements d'audit sont conservés en tant qu'éléments de la base de données NetBackup, aussi longtemps que la période de conservation l'exige. Les enregistrements sont sauvegardés en tant qu'élément de la sauvegarde de catalogue de NetBackup. Le service d'audit NetBackup (`nbaudit`) supprime les enregistrements d'audit obsolètes une fois toutes les 24 heures à 12 h 00 (heure locale).

Par défaut, les enregistrements d'audit sont conservés pendant 90 jours. Utilisez une valeur de durée de conservation d'audit de `0` (zéro) pour ne pas supprimer les enregistrements d'audit.

Pour configurer la période de conservation d'audit

1. Connectez-vous au serveur maître.
2. Ouvrez le répertoire suivant :

   Windows : *install_path*\NetBackup\bin\admincmd

   UNIX : /usr/openv/netbackup/bin/admincmd
3. Saisissez la commande suivante :

   ```
   nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD
   number_of_days -machinename masterserver
   ```

   Où *number_of_days* indique le délai de conservation (en jours) des enregistrements d'audit pour le rapport d'audit.

   Dans l'exemple suivant, les enregistrements des actions de l'utilisateur doivent être conservés pendant 30 jours avant d'être supprimés.

   ```
   nbemmcmd -changesetting -AUDIT_RETENTION_PERIOD 30
   -machinename server1
   ```

   Pour vous assurer que tous les enregistrements d'audit sont inclus dans la sauvegarde du catalogue, configurez la fréquence de sauvegarde du catalogue sur une durée inférieure ou égale à -AUDIT_RETENTION_PERIOD.

Affichage du rapport d'audit détaillé NetBackup

Vous pouvez afficher les actions auditées par NetBackup à partir d'un serveur maître à l'aide de l'interface utilisateur web de NetBackup ou de la console d'administration de NetBackup. Vous pouvez afficher tous les détails des événements d'audit à l'aide de la commande nbauditreport ou dans NetBackup OpsCenter.

Pour plus de détails, consultez le Guide de l'administrateur de NetBackup OpsCenter.

Pour afficher l'intégralité du rapport d'audit

1. Connectez-vous au serveur principal.
2. Entrez la commande suivante pour afficher le rapport d'audit résumé.

   Windows : *install_path*\NetBackup\bin\admincmd\nbauditreport

   UNIX : /usr/openv/netbackup/bin/admincmd\nbauditreport

   Ou bien, exécutez la commande en utilisant les options suivantes.

`-sdate <"MM/DD/YY [HH:[MM[:SS]]]">`	Indique la date et l'heure de début des données à afficher dans le rapport.
`-edate <"MM/DD/YY [HH:[MM[:SS]]]">`	Date et heure de fin des données de rapport.
`-ctgy` *category*	Catégorie de l'action utilisateur exécutée. Les catégories, telles que `POLICY` peuvent contenir plusieurs sous-catégories, telles que des planifications ou des sélections de sauvegarde. Toutes les modifications apportées à une sous-catégorie sont répertoriées comme modifications de la catégorie principale. Consultez le Guide des commandes NetBackup pour connaître les options `-ctgy`.
`-user <`*username*`[:`*domainname*`]>`	Utilisez-la pour indiquer le nom de l'utilisateur dont vous souhaitez afficher les informations d'audit.
`-fmt DETAIL`	L'option `-fmt DETAIL` affiche la liste complète des informations d'audit. Par exemple, lorsqu'une politique est modifiée, cette vue affiche le nom de l'attribut, l'ancienne valeur et la nouvelle valeur. Cette option inclut les sous-options suivantes : ■ `[-notruncate]` . Affiche les anciennes et les nouvelles valeurs d'un attribut modifié sur différentes lignes dans la section de détails du rapport. ■ `[-pagewidth <NNN>]` . Définit la largeur de page dans la section informative du rapport d'audit.

`-fmt PARSABLE` L'option `-fmt PARSABLE` affiche le même ensemble d'informations que le rapport `DETAIL`, mais dans un format analysable. Le rapport utilise le caractère de barre verticale (`|`) comme séparateur entre les données du rapport d'audit. Cette option inclut les sous-options suivantes :

- `[-order<DTU|DUT|TDU|TUD|UDT|UTD>]`. Indiquez l'ordre de présentation des informations.
  `D` (Description)
  `T` (Horodatage)
  `U` (Utilisateur)

3 Le rapport d'audit contient les détails suivants :

`DESCRIPTION` Détails de l'action qui a été exécutée.

`USER` Identité de l'utilisateur qui a exécuté l'action.

Se reporter à "Identité d'utilisateur dans le rapport d'audit" à la page 119.

`TIMESTAMP` Heure à laquelle l'action a été exécutée.

Les informations suivantes s'affichent uniquement si vous utilisez les options `-fmt DETAIL` ou `-fmt PARSABLE`.

`CATEGORY` Catégorie de l'action exécutée par l'utilisateur.

`ACTION` Action exécutée.

`REASON` Raison pour laquelle l'action a été exécutée. Une valeur s'affiche si une raison a été spécifiée pour l'opération qui a créé la modification.

`DETAILS` Décompte de toutes les modifications, avec les anciennes et les nouvelles valeurs.

Exemple de rapport d'audit :

```
[root@server1 admincmd]# ./nbauditreport
TIMESTAMP            USER           DESCRIPTION
04/20/2018 11:52:43  root@server1   Policy 'test_pol_1' was saved but no changes were detected
04/20/2018 11:52:42  root@server1   Schedule 'full' was added to Policy 'test_pol_1'
04/20/2018 11:52:41  root@server1   Policy 'test_pol_1' was saved but no changes were detected
04/20/2018 11:52:08  root@server1   Policy 'test_pol_1' was created
```

```
04/20/2018 11:17:00  root@server1   Audit setting(s) of master server 'server1' were modified

Audit records fetched: 5
```

Identité d'utilisateur dans le rapport d'audit

Le rapport d'audit indique l'identité de l'utilisateur qui a exécuté une action spécifique. L'identité complète de l'utilisateur inclut le nom d'utilisateur et le domaine ou le nom d'hôte associé à l'utilisateur authentifié. L'identité d'un utilisateur apparaît dans le rapport d'audit comme suit :

- Les événements d'audit incluent toujours l'identité complète de l'utilisateur. Les utilisateurs racine et les administrateurs sont connectés en tant que "root@hostname" ou "administrator@hostname".
- Dans NetBackup 8.1.2 et versions ultérieures, les événements de navigation parmi les images et de restauration d'image incluent toujours l'ID de l'utilisateur dans l'événement d'audit. NetBackup 8.1.1 et versions antérieures consigne ces événements sous "root@hostname" ou "administrator@hostname".
- L'ordre des éléments pour le principal de l'utilisateur est "`domaine:nomutilisateur:typeDomaine:idFournisseur`". La valeur de domaine ne s'applique pas aux ordinateurs Linux. Pour cette plate-forme, le principal de l'utilisateur est `:nomutilisateur:typeDomaine:idFournisseur`.
- Toutes les opérations qui ne nécessitent pas d'informations d'authentification ou la connexion de l'utilisateur sont consignées sans identité d'utilisateur.

Désactivation de l'audit

L'audit de NetBackup est activé par défaut. Pour désactiver l'audit amélioré :

Se reporter à "Désactivation de l'audit amélioré" à la page 201.

Pour désactiver l'audit

1. Connectez-vous au serveur maître.
2. Ouvrez le répertoire suivant :

   Windows : *install_path*\NetBackup\bin\admincmd

   UNIX : /usr/openv/netbackup/bin/admincmd
3. Entrez la commande suivante :

   ```
   nbemmcmd -changesetting -AUDIT DISABLED -machinename masterserver
   ```

   Dans l'exemple suivant, l'audit a été désactivé pour `server1`.

   ```
   nbemmcmd -changesetting -AUDIT DISABLED -machinename server1
   ```

Notification d'alerte en cas de problème d'audit (console d'administration NetBackup)

Utilisez l'option de notification d'alerte pour indiquer si vous souhaitez être informé en cas d'échec d'une action couverte par l'audit et pour créer un enregistrement d'audit en conséquence. Cette option se trouve dans la barre d'état de la console d'administration de NetBackup.

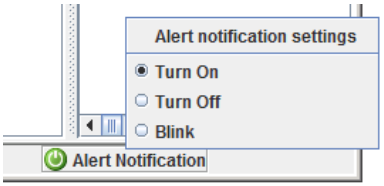


Tableau 4-1 Options de notification d'alerte d'audit

Activer	Un message contextuel semble alerter l'administrateur de la défaillance.
Clignoter	L'icône clignote en cas de défaillance de l'audit. Cliquez sur l'icône pour afficher le message de défaillance.
Désactiver	Les défaillances d'audit ne renvoient pas de notifications. L'icône devient grise.

Envoyer des événements d'audit dans les journaux système

Vous pouvez copier des événements d'audit NetBackup dans les journaux système. Assurez-vous que vous disposez des autorisations suivantes pour exécuter cette tâche :

- L'autorisation de sécurité est visible dans l'interface **Sécurité > Evénements de sécurité**
- Vous pouvez afficher, créer, mettre à jour et supprimer les autorisations dans l'interface **Gestion de NetBackup > Hôtes NetBackup**

Pour envoyer des événements d'audit aux journaux système

1. Dans la partie gauche, sélectionnez **Sécurité > Événements de sécurité**.
2. Dans la partie supérieure droite, cliquez sur **Paramètres de l'événement d'audit**.
3. Activez l'option **Envoyer les événements d'audit dans les journaux système**.
4. Dans la boîte de dialogue **Catégories d'événements d'audit**, sélectionnez les catégories d'audit pour lesquelles vous voulez envoyer les événements d'audit dans les journaux système.

   Pour envoyer des événements d'audit pour toutes les catégories d'audits dans les journaux système, cochez la case **Catégories d'événements d'audit**.
5. Cliquez sur **Enregistrer**.

   Vous pouvez copier les événements d'audit NetBackup dans les journaux système. Par exemple :

   Sur un système Windows, utilisez l'**Observateur d'événements Windows** pour afficher les événements d'audit NetBackup.

   Sur un système Linux, vous pouvez afficher les journaux système à l'emplacement configuré.

Section 1

Gestion des identités et des accès

Chapitre 5

À propos de la gestion des identités et des accès

Ce chapitre traite des sujets suivants :

À propos du contrôle d'accès dans NetBackup

NetBackup fournit les types suivants de contrôle d'accès :

- Console d'administration NetBackup (par défaut)
  Les administrateurs de NetBackup peuvent contrôler qui peut afficher les diverses applications dans NetBackup. Les administrateurs et utilisateurs racine ont un accès complet à la console d'administration NetBackup. Un utilisateur non-racine ou non-administrateur peut accéder à l'application de sauvegarde, d'archivage et de restauration. Cet utilisateur peut également accéder à des applications supplémentaires, telles que définies pour cet utilisateur dans le fichier `auth.conf`.
  Le contrôle d'accès est basé sur l'affichage et non sur le rôle. L'administrateur peut contrôler les applications qu'un utilisateur peut afficher et gérer, mais ne peut pas contrôler les tâches qu'un utilisateur peut effectuer en fonction de son rôle dans l'organisation. Le contrôle d'accès est limité à la console d'administration NetBackup. (Les interfaces telles que le client Sauvegarder, archiver et restaurer et le Client NetBackup MS SQL ne sont pas touchées.)
  Pour plus d'informations sur le contrôle d'accès avec la console d'administration NetBackup, consultez le Guide de l'administrateur de NetBackup, volume I.
- Contrôle d'accès en fonction des rôles (RBAC)
  À partir de la version NetBackup 8.1.2, l'interface utilisateur Web NetBackup fournit un contrôle d'accès basé sur les rôles pour un nombre limité de paramètres de sécurité et de charges de travail. Pour plus d'informations,

consultez le Guide de l'administrateur de la sécurité de l'interface utilisateur Web de NetBackup.

- Audit amélioré
  Cette fonction permet à un utilisateur non-racine ou non-administrateur d'exécuter toutes les opérations NetBackup via une interface de ligne de commande ou la console d'administration NetBackup. L'utilisateur est autorisé à effectuer toutes les opérations ou à n'en effectuer aucune. Cette fonction n'offre pas de contrôle d'accès en fonction du rôle.
  Se reporter à "À propos de l'audit amélioré" à la page 195.
- NetBackup Access Control (NBAC)
  NBAC est la fonctionnalité d'origine de contrôle d'accès basé sur les rôles fournie avec NetBackup pour la console d'administration NetBackup et les interfaces de ligne de commande. Il est recommandé d'utiliser une des autres méthodes de contrôle d'accès pour gérer votre environnement NetBackup.

Méthodes de contrôle d'accès pour la console d'administration NetBackup et les interfaces de ligne de commande

Consultez le tableau suivant pour connaître les différences clés entre les méthodes de contrôle d'accès disponibles pour la console d'administration NetBackup et les interfaces de ligne de commande. (La fonction RBAC dans l'interface utilisateur Web NetBackup fournit seulement le contrôle d'accès pour l'interface utilisateur Web et pour les API NetBackup.) Pour plus d'informations sur NBAC, reportez-vous à la documentation NetBackup pour la version 8.1.2 et les versions antérieures.

Tableau 5-1

Accès et audit	Console d'administration NetBackup et auth.conf	Audit amélioré
Qui peut utiliser la console d'administration NetBackup ?	Les administrateurs et utilisateurs racine ont un accès complet à la console d'administration. Les utilisateurs non-racine ou non-administrateurs sont limités à l'application Sauvegarde, archivage et restauration par défaut. Dans le cas contraire, ces utilisateurs peuvent accéder aux applications définies pour eux dans le fichier `auth.conf`.	Les utilisateurs racine, les administrateurs et les administrateurs NetBackup ont un accès complet à la console d'administration. Les utilisateurs non-racine ou non-administrateurs sont limités à l'application Sauvegarde, archivage et restauration par défaut.

Accès et audit	Console d'administration NetBackup et auth.conf	Audit amélioré
Qui peut utiliser l'interface de ligne de commande ?	Les administrateurs et utilisateurs racine ont un accès complet à l'interface de ligne de commande.	Les utilisateurs racine, les administrateurs et les administrateurs NetBackup ont un accès complet à l'interface de ligne de commande.
Comment un utilisateur est-il audité ?	En tant qu'utilisateur racine ou administrateur	Avec le nom d'utilisateur réel
Compatibilité avec d'autres fonctions	Audit amélioré	NBAC fonctionne indépendamment.

Consultez les diagrammes suivants pour plus de détails sur les méthodes de contrôle d'accès pour la console d'administration NetBackup et les interfaces de ligne de commande.

Figure 5-1 Contrôle d'accès pour des utilisateurs d'interface de ligne de commande avec l'audit amélioré

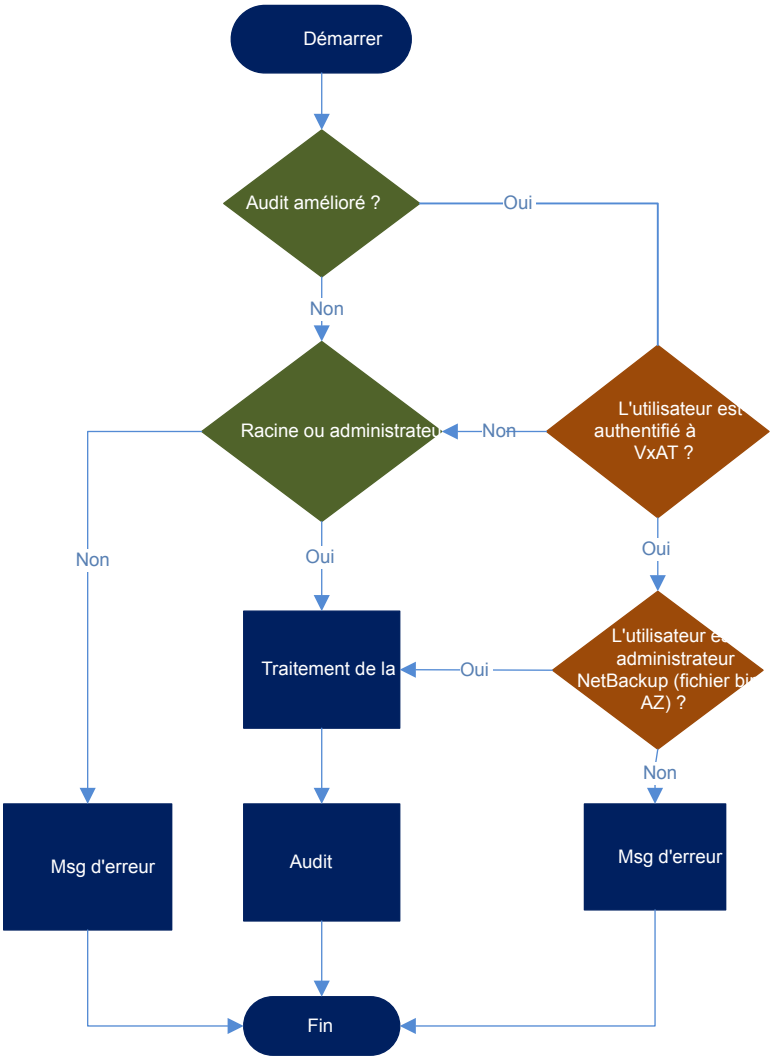
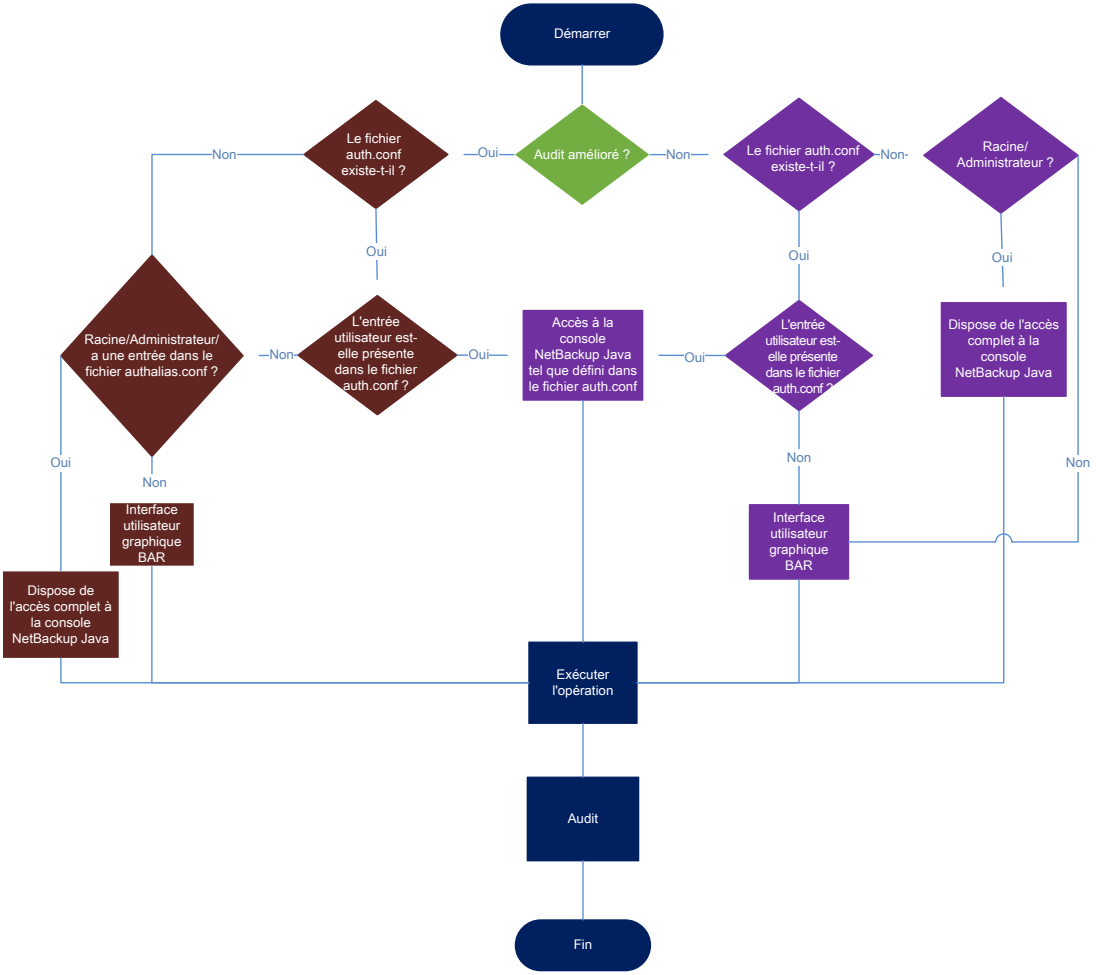


Figure 5-2 Contrôle d'accès pour des utilisateurs de la console d'administration NetBackup avec l'audit amélioré activé



Chapitre 6

Domaines AD et LDAP

Ce chapitre traite des sujets suivants :

Ajout des domaines AD ou LDAP dans NetBackup

NetBackup prend en charge les utilisateurs de domaines Active Directory (AD) ou Lightweight Directory Access Protocol (LDAP).

Si un domaine AD ou LDAP est ajouté dans NetBackup, les utilisateurs du domaine correspondant peuvent se connecter à un serveur maître NetBackup et l'administrateur de sécurité peut attribuer des rôles RBAC (contrôle d'accès basé sur les rôles) à ces utilisateurs de domaine.

Se reporter à "Fonctions RBAC" à la page 151.

La procédure suivante décrit l'ajout d'un domaine AD ou LDAP existant dans NetBackup et l'authentification des utilisateurs du domaine pour accéder à NetBackup.

Pour ajouter un domaine AD ou LDAP dans NetBackup

1 Exécutez la commande suivante pour ajouter un domaine AD ou LDAP dans le serveur maître NetBackup :

```
        vssat addldapdomain -d DomainName -s server_URL
-u user_base_DN -g group_base_DN [-f trusted_CA_file_name] [-t rfc2307 | msad |
{-c user_object_class -a user_attribute -q user_GID_attribute
-un user_display_name_attribute -ui user_ID_attribute[:value_type]
-ud user_description_attribute -x group_object_class -y group_attribute
-z group_GID_attribute -gn group_display_name_attribute
-gi group_ID_attribute[:value_type] -gd group_description_attribute
[-k DN | UID]]} [-b FLAT | BOB] -m admin_user_DN [-w admin_user_password]
[-p SUB | ONE | BASE] [-F]
```

Remarque : Assurez-vous que le nom d'utilisateur spécifié dans l'option `-m` dispose des droits requis pour interroger le serveur AD ou LDAP.

Si vous utilisez LDAPS et que le service d'authentification (`nbatd`) n'approuve pas l'autorité de certification qui a signé le certificat du serveur, utilisez l'option `-f` pour ajouter le certificat d'autorité de certification dans le magasin d'approbation `nbatd`.

Se reporter à "Autorités de certification approuvées par NetBackup Authentication Service" à la page 136.

Pour plus d'informations sur la commande `vssat`, consultez le *Guide de référence des commandes NetBackup*.

Contactez votre administrateur AD pour obtenir les valeurs appropriées pour ces options de ligne de commande. Les valeurs peuvent varier en fonction de la configuration de votre serveur AD.

Par exemple, pour ajouter un domaine AD :

```
        vssat addldapdomain -d domain1 -s ldap://domain1.veritas.com -u
"CN=Users,DC=domain1,DC=veritas,DC=com" -g "CN=Users,DC=domain1,DC=veritas,DC=com" -t msad -m
"CN=user1,CN=Users,DC=domain1,DC=veritas,DC=com" -b BOB
```

2 Exécutez la commande `vssat validateprpl` sur le serveur maître pour vérifier si le domaine AD ou LDAP spécifié a bien été ajouté.

`validateprpl -p` *`username`* `-d ldap:`*`domain_name`* `-b localhost:1556:nbatd`

Exemple de validation d'un domaine AD ou LDAP :

```
vssat validateprpl -p user1 -d ldap:domain1 -b localhost:1556:nba
```

Le nom de domaine doit correspondre à celui utilisé dans l'option de commande `addldapdomain`.

Pour plus d'informations sur la commande `vssat`, consultez le *Guide de référence des commandes NetBackup*.

Si le domaine LDAP ou AD a été ajouté et que la commande `vssat validateprpl` ou `vssat validategroup` échoue, vous devez procéder à certaines opérations de dépannage pour résoudre le problème.

Se reporter à "Dépannage des problèmes de configuration de domaine AD ou LDAP " à la page 130.

Dépannage des problèmes de configuration de domaine AD ou LDAP

Une fois que vous avez ajouté une configuration de domaine AD ou LDAP, vérifiez la configuration à l'aide des commandes `vssat validateprpl` et `vssat validategroup`. Les commandes valident l'utilisateur et le groupe AD / LDAP existants, respectivement.

Si les commandes `vssat validateprpl` et `vssat validategroup` sont exécutées avec succès, le domaine AD ou LDAP associé est correctement ajouté.

Pour plus d'informations sur ces commandes, consultez le Guide de référence des commandes NetBackup.

Si les commandes échouent, le message d'erreur suivant s'affiche :

```
The principal or group does not exist.
```

La validation du domaine AD ou LDAP peut échouer pour l'une des raisons suivantes :

- Impossible d'établir la connexion avec le serveur AD ou LDAP
- Informations d'authentification utilisateur non valides

- Nom unique de base du groupe ou de l'utilisateur non valide
- Plusieurs utilisateurs ou groupes existent avec le même nom sous le nom unique de base du groupe ou le nom unique de base de l'utilisateur
- L'utilisateur ou le groupe n'existe pas

Impossible d’établir la connexion avec le serveur AD ou LDAP

Pour résoudre le problème

1 Vérifiez si les journaux `nbatd` contiennent l’erreur suivante :

```
(authldap.cpp) CAuthLDAP::validatePrpl - ldap_simple_bind_s()
failed for user 'CN=Test User,OU=VTRSUsers,DC=VRTS,DC=com', error
= -1, errmsg = Can’t contact LDAP server,9:debugmsgs,1
```

2 Vérifiez si l'un des scénarios suivants est vrai et réalisez les étapes fournies pour ce scénario.

L'URL du serveur LDAP (option `-s`) qui est fournie avec `vssat addldapdomain` peut être incorrecte

Exécutez la commande suivante pour vérifier :

```
ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d
<debug_level> -o nettimeout=<seconds>
```

Exemple :

```
ldapsearch -H ldaps://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ******** -d 5 -o
nettimeout=60
```

```
TLS: can't connect: TLS error -8179:Peer's Certificate issuer
is not recognized. ldap_sasl_bind(SIMPLE): Can't contact LDAP
server (-1)
```

L'émetteur de certificat du serveur n'est pas une autorité de certification approuvée

Ceci s'applique si l'option `ldaps` est utilisée et peut être validée à l'aide de la commande `ldapsearch` :

```
set env var LDAPTLS_CACERT to cacert.pem
```

```
ldapsearch -H <LDAPS_URI> -D "<admin_user_DN>" -w <passwd> -d
<debug_level> -o nettimeout=<seconds>
```

Chemin d'accès au fichier pour `cacert.pem` :

Windows :

```
<Install_path>\NetBackup\var\global\vxss\eab\data\systemprofile\certstore\trusted\pluggins\ldap\cacert.pem
```

Sous UNIX :

```
/usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/certstore/trusted/pluggins/ldap/cacert.pem
```

Exemple :

```
ldapsearch -H ldaps://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ******** -d 5 -o
nettimeout=60
```

```
TLS: can't connect: TLS error -8179:Peer's Certificate issuer
is not recognized.. ldap_sasl_bind(SIMPLE): Can't contact LDAP
server (-1)
```

NetBackup Authentication Service (`nbatd`) n'approuve pas l'autorité de certification qui a signé le certificat de sécurité du serveur LDAP Se reporter à "Autorités de certification approuvées par NetBackup Authentication Service" à la page 136.	Utilisez l'option `-f` de la commande `vssat addldapdomain` pour ajouter le certificat d'autorité de certification dans le référentiel approuvé du service d'authentification (`nbatd`).

Informations d'authentification utilisateur non valides

Pour résoudre le problème

1. Vérifiez si les journaux `nbatd` contiennent l'erreur suivante :

   ```
   CAuthLDAP::validatePrpl - ldap_simple_bind_s() failed for user
   'CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com', error = 49, errmsg =
   Invalid credentials,9:debugmsgs,1
   ```

2. Vérifiez si le scénario suivant est vrai et réalisez les étapes fournies pour le scénario.

Nom unique de l'utilisateur admin ou mot de passe non valide fourni lors de l'ajout d'un domaine LDAP à l'aide de la commande `vssat addldapdomain`	Exécutez la commande suivante pour vérifier :
	`ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d <debug_level> -o nettimeout=<seconds>`
	Exemple :
	`ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com" -w ******** -d 5 -o nettimeout=60 ldap_bind: Invalid credentials (49)`

Nom unique de base du groupe ou de l'utilisateur non valide

Pour résoudre le problème

1. Vérifiez si les journaux `nbatd` contiennent l'erreur suivante :

   ```
   CAuthLDAP::validatePrpl - ldap_search_s() error = 10, errmsg =
   Referral,9:debugmsgs,1 CAuthLDAP::validatePrpl - ldap_search_s()
   error = 34, errmsg = Invalid DN syntax,9:debugmsgs,1
   ```

2. Vous pouvez voir les erreurs dans les journaux si la valeur du nom unique de base de l'utilisateur (option `-u`) ou du nom unique de base du groupe (option `-g`) est incorrecte.

   Exécutez la commande suivante pour vérifier :

   Exemple :

   ```
   ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test
   User,OU=VRTSUsers,DC=VRTS,DC=com" -w ****** -b
   "OU=VRTSUsers,DC=VRTS,DC=con" "(&(cn=test
   user)(objectClass=user))"
   ```

   ```
   ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test
   User,OU=VRTSUsers,DC=VRTS,DC=com" -w ****** -b "VRTS" "(&(cn=test
   user)(objectClass=user))"
   ```

Plusieurs utilisateurs ou groupes existent avec le même nom sous le nom unique de base de l'utilisateur ou le nom unique de base du groupe

Pour résoudre le problème

1. Vérifiez si les journaux `nbatd` contiennent l'erreur suivante :

   ```
   CAuthLDAP::validateGroup - search returned '2' entries for group
   name 'team_noone', even with referrals set to OFF,9:debugmsgs,1
   ```

2. Ceci s'applique si l'attribut de recherche d'utilisateur (option `-a`) et l'attribut de recherche de groupe (option `-y`) n'ont pas de valeurs uniques pour le nom unique de base de l'utilisateur et le nom unique de base du groupe, respectivement.

   Validez le nombre d'entrées correspondantes pour le nom unique de base existant à l'aide de la commande `ldapsearch`.

   ```
   ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d
   <debug_level> -o nettimeout=<seconds> -b <BASE_DN> <search_filter>
   ```

   Exemple :

```
ldapsearch -H ldap://example.veritas.com:389 -D "CN=Test
User,OU=VRTSUsers,DC=VRTS,DC=com" -w ****** -b "DC=VRTS,DC=com"
"(&(cn=test user)(objectClass=user))" # LDAPv3 # base <DC=VRTS,DC=com>
with scope subtree # filter: (cn=Test User) # requesting: ALL # Test
User, VRTSUsers, VRTS.com dn: CN=Test User,OU=VRTSUsers,DC=VRTS,DC=com
# Test User, RsvUsers, VRTS.com dn: CN=Test
User,OU=RsvUsers,DC=VRTS,DC=com # numEntries: 2
```

L'utilisateur ou le groupe n'existe pas

Pour résoudre le problème

1. Vérifiez si les journaux `nbatd` contiennent l'erreur suivante :

   ```
   CAuthLDAP::validatePrpl - user 'test user' NOT found,9:debugmsgs,4
   CAuthLDAP::validateGroup - group 'test group' NOT
   found,9:debugmsgs,4
   ```

2. Si un utilisateur ou groupe existe dans le domaine LDAP, mais que la commande `vssat validateprpl` ou `vssat validategroup` échoue avec cette erreur, vérifiez que l'utilisateur ou le groupe existe dans le nom de base actuel (options -u et -g) à l'aide de la commande suivante.

   ```
   ldapsearch -H <LDAP_URI> -D "<admin_user_DN>" -w <passwd> -d
   <debug_level> -o nettimeout=<seconds> -b <BASE_DN> <search_filter>
   ```

Autorités de certification approuvées par NetBackup Authentication Service

NetBackup Authentication Service (`nbatd`) approuve les autorités de certification suivantes :

- CyberTrust
- DigiCert GeoTrust
- Certification Services Division
- VeriSign Trust Network
- RSA Security Inc.
- GlobalSign
- Corporation

Chapitre 7

Clés d'accès

Ce chapitre traite des sujets suivants :

Clés d’accès

Les clés d’accès de NetBackup permettent d’accéder aux interfaces NetBackup via des clés d’API et des codes d’accès.

Se reporter à "Codes d'accès" à la page 137.

Codes d'accès

Pour exécuter certaines commandes d'administrateur NetBackup, par exemple `bperror`, vous devez vous authentifier via l'interface utilisateur Web. Vous devez générer un code d'accès via l'interface de ligne de commande, faire approuver la demande d'accès par l'administrateur, puis accéder à la commande.

Grâce à l'authentification sur l'interface utilisateur Web pour l'accès par l'interface de ligne de commande, les administrateurs NetBackup peuvent déléguer les privilèges associés à d'autres utilisateurs. Par défaut, seul un administrateur racine

ou un administrateur peut exécuter des opérations NetBackup par le biais de l'interface de ligne de commande. La prise en charge de l'authentification sur l'interface utilisateur Web permet aux utilisateurs non racine de gérer NetBackup s'ils disposent d'un accès par l'interface de ligne de commande accordé par l'administrateur de sécurité. Vous pouvez également gérer NetBackup avec un rôle utilisateur non RBAC (administrateur du système d'exploitation, par exemple) même si vous n'êtes pas enregistré en tant qu'utilisateur NetBackup. Vous devez générer un nouveau code d'accès à chaque fois que vous souhaitez accéder aux interfaces de ligne de commande.

Obtention d'un accès par interface de ligne de commande via l'authentification sur l'interface utilisateur Web

Pour obtenir un accès par interface de ligne de commande

1. Exécutez la commande suivante :

   ```
   bpnbat -login -logintype webui
   ```

   Un code d'accès est généré.

2. (Facultatif) Exécutez la commande suivante si vous souhaitez que le code soit approuvé par votre administrateur de sécurité :

   ```
   bpnbat -login -logintype webui -requestApproval
   ```

3. Si vous avez le rôle d'administrateur de ligne de commande (CLI), vous pouvez utiliser l'interface utilisateur Web pour approuver la demande d'accès par interface de ligne de commande à l'aide du code d'accès.

   Se reporter à "Approbation d'une demande d'accès par interface de ligne de commande" à la page 139.

   Si vous n'avez pas le rôle d'administrateur de ligne de commande (CLI), demandez à l'administrateur d'approuver la demande d'accès par interface de ligne de commande.

   Se reporter à "Approbation des demandes d'accès par interface de ligne de commande d'autres utilisateurs" à la page 139.

4. Une fois la demande d'accès par interface de ligne de commande approuvée, accédez à l'interface de ligne de commande et exécutez la commande requise.

   Par défaut, la session d'accès par interface de ligne de commande est valide pendant 24 heures.

   Se reporter à "Modification des paramètres d'accès" à la page 140.

Approbation d'une demande d'accès par interface de ligne de commande

Vous pouvez approuver une demande d'accès par interface de ligne de commande à l'aide de l'interface utilisateur Web.

Pour approuver une demande d'accès par interface de ligne de commande

1. Connectez-vous à l'interface utilisateur Web.
2. Sur la droite, cliquez sur l'icône de votre profil utilisateur.
3. Cliquez sur **Approuver la demande d'accès**.
4. Entrez le code d'accès par interface de ligne de commande que vous avez reçu de l'utilisateur qui a besoin d'un accès par interface de ligne de commande et cliquez sur **Examiner**.
5. Examinez les détails de la demande d'accès.
6. Cliquez sur **Approuver**.

Approbation des demandes d'accès par interface de ligne de commande d'autres utilisateurs

Si vous avez le rôle d'administrateur de ligne de commande (CLI), vous pouvez approuver les demandes d'accès d'autres utilisateurs utilisant l'interface utilisateur Web.

Pour approuver une demande d'accès par interface de ligne de commande d'un autre utilisateur

1. Connectez-vous à l'interface utilisateur Web.
2. Sur la gauche, sélectionnez **Sécurité > Clés d'accès > Codes d'accès**.
3. Entrez le code d'accès par interface de ligne de commande que vous avez reçu de l'utilisateur qui a besoin d'un accès par interface de ligne de commande et cliquez sur **Examiner**.
4. Examinez les détails de la demande d'accès.
5. Ajoutez éventuellement des commentaires.
6. Cliquez sur **Approuver**.

Modification des paramètres d'accès

Pour modifier les paramètres d'accès

1. Connectez-vous à l'interface utilisateur Web.
2. Dans la partie gauche, sélectionnez **Sécurité > Clés d'accès**.
3. Sur la droite, sélectionnez **Paramètres d'accès**.
4. Cliquez sur **Modifier**.
5. Saisissez la durée en minutes ou en heures pendant laquelle la session d'accès par interface de ligne de commande sera valide. La valeur minimale est 1 minute et la valeur maximale est 24 heures.

Chapitre 8

Clés d'API

Ce chapitre traite des sujets suivants :

A propos des clés d'API

NetBackup prend en charge l'authentification utilisateur via des clés d'API.

Une clé d'API NetBackup est un jeton pré-authentifié qui permet à un utilisateur NetBackup d'exécuter des commandes NetBackup (telles que `nbcertcmd -createToken` ou `nbcertcmd -revokeCertificate`) ou d'accéder aux API RESTful NetBackup.

A la différence d'un mot de passe, une clé d'API peut rester la même sur une longue période, et vous pouvez définir sa date d'expiration. Par conséquent, les opérations qui nécessitent une authentification (comme l'automatisation), peuvent être exécutées sur une longue période grâce aux clés d'API.

Se reporter à "Création de clés d'API" à la page 141.

Se reporter à "Utilisation d'une clé d'API" à la page 142.

Se reporter à "Gestion d'une clé d'API" à la page 142.

Création de clés d'API

Un utilisateur ne peut disposer que d'une seule clé d'API.

Vous pouvez créer des clés d'API de l'une des manières suivantes :

- A l'aide de l'API `netbackup/security/api-keys POST`
  N'importe quel utilisateur peut créer une clé d'API à l'aide de l'API `api-keys`
- A l'aide de l'interface utilisateur Web NetBackup
  Pour plus d'informations sur la création de clés d'API à l'aide de l'interface utilisateur Web ou des rôles RBAC, consultez le *Guide de l'administrateur de sécurité de l'interface utilisateur Web NetBackup*.

Se reporter à "Utilisation d'une clé d'API" à la page 142.

Se reporter à "Gestion d'une clé d'API" à la page 142.

Gestion d'une clé d'API

Chaque clé d'API est associée à une étiquette de clé d'API. Vous pouvez mettre à jour ou supprimer une clé d'API à l'aide de son étiquette de clé d'API de l'une des manières suivantes :

- Utilisation de l'API `netbackup/security/api-keys`
  Vous pouvez mettre à jour ou supprimer une clé d'API à l'aide de son étiquette de clé d'API.
- A l'aide de l'interface utilisateur Web NetBackup
  Pour plus d'informations sur la gestion des clés d'API à l'aide de l'interface utilisateur Web, consultez le *Guide de l'administrateur de sécurité de l'interface utilisateur Web NetBackup*.

Se reporter à "Création de clés d'API" à la page 141.

Se reporter à "Utilisation d'une clé d'API" à la page 142.

Utilisation d'une clé d'API

Une fois qu'une clé d'API est créée, vous pouvez l'utiliser lorsque vous accédez aux API RESTful ou que vous exécutez des commandes :

Se reporter à "Création de clés d'API" à la page 141.

Utilisation d'une clé d'API lors de l'accès à des API RESTful NetBackup

- Passez la clé d'API dans l'en-tête de demande d'API pour accéder à d'autres API NetBackup.

Utilisation d'une clé d'API lorsque lors de l'exécution de commandes NetBackup

1. Effectuez l'une des opérations suivantes :
   - Exécutez la commande suivante :

`bpnbat -Login -LoginType APIKEY`

Vous pouvez exécuter les commandes NetBackup qui requièrent une authentification pendant les prochaines 24 heures sans exécuter `bpnbat -Login`.

- Définissez une nouvelle variable d'environnement appelée `NETBACKUP_APIKEY` pour la clé d'API.

  Se reporter à "Définition d'une variable d'environnement de clé d'API pour exécuter des commandes NetBackup" à la page 143.

  Vous pouvez exécuter les commandes NetBackup qui requièrent une authentification tant que la clé d'API est valide et que la variable d'environnement est définie.

2 Exécutez une commande telle que `nbcertcmd -createToken`.

Pour plus d'informations sur les commandes NetBackup, consultez le *Guide de référence des commandes NetBackup*.

Définition d'une variable d'environnement de clé d'API pour exécuter des commandes NetBackup

Pour utiliser une clé d'API lors de l'exécution des commandes NetBackup qui nécessitent une authentification utilisateur, vous devez créer une clé d'API et définir une variable d'environnement pour la clé d'API. Une fois la variable d'environnement définie, vous pouvez exécuter les commandes tant que la clé d'API est valide et que la variable d'environnement est définie.

Sur la plate-forme Windows, définissez la variable d'environnement de clé d'API dans le contexte utilisateur.

Exemple de variable d'environnement pour une clé d'API :

`NETBACKUP_APIKEY = MasterServer1:APIKEY1`

Si vous souhaitez définir plusieurs clés d'API, spécifiez le serveur maître et les mappages de clé d'API dans un format séparé par des virgules.

Exemple :

`NETBACKUP_APIKEY = MasterServer1:APIKEY1,MasterServer2:APIKEY2,MasterServer3:APIKEY3`

Vous pouvez également spécifier les mappages dans un fichier, et ce fichier doit être spécifié avec le préfixe '@'.

Par exemple :

`NETBACKUP_APIKEY = @file_path/file_name`

Le contenu du fichier doit apparaître comme suit :

```
MasterServer1:APIKEY1

MasterServer2:APIKEY2

MasterServer3:APIKEY3
```

Se reporter à "Création de clés d'API" à la page 141.

Chapitre 9

Fichier auth.conf

Ce chapitre traite des sujets suivants :

Caractéristiques du fichier d'autorisation (auth.conf)

Par défaut, le fichier d'autorisation ou `auth.conf` autorise l'accès aux fonctions suivantes dans la **console d'administration NetBackup** :

Sur les serveurs NetBackup	Applications et fonctions d'administrateur pour l'utilisateur racine. Fonctions de sauvegarde et de restauration utilisateur pour tous les autres utilisateurs.
Sur les clients NetBackup	Fonctions de sauvegarde et de restauration utilisateur pour tous les utilisateurs.

Emplacement du fichier `auth.conf`

Serveurs NetBackup Windows	`auth.conf.win.template` dans *`install_path`*`\NetBackup\Java` Utilisez ce fichier modèle pour créer un fichier `auth.conf` au même emplacement. Le fichier modèle contient un exemple d'attribution d'autorisations à un utilisateur.

Serveurs NetBackup sous UNIX	`auth.conf` dans *`install_path`*`/NetBackup/Java`
	Il contient les entrées suivantes :
	`root ADMIN=ALL JBP=ALL`
	`* ADMIN=JBP JBP=ENDUSER+BU+ARC`

Configuration du fichier `auth.conf`

Configurez le fichier `auth.conf` comme suit :

- Si le fichier `auth.conf` existe, il doit contenir une entrée. Fournissez une entrée pour chaque utilisateur ou utilisez un astérisque (*) pour indiquer tous les utilisateurs. Les utilisateurs sans entrée dans le fichier ne peuvent pas accéder aux applications NetBackup.
- Les entrées d'utilisateurs spécifiques doivent être indiquées en premier, suivies de toutes les autres entrées comportant un astérisque (*).
- Utilisez le premier champ de chaque entrée pour indiquer le nom d'utilisateur à qui est accordé ou refusé des droits d'accès. Utilisez un astérisque pour indiquer n'importe quel nom d'utilisateur.
- Les champs restants spécifient les droits d'accès spécifiques pour les utilisateurs. Vous ne pouvez pas utiliser un astérisque (*) pour autoriser tous les utilisateurs pour toutes les applications. Chaque utilisateur doit avoir des mots clés d'application spécifiques. Pour refuser toutes les fonctions à un utilisateur spécifique, ne fournissez aucun mot clé pour l'interface. Exemple :

  ```
  mydomain\ray ADMIN= JBP=
  ```

- NetBackup prend désormais en charge des groupes d'utilisateurs pour lesquels le fichier `auth.conf` doit spécifier qu'ils ont besoin d'accéder à certaines fonctions de l'interface utilisateur.
  L'étiquette `<GRP>` est utilisée pour spécifier un groupe d'utilisateurs dans le fichier `auth.conf`. Par exemple :

  ```
  <GRP> domain1\BackupAdmins ADMIN=SUM JBP=BU
  ```

  Dans cet exemple, *domain1* est un domaine NetBackup et *BackupAdmins*, un groupe d'utilisateurs. Tous les utilisateurs du groupe *BackupAdmins* peuvent accéder au nœud Gestion des unités de stockage (`SUM`) de l'interface utilisateur et effectuer des tâches de sauvegarde (`BU`).

Mot-clé `ADMIN`

Spécifie les applications auxquelles l'utilisateur peut accéder. `ADMIN=ALL` autorise l'accès à toutes les applications NetBackup et aux fonctions d'administration qui leur sont associées.

`JBP` mot-clé

Spécifie ce que l'utilisateur peut faire avec l'application client Sauvegarde, archivage et restauration (`jbpSA`). `JBP=ALL` autorise l'accès à toutes les fonctions de Sauvegarde, archivage et restauration, y compris les fonctions d'administration.

Astérisque (*)

Un astérisque dans le premier champ indique que tous les noms d'utilisateur sont acceptés et que l'utilisateur est autorisé à utiliser les applications comme spécifié. La deuxième ligne de la version commercialisée contient un astérisque dans le premier champ. Cet astérisque signifie que NetBackup accepte tous les noms d'utilisateur pour l'accès à l'application cliente **Sauvegarde, archivage et restauration**`jbpSA`. `JBP=ENDUSER+BU+ARC` autorise les utilisateurs uniquement à sauvegarder, archiver et restaurer des fichiers.

Authentification utilisateur

Les informations d'authentification saisies à l'écran de connexion doivent être valides sur l'ordinateur spécifié dans le champ de l'hôte. Le serveur d'application NetBackup effectue l'authentification avec l'ordinateur spécifié. Le nom d'utilisateur est le compte utilisé pour sauvegarder, archiver ou restaurer les fichiers. Pour exécuter des opérations d'administration ou d'utilisation à distance à l'aide de `jbpSA`, un utilisateur doit disposer de comptes valides sur l'ordinateur client ou le serveur UNIX NetBackup. L'application **Sauvegarde, archivage et restauration** (`jbpSA`) nécessite des autorisations d'accès aux fichiers système pour rechercher les répertoires et les fichiers à sauvegarder ou à restaurer.

Le mot de passe doit être identique à celui utilisé lors de la connexion à cet ordinateur. Par exemple, supposez que vous vous connectez à l'aide des informations suivantes :

```
username = joe
password = access
```

Vous devez utiliser le même nom d'utilisateur et le même mot de passe pour vous connecter à NetBackup.

Vous pouvez vous connecter au serveur d'application NetBackup sous un nom d'utilisateur différent du nom utilisé pour la connexion au système d'exploitation. Par exemple, si vous vous connectez au système d'exploitation avec le nom d'utilisateur *Joe*, vous pouvez ultérieurement vous connecter à `jnbSA` en tant que racine.

Prise en charge de groupes d'utilisateurs

Les groupes Active Directory (AD) sont pris en charge dans le fichier `auth.conf` uniquement pour les serveurs maîtres.

Des groupes d'utilisateurs sont définis à l'aide de l'étiquette `<GRP>` dans le fichier `auth.conf`.

Remarque : Exécutez la commande `vssat validateprpl` pour vérifier le format des noms de groupe que vous avez définis dans le fichier `auth.conf`.

Pour plus d'informations sur la commande , consultez le Guide de référence des commandes NetBackup.

- Si un utilisateur fait partie de plusieurs groupes, ses droits d'accès sont combinés. Par exemple, *user1* fait partie des groupes d'utilisateurs *BackupAdmins* et *StorageUnitAdmins*.

  ```
  <GRP> domain1\BackupAdmins ADMIN=SUM JBP=BU
  <GRP> domain1\StorageUnitAdmins ADMIN=CAT JBP=RAWPART
  ```

  Les droits d'accès de *user1* sont combinés comme suit :
  `ADMIN=SUM+CATJBP=BU+RAWPART`

- Si le fichier `auth.conf` contient un utilisateur et le groupe auquel il appartient, les droits d'accès combinés sont attribués à l'utilisateur. Par exemple : *user1* fait partie des groupes d'utilisateurs *BackupAdmins* et *StorageUnitAdmins*.

  ```
  domain\user1 ADMIN=JBP JBP=ENDUSER
  <GRP> domain\BackupAdmins ADMIN=CAT JBP=BU
  <GRP> domain\StorageUnitAdmins ADMIN=SUM JBP=RAWPART
  ```

  Les droits d'accès de *user1* sont les suivants :
  `ADMIN=JBP+SUM+CATJBP=BU+RAWPART+ENDUSER`

- Si le fichier `auth.conf` contient des entrées en double pour un utilisateur et/ou un groupe d'utilisateurs, la première entrée est prise en compte et les droits d'accès combinés sont attribués à l'utilisateur. Par exemple : *user1* fait partie du groupe d'utilisateurs *BackupAdmins* et le fichier `auth.conf` contient deux entrées pour *BackupAdmins*.

  ```
  <GRP> domain1\BackupAdmins ADMIN=CAT JBP=BU
  <GRP> domain1\BackupAdmins ADMIN=SUM JBP=RAWPART
  ```

  Les droits d'accès de *user1* sont les suivants : `ADMIN=CATJBP=BU`

Informations sur l'état de l'application

À la fermeture, certaines informations d'état d'application sont automatiquement enregistrées dans le répertoire de *joe* `$HOME/.java/.userPrefs/vrts`. (Par exemple, l'ordre des colonnes de la table.) Ces informations seront restaurées la prochaine fois que vous vous connecterez au système d'exploitation sous le compte *joe* et que vous lancerez l'application NetBackup. Cette méthode de connexion est utile s'il existe plusieurs administrateurs, car elle enregistre les informations d'état pour chaque administrateur.

Remarque : NetBackup crée un répertoire d'utilisateur `$HOME/.java/.userPrefs/vrts` la première fois qu'un utilisateur quitte une application. Seules les applications NetBackup- utilisent le répertoire `.java/.userPrefs/vrts`.

Chapitre 10

Contrôle d’accès basé sur les rôles

Ce chapitre traite des sujets suivants :

- Administrateur RHV par défaut
- Administrateur SaaS par défaut
- Administrateur AHV par défaut
- Administrateur de sécurité par défaut
- Administrateur de stockage par défaut
- Administrateur de partage universel par défaut
- Administrateur VMware par défaut
- Ajout d'un rôle RBAC personnalisé
- Modifier ou supprimer un rôle personnalisé
- Afficher les utilisateurs dans RBAC
- Ajouter un utilisateur à un rôle (non-SAML)
- Ajout d'un utilisateur de carte à puce à un rôle (non-SAML, sans AD/LDAP)
- Ajouter un utilisateur à un rôle (SAML)
- Supprimer un utilisateur d'un rôle

Fonctions RBAC

L'interface utilisateur Web NetBackup permet d'appliquer le contrôle d'accès basé sur les rôles dans votre environnement NetBackup. Utilisez les fonctions RBAC pour fournir un accès à NetBackup pour les utilisateurs qui n'en dispose pas encore. Pour les utilisateurs actuels de NetBackup disposant d'un accès administrateur, vous pouvez également fournir des autorisations d'accès limitées en fonction de leur rôle dans votre organisation.

Pour plus de détails sur les méthodes de contrôle d'accès de la console d'administration NetBackup, le contrôle d'accès et les informations d'audit pour les administrateurs et les utilisateurs racine, consultez le Guide de sécurité et de chiffrement de NetBackup.

Tableau 10-1 Fonctions RBAC

Fonction	Description
Les rôles permettent aux utilisateurs d'effectuer des tâches spécifiques.	Ajoutez des utilisateurs à un ou plusieurs rôles RBAC par défaut ou créez des rôles personnalisés adaptés au rôle de vos utilisateurs. Affectez un utilisateur au rôle administrateur pour lui donner les autorisations NetBackup complètes. Se reporter à " Rôles RBAC par défaut " à la page 155.
Les utilisateurs peuvent accéder aux zones et fonctions NetBackup adaptées à leur rôle	Les utilisateurs RBAC peuvent effectuer des tâches courantes pour leur rôle d'entreprise, mais ne peuvent pas avoir accès à d'autres domaines et fonctions de NetBackup. RBAC contrôle également les biens que les utilisateurs peuvent afficher ou gérer.
Audit des événements RBAC	NetBackup audite les événements RBAC.
Reprise après incident prête	Les paramètres RBAC sont protégés par le catalogue NetBackup.
L'audit amélioré ou les configurations d'autorisation (`auth.conf`) sont encore disponibles sur les interfaces de versions antérieures.	L'audit amélioré est pris en charge sur toutes les interfaces. Vous pouvez continuer à utiliser les configurations d'autorisation (`auth.conf`) avec la console d'administration NetBackup et les interfaces de ligne de commande. Ces interfaces plus anciennes vous permettent de gérer l'accès à des workflows qui ne sont pas encore pris en charge dans l'interface utilisateur Web NetBackup et dans les API NetBackup. Notez que le fichier `auth.conf` ne restreint pas l'accès à l'interface utilisateur Web de NetBackup ni aux API NetBackup.

Paramètres RBAC

Vous pouvez configurer des paramètres de contrôle d'accès en fonction des rôles utilisateur. Les paramètres RBAC suivants peuvent être configurés :

- Accès à l'interface utilisateur Web pour l'administrateur du système d'exploitation
- Accès par interface de ligne de commande pour l'administrateur du système d'exploitation

Désactivation de l'accès à l'interface utilisateur Web pour l'administrateur du système d'exploitation

Par défaut, un administrateur de système d'exploitation (utilisateur ou membre du groupe) a accès à l'interface utilisateur Web NetBackup et ne doit pas nécessairement être membre d'un rôle RBAC.

Si vous ne souhaitez pas qu'un administrateur du système d'exploitation dispose automatiquement de cet accès, vous pouvez le désactiver. L'administrateur du système d'exploitation doit alors disposer du rôle d'administrateur RBAC pour accéder à l'interface utilisateur Web.

Pour désactiver le contrôle d'accès à l'interface utilisateur Web pour les administrateurs du système d'exploitation

1. Connectez-vous à l'interface utilisateur Web.
2. Dans la partie gauche, sélectionnez **Sécurité > RBAC**.
3. Dans la partie supérieure droite, cliquez sur **Paramètres du contrôle d'accès basé sur les rôles**.
4. Désactivez l'**Accès à l'interface utilisateur Web pour l'administrateur du système d'exploitation**.

Désactivation de l'accès à l'interface de ligne de commande des administrateurs du système d'exploitation

Par défaut, un administrateur du système d'exploitation (utilisateur ou membre du groupe) a accès à l'interface de ligne de commande de NetBackup et ne doit pas nécessairement être membre d'un rôle RBAC.

Si vous ne souhaitez pas qu'un administrateur du système d'exploitation dispose automatiquement de cet accès, vous pouvez le désactiver. L'administrateur du système d'exploitation doit alors se connecter avec `bpnbat -login` pour accéder à l'interface de ligne de commande.

Pour désactiver l'accès à la ligne de commande Web pour les administrateurs du système d'exploitation

1. Connectez-vous à l'interface utilisateur Web.
2. Dans la partie gauche, sélectionnez **Sécurité > RBAC**.
3. Dans la partie supérieure droite, cliquez sur **Paramètres du contrôle d'accès basé sur les rôles**.
4. Désactivez **Accès via la CLI pour l'administrateur du système d'exploitation**.

Configuration de RBAC

Pour configurer le contrôle d'accès basé sur les rôles pour l'interface utilisateur web NetBackup, procédez comme suit.

Tableau 10-2 Étapes de configuration du contrôle d'accès basé sur les rôles

Étape	Action	Description
1	Configurez des domaines Active Directory (AD) ou LDAP.	Pour que vous puissiez ajouter des utilisateurs de domaine, les domaines Active Directory ou LDAP doivent être authentifiés par NetBackup. Consultez le Guide de sécurité et de chiffrement NetBackup.
2	Déterminez les autorisations dont vos utilisateurs ont besoin.	Déterminez les autorisations dont vos utilisateurs ont besoin pour effectuer leurs tâches quotidiennes. Vous pouvez utiliser les rôles RBAC par défaut ou utiliser un rôle par défaut comme modèle pour créer un rôle. Vous pouvez également créer un rôle entièrement personnalisé pour répondre à vos besoins. Se reporter à " Rôles RBAC par défaut " à la page 155. Se reporter à "Ajout d'un rôle RBAC personnalisé" à la page 168.
3	Permet d'ajouter des utilisateurs aux rôles appropriés.	Se reporter à "Ajouter un utilisateur à un rôle (non-SAML)" à la page 171. Se reporter à "Ajouter un utilisateur à un rôle (SAML)" à la page 173. Se reporter à "Ajout d'un utilisateur de carte à puce à un rôle (non-SAML, sans AD/LDAP)" à la page 172.
4	Déterminez les autorisations à accorder aux administrateurs du système d'exploitation.	Se reporter à "Désactivation de l'accès à l'interface utilisateur Web pour l'administrateur du système d'exploitation" à la page 152. Se reporter à "Désactivation de l'accès à l'interface de ligne de commande des administrateurs du système d'exploitation" à la page 153.

Ajouter des domaines AD ou LDAP

NetBackup prend en charge les utilisateurs de domaines Active Directory (AD) ou Lightweight Directory Access Protocol (LDAP). Pour pouvoir ajouter des utilisateurs de domaine aux rôles RBAC, vous devez ajouter le domaine AD ou LDAP. Vous devez également ajouter un domaine avant de configurer ce domaine pour l'authentification par carte à puce.

Vous pouvez utiliser l'API `POST /security/domains/vxat` ou la commande `vssat` pour configurer des domaines.

Pour plus d'informations sur la commande `vssat` et sur ses options, consultez le Guide de référence des commandes de NetBackup. Pour plus d'informations sur le dépannage, consultez Guide de sécurité et de chiffrement NetBackup.

Rôles RBAC par défaut

L'interface utilisateur Web NetBackup fournit les rôles RBAC par défaut suivants avec des autorisations et des paramètres préconfigurés.

Tableau 10-3 Rôles RBAC par défaut dans l'interface utilisateur Web NetBackup

Administrateur	Le rôle Administrateur dispose de toutes les autorisations pour NetBackup et peut gérer tous les aspects de NetBackup.
Administrateur AHV par défaut	Ce rôle dispose de toutes les autorisations nécessaires pour gérer l'hyperviseur Nutanix Acropolis et sauvegarder ces biens avec des plans de protection.
Administrateur cloud par défaut	Ce rôle dispose de toutes les autorisations nécessaires pour gérer les biens cloud et pour les sauvegarder à l'aide de plans de protection.
Administrateur de la ligne de commande (CLI) NetBackup par défaut	Ce rôle dispose de toutes les autorisations nécessaires pour gérer NetBackup à l'aide de la ligne de commande (CLI) de NetBackup. Avec ce rôle, un utilisateur peut exécuter la plupart des commandes NetBackup avec un compte autre que racine. **Remarque :** un utilisateur disposant seulement de ce rôle ne peut pas se connecter à l'interface utilisateur Web.
Administrateur Kubernetes par défaut	Ce rôle dispose de toutes les autorisations nécessaires pour gérer les biens Kubernetes et pour les sauvegarder avec des plans de protection. Les autorisations de ce rôle permettent à l'utilisateur d'afficher et de gérer des travaux pour les biens Kubernetes. Pour afficher tous les travaux portant sur ce type de bien, l'utilisateur doit disposer du rôle par défaut pour cette charge de travail. Si ce n'est pas le cas, il doit disposer d'un rôle personnalisé similaire, et l'option suivante doit être appliquée lors de la création du rôle : **Appliquer les autorisations sélectionnées à tous les biens de charge de travail existants et futurs**.

Service d'opérateur NetBackup Kubernetes par défaut	Ce rôle fournit les autorisations nécessaires pour le compte utilisateur de clé d'API qui est configuré pour le service d'opérateur Kubernetes (plug-in). **Remarque :** un utilisateur disposant seulement de ce rôle ne peut pas se connecter à l'interface utilisateur Web.
Administrateur Microsoft SQL Server par défaut	Ce rôle dispose de toutes les autorisations nécessaires pour gérer les bases de données SQL Server et pour sauvegarder ces biens avec des plans de protection. En plus de ce rôle, l'utilisateur NetBackup doit remplir les conditions suivantes : ■ Il doit être membre du groupe d'administrateurs Windows. ■ Il doit avoir le rôle « sysadmin » dans SQL Server.
Administrateur Oracle par défaut	Ce rôle dispose de toutes les autorisations nécessaires pour gérer les bases de données Oracle et pour les sauvegarder à l'aide de plans de protection.
Administrateur RHV par défaut	Ce rôle dispose de toutes les autorisations nécessaires pour gérer les machines Red Hat Virtualization et pour sauvegarder ces biens avec des plans de protection. Ce rôle permet à l'utilisateur d'afficher et de gérer des travaux pour les biens RHV. L'utilisateur doit disposer de ce rôle afin d'afficher les travaux pour les biens RHV. Si ce n'est pas le cas, il doit disposer d'un rôle personnalisé similaire, et l'option suivante doit être appliquée lors de la création du rôle : **Appliquer les autorisations sélectionnées à tous les biens RHV existants et futurs**.
Administrateur Resiliency par défaut	Ce rôle dispose de toutes les autorisations pour protéger Veritas Resiliency Platform (VRP) pour les biens VMware.
Administrateur SaaS par défaut	Ce rôle dispose de toutes les autorisations pour afficher et gérer les biens SaaS.
Administrateur de sécurité par défaut	Ce rôle dispose des autorisations nécessaires pour gérer la sécurité de NetBackup, notamment le contrôle d'accès basé sur les rôles (RBAC), les certificats, les hôtes, les fournisseurs d'identité et les domaines, les paramètres de sécurité globaux et d'autres autorisations. Ce rôle permet également d'afficher les paramètres et les biens dans la plupart des domaines NetBackup : charges de travail, stockage, licences et autres domaines.

Administrateur de stockage par défaut	Ce rôle dispose des autorisations de configuration du stockage sur disque et de politiques de cycle de vie du stockage. Les paramètres des SLP sont gérés par le rôle Administrateur.
Administrateur de partage universel par défaut	Ce rôle dispose des autorisations de gestion des politiques et des serveurs de stockage. Il peut également gérer les biens des clients de type Windows et Standard, ainsi que pour les partages universels.
Administrateur VMware par défaut	Ce rôle dispose de toutes les autorisations nécessaires pour gérer les machines virtuelles VMware et pour sauvegarder ces biens avec des plans de protection. L'utilisateur doit disposer de ce rôle afin d'afficher les travaux pour les biens VMware. Si ce n'est pas le cas, il doit disposer d'un rôle personnalisé similaire et l'option suivante doit être appliquée lors de la création du rôle : **Appliquer les autorisations sélectionnées à tous les biens VMware existants et futurs**.

Remarque : Veritas se réserve le droit de modifier les autorisations RBAC pour les rôles par défaut dans les versions ultérieures. Toutes les autorisations révisées sont automatiquement appliquées aux utilisateurs possédant ces rôles lors de la mise à niveau de NetBackup. Les copies de rôles par défaut dont vous disposez ne sont pas mises à jour automatiquement. (Ou si vous avez des rôles personnalisés qui sont basés sur les rôles par défaut.) Si vous souhaitez que ces rôles personnalisés incluent les modifications apportées aux rôles par défaut, vous devez appliquer manuellement les modifications manuellement ou recréer les rôles personnalisés.

Administrateur

Le rôle Administrateur dispose de toutes les autorisations pour NetBackup et peut gérer tous les aspects de NetBackup.

- Autorisations RBAC **globales**.
  - **Gestion de NetBackup** : configuration et gestion de NetBackup.
  - **Protection** : politiques de sauvegarde NetBackup et politiques de cycle de vie du stockage.
  - **Sécurité** : paramètres de sécurité NetBackup.

  - **Stockage** : gestion des paramètres de stockage de sauvegarde.
- **Biens** : gestion de tous les types de bien.
- **Plans de protection** : gestion du mode d'exécution des sauvegardes au moyen des plans de protection.
- **Informations d'authentification** : gestion des informations d'authentification pour les biens et d'autres fonctions NetBackup.

Administrateur cloud par défaut

Ce rôle dispose de toutes les autorisations nécessaires pour gérer les biens cloud et pour sauvegarder ces biens avec des plans de protection.

Tableau 10-4 Autorisations RBAC pour le rôle d'administrateur cloud par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	
Images de sauvegarde NetBackup	Afficher le contenu, Afficher
Travaux	Afficher
Serveur de médias	Afficher
Serveurs principaux approuvés	Afficher
Plug-ins de serveur de gestion de snapshots	Afficher, Créer, Mettre à jour, Gérer l'accès
Serveurs de gestion de snapshots	Autorisations complètes
Autorisations globales > Stockage	
Unités de stockage	Afficher
Serveurs de stockage cibles compatibles avec la réplication	Afficher
Biens	
Biens cloud	Autorisations complètes
Plans de protection	Autorisations complètes
Informations d'authentification	Autorisations complètes

Administrateur de la ligne de commande (CLI) NetBackup par défaut

Ce rôle dispose de toutes les autorisations nécessaires pour gérer NetBackup à l'aide de la ligne de commande (CLI) NetBackup. Avec ce rôle, un utilisateur peut exécuter la plupart des commandes NetBackup avec un compte non racine.

Remarque : Un utilisateur disposant seulement de ce rôle ne peut pas se connecter à l'interface utilisateur Web.

Tableau 10-5 Autorisations RBAC pour l'administrateur de ligne de commande (CLI) NetBackup par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	
Sessions de l'interface de ligne de commande	Exécution de l'interface de ligne de commande

Administrateur Kubernetes par défaut

Ce rôle dispose de toutes les autorisations nécessaires pour gérer les biens Kubernetes et pour les sauvegarder avec des plans de protection. Les autorisations de ce rôle permettent à l'utilisateur d'afficher et de gérer des travaux pour les biens Kubernetes. Pour afficher tous les travaux portant sur ce type de bien, l'utilisateur doit disposer du rôle par défaut pour cette charge de travail. Si ce n'est pas le cas, il doit disposer d'un rôle personnalisé similaire, et l'option suivante doit être appliquée lors de la création du rôle : **Appliquer les autorisations sélectionnées à tous les biens de *charge de travail* existants et futurs**.

Tableau 10-6 Autorisations RBAC pour le rôle d'administrateur Kubernetes par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	
Hôtes NetBackup	Afficher, Mettre à jour
Limites des ressources	Afficher, Créer, Mettre à jour, Supprimer
Serveurs principaux approuvés	Afficher

Type	Autorisations
Biens	
Biens Kubernetes	Autorisations complètes
Plans de protection	Autorisations complètes.
Informations d'authentification	Autorisations complètes

Service d'opérateur NetBackup Kubernetes par défaut

Ce rôle fournit les autorisations nécessaires pour le compte utilisateur de clé d'API qui est configuré pour le service d'opérateur Kubernetes (plug-in).

Remarque : Un utilisateur disposant seulement de ces autorisations ne peut pas se connecter à l'interface utilisateur Web.

Tableau 10-7 Autorisations RBAC pour le rôle de service d'opérateur Kubernetes par défaut

Type	Autorisations
Biens	
Biens Kubernetes	Créer, Mettre à jour

Administrateur Oracle par défaut

Ce rôle dispose de toutes les autorisations nécessaires pour gérer les bases de données Oracle et pour les sauvegarder à l'aide de plans de protection.

Tableau 10-8 Autorisations RBAC pour le rôle d'administrateur Oracle par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	
Serveurs principaux approuvés	Afficher
Biens	

Type	Autorisations
Biens Oracle	Autorisations complètes
Informations d'authentification	Autorisations complètes

Administrateur Microsoft SQL Server par défaut

Ce rôle dispose de toutes les autorisations nécessaires pour gérer les bases de données SQL Server et pour sauvegarder ces biens avec des plans de protection. En plus de ce rôle, l'utilisateur NetBackup doit remplir les conditions suivantes :

- Il doit être membre du groupe d'administrateurs Windows.
- Il doit avoir le rôle « sysadmin » dans SQL Server.

Tableau 10-9 Autorisations RBAC pour le rôle d'administrateur Microsoft SQL Server par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	
Travaux	Afficher
Serveurs principaux approuvés	Afficher
Autorisations globales > Stockage	
Unités de stockage	Afficher
Serveurs de stockage cibles compatibles avec la réplication	Afficher
Biens	
Biens SQL Server	Autorisations complètes
Plans de protection	Autorisations complètes
Informations d'authentification	Autorisations complètes

Administrateur Resiliency par défaut

Ce rôle dispose de toutes les autorisations pour protéger Veritas Resiliency Platform (VRP) pour les biens VMware.

Tableau 10-10 Autorisations RBAC pour le rôle d'administrateur Resiliency par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	
Domaine Resiliency	Autorisations complètes
Informations d'authentification	Autorisations complètes

Administrateur RHV par défaut

Ce rôle dispose de toutes les autorisations nécessaires pour gérer les machines Red Hat Virtualization et pour sauvegarder ces biens avec des plans de protection. Ce rôle permet à l'utilisateur d'afficher et de gérer des travaux pour les biens RHV.

L'utilisateur doit disposer de ce rôle afin d'afficher les travaux pour les biens RHV. Si ce n'est pas le cas, il doit disposer d'un rôle personnalisé similaire et l'option suivante doit être appliquée lors de la création du rôle : **Appliquer les autorisations sélectionnées à tous les biens RHV existants et futurs**.

Tableau 10-11 Autorisations RBAC pour le rôle d'administrateur RHV par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	
Hôtes d'accès	Afficher, Créer, Supprimer
Hôtes NetBackup	Afficher, Mettre à jour
Limites des ressources	Afficher, Créer, Mettre à jour, Supprimer
Serveurs principaux approuvés	Afficher
Autorisations globales > Stockage	
Unités de stockage	Afficher
Serveurs de stockage cibles compatibles avec la réplication	Afficher
Biens	
Biens RHV	Autorisations complètes
Plans de protection	Autorisations complètes

Administrateur SaaS par défaut

Ce rôle dispose de toutes les autorisations pour afficher et gérer les biens SaaS.

Tableau 10-12 Autorisations RBAC pour le rôle d'administrateur SaaS par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	
Hôtes NetBackup	Afficher, Créer, Mettre à jour
Biens	
Biens SaaS	Autorisations complètes
Informations d'authentification	Autorisations complètes

Administrateur AHV par défaut

Ce rôle dispose de toutes les autorisations nécessaires pour gérer l'hyperviseur Nutanix Acropolis et sauvegarder ces biens avec des plans de protection.

Tableau 10-13 Autorisations RBAC pour le rôle d'administrateur AHV par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	
Hôtes d'accès	Afficher, Créer, Supprimer
Hôtes sans agent	Afficher
Serveur de médias	Afficher
Hôtes NetBackup	Afficher, Mettre à jour
Images de sauvegarde NetBackup	Afficher, Afficher le contenu
Travaux	Afficher
Limites des ressources	Afficher, Créer, Mettre à jour, Supprimer
Serveurs principaux approuvés	Afficher
Autorisations globales > Stockage	
Unités de stockage	Afficher

Type	Autorisations
Serveurs de stockage cibles compatibles avec la réplication	Afficher
Biens	
Biens AHV	Autorisations complètes
Plans de protection	Autorisations complètes
Informations d'authentification	Autorisations complètes

Administrateur de sécurité par défaut

Ce rôle dispose des autorisations nécessaires pour gérer la sécurité de NetBackup, notamment le contrôle d'accès basé sur les rôles (RBAC), les certificats, les hôtes, les fournisseurs d'identité et les domaines, les paramètres de sécurité globaux et d'autres autorisations. Ce rôle permet également d'afficher les paramètres et les biens dans la plupart des domaines NetBackup, y compris les charges de travail, le stockage, les licences et d'autres domaines.

Tableau 10-14 Autorisations RBAC pour le rôle d'administrateur de sécurité par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	
Toutes les catégories, sauf celles qui sont indiquées	Afficher, Gérer l'accès
Hôtes NetBackup	Autorisations complètes
Serveur de médias	Autorisations complètes
Autorité de certification du serveur principal distant	Autorisations complètes
Serveurs principaux approuvés	Autorisations complètes
Autorisations globales > Protection	
Toutes les catégories	Afficher, Gérer l'accès
Autorisations globales > Sécurité	

Type	Autorisations
Toutes les catégories, sauf celles qui sont indiquées	Afficher, Gérer l'accès
Contrôle d'accès	Autorisations complètes
Gestion des certificats : autorités de certification NetBackup, certificats externes, certificats NetBackup, jetons de sécurité NetBackup	Autorisations complètes
Phrase de passe de reprise après incident	Autorisations complètes
Configuration du fournisseur d'identité et du certificat SAML	Autorisations complètes
Services de gestion des clés	Autorisations complètes
Contraintes de phrase de passe	Mettre à jour (Autorisations complètes)
Paramètres de sécurité globaux	Autorisations complètes
Sessions utilisateur et authentification : clés d'API, certificats d'utilisateur, sessions utilisateur	Autorisations complètes
Autorisations globales > Stockage	
Toutes les catégories	Afficher, Gérer l'accès
Biens	
Toutes les charges de travail	Afficher, Gérer l'accès
Plans de protection	Afficher, gérer l'accès
Informations d'authentification	Afficher, Gérer l'accès

Administrateur de stockage par défaut

Ce dispose des autorisations de configuration du stockage sur disque et de politiques de cycle de vie du stockage. Les paramètres des SLP sont gérés par le rôle **Administrateur**.

Se reporter à "Administrateur" à la page 157.

Tableau 10-15 Autorisations RBAC pour le rôle d'administrateur de stockage par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	
Classification des données	Afficher
Hôtes NetBackup	Afficher
Serveur de médias	Afficher
Autorité de certification du serveur principal distant	Afficher
Niveaux de conservation	Afficher
Serveurs > Serveurs principaux approuvés	Afficher, Créer, Mettre à jour, Supprimer
Autorisations globales > Protection	
Politiques	Afficher
Fenêtres SLP	Autorisations complètes Afficher, Créer, Mettre à jour, Supprimer
Politiques de cycle de vie du stockage	Autorisations complètes Afficher, Créer, Mettre à jour, Supprimer
Autorisations globales > Sécurité	
Jetons de sécurité NetBackup	Afficher, Créer
Services de gestion des clés	Afficher, Afficher les détails de la clé
Autorisations globales > Stockage	
Stockage en cloud	Afficher
Pools de disques	Afficher, Créer, Mettre à jour, Supprimer
Serveurs de stockage	Afficher, Créer, Mettre à jour, Supprimer
Volumes de disques	Afficher, Créer, Mettre à jour
Unités de stockage	Afficher, Créer, Mettre à jour, Supprimer
Média de bande > Groupes de serveurs de médias de bande	Afficher

Type	Autorisations
Média de bande > Pools de volumes de médias de bande	Afficher
Serveurs de stockage cibles compatibles avec la réplication	Afficher

Administrateur de partage universel par défaut

Tableau 10-16 Autorisations RBAC pour le rôle d'administrateur de partage universel par défaut

Type	Autorisations
Autorisations globales > Protection	
Politiques	Afficher
Autorisations globales > Stockage	
Serveurs de stockage	Afficher
Biens	
Types de clients Windows et standard	Restaurer des sauvegardes de systèmes de fichiers
Partages universels	Autorisations complètes

Administrateur VMware par défaut

Ce rôle dispose de toutes les autorisations nécessaires pour gérer les machines virtuelles VMware et pour sauvegarder ces biens avec des plans de protection.

L'utilisateur doit disposer de ce rôle afin d'afficher les travaux pour les biens VMware. Si ce n'est pas le cas, il doit disposer d'un rôle personnalisé similaire, et l'option suivante doit être appliquée lors de la création du rôle : **Appliquer les autorisations sélectionnées à tous les biens VMware existants et futurs**.

Tableau 10-17 Autorisations RBAC pour le rôle d'administrateur VMware par défaut

Type	Autorisations
Autorisations globales > Gestion de NetBackup	

Type		Autorisations
Hôtes d'accès		Afficher, Créer, Supprimer
Hôtes NetBackup		Afficher, Mettre à jour
	Passerelle de protection permanente des données	Afficher, Créer, Supprimer
	Propriétés de l'hôte	Afficher, Créer, Mettre à jour
Images de sauvegarde NetBackup		Afficher, Afficher le contenu
Limites des ressources		Afficher, Créer, Mettre à jour, Supprimer
Serveurs principaux approuvés		Afficher
Autorisations globales > Stockage		
Unités de stockage		Afficher
Serveurs de stockage cibles compatibles avec la réplication		Afficher
Biens		
Biens VMware		Toutes les autorisations
Plans de protection		Autorisations complètes

Ajout d'un rôle RBAC personnalisé

Créez un rôle RBAC personnalisé si vous souhaitez définir manuellement les autorisations et l'accès des utilisateurs aux biens de charge de travail, aux plans de protection et aux informations d'authentification.

Remarque : Veritas se réserve le droit de modifier les autorisations RBAC pour les rôles par défaut dans les versions ultérieures. Toutes les autorisations révisées sont automatiquement appliquées aux utilisateurs possédant ces rôles lors de la mise à niveau de NetBackup. Toutes les copies de rôles par défaut (ou de rôles personnalisés basés sur des rôles par défaut) ne sont pas automatiquement mises à jour.

Pour ajouter un rôle RBAC personnalisé

1. Connectez-vous à l'interface utilisateur Web de NetBackup.
2. Sur le côté gauche, sélectionnez **Sécurité > RBAC** et cliquez sur **Ajouter**.

3 Sélectionnez le type de rôle que vous souhaitez créer .

Vous pouvez effectuer la copie d'un rôle par défaut qui contient toutes les autorisations et les paramètres préconfigurés pour ce type de rôle. Vous pouvez également sélectionner **Rôle personnalisé** pour configurer manuellement toutes les autorisations pour un rôle.

4 Fournissez un **nom de rôle** et une description.

Par exemple, vous pouvez indiquer que ce rôle est défini pour tous les administrateurs de sauvegarde sur un service ou une région particulière.

5 Sur la carte **Autorisations**, cliquez sur **Assigner**.

Les autorisations que vous sélectionnez déterminent les autres paramètres que vous pouvez configurer pour le rôle.

Si vous sélectionnez un type de rôle par défaut, certaines autorisations sont activées uniquement si elles sont requises pour ce type de rôle. (Par exemple, le rôle **Administrateur de stockage par défaut** ne requiert pas d'autorisations pour les plans de protection et le rôle **Administrateur Microsoft SQL Server par défaut** requiert des informations d'authentification.)

- La carte **Charges de travail** est activée lorsque vous sélectionnez l'autorisation d'un **bien**.
- La carte **Plans de protection** est activée lorsque vous sélectionnez des autorisations de **Plans de protection**.
- La carte **Informations d'authentification** est activée lorsque vous sélectionnez les autorisations des **Informations d'authentification**.

6 Configurez les autorisations pour le rôle.

7 Sur la carte **Utilisateurs**, cliquez sur **Assigner**.

8 Lorsque vous avez terminé la configuration du rôle, cliquez sur **Enregistrer**.

Remarque : lorsque vous créez un rôle, vous devez modifier les autorisations relatives aux biens, aux plans de protection ou aux informations d'authentification directement depuis le nœud concerné dans l'interface utilisateur Web. Par exemple, pour modifier les autorisations pour VMware, sélectionnez **Charges de travail > VMware**, puis sélectionnez **Paramètres VMware > Gérer les autorisations**. Ou bien, ouvrez la section d'information d'une machine virtuelle et cliquez sur l'onglet **Autorisations**.

Modifier ou supprimer un rôle personnalisé

Vous pouvez modifier ou supprimer un rôle personnalisé afin de modifier ou de supprimer des autorisations pour les utilisateurs disposant de ce rôle. Les rôles par

défaut ne peuvent pas être modifiés ou supprimés. Vous pouvez uniquement ajouter ou supprimer des utilisateurs dans les rôles par défaut.

Modifier un rôle personnalisé

Remarque : Lorsque vous modifiez les autorisations associées à un rôle personnalisé, ces modifications s'appliquent à tous les utilisateurs auxquels ce rôle est affecté.

Pour modifier un rôle personnalisé

1. Connectez-vous à l'interface utilisateur Web NetBackup.
2. Sur le côté gauche, cliquez sur **Sécurité > RBAC**.
3. Identifiez le rôle personnalisé à modifier dans l'onglet **Rôles** et cliquez dessus.
4. Pour modifier la description du rôle, cliquez sur **Modifier le nom et la description** .
5. Modifiez les autorisations du rôle. Vous pouvez modifier les informations suivantes d'un rôle :

Autorisations globales du rôle	Dans l'onglet **Autorisations globales**, cliquez sur **Modifier**.
Utilisateurs du rôle	Cliquez sur l'onglet **Utilisateurs**.
Définitions d'accès du rôle	Cliquez sur l'onglet **Définitions d'accès**.

6. Pour ajouter ou supprimer des utilisateurs du rôle, cliquez sur l'onglet **Utilisateurs**.

   Se reporter à "Ajouter un utilisateur à un rôle (non-SAML)" à la page 171.

   Se reporter à "Supprimer un utilisateur d'un rôle" à la page 174.
7. Les autorisations relatives aux biens, aux plans de protection et aux informations d'authentification doivent être modifiées directement dans le nœud concerné dans l'interface utilisateur Web.

Supprimer un rôle personnalisé

Remarque : Lorsque vous supprimez un rôle, les utilisateurs auxquels ce rôle est affecté perdent les autorisations correspondantes.

Pour supprimer un rôle personnalisé

1. Connectez-vous à l'interface utilisateur Web NetBackup.
2. Sur le côté gauche, cliquez sur **Sécurité > RBAC**.
3. Cliquez sur l'onglet **Rôles**.
4. Recherchez le rôle personnalisé à supprimer et cochez la case correspondante.
5. Cliquez sur **Supprimer > Oui**.

Afficher les utilisateurs dans RBAC

Vous pouvez afficher les utilisateurs qui ont été ajoutés à RBAC et les rôles auxquels ils sont affectés. La liste **Utilisateurs** est en lecture seule. Pour modifier les utilisateurs affectés à un rôle, vous devez modifier ce dernier.

Afficher les utilisateurs dans RBAC

1. Connectez-vous à l'interface utilisateur Web de NetBackup.
2. Dans le volet gauche, cliquez sur **Sécurité > RBAC**.
3. Cliquez sur l'onglet **Utilisateurs**.
4. La colonne **Rôles** indique chaque rôle auquel l'utilisateur est affecté.

Ajouter un utilisateur à un rôle (non-SAML)

Cette rubrique décrit comment ajouter un utilisateur ou un groupe autre que SAML à un rôle.

Les utilisateurs non-SAML utilisent l'une des méthodes de connexion suivantes : **Connexion à l'aide d'un nom d'utilisateur et d'un mot de passe** ou **Connexion avec une carte à puce**.

Pour ajouter un utilisateur à un rôle (non-SAML)

1. Connectez-vous à l'interface utilisateur Web NetBackup.
2. Dans le volet gauche, cliquez sur **Sécurité > RBAC**.
3. Cliquez sur l'onglet **Rôles**.
4. Cliquez sur le nom du rôle, puis cliquez sur l'onglet **Utilisateurs**.
5. (Conditionnel) Dans la liste **Type de connexion**, sélectionnez une option parmi les suivantes :
   - **Connexion par défaut**. Pour un utilisateur qui se connecte à NetBackup avec son nom d'utilisateur et son mot de passe.

- **Utilisateur de carte à puce**. Pour un utilisateur qui utilise une carte à puce pour se connecter à NetBackup.

Remarque : la liste **Type de connexion** n'est disponible que si une configuration de fournisseur d'identité est disponible pour NetBackup.

6 Entrez le nom de l'utilisateur ou du groupe d'utilisateurs à ajouter.

Pour ce type d'utilisateur	Utilisez ce format	Exemple
Utilisateur ou groupe local	*nom d'utilisateur*	**jane_doe**
	nom du groupe	**admins**
Utilisateur ou groupe Windows	*DOMAINE\nom d'utilisateur*	**WINDOWS\jane_doe**
	DOMAINE\nom du groupe	**WINDOWS\Admins**
Utilisateur ou groupe UNIX	*nom d'utilisateur@domaine*	**john_doe@unix**
	nom du groupe@domaine	**admins@unix**

7 Cliquez sur **Ajouter à la liste**.

8 L'utilisateur doit se déconnecter, puis se reconnecter pour mettre à jour ses autorisations.

Ajout d'un utilisateur de carte à puce à un rôle (non-SAML, sans AD/LDAP)

Cette rubrique explique comment ajouter un utilisateur de carte à puce à un rôle. Dans ce cas, l'utilisateur n'est pas de type SAML et il n'existe aucune association ou mappage de domaine AD ou LDAP. Les groupes d'utilisateurs ne sont pas pris en charge avec ce type de configuration.

Ce type d'utilisateur est spécifique à la méthode de connexion suivante : **Connexion avec une carte à puce**.

Pour ajouter un utilisateur de carte à puce à un rôle (non-SAML, sans AD/LDAP)

1 Connectez-vous à l'interface utilisateur Web NetBackup.

2 Sur le côté gauche, cliquez sur **Sécurité > RBAC**.

3 Cliquez sur l'onglet **Rôles**.

4 Cliquez sur le nom du rôle, puis cliquez sur l'onglet **Utilisateurs**.

5 (Conditionnel) Dans la liste **Type de connexion**, sélectionnez **Utilisateur de carte à puce**.

Remarque : La liste **Type de connexion** n'est disponible que si une configuration de fournisseur d'identité est disponible pour NetBackup. L'option « utilisateur de carte à puce » est disponible dans la liste **Type de connexion** lorsque la configuration de la carte à puce s'effectue sans mappage de domaine AD ou LDAP.

---

6 Entrez le nom de l'utilisateur à ajouter.

Fournissez le nom commun (CN) exact ou le nom principal universel (UPN) figurant sur le certificat.

7 Cliquez sur **Ajouter à la liste**.

8 L'utilisateur doit se déconnecter, puis se reconnecter pour mettre à jour ses autorisations.

Ajouter un utilisateur à un rôle (SAML)

Cette rubrique décrit comment ajouter un utilisateur ou un groupe SAML à un rôle.

Les utilisateurs SAML utilisent l'une des méthodes de connexion suivantes : **Utilisateur SAML** ou **Groupe SAML**.

Pour ajouter un utilisateur à un rôle (SAML)

1 Connectez-vous à l'interface utilisateur Web NetBackup.

2 Dans le volet gauche, cliquez sur **Sécurité > RBAC**.

3 Cliquez sur l'onglet **Rôles**.

4 Cliquez sur le nom du rôle, puis cliquez sur l'onglet **Utilisateurs**.

5 Dans la liste **Type de connexion**, sélectionnez la méthode de connexion **Utilisateur SAML** ou **Groupe SAML**.

6 Entrez le nom de l'utilisateur ou du groupe d'utilisateurs à ajouter.

Par exemple, nbuadmin@my.host.com.

7 Cliquez sur **Ajouter à la liste**.

8 L'utilisateur doit se déconnecter, puis se reconnecter pour mettre à jour ses autorisations.

Supprimer un utilisateur d'un rôle

Vous pouvez supprimer un utilisateur d'un rôle afin de supprimer des autorisations pour cet utilisateur.

Si un utilisateur est supprimé d'un rôle, il doit se déconnecter et se reconnecter pour mettre à jour ses autorisations.

Supprimer un utilisateur d'un rôle

1. Connectez-vous à l'interface utilisateur Web de NetBackup.
2. Dans le volet gauche, cliquez sur **Sécurité > RBAC**.
3. Cliquez sur l'onglet **Rôles**.
4. Cliquez sur le rôle à modifier, puis sélectionnez l'onglet **Utilisateurs**.
5. Sélectionnez l'utilisateur que vous souhaitez supprimer et cliquez sur **Actions > Supprimer > Supprimer**.

Chapitre 11

Carte à puce ou certificat numérique

Ce chapitre traite des sujets suivants :

Configuration de l'authentification utilisateur avec des cartes à puce ou des certificats numériques

Vous pouvez mapper la carte à puce ou le certificat avec le domaine AD ou LDAP pour la validation de l'utilisateur. Vous pouvez également configurer l'authentification utilisateur par carte à puce ou certificat sans domaine AD ou LDAP.

Se reporter à "Configuration de l'authentification par carte à puce avec domaine" à la page 176.

Se reporter à "Configuration de l'authentification par carte à puce sans domaine" à la page 177.

Configuration de l'authentification par carte à puce avec domaine

Si vous voulez mapper des cartes à puce ou certificats avec domaine AD ou LDAP pour la validation des utilisateurs, ajoutez les domaines AD ou LDAP associés à vos utilisateurs NetBackup. Consultez le Guide de sécurité et de chiffrement NetBackup.

Remarque : Effectuez la configuration du contrôle d'accès basé sur les rôles (RBAC) pour les utilisateurs NetBackup avant de configurer l'authentification par carte à puce ou certificat.

Se reporter à "Configuration de RBAC " à la page 154.

Pour configurer NetBackup de sorte à authentifier les utilisateurs avec une carte à puce ou un certificat numérique

1. Connectez-vous à l'interface utilisateur Web NetBackup.
2. En haut à droite, sélectionnez **Paramètres > Authentification par carte à puce**.
3. Activez l'**authentification par carte à puce**.
4. Sélectionnez le domaine AD ou LDAP requis dans l'option **Sélectionner le domaine**.
5. Sélectionnez un **attribut de mappage du certificat** : Nom commun (CN) ou Nom principal universel (UPN).
6. Facultatif : entrez l'**URI OCSP**.

   Si vous ne fournissez pas l'URI OCSP, l'URI du certificat utilisateur sera utilisé.
7. Cliquez sur **Enregistrer**.
8. À droite des **certificats de l'autorité de certification**, cliquez sur **Ajouter**.
9. Recherchez ou glissez-déplacez les **certificats de l'autorité de certification** et cliquez sur **Ajouter**.

   L'authentification par carte à puce requiert une liste des certificats de l'autorité de certification racine ou intermédiaire approuvés. Ajoutez les certificats de l'autorité de certification qui sont associés aux certificats numériques ou aux cartes à puce de l'utilisateur.

   Le fichier de certificat doit être au format `.crt`, `.cer`, `.der`, `.pem` ou `PKCS #7` et ne doit pas dépasser 64 Mo.

10 Sur la page **Authentification par carte à puce**, vérifiez les informations de configuration.

11 Pour que les utilisateurs puissent utiliser un certificat numérique qui n'est pas installé sur une carte à puce, celui-ci doit être chargé dans le gestionnaire de certificats du navigateur.

Consultez la documentation du navigateur pour obtenir des instructions ou contactez votre administrateur de certificats pour plus d'informations.

12 Lorsque les utilisateurs se connectent, ils voient maintenant une option permettant de **se connecter avec un certificat ou une carte à puce**.

Si vous ne voulez pas que les utilisateurs disposent de cette option de connexion, désactivez **Authentification par carte à puce**. (Par exemple, si les certificats ne sont pas encore configurés sur les hôtes de tous les utilisateurs.) Les paramètres que vous avez configurés sont conservés même si vous désactivez l'authentification par carte à puce.

Pour ces utilisateurs, le nom et le type de domaine sont des cartes à puce.

Configuration de l'authentification par carte à puce sans domaine

Vous pouvez configurer l'authentification utilisateur par carte à puce ou certificat sans valider les utilisateurs avec un domaine AD ou LDAP.

Seuls les utilisateurs sont pris en charge en l'absence de domaine AD ou LDAP pour la validation utilisateur. Les groupes d'utilisateurs ne sont pas pris en charge.

Pour configurer NetBackup de sorte à authentifier les utilisateurs avec une carte à puce ou un certificat numérique sans domaine

1 Connectez-vous à l'interface utilisateur web NetBackup.

2 En haut à droite, sélectionnez **Paramètres > Authentification par carte à puce**.

3 Activez l'**authentification par carte à puce**.

4 (Étape conditionnelle) Si un domaine AD ou LDAP est configuré dans votre environnement, sélectionnez l'option **Continuer sans domaine**.

5 Sélectionnez un **attribut de mappage du certificat** : Nom commun (CN) ou Nom principal universel (UPN).

6 Facultatif : entrez l'**URI OCSP**.

Si vous ne fournissez pas l'URI OCSP, l'URI du certificat utilisateur sera utilisé.

7 Cliquez sur **Enregistrer**.

8 À droite des **certificats de l'autorité de certification**, cliquez sur **Ajouter**.

9 Recherchez ou glissez-déplacez les **certificats de l'autorité de certification** et cliquez sur **Ajouter**.

10 L'authentification par carte à puce requiert une liste des certificats de l'autorité de certification racine ou intermédiaire approuvés. Ajoutez les certificats de l'autorité de certification qui sont associés aux certificats numériques ou aux cartes à puce de l'utilisateur.

Le fichier de certificat doit être au format `.crt`, `.cer`, `.der`, `.pem` ou `PKCS #7` et ne doit pas dépasser 64 Mo.

11 Sur la page **Authentification par carte à puce**, vérifiez les informations de configuration.

Pour que les utilisateurs puissent utiliser un certificat numérique qui n'est pas installé sur une carte à puce, celui-ci doit être chargé dans le gestionnaire de certificats du navigateur.

Consultez la documentation du navigateur pour obtenir des instructions ou contactez votre administrateur de certificats pour plus d'informations.

https://iase.disa.mil/pki-pke/Pages/web-browsers.aspx

12 Lorsque les utilisateurs se connectent, ils voient maintenant une option permettant de **se connecter avec un certificat ou une carte à puce**.

Si vous ne voulez pas que les utilisateurs disposent de cette option de connexion, désactivez **Authentification par carte à puce**. (Par exemple, si les certificats ne sont pas encore configurés sur les hôtes de tous les utilisateurs.) Les paramètres que vous avez configurés sont conservés même si vous désactivez l'authentification par carte à puce.

Modifier la configuration pour l'authentification par carte à puce

Si la configuration de l'authentification par carte à puce change, vous pouvez en modifier les détails.

Pour modifier la configuration de l'authentification utilisateur avec domaine

1 Connectez-vous à l'interface utilisateur Web NetBackup.

2 En haut à droite, sélectionnez **Paramètres > Authentification par carte à puce**.

3 Vous pouvez modifier la sélection de domaine AD ou LDAP dans les cas suivants :

- Pour sélectionner un domaine différent du domaine existant.
- Le domaine existant est supprimé et vous voulez sélectionner un nouveau domaine.
- Vous voulez continuer sans le domaine.

Cliquez sur **Modifier**.

4 Sélectionnez un domaine.

Seuls les domaines qui sont configurés pour NetBackup apparaissent dans cette liste.

Si vous ne voulez pas valider les utilisateurs avec domaine, vous pouvez sélectionner **Continuer sans domaine**.

5 Modifiez l'**attribut de mappage du certificat**.

6 Laissez le champ **URI OCSP** vide pour utiliser la valeur **URI** du certificat de l'utilisateur. Sinon, indiquez l'URI à utiliser.

Ajout ou suppression d'un certificat de l'autorité de certification utilisé pour l'authentification par carte à puce

Ajout d'un certificat de l'autorité de certification

L'authentification par carte à puce requiert une liste des certificats de l'autorité de certification racine ou intermédiaire approuvés. Ajoutez les certificats de l'autorité de certification qui sont associés aux certificats numériques de l'utilisateur ou aux cartes à puce.

Pour ajouter un certificat de l'autorité de certification

1 Connectez-vous à l'interface utilisateur Web de NetBackup.

2 En haut à droite, sélectionnez **Paramètres > Authentification par carte à puce**.

3 Cliquez sur **Ajouter**.

4 Recherchez ou faites glisser les **certificats de l'autorité de certification**. Cliquez ensuite sur **Ajouter**.

L'authentification par carte à puce requiert une liste des certificats de l'autorité de certification racine ou intermédiaire approuvés. Ajoutez les certificats de l'autorité de certification qui sont associés aux certificats numériques de l'utilisateur ou aux cartes à puce.

Les types de fichiers de certificat doivent être au format `DER`, `PEM` ou `PKCS #7` et ne doivent pas dépasser 1 Mo.

Suppression d'un certificat de l'autorité de certification

Vous pouvez supprimer un certificat de l'autorité de certification s'il n'est plus utilisé pour l'authentification par carte à puce. Si un utilisateur tente d'utiliser le certificat de carte à puce ou le certificat numérique associé, il n'est pas en mesure de se connecter à NetBackup.

Pour supprimer un certificat de l'autorité de certification

1 Connectez-vous à l'interface utilisateur Web de NetBackup.

2 En haut à droite, sélectionnez **Paramètres > Authentification par carte à puce**.

3 Sélectionnez les certificats de l'autorité de certification que vous voulez supprimer.

4 Cliquez sur **Supprimer > Supprimer**.

Désactivation ou désactivation temporaire de l'authentification par carte à puce

Vous pouvez désactiver l'authentification par carte à puce si vous ne voulez plus utiliser cette méthode d'authentification pour le serveur principal. Il en est de même si vous avez besoin d'effectuer toute autre configuration pour que les utilisateurs puissent utiliser les cartes à puce.

Pour désactiver l'authentification par carte à puce

1. Connectez-vous à l'interface utilisateur Web de NetBackup.
2. En haut à droite, sélectionnez **Paramètres > Authentification par carte à puce**.
3. Désactivez l'option **Authentification par carte à puce**.

   Les paramètres que vous avez configurés sont conservés même si vous désactivez l'authentification par carte à puce.

Chapitre 12

Authentification unique (SSO)

Ce chapitre traite des sujets suivants :

À propos de la configuration de l'authentification unique (SSO)

Vous pouvez configurer l'authentification unique avec n'importe quel fournisseur d'identité qui utilise le protocole SAML 2.0 pour l'échange des informations d'authentification et d'autorisation. Notez que vous pouvez configurer un fournisseur d'identité avec plusieurs produits Veritas. Par exemple, le même fournisseur d'identité peut être configuré avec NetBackup et avec APTARE.

Notez les conditions requises et limitations suivantes :

- Pour utiliser l'authentification SSO, le fournisseur d'identité configuré dans votre environnement doit être compatible avec le protocole SAML 2.0.
- Seuls les fournisseurs d'identité qui utilisent les services d'annuaire AD ou LDAP sont pris en charge.
- La configuration du fournisseur d'identité requiert les API NetBackup ou la commande NetBackup`nbidpcmd`.
- Les utilisateurs SAML ne peuvent pas utiliser les API. Les clés d'API sont utilisées pour authentifier un utilisateur et ne peuvent pas être utilisées avec un utilisateur authentifié via SAML.
- La déconnexion globale n'est pas prise en charge.

Configurer NetBackup pour l'authentification unique (SSO)

Cette section décrit la procédure de paramétrage des informations de configuration de la relation de confiance et des échanges entre le fournisseur d'identité et le serveur principal NetBackup. Avant de poursuivre, vérifiez que votre environnement remplit les conditions suivantes :

- Un fournisseur d'identité est configuré et déployé dans votre environnement.
- Le fournisseur d'identité est configuré pour authentifier les utilisateurs de domaine Active Directory (AD) ou LDAP (Lightweight Directory Access Protocol).

Tableau 12-1 Procédure de configuration de NetBackup pour l'authentification unique (SSO)

Étape	Action	Description
1.	Téléchargez le fichier XML de métadonnées du fournisseur d'identité	Téléchargez et enregistrez le fichier XML de métadonnées du fournisseur d'identité à partir du fournisseur d'identité. Les métadonnées SAML stockées dans les fichiers XML sont utilisées pour partager des informations de configuration entre le fournisseur d'identité et le serveur principal NetBackup. Le fichier XML de métadonnées du fournisseur d'identité est utilisé pour ajouter la configuration du fournisseur d'identité sur le serveur principal NetBackup.
2.	Configuration du keystore SAML et ajout et activation de la configuration du fournisseur d'identité sur le serveur principal NetBackup	Se reporter à "Configuration du keystore SAML" à la page 184. Se reporter à "Configuration du keystore SAML et ajout et activation de la configuration du fournisseur d'identité" à la page 188.

Étape	Action	Description
3.	Téléchargez le fichier XML de métadonnées du fournisseur de services	Le serveur principal NetBackup est le fournisseur de services dans l'environnement NetBackup. Pour accéder au fichier XML de métadonnées du fournisseur de services à partir du serveur principal NetBackup, entrez l'URL suivante dans votre navigateur : `https://masterserver/netbackup/sso/saml2/metadata` Où *masterserver* est l'adresse IP ou le nom d'hôte du serveur principal NetBackup.
4.	Inscrivez le serveur principal NetBackup en tant que fournisseur de services auprès du fournisseur d'identité	Se reporter à "Inscrire le serveur principal NetBackup auprès du fournisseur d'identité" à la page 190.
5.	Ajoutez des utilisateurs et des groupes SAML qui utilisent l'authentification SSO pour les rôles RBAC nécessaires.	Les utilisateurs et groupes d'utilisateurs SAML sont disponibles dans RBAC uniquement si le fournisseur d'identité est configuré et activé sur le serveur principal NetBackup. Pour connaître la procédure d'ajout de rôles RBAC, consultez la rubrique suivante. Se reporter à "Ajouter un utilisateur à un rôle (non-SAML)" à la page 171.

Après l'installation initiale, vous pouvez activer, mettre à jour, désactiver ou supprimer la configuration du fournisseur d'identité.

Se reporter à "Gérer la configuration d'un fournisseur d'identité" à la page 191.

Après l'installation initiale, vous pouvez mettre à jour, renouveler ou supprimer le keystore SAML de l'autorité de certification NetBackup. Vous pouvez également configurer et gérer le keystore SAML de l'autorité de certification externe.

Configuration du keystore SAML

Pour établir une relation de confiance entre le serveur principal NetBackup et le serveur de fournisseur d'identité, vous devez configurer un keystore SAML sur le serveur principal NetBackup. Selon que vous utilisez l'autorité de certification NetBackup ou une autorité de certification externe (ECA), reportez-vous à l'une des sections suivantes :

Remarque : Si vous utilisez une combinaison autorité de certification externe et autorité de certification NetBackup dans votre environnement, par défaut, l'autorité de certification externe est utilisée lors de l'établissement de la relation de confiance avec le serveur de fournisseur d'identité.

Remarque : La configuration du keyStore SAML à l'aide de fichiers batch, tels que `configureCerts.bat`, `configureCerts`, `configureSAMLECACert.bat`, `configureSAMLECACert` et leurs options correspondantes est obsolète.

Configuration d'un keystore d'autorité de certification NetBackup

Si vous utilisez l'autorité de certification NetBackup, créez le keystore d'autorité de certification NetBackup sur le serveur principal NetBackup.

Pour créer un keystore d'autorité de certification NetBackup

1. Connectez-vous au serveur principal NetBackup en tant qu'utilisateur racine ou administrateur.
2. Exécutez la commande suivante :

   ```
   nbidpcmd -cCert -M master_server -f
   ```

   `-f` est facultative. Utilisez l'option pour forcer la mise à jour.

Une fois le keystore de l'autorité de certification NetBackup créée, mettez à jour le keystore d'autorité de certification NetBackup à chaque renouvellement du certificat de l'autorité de certification NetBackup.

Pour renouveler le keystore d'autorité de certification NetBackup

1. Connectez-vous au serveur principal NetBackup en tant qu'utilisateur racine ou administrateur.
2. Exécutez la commande suivante :

   ```
   nbidpcmd -rCert -M master_server
   ```

3 Pour télécharger le nouveau fichier XML de métadonnées du fournisseur de services à partir du serveur principal NetBackup, entrez l'URL suivante dans votre navigateur :

   https://*primaryserver*/netbackup/sso/saml2/metadata

   Où *primaryserver* est l'adresse IP ou le nom d'hôte du serveur principal NetBackup.

4 Chargez le nouveau fichier XML de métadonnées du fournisseur de services sur le fournisseur d'identité.

   Se reporter à "Inscrire le serveur principal NetBackup auprès du fournisseur d'identité" à la page 190.

Pour supprimer le keystore d'autorité de certification NetBackup

1 Connectez-vous au serveur principal NetBackup en tant qu'utilisateur racine ou administrateur.

2 Exécutez la commande suivante

```
nbidpcmd -dCert -M master_server
```

3 Pour télécharger le nouveau fichier XML de métadonnées du fournisseur de services à partir du serveur principal NetBackup, entrez l'URL suivante dans votre navigateur :

   https://*primaryserver*/netbackup/sso/saml2/metadata

   Où *primaryserver* est l'adresse IP ou le nom d'hôte du serveur principal NetBackup.

4 Chargez le nouveau fichier XML de métadonnées du fournisseur de services sur le fournisseur d'identité.

5 Se reporter à "Inscrire le serveur principal NetBackup auprès du fournisseur d'identité" à la page 190.

Configuration d'un keystore d'autorité de certification externe (ECA)

Si vous utilisez une autorité de certification externe, importez le keystore d'autorité de certification externe sur le serveur principal NetBackup.

Remarque : Si vous utilisez une combinaison autorité de certification externe et autorité de certification NetBackup dans votre environnement, par défaut, l'autorité de certification externe est utilisée lors de l'établissement de la relation de confiance avec le serveur de fournisseur d'identité. Pour utiliser l'autorité de certification NetBackup, vous devez d'abord supprimer le keystore d'autorité de certification externe.

Pour configurer un keystore d'autorité de certification externe

1. Connectez-vous au serveur principal en tant qu'utilisateur racine ou administrateur.
2. Vous pouvez configurer le keystore de l'autorité de certification externe SAML de deux façons, avec le keystore configuré de l'autorité de certification externe NetBackup ou en fournissant la chaîne de certificats de l'autorité de certification externe et la clé privée. Exécutez les commandes suivantes selon la configuration recherchée :
   - Exécutez la commande suivante pour utiliser le keystore configuré par l'autorité de certification externe NetBackup :
     `nbidpcmd -cECACert -uECA` *`existing ECA configuration`* `[-f] [-M` *`primary_server`*`]`
   - Exécutez la commande suivante pour utiliser la chaîne de certificats de l'autorité de certification externe et la clé privée fournies par l'utilisateur :
     `nbidpcmd -cECACert -certPEM` *`certificate chain file`* `-privKeyPath` *`private key file`* `[-ksPassPath` *`Keystore Passkey File`*`] [-f] [-M <master_server>]`
   - Le fichier de chaîne de certificat spécifie le chemin d'accès au fichier de chaîne de certificats. Ce fichier doit être au format PEM et accessible par le serveur principal servant à la configuration.
   - Le fichier de clé privée spécifie le chemin d'accès au fichier de clé privée. Ce fichier doit être au format PEM et accessible par le serveur principal servant à la configuration.
   - Le fichier de clé du keystore spécifie le chemin du fichier de mot de passe du keystore et doit être accessible par le serveur principal servant à la configuration.
   - Le serveur principal correspond au nom d'hôte ou à l'adresse IP du serveur principal sur lequel vous allez configurer le keystore de l'autorité de certification externe SAML. Le serveur principal NetBackup sur lequel vous exécutez la commande est sélectionné par défaut.

Pour supprimer le keystore d'autorité de certification externe

1. Connectez-vous au serveur principal en tant qu'utilisateur racine ou administrateur.
2. Pour télécharger le nouveau fichier XML de métadonnées du fournisseur de services à partir du serveur principal NetBackup, entrez l'URL suivante dans votre navigateur :

   https://*primaryserver*/netbackup/sso/saml2/metadata

   Où *primaryserver* est l'adresse IP ou le nom d'hôte du serveur principal NetBackup.
3. Chargez le nouveau fichier XML de métadonnées du fournisseur de services sur le fournisseur d'identité.

   Se reporter à "Inscrire le serveur principal NetBackup auprès du fournisseur d'identité" à la page 190.

Configuration du keystore SAML et ajout et activation de la configuration du fournisseur d'identité

Avant de passer aux étapes suivantes, vous devez télécharger le fichier XML de métadonnées du fournisseur d'identité et l'enregistrer sur le serveur principal NetBackup.

Pour configurer le keystore SAML et ajouter et activer une configuration du fournisseur d'identité

1. Connectez-vous au serveur principal en tant qu'utilisateur racine ou administrateur.
2. Exécutez la commande suivante.

   Pour la configuration du fournisseur d'identité et du keystore SAML de l'autorité de certification NetBackup :

   ```
   nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file
   [-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user
   group field] [-cCert] [-f] [-M primary server]
   ```

   D'autre part, pour la configuration du fournisseur d'identité et du keystore SAML de l'autorité de certification externe :

   Vous pouvez configurer le keystore de l'autorité de certification externe SAML de deux façons, avec le keystore configuré de l'autorité de certification externe NetBackup ou en fournissant la chaîne de certificats de l'autorité de certification externe et la clé privée. Exécutez les commandes suivantes selon la configuration recherchée :

- Utilisation du keystore configuré par l'autorité de certification externe de NetBackup :

  `nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user group field] -cECACert -uECA existing ECA configuration [-f] [-M Primary Server]`

- Utilisation de la chaîne de certificats de l'autorité de certification externe et de la clé privée fournie par l'utilisateur :

  `nbidpcmd -ac -n IDP configuration name -mxp IDP XML metadata file[-t SAML2] [-e true | false] [-u IDP user field] [-g IDP user group field] -cECACert -certPEM certificate chain file -privKeyPath private key file [-ksPassPath KeyStore passkey file] [-f] [-M primary server]`

Remplacez les variables comme suit :

- *`IDP configuration name`* est un nom unique attribué à la configuration du fournisseur d'identité.
- *`IDP XML metadata file`* est le chemin d'accès au fichier XML de métadonnées, qui contient les détails de la configuration du fournisseur d'identité codés au format Base64URL.
- `-e true | false` active ou désactive la configuration du fournisseur d'identité. La configuration d'un fournisseur d'identité doit être ajoutée et activée, sans quoi, les utilisateurs ne pourront pas se connecter à l'aide de l'option Authentification unique (SSO). Il est possible d'ajouter plusieurs configurations de fournisseur d'identité sur un serveur principal NetBackup, mais vous ne pouvez en activer qu'une à la fois.
- *`IDP user field`* et *`IDP user group field`* sont les noms d'attribut SAML, qui sont mappés vers les attributs `userPrincipalName` et `memberOf` du domaine AD ou LDAP.

  Remarque : Assurez-vous que les noms d'attribut SAML sont définis au format ***nom d'utilisateur@nom du domaine*** et **(CN =*nom du groupe*, DC =*nom du domaine*)** respectivement.

- *`primary Server`* est le nom d'hôte ou l'adresse IP du serveur principal pour lequel vous voulez ajouter ou modifier la configuration du fournisseur d'identité. Le serveur principal NetBackup sur lequel vous exécutez la commande est sélectionné par défaut.

- *Certificate Chain File* correspond au chemin d'accès du fichier de chaîne de certificats. Ce fichier doit être au format PEM et accessible par le serveur principal servant à la configuration.

  Private Key File désigne le chemin d'accès au fichier de clé privée. Ce fichier doit être au format PEM et accessible par le serveur principal servant à la configuration.

  KeyStore Passkey File spécifie le chemin du fichier de mot de passe du keystore et doit être accessible par le serveur principal servant à la configuration.

Par exemple :`nbidpcmd -ac -n veritas_configuration -mxp file.xml -t SAML2 -e true -u username -g group-name -cCert -M primary_server.abc.com`

Inscrire le serveur principal NetBackup auprès du fournisseur d'identité

Le serveur principal NetBackup doit être inscrit en tant que fournisseur de services auprès du fournisseur d'identité. Pour connaître la procédure spécifique à un fournisseur d'identité particulier, consultez le tableau suivant :

Tableau 12-2 Procédure spécifique au fournisseur d'identité pour l'inscription du serveur principal NetBackup

Nom du fournisseur d'identité	Lien vers la procédure
ADFS	https://www.veritas.com/docs/100047744
Okta	https://www.veritas.com/docs/100047745
PingFederate	https://www.veritas.com/docs/100047746
Azure	https://www.veritas.com/docs/100047748
Shibboleth	https://www.veritas.com/docs/00047747

L'inscription d'un fournisseur de services auprès d'un fournisseur d'identité implique généralement les opérations suivantes :

Chargement du fichier XML de métadonnées du fournisseur de services dans le fournisseur d'identité

Le fichier XML de métadonnées du fournisseur de services contient le certificat, l'ID d'entité, l'URL du service consommateur d'assertion (URL ACS) et une URL

de déconnexion (SingleLogoutService). Le fichier XML de métadonnées du fournisseur de services est requis par le fournisseur d'identité pour établir la confiance et échanger des informations d'authentification et d'autorisation avec le fournisseur de services.

Mappage des attributs SAML vers leurs attributs AD ou LDAP

Les mappages d'attributs sont utilisés pour mapper les attributs SAML dans la configuration SSO avec ses attributs correspondants dans le répertoire AD ou LDAP. Les mappages d'attributs SAML sont utilisés pour générer des réponses SAML qui sont envoyées au serveur principal NetBackup. Veillez à définir des attributs SAML qui mappent vers `userPrincipalName` et les attributs `memberOf` et dans le répertoire AD ou LDAP. Les attributs SAML doivent respecter les formats suivants :

Tableau 12-3

Attribut AD ou LDAP correspondant	Format d'attribut SAML
`userPrincipalName`	***nom_utilisateur@nom_domaine***
`memberOf`	**(CN =*nom du groupe*, DC =*nom du domaine*)**

Remarque : lors de l'ajout de la configuration du fournisseur d'identité sur le serveur principal NetBackup, les valeurs saisies pour les options d'utilisateur (`-u`) et de groupe d'utilisateurs (`-g`) doivent correspondre aux noms d'attribut SAML mappés aux attributs `userPrincipalName` et `memberOf` dans AD ou LDAP.

Se reporter à "Configuration du keystore SAML et ajout et activation de la configuration du fournisseur d'identité" à la page 188.

Gérer la configuration d'un fournisseur d'identité

Vous pouvez gérer les configurations de fournisseur d'identité sur le serveur principal NetBackup à l'aide des options d'activation (`-e true`), de mise à jour (`-uc`), de désactivation (`-e false`) et de suppression (`-dc`) de la commande `nbidpcmd`.

Activer la configuration d'un fournisseur d'identité

Par défaut, aucune configuration de fournisseur d'identité n'est activée dans l'environnement du produit. Si vous n'avez pas activé le fournisseur d'identité lors

de son ajout, vous pouvez utiliser les options `-uc -e true` pour mettre à jour et activer sa configuration.

Pour activer la configuration d'un fournisseur d'identité

1. Connectez-vous au serveur principal en tant qu'utilisateur racine ou administrateur.
2. Exécutez la commande suivante :

   `nbidpcmd -uc -n` *`IDP configuration name`* `-e true`

   `IDP configuration name` est un nom unique attribué à la configuration du fournisseur d'identité.

Remarque : Il est possible de configurer plusieurs fournisseurs d'identité sur un serveur principal NetBackup, mais vous ne pouvez en activer qu'un à la fois.

Mettre à jour la configuration d'un fournisseur d'identité

Vous pouvez mettre à jour le fichier XML de métadonnées associé à la configuration d'un fournisseur d'identité.

Pour mettre à jour le fichier XML de métadonnées d'un fournisseur d'identité dans sa configuration

1. Connectez-vous au serveur principal en tant qu'utilisateur racine ou administrateur.
2. Exécutez la commande suivante :

   `nbidpcmd -uc -n` *`IDP configuration name`* `-mxp` *`IDP XML metadata file`*

   Remplacez les variables comme suit :

   - *`IDP configuration name`* est un nom unique attribué à la configuration du fournisseur d'identité.
   - *`IDP XML metadata file`* est le chemin d'accès au fichier XML de métadonnées, qui contient les détails de la configuration du fournisseur d'identité codés au format Base64URL.

Pour actualiser les valeurs associées à un utilisateur ou groupe d'utilisateurs dans la configuration d'un fournisseur d'identité, vous devez d'abord supprimer cette dernière. L'option Authentification unique (SSO) n'est pas disponible pour les utilisateurs tant que vous n'avez pas ré-ajouté la configuration avec les nouvelles valeurs associées à l'utilisateur ou au groupe d'utilisateurs du fournisseur d'identité.

Pour mettre à jour l'utilisateur ou le groupe d'utilisateurs d'un fournisseur d'identité dans sa configuration

1. Connectez-vous au serveur principal en tant qu'utilisateur racine ou administrateur.
2. Supprimez la configuration du fournisseur d'identité.

   `nbidpcmd -dc -n` *`IDP configuration name`*

   `IDP configuration name` est un nom unique attribué à la configuration du fournisseur d'identité.
3. Pour ajouter et activer de nouveau la configuration, exécutez la commande suivante :

   `nbidpcmd -ac -n` *`IDP configuration name`* `-mxp` *`IDP XML metadata file`* `[-t SAML2] [-e true | false] [-u` *`IDP user`*`] [-g` *`IDP user group field`*`] [-M` *`Master Server`*

   Remplacez les variables comme suit :

   - *`IDP configuration name`* est un nom unique attribué à la configuration du fournisseur d'identité.
   - *`IDP XML metadata file`* est le chemin d'accès au fichier XML de métadonnées, qui contient les détails de la configuration du fournisseur d'identité codés au format Base64URL.
   - `-e true | false` active ou désactive la configuration du fournisseur d'identité. Un fournisseur d'identité doit être disponible et activé, sans quoi, les utilisateurs ne pourront pas se connecter à l'aide de l'option Authentification unique (SSO). Il est possible d'ajouter plusieurs configurations de fournisseur d'identité sur un serveur principal NetBackup, mais vous ne pouvez en activer qu'une à la fois.
   - *`IDP user field`* et *`IDP user group field`* sont les noms d'attribut SAML, qui sont mappés vers les attributs `userPrincipalName` et `memberOf` du domaine AD ou LDAP.

     Remarque : Assurez-vous que les noms d'attribut SAML sont définis au format ***nom d'utilisateur@nom du domaine*** et **(CN =*nom du groupe*, DC =*nom du domaine*)** respectivement.

   - *`Master Server`* est le nom d'hôte ou l'adresse IP du serveur principal sur lequel vous voulez ajouter ou modifier la configuration du fournisseur d'identité. Le serveur principal NetBackup sur lequel vous exécutez la commande est sélectionné par défaut.

Désactiver la configuration d'un fournisseur d'identité

Si une configuration de fournisseur d'identité est désactivée dans l'environnement du produit, l'option Authentification unique de ce fournisseur d'identité n'est pas disponible pour les utilisateurs lorsqu'ils se connectent.

Pour désactiver la configuration d'un fournisseur d'identité

1. Connectez-vous au serveur principal en tant qu'utilisateur racine ou administrateur.
2. Exécutez la commande suivante :

   ```
   nbidpcmd -uc -n IDP configuration name -e false
   ```

   IDP configuration name est un nom unique attribué à la configuration du fournisseur d'identité.

Supprimer la configuration d'un fournisseur d'identité

Si la configuration d'un fournisseur d'identité est supprimée, l'option Authentification unique (SSO) n'est pas disponible pour les utilisateurs lorsqu'ils se connectent.

Pour supprimer la configuration d'un fournisseur d'identité

1. Connectez-vous au serveur principal en tant qu'utilisateur racine ou administrateur.
2. Exécutez la commande suivante :

   ```
   nbidpcmd -dc -n IDP configuration name
   ```

   IDP configuration name est un nom unique attribué à la configuration du fournisseur d'identité.

Chapitre 13

Audit amélioré

Ce chapitre traite des sujets suivants :

À propos de l'audit amélioré

Avec l'audit amélioré, les administrateurs NetBackup peuvent déléguer les droits administrateur NetBackup à d'autres utilisateurs désignés. La fonction permet ainsi aux utilisateurs non-racine de gérer NetBackup. Les journaux d'audit saisissent des informations sur l'utilisateur actif qui apporte des modifications à l'environnement NetBackup. Elles aident les sociétés à suivre les informations de clés au sujet de l'activité utilisateur qui est importante pour les exigences de conformité d'audit. En particulier, il s’agit d’une fonction que les clients des secteurs fortement réglementés trouvent utile.

L’audit amélioré n’est pas pris en charge sur les appliances NetBackup, NetBackup Flex Scale et sur les appliances Flex.

Remarque : Tout échec d’autorisation est également audité à l’aide de l’audit amélioré.

Par défaut, seul un utilisateur racine ou un administrateur peut exécuter des opérations NetBackup par le biais de l'interface de ligne de commande. Cependant, avec NetBackup configuré pour l'audit amélioré et avec les droits administrateur NetBackup appropriés, les utilisateurs peuvent exécuter des opérations NetBackup par le biais de l'interface de ligne de commande. L'audit amélioré fournit le contrôle d'accès brut où l'utilisateur est un administrateur ou non.

Remarque : NBAC et l'audit amélioré sont des fonctions qui s'excluent mutuellement.

Remarque : Pour l'instant, la prise en charge de l'audit amélioré est disponible pour les opérations de l'utilisateur telles que les politiques NetBackup, les travaux, les unités de stockage, les pools de disques, les serveurs de stockage, les catalogues et les propriétés d'hôte, le déploiement de certificat et la génération de jeton.

Le tableau suivant présente les commandes où les actions de l'utilisateur sont auditées avec l'audit amélioré :

Tableau 13-1 Commandes et catégories prises en charge pour l'audit amélioré

Catégorie	Commandes
Politique	`bpplcatdrinfo, bpplclients, bppldelete, bpplinclude, bpplinfo, bppllist, bpplsched, bpplschedrep, bpplschedwin, bpplvalid, bppolicynew`
Travaux	`bpdbjobs`
Unité de stockage	`bpstuadd, bpstuddel, bpsturep, bpstulist`
Pool de disques	`nbdevconfig and nbdevquery`
Serveurs de stockage	`nbdevconfig and nbdevquery`
Catalogues	`bpexpdate, bpcatlist, bpimmedia, bpimagelist, bpverify, and nbdeployutil`
Propriétés de l'hôte	`bpconfig, bpsetconfig, bpgetconfig, nbsetconfig, nbgetconfig, and nbemmcmd`
Jetons de sécurité	`createToken, deleteToken, and cleanupToken`
Certificats	`getCertificate, revokeCertificate, signCertificate, and renewCertificate`

Activation de l'audit amélioré

Utilisez la procédure suivante pour activer l'audit amélioré.

Pour configurer NetBackup pour l'audit amélioré

1 Exécutez la commande `bpnbaz -SetupExAudit` sur le serveur maître.

Remarque : Dans une installation de NetBackup en cluster, tandis que vous configurez NetBackup pour activer l'audit amélioré, vous devez exécuter la commande `bpnbaz -SetupExAudit` uniquement sur le nœud actif.

---

2 Redémarrez les services NetBackup.

Se reporter à "Désactivation de l'audit amélioré" à la page 201.

Se reporter à "Configuration d'audit amélioré" à la page 197.

Configuration d'audit amélioré

Vous devez effectuer quelques étapes de configuration supplémentaires pour certains scénarios relatifs à l'audit amélioré. Ces étapes s'appliquent lorsque vous exécutez une opération de changement de serveur.

- Un certificat de sécurité est obligatoire quand vous vous connectez à un serveur de médias via la **Console d'administration NetBackup**.
  Se reporter à "Connexion à un serveur de médias avec l'audit amélioré" à la page 197.
- Quand vous changez de serveur, d'un serveur maître à un autre serveur maître, vous devez exécuter des étapes supplémentaires sur le serveur maître.
  Se reporter à "Modification d'un serveur sur les domaines NetBackup" à la page 198.

Connexion à un serveur de médias avec l'audit amélioré

Pour l'audit amélioré, un certificat de sécurité est obligatoire quand un utilisateur souhaite se connecter à un serveur de médias via la Console d'administration NetBackup. Des étapes supplémentaires doivent être exécutées sur le serveur maître pour obtenir le certificat pour chaque serveur de médias. Consultez la procédure suivante pour plus de détails :

Pour générer un certificat de sécurité pour un serveur

1. Exécutez la commande `bpnbaz -ProvisionCert target.server.com` sur le serveur maître. Ici, `target.server.com` correspond au nom du serveur de médias.

   Exemple d'utilisation : `acme.domain.mycompany.com` est un serveur de médias auquel un utilisateur souhaite apporter une modification de serveur

   Exécutez la commande `bpnbaz -ProvisionCert acme.domain.mycompany.com` sur le serveur maître.

   Voici un exemple de sortie :

   ```
   bpnbaz -ProvisionCert acme.domain.mycompany.com

   Setting up security on target host: acme.domain.mycompany.com

   Certificate deployed successfully

   Operation completed successfully.
   ```

2. Redémarrez toujours les services sur les serveurs de médias après avoir généré un certificat.

Remarque : La génération d'un certificat de sécurité est une activité ponctuelle.

Modification d'un serveur sur les domaines NetBackup

Pour l'audit amélioré, quand vous exécutez une opération de modification de serveur à partir d'un serveur maître ou de médias dans un domaine NetBackup vers un hôte (serveur maître ou de médias ou client) dans un autre domaine NetBackup, vous devez exécuter les étapes supplémentaires sur chaque serveur NetBackup. Vous devez également installer une confiance sur les deux serveurs maîtres.

Remarque : L'exécution de ces étapes est une activité ponctuelle.

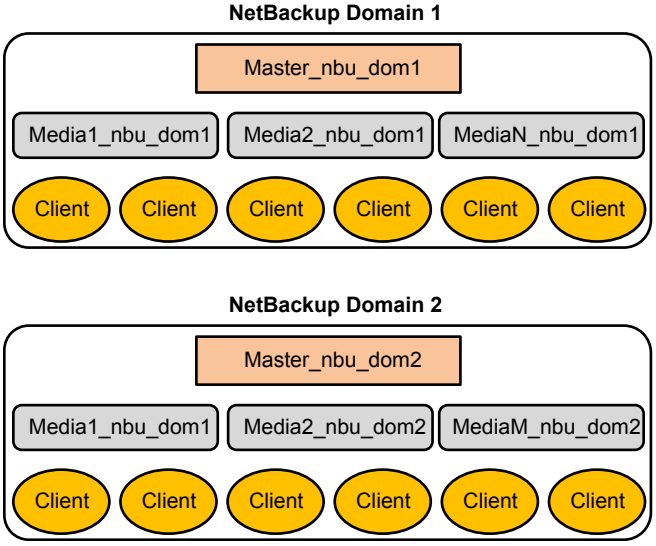
Les étapes suivantes vous aident à modifier le serveur et à installer la confiance sur les deux serveurs maîtres.

Pour passer d'un serveur maître à un autre serveur maître

1. Nous avons deux domaines NetBackup, `NetBackup Domain 1` et `NetBackup Domain 2`.

   Tenez compte de deux serveurs maîtres, `Master_nbu_dom1` et `Master_nbu_dom2`. `Master_nbu_dom1` a des serveurs de médias `Media1_nbu_dom1`, `Media2_nbu_dom1`, `MediaN_nbu_dom1` et un ensemble de

clients. De même, `Master_nbu_dom2` a des serveurs de médias `Media1_nbu_dom2`, `Media2_nbu_dom2`, `MediaM_nbu_dom2` et un ensemble de clients, comme indiqué dans l'image :



L'utilisateur est connecté à l'un des serveurs dans `NetBackup Domain 1` (maître ou de médias), par exemple, `Master_server_nbu_dom1`, et souhaite changer de serveur pour l'un des hôtes dans NetBackup Domain 2, par exemple `Host_nbu_dom2`. Il est obligatoire que les deux serveurs maîtres (ici `Master_nbu_dom1` et `Master_nbu_dom2`) établissent une confiance. `Host_nbu_dom2` doit établir une confiance avec `Master_server_nbu_dom1`.

2 Pour installer la confiance, vous devez appeler un ensemble de commandes sous UNIX et Windows :

Sous UNIX et Linux :

```
/usr/openv/netbackup/sec/at/bin/vssat setuptrust -b
Master_server_nbu_dom1:1556:nbatd -s high on Host_nbu_dom2.
```

Sous Windows :

```
install_path\NetBackup\sec\at\bin\vssat.bat
```

3 Vous devez ajouter une entrée de serveur supplémentaire dans Host_nbu_dom2 pour Master_server_nbu_dom1 dans le fichier bp.conf. Exécutez la commande suivante :

```
SERVER = Master_server_nbu_dom1 /*this should __not__ be the first
SERVER entry*/
```

Vous pouvez également ajouter l'entrée de serveur supplémentaire en vous connectant au serveur maître de via la console d'administration NetBackup.

4 L'hôte qui dispose de la console d'administration NetBackup ou de la console d'administration à distance doit également approuver le certificat X.509 NBATD sur `Master_server_nbu_dom2`.

La confiance peut être installée en se connectant directement au serveur maître `Master_server_nbu_dom2`via l'interface graphique utilisateur.

Vous pouvez également appeler `/usr/openv/java/sec/at/bin/vssat setuptrust -b`

`Master_server_nbu_dom2:1556:nbatd -s high` sur l'hôte de la console d'administration NetBackup.

Conditions requises en cas d'utilisation de Changer de serveur avec NBAC ou l'audit amélioré

Une configuration supplémentaire est requise pour exécuter l'opération Changer de serveur si NetBackup Access Control ou l'audit amélioré est utilisé.

Les étapes suivantes supposent que NBAC ou l'audit amélioré est déjà configuré.

Configuration pour la prise en charge de l'opération Changer de serveur : *fromServer - > toServer*

- Ajoutez *fromServer* à la liste Serveurs supplémentaires des propriétés d'hôte sur *toServer*.
- Si *fromServer* et *toServer* sont sur des domaines NetBackup différents (serveurs de médias de serveurs maîtres différents) :
  - Exécutez la commande `vssat` pour installer la confiance entre les serveurs maîtres de *fromServer* et de *toServer*. (Se reporter à "Modification d'un serveur sur les domaines NetBackup" à la page 198. Reportez-vous à l'étape 2 de cette procédure.)
  - Ajoutez le serveur maître de *fromServer* à la liste Serveurs supplémentaires des propriétés d'hôte sur *toServer*.
- Si *fromServer* ou *toServer* sont des serveurs de médias :
  - Exécutez la commande `bpnbaz -ProvisionCert` pour déployer le certificat de sécurité (ordinateur) si nécessaire. (Se reporter à "Connexion à un serveur de médias avec l'audit amélioré" à la page 197.)

Étapes de configuration supplémentaires

Pour utiliser le fichier auth.conf :

- Ajoutez l'entrée `USER` au fichier auth.conf sur chaque serveur.
- Si NBAC est activé, exécutez `nbsetconfig` sur chaque serveur pour ajouter l'entrée : `USE_AUTH_CONF_NBAC = YES`

Pour utiliser Remote Administration Console :

- Installez la confiance avec chaque serveur maître à l'aide de la commande `vssat` ou ouvrez une session explicitement sur chaque serveur au moins une fois. (Se reporter à "Modification d'un serveur sur les domaines NetBackup" à la page 198. Reportez-vous à l'étape 2 de cette procédure.)

Pour dépanner la configuration après l'installation, utilisez `nslookup` et `bptestnetconn -a -s` pour vérifier les communications serveur.

Désactivation de l'audit amélioré

Lorsque vous activez l'audit amélioré, l'option `USE_AUTHENTICATION` est définie sur ON. Pour désactiver l'audit amélioré, vous devez définir l'option `USE_AUTHENTICATION` sur OFF. Les étapes suivantes vous aident :

Pour désactiver l'audit amélioré

1. Exécutez la commande `bpnbaz -DisableExAudit`.
2. Redémarrez les services NetBackup.

Gestion des utilisateurs avec l'audit amélioré

Avec la configuration de NetBackup pour l'audit amélioré, l'administrateur peut :

- Octroyer les droits d'administrateur NetBackup aux utilisateurs et les révoquer.
- Recherchez un utilisateur qui a des droits d'administrateur NetBackup.
- Répertoriez les utilisateurs disposant de droits d'administrateur NetBackup.

Remarque : Seul un utilisateur avec des droits d'administrateur NetBackup peut effectuer des tâches de gestion des utilisateurs.

Utilisez la commande `bpnbaz` pour effectuer des tâches de gestion d'utilisateur. Les commandes d'ajout, de suppression, de recherche et de liste des utilisateurs doivent être exécutées avec les options suivantes :

```
bpnbaz -[AddUser | DelUser] Domain_Type:Domain_Name:User_Name [-M
server] [-credfile][-reason]

bpnbaz -LookupUser Domain_Type:Domain_Name:User_Name [-M server]
[-credfile] bpnbaz -ListUsers [-M server] [-credfile]

bpnbaz -ListUsers Domain_Type:Domain_Name:User_Name [-M server]
[-credfile] bpnbaz -ListUsers [-M server] [-credfile]
```

Le tableau suivant présente des informations sur chaque commande :

Tableau 13-2

Commande	Description	Exemple d'utilisation
-AddUser	Permet à l'utilisateur d'octroyer des droits d'administrateur NetBackup.	`bpnbaz -AddUser unixpwd:v-123790b.punin.sen.veritas.com:Debbie`
-DelUser	Permet à l'utilisateur de révoquer les droits d'administrateur NetBackup.	`bpnbaz -DelUser unixpwd:v-123790b.punin.sen.veritas.com:Debbie`
-LookupUser	Permet à l'utilisateur de rechercher l'utilisateur ou les utilisateurs qui ont des privilèges d'administration.	`bpnbaz -LookupUser unixpwd:v-123790b.punin.sen.veritas.com:Debbie`
-ListUsers	Permet à l'utilisateur de répertorier les utilisateurs disposant de privilèges d'administrateur NetBackup.	`bpnbaz -ListUsers`

Pour plus d'informations sur la commande `bpnbaz`, consultez le Guide de référence des commandes NetBackup.

Authentification utilisateur avec l'audit amélioré

Par défaut, NetBackup n'exige pas l'authentification utilisateur. Cependant, quand NetBackup est configuré pour l'audit amélioré, l'authentification utilisateur à partir du serveur maître est obligatoire.

L'utilisateur doit utiliser la commande `bpnbat -login`pour l'authentification.

Le processus de connexion pour les utilisateurs Windows et UNIX varie.

UNIX

- L'exécution de la commande `bpnbat -login` est obligatoire pour tous les utilisateurs excepté l'utilisateur racine.

Windows

- L'administrateur se connecte automatiquement via l'option Single Sign On (SSO).
- Un utilisateur standard se connecte également via l'option SSO. Mais si l'option SSO échoue, l'utilisateur doit exécuter la commande `bpnbat -login`. L'utilisateur peut également exécuter la commande `bpnbat -GetBrokerCert` pour établir une connexion sécurisée avec le serveur.

Impact de l'audit amélioré sur l'autorisation de la console d'administration NetBackup

L'accès à la ligne de commande et à la console d'administration NetBackup fonctionne différemment quand vous configurez l'audit amélioré. Les entrées dans le fichier `auth.conf` remplacent le contrôle d'accès pour la console d'administration NetBackup.

Se reporter à "Gestion des utilisateurs avec l'audit amélioré " à la page 201.

Si des droits administrateur ont été octroyés à un utilisateur, ce dernier peut exécuter toutes les opérations NetBackup pouvant faire l'objet d'un audit par le biais de l'interface de ligne de commande. Consultez le tableau suivant pour plus d'informations au sujet de l'accès utilisateur :

Tableau 13-3 Accès utilisateur

Entrée authentic.conf	Accès par interface de ligne de commande	Accès à l'interface Java
Debbie a une entrée dans le fichier authentic.conf.	Aucun accès	Accès comme spécifié dans le fichier `auth.conf`
Debbie a des privilèges d'administrateur NetBackup, mais n'a aucune entrée dans le fichier `auth.conf`.	Accès complet	Accès complet

Entrée authentic.conf	Accès par interface de ligne de commande	Accès à l'interface Java
Debbie a des privilèges d'administrateur NetBackup et a également une entrée dans le fichier `auth.conf`.	Accès complet	Accès comme spécifié dans le fichier `auth.conf`
Debbie n'a pas d'entrée dans le fichier `auth.conf` et n'a pas non plus de privilèges d'administrateur NetBackup.	Aucun accès	Aucun accès

Chapitre 14

Sécurité de NetBackup Access Control (NBAC)

Ce chapitre traite des sujets suivants :

À propos de l'utilisation de NBAC (NetBackup Access Control)

NetBackup Access Control (NBAC) est la méthode de contrôle d'accès héritée pour NetBackup et elle n'est plus mise à jour. Il est recommandé d'utiliser le contrôle d'accès basé sur les rôles (RBAC) avec l'interface utilisateur Web.

Le NBAC (NetBackup Access Control) est le contrôle d'accès basé sur rôle qui est utilisé pour les serveurs maîtres, les serveurs de médias et les clients. Vous pouvez utiliser NBAC lorsque vous souhaitez :

- Utiliser un jeu d'autorisations pour différents niveaux d'administrateurs pour une application. Une application de sauvegarde peut posséder des opérateurs (pour charger et décharger les bandes, par exemple). Elle peut posséder des administrateurs locaux (qui gèrent l'application dans un site), et peut également posséder des administrateurs généraux pouvant avoir la responsabilité de plusieurs sites et devant déterminer la politique de sauvegarde. Notez que cette fonction est très utile car elle empêche les erreurs de l'utilisateur. Si des administrateurs débutants ne peuvent réaliser certaines opérations, ils ne peuvent pas non plus commettre des erreurs par inadvertance.
- Séparer les administrateurs de sorte que l'autorisation racine du système ne soit pas requise pour gérer le système. Vous pouvez ensuite séparer les administrateurs des systèmes de ceux administrant les applications.

Le tableau suivant répertorie les considérations NBAC.

Tableau 14-1 Considérations NBAC

Considération ou problème	Description ou résolution
Conditions préalables à la configuration de NBAC	Cette liste de conditions requises peut être utile avant de commencer la configuration de NBAC. Ces éléments assurent une installation plus facile. Les informations relatives à cette installation sont répertoriées ci-dessous : ■ Nom d'utilisateur ou mot de passe du serveur maître (autorisation racine ou administrateur). ■ Nom du serveur maître ■ Nom de tous les serveurs de médias connectés au serveur maître ■ Nom des clients à sauvegarder ■ Nom de l'hôte ou adresse IP **Remarque :** Les noms d'hôte doivent correspondre à une adresse IP valide. ■ Utilisez les commandes `ping` ou `traceroute` comme outils pour garantir que les hôtes sont affichés. Ces commandes garantissent également que vous n'avez pas configuré de pare-feu ou autre obstruction susceptible de bloquer l'accès.
Déterminez si le serveur maître, le serveur de médias ou le client doivent être mis à niveau.	Déterminez si le serveur maître, le serveur de médias ou le client doivent être mis à niveau comme suit : ■ Certaines fonctions sont fournies en mettant à niveau les serveurs maîtres, à l'aide des serveurs de médias ou de mises à niveau des clients. ■ NetBackup fonctionne avec un serveur maître de révision supérieure et des clients et serveurs de médias de révision inférieure. ■ Le contenu des fonctions détermine les éléments déployés. ■ Si nécessaire, le déploiement peut être effectué par étapes.
Informations à propos des rôles	Déterminez le rôle dans la configuration comme suit : ■ Qui gère les hôtes (l'autorisation racine sur le serveur maître correspond à l'administrateur principal). ■ Pour commencer, déterminez des rôles, puis ajoutez des rôles selon les besoins.
Conditions de licence NBAC	Aucune licence n'est requise pour activer les contrôles d'accès.

Considération ou problème	Description ou résolution
Autorisations NBAC et KMS	Généralement, en utilisant NBAC et en exécutant la commande `Setupmaster`, les autorisations du groupe associé à NetBackup (par exemple, NBU_Admin et KMS_Admin) sont créées. Les utilisateurs racines et administrateurs par défaut sont également ajoutés à ces groupes. Dans certains cas, les utilisateurs racines et administrateurs ne sont pas ajoutés au groupe KMS lorsque NetBackup est mis à niveau. La solution consiste à leur accorder des autorisations NBU_Admin et KMS_Admin manuellement.
Messages d'erreur WSFC (Windows Server Failover Clustering) lors du décrochage des services de sécurité partagés de PBX	Dans les environnements MSCS, l'exécution de la commande `bpnbaz -UnhookSharedSecSvcsWithPBX <virtualhostname>` peut déclencher des messages d'erreur. Cependant les services Authentication and Authorization partagés sont décrochés avec succès du PBX et les erreurs peuvent être ignorées.
Erreurs possibles de nœud de cluster	Dans un environnement en cluster, quand la commande `bpnbaz -setupmaster` est exécutée dans le cadre de l'administrateur local, les entrées `AUTHENTICATION_DOMAIN` peuvent ne pas contenir les autres entrées de nœud de cluster. Dans un tel cas, ces entrées doivent être ajoutées manuellement à partir des Propriétés de l'hôte dans le fichier `bp.conf`.
La récupération de catalogue échoue quand NBAC est défini sur le mode **REQUIS**	Si NBAC s'exécute en mode **REQUIS** et qu'une récupération de catalogue a eu lieu, NBAC doit être réinitialisé de nouveau du mode **INTERDIT** au mode **REQUIS**.
La validation de politique échoue en mode NBAC (USE_VXSS = REQUIS)	Les opérations de sauvegarde, restauration et vérification de la politique pour le snapshot peuvent échouer dans le mode NBAC activé si l'une des opérations suivantes a eu lieu. ■ Le principe authentifié est supprimé du groupe NBAC : Groupe NBU_Users ■ Les autorisations de sauvegarde et de restauration du groupe NBU_User ont été supprimées
La commande bpnbaz -setupmaster échoue avec l'erreur « Impossible de contacter le service d'autorisation »	Si un utilisateur autre qu'un administrateur tente de modifier la sécurité de NetBackup, la commande bpnbaz -setupmaster échoue. Seul un administrateur qui fait partie du groupe d'administration dispose d'autorisations pour modifier la sécurité de NetBackup et activer NBAC.

Considération ou problème	Description ou résolution
Echec de configuration du courtier d'authentification lors de l'installation.	La configuration non valide du nom de domaine du système entraîne l'échec pendant la configuration du courtier d'authentification. Pour corriger ce problème, utilisez la commande `bpnbaz -configureauth` pour configurer le courtier d'authentification. Pour plus d'informations sur la commande `bpnbaz`, consultez le *Guide de référence des commandes NetBackup* :
Des erreurs d'interface graphique utilisateur NetBackup peuvent se produire si NBAC est activé sur un système sur lequel l'audit amélioré était précédemment activé.	Lorsque le serveur NetBackup passe de l'audit amélioré à NBAC, assurez-vous que tous les répertoires qui portent le nom des utilisateurs sont supprimés du répertoire suivant : Windows : *`install_path`*`\NetBackup\logs\user_ops` UNIX, Linux : `/usr/openv/netbackup/logs/user_ops` La rubrique suivante contient des détails supplémentaires : Se reporter à "Résolution des problèmes NBAC" à la page 229.

Administration de la gestion de l'accès NetBackup

L'accès à NetBackup peut être contrôlé en définissant des groupes d'utilisateurs et en accordant des autorisations explicites à ces groupes. Vous pouvez configurer les groupes d'utilisateurs et assigner des autorisations. Sélectionnez **Gestion de l'accès** dans la **console d'administration NetBackup**.

Remarque : Pour que la **console d'administration NetBackup** fonctionne, l'utilisateur doit être autorisé à se connecter à distance au système.

Remarque : Si quelques serveurs de médias ne sont pas configurés avec le contrôle d'accès, les utilisateurs non racine/non administrateur ne peuvent pas gérer ces serveurs.

A propose de la configuration de NetBackup Access Control (NBAC)

Remarque : NBAC est déjà installé en tant qu'élément de l'installation de NetBackup. Seule la configuration de NBAC est requise pour cette version.

Les instructions de configuration de NBAC concernent une configuration de NBAC dans des environnements non HA. NetBackup prend en charge une grande variété d'environnements HA à travers des environnements Linux, Solaris et Windows. La configuration de NBAC est la suivante :

- Si nécessaire, établissez un cluster pour le serveur maître. Les informations de HA sont décrites dans le Guide de l'administrateur NetBackup dans les environnements hautement disponibles pour la réplication et la reprise après incident. Les informations de mise en cluster sont décrites dans le Guide de l'administrateur de serveur maître en cluster NetBackup.
- Configurez l'utilisation de NBAC à l'aide des instructions.
  Se reporter à "Configuration de NBAC (NetBackup Access Control)" à la page 210.

Configuration de NBAC (NetBackup Access Control)

Remarque : Les installations manuelles de client d'authentification et d'autorisation doivent être effectuées pour les serveurs de médias et les hôtes de client antérieurs. Les clients d'authentification et d'autorisation sont intégrés à NetBackup. Aucun serveur d'authentification et d'autorisation n'est nécessaire sur les serveurs de médias et les clients.

Pour plus d'informations sur l'ordre de configuration de NBAC, voir la procédure suivante.

Configuration de NBAC (NetBackup Access Control)

1. Configurez le serveur maître pour NBAC (NetBackup Access Control).

   Se reporter à "Configuration de NBAC (NetBackup Access Control) sur les serveurs maîtres autonomes" à la page 212.

   Remarque : Le serveur maître peut être installé en mode autonome ou dans une configuration hautement disponible sur un cluster.

2. Configurez les serveurs de médias pour NBAC.

   Se reporter à "Configuration de NBAC (NetBackup Access Control) sur des serveurs de médias" à la page 215.

3. Configurez les clients pour NBAC.

   Se reporter à "Installation et configuration du contrôle d'accès sur des clients" à la page 217.

Présentation générale de la configuration de NBAC

Cette rubrique contient des recommandations pour configurer le NBAC (NetBackup Access Control) en utilisant la commande `bpnbaz`. Cette commande est disponible dans le répertoire *`chemin_installation`*`/bin/admincmd`.

L'utilitaire `bpnbaz` est requis pour configurer NBAC sur les serveurs maîtres, les serveurs de médias et les clients. Cet outil configure également NBAC pour tous les hôtes de client et de médias de révision antérieure. Notez que les services doivent être redémarrés sur chacun des serveurs et clients après configuration. Cette rubrique présente un exemple d'utilisation de ces commandes et fournit des détails spécifiques sur l'utilisation recommandée :

Se reporter à "Résumé des commandes de configuration de NBAC" à la page 217.

Puisque la configuration est effectuée depuis le serveur maître, assurez-vous qu'il existe des liaisons de communication opérationnelles entre le serveur maître, les serveurs de médias et les clients. Passez en revue les conditions requises pour vous assurer que vous avez noté tous les serveurs de médias et les clients associés ainsi que les adresses permettant de communiquer avec eux.

Se reporter à "À propos de l'utilisation de NBAC (NetBackup Access Control)" à la page 206.

Un ensemble de commandes de système d'exploitation et une commande NetBackup sont utiles pour le premier niveau de dépannage. Les commandes de système d'exploitation sont `ping`, `traceroute` et `telnet`. La commande NetBackup est `bpclntcmd`. Utilisez ces commandes pour vérifier que les hôtes peuvent

communiquer entre eux. Consultez la rubrique suivante pour obtenir des informations de dépannage :

Se reporter à "Astuces de configuration et de résolution de problèmes pour NetBackup Authentication and Authorization" à la page 230.

Configuration de NBAC (NetBackup Access Control) sur les serveurs maîtres autonomes

Les procédures suivantes décrivent comment configurer NBAC (NetBackup Access Control) sur les serveurs maîtres qui sont installés sur un seul ordinateur. Un serveur maître requiert un serveur d'authentification et un serveur d'autorisation.

Le tableau suivant décrit les noms d'hôte pour les exemples de configuration de NBAC.

Tableau 14-2 Exemple de noms d'hôte

Nom d'hôte	Windows	UNIX
Serveurs maîtres	win_master	UNIX_master
Serveurs de médias	win_media	UNIX_media
Clients	win_client	UNIX_client

La procédure suivante décrit comment configurer NBAC sur les serveurs maîtres autonomes.

Remarque : Utilisez `-setupmaster` et définissez `USE_VXSS = AUTOMATIC` sur le serveur maître. Si `USE_VXSS = REQUIRED` est défini sur le serveur maître et qu'une tentative est faite pour configurer NBAC sur le serveur de médias, l'erreur suivante peut se produire : le serveur maître de NetBackup est configuré en mode `REQUIRED` . Veuillez définir le mode sur `AUTOMATIC` pour terminer la configuration du serveur de médias.

Configuration de NBAC sur les serveurs maîtres autonomes

1. Terminez toutes les installations ou mises à niveau de serveur maître NetBackup.
2. Exécutez la commande `bpnbaz -setupmaster`.

   Saisissez **o**. Le système commence à recueillir des données de configuration. Ensuite, il commence à configurer les informations d'autorisation.

3 Redémarrez les services NetBackup sur cet ordinateur une fois la commande `bpnbaz -setupmaster` terminée.

4 Poursuivez avec la configuration des serveurs de médias. Se reporter à "Configuration de NBAC (NetBackup Access Control) sur des serveurs de médias" à la page 215.

Installation du serveur maître NetBackup hautement disponible sur un cluster

La procédure suivante vous permet d'installer le serveur maître NetBackup hautement disponible sur un cluster.

Installation de NetBackup avec mise en cluster

1 Configurez le système de cluster sur lequel le serveur maître NetBackup doit être installé.

2 Installez le serveur maître NetBackup sur tous les nœuds du cluster.

3 Mettez le serveur maître NetBackup en cluster.

Les informations de haute disponibilité pour la réplication et la reprise après incident sont décrites dans le Guide de l'administrateur de NetBackup dans les environnements hautement disponibles

Les informations de mise en cluster sont décrites dans le Guide de l'administrateur de serveur maître en cluster NetBackup.

4 Effectuez une sauvegarde de test pour vous assurer qu'elle fonctionne dans le domaine NetBackup sans activer NBAC.

Configuration de NBAC (NetBackup Access Control) sur un serveur maître faisant partie d'un cluster

Remarque : Dans un environnement Windows en cluster, une fois le maître d'installation exécuté, l'entrée `AUTHENTICATION_DOMAIN` dans les nœuds passifs peut être identique au nom de nœud actif. Ce n'est pas acceptable. Après le basculement sur un nœud passif, lorsque `MFC UI` est lancé (avec <[nom d'ordinateur local] >\[utilisateur Administrateur]), un message d'erreur contextuel lié à l'authentification s'affiche. Pour contourner ce problème, il est possible d'ajouter le nom du nœud local en tant que domaine d'authentification dans `AUTHENTICATION_DOMAIN` sur les nœuds passifs après la configuration du serveur maître (avant le basculement). Avant de mettre à jour la valeur de l'entrée `AUTHENTICATION_DOMAIN`, récupérez la valeur actuelle en utilisant la commande `bpgetconfig`. Ajoutez ensuite le nom du nœud local comme domaine d'authentification dans la liste des domaines existante en utilisant la commande `bpsetconfig`. Pour quitter et enregistrer dans l'invite de commande `bpsetconfig`, appuyez sur `Ctrl + Z`, puis appuyez sur la touche `Enter`.

Remarque : Le retour du mode de NBAC de `REQUIRED` à `PROHIBITED` sur le nœud actif d'un cluster peut entraîner une défaillance du cluster. La solution à ce problème est de procéder comme suit. Sur un nœud actif, exécutez la commande `bpclusterutil -disableSvc nbazd` suivie de la commande `bpclusterutil -disableSvc nbatd`. Modifiez la valeur de `bp.conf USE_VXSS=AUTOMATIC` ou de `REQUIRED` par `PROHIBITED` en utilisant la commande `bpsetconfig`. Exécutez la commande `bpclusterutil -enableSvc nbazd` suivie de la commande `bpclusterutil -enableSvc nbatd` sur le nœud actif tout en passant `NBAC` en mode `REQUIRED` pour contrôler les services de sécurité.

Vous pouvez utiliser la procédure suivante pour configurer NBAC (NetBackup Access Control) sur un serveur maître en cluster.

Configuration de NBAC (NetBackup Access Control) sur un serveur maître faisant partie d'un cluster

1. Connexion au nœud de cluster principal.
2. Si vous utilisez Windows, ouvrez une console de commande.
3. Sous UNIX, accédez au répertoire `/usr/openv/netbackup/bin/admincmd`. Pour Windows, remplacez le répertoire par *chemin_installation*`\NetBackup\bin\admincmd`.
4. Exécutez `bpnbaz -setupmaster` sur le nœud actif.

5 Connectez-vous à la console d'administration sur le serveur maître.

6 Redémarrez les services NetBackup pour vous assurer que les paramètres NBAC sont appliqués.

Configuration de NBAC (NetBackup Access Control) sur des serveurs de médias

La procédure suivante décrit comment configurer NBAC (NetBackup Access Control) sur des serveurs de médias dans une configuration NetBackup. Ces étapes sont nécessaires pour les serveurs de médias qui ne sont pas coimplantés avec le serveur maître.

Remarque : Utilisez `-setupmedia` et définissez `USE_VXSS = AUTOMATIC` sur le serveur maître. Si `USE_VXSS = REQUIRED` est défini sur le serveur maître et qu'une tentative est faite pour configurer NBAC sur le serveur de médias, l'erreur suivante peut se produire : le serveur maître de NetBackup est configuré en mode `REQUIRED`. Veuillez définir le mode sur `AUTOMATIC` pour terminer la configuration du serveur de médias.

Configuration du contrôle d'accès sur les serveurs de médias

1. Connectez-vous à l'ordinateur de serveur maître.
2. Exécutez la commande `bpnbat -login`.

   Assurez-vous d'exécuter la commande `bpnbat -login` avant la commande `bpnbaz -setupmedia` pour éviter une erreur de commande.

   La commande `bpnbaz -setupmedia` possède certaines options.

   Pour fonctionner, cette commande nécessite une extension pour l'hôte individuel ou l'option `-all` (tout).

   Se reporter à "Résumé des commandes de configuration de NBAC" à la page 217.

   Il est recommandé d'effectuer d'abord une exécution directe de la configuration avec l'option `-dryrun`. Elle peut être utilisée avec une configuration `-all` et une configuration de serveur unique. Par défaut, la liste d'hôte découverte est écrite dans le fichier `SetupMedia.nbac`. Vous pouvez également fournir votre propre nom de fichier de sortie avec l'option `-out <output file>`. Si vous utilisez votre propre fichier de sortie, il doit être transmis avec l'option `-file` pour les prochaines exécutions. La commande d'exécution à vide (dry run) ressemblerait à ceci :

   `bpnbaz -SetupMedia -all -dryrun [-out <outfile>]` ou

   `bpnbaz -SetupMedia <media.server.com> -dryrun [-out <outfile>].`

   Si tous les serveurs de médias que vous voulez mettre à jour se trouvent dans le fichier journal, utilisez l'option `-dryrun`. Vous pouvez exécuter la commande `-all` pour tout faire en une seule fois. Par exemple, vous pouvez utiliser :

   `bpnbaz -SetupMedia -all` ou

   `bpnbaz -SetupMedia -file <progress file>.`

   Notez que l'option `-all` met à jour tous les serveurs de médias consultés lors de chaque exécution. Si vous voulez l'exécuter pour un ensemble sélectionné de serveurs de médias, vous pouvez le faire. Gardez seulement les noms d'hôte de serveur de médias que vous avez voulu configurer dans un fichier et passez ce fichier en utilisant l'option `-file`. Ce fichier d'entrée serait soit `SetupMedia.nbac`, soit le nom de fichier personnalisé que vous avez fourni avec l'option `-out` dans l'exécution à vide précédente. Par exemple vous avez pu utiliser : `- bpnbaz -SetupMedia -file SetupMedia.nbac`.

   Pour configurer un serveur de médias unique, spécifiez le nom d'hôte du serveur de médias comme option. Par exemple, utilisez :

   `bpnbaz -SetupMedia <media.server.com>.`

3 Redémarrez les services NetBackup sur les serveurs de médias cibles une fois la commande exécutée.

Cela installe NBAC sur les hôtes cibles. Si la configuration de quelques hôtes cibles ne se terminait pas, vous pouvez vérifier le fichier de sortie.

Passez à la configuration du contrôle d'accès pour les hôtes clients après cette étape.

Se reporter à "Installation et configuration du contrôle d'accès sur des clients" à la page 217.

Installation et configuration du contrôle d'accès sur des clients

Les étapes suivantes décrivent l'installation et la configuration de NetBackup Access Control sur des clients dans une configuration NetBackup. Un client a besoin d'un logiciel client d'authentification.

Utilisez la procédure suivante pour installer et configurer le contrôle d'accès sur des clients.

1 Assurez-vous qu'aucune sauvegarde n'est en cours d'exécution.

2 Pour installer le client, exécutez la commande suivante sur le serveur maître :

```
bpnbaz -setupClient
```

Ajout de bases de données d'authentification et d'autorisation dans les sauvegardes automatiques de catalogue NetBackup

Si l'environnement de NetBackup utilise la méthode de sauvegarde de catalogue automatique en ligne, aucune configuration supplémentaire n'est nécessaire pour inclure les bases de données d'authentification et d'autorisation NetBackup dans la sauvegarde de catalogue.

Résumé des commandes de configuration de NBAC

Le tableau suivant récapitule les commandes qui sont utilisées dans les séquences de configuration rapide de NBAC.

Les conventions suivantes sont fréquemment utilisées dans la synthèse d'utilisation de la commande.

Les parenthèses [ ] indiquent que le composant de ligne de commande inclus est facultatif.

Le caractère de barre verticale (|) indique les différents arguments facultatifs à choisir. Par exemple, lorsqu'une commande a le format : `command arg1|arg2` vous pouvez sélectionner la variable `arg1` ou `arg2`.

Tableau 14-3 Résumé des commandes de configuration de NBAC

Commande	Description
`bpnbaz -GetConfiguredHosts [target.server.com [-out file] | -all [-outfile] | -file progress.file]`	La commande `bpnbaz -GetConfiguredHosts` est utilisée pour obtenir l'état de NBAC sur l'hôte. Les options `-all` ou `target.server.com` sont requises pour cette commande. Syntaxe : ■ *target.server.com* est le nom d'une cible unique. Si, par exemple, vous souhaitez connaître l'état de NBAC sur un unique hôte, utilisez cette option. ■ L'option `-out` est utilisée pour spécifier un nom de fichier de sortie personnalisé. Par défaut, la sortie est enregistrée dans le fichier `SetupMedia.nbac`. Cette option peut être utilisée avec `-all` et les options de configuration de l'hôte unique. ■ `-all` est une option examinant toutes les politiques et collectant tous les noms d'hôte unique. Ces noms d'hôte se trouvent dans les politiques. Cette option collecte également tous les serveurs de médias configurés et capture l'état NBAC de chaque hôte dans le fichier `ConfiguredHosts.nbac`. ■ `-file progress.file` est une option utilisée pour spécifier le ou les noms d'hôte à lire depuis `progress_file`. Cette option attend un nom d'hôte par ligne dans progress_file. CLI met à jour `progress_file` avec l'état NBAC de l'hôte. Le caractère `#` est ajouté après `hostname` suivi de l'état NBAC. ■ Lorsqu'il est utilisé avec l'option `target.server.com` ou`-all` l'état du ou des hôtes est capturé dans le fichier `ConfiguredHosts.nbac`.

Commande	Description
`bpnbaz -SetupMaster [-fsa [<domain type>:<domain name>:]<user name>]`	La commande`bpnbaz -SetupMaster` est exécutée pour configurer le serveur maître pour l'utilisation de NBAC. Le serveur d'autorisation et le courtier d'authentification d'autorisation doivent être installés et en cours d'exécution sur le serveur maître. Utilisez la commande `bpnbaz -SetupMaster -fsa` avec l'option Premier administrateur de sécurité pour configurer un utilisateur particulier du système d'exploitation comme Administrateur NBU. Syntaxe : ■ l'option `-fsa` est utilisée pour configurer un utilisateur spécifique du système d'exploitation comme Administrateur NBU. Lorsque vous utilisez cette option, vous devez fournir le mot de passe pour votre identité actuelle d'utilisateur du système d'exploitation. ■ *domain type* est le type de domaine réseau que vous utilisez. Par exemple, la commande `bpnbaz -SetupMaster -fsa nt:ENTERPRISE:jdoe` configure l'utilisateur du domaine d'entreprise Windows `jdoe` comme Administrateur NBU. ■ *domain name* est le nom du domaine particulier que vous utilisez. Par exemple, la commande `bpnbaz -SetupMaster -fsa jdoe` prend le type de domaine de l'utilisateur actuellement connecté (Windows/UNIXPWD), le nom de domaine et configure l'utilisateur `jdoe` dans ce domaine. ■ *user name* est le nom d'utilisateur particulier du système d'exploitation que vous désignez en tant qu'administrateur NBU. **Remarque :** L'existence de l'utilisateur est vérifiée dans le domaine spécifié. Le comportement existant de configuration de l'administrateur connecté ou racine comme administrateur NBU est préservé.

Commande	Description
`bpnbaz -SetupMedia [ media.server.com [-out file] | -all [-out file] | -file progress.file ] [-dryrun] [-disable]`	La commande de `bpnbaz -SetupMedia` est exécutée sur le serveur maître par un membre du groupe NBU_Administrator. Elle ne doit pas être exécutée avant qu'une commande `bpnbaz -SetupMaster` ait été effectuée. Dans ce cas, le serveur maître et le serveur de médias cible doivent être connectés. Les options `-all` ou `target.server.com` sont requises pour cette commande. Syntaxe : ■ *media.server.com* est le nom d'un hôte cible unique. nom d'un hôte cible unique. Utilisez cette option pour ajouter un seul hôte supplémentaire à utiliser avec NBAC. ■ L'option `-out` est utilisée pour spécifier un nom de fichier de sortie personnalisé. Par défaut, la sortie est enregistrée dans le fichier `SetupMedia.nbac`. Cette option peut être utilisée avec `-all` et les options de configuration de l'hôte unique. ■ `-all` examine toutes les unités de stockage et collecte tous les noms d'hôte unique présents dans les unités de stockage. Celles-ci peuvent être interrogées dans un ordre défini. Les résultats sont enregistrés dans le fichier de progression. ■ L'option`-file` *`progress_file`* est utilisée pour spécifier un fichier d'entrée avec un ensemble spécifique de noms d'hôte de serveur de médias. Après l'exécution, l'état de chaque serveur de médias est mis à jour dans le fichier de progression. Les configurations réussies sont commentés pour les exécutions ultérieures. Cette commande peut être répétée jusqu'à ce que tous les serveurs de médias du fichier d'entrée soient configurés. ■ `-dryrun` peut générer la liste des noms de serveur de médias et les enregistrer dans le journal. Cette option peut fonctionner avec media.server.com mais est prévue pour être utilisé avec l'option `-all`. ■ L'option `-disable` peut désactiver NBAC (USE_VXSS = PROHIBITED) sur les hôtes cibles.

Commande	Description
`bpnbaz -SetupClient [ client.server.com [-out file] | -all [-images] [-out file] | -file progress.file ] [-dryrun] [-disable]`	

Commande	Description
	La commande `bpnbaz -SetupClient` est utilisée pour installer NBAC sur les clients. Elle ne doit pas être exécutée avant qu'une commande `bpnbaz -SetupMaster` ait été effectuée. La commande `bpnbaz -SetupClient` doit s'exécuter depuis le serveur maître. Le serveur maître et les systèmes client cibles doivent communiquer. Les options `-all` ou `target.server.com` sont requises pour cette commande. Syntaxe : ■ *client.server.com* est le nom d'un hôte cible unique. Si, par exemple, vous souhaitiez ajouter un hôte unique supplémentaire à utiliser avec NBAC, ce nom est l'option que vous devez utiliser. ■ L'option `-out` est utilisée pour spécifier un nom de fichier de sortie personnalisé. Les données sortantes sont écrites dans le fichier `SetupClient.nbac` par défaut. Cette option peut être utilisée avec `-all` et les options de configuration de l'hôte unique. L'option `-out` est utilisée pour spécifier un nom de fichier de sortie personnalisé. Les données sortantes sont écrites dans le fichier `SetupClient.nbac` par défaut. Cette option peut être utilisée avec `-all` et les options de configuration de l'hôte unique. ■ L'option `-all` parcourt toutes les politiques et collecte tous les noms d'hôte uniques présents dans les politiques. Les politiques sont interrogées dans un ordre donné. Les résultats sont enregistrés dans le fichier de progression. ■ L'option `-images` recherche toutes les images pour les noms d'hôte uniques. Cette option n'est pas recommandée aux clients possédant de grands catalogues, sauf s'ils ajoutent l'option -dryrun. Cette option collecte tous les clients uniques contenus dans le catalogue d'images. Des catalogues plus anciens peuvent contenir un plus grand nombre d'hôtes désactivés, des hôtes déplacés vers de nouveaux serveurs maîtres ou renommés. L'heure d'exécution de la commande peut augmenter le nombre de tentatives effectuées pour contacter les hôtes non joignables. ■ L'option `-dryrun` génère la liste des noms de clients et les consigne dans le fichier journal. Suite à cela, les systèmes cibles ne sont pas réellement configurés. ■ L'option `-disable` désactive NBAC (USE_VXSS = PROHIBITED) sur les hôtes cibles. ■ L'option `-file progress.file` est utilisée pour spécifier un nom de fichier différent pour le journal de progression. L'interface de ligne de commande lit les noms d'hôte du fichier progress.file. L'état est ajouté en regards de chaque nom d'hôte avec une [valeur séparée par #]. Les exécutions terminées sont commentées. Cette commande peut être exécutée plusieurs fois, jusqu'à ce que tous les clients situés dans

Commande	Description
	`progress_file` soient configurés.

Unification des infrastructures de gestion NetBackup à l'aide de la commande setuptrust

Remarque : Elle est réalisée automatiquement si le nom du serveur OpsCenter est fourni au moment de l'installation. Dans le cas contraire, une commande ajoute le nom du serveur OpsCenter au serveur maître NetBackup. qui établit la confiance côté NetBackup.

Les serveurs de gestion de produits Veritas doivent communiquer afin que l'administrateur d'un produit ait l'autorisation d'administrer un autre produit. Cette communication garantit que les procédures d'application d'un serveur de gestion fonctionnent avec un autre serveur. Pour garantir les communications, vous pouvez utiliser un serveur de sécurité indépendant commun appelé courtier d'authentification. Si tous les serveurs de gestion pointent vers un courtier d'authentification commun, l'autorisation de chacun des serveurs est basée sur un certificat commun. Il est également possible de garantir les communications à l'aide de la commande `setuptrust`. Cette commande est utilisée pour établir la confiance entre les deux serveurs de gestion. La commande est émise depuis le serveur de gestion qui doit faire confiance un autre serveur de gestion. Les informations sur la sécurité sont transférées depuis cet hôte vers celui demandant l'établissement de la confiance. Une confiance à sens unique est établie. L'établissement d'une confiance bi-directionnelle (mutuelle) est effectué en émettant la commande de `setuptrust` depuis chacun des deux serveurs impliqués. Par exemple, une configuration NetBackup peut être composée d'un serveur OpsCenter (OPS) et de trois serveurs maîtres (A, B et C). Des politiques NBAC et la gestion pour des clients et serveurs de médias sont reliées à chacun des serveurs maîtres.

La première étape consiste à établir la confiance entre le serveur OpsCenter (OPS) et chacun des serveurs maîtres (A, B et C). Cette confiance garantit que le serveur OpsCenter reçoit des communications sécurisées depuis chacun des serveurs maîtres, clients et serveurs de médias connectés à chacun des serveurs maîtres. Une séquence de ces événements est décrite ci-dessous :

- Le serveur OPS établit la confiance avec le serveur maître A.
- Le serveur OPS établit la confiance avec le serveur maître B.
- Le serveur OPS établit la confiance avec le serveur maître C.

Si le serveur OpsCenter est configuré pour exécuter des actions sur les différents serveurs maîtres, une relation de confiance doit être établie entre chacun des serveurs maîtres et le serveur OpsCenter (OPS). Une séquence de ces événements est décrite ci-dessous. Dans ce cas, la commande `setuptrust` est exécutée six fois.

- Le serveur maître A établit la confiance avec le serveur OpsCenter (OPS).
- Le serveur maître B établit la confiance avec le serveur OpsCenter (OPS).
- Le serveur maître C établit la confiance avec le serveur OpsCenter (OPS).
- Le serveur OpsCenter (OPS) établit la confiance avec le serveur maître A.
- Le serveur OpsCenter (OPS) établit la confiance avec le serveur maître B.
- Le serveur OpsCenter (OPS) établit la confiance avec le serveur maître C.

Remarque : NetBackup et OpsCenter établissent la confiance automatiquement. Il peut être nécessaire d'effectuer manuellement ces opérations `setuptrust` sur les anciens serveurs maîtres NetBackup. A la fin de l'installation du serveur maître NetBackup, il existe une question sur le nom d'hôte du serveur OpsCenter. A l'aide de cette question, le serveur maître peut établir une confiance mutuelle.

Des détails sur la commande `setuptrust` sont disponibles dans le Guide de référence des commandes NetBackup. Se reporter à "Utilisation de la commande setuptrust" à la page 224.

Utilisation de la commande setuptrust

Vous pouvez utiliser la commande `setuptrust` pour contacter le courtier avec lequel établir la confiance, obtenir son certificat ou des détails par transmission filaire et ajouter les détails au référentiel de confiance si les détails fournis sont dignes de confiance. L'administrateur de sécurité peut configurer l'un des niveaux de sécurité suivants pour la distribution des certificats racines :

- Sécurité élevée (2) : si une racine avec laquelle aucune relation de confiance n'avait précédemment été établie est acquise depuis l'homologue (si aucun certificat possédant la même signature n'existe dans la mémoire approuvée), l'utilisateur est invité à vérifier le hachage.
- Sécurité moyenne (1) : une relation de confiance est établie avec le premier courtier d'authentification sans demande de confirmation. Pour toute tentative ultérieure d'établir une relation de confiance avec d'autres courtiers d'authentification, l'utilisateur est invité à vérifier le hachage avant que le certificat soit ajouté à la mémoire approuvée.

- Sécurité faible (0) : Le certificat de courtier d'authentification n'est toujours fait confiance sans aucune incitation. L'interface de ligne de commande `vssat` se trouve dans le répertoire " fichier " du service d'authentification.

La commande `setuptrust` utilise la syntaxe suivante :

```
vssat setuptrust --broker <host[:port]> --securitylevel high [-F]
```

La commande `setuptrust` utilise les arguments suivants :

Les arguments `broker`, `host` et `port` sont les premiers. L'hôte et le port du courtier avec lequel établir la confiance. Le port enregistré pour l'authentification est 2821. Si le courtier a été configuré avec un autre numéro de port, consultez votre administrateur de sécurité pour plus d'informations.

Utilisez l'option `-F` (`--enable_fips`) pour exécuter la commande `vssat` en mode FIPS. Le mode FIPS est désactivé par défaut.

Configuration des propriétés de l'hôte de contrôle d'accès pour le serveur maître et de médias

Pour configurer les propriétés de l'hôte de contrôle d'accès pour le serveur maître ou le serveur de médias, développez **Gestion NetBackup > Propriétés de l'hôte > Serveurs maîtres *ou* Media Servers > *server name* > Access Control**.

Définissez **NetBackup Product Authentication and Authorization** sur **Requis** ou **Automatique**. Le paramètre **Automatique** prend en compte le fait qu'il peut y avoir des hôtes dans la configuration qui ne sont pas encore configurés pour NBAC. Le serveur tente de négocier la connexion la plus sécurisée possible quand elle communique avec d'autres systèmes NetBackup. Le paramètre **Automatique** doit être utilisé jusqu'à ce que tous les clients et serveurs soient configurés pour NBAC.

Quand **Automatique** est sélectionné, vous pouvez spécifier les ordinateurs ou les domaines requis pour utiliser **NetBackup Product Authentication and Authorization**. Sinon, vous pouvez spécifier les ordinateurs qui ne sont pas autorisés à utiliser **NetBackup Product Authentication and Authorization**.

Onglet Domaine d'authentification

L'onglet **Domaine d'authentification** est utilisé pour définir les éléments qui suivent :

- La nature des serveurs d'authentification prenant en charge les mécanismes d'authentification
- Ce que chaque domaine prend en charge.

Ajoutez le domaine pour lequel vous souhaitez que les utilisateurs s'authentifient.

Les exemples suivants contiennent six domaines d'authentification.

Remarque : Si un domaine d'authentification UNIX est utilisé, saisissez le nom de domaine complet de l'hôte effectuant l'authentification.

Remarque : Les types d'authentification pris en charge sont `NIS`, `NISPLUS`, `WINDOWS`, `vx` et `unixpwd` (`unixpwd` est le réglage par défaut).

---

service d'autorisation, onglet

Remarque : Aucune modification de cet onglet n'est autorisée, il est en lecture seule.

Dans les propriétés de l'hôte de **contrôle d'accès**, vous pouvez voir le nom d'hôte sous l'onglet **Service d'autorisation**. Toutes ces informations sont grisées car elles sont en lecture seule. Vous ne pouvez apporter aucune modification à cet écran.

Onglet Attributs réseau

Affichez les propriétés de l'hôte de **contrôle d'accès** dans l'onglet **Attributs réseau**. Ajoutez le serveur maître à la liste **Réseaux**. Puis, définissez **NetBackup Product Authentication and Authorization** sur **Requis**.

Chaque nouveau client ou serveur de médias NetBackup (ou ultérieure) ajouté au maître NetBackup doit avoir ses propriétés de **contrôle d'accès** configurées. Ces propriétés sont configurées sur lui-même et sur le maître. Cette configuration peut être faite via les propriétés hôtes sur le serveur maître.

Boîte de dialogue Propriétés d'hôte du contrôle d'accès pour le client

Sélectionnez le client NetBackup dans les propriétés de l'hôte. (Sur le serveur maître, dans la **console d'administration NetBackup**, développez **Gestion NetBackup > Propriétés de l'hôte > Clients > *Clients sélectionnés* > Contrôle d'accès**.)

Définissez **NetBackup Product Authentication and Authorization** sur **Requis** ou **Automatique**. Dans cet exemple, **Automatique** est sélectionné.

Onglet Domaine d’authentification pour le client

Sélectionnez le client NetBackup dans les propriétés de l’hôte. Cette sélection peut être utilisée pour contrôler les systèmes pouvant nécessiter ou interdire l’utilisation de NetBackup Product Authentication and Authorization pour chacun des ordinateurs. Notez que les paramètres des deux systèmes doivent correspondre pour pouvoir communiquer.

Dans les propriétés de l’hôte de **Contrôle d’accès**, sous l’onglet **Domaine d’authentification**, ajoutez la liste des domaines qu’un client peut utiliser pour s’authentifier. Vous pouvez cliquer sur **Rechercher** pour obtenir une liste des domaines d’authentification disponibles. Cliquez ensuite sur **Ajouter** pour créer une liste de domaines d’authentification sélectionnés.

Onglet Attributs réseau pour le client

Dans les propriétés de l’hôte **Contrôle d’accès** de l’onglet **Paramètres réseau**, ajoutez la liste des réseaux que le client peut utiliser pour s’authentifier.

Utilisation du contrôle d'accès NetBackup (NBAC) avec Auto Image Replication

Si Auto Image Replication est configuré pour deux domaines et que le contrôle d'accès NetBackup (NBAC) est utilisé, il doit être utilisé dans le domaine source et le domaine cible. La configuration pour les serveurs maîtres doit être de type `USE_VXSS = REQUIRED` ou `USE_VXSS = AUTOMATIC`. (Cependant, le paramètre peut être `REQUIRED` dans un domaine et `AUTOMATIC` dans l’autre.

Auto Image Replication n'est pas prise en charge entre les domaines de serveur maître, où un serveur maître est configuré pour utiliser NBAC et NBAC est désactivé sur l'autre serveur maître. Autrement dit, la configuration pour un serveur maître est `USE_VXSS = AUTOMATIC` ou `USE_VXSS = REQUIRED` et, sur l'autre serveur maître, `USE_VXSS = PROHIBITED` (désactivé).

La configuration suivante est supplémentaire si NBAC est utilisé dans les domaines de serveur maître :

- Dans le domaine de serveur maître source :
  L'administrateur doit s'assurer que les autorisations du serveur maître cible sont définies correctement avant le début de la configuration pour l'opération.
- Dans le domaine de serveur maître cible :
  L'administrateur de sécurité du domaine cible doit donner à l'administrateur du domaine source les autorisations correctes. L'administrateur de domaine source

a besoin des autorisations Parcourir, Lire et Configurer sur les objets suivants : **HostProperties**, **DiskPool** et **DevHost**.

L'administrateur du domaine source peut être ajouté en tant que membre à n'importe quel groupe existant ayant les trois autorisations.

Prenons l'exemple suivant :

Deux domaines NBAC contiennent chacun un serveur maître :

- Domaine NBAC source de réplication : *DomainA* contient *Master-A*
- Domaine NBAC cible de réplication : *DomainB* contient *Master-B*

NBAC est activé sur les deux domaines NBAC est activé sur les deux domaines (si NBAC est utilisé dans un domaine, il doit être utilisé dans l'autre).

Pour que *UserA* crée une Auto Image Replication SLP avec *Master-B* comme cible, *UserA* doit y être autorisé sur *Master-B*.

Un administrateur de sécurité (*UserB*) dans *DomainB* doit créer un groupe d'utilisateurs (*NB_InterDomainUsers*, par exemple) et accorder l'autorisation de recherche, de lecture et de configuration dans les zones suivantes :

- **HostProperties**
- **DiskPool**
- **DevHost**

L'administrateur de la sécurité de *DomainB* (*UserB*) assigne alors *NB_InterDomainUsers* à `DomainA\UserA` à l'aide de la commande `bpnbaz -AddUser`.

Dépannage de la gestion de l'accès

Pour dépanner la gestion de l'accès et déterminer si certains processus et fonctionnalités fonctionnent correctement :

Se reporter à "Astuces de configuration et de résolution de problèmes pour NetBackup Authentication and Authorization" à la page 230.

Ces points de vérification incluent :

- Points de vérification Windows
  Se reporter à "Points de vérification de Windows" à la page 236.
- Points de vérification UNIX
  Se reporter à "Points de vérification UNIX" à la page 245.
- Points de vérification dans un environnement mixte avec un serveur maître UNIX

Se reporter à "Points de vérification dans un environnement mixte avec un serveur maître UNIX" à la page 253.

- Points de vérification dans un environnement mixte avec un serveur maître Windows
  Se reporter à "Points de vérification dans un environnement mixte avec un serveur maître Windows" à la page 259.

Résolution des problèmes NBAC

Le tableau suivant répertorie les problèmes liés à NBAC et leurs solutions :

Tableau 14-4 Problèmes liés à NBAC

Problème et origine	Solution
Une sauvegarde ou restauration dirigée par l'utilisateur échoue Une sauvegarde ou restauration dirigée par l'utilisateur échoue avec NBAC en mode automatisé. L'interface Sauvegarde, archivage et restauration affiche des erreurs dans l'interface Windows lorsque NBAC est configuré. Un échec de sauvegarde ou de restauration peut se produire lorsqu'une installation de NetBackup sur un serveur maître UNIX est configurée avec NBAC et que vous tentez d'utiliser l'interface Windows sans configurer au préalable l'interface pour ce type d'installation. L'échec peut également être dû à la présence d'un certificat ayant expiré dans le répertoire d'origine.	Configurez l'interface Windows pour prendre en charge l'installation. Au moins un système Microsoft Windows doit agir en tant que courtier d'authentification pour authentifier les utilisateurs du domaine Active Directory. Consultez la note technique TECH199281 pour connaître les étapes de configuration de l'interface Windows pour permettre aux utilisateurs existants d'Active Directory de gérer, contrôler ou utiliser un environnement NetBackup situé principalement sur des plates-formes UNIX/Linux. Après avoir correctement configuré l'installation, exécutez la commande `bpnbat -logout` pour vous en déconnecter avant de redémarrer l'interface.
Echec d'authentification avec erreur 116 L'authentification échoue avec l'erreur « `error 116-VxSS authentication` » lorsque vous tentez d'installer NBAC sur un hôte cible.	Vérifiez que l'authentification NBAC est correctement configurée et que vos informations d'authentification sont valides pour l'hôte cible.
Erreur lorsqu'un utilisateur non administrateur du groupe NBU_Operator tente d'utiliser Access Management Un utilisateur non administrateur est ajouté au groupe NBU_Operator. Des autorisations de lecture, navigation et configuration sont affectées avec l'autorisation de configurer les propriétés d'hôte. Toutefois, lorsque l'utilisateur tente d'ouvrir l'utilitaire Access Management, une erreur s'affiche.	Les utilisateurs du groupe NBU_Operator disposent d'autorisations limitées. L'utilisateur doit disposer d'un jeu d'autorisations différent pour pouvoir utiliser l'utilitaire Access Management. Pour les autorisations requises, ajoutez l'utilisateur au groupe NBU_Security_Admin. Pour plus d'informations sur les groupes d'utilisateurs : Se reporter à "Groupes d'utilisateurs NetBackup par défaut" à la page 271.

Problème et origine	Solution
La fonctionnalité de fichier d'autorisation (auth.conf) ne fonctionne pas dans un environnement NBAC. Par défaut, le fichier auth.conf est pris en charge par l'interface Java uniquement dans des environnements non NBAC.	Pour que le fichier auth.conf fonctionne dans un environnement NBAC, utilisez les commandes `nbgetconfig` et `nbsetconfig` pour ajouter l'entrée `USE_AUTH_CONF_NBAC` au registre Windows ou au fichier bp.conf sous UNIX. L'entrée doit être définie sur `YES`, comme suit : `USE_AUTH_CONF_NBAC = YES` Pour plus d'informations sur le fichier auth.conf, consultez le Guide de l'administrateur NetBackup, volume I.
Erreur lors du basculement du serveur NetBackup de l'audit amélioré à NBAC La console d'administration NetBackup crée des répertoires utilisateur avec *nom utilisateur* comme nom de répertoire dans `netbackup/logs/user_ops`. Pour l'audit amélioré, ces répertoires sont utilisés par les processus NetBackup qui s'exécutent avec des privilèges racines. Pour NBAC, ces répertoires sont utilisés par les processus NetBackup qui s'exécutent sans privilèges racines. Des erreurs d'interface utilisateur graphique NetBackup peuvent se produire dans le cas suivant : ■ Les répertoires utilisateur créés lorsque l'audit amélioré était activé existent toujours lorsque NBAC est activé, et ■ aucun de ces utilisateurs ne dispose de privilèges racine. Exemples d'erreurs : ■ Dans l'interface Sauvegarde, archivage et restauration, aucun travail n'apparaît dans l'onglet **Progression de la tâche**. ■ Pour une restauration de machine virtuelle VMware, la vérification de prérécupération signale l'erreur 12.	**1** Sur chaque serveur NetBackup auquel les utilisateurs se connectent à l'aide de l'interface utilisateur graphique, supprimez les répertoires utilisateur dans le répertoire suivant : Windows : *`install_path`*`\NetBackup\logs\user_ops` UNIX, Linux : `/usr/openv/netbackup/logs/user_ops` **2** Lorsque les répertoires sont supprimés, redémarrez l'interface utilisateur graphique de NetBackup.

Astuces de configuration et de résolution de problèmes pour NetBackup Authentication and Authorization

Le tableau suivant présente des astuces utiles pour la configuration et la résolution de problèmes pour **NetBackup Authentication and Authorization**. En outre, le tableau contient également des informations sur quelques problèmes connus et des astuces pour les résoudre :

Tableau 14-5 Astuces de configuration et de résolution de problèmes pour NetBackup Authentication and Authorization

Rubrique	Astuces de configuration
Vérification des paramètres de serveur maître	L'exécution de la commande `bpnbat -whoami` et la spécification des informations d'authentification d'ordinateur indiquent dans quel domaine un hôte est enregistré et le nom de l'ordinateur que le certificat représente. `bpnbat -whoami -cf "`*`install_path`*`\netbackup\var\vxss\credentials\ master.company.com "Name: master.company.com Domain: NBU_Machines@master.company.com Issued by: /CN=broker/OU=root@master.company.com/O=vx Expiry Date: Oct 31 20:17:51 2007 GMT Authentication method: Veritas Private Security Operation completed successfully.` Si le domaine listé n'est pas NBU_Machines@master.company.com, considérez l'exécution de la commande `bpnbat -addmachine` pour le nom en question (maître). La commande est exécutée sur l'ordinateur qui sert le domaine NBU_Machines (maître). Puis, sur l'ordinateur où vous voulez placer les informations d'authentification, exécutez : `bpnbat -loginmachine`

Établissement des informations d'authentification racine	Si vous avez des problèmes pour installer le serveur d'authentification ou le serveur d'autorisation et que l'application se plaint à propos de vos habilitations comme `root` : assurez-vous que la variable environnementale `$HOME` est correcte pour `root`.
	
	Utilisez la commande suivante pour découvrir la valeur actuelle :
	
	`echo $HOME`
	
	Cette valeur doit être conforme au répertoire d'origine de la racine, qui se trouve généralement dans le fichier `/etc/passwd`.
	
	Notez qu'en basculant sur la `root`, vous pouvez devoir utiliser :
	
	`su -`
	
	au lieu seulement de `su` pour conditionner correctement les variables d'environnement de la `root`.

Rubrique	Astuces de configuration
Message d'informations d'authentification expirées	Si vos informations d'authentification sont arrivées à expiration ou sont incorrectes, vous pouvez recevoir le message suivant lors de l'exécution des commandes `bpnbaz` ou `bpnbat` : `Supplied credential is expired or incorrect. Please reauthenticate and try again.` Exécutez `bpnbat -Login` pour mettre à jour les informations d'authentification arrivées à expiration.
Journaux de débogage utiles	Les journaux suivants sont utiles pour déboguer le contrôle d'accès NetBackup : Sur le serveur maître : `admin`, `bpcd`, `bprd`, `bpdbm`, `bpjobd`, `bpsched` Sur le client : `admin`, `bpcd` Contrôle d'accès : `nbatd`, `nbazd`. Si le serveur maître utilise NetBackup Access Control (NBAC) en mode REQUIS et que la base de données EMM est distante, les informations de consignation s'affichent alors dans le journal `bpdbm`. Consultez Guide de dépannage NetBackup pour des instructions sur la consignation appropriée.
Emplacement de stockage des informations d'authentification	Les informations d'authentification de NetBackup Authentication and Authorization sont enregistrées dans les répertoires suivants : UNIX : Informations d'authentification de l'utilisateur : `$HOME/.vxss` Informations d'authentification de l'ordinateur : `/usr/openv/var/vxss/credentials/` Windows : <user_home_dir>\Application Data\VERITAS\VSS
Effet du temps du système sur le contrôle d'accès	Les informations d'authentification ont une heure d'émission et une heure d'expiration. Les ordinateurs ayant d'importantes anomalies d'horloge affichent des informations d'authentification émises dans le futur ou prématurément expirées. Envisagez de synchroniser le temps si vous avez des difficultés de communication entre les systèmes.

Rubrique	Astuces de configuration

Ports NetBackup Authentication and Authorization	Les services de daemon NetBackup Authentication and Authorization utilisent les ports 13783 et 13722 pour le serveur de médias et les clients de niveau précédent. Les services utilisent les connexions PBX.
	Vous pouvez vérifier que les processus écoutent avec les commandes suivantes :
	Authentification :
	UNIX
	`netstat -an | grep 13783`
	Windows
	`netstat -a -n | find "13783"`
	Autorisation :
	UNIX
	`netstat -an | grep 13722`
	Windows
	`netstat -a -n | find "13722"`

Arrêt des daemons NetBackup Authentication and Authorization pour les services partagés	Lors de l'arrêt des services NetBackup Authentication and Authorization, arrêtez d'abord l'autorisation, puis arrêtez l'authentification.
	UNIX - Utilisez les commandes suivantes.
	Pour arrêter l'autorisation, utilisez le signal de fin comme indiqué dans l'exemple :
	`# ps -fed |grep nbazd`
	`root 17018 1 4 08:47:35 ? 0:01 ./nbazd`
	`root 17019 16011 0 08:47:39 pts/2 0:00 grep nbazd`
	`# kill 17018`
	Pour arrêter l'authentification, utilisez le signal de fin comme indiqué dans l'exemple :
	`# ps -fed |grep nbatd`
	`root 16018 1 4 08:47:35 ? 0:01 ./nbatd`
	`root 16019 16011 0 08:47:39 pts/2 0:00 grep nbatd`
	`# kill 16018`
	Windows
	Utilisez l'utilitaire Services fourni par Windows, car ces services n'apparaissent pas dans le moniteur d'activité NetBackup.

Rubrique	Astuces de configuration
Si vous vous verrouillez hors de NetBackup	Vous pouvez vous verrouiller en dehors de la **console d'administration NetBackup** si le contrôle d'accès n'est pas correctement configuré. Le cas échéant, utilisez `vi` pour lire les entrées bp.conf (UNIX) ou `regedit` (Windows) et afficher le Registre Windows à l'emplacement suivant : `HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\config` Vous pouvez vérifier si les entrées suivantes sont correctement définies : AUTHORIZATION_SERVICE, AUTHENTICATION_DOMAIN et USE_VXSS. L'administrateur peut ne pas vouloir utiliser le contrôle d'accès NetBackup ou ne pas avoir installé les bibliothèques d'autorisation. Vérifiez que l'entrée `USE_VXSS` est définie sur `Prohibited` ou totalement supprimée.
Les sauvegardes des unités de stockage sur des serveurs de médias peuvent ne pas fonctionner dans un environnement de NBAC	Le nom d'hôte d'un système du domaine NetBackup (serveur maître, serveur de médias ou client) et le nom d'hôte spécifié dans le fichier `bp.conf` devraient être identiques.
Utilisation de l'utilitaire nbac_cron	L'utilitaire `nbac_cron.exe` permet de créer des identités sous lesquelles exécuter la commande cron ou des travaux. Pour plus d'informations sur l'utilitaire `nbac_cron` : Se reporter à "A propos de l'utilitaire nbac_cron" à la page 265. `nbac_cron.exe` se trouve à l'emplacement suivant : UNIX -`/opt/openv/netbackup/bin/goodies/nbac_cron` Windows -*`install_path`*`\netbackup\bin\goodies\nbac_cron.exe` Pour des informations détaillées sur l'utilisation de l'utilitaire `nbac_cron` : Se reporter à "Utilisation de l'utilitaire nbac_cron" à la page 266.
Activation de NBAC après une récupération sous Windows	La procédure suivante permet d'activer manuellement NBAC après une récupération sous Windows. ■ Ajoutez `AUTHENTICATION_DOMAIN`, `AUTHORIZATION_SERVICE` et les entrées `USE_VXSS` dans le registre. ■ Définissez le type de services NetBackup Authentication and Authorization sur `AUTOMATIC`. ■ Redémarrez les services NetBackup. ■ Vérifiez que les services `nbatd` et `nbazd` sont en cours d'exécution. **Remarque :** Sur un cluster, exécutez les commandes `bpclusterutil -enableSvc nbatd` et `bpclusterutil -enable nbazd` .

Rubrique	Astuces de configuration
Dans les installations en cluster, la commande `setupmaster` peut échouer	Dans le cas des installations en cluster où le fichier de configuration est sur un disque partagé, le fait que la commande `setupmaster` peut échouer est un problème connu.
Problème connu lorsque, sur un cluster, les services de sécurité partagés (`vxatd` ou `vxazd`) sont mis en cluster avec le serveur maître	Sur un cluster, le fait que les services de sécurité partagés (`vxatd` ou `vxazd`) soient mis en cluster avec le serveur maître est un problème connu. En exécutant la commande `bpnbaz -SetupMaster` et en installant la sécurité (NBAC), gelez les groupes de service partagés des services de sécurité, et ce de manière continue le cas échéant, ou mettez les services hors ligne (mais vérifiez que leur disque partagé est en ligne) et exécutez la commande `setupmaster`.
Problème connu lorsque, dans une mise à niveau de serveur maître mis en cluster avec NBAC, toutes les entrées `AUTHENTICATION_DOMAIN` du fichier `bp.conf` sont mises à jour avec le nom virtuel du serveur maître comme courtier d'authentification	Dans une mise à niveau de serveur maître mis en cluster avec NBAC, le fait que toutes les entrées `AUTHENTICATION_DOMAIN` du fichier `bp.conf` soient mises à jour avec le nom virtuel de serveur maître comme courtier d'authentification est un problème connu. Toute entrée de domaine présente se référant à un courtier d'authentification différente autre que le serveur maître (et le serveur maître n'entretenant pas ce domaine) doit être manuellement supprimée du fichier `bp.conf`.
Problème connu sur les ordinateurs Windows 2003 en pile double	Sur les ordinateurs Windows 2003 à double pile, un problème connu existe. Vous avez besoin du correctif Microsoft `kb/928646` disponible sur le site `http://support.microsoft.com/`.
Problème connu relatif aux échecs de contrôle d'accès et aux noms d'hôte courts et longs	Les échecs liés au contrôle d'accès font partie d'un problème connu. Déterminez si les noms d'hôte courts et longs peuvent se résoudre correctement et renvoient à la même adresse IP.
Problème connu lorsque, dans une mise à niveau de cluster avec NBAC, la commande `ClusterName` du profil de courtier est définie par le nom virtuel d'AT	Dans une mise à niveau de cluster avec NBAC, le fait que la commande `ClusterName` du profil de courtier soit définie par le nom virtuel d'AT est un problème connu. La migration s'effectue telle quelle vers le courtier incorporé. Dans le profil du courtier incorporé, `UseClusterNameAsBrokerName` est défini sur 1. Lorsqu'une demande est envoyée pour des cartes de domaine de courtier, elle utilise le nom virtuel d'AT partagé comme nom de courtier. La commande `bpnbaz -GetDomainInfosFromAuthBroker` renvoie aucun. Dans la mise à niveau, le fichier `bp.conf` est mis à jour pour avoir le nom virtuel de NetBackup.

Rubrique	Astuces de configuration
Problème connu lorsque plusieurs instances de `bpcd` entraînent une possibilité d'erreur	Dans la commande `bpnbaz -SetupMedia`, le fait que `bprd` utilise le protocole `AT_LOGINMACHINE_RQST` pour parler avec `bpcd` sur la zone de destination est un problème connu. Une nouvelle instance de `bpcd` est engendrée. Une fois la commande terminée, elle essaie de libérer une baie de `char` comme pointeur régulier entraînant probablement `bpcd` à vider la mémoire du côté client. La fonctionnalité ne doit pas être perdue car cette instance `bpcd` est seulement créée temporairement et se ferme normalement. La commande `bpcd` parent est inchangée.
Problème connu lorsque les clusters utilisent l'AT partagé avec les fichiers de configuration sur le lecteur partagé	Le fait que des clusters utilisent l'AT partagé avec les fichiers de configuration sur le lecteur partagé est un problème connu. Le décrochage des services partagés fonctionne uniquement sur le nœud où ce lecteur partagé est accessible. Le décrochage échoue sur les nœuds restants. Cela implique que l'exécution de `bpnbaz -SetupMaster` pour gérer des parties du courtier distant est un échec. Vous devrez configurer manuellement les nœuds passifs. Exécutez `bpnbaz -SetupMedia` pour chaque nœud passif.
Problème connu relatif aux utilitaires de base de données prenant en charge `NBAZDB`	Le fait que certains utilitaires de base de données prennent en charge `NBAZDB` et d'autres non est un problème connu. Les utilitaires de base de données suivants prennent en charge `NBAZDB` : `nbdb_backup`, `nbdb_move`, `nbdb_ping`, `nbdb_restore` et `nbdb_admin`. Les utilitaires suivants ne prennent pas en charge `NBAZDB` : `nbdb_unload` et `dbadm`.

Points de vérification de Windows

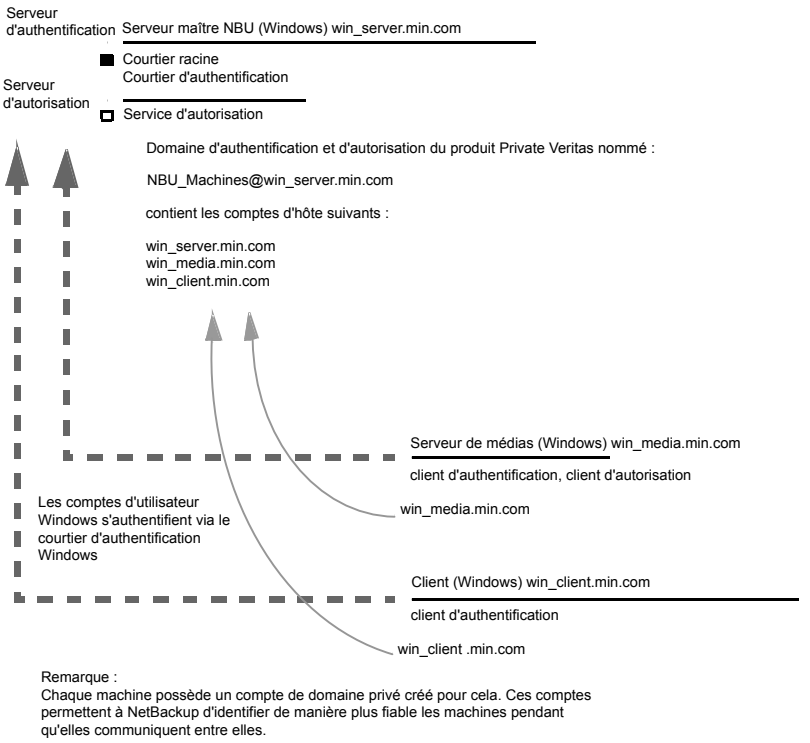
Les procédures de configuration suivantes peuvent vous aider à vérifier si le serveur maître, le serveur de médias et le client sont configurés correctement pour le contrôle d'accès.

Ces points de vérification Windows incluent :

- Se reporter à "Points de vérification du serveur maître pour Windows" à la page 237.
- Se reporter à "Points de vérification du serveur de médias pour Windows" à la page 241.
- Se reporter à "Windowspoints de vérification client" à la page 243.

Figure 14-1 affiche une configuration d'exemple contenant des systèmes Windows uniquement.

Figure 14-1 Configuration d'exemple contenant des systèmes de Windows uniquement



Points de vérification du serveur maître pour Windows

Les rubriques suivantes décrivent les procédures pour :

- Vérifier les paramètres Windows de serveur maître.
- Vérifier les ordinateurs autorisés à effectuer des recherches d'autorisation.
- Vérifier que la base de données est configurée correctement.
- Vérifier que les processus `nbatd` et `nbazd` sont en cours d'exécution.
- Vérifier que les propriétés d'hôte sont configurées correctement.

Le tableau suivant décrit les procédures de vérification de serveur maître pour Windows.

Tableau 14-6 Procédures de vérification de serveur maître pour Windows

Procédure	Description

Vérifier les paramètres de serveur maître Windows	Vous pouvez déterminer le domaine dans lequel un hôte est enregistré (où réside le courtier d'authentification principal). Ou vous pouvez déterminer le nom de l'ordinateur que le certificat représente. Exécutez `bpnbat` avec `-whoami` et spécifiez le fichier des informations d'authentification de l'hôte. Les informations d'authentification de serveur se trouvent dans le répertoire `c:\Program Files\Veritas\Netbackup\var\vxss\credentials\`….
	
	Par exemple :
	
	`bpnbat -whoami -cf "c:\Program Files\Veritas\Netbackup\var\vxss\credentials\ win_master"`
	`Name: win_master.company.com`
	`Domain: NBU_Machines@win_master.company.com`
	`Issued by: /CN=broker/OU=root@win_master.company.com/ O=vx`
	`Expiry Date: Oct 31 20:17:51 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`
	
	Si le domaine listé n'est pas NBU_Machines@win_master.company.com, considérez l'exécution de la commande `bpnbat -addmachine` pour le nom en question (win_master). Cette commande est exécutée sur l'ordinateur dont le courtier d'authentification sert le domaine NBU_Machines (win_master).
	
	Puis, sur l'ordinateur où vous voulez placer le certificat (win_master), exécutez :
	
	`bpnbat -loginmachine`
	
	Remarque : Ayant déterminé l'heure d'expiration des informations d'authentification d'un utilisateur, gardez à l'esprit que la sortie affiche l'heure d'expiration GMT, et non pas l'heure locale.
	
	Remarque : Pour les procédures restantes dans cette section de vérification, supposez que les commandes sont exécutées depuis une fenêtre de la console, et que l'identité de l'utilisateur en question a exécuté `bpnbat -login` depuis cette fenêtre. L'utilisateur est une identité membre du groupe NBU_Security Admin. Cette identité est généralement la première identité avec laquelle la sécurité a été installée.

Procédure	Description
Vérifier les ordinateurs présents dans le courtier d'authentification	Pour vérifier quels sont les ordinateurs présents dans le courtier d'authentification, connectez-vous en tant que membre du groupe d'administrateurs et exécutez la commande suivante : `bpnbat -ShowMachines` Cette commande affiche les ordinateurs pour lesquels vous avez exécuté `bpnbat -AddMachine`. **Remarque :** Si un hôte n'est pas sur la liste, exécutez `bpnbat -AddMachine` depuis le serveur maître. Exécutez ensuite `bpnbat -loginMachine` depuis l'hôte en question.

Vérifier les ordinateurs autorisés à effectuer des recherches d'autorisation	Pour vérifier quels sont les ordinateurs autorisés à effectuer des recherches d'autorisation, connectez-vous en tant que membre du groupe d'administrateurs et exécutez la commande suivante :
	
	`bpnbaz -ShowAuthorizers`
	
	Cette commande indique que win_master et win_media (serveur maître et serveur de médias) sont autorisés à effectuer des recherches d'autorisation. Notez que les deux serveurs sont authentifiés contre le même domaine privé (type de domaine vx), NBU_Machines@win_master.company.com.
	
	Remarque : Exécutez cette commande en tant qu'administrateur local ou en tant que `root`. L'administrateur local doit être un membre du groupe d'utilisateurs NBU_Security Admin.
	
	`bpnbaz -ShowAuthorizers`
	`==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@win_master.company.com`
	`Name: win_master.company.com`
	`==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@win_master.company.com`
	`Name: win_media.company.com`
	`Operation completed successfully.`
	
	Si un serveur maître ou un serveur de médias n'est pas sur la liste des ordinateurs autorisés, exécutez `bpnbaz -allowauthorization server_name` pour ajouter l'ordinateur manquant.

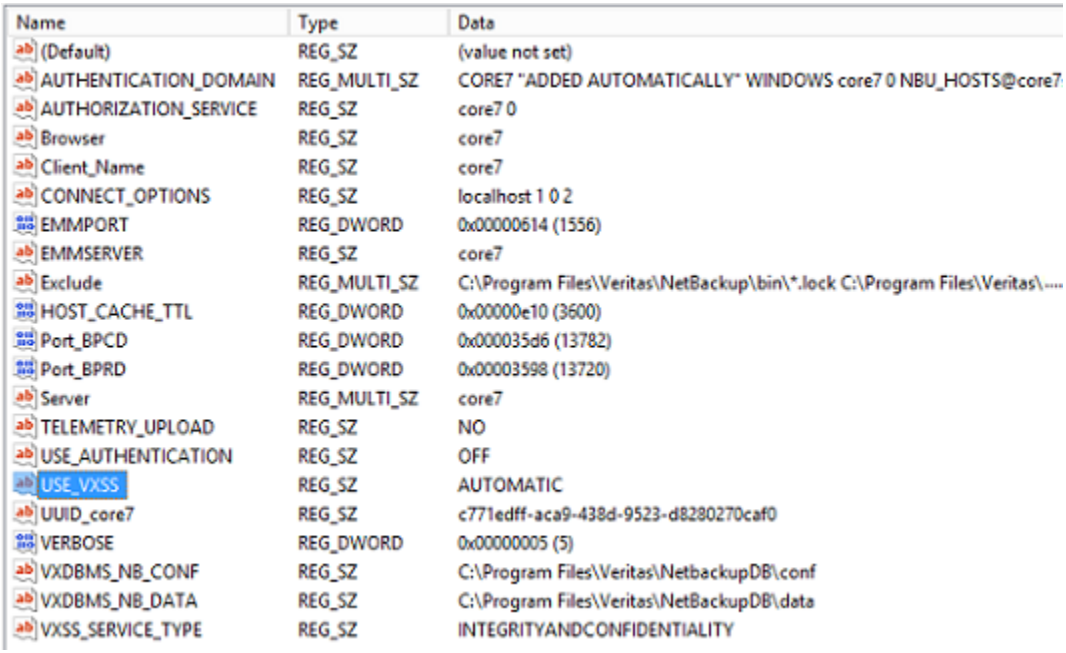
Procédure	Description

Vérifier que la base de données est correctement configurée	Pour vérifier que la base de données est configurée correctement, exécutez `bpnbaz -listgroups` :
	
	`bpnbaz -listgroups`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_SAN Admin`
	`NBU_User`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	
	Si les groupes n'apparaissent pas ou si `bpnbaz -listmainobjects` ne renvoie pas les données, vous devez exécuter `bpnbaz -SetupSecurity`.

Vérifier que les processus `nbatd` et `nbazd` sont en cours d'exécution	Le Gestionnaire des tâches de Windows vous permet de vérifier que `nbatd.exe` et `nbazd.exe` sont en cours d'exécution sur l'hôte indiqué. Si nécessaire, démarrez-les.
Vérifier que les propriétés d'hôte sont correctement configurées	Dans les propriétés d'hôte de contrôle d'accès, vérifiez que la propriété NetBackup Authentication and Authorization est définie correctement. (Le paramètre est défini sur Automatique ou sur Requis, selon que les ordinateurs utilisent NetBackup Authentication and Authorization ou non. Si tous les ordinateurs n'utilisent pas NetBackup Authentication and Authorization, définissez-le sur Automatique.) Les propriétés d'hôte peuvent également être vérifiées en regardant USE_VXSS dans le registre à : `HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\config.` Figure 14-2 pour un exemple des paramètres de propriétés d'hôte dans l'onglet Domaine d' **authentification**. Dans les propriétés d'hôte de **Contrôle d'accès**, vérifiez que les domaines d'authentification énumérés sont correctement orthographiés et indiquez les serveurs appropriés (courtiers d'authentification valides). Si tous les domaines sont basés sur Windows, ils doivent indiquer un ordinateur Windows qui exécute le courtier d'authentification.

Le schéma suivant affiche les paramètres des propriétés d'hôte dans l'onglet Domaine d' **authentification**.

Figure 14-2 Paramètres des propriétés d'hôte



Name	Type	Data
(Default)	REG_SZ	(value not set)
AUTHENTICATION_DOMAIN	REG_MULTI_SZ	CORE7 "ADDED AUTOMATICALLY" WINDOWS core7 0 NBU_HOSTS@core7
AUTHORIZATION_SERVICE	REG_SZ	core7 0
Browser	REG_SZ	core7
Client_Name	REG_SZ	core7
CONNECT_OPTIONS	REG_SZ	localhost 1 0 2
EMMPORT	REG_DWORD	0x00000614 (1556)
EMMSERVER	REG_SZ	core7
Exclude	REG_MULTI_SZ	C:\Program Files\Veritas\NetBackup\bin*.lock C:\Program Files\Veritas\...
HOST_CACHE_TTL	REG_DWORD	0x00000e10 (3600)
Port_BPCD	REG_DWORD	0x000035d6 (13782)
Port_BPRD	REG_DWORD	0x00003598 (13720)
Server	REG_MULTI_SZ	core7
TELEMETRY_UPLOAD	REG_SZ	NO
USE_AUTHENTICATION	REG_SZ	OFF
USE_VXSS	REG_SZ	AUTOMATIC
UUID_core7	REG_SZ	c771edff-aca9-438d-9523-d8280270caf0
VERBOSE	REG_DWORD	0x00000005 (5)
VXDBMS_NB_CONF	REG_SZ	C:\Program Files\Veritas\NetbackupDB\conf
VXDBMS_NB_DATA	REG_SZ	C:\Program Files\Veritas\NetBackupDB\data
VXSS_SERVICE_TYPE	REG_SZ	INTEGRITYANDCONFIDENTIALITY

Points de vérification du serveur de médias pour Windows

Les rubriques suivantes décrivent les procédures de vérification de serveur de médias Sous Windows :

- Vérifiez le serveur de médias.
- Vérifiez que le serveur a accès à la base de données d'autorisation.
- Impossible de charger le message de la bibliothèque

Le tableau suivant décrit les procédures de vérification de serveur de médias pour Windows.

Tableau 14-7 Procédures de vérification de serveur de médias pour Windows

Procédure	Description

Vérifier le serveur de médias	Pour déterminer contre quel courtier d'authentification le serveur de médias est authentifié, exécutez `bpnbat -whoami` avec `-cf` pour le fichier d'informations d'authentification du serveur de médias. Les informations d'authentification de serveur se trouvent dans le répertoire `c:\Program Files\Veritas\Netbackup\var\vxss\credentials\`….
	
	Par exemple :
	
	`bpnbat -whoami -cf "c:\Program Files\Veritas\Netbackup\var\vxss\credentials\ win_media.company.com"`
	`Name: win_media.company.com`
	`Domain: NBU_Machines@win_master.company.com`
	`Issued by: /CN=broker/OU=root@win_master.company.com/ O=vx`
	`Expiry Date: Oct 31 20:11:40 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`
	
	Si le domaine listé n'est pas NBU_Machines@win_master.company.com, considérez l'exécution de la commande `bpnbat -addmachine` pour le nom en question (win_media). Cette commande est exécutée sur l'ordinateur dont le courtier d'authentification sert le domaine NBU_Machines (win_master).
	
	Puis, sur l'ordinateur où vous voulez placer le certificat (win_media), exécutez :
	
	`bpnbat -loginmachine`

Procédure	Description

Vérifiez que le serveur a accès à la base de données d'autorisation	Pour vérifier que le serveur de médias peut accéder à la base de données d'autorisation dont il a besoin, exécutez `bpnbaz -ListGroups -CredFile "machine_credential_file"`
	
	Par exemple :
	
	`bpnbaz -ListGroups -CredFile "C:\Program Files\Veritas\NetBackup\var\vxss\credentials\ win_media.company.com"`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_SAN Admin`
	`NBU_User`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	
	Si cette commande échoue, exécutez `bpnbaz -AllowAuthorization` sur le serveur maître qui est le serveur d'autorisation (win_master.company.com).

Impossible de charger le message de bibliothèque	Vérifiez le serveur de médias et qu'il a accès à la base de données appropriée. Cette vérification vous informe indirectement que les bibliothèques client **NetBackup Authentication and Authorization** pour l'authentification et l'autorisation sont correctement installées. Si l'une ou l'autre de ces procédures échoue avec le message "Impossible de charger les bibliothèques", assurez-vous que les bibliothèques client d'authentification et d'autorisation sont installées. Vous pouvez également vérifier que les domaines d'authentification sont corrects en affichant les propriétés d'hôte de contrôle d'accès pour ce serveur de médias.

Windowspoints de vérification client

Vérifiez que les bibliothèques client d'authentification sont installées.

- Vérifiez que les domaines d'authentification sont corrects.
- Le tableau suivant décrit les procédures de vérification client pour Windows.
- Vérifiez que les domaines d'authentification sont corrects.

Le tableau suivant décrit les procédures de vérification client pour Windows.

Tableau 14-8 Procédures de vérification client pour Windows

Procédure	Description

Vérifier les informations d'authentification du client	Vérifiez que les informations d'authentification du client correspondent bien au client et qu'elles proviennent du domaine approprié. Exécutez `bpnbat -whoami` avec -cf comme fichier d'informations d'authentification du client.
	
	Par exemple :
	
	`bpnbat -whoami -cf "install_path`
	`\Netbackup\var\vxss\credentials\`
	`win_client.company.com`
	`"`
	`Name: win_client.company.com`
	`Domain: NBU_Machines@win_master.company.com`
	`Issued by: /CN=broker/OU=root@win_master.company.com/`
	`O=vx`
	`Expiry Date: Oct 31 20:11:45 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`
	
	Si le domaine listé n'est pas NBU_Machines@win_master.company.com, considérez l'exécution de la commande `bpnbat -addmachine` pour le nom en question (win_client). Cette commande est exécutée sur l'ordinateur dont le courtier d'authentification sert le domaine NBU_Machines (win_master).
	
	Puis, sur l'ordinateur où vous voulez placer le certificat (win_client), exécutez : `bpnbat -loginmachine`

Vérifier que les bibliothèques client d'authentification sont installées	**Remarque :**
	
	Exécutez `bpnbat -login` sur le client pour vérifier que les bibliothèques client d'authentification sont installées.
	
	`bpnbat -login`
	`Authentication Broker: win_master`
	`Authentication port [Enter = default]:`
	`Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd)`
	`: WINDOWS`
	`Domain: ENTERPRISE`
	`Name: Smith`
	`Password:Operation completed successfully.`
	
	Si les bibliothèques ne sont pas installées, un message s'affiche : Les bibliothèques NetBackup Authentication and Authorization ne sont pas installées. Cette vérification peut également être faite en regardant Ajout/Suppression de programmes Windows.

Procédure	Description
Vérifiez que les domaines d'authentification sont corrects	Vérifiez que tous les domaines d'authentification définis pour le client sont corrects dans les propriétés d'hôte de **Contrôle d'accès** ou à l'aide de la commande `regedit`. Vérifiez que les domaines sont correctement orthographiés. Vérifiez que les courtiers d'authentification qui sont listés pour chacun des domaines sont valides pour ce type de domaine.

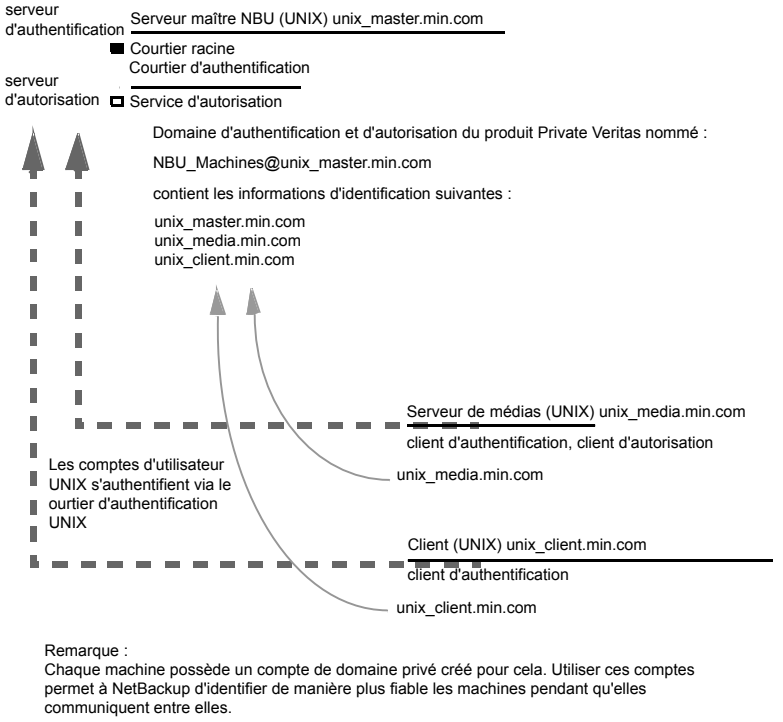
Points de vérification UNIX

Les procédures suivantes (ainsi que le schéma ci-dessous) vous permettent de vérifier si le serveur maître, le serveur de médias et le client UNIX sont configurés correctement pour le contrôle d'accès :

- Vérification de serveur maître UNIX
  Se reporter à "Vérification de serveur maître UNIX" à la page 246.
- Vérification de serveur de médias UNIX
  Se reporter à "Vérification de serveur de médias UNIX" à la page 249.
- Vérification de client UNIX
  Se reporter à "Vérification de client UNIX" à la page 251.

L'exemple suivant affiche une configuration d'exemple contenant seulement des systèmes UNIX.

Figure 14-3 Configuration d'exemple contenant des systèmes UNIX seulement



Vérification de serveur maître UNIX

Utilisez les procédures suivantes pour vérifier le serveur maître UNIX :

- Vérifier les paramètres de serveur maître UNIX.
- Vérifier les ordinateurs autorisés à effectuer des recherches d'autorisation.
- Vérifier que la base de données est configurée correctement.
- Vérifier que les processus `nbatd` et `nbazd` sont en cours d'exécution.
- Vérifier que les propriétés d'hôte sont configurées correctement.

Le tableau suivant décrit le processus de vérification pour le serveur maître UNIX.

Tableau 14-9 Processus de vérification pour le serveur maître UNIX

Processus	Description

Vérifier les paramètres de serveur maître UNIX	Déterminez dans quel domaine un hôte est enregistré (où réside le courtier d'authentification principal) et déterminez le nom de l'ordinateur que le certificat représente. Exécutez `bpnbat` avec `-whoami` avec `-cf` pour le fichier d'informations d'authentification du serveur maître. Les informations d'authentification du serveur se trouvent dans le répertoire `/usr/openv/var/vxss/credentials/`.
	
	Par exemple :
	
	`bpnbat -whoami -cf`
	`/usr/openv/var/vxss/credentials/unix_master.company.com`
	`Name: unix_master.company.com`
	`Domain: NBU_Machines@unix_master.company.com`
	`Issued by: /CN=broker/OU=root@unix_master/O=vx`
	`Expiry Date: Oct 31 15:44:30 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`
	
	Si le domaine listé n'est pas NBU_Machines@unix_master.company.com, ou si le fichier n'existe pas, considérez l'exécution de la commande `bpnbat -addmachine` pour le nom en question (unix_master). Exécutez cette commande sur l'ordinateur qui sert le domaine NBU_Machines (unix_master).
	
	Puis, sur l'ordinateur où vous voulez placer le certificat (unix_master), exécutez : `bpnbat -loginmachine`
	
	Remarque : Lorsque vous déterminez si les informations d'authentification sont arrivées à expiration, souvenez-vous que la sortie affiche l'heure d'expiration GMT, et non pas l'heure locale.
	
	Remarque : Pour les procédures restantes dans cette rubrique de vérification, supposez que les commandes sont exécutées depuis une fenêtre de la console. La fenêtre dans laquelle l'identité de l'utilisateur est en question a exécuté `bpnbat -login` en utilisant une identité membre du groupe NBU_Security Admin. Cette identité est généralement la première identité avec laquelle la sécurité a été installée.

Vérifier les ordinateurs présents dans le courtier d'authentification	Pour vérifier quels sont les ordinateurs présents dans le courtier d'authentification, connectez-vous en tant que membre du groupe d'administrateurs et exécutez la commande suivante :
	
	`bpnbat -ShowMachines`
	
	La commande suivante affiche les ordinateurs que vous avez exécutés :
	
	`bpnbat -AddMachine`

Processus	Description

Vérifier les ordinateurs autorisés à effectuer des recherches d'autorisation	Pour vérifier quels sont les ordinateurs autorisés à effectuer des recherches d'autorisation, connectez-vous en tant que racine sur le courtier d'autorisation et exécutez la commande suivante :
	
	`bpnbaz -ShowAuthorizers`
	` ==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@unix_master.company.com`
	`Name: unix_master.company.com`
	
	` ==========`
	`Type: User`
	`Domain Type: vx`
	`Domain:NBU_Machines@unix_master.company.com`
	`Name: unix_media.company.com`
	
	`Operation completed successfully.`
	
	Cette commande indique qu'unix_master et unix_media sont autorisés à effectuer des recherches d'autorisation. Notez que les deux serveurs sont authentifiés contre le même domaine vx (domaine privé Veritas), NBU_Machines@unix_master.company.com.
	
	Si un serveur maître ou un serveur de médias ne fait pas partie de la liste des ordinateurs autorisés, exécutez `bpnbaz -allowauthorization <server_name>` pour ajouter l'ordinateur manquant.

Vérifier que la base de données est correctement configurée	Pour vérifier que la base de données est configurée correctement, exécutez `bpnbaz -listgroups` :
	
	`bpnbaz -listgroups`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_SAN Admin`
	`NBU_User`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	
	Si les groupes n'apparaissent pas ou si `bpnbaz -listmainobjects` ne renvoie pas les données, exécutez `bpnbaz -SetupSecurity`.

Processus	Description

Vérifier que les processus nbatd et nbazd sont en cours d'exécution	Exécutez la commande `ps` pour vérifier que les processus `nbatd` et `nbazd` sont en cours d'exécution sur l'hôte indiqué. Si nécessaire, démarrez-les.
	Par exemple :
	`ps -fed |grep vx`
	`root 10716 1 0 Dec 14 ? 0:02 /usr/openv/netbackup/bin/private/nbatd`
	`root 10721 1 0 Dec 14 ? 4:17 /usr/openv/netbackup/bin/private/nbazd`

Vérifier que les propriétés d'hôte sont correctement configurées	Dans les propriétés d'hôte de **Contrôle d'accès**, vérifiez que la propriété **NetBackup Authentication and Authorization** est définie correctement. (Le paramètre est défini sur **Automatique** ou **Requis**, selon que tous les ordinateurs utilisent **NetBackup Authentication and Authorization** ou non. Si tous les ordinateurs n'utilisent pas **NetBackup Authentication and Authorization**, définissez-le sur **Automatique**.)
	Dans les propriétés d'hôte de **Contrôle d'accès**, vérifiez que les domaines d'authentification de la liste sont correctement orthographiés. Vérifiez également qu'ils indiquent les serveurs appropriés (courtiers d'authentification valides). Si tous les domaines sont basés sur UNIX, ils doivent indiquer un ordinateur UNIX qui exécute le courtier d'authentification.
	Ce processus peut également être vérifié dans `bp.conf` en utilisant `cat`.
	`cat bp.conf`
	`SERVER = unix_master`
	`SERVER = unix_media`
	`CLIENT_NAME = unix_master`
	`AUTHENTICATION_DOMAIN = company.com "default company NIS namespace"`
	`NIS unix_master 0`
	`AUTHENTICATION_DOMAIN = unix_master "unix_master password file"`
	`PASSWD unix_master 0`
	`AUTHORIZATION_SERVICE = unix_master.company.com 0`
	`USE_VXSS = AUTOMATIC`
	`#`

Vérification de serveur de médias UNIX

Pour vérifier le serveur de médias UNIX, procédez comme suit :

- Vérifiez le serveur de médias.
- Vérifiez que le serveur a accès à la base de données d'autorisation.
- Considérez l'impossibilité à charger le message de la bibliothèque.

Le tableau suivant décrit les procédures de vérification pour le serveur de médias UNIX.

Tableau 14-10 Processus de vérification pour le serveur de médias UNIX

Processus	Description

Vérifier le serveur de médias	Pour déterminer contre quel courtier d'authentification le serveur de médias est authentifié, exécutez `bpnbat -whoami` avec -cf pour le fichier d'informations d'authentification du serveur de médias. Les informations d'authentification du serveur se trouvent dans le répertoire `/usr/openv/var/vxss/credentials/`.
	
	Par exemple :
	
	`bpnbat -whoami -cf`
	`/usr/openv/var/vxss/credentials/unix_media.company.com`
	`Name: unix_media.company.com`
	`Domain: NBU_Machines@unix_master.company.com`
	`Issued by: /CN=broker/OU=root@unix_master.company.com/`
	`O=vx`
	`Expiry Date: Oct 31 14:48:08 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`
	
	Si le domaine listé n'est pas NBU_Machines@unix_master.company.com, considérez l'exécution de la commande `bpnbat -addmachine` pour le nom en question (unix_media). Cette commande est exécutée sur l'ordinateur dont le courtier d'authentification sert le domaine NBU_Machines (unix_master).
	
	Puis, sur l'ordinateur où vous voulez placer le certificat (unix_master), exécutez : `bpnbat -loginmachine`

Vérifiez que le serveur a accès à la base de données d'autorisation	Pour vérifier que le serveur de médias peut accéder à la base de données d'autorisation dont il a besoin, exécutez `bpnbaz -ListGroups`
	
	"machine_credential_file"
	
	Par exemple :
	
	`bpnbaz -ListGroups -CredFile`
	`/usr/openv/var/vxss/credentials/unix_media.company.com`
	`NBU_User`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	
	Si cette commande échoue, exécutez `bpnbaz -AllowAuthorization` sur le serveur maître qui est le serveur d'autorisation (unix_master). Notez que vous devez être connecté en tant que racine ou administrateur.

Processus	Description
Impossible de charger le message de bibliothèque	Vérifiez le serveur de médias et qu'il a accès à la base de données appropriée. Cette vérification vous informe indirectement que les bibliothèques client NetBackup Authentication and Authorization pour l'authentification et l'autorisation sont correctement installées. Si l'une de ces procédures échoue et affiche le message "impossible de charger les bibliothèques," vérifiez que les bibliothèques client d'authentification et d'autorisation sont bien installées. Vous pouvez également vérifier que les domaines d'authentification sont corrects. Effectuez cette vérification en affichant les propriétés d'hôte de contrôle d'accès pour ce serveur de médias ou en utilisant `cat(1)ing` pour le fichier `bp.conf`.

Vérification de client UNIX

Les procédures suivantes sont utilisées pour vérifier le client UNIX :

- Vérifier les informations d'authentification du client UNIX.
- Vérifiez que les bibliothèques client d'authentification sont installées.
- Vérifiez que les domaines d'authentification sont corrects.

Le tableau suivant décrit les procédures de vérification pour le client UNIX.

Tableau 14-11 Procédures de vérification pour le client UNIX

Procédures	Description

Vérifier les informations d'authentification du client UNIX	Vérifiez que les informations d'authentification du client correspondent bien au client et qu'elles proviennent du domaine approprié. Exécutez `bpnbat -whoami` avec -cf comme fichier d'informations d'authentification du client.
	
	Par exemple :
	
	`bpnbat -whoami -cf`
	`/usr/openv/var/vxss/credentials/unix_client.company.com`
	`Name: unix_client.company.com`
	`Domain: NBU_Machines@unix_master.company.com`
	`Issued by: /CN=broker/OU=root@unix_master.company.com/O=vx`
	`Expiry Date: Oct 31 14:49:00 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`
	
	Si le domaine listé n'est pas NBU_Machines@unix_master.company.com, considérez l'exécution de la commande `bpnbat -addmachine` pour le nom en question (unix_client). Cette commande est exécutée sur l'ordinateur dont le courtier d'authentification sert le domaine NBU_Machines (unix_master).
	
	Puis, sur l'ordinateur où vous voulez placer le certificat (unix_client), exécutez : `bpnbat -loginmachine`

Vérifier que les bibliothèques client d'authentification sont installées	Exécutez `bpnbat -login` sur le client pour vérifier que les bibliothèques client d'authentification sont installées.
	
	`bpnbat -login`
	`Authentication Broker: unix_master.company.com`
	`Authentication port [Enter = default]:`
	`Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd): NIS`
	`Domain: min.com`
	`Name: Smith`
	`Password:`
	`Operation completed successfully.`

Procédures	Description

Vérifiez que les domaines d'authentification sont corrects	Vérifiez que tous les domaines d'authentification définis pour le client sont corrects dans les propriétés d'hôte de **Contrôle d'accès** ou à l'aide de la commande `cat(1)`. Vérifiez que les domaines sont correctement orthographiés. Vérifiez également que les courtiers d'authentification qui sont listés pour chacun des domaines sont valides pour ce type de domaine.
	
	Ce processus peut également être vérifié dans `bp.conf` en utilisant `cat(1)`.
	
	`cat bp.conf`
	`SERVER = unix_master`
	`SERVER = unix_media`
	`CLIENT_NAME = unix_master`
	`AUTHENTICATION_DOMAIN = min.com "default company NIS namespace"`
	`NIS unix_master 0`
	`AUTHENTICATION_DOMAIN = unix_master.company.com "unix_master password file" PASSWD unix_master 0`
	`AUTHORIZATION_SERVICE = unix_master.company.com 0`
	`USE_VXSS = AUTOMATIC`

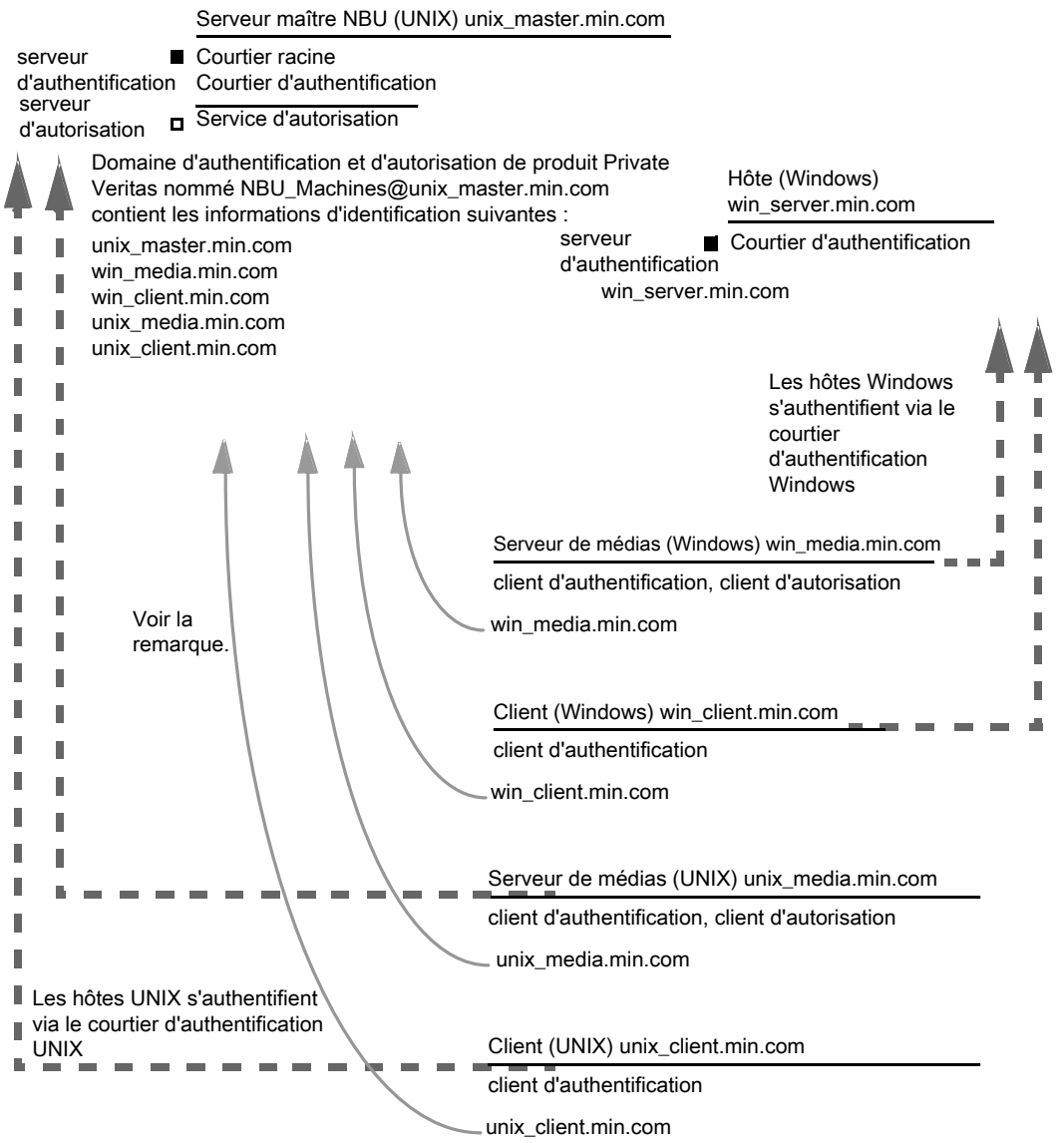
Points de vérification dans un environnement mixte avec un serveur maître UNIX

Les procédures suivantes permettent de vérifier la configuration du serveur maître, du serveur de médias et du client. Ceux-ci doivent être configurés pour un environnement hétérogène NetBackup Access Control. Le serveur maître est un ordinateur UNIX.

- Points de vérification du serveur maître pour système UNIX mixte
- Points de vérification du serveur de médias pour système UNIX mixte
- Points de vérification client pour système UNIX mixte

Figure 14-4 pour un exemple de configuration mixte contenant un serveur maître UNIX.

Figure 14-4 Exemple de configuration mixte contenant un serveur maître UNIX



Remarque :
Chaque machine possède un compte de domaine privé. Grâce à ces comptes, NetBackup peut identifier les machines avec plus de fiabilité lorsqu'elles communiquent entre elles.

Vérification de serveur maître pour un serveur maître mixte UNIX

Consultez la rubrique suivante pour voir la procédure de vérification pour un serveur maître UNIX :

Se reporter à "Vérification de serveur maître UNIX" à la page 246.

Points de vérification de serveur de médias pour un serveur maître mixte UNIX

Le tableau suivant décrit les procédures de vérification de serveur de médias pour un serveur maître mixte UNIX.

Tableau 14-12 Procédures de vérification pour un serveur maître mixte UNIX

Procédure	Description
Vérifiez le serveur de médias UNIX	Consultez la rubrique suivante pour voir la procédure de vérification pour un serveur de médias UNIX : Se reporter à "Vérification de serveur de médias UNIX" à la page 249.

Vérifiez le serveur de médias Windows	Vérifiez que le certificat d'ordinateur provient du courtier d'authentification racine qui figure sur le serveur maître UNIX (unix_master).
	
	S'il manque un certificat, exécutez les commandes suivantes pour corriger le problème :
	
	■ `bpnbat -addmachine` sur le courtier d'authentification racine (dans cet exemple, unix_master)
	■ `bpnbat -loginmachine` (dans cet exemple, win_media)
	
	Par exemple :
	
	`bpnbat -whoami -cf "install_path`
	`\Netbackup\var\vxss\credentials\`
	`win_media.company.com"`
	`Name: win_media.company.com`
	`Domain: NBU_Machines@unix_master.company.com`
	`Issued by: /CN=broker/OU=root@`
	`unix_master.company.com/O=vx`
	`Expiry Date: Oct 31 20:11:04 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`

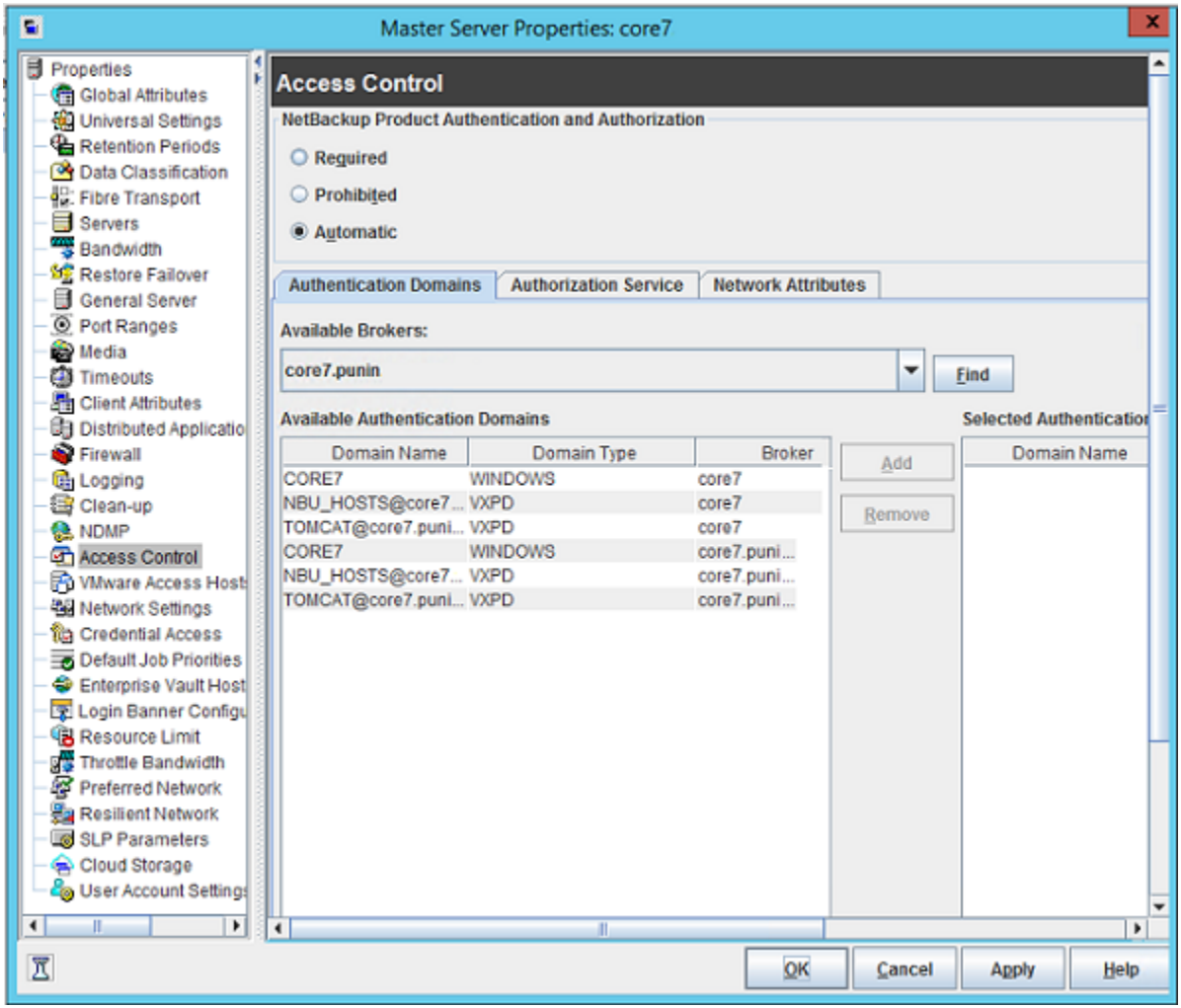
Procédure	Description

Vérifiez qu'un serveur de médias est en droit d'effectuer des consultations d'autorisation	Assurez-vous que le serveur de médias est en droit d'effectuer des contrôles d'autorisation en exécutant `bpnbaz -listgroups -CredFile`.
	
	Par exemple :
	
	`bpnbaz -listgroups -CredFile "install_path\Netbackup\var\vxss\credentials\ win_media.company.com"`
	`NBU_User`
	`NBU_Operator`
	`NBU_Admin`
	`NBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	
	Si le serveur de médias n'est pas en droit d'effectuer des contrôles d'autorisation, exécutez `bpnbaz -allowauthorization` sur le serveur maître pour le nom de serveur de médias en question.

Impossible de charger le message de bibliothèque	Vérifiez que le serveur de médias Windows peut effectuer indirectement des contrôles d'autorisation. Cette vérification vous informe que les bibliothèques client **NetBackup Authentication and Authorization** sont correctement installées pour l'authentification et l'autorisation. Si l'une ou l'autre de ces procédures échoue avec le message "Impossible de charger les bibliothèques", assurez-vous que les bibliothèques client d'authentification et d'autorisation sont installées.
Vérifiez les domaines d'authentification	Vérifiez que les domaines d'authentification sont corrects en consultant les propriétés d'hôte de contrôle d'accès pour ce serveur de médias. Vous pouvez également utiliser `regedit` (ou `regedit32`) directement sur le serveur de médias à l'emplacement suivant : `HKEY_LOCAL_MACHINE\SOFTWARE\Veritas\NetBackup\CurrentVersion\config\AUTHENTICATION_DOMAIN`

Procédure	Description
Domaines d'authentification interplateformes	Dans les environnements mixtes, veillez à vous assurer que les types de domaine appropriés désignent les courtiers d'authentification corrects. L'exemple d'onglet de domaine d'authentification affiche les domaines d'authentification Windows disponibles pour être ajoutés au courtier Windows. Dans ce cas, il ne s'agit pas d'un environnement mixte car les deux systèmes sont basés sur Windows. En présence d'une combinaison de domaines Windows et UNIX, il est important de faire correspondre les courtiers aux domaines d'authentification les plus utiles. Figure 14-5 pour afficher des informations sur la correspondance de la plateforme avec les domaines d'authentification les plus utiles.

Figure 14-5 Domaines d'authentification interplateformes



Points de vérification client pour un serveur maître mixte UNIX

Consultez la rubrique suivante pour les procédures de vérification des ordinateurs client UNIX :

Se reporter à "Vérification de client UNIX" à la page 251.

Le tableau suivant décrit les procédures pour vérifier les clients Windows.

Tableau 14-13 Procédures pour vérifier les clients Windows

Procédures	Description

Vérifier les informations d'authentification du client Windows	Vérifiez que les informations d'authentification du client correspondent bien au client et qu'elles proviennent du domaine approprié. Exécutez `bpnbat -whoami` avec -cf comme fichier d'informations d'authentification du client.
	Par exemple :
	`bpnbat -whoami -cf "c:\Program Files\Veritas\Netbackup\var\vxss\credentials\ win_client.company.com`
	`Name: win_client.company.com`
	`Domain: NBU_Machines@unix_master.company.com`
	`Issued by: /CN=broker/OU=root@unix_master.company.com/ O=vx`
	`Expiry Date: Oct 31 19:50:50 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`

Vérifier que les bibliothèques client d'authentification sont installées	Exécutez `bpnbat -login` sur le client pour vérifier que les bibliothèques client d'authentification sont installées.
	Par exemple :
	`bpnbat -login`
	`Authentication Broker: unix_master.company.com`
	`Authentication port [Enter = default]:`
	`Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd) : NIS`
	`Domain: min.com`
	`Name: Smith`
	`Password:`
	`Operation completed successfully.`

Vérifier le courtier d'authentification Windows	Vérifiez que le courtier d'authentification Windows a établi une confiance mutuelle avec le courtier d'authentification UNIX principal. Vérifiez également qu'il utilise le courtier UNIX comme courtier racine.

Points de vérification dans un environnement mixte avec un serveur maître Windows

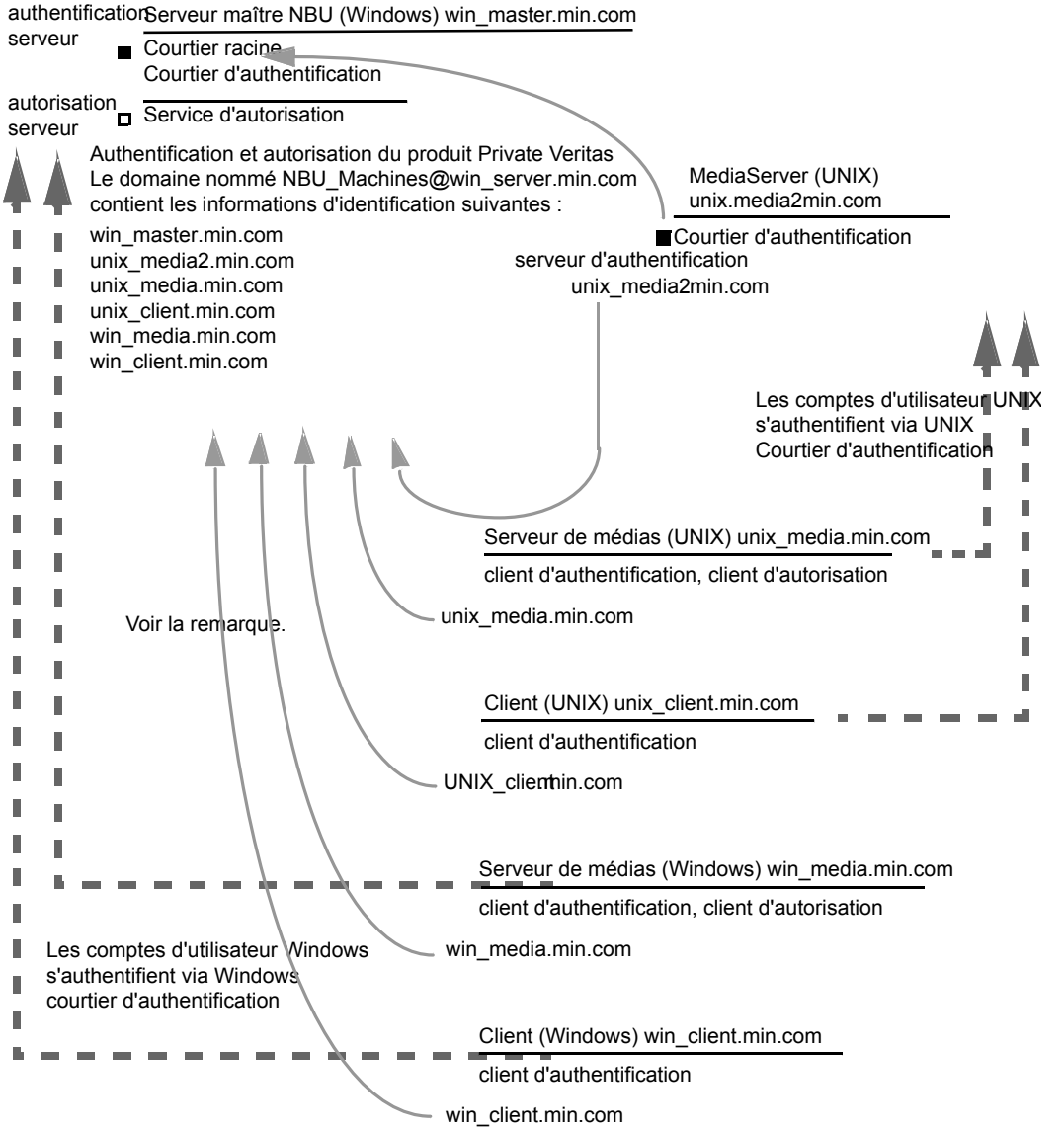
Les procédures suivantes permettent de vérifier la configuration du serveur maître, du serveur de médias et du client. Ils doivent être configurés pour un environnement NetBackup Access Control hétérogène. Le serveur maître est un ordinateur Windows.

- Points de vérification du serveur maître pour système Windows mixte
  Se reporter à "Points de vérification du serveur maître pour un serveur maître mixte UNIX" à la page 262.
- Points de vérification du serveur de médias pour système Windows mixte
  Se reporter à "Points de vérification du serveur maître pour un serveur maître mixte Windows" à la page 262.
- Points de vérification client pour système Windows mixte

Se reporter à "Points de vérification de client pour un serveur maître mixte Windows" à la page 264.

Figure 14-6 pour un exemple de configuration contenant un serveur maître Windows.

Figure 14-6 Exemple de configuration mixte contenant un serveur maître Windows



Remarque :
Chaque machine possède un compte de domaine privé. Grâce à ces comptes, NetBackup peut identifier de
plus fiable les machines pendant qu'elles communiquent entre elles.

Points de vérification du serveur maître pour un serveur maître mixte UNIX

Consultez la rubrique suivante pour les procédures de vérification pour un maître mixte de Windows :

Se reporter à "Points de vérification du serveur maître pour Windows" à la page 237.

Points de vérification du serveur maître pour un serveur maître mixte Windows

Le tableau suivant décrit les procédures de vérification de serveur de médias pour un serveur maître mixte Windows.

Tableau 14-14 Procédures de vérification de serveur maître pour un serveur maître mixte Windows

Procédure	Description
Vérifiez le serveur de médias Windows pour un serveur maître mixte Windows	Consultez la rubrique suivante pour les procédures de vérification d'un serveur de médias Windows : Se reporter à "Points de vérification du serveur de médias pour Windows" à la page 241.

Vérifiez le serveur de médias UNIX	Vérifiez que le certificat d'ordinateur est émis par le courtier d'authentification racine qui se trouve sur le serveur maître Windows (win_master). Pour déterminer sur quel courtier d'authentification l'authentification du serveur de médias est effectuée, exécutez `bpnbat -whoami` avec -cf comme fichier d'informations d'authentification du serveur de médias.
	
	Par exemple :
	
	`bpnbat -whoami -cf /usr/openv/var/vxss/credentials/unix_media.company.com`
	`Name: unix_media.company.comDomain: NBU_Machines@ win_master.company.com`
	`Issued by: /CN=broker/OU=root@win_master.company.com/ O=vx`
	`Expiry Date: Oct 31 14:48:08 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`

Procédure	Description

Vérifiez que le serveur a accès à la base de données d'autorisation	Pour s'assurer que le serveur de médias peut accéder la base de données d'autorisation, il doit effectuer des contrôles d'autorisation. Exécutez `bpnbaz -ListGroups -CredFile "/usr/openv/var/vxss/credentials/<hostname>"`
	
	Par exemple :
	
	`bpnbaz -ListGroups -CredFile\`
	`/usr/openv/var/vxss/credentials/unix_media.company.com`
	`NBU_Operator`
	`NBU_AdminNBU_SAN Admin`
	`NBU_UserNBU_Security Admin`
	`Vault_Operator`
	`Operation completed successfully.`
	
	Si le serveur de médias n'est pas en droit d'effectuer des contrôles d'autorisation, exécutez `bpnbaz -allowauthorization` sur le serveur maître pour le nom de serveur de médias en question.

Impossible de charger le message de la bibliothèque	Vérifiez le serveur de médias et son accès indirect à la base de données appropriée. Cette vérification vous informe que les bibliothèques client NetBackup Authentication and Authorization sont correctement installées pour l'authentification et l'autorisation. Si l'une ou l'autre de ces procédures échoue avec le message "Impossible de charger les bibliothèques", assurez-vous que les bibliothèques client d'authentification et d'autorisation sont installées.

Procédure	Description

Domaines d'authentification interplateformes	Vous pouvez également vérifier que les domaines d'authentification sont corrects en affichant les propriétés d'hôte de contrôle d'accès pour ce serveur de médias. Vous pouvez également effectuer la vérification en exécutant `cat(1)ing` sur le fichier `bp.conf`.
	
	Dans les environnements mixtes, veillez à vous assurer que les types de domaine appropriés désignent les courtiers d'authentification corrects.
	
	Dans l'exemple, notez que les domaines PASSWD et NIS désignent unix_media2.company.com qui, dans cet exemple, est le courtier d'authentification UNIX :
	
	`cat bp.conf`
	`SERVER = win_master.company.com`
	`MEDIA_SERVER = unix_media.company.com`
	`MEDIA_SERVER = unix_media2.company.com`
	`CLIENT_NAME = unix_media`
	`AUTHENTICATION_DOMAIN = win_master "win_master domain"`
	`WINDOWS win_master.company.com`
	`0`
	`AUTHENTICATION_DOMAIN = enterprise "enterprise domain"`
	`WINDOWS win_master.company.com 0`
	`AUTHENTICATION_DOMAIN = unix_media2.company.com "local`
	`unix_media2 domain" PASSWD unix_media2.company.com 0`
	`AUTHENTICATION_DOMAIN = min.com "NIS domain" NIS`
	`unix_media.company.com 0`
	`AUTHORIZATION_SERVICE = win_master.company.com 0`
	`USE_VXSS = AUTOMATIC`

Points de vérification de client pour un serveur maître mixte Windows

Le tableau suivant décrit les procédures de vérification de client pour un serveur maître mixte Windows.

Tableau 14-15 Procédures de vérification pour un serveur maître mixte Windows

Procédure	Description
Vérifiez les informations d'authentification du client Windows	Consultez la rubrique suivante pour les procédures de vérification des clients Windows : Se reporter à "Windowspoints de vérification client" à la page 243.

Procédure	Description

Vérification les informations d'authentification du client Windows	Vérifiez que les informations d'authentification du client correspondent bien au client et qu'elles proviennent du domaine approprié. Exécutez `bpnbat -whoami` avec -cf comme fichier d'informations d'authentification du client.
	Par exemple :
	`bpnbat -whoami -cf \`
	`"/usr/openv/var/vxss/credentials/`
	`unix_client.company.com"`
	`Name: unix_client.company.com`
	`Domain: NBU_Machines@win_master.company.com`
	`Issued by: /CN=broker/OU=root@`
	`win_master.company.com/O=vx`
	`Expiry Date: Oct 31 21:16:01 2007 GMT`
	`Authentication method: Veritas Private Security`
	`Operation completed successfully.`

Vérifier que les bibliothèques client d'authentification sont installées	Exécutez `bpnbat -login` sur le client pour vérifier que les bibliothèques client d'authentification sont installées.
	`bpnbat -login`
	`Authentication Broker: unix_media2.company.com`
	`Authentication port [Enter = default]:`
	`Authentication type (NIS, NIS+, WINDOWS, vx, unixpwd)`
	`: NIS`
	`Domain: min.com`
	`Name: Smith`
	`Password:`
	`You do not currently trust the server:`
	`unix_media.company.com, do`
	`you wish to tr`
	`ust it? (y/n):`
	`y`
	`Operation completed successfully.`

Vérification le courtier d'authentification UNIX	Assurez-vous que le courtier d'authentification UNIX bénéficie d'une confiance mutuelle avec le courtier d'authentification des fenêtres principales ou qu'il utilise le courtier Windows en tant que courtier racine.

A propos de l'utilitaire nbac_cron

Des opérations NetBackup peuvent être exécutées comme travaux planifiés, à l'aide de l'utilitaire cron. Quand NBAC est activé, ces travaux peuvent être exécutés dans le contexte d'un utilisateur du système d'exploitation disposant des privilèges

lui permettant d'exécuter les commandes requises. Vous pouvez utiliser l'utilitaire nbac_cron.exe pour créer les informations d'authentification qui sont nécessaires pour exécuter les travaux cron ou AT. Ces informations d'authentification sont valables plus longtemps que les informations d'authentification obtenues quand un utilisateur effectue une connexion `bpnbat`. Dans ce cas, la validité est d'un an.

L'utilitaire se trouve à l'emplacement suivant :

`-/opt/openv/netbackup/bin/goodies/nbac_cron`

Pour les étapes détaillées de configuration de l'utilitaire nbac_cron et d'exécution d'un travail cron, consultez la rubrique suivante :

Se reporter à "Utilisation de l'utilitaire nbac_cron" à la page 266.

Utilisation de l'utilitaire nbac_cron

Les étapes suivantes vous permettent de créer des informations d'authentification pour exécuter des travaux cron.

Utilisation de l'utilitaire nbac_cron pour exécuter des travaux cron

1. Exécutez la commande `nbac_cron-addCron` en tant qu'utilisateur racine ou administrateur sur le serveur maître.

```
root@amp# /usr/openv/netbackup/bin/goodies/nbac_cron -AddCron

# nbac_cron -AddCron

This application will generate a Veritas private domain identity
that can be used in order to run unattended cron and/or at jobs.

User name to create account for (e.g. root, JSmith etc.): Dan

Password:*****

Password:*****

Access control group to add this account to [NBU_Admin]:

Do you with to register this account locally for root(Y/N) ? N

In order to use the account created please login as the OS
identity that will run the at or cron jobs. Then run nbac_cron
-setupcron or nbac_cron -setupat. When nbac_cron -setupcron or
nbac_cron -setupat is run the user name, password and
authentication broker will need to be supplied. Please make note
of the user name, password, and authentication broker. You may
rerun this command at a later date to change the password for an
account.
```

```
Operation completed successfully.
```

Si vous ne spécifiez pas explicitement un groupe de contrôle d'accès (par exemple, NBU_Operator ou Vault_Operator) auquel ajouter l'utilisateur, l'utilisateur cron (ici, Daniel) est ajouté au groupe NBU_Admin.

Si vous répondez "Oui" pour enregistrer le compte localement pour l'utilisateur racine, la commande `nbac_cron –SetupCron` est automatiquement exécutée pour l'utilisateur cron (cron_user) en tant qu'utilisateur racine. Si vous prévoyez d'exécuter les travaux cron en tant qu'utilisateur de système d'exploitation non-racine, vous devez répondre "non" à cette question et exécuter manuellement la commande `nbac_cron –SetupCron` en tant qu'utilisateur de système d'exploitation non-racine.

Une identité est générée dans le domaine privé Veritas. Cette identité peut être utilisée pour exécuter les travaux cron.

2 Maintenant, exécutez la commande `nbac_cron-SetupCron` en tant qu'utilisateur du système d'exploitation qui veut exécuter les travaux cron pour obtenir les informations d'authentification pour cette identité.

```
[dan@amp ~]$ /usr/openv/netbackup/bin/goodies/nbac_cron -SetupCron

This application will now create your cron and/or at identity.

Authentication Broker: amp.sec.punin.sen.veritas.com

Name: Dan

Password:*****

You do not currently trust the server:
amp.sec.punin.sen.veritas.com, do you wish to trust it? (Y/N): Y

Created cron and/or at account information. To use this account
in your own cron or at jobs make sure that the environment
variable VXSS_CREDENTIAL_PATH is set to
"/home/dan/.vxss/credentials.crat"

Operation completed successfully.
```

Le message "Vous ne faites actuellement pas confiance au serveur" s'affiche une seule fois si vous n'avez pas déjà fait confiance au courtier.

Les informations d'authentification sont créées dans le répertoire d'origine de l'utilisateur : `user/.vxss/credentials.crat`. Les informations d'authentification sont valables un an à partir du moment où elles sont générées.

Si nécessaire, vous pouvez vérifier les informations d'authentification comme montré :

```
dan@amp~]$ /usr/openv/netbackup/bin/bpnbat -whoami -cf
~dan/.vxss/credentials.crat

Name: CronAt_dan

Domain: CronAtUsers@amp.sec.punin.sen.veritas.com

Issued by: /CN=broker/OU=amp.sec.punin.sen.veritas.com

Expiry Date: Feb 4 13:36:08 2016 GMT

Authentication method: Veritas Private Domain

Operation completed successfully.
```

Vous devez réexécuter l'opération `SetupCron` (étape 2) pour renouveler les informations d'authentification avant qu'elles n'expirent.

3 Vous pouvez maintenant créer vos propres travaux cron. Assurez-vous que le chemin d'accès `VXSS_CREDENTIAL_PATH` est défini pour rediriger vers les informations d'authentification que vous avez créées ci-dessus avant de planifier un nouveau travail.

Utilisation de l'utilitaire Gestion de l'accès

Les utilisateurs qui sont assignés au groupe d'utilisateurs **Administrateur de sécurité NetBackup** ont accès au nœud **Gestion de l'accès** dans NetBackup Administration Console. Les utilisateurs et administrateurs NetBackup affectés à un autre groupe d'utilisateurs peuvent consulter le nœud **Gestion de l'accès**. Ce nœud est visible dans **NetBackup Administration Console**, mais ne peut pas être développé.

Si un utilisateur autre qu'un Administrateur de sécurité tente de sélectionner **Gestion de l'accès**, un message d'erreur s'affiche. Les options de barre d'outils et éléments de menu spécifiques à la **Gestion de l'accès** ne sont pas affichés.

Une fois cette opération terminée, les groupes d'utilisateurs NetBackup par défaut doivent s'afficher dans la fenêtre **NetBackup Administration Console > Gestion de l'accès > Groupes d'utilisateurs NBU**.

Pour répertorier les groupes dans la ligne de commande, exécutez la commande `bpnbaz -ListGroups` sur l'ordinateur sur lequel le logiciel de serveur d'autorisation est installé.

UNIX

`bpnbaz` se trouve dans le répertoire `/usr/openv/netbackup/bin/admincmd`

Windows

`bpnbaz` se trouve dans le répertoire
`Install_path``\Veritas\NetBackup\bin\admincmd`

(vous devez être connecté en tant qu'Administrateur de sécurité à l'aide de `bpnbat -login`)

```
bpnbaz -ListGroups
 NBU_User
 NBU_Operator
 NBU_Admin
 NBU_Security Admin
 Vault_Operator
 NBU_SAN Admin
 NBU_KMS Admin
 Operation completed successfully.
```

Les groupes d'utilisateurs NetBackup sont répertoriés. Ce processus vérifie que l'administrateur de sécurité peut accéder aux groupes d'utilisateurs.

Détermination de l'accès à NetBackup

L'utilitaire **Gestion de l'accès** permet l'accès à un seul groupe d'utilisateur. Par défaut, le groupe d'utilisateurs NBU_Security Admin définit les aspects de la Gestion d'accès NetBackup :

- Autorisations des utilisateurs individuels ;
  Se reporter à "Utilisateurs individuels" à la page 270.
- Création de groupes d'utilisateurs.
  Se reporter à "Groupes d'utilisateurs" à la page 270.

Déterminez tout d'abord les ressources NetBackup auxquelles vos utilisateurs ont besoin d'accéder Pour les ressources et les autorisations associées :

Se reporter à "Affichage des autorisations d'utilisateur particulières des groupes d'utilisateurs NetBackup" à la page 277.

L'administrateur de sécurité doit tout d'abord déterminer les points communs des différents utilisateurs, puis créer des groupes d'utilisateurs avec les autorisations nécessaires pour ces utilisateurs. Les groupes d'utilisateurs correspondent généralement à un rôle, notamment les rôles d'administrateur, d'opérateur ou d'utilisateurs finaux.

Envisagez de baser les groupes d'utilisateurs sur un ou plusieurs des critères suivants :

- Unités fonctionnelles de votre entreprise (administration UNIX, par exemple) ;

- Ressources NetBackup (lecteurs, stratégies, par exemple) ;
- Emplacement (côte Est ou côte Ouest, par exemple) ;
- Responsabilités individuelles (opérateur de bande, par exemple).

Notez que les autorisations sont accordées aux membres des groupes d'utilisateurs et non en fonction de l'hôte. Les personnes peuvent agir dans la mesure accordée par leur autorisation. Aucune restriction n'est établie sur le nom de l'ordinateur.

Utilisateurs individuels

L'utilitaire **Gestion de l'accès** NetBackup utilise vos utilisateurs, groupes et domaines existants définis par le système d'exploitation. L'utilitaire **Gestion de l'accès** ne conserve aucune liste d'utilisateurs et de mots de passe. Lors de la définition des membres des groupes, l'administrateur de sécurité spécifie les utilisateurs du système d'exploitation existants en tant que membres des groupes d'utilisateurs.

Chaque utilisateur authentifié appartient à un groupe d'utilisateurs d'autorisation au minimum. Par défaut, chaque utilisateur appartient au groupe d'utilisateurs NBU_Users, qui contient tous les utilisateurs authentifiés.

Tous les utilisateurs authentifiés sont les membres implicites du groupe d'utilisateurs NBU_Users. Tous les autres groupes doivent avoir des membres définis explicitement. L'administrateur de sécurité NetBackup peut supprimer un membre ajouté manuellement à d'autres groupes. Cependant, l'administrateur de sécurité peut ne pas supprimer les membres implicites prédéfinis des groupes NBU_Security Admin. Les groupes et utilisateurs du système d'exploitation peuvent être ajoutés à un groupe d'autorisation.

Groupes d'utilisateurs

La fonction **Gestion de l'accès** NetBackup peut être configurée en assignant des autorisations aux groupes d'utilisateurs, puis en assignant des utilisateurs aux groupes d'utilisateurs. Généralement, les autorisations sont attribuées par groupe et non directement aux utilisateurs individuels.

Une fois l'installation réussie, NetBackup fournit les groupes d'utilisateurs par défaut complétant la manière dont les sites gèrent souvent les tâches du fonctionnement de NetBackup. Les groupes d'utilisateurs sont répertoriés sous `Access Management > NBU User Groups`. Le contenu de **Gestion de l'accès** est seulement visible aux membres du groupe NBU_Security Admin.

L'administrateur de sécurité peut utiliser les groupes d'utilisateurs NetBackup par défaut ou créer des groupes d'utilisateurs.

Groupes d'utilisateurs NetBackup par défaut

Les utilisateurs disposant d'autorisations dans chacun des groupes d'utilisateurs par défaut sont directement reliés au nom de groupe. En fait, l'objet d'une autorisation est relié à un nœud dans l'arborescence de **NetBackup Administration Console**.

Le tableau suivant présente chaque groupe d'utilisateurs NetBackup par défaut.

Tableau 14-16 Groupes d'utilisateurs NetBackup par défaut

Groupe d'utilisateurs par défaut	Description
Opérateur (NBU_Operator)	La tâche principale du groupe d'utilisateurs NBU_Operator est de contrôler les travaux. Par exemple, les membres du groupe d'utilisateurs NBU_Operator peuvent contrôler des travaux et informer un administrateur de NetBackup de la présence d'un problème. L'administrateur peut ensuite traiter le problème. Avec les autorisations par défaut, un membre du groupe d'utilisateurs NBU_Operator ne dispose probablement pas d'un accès suffisant pour traiter des problèmes plus importants. Les membres du groupe d'utilisateurs NBU_Operator possèdent les autorisations leur permettant d'effectuer des tâches telles que le déplacement de bandes, l'utilisation de lecteurs ou la réalisation d'inventaires de robots.
Administrateur (NBU_Admin)	Les membres du groupe d'utilisateurs NBU_Admin possèdent les autorisations d'accès, de configuration et d'utilisation complètes sur tous les objets d'autorisation NetBackup. Quelques exceptions existent pour les administrateurs SAN. En d'autres termes, les membres disposent de toutes les fonctions actuellement disponibles pour les administrateurs sans que la Gestion de l'accès soit installée. Cependant, en tant que membres de ce groupe, ils ne se connectent pas nécessairement au système d'exploitation en tant que racine ou administrateur. **Remarque :** Les membres du groupe d'utilisateurs NBU_Admin ne peuvent pas consulter Gestion de l'accès et, par conséquent, ne peuvent pas attribuer des autorisations à d'autres groupes d'utilisateurs.
Administrateur SAN (NBU_SAN Admin)	Par défaut, les membres du groupe d'utilisateurs (NBU_SAN Admin) possèdent des autorisations complètes de navigation, lecture, utilisation et configuration sur les pools de disques et propriétés de l'hôte. Ces autorisations vous permettent de configurer l'environnement SAN et son interaction avec NetBackup.

Groupe d'utilisateurs par défaut	Description
Utilisateur (NBU_User)	Le groupe d'utilisateurs NBU_User est le groupe d'utilisateurs NetBackup par défaut possédant le moins d'autorisations. Les membres du groupe d'utilisateurs NBU_User peuvent uniquement sauvegarder, restaurer et archiver des fichiers sur leur hôte local. Les membres de groupe d'utilisateurs de NBU_User peuvent utiliser l'interface client NetBackup (BAR).
Administrateur de sécurité (NBU_Security Admin)	Généralement, le groupe d'utilisateurs NBU_Security Admin comprend très peu de membres. La seule autorisation dont l'administrateur de sécurité dispose par défaut est de configurer le contrôle d'accès dans **Gestion de l'accès**. La configuration du contrôle d'accès comprend les possibilités suivantes : ■ Affichage du contenu de la fonction **Gestion de l'accès** dans la **NetBackup Administration Console**. ■ Création, modification et suppression des d'utilisateurs et de groupes d'utilisateurs. ■ Assignation d'utilisateurs aux groupes d'utilisateurs. ■ Assignation d'autorisations aux groupes d'utilisateurs.
Opérateur de centre de sauvegarde (Vault_Operator)	Le groupe d'utilisateurs Vault_Operator est le groupe d'utilisateurs par défaut possédant les autorisations requises pour effectuer les actions d'opérateur nécessaires au processus Vault (centre de sauvegarde).
Administrateur KMS (NBU_KMS Admin)	Par défaut, les membres du groupe d'utilisateurs NBU_KMS Admin possèdent des autorisations complètes de navigation, lecture, utilisation et configuration des propriétés de gestion des clés du chiffrement. Ces autorisations garantissent que les membres peuvent configurer l'environnement KMS et son interaction avec NetBackup.
Groupes d'utilisateurs supplémentaires	L'administrateur de sécurité (membre du groupe NBU_Security Admin ou équivalent) peut créer des groupes d'utilisateurs selon les besoins. Les groupes d'utilisateurs par défaut peuvent être sélectionnés, modifiés et enregistrés. Il est recommandé de copier, de renommer, puis d'enregistrer les groupes afin de conserver les paramètres par défaut pour référence ultérieure.

Configuration des groupes d'utilisateurs

L'administrateur de sécurité peut créer des groupes d'utilisateurs. Développez **Gestion de l'accès > Actions > Nouveau groupe** ou sélectionnez un groupe d'utilisateurs existant et développez **Gestion de l'accès > Actions > Copie au nouveau groupe**.

Création d'un groupe d'utilisateurs

Vous pouvez utiliser la procédure suivante pour créer un groupe d'utilisateur.

Pour créer un groupe d'utilisateurs

1. En tant que membre du groupe d'utilisateurs NBU_Security Admin (ou d'équivalent), développez **Gestion de l'accès > Groupes d'utilisateurs NBU.**
2. Sélectionnez **Actions > Nouveau groupe d'utilisateurs**. La boîte de dialogue Ajouter un nouveau groupe d'utilisateurs s'affiche, dans l'onglet **Général**.
3. Saisissez le nom du groupe dans le champ **Nom**, puis cliquez sur l'onglet **Utilisateurs**.
4. Sélectionnez les utilisateurs définis que vous souhaitez affecter à ce nouveau groupe d'utilisateurs. Cliquez ensuite sur **Assigner**. Sinon, pour inclure tous les utilisateurs définis dans le groupe, cliquez sur **Assigner tout**. Pour supprimer des utilisateurs de la liste des utilisateurs assignés, sélectionnez le nom de l'utilisateur, puis cliquez sur **Supprimer**.
5. Cliquez sur l'onglet **Autorisations**.
6. Sélectionnez une ressource de la liste Ressources et sélectionnez un objet d'autorisation. Sélectionnez ensuite les autorisations pour l'objet.
7. Cliquez sur **OK** pour enregistrer le groupe d'utilisateurs et les autorisations du groupe.

Création d'un groupe d'utilisateurs en copiant un groupe d'utilisateurs existant

Vous pouvez utiliser la procédure suivante pour créer un groupe d'utilisateurs en copiant un groupe d'utilisateurs existant.

Pour créer un groupe d'utilisateurs en copiant un groupe d'utilisateurs existant

1. En tant que membre du groupe d’utilisateurs NBU_Security Admin (ou d’équivalent), développez **Gestion de l’accès > Groupes d’utilisateurs NBU.**
2. Sélectionnez un groupe d'utilisateurs existant dans le volet **Détails** (volet situé du côté gauche de **NetBackup Administration Console**).
3. Sélectionnez **Actions > Copier vers un nouveau groupe d'utilisateurs**. Une boîte de dialogue basée sur le groupe d'utilisateurs sélectionné s'affiche, dans l'onglet **Général**.
4. Saisissez le nom du groupe dans le champ **Nom**, puis cliquez sur l'onglet **Utilisateurs**.

5 Sélectionnez les utilisateurs définis que vous souhaitez affecter à ce nouveau groupe d'utilisateurs. Cliquez ensuite sur **Assigner**. Sinon, pour inclure tous les utilisateurs définis dans le groupe, cliquez sur **Assigner tout**. Pour supprimer des utilisateurs de la liste des utilisateurs assignés, sélectionnez le nom de l'utilisateur, puis cliquez sur **Supprimer**.

6 Cliquez sur l'onglet **Autorisations**.

7 Sélectionnez une ressource dans la liste Ressources et sélectionnez un objet d'autorisation, puis sélectionnez les autorisations de l'objet.

8 Cliquez sur **OK** pour enregistrer le groupe d'utilisateurs et les autorisations du groupe. Le nouveau nom du groupe d'utilisateurs s'affiche dans le volet **Détails**.

Attribution d'un nom à un groupe d'utilisateurs

Une fois qu'un groupe d'utilisateurs NetBackup a été créé, il ne peut pas être renommé. Cependant, il est possible de renommer directement un groupe en suivant les étapes suivantes : copiez le groupe d'utilisateurs, donnez un nouveau nom à la copie, assurez-vous que les adhésions du groupes sont les mêmes que celles du groupe d'origine, puis supprimez le groupe d'utilisateurs NetBackup d'origine.

Ajout d'un nouvel utilisateur au groupe d'utilisateurs

Cliquez sur **Nouvel utilisateur** pour ajouter un utilisateur à la liste des **Utilisateurs définis**. Une fois que vous avez ajouté un utilisateur, le nom s'affiche dans la liste **Utilisateurs définis** et l'administrateur de sécurité peut assigner l'utilisateur au groupe d'utilisateurs.

Se reporter à "Assignation d'un utilisateur à un groupe d'utilisateurs" à la page 276.

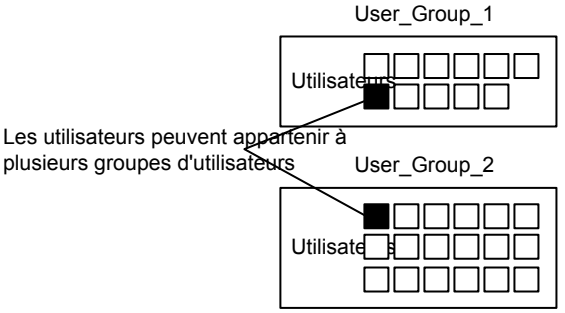
A propos de la définition d'un groupe d'utilisateurs et des utilisateurs

NetBackup authentifie les utilisateurs existants dans le système d'exploitation au lieu de requérir la création d'utilisateurs NetBackup avec un mot de passe et un profil NetBackup.

Les utilisateurs peuvent appartenir à plusieurs groupes d'utilisateurs et posséder un accès combiné pour les deux groupes.

Figure 14-7 présente la définition d'un groupe d'utilisateurs.

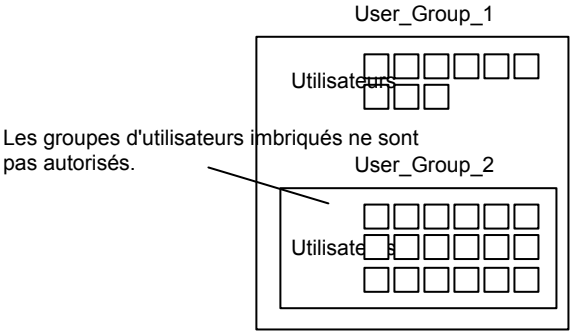
Figure 14-7 Définition d'un groupe d'utilisateurs



Les utilisateurs peuvent être membres de plusieurs groupes d'utilisateurs en même temps, mais NetBackup n'autorise pas l'imbrication de groupes d'utilisateurs. Par exemple, les membres d'un groupe d'utilisateurs peuvent appartenir à plusieurs groupes d'utilisateur, tandis qu'un groupe d'utilisateurs ne peut pas appartenir à un autre groupe d'utilisateurs.

Le schéma suivant indique que les groupes d'utilisateurs imbriqués ne sont pas autorisés.

Figure 14-8 Les groupes d'utilisateurs imbriqués ne sont pas autorisés.



Connexion en tant que nouvel utilisateur

Vous pouvez utiliser la procédure suivante pour vous connecter en tant que nouvel utilisateur.

Pour se connecter en tant que nouvel utilisateur

- Développez **Fichier > Connexion en tant que nouvel utilisateur** (Windows). Cette option est disponible uniquement sur les systèmes qui sont configurés pour le contrôle d'accès. Il est utile de fonctionner avec les privilèges minimum. Une personne doit alors se connecter à un compte possédant plus de privilèges.

Assignation d'un utilisateur à un groupe d'utilisateurs

Vous pouvez utiliser la procédure suivante pour assigner un utilisateur à un groupe d'utilisateurs. Un utilisateur est assigner depuis un espace de nom préexistant (NIS, Windows, etc.) vers un groupe d'utilisateurs NBU. Aucun compte utilisateur n'est créé au cours de cette procédure.

Pour ajouter un utilisateur à un groupe d'utilisateurs

1. En tant que membre du groupe d'utilisateurs NBU_Security Admin (ou d'équivalent), développez **Gestion de l'accès > Groupes d'utilisateurs NBU.**
2. Cliquez deux fois sur le groupe d'utilisateurs auquel vous souhaitez ajouter un utilisateur.
3. Sélectionnez l'onglet **Utilisateurs**, puis cliquez sur **Ajouter un utilisateur**.
4. Entrez le nom d'utilisateur et le domaine d'authentification. Sélectionnez le type de domaine de l'utilisateur : NIS, NIS+, PASSWD, Windows ou Vx.
5. Sélectionnez le **Type de domaine** de l'utilisateur :
   - NIS
     Network Information Services
   - NIS+
     service NIS
   - PASSWD
     Fichier de mot de passe UNIX sur le serveur d'authentification
   - Windows
     Contrôleur de domaine principal ou annuaire Active Directory
   - Vx
     Base de données privée Veritas
6. Pour l'option **Type d'utilisateur**, indiquez si l'utilisateur est un utilisateur individuel ou un domaine de système d'exploitation.
7. Cliquez sur **OK**. Le nom est ajouté à la liste des **Utilisateurs assignés**.

A propos des objets d’autorisation et des autorisations

En règle générale, un objet d’autorisation est lié à un nœud dans l’arborescence de la **console d’administration NetBackup**.

Le volet **Objets d’autorisation** contient les objets NetBackup auxquels vous pouvez accorder des autorisations.

Le volet **Autorisations de "DevHost"** indique les jeux d’autorisations pour lesquels le groupe d’utilisateurs sélectionné est configuré.

L’un des jeux d’autorisations suivants peut être accordé à un objet d’autorisation :

- **Parcourir** / **Lecture**
- **Exécuter**
- **Configurer**

La présence d’une lettre en minuscule dans la colonne **Autorisations de "DevHost"** indique certaines des autorisations (mais pas toutes) parmi un jeu d’autorisations. Des autorisations ont été accordées à l’objet.

Affichage des autorisations d'utilisateur particulières des groupes d'utilisateurs NetBackup

Les autorisations accordées à chacun des groupes d'utilisateurs NBU renvoient au nom de l'objet d'autorisation. Les groupes d'utilisateurs NBU incluent les groupes suivants : NBU_Operator, NBU_Admin, NBU_SAN Admin, NBU_User, NBU_Security Admin et Vault_Operator.

En raison de la complexité des interdépendances entre les ressources, il est impossible de mapper l'accès à une ressource ou à une autorisation dans certains emplacements. Il peut exister dans les ressources de multiples autorisations implicites devant être évaluées pour décider d'un contrôle d'accès. Ce mélange de autorisations peut entraîner des différences entre les autorisations sur les ressources et l'accès aux ressources. Ces différences potentielles sont en grande partie limitées à un accès en lecture. Par exemple, un utilisateur Security_Admin peut ne pas posséder les autorisations de répertorier des stratégies ou de les parcourir. L'administrateur a besoin d'accéder aux politiques car elles contiennent les informations client requises pour configurer la sécurité des clients.

Remarque : Il peut y avoir une anomalie d'autorisations. Les utilisateurs NBU_User, NBU_KMS_Admin, NBU_SAN et Vault_Operator ne peuvent pas accéder aux propriétés d'hôte de l'interface graphique utilisateur Java. La recherche des données pour la référence de propriétés d'hôte se fait également pour l'objet de politique. Cette anomalie signifie que pour accéder aux propriétés d'hôte, l'utilisateur doit avoir l'accès en lecture/navigation sur l'objet de politique. Donner manuellement l'accès en lecture à l'objet de politique résout le problème.

Remarque : Pour plus d'informations sur le sujet, consultez le site Web Support technique de Veritas.

Pour afficher les autorisations d'utilisateur particulières

1. Dans **NetBackup Administration Console**, développez **Gestion de l'accès > Groupes d'utilisateurs NBU**.
2. Cliquez deux fois sur le groupe NBU_Operator, NBU_Admin, NBU_SAN Admin, NBU_User, NBU_Security Admin ou Vault_Operator approprié dans la fenêtre **Sécurité**.
3. Dans la fenêtre **NBU_Operator**, sélectionnez l'onglet **Autorisations**.
4. Dans le volet **Objets d'autorisation**, sélectionnez l'objet d'autorisation désiré. Le volet **Autorisations** affiche les autorisations pour cet objet d'autorisation.

Octroi des autorisations

Vous pouvez utiliser la procédure suivante pour accorder une autorisation aux membres d'un groupe d'utilisateurs.

Pour accorder une autorisation aux membres d'un groupe d'utilisateurs

1. Sélectionnez un objet d'autorisation.
2. Marquez ensuite une autorisation que vous souhaitez accorder aux membres du groupe d'utilisateurs actuellement sélectionné.

Lorsqu'un groupe d'utilisateurs est copié pour créer un groupe d'utilisateurs, les paramètres d'autorisations sont également copiés.

Objets d'autorisation

Les tableaux suivants répertorient les objets d'autorisation dans l'ordre dans lequel ils s'affichent dans la fenêtre **NBU_Operator** de la **console d'administration NetBackup**.

Les tableaux indiquent également les relations entre les objets d'autorisation et les autorisations par défaut de chacun des groupes d'utilisateurs NBU comme suit :

- La lettre "X" indique que le groupe d'utilisateurs spécifié est autorisé à effectuer l'activité.
- Les caractères "---" indiquent que le groupe d'utilisateurs spécifié n'est pas autorisé à effectuer l'activité.

Autorisations de l'objet d'autorisation Politique

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Politique.

Tableau 14-17 Autorisations de l'objet d'autorisation Médias

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_ KMS Admin
Parcourir	Parcourir	X	X	---	---	---	X	---
Lecture	Lecture	X	X	---	---	---	X	---
Exécuter	Codes-barres de mise à jour	X	X	---	---	---	X	---
	Ejection	X	X	---	---	---	X	---
	Déplacer	X	X	---	---	---	X	---
	Attribuer	X	X	---	---	---	X	---
	Supprimer l'affectation	X	X	---	---	---	X	---
	Mettre à jour la base de données	X	X	---	---	---	X	---
Configurer	Nouveau	---	X	---	---	---	X	---
	Supprimer	---	X	---	---	---	X	---
	Faire expirer	---	X	---	---	---	X	---

Autorisations de l'objet d'autorisation Lecteur

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Lecteur.

Tableau 14-18 Autorisations de l'objet d'autorisation Politique

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	---	---	---	---	---
Lecture	Lecture	X	X	---	---	---	---	---
Exécuter	Sauvegarde :	X	X	---	---	---	---	---
Configurer	Activer	---	X	---	---	---	---	---
	Désactiver	---	X	---	---	---	---	---
	Nouveau	---	X	---	---	---	---	---
	Supprimer	---	X	---	---	---	---	---

Autorisations de l'objet d'autorisation Rapport

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Lecteur.

Tableau 14-19 Autorisations de l'objet d'autorisation Lecteur

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	X	---	---	X	---
Lecture	Lecture	X	X	X	---	---	X	---
Exécuter	Démarré	X	X	---	---	---	---	---
	Arrêté	X	X	---	---	---	---	---
	Réinitialiser	X	X	---	---	---	---	---
	Attribuer	X	---	---	---	---	---	---
	Supprimer l'affectation	X	---	---	---	---	---	---
Configurer	Nouveau	---	X	---	---	---	---	---
	Supprimer	---	X	---	---	---	---	---

Autorisations de l'objet d'autorisation Rapport

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Catalogue NetBackup. Les rapports incluent uniquement l'ensemble d'autorisations d'accès mais aucun ensemble d'autorisations Configurer ou Utiliser.

Tableau 14-20 Autorisations de l'objet d'autorisation Rapport

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	---	X	---	---	---	X	---
Lecture	Lecture	---	X	---	---	---	X	---

Autorisations de l'objet d'autorisation NBU_Catalog

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Catalogue NetBackup.

Tableau 14-21 Autorisations de l'objet d'autorisation NBU_Catalog

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	---	X	---	---	---	X	---
Lecture	Lecture	---	X	---	---	---	X	---
Exécuter	Sauvegarde :	---	X	---	---	---	---	---
	Restauration	---	X	---	---	---	---	---
	Vérification	---	X	---	---	---	---	---
	Dupliquer	---	X	---	---	---	---	---
	Importation	---	X	---	---	---	---	---
	Faire expirer	---	X	---	---	---	---	---
Configurer	Nouveau	---	X	---	---	---	---	---
	Supprimer	---	X	---	---	---	---	---
	Lire la configuration	---	X	---	---	---	---	---
	Définir la configuration	---	X	---	---	---	---	---

Autorisations de l'objet d'autorisation Robot

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Robot.

Tableau 14-22 Autorisations de l'objet d'autorisation Robot

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	X	---	---	X	---
Lecture	Lecture	X	X	X	---	---	X	---
Exécuter	inventaire	X	X	---	---	---	X	---
Configurer	Nouveau	---	X	---	---	---	X	---
	Supprimer	---	X	---	---	---	X	--

Autorisations d'objet d'autorisation d'unité de stockage

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Unité de stockage.

Tableau 14-23 Autorisations d'objet d'autorisation d'unité de stockage

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	---	---	---	---	---
Lecture	Lecture	X	X	---	---	---	---	---
Configurer	Attribuer	---	X	---	---	---	---	---
	Nouveau	---	X	---	---	---	---	---
	Supprimer	---	X	---	---	---	---	---

Autorisations de l'objet d'autorisation DiskPool

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation DiskPool.

Tableau 14-24 Autorisations de l'objet d'autorisation DiskPool

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	X	---	---	---	---
Lecture	Lecture	X	X	X	---	---	---	---
Exécuter	Nouveau	---	X	X	---	---	---	---
	Supprimer	---	X	X	---	---	---	---
	Modifier	---	X	X	---	---	---	---
	Monter	---	X	X	---	---	---	---
	Démonter	---	X	X	---	---	---	---
Configurer	Lire la configuration	---	X	X	---	---	---	---
	Définir la configuration	---	---	X	---	---	---	---

Autorisations de l'objet d'autorisation BuAndRest (Sauvegarde et restauration)

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Sauvegarde et restauration.

Tableau 14-25 Autorisations de l'objet d'autorisation BuAndRest (Sauvegarde et restauration)

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	X	X	---	---	X
Lecture	Lecture	X	X	X	X	---	---	X

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Exécuter	Sauvegarde :	X	X	X	X	---	---	X
	Restauration	X	X	X	X	---	---	X
	Autre client	X	X	---	---	---	---	---
	Autre serveur	X	X	---	---	---	---	---
	Accès administrateur	X	X	---	---	---	---	---
	Agent de base de données	---	---	---	---	---	---	---
	Liste	---	---	X	X	---	---	X

Autorisations de l'objet d'autorisation Travail

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Travail.

Tableau 14-26 Autorisations de l'objet d'autorisation Travail

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	---	---	---	X	---
Lecture	Lecture	X	X	---	---	---	X	---
Exécuter	Interrompre	X	X	---	---	---	X	---
	Reprendre	X	X	---	---	---	X	---
	Annuler	X	X	---	---	---	X	---
	Supprimer	X	X	---	---	---	X	---
	Redémarrer	X	X	---	---	---	X	---
	Nouveau	X	X	---	---	---	X	---

Autorisations de l'objet d'autorisation Service

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Service.

Tableau 14-27 Autorisations de l'objet d'autorisation Service

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	---	---	---	X	---
Lecture	Lecture	X	X	---	---	---	X	---
Exécuter	Arrêter	X	X	---	---	---	---	---

Les autorisations de lecture et de navigation n'ont aucun effet sur l'onglet Daemons. Ces informations sont collectées depuis le serveur à l'aide des appels de niveau utilisateur. Les appels sont utilisés pour accéder à la liste de tâches de processus et sont visibles par tous les utilisateurs à des fins informatives.

Si un utilisateur n'appartient pas au groupe d'utilisateurs NBU_Admin, mais est connecté en tant qu'administrateur du système d'exploitation (administrateur ou racine) :

- L'utilisateur peut redémarrer un service depuis la **Console d'administration NetBackup** ou depuis la ligne de commande.
- L'utilisateur peut arrêter un service depuis la **Console d'administration NetBackup** ou depuis la ligne de commande.

Si un utilisateur n'appartient pas au groupe d'utilisateurs NBU_Admin, mais est connecté en tant qu'administrateur du système d'exploitation (`root`), cet utilisateur peut redémarrer un daemon de la ligne de commande uniquement :

```
/etc/init.d/netbackup start
```

Si un utilisateur n'appartient pas au groupe d'utilisateurs NBU_Admin, mais n'est pas connecté en tant qu'administrateur du système d'exploitation (administrateur) :

- L'utilisateur ne peut pas redémarrer un service depuis la **Console d'administration NetBackup** ou depuis la ligne de commande.
- L'utilisateur ne peut pas arrêter un service depuis la **Console d'administration NetBackup** mais il peut utiliser la ligne de commande (par exemple, `bprdreq -terminate`, `bpdbm -terminate` ou `stopltid`).

Si un utilisateur appartient au groupe d'utilisateurs NBU_Admin, mais n'est pas connecté en tant qu'administrateur du système d'exploitation (`root`), cet utilisateur ne peut pas redémarrer un daemon depuis la **Console d'administration NetBackup** ou depuis la ligne de commande.

Autorisations de l'objet d'autorisation Propriétés d'hôte

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Propriétés d'hôte.

Tableau 14-28 Autorisations de l'objet d'autorisation Propriétés d'hôte

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	X	X	X	X	X
Lecture	Lecture	X	X	X	X	X	X	X
Configurer	Nouveau	---	X	---	---	---	---	---
	Supprimer	---	X	---	---	---	---	--

Autorisations de l'objet d'autorisation Licence

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Licence.

Tableau 14-29 Autorisations de l'objet d'autorisation Licence

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	X	X	X	X	X
Lecture	Lecture	X	X	X	X	X	X	X
Configurer	Attribuer	---	X	---	---	---	---	---
	Nouveau	---	X	---	---	---	---	---
	Supprimer	---	X	---	---	---	---	---

Autorisations de l'objet d'autorisation Groupe de volumes

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Groupe de volumes.

Tableau 14-30 Autorisations de l'objet d'autorisation Groupe de volumes

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	---	---	---	X	---

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Lecture	Lecture	X	X	---	---	---	X	---
Configurer	Nouveau	---	X	---	---	---	---	---
	Supprimer	---	X	---	---	---	---	---

Autorisations de l'objet d'autorisation Pool de volumes

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Pool de volumes.

Tableau 14-31 Autorisations de l'objet d'autorisation Pool de volumes

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	---	---	---	X	---
Lecture	Lecture	X	X	---	---	---	X	---
Configurer	Attribuer	---	X	---	---	---	---	---
	Nouveau	---	X	---	---	---	---	---
	Supprimer	---	X	---	---	---	---	---

Autorisations de l'objet d'autorisation DevHost (Hôte de périphérique)

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Hôte de périphérique.

Remarque : L'objet DevHost contrôle l'accès au nœud **Gestion des médias et des périphériques > informations d'authentification**.

Tableau 14-32 Autorisations de l'objet d'autorisation DevHost (Hôte de périphérique)

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	X	---	---	X	---
Lecture	Lecture	X	X	X	---	---	X	---

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Exécuter	Arrêter	X	X	---	---	---	---	---
	Synchroniser	X	X	---	---	---	---	---
Configurer	Nouveau	---	X	---	---	---	---	---
	Supprimer	---	X	---	---	---	---	---

Autorisations de l'objet d'autorisation Sécurité

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Sécurité.

Tableau 14-33 Autorisations de l'objet d'autorisation Sécurité

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	---	---	---	---	X	---	---
Lecture	Lecture	---	---	---	---	X	---	---
Configurer	Sécurité	---	---	---	---	X	---	---

Autorisations de l'objet d'autorisation Serveur FAT

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Serveur FAT.

Tableau 14-34 Autorisations de l'objet d'autorisation Serveur FAT

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	X	---	---	---	---
Lecture	Lecture	X	X	X	---	---	---	---
Configurer	Modifier	---	X	X	---	---	---	---
	Modifier la configuration SAN	---	---	X	---	---	---	---

Autorisations de l'objet d'autorisation Client FAT

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Client FAT.

Tableau 14-35 Autorisations de l'objet d'autorisation Client FAT

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	X	---	---	---	---
Lecture	Lecture	X	X	X	---	---	---	--
Exécuter	Découvrir	---	X	X	---	---	---	---
Configurer	Modifier	---	X	X	---	---	---	---

Autorisations de l'objet d'autorisation Centre de sauvegarde

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Centre de sauvegarde.

Tableau 14-36 Autorisations de l'objet d'autorisation Centre de sauvegarde

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	---	X	---	---	---	X	---
Lecture	Lecture	---	X	---	---	---	X	---
Exécuter	Gérer les conteneurs	---	X	---	---	---	X	---
	Exécuter les rapports	---	X	---	---	---	X	---
Configurer	Modifier	---	X	---	---	---	---	---
	Exécuter les sessions	---	X	---	---	---	---	---

Autorisations de l'objet d'autorisation Groupe de serveurs

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation Groupe de serveurs.

Tableau 14-37 Autorisations de l'objet d'autorisation Groupe de serveurs

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	X	X	---	---	---	X	---
Lecture	Lecture	X	X	---	---	---	X	---
Configurer	Nouveau	---	X	---	---	---	---	---
	Supprimer	---	X	---	---	---	---	---
	Modifier	---	X	---	---	---	---	---

Autorisations de l'objet d'autorisation du groupe de système de gestion des clés (Kms)

Le tableau suivant présente les autorisations qui sont associées à l'objet d'autorisation du groupe Kms.

Tableau 14-38 Autorisations de l'objet d'autorisation du groupe Kms

Définir	Activité	NBU_Operator	NBU_Admin	NBU_SAN Admin	NBU_User	NBU_Security Admin	Vault_Operator	NBU_KMS Admin
Parcourir	Parcourir	---	X	---	---	---	---	X
Lecture	Lecture	---	X	---	---	---	---	X
Configurer	Nouveau	---	---	---	---	---	---	X
	Supprimer	---	---	---	---	---	---	X
	Modifier	---	---	---	---	---	---	X

Mise à niveau de NBAC (NetBackup Access Control)

Remarque : Si NBAC est activé, il est mis à niveau en tant qu'élément de la mise à niveau de NetBackup. Consultez le Guide de mise à niveau NetBackup pour des instructions pour la mise à niveau de NetBackup. Vérifiez que les services AT et AZ actuels sont en cours d'exécution lors de la mise à niveau. Si NetBackup s'exécute dans un serveur mis en cluster, vérifiez que les deux services sont en cours d'exécution dans le nœud actif où s'exécute NetBackup et où s'effectue la mise à niveau.

La procédure suivante décrit la mise à niveau de NBAC (NetBackup Access Control).

Mise à niveau de NBAC (NetBackup Access Control)

1. Sur le serveur maître, arrêtez NetBackup.
2. Mettez à niveau NetBackup.

   Sur les serveurs de médias et les ordinateurs client, arrêtez d'abord NetBackup puis mettez à niveau NetBackup. Notez que les packages partagés d'authentification et d'autorisation ne sont plus utilisés sur les serveurs de médias et les ordinateurs client. Ces produits peuvent être supprimés si aucun autre produit Veritas ne les utilise.

Section 2

Chiffrement des données en transit

Chapitre 15

Autorité de certification NetBackup et certificats NetBackup

Ce chapitre traite des sujets suivants :

- Migration de l'autorité de certification NetBackup

Présentation des certificats de sécurité dans NetBackup

NetBackup utilise les certificats de sécurité pour authentifier les hôtes NetBackup. Les certificats de sécurité sont conformes à la norme ICP (Infrastructure à clés publiques) X.509. Un serveur maître agit en tant qu'autorité de certification (AC) et émet des certificats numériques pour les hôtes.

Tous les certificats de sécurité générés avant NetBackup 8.0 sont désormais appelés certificats basés sur un nom d'hôte. NetBackup est en train de remplacer ces certificats plus anciens par des certificats basés sur l'ID d'hôte plus récents. La transition sera terminée dans les versions futures et l'utilisation de certificats basée sur le nom d'hôte sera éliminée.

Cependant, la transition est en cours et NetBackup a toujours besoin des anciens certificats basés sur un nom d'hôte pour certaines opérations. Le tableau suivant répertorie les diverses opérations pour lesquelles un certificat basé sur un nom d'hôte est requis.

Remarque : Tous les hôtes NetBackup 8.1 doivent avoir un certificat basé sur l'ID d'hôte.

Tableau 15-1 Conditions des certificats basés sur un nom d'hôte pour les hôtes NetBackup 8.1

Opération ou composant	Type de certificat requis
NetBackup Access Control (NBAC)	Si NBAC est activé sur un hôte NetBackup, celui-ci requiert un certificat basé sur un nom d'hôte. Ceux-ci sont automatiquement déployés quand NBAC est activé.
Opérations d'audit amélioré	Les opérations d'audit amélioré requièrent que les hôtes aient des certificats basés sur le nom d'hôte. Se reporter à "Déploiement de certificats basés sur le nom d'hôte" à la page 326.
Stockage en cloud	Applicable uniquement aux serveurs de médias NetBackup versions 8.0 à 8.1.2. Pour utiliser NetBackup CloudStore Service Container, le certificat basé sur le nom d'hôte doit être installé sur le serveur de médias. Si le certificat n'est pas installé, Service Container ne peut pas démarrer. Se reporter à "Déploiement de certificats basés sur le nom d'hôte" à la page 326. Pour plus d'informations, consultez le *Guide de l'administrateur NetBackup Cloud*.

Communication sécurisée dans NetBackup

Les hôtes NetBackup 8.1 (ou version plus récente) peuvent communiquer entre eux uniquement en mode sécurisé. Les hôtes NetBackup 8.1 doivent disposer d'un certificat d'autorité de certification (CA) et d'un certificat basé sur l'ID d'hôte pour que la communication aboutisse. NetBackup utilise le protocole de sécurité TLS (Transport Layer Security) pour la communication avec l'hôte, où chaque hôte doit présenter son certificat de sécurité et valider le certificat de l'hôte homologue par rapport au certificat de l'autorité de certification (CA).

Toutes les communications de contrôle (ou canaux de contrôle) entre les hôtes NetBackup sont sécurisées à l'aide des certificats de version 1.2 et X.509 du protocole de sécurité TLS (Transport Layer Security). La communication de contrôle est utilisée par le logiciel NetBackup pour lancer, contrôler et surveiller les opérations de sauvegarde, d'archivage et de restauration.

La communication de données comprend les données sauvegardées à l'aide de NetBackup. Les politiques de sécurité exigent que les administrateurs de sauvegarde s'assurent que le canal sur lequel les clients NetBackup envoient des métadonnées et des données aux serveurs NetBackup est sécurisé. Dans NetBackup 10.0 et versions ultérieures, les images et métadonnées de sauvegarde sont chiffrées sur le réseau par des communications sécurisées. Cette fonction est appelée "chiffrement du canal de données" ou "chiffrement des données en transit" (DTE).

Les canaux suivants sont classés en tant que canaux de données :

- Flux TAR (client vers serveur de médias) : canal sur lequel le flux TAR/flux de données circule entre le client et le serveur de médias. Lors d'une opération de sauvegarde, le serveur de médias reçoit les données du client et les envoie au stockage (par exemple, via un plug-in OST). Le sens est inversé lors d'une restauration.
- Flux TAR (serveur de médias vers serveur de médias) : canal est utilisé lors de la duplication.
- Informations de catalogue (client vers serveur de médias) : canal sur lequel les informations du catalogue et les commandes de contrôle circulent entre le client et le serveur de médias. Le volume de données transmises sur ce canal est proportionnel au nombre de fichiers et de répertoires sauvegardés. Le serveur de médias envoie au serveur principal les informations de catalogue transmises par le client.
- Informations du catalogue (serveur de médias vers serveur principal) : canal sur lequel les informations du catalogue circulent du serveur de médias vers le serveur principal.

Deux nœuds de la **console d'administration NetBackup** fournissent des paramètres de communication sécurisée : **Gestion des hôtes** et **Paramètres de sécurité globaux**.

Se reporter à "À propos de la gestion des hôtes" à la page 298.

Se reporter à "Ajout de mappages d'ID d'hôte vers le nom d'hôte" à la page 299.

Se reporter à "À propos des paramètres de sécurité globale" à la page 315.

Se reporter à "À propos des paramètres de communication sécurisée" à la page 316.

Se reporter à "À propos des paramètres de reprise après incident" à la page 321.

Deux commandes , `nbhostmgmt` et `nbhostidentity`, ainsi que les améliorations apportées à `nbcertcmd` et `nbseccmd`, fournissent des options pour gérer le déploiement de certificat, et d'autres paramètres de sécurité.

À propos des utilitaires de gestion de la sécurité

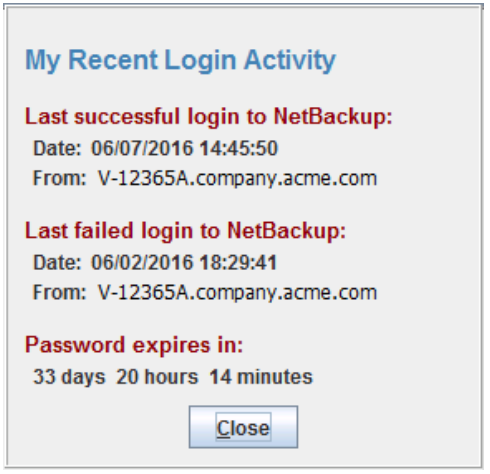
Le nœud **Console d'administration NetBackup > Gestion de la sécurité** est visible uniquement pour les administrateurs du serveur principal NetBackup.

Gestion de la sécurité contient les utilitaires permettant d'afficher l'activité de connexion, de gérer les certificats basés sur l'ID d'hôte et de configurer les communications sécurisées dans le domaine.

- Utilisez **Événements de sécurité** pour afficher les informations de connexion sur l'administrateur actuel et les modifications utilisateur apportées aux certificats, aux jetons, aux hôtes et aux configurations de sécurité. Vous pouvez également afficher des informations sur les connexions d'hôte.
- Utilisez le nœud **Gestion de l'hôte** pour effectuer des opérations d'hôte NetBackup, telles que l'ajout ou l'approbation d'ID d'hôte pour les mappages de nom d'hôte, la réinitialisation d'hôte ou l'ajout de commentaires pour un hôte.
  Se reporter à "Onglet Hôtes" à la page 298.
- Utilisez le nœud **Gestion des certificats** pour exécuter des opérations propres aux certificats, telles que l'affichage, la révocation ou le renouvellement.
  Se reporter à "À l'aide de l'utilitaire de gestion de certificat pour émettre et déployer des certificats basés sur l'ID d'hôte" à la page 330.
- Utilisez le nœud **Paramètres de sécurité globaux** pour configurer les paramètres de sécurité, par exemple, activer la communication non sécurisée, phrase de passe du package de reprise après incident, niveau de déploiement de certificat et ainsi de suite.
  Se reporter à "À propos des paramètres de sécurité globale" à la page 315.

Activité de connexion

NetBackup capture des informations sur l'historique d'accès des utilisateurs et conserve une trace du moment où le mot de passe d'un utilisateur expirera. Les informations sont affichées dans la fenêtre **Mes activités de connexion récentes** dans le coin supérieur droit de la **console d'administration NetBackup**.



La fenêtre **Mes activités de connexion récentes** se ferme lorsque vous commencez à utiliser la **console d'administration NetBackup**.

Les informations d'expiration de mot de passe ne sont pas disponibles dans les scénarios suivants :

- si vous vous êtes connecté à distance au serveur maître à l'aide de la fonctionnalité Single Sign-On (SSO) de la **console d'administration NetBackup** ;
- Si vous vous êtes connecté au serveur maître UNIX ou Linux à l'aide de la **console d'administration NetBackup**.

Remarque : Les détails d'expiration de connexion et de mot de passe sont affichés uniquement après les premières connexion et déconnexion réussies sur la **console d'administration NetBackup**.

Les détails de connexion ne sont pas automatiquement actualisés. Vous devez vous déconnecter de la **console d'administration NetBackup** puis vous reconnecter pour afficher les dernières informations sur les détails de la dernière connexion.

Ces informations sont également affichées dans **Événements de sécurité** sur l'onglet **Historique d'accès**.

À propos de la gestion des hôtes

Le noeud **Gestion de la sécurité > Gestion des hôtes** permet de mapper les noms d'hôte à leurs ID d'hôte correspondants. Le mappage approprié entre les noms d'hôte mappés à un ID d'hôte est important pour les communications d'hôte sécurisées.

Se reporter à "Communication sécurisée dans NetBackup" à la page 295.

Se reporter à "Ajout de mappages d'ID d'hôte vers le nom d'hôte" à la page 299.

Se reporter à "Réinitialisation des attributs d'hôte NetBackup" à la page 310.

Onglet Hôtes

L'onglet **Hôtes** fournit les informations suivantes :

Hôte	Le nom de l'hôte. **Remarque :** Le nœud **Gestion de l'hôte** affiche uniquement les hôtes qui ont un ID d'hôte.
Noms d'hôtes/Adresses IP mappés	Noms d'hôte ou adresses IP mappés vers l'ID d'hôte du client sélectionné. Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.
Version	Version de NetBackup qui est installée sur l'hôte.
Autoriser la validité de renouvellement automatique de certificat	Heure jusqu'à laquelle le certificat peut être renouvelé sur l'hôte sans nécessiter de jeton de renouvellement. Par défaut, l'option **Autoriser le renouvellement automatique de certificat** a une période de validité de 48 heures. Se reporter à "Autoriser ou ne pas autoriser le renouvellement de certificat automatique" à la page 312.
Système d'exploitation	La version du système d'exploitation qui est installée sur l'hôte.
Type de système d'exploitation	Le type de système d'exploitation (Windows ou UNIX) qui est installé sur l'hôte.
Architecture de l'UC	L'architecture de l'unité centrale qui est utilisée sur l'hôte.

Sécurisé	Indique si la communication de l'hôte est sécurisée. S'il s'agit d'un hôte 8.1, la communication est sécurisée et il peut communiquer en toute sécurité.
Commentaire	Commentaire ou informations supplémentaires que vous avez ajouté(es) pour l'hôte.
Description du matériel	Le matériel qui est utilisé sur l'hôte.
ID de l'hôte NetBackup	Un identifiant unique pour l'hôte.
EEB NetBackup	Indique si les EEB NetBackup (Emergency Engineering Binary) sont installés ou non.
Serveurs	Serveurs supplémentaires associés à l'hôte.
Serveur principal	Serveur principal associé à l'hôte.
Emis le	Date à laquelle le certificat basé sur l'ID d'hôte a été émis vers l'hôte.
Date de dernière mise à jour	Date à laquelle le certificat basé sur l'ID d'hôte a été mis à jour.
Plate-forme VxUpdate	Identifie le package VxUpdate nécessaire pour la mise à niveau de l'hôte.
Packages installés	Packages NetBackup installés sur l'hôte.

Ajout de mappages d'ID d'hôte vers le nom d'hôte

Plusieurs noms d'hôte ou adresses IP peuvent être associés aux hôtes. Pour une communication réussie entre les hôtes, tous les noms d'hôte et adresses IP appropriés doivent être mappés vers les ID d'hôte respectifs.

Pendant la communication, NetBackup peut détecter de nouveaux noms d'hôte ou adresses IP relatifs à un ID d'hôte. Ces noms d'hôte ou adresses IP peuvent être automatiquement ou manuellement mappés vers l'ID d'hôte respectif pour que la communication réussisse.

Les noms d'hôte ou adresses IP qui sont détectés par le système sont automatiquement mappés à l'ID d'hôte respectif si l'option **Mapper automatiquement l'ID d'hôte aux noms d'hôte** est sélectionnée dans l'onglet **Gestion de la sécurité > Paramètres de sécurité globaux > Communication sécurisée**.

Se reporter à "Mappage automatique des ID d'hôte vers les noms d'hôte et adresses IP" à la page 321.

Remarques importantes

Consultez les remarques suivantes relatives aux mappages de l'ID d'hôte vers le nom d'hôte :

- Dans le cas d'hôtes DHCP (Dynamic Host Configuration Protocol), les adresses IP dynamiques peuvent être détectées par le système lors de la communication et ajoutées en tant que mappages d'ID d'hôte au nom d'hôte. Vous devez supprimer ces mappages.
- Dans le cas d'une configuration en cluster, le nom d'hôte et le nom de domaine qualifié complet (FQDN) du nom virtuel sont découverts lors de la communication de l'hôte.
- Si vous redéployez un certificat sur un hôte à l'aide d'un nom d'hôte qui n'est pas mappé avec l'ID d'hôte existant, un nouveau certificat est déployé et un nouvel ID d'hôte est envoyé à l'hôte car NetBackup le considère comme un hôte différent. Pour éviter cette situation, vous devez mapper tous les noms d'hôte disponibles avec l'ID d'hôte existant.

Utilisez la procédure suivante pour mapper manuellement un ID d'hôte spécifique vers les noms d'hôte ou les adresses IP correspondants.

Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.

Se reporter à "Suppression de mappages d'ID d'hôte vers le nom d'hôte" à la page 302.

Pour ajouter des mappages d'ID d'hôte vers le nom d'hôte

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité > Gestion des certificats**.
2. Dans l'onglet **Hôtes**, volet des détails, cliquez avec le bouton droit de la souris sur l'hôte que vous souhaitez modifier.
3. Cliquez sur l'option **Ajouter ou supprimer des mappages d'hôtes**.

4 Dans l'écran **Ajouter ou supprimer des mappages d'hôtes**, l'ID d'hôte de l'hôte du client sélectionné s'affiche avec les mappages existants.

Cliquez sur **Ajouter**.

5 Dans la boîte de dialogue **Ajouter un mappage**, fournissez les détails suivants :

Nom du mappage	Indiquez le mappage de l'ID d'hôte vers le nom d'hôte. **Remarque :** Les mappages d'ID d'hôte vers le nom d'hôte ne sont pas sensibles à la casse.
Motif de l'audit	À des fins d'audit, indiquez le motif de l'ajout de ce mappage ou fournissez des informations supplémentaires.
Enregistrer	Cliquez pour enregistrer le mappage que vous avez ajouté et continuer à ajouter d'autres mappages pour le même ID d'hôte.
Annuler	Cliquez pour fermer la boîte de dialogue sans enregistrer les modifications.

Pour ajouter un mappage d'ID d'hôte vers le nom d'hôte à l'aide de l'interface de ligne de commande

1 Exécutez la commande suivante pour authentifier votre connexion aux services web :

```
bpnbat -login -loginType WEB
```

2 Exécutez la commande suivante pour ajouter un mappage d'ID d'hôte vers le nom d'hôte :

```
nbhostmgmt -add -hostid host_ID -mappingname mapping_name
```

Boîte de dialogue Ajouter ou supprimer des mappages d’hôtes

Plusieurs noms d’hôte ou adresses IP peuvent être associés aux hôtes. Pour une communication réussie entre les hôtes, tous les noms d’hôte et adresses IP appropriés doivent être mappés vers les ID d’hôte respectifs.

Dans l’onglet **Gestion de la sécurité > Gestion des hôtes > Hôtes**, cliquez avec le bouton droit de la souris sur l’hôte à modifier et cliquez sur l’option **Ajouter ou supprimer des mappages d’hôtes** pour ouvrir la boîte de dialogue.

Seul l’administrateur système peut accéder aux propriétés **Ajouter ou supprimer des mappages d’hôtes** d’un hôte NetBackup.

Se reporter à "Ajout de mappages d'ID d'hôte vers le nom d'hôte" à la page 299.

Se reporter à "Suppression de mappages d'ID d'hôte vers le nom d'hôte" à la page 302.

La boîte de dialogue **Ajouter ou supprimer des mappages d'hôtes** contient les propriétés suivantes.

ID de l'hôte NetBackup	Affiche l'ID de l'hôte sélectionné.
Noms d'hôtes/Adresses IP mappés	Répertorie les noms d'hôte et adresses IP qui sont mappés à l'ID de l'hôte client.
Découvert automatiquement	Indique si le nom d'hôte ou l'adresse IP mappé a été découvert automatiquement par le système ou non.
Créé le	Date et heure de création du mappage.
Date de dernière mise à jour	Date et heure de la dernière mise à jour du mappage.
Ajouter	Cliquez pour ajouter de nouveaux mappages d'ID d'hôte au nom de l'hôte client. La boîte de dialogue **Ajouter un mappage** s'affiche. Se reporter à "Ajout de mappages d'ID d'hôte vers le nom d'hôte" à la page 299.
Supprimer	Cliquez pour supprimer le mappage sélectionné d'ID d'hôte au nom de l'hôte client. La boîte de dialogue **Supprimer le mappage** s'affiche. Se reporter à "Suppression de mappages d'ID d'hôte vers le nom d'hôte" à la page 302. **Remarque :** Les opérations effectuées sur les boîtes de dialogue **Ajouter un mappage** et **Supprimer le mappage** mettent directement à jour la base de données NetBackup.
Fermer	Cliquez pour fermer la boîte de dialogue **Ajouter ou supprimer des mappages d'hôtes**.
Aide	Cliquez pour consulter l'aide.

Suppression de mappages d'ID d'hôte vers le nom d'hôte

Utilisez la procédure suivante pour supprimer les mappages de l'ID d'hôte vers le nom d'hôte.

Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.

Se reporter à "Ajout de mappages d'ID d'hôte vers le nom d'hôte" à la page 299.

Pour supprimer des mappages d'ID d'hôte vers le nom d'hôte

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité > Gestion des certificats**.
2. Dans le volet de détails, sous l'onglet **Hôtes**, cliquez avec le bouton droit de la souris sur l'hôte du client que vous voulez modifier.
3. Cliquez sur l'option **Ajouter ou supprimer des mappages d'hôtes**.
4. Dans l'écran **Ajouter ou supprimer des mappages d'hôtes**, l'ID d'hôte de l'hôte du client sélectionné s'affiche avec les mappages existants.
5. Sélectionnez le mappage que vous voulez supprimer.
6. Cliquez sur **Supprimer**.
7. Dans la boîte de dialogue **Supprimer le mappage**, spécifiez le motif d'audit pour supprimer le mappage sélectionné à des fins d'audit.
8. Cliquez sur **Oui**.

Pour supprimer un mappage d'ID d'hôte vers le nom d'hôte à l'aide de l'interface de ligne de commande

1. Exécutez la commande suivante pour authentifier votre connexion aux services web :

   ```
   bpnbat -login -loginType WEB
   ```

2. Exécutez la commande suivante pour supprimer un mappage d'ID d'hôte vers le nom d'hôte :

   ```
   nbhostmgmt -delete -hostid host_ID-mappingname mapping_name
   ```

Onglet Mappages pour approbation

Utilisez l'onglet **Gestion de la sécurité > Gestion des hôtes > Mappages à approuver** pour afficher les mappages d'ID d'hôte à un nom d'hôte en attente d'approbation.

Les options suivantes sont disponibles sous l'onglet **Mappages pour approbation** :

Hôte	Nom de l'hôte sélectionné.
Mappage découvert automatiquement	Mappage d'ID d'hôte à un nom d'hôte découvert au sujet de l'hôte pendant la communication.

Conflit	États s'il existe un conflit dans les mappages. Par exemple, dans une configuration de cluster, un mappage peut être partagé entre les ID d'hôte.
Découvert le	Date et heure de la découverte du mappage par le système.
ID de l'hôte NetBackup	ID de l'hôte

Se reporter à "Affichage des mappages découverts automatiquement" à la page 304.

Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.

Remarque : Si l'option **Mapper automatiquement l'ID d'hôte aux noms d'hôte** de l'onglet **Gestion de la sécurité > Paramètres de sécurité globale > Communication sécurisée** est sélectionnée, l'onglet **Mappages à approuver** affiche uniquement les mappages en conflit.

Se reporter à "Mappage automatique des ID d'hôte vers les noms d'hôte et adresses IP" à la page 321.

Affichage des mappages découverts automatiquement

Pendant la communication, NetBackup peut détecter de nouveaux noms d'hôte ou adresses IP relatifs à un ID d'hôte. Vous pouvez afficher les mappages d'ID d'hôte vers des noms d'hôte qui sont découverts automatiquement.

Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.

Pour afficher des mappages d'ID d'hôte vers des noms d'hôte

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité > Gestion des certificats**.
2. Dans le volet des détails, cliquez sur l'onglet **Mappages à approuver**.

   Se reporter à "Onglet Mappages pour approbation" à la page 303.

   Remarque : Si l'option **Mapper automatiquement l'ID d'hôte aux noms d'hôte** de l'onglet **Gestion de la sécurité > Paramètres de sécurité globale > Communication sécurisée** est sélectionnée, l'onglet **Mappages à approuver** affiche uniquement les mappages en conflit.

   Se reporter à "Mappage automatique des ID d'hôte vers les noms d'hôte et adresses IP" à la page 321.

Boîte de dialogue Détails des mappages

Utilisez la boîte de dialogue **Détails des mappages** pour accepter ou rejeter les mappages d'ID d'hôte à un nom d'hôte en attente.

Dans l'onglet **Gestion de la sécurité > Gestion de l'hôte > Mappages à approuver**, cliquez avec le bouton droit de la souris sur le mappage d'ID d'hôte à un nom d'hôte à approuver ou rejeter et cliquez sur **Détails des mappages** pour ouvrir la boîte de dialogue.

Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.

Se reporter à "Approbation des mappages d'ID d'hôte vers le nom d'hôte" à la page 306.

Se reporter à "Rejet des mappages d'ID d'hôte vers le nom d'hôte" à la page 307.

Se reporter à "Onglet Mappages pour approbation" à la page 303.

Les options suivantes sont disponibles dans la boîte de dialogue :

Hôte	Affiche le nom de l'hôte pour lequel vous souhaitez approuver ou rejeter le mappage.
Noms d'hôtes/Adresses IP mappés	Répertorie les mappages existants qui sont associés à l'hôte.
ID de l'hôte NetBackup	Affiche l'ID de l'hôte.

Conflit de mappage - Partagé avec les hôtes	**Remarque :** Ces informations sont affichées si le mappage sélectionné est déjà associé à d'autres hôtes. Ce tableau répertorie les informations de tous les hôtes sur lesquels le mappage sélectionné est partagé. Par exemple, dans une configuration en cluster, plusieurs ID d'hôte partagent le même nom virtuel. Si un mappage est ajouté pour un ID d'hôte et que ce même mappage est reconnu sur un autre ID d'hôte, il est répertorié dans l'onglet **Mappages à approuver**. Vous pouvez approuver ce mappage ou le rejeter à l'aide de la boîte de dialogue **Détails des mappages**. ■ Hôte - affiche le nom de l'hôte auquel le mappage sélectionné est déjà associé. ■ ID de l'hôte NetBackup - affiche l'ID de l'hôte auquel le mappage sélectionné est déjà associé. Se reporter à "Scénarios de mappages partagés ou de cluster" à la page 308.
Raison	Indiquez la raison de l'approbation ou du rejet du mappage.
Approuver	Cliquez pour approuver le mappage en attente.
Rejeter	Cliquez pour rejeter le mappage en attente.
Fermer	Cliquez pour fermer la boîte de dialogue sans enregistrer les modifications.
Aide	Cliquez pour consulter l'aide.

Approbation des mappages d'ID d'hôte vers le nom d'hôte

Cette section présente la procédure permettant d'approuver les mappages d'ID vers le nom d'hôte qui sont en attente d'approbation.

Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.

Se reporter à "Rejet des mappages d'ID d'hôte vers le nom d'hôte" à la page 307.

Pour approuver un mappage d'ID vers un nom d'hôte

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité > Gestion des certificats**.
2. Dans le volet des détails, cliquez sur l'onglet **Mappages à approuver**.

3. Sélectionnez le mappage que vous souhaitez approuver et cliquez avec le bouton droit de la souris.
4. Dans les options du clic droit, cliquez sur **Approuver**. Les mappages sélectionnés sont approuvés.

   Sinon, cliquez sur **Détails des mappages** dans les options du clic droit. Utilisez la boîte de dialogue **Détails des mappages** pour approuver le mappage sélectionné.

   Se reporter à "Boîte de dialogue Détails des mappages" à la page 305.

Rejet des mappages d'ID d'hôte vers le nom d'hôte

Cette section présente la procédure permettant de rejeter les mappages d'ID vers le nom d'hôte qui sont en attente d'approbation.

Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.

Se reporter à "Approbation des mappages d'ID d'hôte vers le nom d'hôte" à la page 306.

Pour rejeter un mappage d'ID vers un nom d'hôte

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité > Gestion des certificats**.
2. Dans le volet des détails, cliquez sur l'onglet **Mappages à approuver**.
3. Sélectionnez le mappage que vous souhaitez rejeter et cliquez avec le bouton droit de la souris.
4. Dans les options du clic droit, cliquez sur **Rejeter**. Les mappages sélectionnés ont été rejetés.

   Sinon, cliquez sur **Détails des mappages** dans les options du clic droit. Utilisez la boîte de dialogue **Détails des mappages** pour rejeter le mappage sélectionné.

Ajout de mappages partagés ou de cluster

Dans certains scénarios, les mappages d'ID d'hôte vers le nom d'hôte sont partagés entre les ID d'hôte. Par exemple, dans une configuration de cluster, le nom virtuel est partagé entre tous les nœuds. Vous devez ajouter ces mappages partagés à l'aide de la **console d'administration NetBackup** pour que le serveur maître puisse communiquer avec les nœuds.

Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.

Pour ajouter des mappages partagés

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité > Gestion des certificats**.
2. Dans l'onglet **Hôtes**, volet des détails, cliquez avec le bouton droit de la souris pour afficher les options.
3. Dans les options du clic droit, sélectionnez **Ajouter des mappages partagés ou de cluster**.
4. Dans la boîte de dialogue **Ajouter des mappages partagés ou de cluster**, indiquez le nom du mappage partagé.

   Se reporter à "Boîte de dialogue Ajouter des mappages partagés ou de cluster" à la page 309.
5. Sélectionnez les ID d'hôte à mapper avec le nom de mappage partagé spécifié.
6. Cliquez sur **Enregistrer**.

Scénarios de mappages partagés ou de cluster

Les mappages d'ID d'hôte vers des noms d'hôte peuvent être partagés sur plusieurs hôtes dans les scénarios suivants :

- si plusieurs hôtes de différents domaines utilisent le même nom d'hôte ;
- dans une configuration de cluster où le même nom virtuel est utilisé par plusieurs nœuds de cluster.

Toutefois, dans un scénario où les hôtes associés n'ont pas le même état de communication (certains hôtes étant dans la version 8.0 ou une version antérieure et pouvant communiquer de manière non sécurisée et d'autres étant dans la version 8.1 ou une version ultérieure et pouvant communiquer de manière sécurisée), la communication peut échouer.

Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.

Scénario 1 - Plusieurs hôtes de différents domaines utilisent le même nom d'hôte

Prenons l'exemple suivant :

- Hôte1 – abc.secure.domain1.com, version – 8.1, politique – P1
- Hôte2 – abc.insecure.domain2.com, version – 7.7.3, politique – P2
- L'hôte1 et l'hôte2 utilisent le même nom – abc – comme nom d'hôte. L'administrateur de sécurité ajoute abc comme mappage partagé pour l'hôte2.
  Se reporter à "Ajout de mappages partagés ou de cluster" à la page 307.

- Une communication non sécurisée avec des hôtes versions 8.0 et antérieures est activée.
  Se reporter à "À propos de la communication non sécurisée avec les hôtes 8.0 et versions antérieures" à la page 319.
- Lorsque l'hôte2 démarre une communication avec un autre hôte, le serveur maître valide l'état de la communication de l'hôte2 (non sécurisé), qui est différent de celui de l'hôte1 (sécurisé). Comme les deux hôtes utilisent le même nom d'hôte, mais que l'état de leur communication ne correspond pas, la communication avec l'hôte2 échoue.
- Recommandation : l'hôte2 doit être mis à niveau vers la version 8.1 ou une version ultérieure.

Scénario 2 - Configuration de cluster où le même nom virtuel est utilisé par plusieurs nœuds de cluster

Prenons l'exemple suivant :

- Hôte1 – abc.secure.domain1.com, nœud de cluster actif, version – 8.1
- Hôte2 – abc.secure.domain1.com, nœud de cluster inactif, version – 8.0
- L'hôte1 et l'hôte2 utilisent le même nom virtuel abc. L'administrateur de sécurité ajoute abc comme mappage partagé ou de cluster pour l'hôte2.
  Se reporter à "Ajout de mappages partagés ou de cluster" à la page 307.
- Une communication non sécurisée avec des hôtes versions 8.0 et antérieures est activée.
  Se reporter à "À propos de la communication non sécurisée avec les hôtes 8.0 et versions antérieures" à la page 319.
- L'hôte1 bascule vers l'hôte2. Le serveur maître valide l'état de la communication de l'hôte2 (non sécurisé), qui est différent de celui de l'hôte1 (sécurisé). Comme l'état de communication des deux hôtes ne correspond pas, la communication avec l'hôte2 échoue.
- Recommandation : l'hôte2 doit être mis à niveau vers la version 8.1.
- Solution de contournement : supprimez le mappage abc de l'ID d'hôte vers le nom d'hôte pour l'hôte1. En cas de mappage partagé, si les hôtes associés ne disposent pas du même état de communication (sécurisé), la communication échoue pour l'hôte ayant l'état de communication non sécurisé.

Boîte de dialogue Ajouter des mappages partagés ou de cluster

Utilisez cette option pour ajouter des mappages de cluster ou partagés. Dans l'onglet **Gestion de la sécurité > Gestion des hôtes > Hôtes**, dans les options

contextuelles, cliquez sur **Ajouter des mappages partagés ou de cluster** pour ouvrir la boîte de dialogue.

Les options suivantes sont disponibles dans la boîte de dialogue **Ajouter des mappages partagé ou de cluster** :

Nom de mappage partagé ou nom virtuel du cluster	Entrez le nom de mappage qui doit être partagé par plusieurs identifiants d'hôte.
Sélectionner des hôtes	Cliquez sur le bouton pour répertorier tous les hôtes et sélectionnez ceux que vous voulez mapper avec le nom de mappage spécifié. La fenêtre contextuelle **Sélectionner des hôtes** répertorie tous les hôtes disponibles. Sélectionnez les hôtes requis et cliquez sur **Ajouter à la liste**. Les hôtes sélectionnés s'affichent dans la liste dans la boîte de dialogue **Ajouter des mappages partagés ou de cluster**.
Hôte	Nom de l'hôte que vous voulez mapper avec le nom de partage spécifié.
ID de l'hôte NetBackup	ID de l'hôte que vous voulez mapper avec le nom de partage spécifié.
Enregistrer	Cliquez pour enregistrer le mappage.
Annuler	Cliquez pour fermer la boîte de dialogue sans enregistrer les modifications.
Aide	Cliquez pour consulter l'aide.

Se reporter à "Ajout de mappages partagés ou de cluster" à la page 307.

Se reporter à "Scénarios de mappages partagés ou de cluster" à la page 308.

Réinitialisation des attributs d'hôte NetBackup

Dans certains scénarios, vous pouvez avoir à nettoyer ou réinitialiser les attributs d'hôte : par exemple, si vous avez mis à niveau l'hôte sur une version antérieure.

Dans ce cas, vous devez réinitialiser l'ID de l'hôte sur les informations de mappage du nom d'hôte, sur l'état de communication et ainsi de suite pour établir la communication avec succès.

Lisez les notes suivantes avant de réinitialiser les attributs d'hôte

- Vous devez réinitialiser les attributs de l'hôte mis à niveau sur une version antérieure si vous souhaitez que le serveur maître communique avec l'hôte dans un mode non sécurisé.
- La réinitialisation des attributs d'hôte réinitialise les ID de l'hôte sur les informations de mappage du nom d'hôte, sur l'état de communication et ainsi de suite. Cette opération ne réinitialise pas l'ID, le nom ou les certificats de sécurité de l'hôte.
- Après avoir réinitialisé les attributs d'hôte, la connexion (indicateur de sécurité) n'est pas sécurisée. Lors de la communication d'hôte suivante, l'état de la connexion est mis à jour en conséquence.
- Si vous avez utilisé par erreur l'option **Réinitialiser les attributs de l'hôte**, vous pouvez annuler les modifications en redémarrant le service `bpcd`. Sinon, les attributs de l'hôte sont automatiquement mis à jour avec les valeurs appropriées au bout de 24 heures.

Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.

Réinitialisation des attributs d'hôte

Le serveur maître NetBackup 8.1 peut communiquer en toute sécurité avec tous les hôtes 8.1. Il communique cependant de manière non sécurisée avec les hôtes des versions 8.0 et antérieures.

Dans certains scénarios, vous pouvez avoir à mettre à niveau un client NetBackup sur une version antérieure, de la version 8.1 sur la version 8.0 ou une version antérieure. Après la mise à niveau sur une version antérieure, le serveur maître ne peut pas communiquer avec le client, car l'état de communication pour le client est toujours défini en mode sécurisé. L'état de communication n'est pas automatiquement mis à jour en mode non sécurisé après la mise à niveau sur une version antérieure.

Utilisez l'une des options suivantes pour réinitialiser un hôte :

Pour réinitialiser un hôte à l'aide de la console d'administration NetBackup

1. Développez **Gestion de la sécurité > Gestion des certificats**.
2. Sous l'onglet **Hôtes**, dans le volet de détails, avec le bouton droit de la souris, cliquez sur l'hôte que vous avez mis à niveau sur une version antérieure et que vous voulez réinitialiser, puis cliquez sur **Réinitialiser les attributs de l'hôte**.

Remarque : Pour reprendre la communication non sécurisée avec les hôtes mis à niveau sur une version antérieure, vérifiez que l'option **Activer la communication non sécurisée avec les hôtes 8.0 et versions antérieures** de l'onglet **Gestion de la sécurité > Paramètres de sécurité globaux** est sélectionnée.

Pour réinitialiser les attributs d'hôte à l'aide de l'interface de ligne de commande

1. Exécutez la commande suivante pour authentifier votre connexion aux services Web :

   ```
   bpnbat -login -loginType WEB
   ```

2. Exécutez la commande suivante pour réinitialiser l'hôte :

   ```
   nbemmcmd -resethost
   ```

Autoriser ou ne pas autoriser le renouvellement de certificat automatique

Cette section fournit les procédures permettant d'autoriser et de ne pas autoriser le renouvellement de certificat automatique.

L'option **Autoriser le renouvellement de certificat automatique** active le paramètre `autoreissue` d'un hôte, ce qui vous permet de déployer un certificat sur l'hôte sans avoir recours à un jeton de renouvellement.

Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.

Par défaut, le paramètre `autoreissue` est activé pendant 2 880 minutes (48 heures ou 2 jours). Après cette durée, le paramètre est désactivé et l'opération de renouvellement de certificat requiert un jeton de renouvellement.

Se reporter à "Configuration de la validité du paramètre `autoreissue` pour un hôte" à la page 314.

Pour désactiver manuellement le paramètre `autoreissue`, utilisez l'option **Ne pas autoriser le renouvellement automatique de certificat**.

Remarque : Pendant le processus BMR (Bare Metal Restore), l'indicateur `autoreissue` est défini automatiquement.

Pour plus d'informations sur Bare Metal Restore, consultez le *Guide de l'administrateur de NetBackup Bare Metal Restore*.

Pour autoriser le renouvellement de certificat automatique à l'aide de la console d'administration NetBackup

1. Développez **Gestion de la sécurité** > **Gestion des hôtes**.
2. Dans le volet droit, sélectionnez l'hôte pour lequel vous souhaitez autoriser le renouvellement de certificat automatique.
3. Cliquez avec le bouton droit de la souris sur l'hôte et sélectionnez l'option **Autoriser le renouvellement de certificat automatique**.

Pour autoriser le renouvellement de certificat automatique à l'aide de l'interface de ligne de commande

1. Exécutez la commande suivante pour authentifier votre connexion aux services Web :

   ```
   bpnbat -login -loginType WEB
   ```

2. Exécutez la commande suivante pour activer le paramètre `autoreissue`, qui permet à son tour le renouvellement de certificat automatique :

   ```
   nbhostmgmt -allowautoreissuecert -hostid host_ID -autoreissue 1
   ```

Ne pas autoriser le renouvellement de certificat automatique à l'aide de la console d'administration NetBackup

1. Développez **Gestion de la sécurité** > **Gestion des hôtes**.
2. Dans le volet droit, sélectionnez l'hôte pour lequel ne pas autoriser le renouvellement de certificat automatique.
3. Cliquez avec le bouton droit de la souris sur l'hôte et sélectionnez l'option **Ne pas autoriser le renouvellement de certificat automatique**.

Ne pas autoriser le renouvellement de certificat automatique à l'aide de l'interface de ligne de commande

1. Exécutez la commande suivante pour authentifier votre connexion aux services Web :

   ```
   bpnbat -login -loginType WEB
   ```

2. Exécutez la commande suivante pour désactiver le paramètre `autoreissue`, qui permet à son tour de ne pas autoriser le renouvellement de certificat automatique :

   ```
   nbhostmgmt -allowautoreissuecert -hostid host_ID -autoreissue 0
   ```

Configuration de la validité du paramètre `autoreissue` pour un hôte

Lorsque vous autorisez le renouvellement automatique d'un certificat basé sur l'ID d'un hôte, le paramètre `autoreissue` est activé par défaut pendant 2 880 minutes (48 heures ou 2 jours). Après cette durée, le paramètre est réinitialisé et l'opération de renouvellement de certificat requiert un jeton de renouvellement.

Vous pouvez configurer la durée du renouvellement automatique d'un certificat ou le réglage time-to-live (TTL) pour le paramètre `autoreissue` en mettant à jour le fichier `web.conf`.

Configuration de la validité du paramètre `autoreissue` ou du réglage time-to-live (TTL)

1. Ouvrez le fichier `web.conf`. L'emplacement du fichier est le suivant :

   Sous Windows :`Install_Path\var\global\wsl\config\web.conf`

   Sous Linux :`/usr/openv/var/global/wsl/config/web.conf`

2. Configurez le réglage time-to-live (TTL) pour le paramètre `autorissue` en minutes. Par exemple :

   ```
   ttl.autoReissue.minutes = 1440
   ```

   Remarque : La plage valide pour le paramètre TTL `autoreissue` est comprise entre 0 et 43 200 minutes (ou 30 jours).

   Si la valeur TTL que vous avez configurée n'est pas comprise dans la plage valide, le serveur continue à utiliser la dernière valeur TTL configurée.

   ---

3. Pour que la nouvelle valeur TTL `autoreissue` prenne effet, effectuez l'une des opérations suivantes :

- Redémarrez le service NetBackup Web Management Console (WMC).
- Exécutez la commande suivante :
  Sous Windows : *Install_Path*\bin\nbhostdbcmd -reloadconfig -host
  Sous UNIX : *NETBACKUP_INSTALL_DIR*\bin\nbhostdbcmd -reloadconfig -host

Ajout ou suppression d'un commentaire pour un hôte

Vous pouvez fournir des informations supplémentaires concernant un hôte NetBackup à l'aide de la boîte de dialogue **Ajouter ou modifier le commentaire**. Par exemple, si un hôte est mis hors service, vous pouvez ajouter un commentaire pour expliquer pourquoi et quand il a été mis hors service.

Pour ajouter ou modifier un commentaire pour un hôte

1. Développez **Gestion de la sécurité > Gestion des certificats**.
2. Sous l'onglet **Hôtes**, dans le volet des détails, cliquez avec le bouton droit de la souris sur l'hôte pour lequel vous souhaitez fournir des informations supplémentaires, puis cliquez sur **Ajouter ou modifier un commentaire**.
3. Dans la boîte de dialogue **Ajouter ou modifier un commentaire**, dans le volet **Commentaire**, entrez les informations requises ou les commentaires.

   Cliquez sur **Enregistrer**.

Pour supprimer un commentaire d'un hôte

1. Développez **Gestion NetBackup > Gestion de la sécurité > Gestion des hôtes**.
2. Sous l'onglet **Hôtes**, volet des détails, cliquez avec le bouton droit de la souris sur l'hôte pour lequel vous souhaitez supprimer un commentaire, puis cliquez sur **Supprimer le commentaire**.

À propos des paramètres de sécurité globale

Le nœud **Gestion de la sécurité > Paramètres de sécurité globale** permet de configurer les paramètres cruciaux pour la communication sécurisée dans NetBackup.

Se reporter à "Communication sécurisée dans NetBackup" à la page 295.

Se reporter à "À propos des paramètres de reprise après incident" à la page 321.

Se reporter à "À propos des paramètres de communication sécurisée" à la page 316.

À propos des paramètres de communication sécurisée

NetBackup fournit des paramètres que vous pouvez configurer pour la communication sécurisée entre les hôtes.

Tableau 15-2 Paramètres de communication sécurisée

Paramètre	Description
Autorité de certification	Affiche les autorités de certification prises en charge par votre domaine NetBackup. Le serveur Web NetBackup peut être configuré pour autoriser le domaine NetBackup à utiliser : ■ Uniquement les certificats signés par l'autorité de certification NetBackup ■ Uniquement les certificats signés par l'autorité de certification externe ■ Les certificats signés par l'autorité de certification NetBackup et l'autorité de certification externe Utilisez la commande `-configureWebServerCerts` pour la configuration des certificats du serveur Web. Pour plus d'informations, consultez le *NetBackupGuide de référence des commandes* .

Paramètre	Description
Activer la communication non sécurisée avec des hôtes NetBackup 8.0 et versions antérieures	NetBackup communique de manière non sécurisée avec les hôtes des versions 8.0 et antérieures. Pour accroître la sécurité, procédez à la mise à niveau de tous vos hôtes vers la version actuelle et désactivez ce paramètre. Vous garantissez ainsi une communication sécurisée entre les hôtes NetBackup. Cette option est sélectionnée par défaut, ce qui permet à NetBackup de communiquer avec des hôtes, y compris des hôtes de versions 8.0 et antérieures, pouvant être présents dans l'environnement NetBackup existant. L'option permet également au serveur maître NetBackup 8.1 ou version ultérieure et au serveur OpsCenter de communiquer. Se reporter à "Désactivation de la communication non sécurisée" à la page 318. Se reporter à "À propos de la communication non sécurisée avec les hôtes 8.0 et versions antérieures" à la page 319. Si vous avez configuré Auto Image Replication, vérifiez ce qui suit avant de décocher l'option : Le serveur maître approuvé que vous avez spécifié pour la réplication d'image est dans une version ultérieure à NetBackup 8.0. Pour plus d'informations, consultez le *Guide de l'administrateur NetBackup, volume I*.

Paramètre	Description
Mapper automatiquement l'ID d'hôte NetBackup aux noms d'hôtes	Plusieurs noms d'hôte ou adresses IP peuvent être associés aux hôtes. Pour une communication réussie entre les hôtes, tous les noms d'hôte et adresses IP appropriés doivent être mappés vers les ID d'hôte respectifs. Pendant la communication, NetBackup peut détecter de nouveaux noms d'hôte ou adresses IP relatifs à un ID d'hôte. Sélectionnez cette option pour mapper automatiquement l'ID d'hôte aux noms d'hôte ou adresses IP qui sont détectés par le système. Par défaut, l'option est sélectionnée. Pour plus de sécurité, désélectionnez cette option de sorte que l'administrateur NetBackup puisse vérifier manuellement les mappages et les approuver. Se reporter à "Mappage automatique des ID d'hôte vers les noms d'hôte et adresses IP" à la page 321.
Niveau de sécurité pour le déploiement de certificat	L'approche de déploiement de certificat est déterminée en fonction du niveau de sécurité configuré sur le serveur maître NetBackup. Par exemple, si le niveau de sécurité est défini sur **Très élevée**, un jeton d'autorisation est nécessaire pour le déploiement de certificat. **Remarque :** Les niveaux de sécurité pour le déploiement de certificat sont spécifiques des certificats signés par l'autorité de certification NetBackup. Si le serveur Web NetBackup n'est pas configuré pour utiliser les certificats NetBackup pour les communications sécurisées, cette option n'est pas accessible. Se reporter à "À propos des niveaux de sécurité de déploiement de certificats NetBackup" à la page 334. Se reporter à "Configuration des niveaux de sécurité de déploiement de certificats" à la page 337.

Désactivation de la communication non sécurisée

Par défaut, NetBackup peut communiquer avec les hôtes de version 8.0 et de versions antérieures. Pour plus de sécurité, vous devez mettre à niveau tous les

hôtes vers la version actuelle et désactiver la communication avec les hôtes de version 8.0 et de versions antérieures.

Se reporter à "À propos des paramètres de communication sécurisée" à la page 316.

Pour désactiver la communication non sécurisée

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité > Paramètres de sécurité globaux**.
2. Dans le volet des détails, cliquez sur l'onglet **Communication sécurisée**.
3. Désactivez l'option **Activer la communication non sécurisée avec les hôtes 8.0 et versions antérieures**.
4. Cliquez sur **Enregistrer**.

Remarque : Si vous désactivez les communications non sécurisées, il est recommandé de redémarrer les services pour mettre fin à toutes les connexions non sécurisées déjà établies.

À propos de la communication non sécurisée avec les hôtes 8.0 et versions antérieures

NetBackup communique correctement avec les hôtes 8.0 ou versions antérieures.

Si l'environnement contient des hôtes NetBackup 8.0 ou versions antérieures, vous pouvez autoriser la communication non sécurisée avec eux en utilisant l'option **Activer la communication non sécurisée avec les hôtes 8.0 et antérieurs** dans la **console d'administration NetBackup**.

L'option est disponible dans l'onglet **Gestion de la sécurité > Paramètres de sécurité globale > Communication sécurisée**.

L'option permet également au serveur maître NetBackup 8.1 ou version ultérieure et au serveur OpsCenter de communiquer.

Par défaut, la communication non sécurisée est activée. Cependant, pour renforcer la sécurité, mettez à niveau tous les hôtes vers la version actuelle, et désactivez la communication avec les hôtes 8.0 et versions antérieures.

Se reporter à "Désactivation de la communication non sécurisée" à la page 318.

Se reporter à "Communication avec un hôte 8.0 ou une version antérieure dans plusieurs domaines NetBackup" à la page 320.

Remarque : Si vous avez configuré Auto Image Replication (AIR), vérifiez ce qui suit avant de désactiver la communication non sécurisée. Le serveur maître approuvé que vous avez spécifié pour la réplication d'image correspond à une version postérieure à NetBackup 8.0.

Se reporter à "Communication sécurisée dans NetBackup" à la page 295.

Communication avec un hôte 8.0 ou une version antérieure dans plusieurs domaines NetBackup

Cette section fournit des informations sur l'impact de l'option **Activer la communication non sécurisée avec les hôtes 8.0 et versions antérieures** sur la communication d'hôte lorsque l'un des hôtes NetBackup se trouve dans plusieurs domaines.

Imaginez le scénario suivant :

- L'hôte A possède la version 8.1, qui est présente dans plusieurs domaines NetBackup, appelés M1 et M2.
- L'hôte B possède la version 8.0, qui est présente dans un domaine NetBackup, appelé M3.
- L'option **Activer la communication non sécurisée avec les hôtes 8.0 et versions antérieures** est désactivée sur le serveur maître M1, ce qui signifie que les hôtes qui sont associés à M1 ne peuvent pas communiquer avec les hôtes de version 8.0 ou de versions antérieures.
- L'option **Activer la communication non sécurisée avec les hôtes 8.0 et versions antérieures** est sélectionnée sur le serveur maître M2, ce qui signifie que les hôtes qui sont associés à M2 peuvent communiquer avec les hôtes de version 8.0 ou de versions antérieures.
- Le fichier de configuration (fichier `bp.conf` sur UNIX ou sur clés de registre sous Windows) pour l'hôte A contient « M2 » comme première entrée dans la liste de serveurs maîtres.

Lorsque l'hôte A lance la communication avec l'hôte B, le statut de l'option **Activer la communication non sécurisée avec les hôtes 8.0 et versions antérieures** est vérifié pour le premier serveur maître qui apparaît dans le fichier de configuration de l'hôte A, M2. Selon l'option définie pour M2, la communication avec les hôtes de version 8.0 ou de versions antérieures est autorisée. Par conséquent, la communication entre l'hôte A et l'hôte B est établie avec succès.

Mappage automatique des ID d'hôte vers les noms d'hôte et adresses IP

Pour une communication réussie entre les hôtes NetBackup, tous les noms d'hôte et adresses IP appropriés doivent être mappés vers les ID d'hôte respectifs. Vous pouvez choisir de mapper automatiquement l'ID d'hôte vers les noms d'hôte respectifs (et adresses IP) ou d'autoriser l'administrateur NetBackup à vérifier les mappages avant de les approuver.

Se reporter à "Boîte de dialogue Ajouter ou supprimer des mappages d'hôtes" à la page 301.

Remarque : Pour plus de sécurité, désélectionnez cette option de sorte que l'administrateur NetBackup puisse vérifier manuellement les mappages et les approuver.

Pour mapper automatiquement les ID d'hôte vers les noms d'hôte ou adresses IP

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** > **Paramètres de sécurité globaux**.
2. Dans le volet des détails, cliquez sur l'onglet **Communication sécurisée**.
3. Sélectionnez l'option **Mapper automatiquement les ID d'hôte vers les noms d'hôte**.
4. Cliquez sur **Enregistrer**.

Se reporter à "À propos des paramètres de communication sécurisée" à la page 316.

À propos des paramètres de reprise après incident

Pour plus de sécurité, un package de reprise après incident est créé pendant chaque sauvegarde de catalogue.

Se reporter à "Packages de reprise après incident" à la page 325.

Pendant chaque sauvegarde de catalogue, un package de reprise après incident est créé et chiffré avec la phrase de passe que vous avez définie. Vous devez fournir cette phrase de passe de chiffrement lors de l'installation de NetBackup sur le serveur maître en mode de reprise après incident.

Les options suivantes s'affichent dans l'onglet **Reprise après incident** :

Tableau 15-3 Paramètres de reprise après incident

Paramètre	Description
Phrase de passe	Entrez la phrase de passe pour chiffrer les packages de reprise après incident. ■ Par défaut, la phrase de passe doit contenir entre 8 et 1 024 caractères. Vous pouvez définir les contraintes de phrase de passe à l'aide de l'option de commande `nbseccmd -setpassphraseconstraints`. ■ La phrase de passe existante et la nouvelle phrase doivent être différentes. ■ Seuls les caractères suivants sont acceptés pour la phrase de passe : espaces, caractères majuscules (de A à Z), caractères minuscules (de a à z), chiffres (de 0 à 9) et caractères spéciaux. Voici les caractères spéciaux acceptés : ~ ! @ # $ % ^ & * ( ) _ + - = ` { } [ ] | : ; ' , . / ? < > " Se reporter à "Définition d'une phrase de passe pour chiffrer des packages de reprise après incident" à la page 323.
Confirmer la phrase de passe	Saisissez à nouveau la phrase de passe pour la confirmer.

Attention : Assurez-vous que la phrase de passe contient uniquement des caractères valides. Si vous entrez un caractère non valide, vous risquez de rencontrer des problèmes pendant la restauration de package de reprise après incident. La phrase de passe peut ne pas être validée et vous ne pourrez peut-être pas restaurer le package de reprise après incident.

Prenez en compte les informations suivantes avant de modifier la phrase de passe d'un package de reprise après incident :

- Les packages de reprise après incident ultérieurs sont chiffrés avec la nouvelle phrase de passe que vous avez définie.
- Si vous modifiez la phrase de passe à tout moment, elle n'est pas modifiée pour les packages de reprise après incident précédents. Seuls les nouveaux packages de reprise après incident sont associés à la nouvelle phrase de passe.
- La phrase de passe que vous fournissez lors de l'installation de NetBackup sur le serveur maître en mode de reprise après incident doit correspondre à celle du package de reprise après incident à partir duquel vous souhaitez récupérer l'identité de l'hôte de serveur maître.

Définition d'une phrase de passe pour chiffrer des packages de reprise après incident

Pendant chaque sauvegarde de catalogue, un package de reprise après incident est créé et chiffré avec la phrase de passe que vous avez définie.

Se reporter à "Packages de reprise après incident" à la page 325.

Workflow pour définir une phrase de passe pour chiffrer des packages de reprise après incident et pour l'utiliser après un incident :

Vérifiez le workflow suivant pour en savoir plus sur la restauration d'un package de reprise après incident :

1. Définissez un mot de passe de chiffrement pour les packages de reprise après incident.
2. Créez une politique de catalogue.

   Prenons les scénarios suivants :

   - Si vous n'avez pas défini la phrase de passe plus tôt, NetBackup vous empêche de configurer une nouvelle politique de sauvegarde de catalogue.
   - Si la politique de sauvegarde du catalogue est mise à niveau à partir d'une version précédente, les sauvegardes de catalogue continuent à échouer jusqu'à ce que la phrase de passe soit définie.

   Remarque : Les sauvegardes de catalogue peuvent échouer avec le code d'état 144 même si la phrase de passe est définie. Ceci est dû au fait que le mot de passe peut être corrompu. Pour résoudre ce problème, vous devez redéfinir la phrase de passe.

   ---

3. Après un incident, lorsque vous installez NetBackup sur le serveur maître dans un mode de reprise après incident, entrez la phrase de passe que vous avez définie plus tôt. NetBackup déchiffre le package de reprise après incident à l'aide de cette phrase de passe et obtient l'identité du serveur maître pendant l'installation.

   Attention : Si vous ne parvenez pas à fournir la phrase de passe adéquate lors de l'installation de NetBackup sur le serveur maître après un sinistre, vous devrez peut-être redéployer les certificats sur tous les hôtes NetBackup. Pour plus d'informations, consultez l'article suivant :

   https://www.veritas.com/content/support/en_US/article.100033743

   ---

4. Une fois l'identité du serveur maître à nouveau en place, la communication sécurisée entre le serveur maître et le serveur de médias est établie et vous pouvez effectuer la récupération de catalogue.
5. Une fois la récupération de catalogue effectuée, vous devez redéfinir la phrase de passe du package de reprise après incident, car la phrase de passe n'est pas récupérée pendant la récupération de catalogue. Les sauvegardes de catalogue que vous configurez dans une nouvelle instance de NetBackup continuent d'échouer jusqu'à ce que vous définissiez le mot de passe.

Pour définir ou modifier une phrase de passe

1 Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** > **Paramètres de sécurité globaux**.

2 Dans le volet des détails, cliquez sur l'onglet **Reprise après incident**.

Se reporter à "À propos des paramètres de reprise après incident" à la page 321.

3 Entrez la **phrase de passe** et **confirmez la phrase de passe**.

Vérifiez les règles de mot de passe suivantes :

- La phrase de passe existante et la nouvelle phrase doivent être différentes.
- Par défaut, la phrase de passe doit contenir entre 8 et 1 024 caractères. Vous pouvez définir les contraintes de phrase de passe à l'aide de l'option de commande `nbseccmd -setpassphraseconstraints`.
- Seuls les caractères suivants sont acceptés pour la phrase de passe : espaces, caractères majuscules (de A à Z), caractères minuscules (de a à z), chiffres (de 0 à 9) et caractères spéciaux. Voici les caractères spéciaux acceptés : ~ ! @ # $ % ^ & * ( ) _ + - = ` { } [ ] | : ; ' , . / ? < > "

Attention : Si vous entrez un caractère non valide, vous risquez de rencontrer des problèmes pendant la restauration de package de reprise après incident. La phrase de passe peut ne pas être validée et vous ne pourrez peut-être pas restaurer le package de reprise après incident.

4 Cliquez sur **Enregistrer**. Si la phrase de passe existe déjà, elle est écrasée.

Pour définir ou modifier une phrase de passe à l'aide de l'interface de ligne de commande

1. L'administrateur NetBackup doit être connecté au service de gestion Web de NetBackup pour effectuer cette tâche. Pour vous connecter, utilisez la commande suivante :

   ```
   bpnbat -login -loginType WEB
   ```

2. Exécutez la commande suivante pour définir une phrase de passe pour chiffrer des packages de reprise après incident :

   ```
   nbseccmd -drpkgpassphrase
   ```

3. Entrez la phrase de passe.

   Si une phrase de passe existe déjà, elle est écrasée.

Packages de reprise après incident

Pour plus de sécurité, un package de reprise après incident est créé pendant chaque sauvegarde de catalogue. Le package de reprise après incident porte l'extension `.drpkg`.

Le package de reprise après incident (DR) stocke l'identité de l'hôte du serveur maître. NetBackup requiert ce package pour obtenir l'identité du serveur maître après un incident. Une fois que vous avez récupéré l'identité de l'hôte, vous pouvez effectuer la récupération de catalogue.

Le package de reprise après incident contient les informations suivantes :

- Certificats signés par l'autorité de certification NetBackup et clés privées du certificat du serveur maître et du certificat de l'autorité de certification NetBackup
- Informations sur les hôtes du domaine
- Paramètres de sécurité
- Certificats signés par l'autorité de certification externe
  Certificats signés par l'autorité de certification externe à partir du magasin de certificats Windows, le cas échéant
- Options de configuration NetBackup qui sont propres aux certificats signés par l'autorité de certification externe
- Configuration du service de gestion des clés (KMS)

Remarque : Par défaut, la configuration KMS n'est pas sauvegardée lors de la sauvegarde du catalogue. Définissez l'option de configuration KMS_CONFIG_IN_CATALOG_BKUP sur 1 pour inclure la configuration KMS dans le package de reprise après incident lors de la sauvegarde du catalogue.

Remarque : Vous devez définir une phrase de passe pour le package de reprise après incident pour que les sauvegardes de catalogue réussissent.

Se reporter à "À propos des paramètres de reprise après incident" à la page 321.

Se reporter à "Définition d'une phrase de passe pour chiffrer des packages de reprise après incident" à la page 323.

À propos des certificats basés sur le nom d'hôte

Par défaut, les serveurs maîtres individuels NetBackup sont provisionnés avec un certificat basé sur le nom d'hôte pendant l'installation. Pour provisionner un certificat basé sur le nom d'hôte sur un serveur de médias ou de client, l'administrateur de NetBackup exécute la commande `bpnbaz` sur le serveur maître pour transférer le certificat à d'autres hôtes.

Se reporter à "Présentation des certificats de sécurité dans NetBackup" à la page 294.

Déploiement de certificats basés sur le nom d'hôte

Sélectionnez l'une des procédures suivantes pour déployer un certificat de sécurité basé sur le nom d'hôte sur les hôtes NetBackup. Seul un administrateur NetBackup peut déployer des certificats.

Tableau 15-4 Déploiement de certificats basés sur le nom d'hôte

Procédure	Description et lien vers la procédure
Déploiement d'un certificat de sécurité basé sur le nom d'hôte pour un serveur maître dans un cluster	Suivez la procédure ci-après pour déployer les certificats de sécurité basés sur le nom d'hôte sur tous les nœuds dans un cluster de serveurs maîtres NetBackup.
Déploiement d'un certificat de sécurité basé sur le nom d'hôte pour les serveurs de médias ou de clients	Cette procédure utilise la vérification de l'adresse IP pour identifier l'hôte NetBackup cible, puis pour déployer le certificat. Cette procédure permet de déployer un certificat de sécurité basé sur le nom d'hôte pour un hôte individuel, pour tous les serveurs de médias ou pour tous les clients.

Remarque : Le déploiement d'un certificat basé sur le nom d'hôte est une activité unique pour un hôte. Si un certificat basé sur le nom d'hôte a été déployé pour une version antérieure ou pour un correctif, il n'est pas nécessaire de le faire à nouveau.

Déploiement d'un certificat de sécurité basé sur le nom d'hôte pour un serveur maître dans un cluster

Utilisez cette procédure pour déployer les certificats basés sur le nom d'hôte sur tous les nœuds de cluster.

Vérifiez ce qui suit avant de déployer un certificat basé sur le nom d'hôte :

- Tous les nœuds du cluster ont un certificat basé sur l'ID d'hôte.
- Tous les noms de domaine complets (FQHN) et les noms courts des nœuds de cluster sont mappés à leurs ID d'hôte respectifs.
  Se reporter à "Ajout de mappages d'ID d'hôte vers le nom d'hôte" à la page 299.

Pour déployer un certificat de sécurité basé sur le nom d'hôte pour un serveur maître NetBackup dans un cluster

1. Exécutez la commande suivante sur le nœud actif du cluster du serveur maître :

   Sous Windows : *`Install_path`*`\NetBackup\bin\admincmd\bpnbaz -setupat`

   UNIX : `/usr/openv/netbackup/bin/admincmd/bpnbaz -setupat`

2. Redémarrez le service NetBackup Service Layer (`nbsl`) et le service NetBackup Vault Manager (`nbvault`) sur le nœud actif du serveur maître.

Déploiement d'un certificat de sécurité basé sur le nom d'hôte sur les serveurs de médias ou les clients

Cette procédure fonctionne bien lorsque vous déployez simultanément des certificats de sécurité basés sur le nom d'hôte sur de nombreux hôtes. Comme pour le déploiement de NetBackup, cette méthode requiert la sécurisation du réseau.

Pour déployer un certificat de sécurité basé sur le nom d'hôte pour les serveurs de médias ou les clients

1. Exécutez la commande suivante sur le serveur maître, selon votre environnement. Indiquez un nom d'hôte ou effectuez le déploiement sur tous les serveurs de médias ou clients.

   Sous Windows : `Install_path\NetBackup\bin\admincmd\bpnbaz -ProvisionCert host_name|-AllMediaServers|-AllClients`

   Sous UNIX : `/usr/openv/netbackup/bin/admincmd/bpnbaz -ProvisionCert host_name|-AllMediaServers|-AllClients`

2. Démarrez le service NetBackup Service Layer (`nbsl`) sur le serveur de médias.

   Aucun service ne doit être redémarré si l'hôte cible est un client NetBackup.

Remarque : Si vous utilisez des IP dynamiques sur les hôtes (DHCP), assurez-vous que les noms d'hôte et les adresses IP sont répertoriés correctement sur le serveur maître. Pour ce faire, exécutez la commande NetBackup `bpclient` suivante sur le serveur maître :

Sous Windows : `Install_path\NetBackup\bin\admincmd\bpclient -L -All`

Sous UNIX : `/usr/openv/netbackup/bin/admincmd/bpclient -L -All`

À propos des certificats basés sur l'ID d'hôte

Chaque hôte dans un domaine NetBackup a une identité unique qui correspond à un ID d'hôte ou un identificateur unique universel (UUID). Le serveur maître est l'autorité de certification (CA). Il assigne aux hôtes des certificats basés sur l'ID de l'hôte et stocke les informations d'hôte dans la base de données `nbdb`. L'autorité de certification gère la liste de tous les ID d'hôte qui ont des certificats (ou des certificats révoqués). L'ID de l'hôte est utilisé dans de nombreuses opérations de gestion de certificat pour identifier l'hôte.

Les ID d'hôte sont générés aléatoirement par le système et ne sont pas liés aux propriétés du matériel.

NetBackup fournit une liste des certificats basés sur l'ID de l'hôte que vous avez révoqués.

Se reporter à "À propos de la liste de révocations des certificats basés sur l'ID d'hôte" à la page 362.

Se reporter à "Présentation des certificats de sécurité dans NetBackup" à la page 294.

Seul un administrateur NetBackup peut contrôler les paramètres associés à la révocation et au déploiement des certificats.

L'ID de l'hôte ne change pas, même si le nom de l'hôte change.

Si un hôte obtient des certificats de plusieurs domaines NetBackup, il dispose de plusieurs ID d'hôte qui correspondent à chaque domaine NetBackup.

Lorsque le serveur maître est configuré comme membre d'un cluster, chaque nœud du cluster reçoit un ID d'hôte unique. Un ID de l'hôte supplémentaire est attribué pour le nom virtuel. Par exemple, si le cluster du serveur maître est composé de *N* nœuds, le nombre d'ID d'hôte assignés pour le cluster de serveur maître est *N* + 1.

Conditions requises de connexion web pour les options de commande nbcertcmd

La commande `nbcertcmd` peut être utilisée pour effectuer toutes les opérations qui sont associées aux certificats basés sur l'ID d'hôte. Cependant, certaines options `nbcertcmd` nécessitent que l'utilisateur se connecte d'abord au service NetBackup Web Management (`nbwmc`).

- Pour vous connecter au service de gestion Web NetBackup, exécutez la commande suivante :

  ```
  bpnbat -login -logintype WEB
  ```

  Le compte doit disposer des droits d'administrateur NetBackup.
  Voici une exemple de connexion `WEB` :

  ```
  bpnbat -login -LoginType WEB
  Authentication Broker: server.domain.com
  Authentication port [0 is default]: 0
  Authentication type (NIS, NISPLUS, WINDOWS, vx, unixpwd, ldap): unixpwd
  Domain: server.domain.com
  Login Name: root
  Password: ********
  Operation completed successfully.
  ```

- La commande `bpnbat -login -logintype AT` crée une session avec le courtier d'authentification NetBackup (`nbatd`). (Le courtier d'authentification NetBackup ne peut pas toujours être le serveur maître.)

  Remarque : Une session `nbatd` n'est pas nécessaire pour exécuter les commandes `nbcertcmd`.

- Si ni `WEB` ni `AT` n'est indiqué, `bpnbat -login` crée une session pour les deux `nbatd` et `nbwmc`. (Cela est vrai si le courtier d'authentification se trouve sur le serveur maître.)

Remarque : Le courtier d'authentification pour une connexion WEB est le serveur maître lorsque le service `nbwmc` s'exécute uniquement sur le serveur maître.

Le Guide de référence des commandes NetBackup répertorie les informations détaillées du privilège nécessaire à chaque option `nbcertcmd`. Ce guide contient également des informations détaillées sur l'exécution de la commande `bpnbat`.

À l'aide de l'utilitaire de gestion de certificat pour émettre et déployer des certificats basés sur l'ID d'hôte

Le processus de déploiement du certificat basé sur l'ID d'hôte varie en fonction du niveau de sécurité de déploiement du certificat configuré sur le serveur maître. Les niveaux sont **Moyen**, **Elevé**, et **Très élevé**. Par défaut, le niveau de sécurité est **Haut**.

Un certificat basé sur un ID d'hôte est déployé automatiquement sur le serveur maître lors d'une installation ou d'une mise à niveau.

Les certificats basés sur un ID d'hôte sont déployés sur les hôtes après confirmation de la signature. La nécessité d'un jeton d'autorisation dépend du niveau de sécurité.

Ces niveaux déterminent la nature des vérifications de l'autorité de certification (CA) effectuées lorsque cette dernière reçoit une demande de certificat d'un hôte NetBackup. Sélectionnez le niveau de déploiement du certificat selon les exigences de sécurité de votre environnement NetBackup.

Se reporter à "À propos des niveaux de sécurité de déploiement de certificats NetBackup" à la page 334.

Dans certains scénarios, le déploiement de certificat requiert l'utilisation de jetons d'autorisation gérés par un administrateur NetBackup. L'administrateur NetBackup crée et partage ces jetons avec les administrateurs d'hôtes individuels pour le déploiement de certificat sur leurs hôtes locaux. Le déploiement d'un certificat peut se faire facilement, ce qui permet un déploiement évolutif sur plusieurs hôtes NetBackup sans nécessiter d'intervention de l'administrateur NetBackup.

Tableau 15-5 Conditions requises de déploiement à chaque niveau de déploiement de certificat ou d'un scénario

Niveau de déploiement de certificat ou scénario	Un jeton d'autorisation est-il requis ?	Déploiement du certificat basé sur l'ID d'hôte ?
Paramètre de niveau de déploiement de certificat sur **Très élevé**	Oui. Toutes les demandes de certificat requièrent un jeton d'autorisation. L'administrateur du serveur maître crée un jeton à utiliser sur l'hôte du serveur non maître : Se reporter à "Création de jetons d'autorisation" à la page 358.	L'administrateur de l'hôte du serveur non-maître doit obtenir un jeton d'autorisation de l'administrateur du serveur maître et l'utiliser pour déployer le certificat basé sur un ID d'hôte. Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.
Paramètre de niveau de déploiement de certificat sur **Elevé** (par défaut)	Peut-être. Les certificats sont déployés sans jetons sur les hôtes qui sont connus du serveur maître. La rubrique suivante explique les conséquences de la connaissance des certificats par le serveur maître : Se reporter à "À propos des niveaux de sécurité de déploiement de certificats NetBackup" à la page 334. Si l'hôte n'est pas connu du serveur maître, le certificat doit être déployé à l'aide d'un jeton d'autorisation. L'administrateur du serveur maître crée un jeton à utiliser sur l'hôte du serveur non-maître : Se reporter à "Création de jetons d'autorisation" à la page 358.	Si un certificat basé sur un ID d'hôte a été déployé, aucune action supplémentaire n'est requise. Si un jeton est requis, l'administrateur de l'hôte du serveur non-maître doit en obtenir un de l'administrateur du serveur maître et l'utiliser pour déployer le certificat basé sur un ID d'hôte. Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.
Paramètre de niveau de déploiement de certificat sur **Moyen**	Non. Les certificats peuvent être déployés sur tous les hôtes qui en demandent un. Se reporter à "Déploiement automatique du certificat basé sur l'ID de l'hôte" à la page 338. **Remarque :** Un certificat ne peut pas être déployé si le serveur maître ne peut pas vérifier que le nom d'hôte demandé correspond à l'adresse IP d'origine de la demande de certificat.	Si un certificat basé sur un ID d'hôte a été déployé, aucune action supplémentaire n'est requise. Si le serveur maître ne peut pas vérifier le nom d'hôte, un certificat basé sur un ID d'hôte doit être déployé à l'aide d'un jeton. Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.
Réémission de certificat	Oui. Un renouvellement de certificat requiert un jeton de renouvellement dans la plupart des cas.	Se reporter à "Création d'un jeton de renouvellement" à la page 354.

Niveau de déploiement de certificat ou scénario	Un jeton d'autorisation est-il requis ?	Déploiement du certificat basé sur l'ID d'hôte ?
Hôtes qui ne peuvent pas communiquer directement avec le serveur maître (par ex., hôtes NetBackup situés dans une zone démilitarisée (DMZ)).	Oui. NetBackup peut automatiquement détecter si un hôte dispose d'une connectivité avec le serveur maître. S'il n'existe aucune connectivité, NetBackup tente d'utiliser le tunnel HTTP intégré sur un serveur de médias pour envoyer la demande de certificat au serveur maître. Se reporter à "Communication entre un client NetBackup situé dans une zone démilitarisée et un serveur maître, via un tunnel HTTP" à la page 384.	Se reporter à "Déploiement de certificats sur un client qui n'a aucune connectivité avec le serveur maître" à la page 349.
Déploiement et génération de certificats pour les clients NAT	Oui. Pendant le déploiement des certificats NetBackup sur un client NAT, vous devez fournir un jeton d'autorisation, quel que soit le niveau de sécurité de déploiement de certificats défini sur le serveur maître, car le serveur maître ne peut pas résoudre le nom d'hôte sur l'adresse IP à partir de laquelle la demande est envoyée.	Pour plus d'informations sur la prise en charge des clients NAT dans NetBackup, consultez le Guide de l'administrateur NetBackup, volume I.

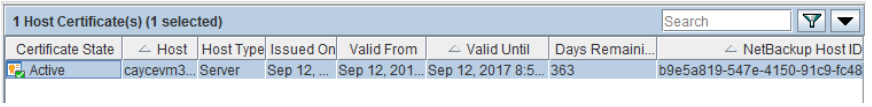
Affichage des détails de certificat basé sur l'ID d'hôte

Les détails de chaque certificat basé sur l'ID d'hôte peuvent être affichés dans la **console d'administration NetBackup** ou à l'aide de la commande `nbcertcmd`.

Pour afficher les détails du certificat dans la console d'administration NetBackup

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** > **Gestion de certificat**.

   Les détails du certificat sont affichés dans le volet droit.



2. Par défaut, les ID de l'hôte ne sont pas affichés. (Voir Tableau 15-6.)

   Pour afficher ou masquer des colonnes, cliquez avec le bouton droit de la souris dans le volet droit et sélectionnez **Colonnes > disposition**. Sélectionner les colonnes à afficher ou masquer dans la boîte de dialogue **Disposition des colonnes**.

Tableau 15-6 Détails masqués et affichés du certificat

En-tête de colonne	Description	Affiché par défaut
Etat du certificat	L'état du certificat (**Actif**, **Révoqué**, ou **Expiré**).	Oui
Hôte	Le nom de l'hôte sur lequel le certificat est émis.	Oui
Type d'hôte	Le type d'hôte (serveur ou client).	Oui
Emis le	La date et l'heure auxquels le certificat a été émis.	Oui
Valide à partir du	La date à laquelle le certificat devient valide.	Oui
Valide jusqu'au	La date jusqu'à laquelle le certificat reste valide.	Oui
Nombre de jours restants avant expiration	Nombre de jours jusqu'à l'expiration du certificat.	Oui
Version de certificat	Version du certificat basé sur l'ID d'hôte déployé sur l'hôte.	Non
ID de l'hôte NetBackup	ID unique assigné à l'hôte.	Non
Numéro de série	Spécifie le numéro de série du certificat.	Non
Motif de la révocation	La raison pour une révocation de certification, si l'administrateur a saisi une raison au moment de révocation.	Non
Date de dernière mise à jour	Date lorsque les détails du certificat ont été mis à jour.	Non

Pour afficher les détails du certificat à l'aide de la commande nbcertcmd

- Pour afficher tous les identifiants qui sont affectés à un hôte de différents serveurs maîtres, exécutez la commande suivante sur un hôte NetBackup :

  ```
  nbcertcmd -listCertDetails
  ```

À propos des niveaux de sécurité de déploiement de certificats NetBackup

Les niveaux de sécurité pour le déploiement de certificat sont spécifiques des certificats signés par l'autorité de certification NetBackup. Si le serveur Web NetBackup n'est pas configuré pour utiliser les certificats NetBackup pour les communications sécurisées, les niveaux de sécurité ne sont pas accessibles.

Le niveau de déploiement du certificat NetBackup détermine les vérifications qui sont effectuées avant que l'autorité de certification NetBackup n'émette un certificat pour un hôte NetBackup. Il détermine également la fréquence d'actualisation de la liste de révocation des certifications (CRL) NetBackup sur l'hôte.

Les certificats NetBackup sont déployés sur des hôtes pendant l'installation (une fois que l'administrateur de l'hôte confirme la signature du serveur maître) ou avec la commande `nbcertcmd`. Choisissez un niveau de déploiement correspondant aux contraintes de sécurité de votre environnement NetBackup.

Remarque : Pendant le déploiement du certificat NetBackup sur un client NAT, vous devez fournir un jeton d'autorisation, quel que soit le niveau de sécurité de déploiement de certificats défini sur le serveur maître. car le serveur maître ne peut pas résoudre le nom d'hôte sur l'adresse IP à partir de laquelle la demande est envoyée.

Pour plus d'informations sur la prise en charge de NAT dans NetBackup, consultez le Guide de l'administrateur NetBackup, volume I.

Se reporter à "À l'aide de l'utilitaire de gestion de certificat pour émettre et déployer des certificats basés sur l'ID d'hôte" à la page 330.

Se reporter à "Configuration des niveaux de sécurité de déploiement de certificats" à la page 337.

Tableau 15-7 Description des niveaux de sécurité de déploiement de certificats NetBackup

Niveau de sécurité	Description	Actualisation de la liste de révocation des certifications
Très élevé	Un jeton d'autorisation est nécessaire pour chaque nouvelle demande de certificat NetBackup. Se reporter à "Création de jetons d'autorisation" à la page 358.	La liste de révocation des certifications qui est présente sur l'hôte est actualisée toutes les heures. Se reporter à "À propos de la liste de révocations des certificats basés sur l'ID d'hôte" à la page 362.

Niveau de sécurité	Description	Actualisation de la liste de révocation des certifications
Elevé(par défaut)	Aucun jeton d'autorisation n'est requis si l'hôte est connu du serveur maître. Un hôte est considéré comme étant connu du serveur maître si l'hôte se trouve dans les entités suivantes : **1** L'hôte est répertorié pour l'une des options suivantes dans le fichier de configuration NetBackup (registre Windows ou fichier `bp.conf` sous UNIX) : ■ APP_PROXY_SERVER ■ DISK_CLIENT ■ ENTERPRISE_VAULT_REDIRECT_ALLOWED ■ MEDIA_SERVER ■ NDMP_CLIENT ■ SERVER ■ SPS_REDIRECT_ALLOWED ■ TRUSTED_MASTER ■ VM_PROXY_SERVER ■ MSDP_SERVER Pour plus d'informations sur les options de configuration de NetBackup, consultez le Guide de l'administrateur NetBackup, volume I. **2** Si l'hôte est répertorié sous un nom de client dans le fichier `altnames` (ALTNAMESDB_PATH). **3** L'hôte apparaît dans la base de données EMM du serveur maître. **4** Au moins une image de catalogue du client existe. L'image ne doit pas être antérieure à 6 mois. **5** Le client figure dans au moins une politique de sauvegarde. **6** Le client est un client hérité. Il s'agit d'un client qui a été ajouté à l'aide des propriétés d'hôte **Attributs client**. Se reporter à "Création de jetons d'autorisation" à la page 358.	La liste de révocation des certifications présente sur l'hôte est actualisée toutes les 4 heures.
Moyen	Les certificats sont émis sans jeton d'autorisation si le serveur maître peut résoudre le nom d'hôte sur l'adresse IP d'où la demande provient.	La liste de révocation des certifications présente sur l'hôte est actualisée toutes les 8 heures.

Configuration des niveaux de sécurité de déploiement de certificats

Utilisez la **console d'administration NetBackup** ou la commande `nbcertcmd` pour configurer le niveau de sécurité de déploiement du certificat dans le domaine NetBackup.

Ces niveaux de sécurité sont propres aux certificats signés par l'autorité de certification NetBackup.

Pour configurer le niveau de déploiement du certificat à l'aide de la console d'administration NetBackup

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** et exécutez l'une des opérations suivantes :
   - Accédez à **Gestion des certificats**. Dans le menu **Actions**, sélectionnez **Configurer les paramètres de sécurité**.
   - Accédez à **Paramètres de sécurité globaux**.
2. Dans l'écran **Niveau de sécurité pour le déploiement de certificat**, faites glisser l'indicateur sur l'un des trois niveaux : **Très haut**, **Haut** (par défaut) ou **Moyen**.
3. Cliquez sur **OK**.

Pour configurer le niveau de déploiement de certificat à l'aide de la ligne de commande

1. L'administrateur du serveur maître doit être connecté au service de gestion Web de NetBackup pour exécuter cette tâche. Pour vous connecter, utilisez la commande suivante :

   ```
   bpnbat -login -logintype WEB
   ```

   Se reporter à "Conditions requises de connexion web pour les options de commande nbcertcmd" à la page 329.
2. Exécutez la commande suivante pour afficher le niveau de sécurité actuel :

   ```
   nbcertcmd -getSecConfig -certDeployLevel -server
   master_server_name
   ```
3. Exécutez la commande suivante pour modifier le niveau de sécurité :

   ```
   nbcertcmd -setSecConfig -certDeployLevel 0-2 -server
   master_server_name
   ```

   Où `0` est Très haut, `1` est Haut (par défaut) et `2` est Moyen.

Pour plus d'informations sur `nbcertcmd`, consultez le *Guide de référence des commandes NetBackup*.

Déploiement automatique du certificat basé sur l'ID de l'hôte

Un certificat basé sur l'ID d'hôte est automatiquement déployé sur le serveur maître NetBackup en tant qu'élément de l'installation de NetBackup.

Ces certificats sont déployés sur d'autres hôtes NetBackup (après la vérification de la signature) selon le niveau de déploiement de certificat.

L'autorité de certification (CA) sur le serveur maître NetBackup peut accepter ou rejeter la demande de certificat, selon le niveau de déploiement de certificat et la capacité du serveur maître à vérifier les informations d'hôte.

Vous pouvez vérifier la liste des certificats déployés sur un hôte NetBackup à l'aide de la commande suivante :

```
nbcertcmd -listCertDetails
```

Lorsqu'une demande de certificat est rejetée, l'administrateur de l'hôte doit demander à l'administrateur NetBackup de générer et partager un jeton d'autorisation pour déployer le certificat manuellement.

Se reporter à "Création de jetons d'autorisation" à la page 358.

Se reporter à "À propos des niveaux de sécurité de déploiement de certificats NetBackup" à la page 334.

Déploiement des certificats basés sur l'ID de l'hôte

Selon le niveau de sécurité de déploiement de certificat, un hôte non maître peut nécessiter un jeton d'autorisation pour pouvoir obtenir un certificat basé sur l'ID d'hôte de l'autorité de certification (serveur maître). Lorsque les certificats ne sont pas déployés automatiquement, ils doivent être déployés manuellement par l'administrateur sur un hôte NetBackup à l'aide de la commande `nbcertcmd`.

La rubrique suivante décrit les niveaux de déploiement et indique si le niveau requiert un jeton d'autorisation.

Se reporter à "À propos des niveaux de sécurité de déploiement de certificats NetBackup" à la page 334.

Déploiement lorsqu'aucun jeton n'est nécessaire

Utilisez la procédure suivante lorsque le niveau de sécurité est tel qu'un administrateur d'hôte peut déployer un certificat sur un hôte non maître sans nécessiter de jeton d'autorisation.

Pour générer et déployer un certificat basé sur l'ID d'hôte lorsqu'aucun jeton n'est nécessaire.

1. L'administrateur de l'hôte exécute la commande suivante sur l'hôte non maître pour s'assurer que le serveur maître peut être approuvé :

   ```
   nbcertcmd -getCACertificate
   ```

   Se reporter à "Installation de la confiance avec le serveur maître (Autorité de certification)" à la page 343.

2. Exécutez la commande suivante sur l'hôte non maître :

   ```
   nbcertcmd -getCertificate
   ```

   Remarque : Pour communiquer avec plusieurs domaines NetBackup, l'administrateur de l'hôte doit demander un certificat à chaque serveur maître à l'aide de l'option `-server`.

   Exécutez la commande suivante pour obtenir un certificat à partir d'un serveur maître spécifique :

   ```
   nbcertcmd -getCertificate -server master_server_name
   ```

3. Pour vérifier que le certificat est déployé sur l'hôte, exécutez la commande suivante :

   ```
   nbcertcmd -listCertDetails
   ```

Déploiement lorsqu'un jeton est nécessaire

Utilisez la procédure suivante lorsque le niveau de sécurité est tel qu'un hôte requiert un jeton d'autorisation pour pouvoir déployer un certificat basé sur l'ID d'hôte à partir de l'autorité de certification.

Pour générer et déployer un certificat hôte basé sur l'ID d'hôte lorsqu'un jeton est requis

1. L'administrateur de l'hôte doit avoir obtenu la valeur de jeton d'autorisation de l'autorité de certification avant de poursuivre. Le jeton peut être transmis à l'administrateur par courrier électronique, par fichier ou verbalement, selon les diverses directives de sécurité de l'environnement.

2. Exécutez la commande suivante sur l'hôte de serveur non-maître pour établir si le serveur maître peut être approuvé :

   ```
   nbcertcmd -getCACertificate
   ```

   Se reporter à "Installation de la confiance avec le serveur maître (Autorité de certification)" à la page 343.

3 Exécutez la commande suivante sur l'hôte non maître non et entrez le jeton lorsque vous y êtes invité :

```
nbcertcmd -getCertificate -token
```

Remarque : Pour communiquer avec plusieurs domaines NetBackup, l'administrateur de l'hôte doit demander un certificat à chaque serveur maître à l'aide de l'option `-server`.

Si l'administrateur a obtenu le jeton dans un fichier, entrez ce qui suit :

```
nbcertcmd -getCertificate -file authorization_token_file
```

4 Pour vérifier que le certificat est déployé sur l'hôte, exécutez la commande suivante :

```
nbcertcmd -listCertDetails
```

Utilisez l'option `-cluster` pour afficher les certificats de cluster.

Déploiement asynchrone de certificats basés sur l'ID de l'hôte

Des certificats basés sur l'ID de l'hôte sont automatiquement déployés sur les hôtes NetBackup pendant l'installation ou la mise à niveau. Pour que le certificat soit déployé automatiquement, l'hôte sur lequel le déployer doit être connecté au serveur maître.

Dans certains scénarios, vous pouvez créer, signer et déployer des certificats basés sur l'ID de l'hôte de façon asynchrone, l'hôte et le serveur maître n'ayant pas besoin d'être connectés au moment du déploiement.

Déploiement d'un certificat basé sur l'ID de l'hôte de façon asynchrone

1. Cette commande peut être exécutée seulement par l'administrateur de l'hôte.

   Créez une demande de signature de certificat. Exécutez la commande suivante sur l'hôte de serveur non maître sur lequel déployer le certificat :

   ```
   nbcertcmd -createCertRequest -requestFile request_file_name
   -server master_server_name
   ```

   Copiez éventuellement le fichier de la demande de signature de certificat (CSR) vers un hôte NetBackup.

2. Obtenez un certificat signé à partir du serveur maître sur l'hôte. Un jeton d'autorisation est requis. Si l'hôte dispose déjà d'un certificat, un jeton de renouvellement est requis.

   Sur l'hôte, exécutez la commande suivante :

   ```
   nbcertcmd -signCertificate -requestFile request_file_name
   -certificateFile certificate_file_name -token
   ```

   Remarque : assurez-vous d'utiliser l'option `-signCertificate` sur un hôte doté de la même version de NetBackup que celle utilisée pour générer la demande de signature de certificat ou d'une version ultérieure.

3. Copiez le certificat signé créé à l'étape 2 et fournissez-le à l'administrateur de l'hôte.

4. Cette commande peut être exécutée seulement par l'administrateur de l'hôte.

   Pour déployer le certificat signé sur l'hôte, exécutez la commande suivante sur le client :

   ```
   nbcertcmd -deployCertificate -certificateFile
   certificate_file_name
   ```

Implication du décalage d'horaire sur la validité du certificat

Quand un serveur maître émet un certificat, il détermine combien de temps le certificat sera valide pour l'hôte. Le serveur maître définit la période de validité du certificat sur base de sa propre heure, enregistrant deux horodatages : **Pas avant** et **Pas après**. Le certificat est uniquement valide entre ces deux horodatages.

L'horloge sur le serveur maître et l'horloge sur l'hôte qui recevra le certificat doivent être synchronisées afin que le certificat soit valide pendant toute la période prévue par les horodatages.

Les hôtes peuvent résider dans différents fuseaux horaires, tant que l'horloge sur chaque hôte est réglée sur l'heure correcte pour le fuseau horaire de cet hôte. En règle générale, il est recommandé d'utiliser un service tel que le protocole NTP (Network Time Protocol) afin que toutes les horloges sur tous les hôtes dans le domaine NetBackup restent automatiquement synchronisées.

Si les horloges ne sont pas synchronisées, la différence peut entraîner les conséquences suivantes :

- Si l'horloge de l'hôte est en avance sur le serveur maître, la période de validité du certificat sera inférieure à celle prévue sur cet hôte en particulier. Si la différence est extrême et que les horloges varient en plus de la période de validité du certificat, il est possible que si le serveur maître a émis un nouveau certificat, il pourrait être traité comme expiré.
- Si l'horloge de l'hôte retarde par rapport à celle du serveur maître, un nouveau certificat émis par le serveur maître pourrait être considéré comme inutilisable par l'hôte parce que l'hôte considère le certificat comme n'étant plus valide.

Pour déterminer si l'horloge du serveur maître et l'horloge de l'hôte sont synchronisées

1. Exécutez la commande suivante sur l'hôte pour déterminer si l'horloge de l'hôte est synchronisée avec l'horloge du serveur maître :

   ```
   nbcertcmd -checkClockSkew -server master_server_name
   ```

2. La commande renvoie l'un des résultats suivants :

   - Si les deux horloges sont synchronisées, il s'affiche ce qui suit :

     ```
     The current host clock is in sync with the master server.
     ```

   - Si l'hôte actuel retarde par rapport au serveur maître, la commande signale la différence en secondes :

     ```
     The current host clock is behind the master server by 36
     seconds(s).
     ```

   - Si l'hôte actuel avance par rapport au serveur maître, la commande signale la différence en secondes :

     ```
     The current host clock is ahead of the master server by 86363
     second(s).
     ```

   - Si la commande est exécutée sur le serveur maître, la commande ignore la vérification et affiche les éléments suivants :

     ```
     Specified server is same as the current host. Clock skew check
     is skipped.
     ```

   Si le décalage d'horaire sur l'hôte pose un problème avec la période de validité du certificat, effectuez les mesures correctives nécessaires.

Installation de la confiance avec le serveur maître (Autorité de certification)

Chaque hôte NetBackup doit commencer par faire confiance au serveur maître NetBackup, qui agit en tant qu'Autorité de certification (AC). La relation de confiance est essentielle pour que l'hôte puisse demander un certificat basé sur l'ID d'hôte. Le certificat de l'autorité de certification peut être utilisé pour authentifier d'autres hôtes du domaine et est enregistré dans le magasin d'approbation de chaque hôte. L'établissement de la confiance implique de demander un certificat au serveur maître.

Se reporter à "Déploiement automatique du certificat basé sur l'ID de l'hôte" à la page 338.

Ajout d'un certificat de l'autorité de certification au magasin d'approbation d'un hôte

Exécutez la commande `nbcertcmd -listCACertDetails` pour consulter la liste des certificats de l'autorité de certification qui se trouvent dans le magasin d'approbation de l'hôte. Le résultat de la commande affiche tous les serveurs maîtres auxquels l'hôte fait déjà confiance.

Pour établir la confiance avec le serveur maître (AC)

1. L'administrateur de l'hôte doit avoir la signature de certificat racine qui a été communiquée via une source authentique. La source est le plus souvent l'administrateur de serveur maître, qui a communiqué la signature par courrier électronique, par fichier ou sur un site Web interne. La rubrique suivante décrit ce processus :

   Se reporter à "Recherche et communication de la signature de l'autorité de certification" à la page 345.

2. À partir de l'hôte NetBackup, exécutez la commande suivante :

   ```
   nbcertcmd -getCACertificate -server master_server_name
   ```

3 Dans le résultat de confirmation, entrez **o** pour continuer.

Par exemple :

```
nbcertcmd -getCACertificate -server master1
Authenticity of root certificate cannot be established.
The SHA1 fingerprint of root certificate is B8:2B:91:E1:4E:78:D2:
25:86:4C:29:C5:92:16:00:8D:E8:2F:33:DD.
```

Remarque : La signature qui est affichée doit correspondre à la signature de certificat racine que l'administrateur de l'hôte a reçu de l'administrateur du serveur maître. Entrez **o** pour donner votre accord pour ajouter le certificat de l'Autorité de certification au magasin d'approbation de l'hôte.

```
Are you sure you want to continue using this certificate ? (y/n): y
The validation of root certificate fingerprint is successful.
CA certificate stored successfully.
```

4 L'administrateur effectue ensuite la tâche suivante :

Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.

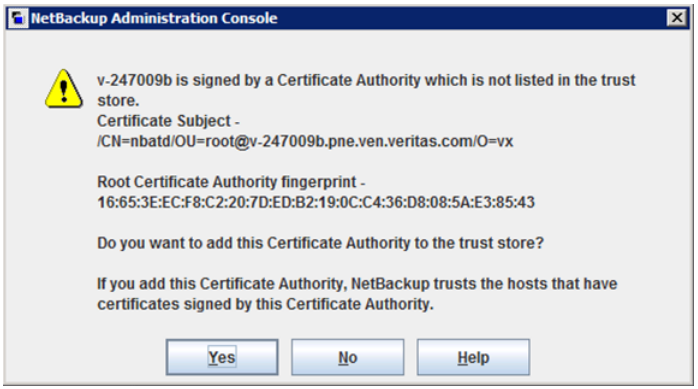
Pour plus d'informations sur cette commande, consultez le Guide de référence des commandes NetBackup.

Ajout d'un certificat de l'autorité de certification par message dans la console d'administration NetBackup

La **console d'administration NetBackup** et les interfaces utilisateur **Sauvegarde, archivage et restauration** communiquent avec les hôtes NetBackup (serveur maître, serveur de médias ou client) via un canal sécurisé. NetBackup sécurise ce canal à l'aide d'un certificat de sécurité basé sur l'ID d'hôte ou le nom d'hôte NetBackup émis par l'autorité de certification NetBackup.

Figure 15-1 s'affiche dans la **console d'administration NetBackup** dans le cas suivant : un utilisateur exécute la **console d'administration NetBackup** sur un hôte NetBackup. L'utilisateur tente de se connecter à un autre hôte NetBackup (hôte cible) à l'aide de la **console d'administration NetBackup**. Cependant, l'autorité de certification qui a émis le certificat de sécurité pour l'hôte cible ne figure pas dans le magasin d'approbation de l'hôte sur lequel l'utilisateur a lancé la console.

Figure 15-1 Message recherchant s'il faut ajouter une autorité de certification au magasin d'approbation



Pour vérifier la signature de l'autorité de certification affichée dans la boîte de dialogue, consultez la rubrique suivante :

Se reporter à "Recherche et communication de la signature de l'autorité de certification" à la page 345.

Si l'utilisateur sélectionne **Oui** dans ce message, l'autorité de certification est ajoutée au magasin d'approbation de l'hôte sur lequel s'exécute la console. Cet hôte approuve ensuite tous les hôtes qui disposent d'un certificat signé par l'autorité de certification qui est répertoriée dans le message.

Recherche et communication de la signature de l'autorité de certification

L'administrateur du serveur maître doit trouver la signature du certificat de l'autorité de certification et la communiquer à l'administrateur de l'hôte individuel de sorte que l'hôte puisse ajouter le certificat de l'autorité de certification à son magasin d'approbation.

Les signatures SHA-1 et SHA-256 sont prises en charge.

Pour trouver la signature du certificat de l'autorité de certification

1 L'administrateur du serveur maître peut trouver la signature à l'aide de la **console d'administration NetBackup** ou de la ligne de commande :

Utilisation de la **console d'administration NetBackup** :

- Développez **Gestion de la sécurité > Gestion des certificats**.
- Dans le menu **Actions**, sélectionnez **Afficher l'autorité de certification**. La boîte de dialogue **Détails de l'autorité de certification** apparaît.

- Les informations suivantes sont affichées :

Nom de l'objet	Identifie le certificat pour le serveur maître souhaité.
Date de début	Date d'activation du certificat.
Date d'expiration	Date d'expiration du certificat.
Signature SHA-1	Valeur de hachage du certificat calculée à l'aide de l'algorithme SHA-1.
Signature SHA-256	Valeur de hachage du certificat calculée à l'aide de l'algorithme SHA-256.
Copier	Utilisez cette option pour aider l'administrateur à communiquer la signature SHA-1 ou SHA-256 à l'administrateur de l'hôte.

À l'aide de la ligne de commande :

- Exécutez la commande suivante sur le serveur maître pour afficher la signature de certificat racine :

  ```
  nbcertcmd -listCACertDetails
  ```

Si plusieurs certificats de l'autorité de certification sont affichés, utilisez le **Nom de l'objet**.

2 L'administrateur du serveur maître communique la signature à l'administrateur de l'hôte par courrier électronique, par fichier ou via un site Web interne.

L'administrateur de l'hôte utilise la signature pour vérifier la signature qui s'affiche lorsque l'hôte exécute `nbcertcmd -getCACertificate`. Cette opération permet de vérifier l'authenticité du certificat de l'autorité de certification.

Utilisation de la commande vssat pour afficher la signature de certificat de l'autorité de certification

La commande `vssat` peut également être utilisée pour afficher la signature de certificat de l'autorité de certification. Utilisez `vssat` avec les options suivantes :

```
vssat showcred -p nbatd
```

Notez cependant les différences suivantes entre l'utilisation de `nbcertcmd -listCACertDetails` et l'utilisation de `vssat` :

- `vssat`affiche la signature sous forme de hachage et n'inclut pas les séparateurs de deux-points.
- Si l'hôte fait confiance à plusieurs autorités de certification, la commande `nbcertcmd` affiche tous les certificats d'autorité de certification. Le **Nom d'objet** affiche l'identité de l'autorité de certification.

Forcer ou remplacer le déploiement d'un certificat

Dans certaines situations, il peut s'avérer nécessaire d'utiliser l'option `-force` avec la commande `nbcertcmd -getCertificate`. Par exemple, pour forcer le déploiement d'un certificat sur un hôte ou pour remplacer les informations de certificat basées sur l'ID d'hôte existantes et récupérer un nouveau certificat.

Forcer le déploiement d'un certificat

Un hôte peut déjà avoir un certificat basé sur l'ID d'hôte, mais il a besoin de remplacer l'ancien certificat par un nouveau. Cette opération est nécessaire, par exemple, lorsqu'un serveur maître est remplacé par un nouveau serveur. Les clients ayant l'ancien certificat sur l'ancien serveur, lorsque la commande `nbcertcmd -getCertificate` est exécutée sur les clients, elle échoue avec l'erreur suivante :

```
Certificate already exists for the server.
```

Utilisez la procédure suivante pour remplacer les informations de certificat basées sur l'ID d'hôte existantes et récupérer un nouveau certificat.

Pour forcer le déploiement d'un certificat sur un hôte

- L'administrateur de l'hôte exécute la commande suivante sur l'hôte de serveur non maître :

  ```
  nbcertcmd -getCertificate -server master_server_name -force
  ```

  - Selon le paramètre de sécurité sur le serveur maître, il est possible qu'un jeton doive également être spécifié.
    Se reporter à "Création de jetons d'autorisation" à la page 358.
  - Utilisez l'option `-cluster` pour déployer un certificat de cluster.

Remplacer les informations de certificat basées sur l'ID d'hôte existantes et récupérer un nouveau certificat

Un hôte peut avoir émis un certificat, mais au fil du temps le certificat a été endommagé ou le fichier du certificat a été supprimé.

L'administrateur de l'hôte du serveur non maître peut exécuter la commande suivante pour confirmer l'état du certificat :

```
nbcertcmd -listCertDetails
```

- Si le certificat est endommagé, la commande échoue avec l'erreur suivante :
  `Certificate could not be read from the local certificate store.`
- Si aucun détail du certificat ne s'affiche, le certificat n'est pas disponible.

Utilisez la procédure suivante pour remplacer les informations du certificat basées sur l'ID d'hôte existantes et récupérer un nouveau certificat.

Pour récupérer un nouveau certificat basé sur l'ID d'hôte

- L'administrateur de l'hôte exécute la commande suivante sur l'hôte de serveur non maître :

  ```
  nbcertcmd -getCertificate -force
  ```

  - Selon le paramètre de sécurité sur le serveur maître, il est possible qu'un jeton doive également être spécifié.
    Se reporter à "Création de jetons d'autorisation" à la page 358.
  - Utilisez l'option `-cluster` pour déployer un certificat de cluster.

Conservation des certificats basés sur l'ID d'hôte lors de la réinstallation de NetBackup sur des hôtes non maîtres

Les administrateurs peuvent souhaiter désinstaller NetBackup d'un hôte, puis effectuer une nouvelle installation sur le même hôte. Consultez la procédure suivante pour obtenir des instructions sur la façon de conserver l'identité d'un hôte dans le processus de désinstallation/réinstallation.

Pour conserver des certificats basés sur l'ID d'hôte lors de la réinstallation de NetBackup

1. Arrêtez tous les services NetBackup sur l'hôte.
2. Sauvegardez les répertoires suivants :

   Windows :

   Install_path\NetBackup\var\VxSS

   Install_path\NetBackup\var\webtruststore

   UNIX :

   /usr/openv/var/vxss

   /usr/openv/var/webtruststore
3. Lorsque NetBackup Cluster Server est utilisé, sauvegardez également les répertoires suivants :

   Shared_disk\var\global\vxss

   Shared_disk\var\global\webtruststore
4. Réinstallez NetBackup sur l'hôte.
5. Restaurez les données qui ont été sauvegardées à l'étape 2 et à l'étape 3.

Déploiement de certificats sur un client qui n'a aucune connectivité avec le serveur maître

NetBackup peut détecter si un hôte dispose d'une connectivité avec le serveur maître. S'il n'existe aucune connectivité, NetBackup tente automatiquement d'utiliser le tunnel HTTP intégré sur un serveur de médias pour envoyer la demande de connexion au serveur maître.

Si NetBackup ne peut pas automatiquement détecter la connectivité de l'hôte avec le serveur maître ou trouver un serveur de médias approprié pour envoyer la demande de connexion, vous devez configurer manuellement les options de tunnel HTTP.

Se reporter à "Communication entre un client NetBackup situé dans une zone démilitarisée et un serveur maître, via un tunnel HTTP" à la page 384.

Pour déployer un certificat sur un client qui n'a aucune connectivité avec le serveur maître, consultez la rubrique suivante :

Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.

Remarque : La demande est envoyée par l'intermédiaire d'un hôte différent, le serveur maître ne peut pas valider l'authenticité de la demande de certificat, et, par conséquent, un jeton d'autorisation est nécessaire.

À propos de l'expiration et du renouvellement des certificats basés sur l'ID d'hôte

Les certificats basés sur l'ID d'hôte NetBackup expirent un an après leur date d'émission. Ils sont automatiquement renouvelés 180 jours avant la date d'expiration. Une demande de renouvellement de certificat est envoyée périodiquement jusqu'à ce qu'un certificat soit renouvelé avec succès. Le renouvellement automatique garantit la transparence du processus de renouvellement pour les utilisateurs.

Remarque : Vous pouvez désactiver le renouvellement automatique des certificats basés sur l'ID d'hôte en utilisant le paramètre `DISABLE_CERT_AUTO_RENEW` du fichier de configuration NetBackup (registre Windows ou fichier `bp.conf` sous UNIX).

Pour plus d'informations, reportez-vous au *Guide de l'administrateur NetBackup, Volume I*.

La demande de renouvellement est toujours authentifiée à l'aide du certificat existant. Par conséquent, le processus de renouvellement ne requiert pas l'utilisation d'un jeton d'autorisation, quel que soit le niveau de sécurité de déploiement du certificat.

Si le certificat existant n'a pas expiré, l'administrateur de l'hôte peut lancer une demande de renouvellement manuelle, comme décrit dans la procédure suivante.

Pour renouveler manuellement un certificat basé sur l'ID d'hôte

- L'administrateur de l'hôte exécute la commande suivante sur l'hôte de serveur non maître :

  ```
  nbcertcmd -renewCertificate
  ```

  - Les certificats correspondant aux domaines NetBackup autres que le domaine principal peuvent être renouvelés manuellement en spécifiant l'option `-server`.
  - Utilisez l'option `-cluster` pour renouveler le certificat du cluster du serveur NetBackup en cluster.

Dans un scénario où le certificat a expiré, l'administrateur de l'hôte doit renouveler manuellement le certificat.

Se reporter à "Renouvellement des certificats basés sur l'ID d'hôte" à la page 353.

Suppression des certificats sensibles et des clés des serveurs de médias et des clients

Dans le processus de clonage, utilisez la commande suivante pour supprimer certains certificats et certaines clés sensibles des serveurs de médias NetBackup et des clients dans les scénarios suivants :

- Exécutez la commande sur la machine virtuelle clonée à partir d'un hôte NetBackup actif.
- Exécutez la commande avant de créer une image gold d'une machine virtuelle pour le clonage.

```
nbcertcmd -deleteAllCertificates
```

Remarque : Cette commande est uniquement autorisée sur les serveurs de médias et les clients. La commande n'est pas autorisée sur les serveurs maîtres.

Cette opération supprime ou tronque les informations sensibles appropriées (certificats et clés) des emplacements suivants :

Windows :

- `C:\Program Files\Veritas\NetBackup\var\VxSS\certmapinfo.json`
- `C:\Program Files\Veritas\NetBackup\var\VxSS\credentials\<certificate>`

  Par exemple :

  `C:\Program Files\Veritas\NetBackup\var\VxSS\credentials\6d92d4dd-ed2d-43de-adb1-bf333aa2cc3c`
- `C:\Program Files\Veritas\NetBackup\var\VxSS\credentials\keystore\PrivKeyFile.pem` (tronqué)
- `C:\Program Files\Veritas\NetBackup\var\VxSS\at\systemprofile\certstore\<certificate>`

  Par exemple :

  `C:\Program Files\Veritas\NetBackup\var\VxSS\at\systemprofile\certstore\9345b05e-lilycl2nb!1556!nbatd!1556.0`
- `C:\Program Files\Veritas\NetBackup\var\VxSS\at\systemprofile\certstore\keystore\PrivKeyFile.pem` (tronqué)
- `C:\Program Files\Veritas\NetBackup\var\VxSS\at\systemprofile\certstore\keystore\PubKeyFile.pem`

UNIX :

- `/usr/openv/var/vxss/certmapinfo.json`
- `/usr/openv/var/vxss/credentials/<certificate>`
  Par exemple :
  `/usr/openv/var/vxss/credentials/f4f72ef3-2cfc-42a4-ab5a-65fd09e8b63e`
- `/usr/openv/var/vxss/credentials/keystore/PrivKeyFile.pem` (shredded)
- `/var/vxss/at/root/.VRTSat/profile/certstore/<certificate>`
- `/var/vxss/at/root/.VRTSat/profile/certstore/keystore/PubKeyFile.pem`
- `/var/vxss/at/root/.VRTSat/profile/certstore/keystore/PrivKeyFile.pem` (shredded)

Nettoyage des informations de certificat basé sur un ID d'hôte à partir d'un hôte avant de cloner une machine virtuelle

Le clonage d'une machine virtuelle peut entraîner un risque de vol d'identité. Les hôtes multiples ne doivent pas avoir la même paire de clés. Cette procédure garantit que chaque copie de l'hôte obtient une paire de clés unique et une identité.

Effectuez la procédure suivante avant de cloner une machine virtuelle (ou avant de créer une bonne image d'un ordinateur pour le clonage) s'il s'agit d'une opération unique.

Pour nettoyer les informations du certificat basé sur l'ID d'hôte à partir d'un hôte avant le clonage

1. Arrêtez tous les services NetBackup sur l'hôte.
2. Supprimez tous les fichiers et répertoires à partir des emplacements suivants :

   Windows :

   `Install_path\NetBackup\var\VxSS\at\*`

   `Install_path\NetBackup\var\VxSS\credentials\*`

   `Install_path\NetBackup\var\webtruststore\*`

   UNIX :

   `/usr/openv/var/vxss/at/*`

   `/usr/openv/var/vxss/credentials/*`

   `/usr/openv/var/webtruststore/*`

3. Supprimez le fichier suivant :

   Sous Windows : *Install_path*\NetBackup\var\VxSS\certmapinfo.json

   Sous UNIX : /usr/openv/var/vxss/certmapinfo.json

4. À l'emplacement d'utilisation de NetBackup, effectuez les étapes suivantes en plus :

5. Supprimez tous les fichiers et répertoires à partir des emplacements suivants :

   Shared_disk\var\global\vxss\at*

   Shared_disk\var\global\vxss\credentials*

   Shared_disk\var\global\webtruststore*

6. Supprimez le fichier suivant :

   Shared_disk\var\global\vxss\certmapinfo.json

7. Procédez au clonage de la machine virtuelle.

Renouvellement des certificats basés sur l'ID d'hôte

Un certificat doit être renouvelé dans un des cas suivants :

- Le certificat a été révoqué et vous déterminez par la suite que cet hôte est à nouveau digne de confiance.
- Le certificat a expiré.
- NetBackup a été réinstallé sur l'hôte sur lequel un certificat a déjà été émis.
- Le nom de l'hôte a été modifié.
- La paire de clés pour l'hôte a été modifiée.

Le renouvellement d'un certificat permet d'empêcher des utilisateurs malveillants d'usurper l'identité d'un hôte NetBackup existant déjà enregistré sur le serveur maître NetBackup. Dans la plupart des cas, un jeton de renouvellement est requis pour le renouvellement de certificat.

- Le renouvellement d'un certificat basé sur l'ID d'hôte pour un hôte NetBackup est différent du déploiement initial du certificat. Utilisez la procédure suivante pour renouveler un certificat.
  Se reporter à "Création d'un jeton de renouvellement" à la page 354.
- Une fois qu'un jeton de renouvellement est obtenu, le processus de renouvellement de certificat est semblable au déploiement d'un certificat manuel à l'aide d'un jeton d'autorisation.
  Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.

Lorsque le serveur maître reçoit une demande de renouvellement de certificat, il révoque d'abord tous les certificats précédemment valides pour cet hôte et génère un nouveau certificat, si nécessaire.

Création d'un jeton de renouvellement

Un certificat basé sur l'ID d'hôte peut être renouvelé si l'hôte du serveur non maître est déjà enregistré avec le serveur maître mais que son certificat basé sur l'ID d'hôte n'est plus valide. Par exemple, un certificat n'est pas valide lorsqu'il a expiré, qu'il est révoqué ou est égaré.

Un jeton de renouvellement est un type de jeton qui peut être utilisé pour renouveler un certificat. C'est un type spécial de jeton, car il conserve le même ID d'hôte en tant que certificat d'origine. Puisqu'un jeton de renouvellement est lié à un hôte spécifique, le jeton ne peut pas être utilisé pour demander des certificats pour des hôtes supplémentaires.

Pour créer un jeton de renouvellement à l'aide de la console d'administration NetBackup

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité**.
2. Sélectionnez le nœud **Gestion des certificats** ou **Gestion des hôtes**.
3. Dans le volet droit, sélectionnez l'hôte qui requiert un jeton de renouvellement.
4. A partir du menu **Actions**, sélectionnez **Générer renouvellement de jeton**.
5. Dans la boîte de dialogue **Créer renouvellement de jeton**, entrez un nom pour le jeton.
6. Sélectionnez une date de validité du jeton à partir de l'option **Valide jusqu'à**.
7. Dans le champ **Raison**, entrez une raison pour le jeton de renouvellement. La raison s'affiche dans le journal en tant qu'événement d'audit.
8. Cliquez sur **Créer**.

9 Le jeton de renouvellement apparaît dans une boîte de dialogue. Sélectionnez **Copier** pour enregistrer la valeur du jeton dans le presse-papiers.

10 Transmettez la valeur du jeton à l'administrateur de l'hôte de serveur non-maître. La manière dont le jeton est transmis dépend de divers facteurs de sécurité dans l'environnement. Le jeton peut être transmis par courrier électronique, par fichier ou verbalement.

L'administrateur de l'hôte de serveur non maître déploie le jeton pour obtenir un autre certificat basé sur l'ID d'hôte. Consultez la rubrique suivante pour obtenir des instructions :

Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.

Pour créer un jeton de renouvellement à l'aide de la commande nbcertcmd

1 L'administrateur du serveur maître doit être connecté au service de gestion Web de NetBackup pour exécuter cette tâche. Utilisez la commande suivante pour la connexion :

```
bpnbat -login -logintype WEB
```

Se reporter à "Conditions requises de connexion web pour les options de commande nbcertcmd" à la page 329.

2 Exécutez une des commandes suivantes sur le serveur maître:

Utilisez le nom d'hôte pour lequel le certificat doit être renouvelé :

```
nbcertcmd -createToken -name token_name -reissue -host host_name
```

Remarque : Vous devez fournir le nom principal de l'hôte pour lequel vous souhaitez renouveler le certificat. Si vous ne spécifiez aucun des mappages d'ID d'hôte vers le nom d'hôte qui sont ajoutés pour l'hôte, le certificat ne peut pas être renouvelé.

Utilisez l'ID d'hôte pour lequel le certificat doit être renouvelé :

```
nbcertcmd -createToken -name token_name -reissue -hostId host_id
```

Des paramètres supplémentaires peuvent être utilisés pour indiquer la durée de validité et la raison de la création.

Pour plus d'informations sur la commande `nbcertcmd`, consultez le Guide de référence des commandes NetBackup.

Étapes supplémentaires pour la demande d'un certificat pour un hôte NetBackup renommé

En plus du renouvellement d'un jeton, les étapes suivantes sont requises pour demander un certificat pour un hôte NetBackup renommé.

Pour demander un certificat pour un hôte après un changement de nom d'hôte

1. L'administrateur NetBackup du serveur maître génère un jeton de renouvellement pour l'hôte NetBackup renommé.
2. Ajoutez le nouveau nom d'hôte comme l'un des mappages approuvés d'ID d'hôte vers le nom d'hôte à l'aide de la **console d'administration NetBackup**.

   Se reporter à "Ajout de mappages d'ID d'hôte vers le nom d'hôte" à la page 299.

   Vous pouvez également utiliser l'option de l'interface de ligne de commande `nbhostmgmt -add`.

   Pour plus d'informations sur la commande, consultez le Guide de référence des commandes NetBackup.
3. L'administrateur NetBackup doit révoquer le certificat basé sur l'ID d'hôte pour l'hôte renommé.

   Se reporter à "Révoquer un certificat basé sur l'ID d'hôte" à la page 367.

   Remarque : Une fois que le certificat est révoqué, l'hôte ne peut plus communiquer avec le service de NetBackup Web Management Console (`nbwmc`). Lorsque l'hôte obtient un nouveau certificat à l'aide du jeton de renouvellement, il peut à nouveau communiquer avec `nbwmc`.
4. Une fois que le certificat est révoqué, l'administrateur de l'hôte du serveur non-maître doit utiliser le jeton de renouvellement pour obtenir un certificat pour l'hôte renommé.

   Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.

Modification de la paire de clés pour un hôte

Envisagez de modifier une paire de clés uniquement si une clé est compromise ou fuite. Modification des résultats d'une paire de clés dans un nouveau certificat basé sur l'ID d'hôte et un nouveau certificat basé sur le nom d'hôte.

La procédure suivante décrit la modification d'une paire de clés pour un hôte et l'obtention d'un nouveau certificat à l'aide de la nouvelle paire de clés.

N'effectuez pas la procédure sur serveur maître, uniquement sur un hôte de serveur non-maître.

Pour modifier une paire de clés pour un hôte

1. L'administrateur de l'hôte NetBackup sauvegarde les répertoires suivants :

   Windows : `Install_path\NetBackup\var\VxSS\at\systemprofile`

   UNIX : `/usr/openv/var/vxss/at/root`

2. L'administrateur de l'hôte NetBackup supprime le répertoire de l'hôte.
3. Redémarrez les services NetBackup sur l'hôte.
4. L'administrateur de serveur maître effectue les étapes suivantes :
   - Connectez-vous au service de gestion web NetBackup :

     ```
     bpnbat -login -logintype WEB
     ```

     Se reporter à "Conditions requises de connexion web pour les options de commande nbcertcmd" à la page 329.
   - Révoquez le certificat basé sur l'ID d'hôte :

     ```
     nbcertcmd -revokeCertificate -host host_name
     ```
   - Générez un jeton de renouvellement pour l'hôte NetBackup sur lequel la paire de clés doit être modifiée.
     Se reporter à "Création d'un jeton de renouvellement" à la page 354.
   - Déployez un nouveau certificat basé sur le nom d'hôte :

     ```
     bpnbaz –ProvisionCert host_name
     ```
5. L'administrateur d'hôte NetBackup utilise le jeton de renouvellement pour déployer un nouveau certificat basé sur l'ID d'hôte avec une paire de clés mise à jour.

   Pour entrer le jeton directement, utilisez la commande suivante :

   ```
   nbcertcmd -getCertificate -force -token
   ```

   Utilisez la commande suivante si le jeton est dans un fichier :

   ```
   nbcertcmd -getCertificate -force -file /directory/token_file
   ```
6. Si l'hôte a plus d'un serveur maître, répétez le début du processus à l'étape 4 pour chaque serveur maître.
7. Redémarrez les services NetBackup sur l'hôte NetBackup où la clé a été modifiée.

À propos de la gestion des jetons pour les certificats basés sur l'ID d'hôte

Les administrateurs du serveur de maître utilisent l'utilitaire **Gestion de jeton** pour effectuer les tâches suivantes :

- Créer de nouveaux jetons d'autorisation
  Selon le niveau de sécurité, un jeton d'autorisation peut être requis pour un hôte NetBackup non maître afin d'obtenir un certificat basé sur l'ID d'hôte. L'administrateur NetBackup du serveur maître génère le jeton et le partage avec l'administrateur de l'hôte non-maître. Cet administrateur peut alors déployer le certificat sans la présence de l'administrateur du serveur maître.
  Se reporter à "Création de jetons d'autorisation" à la page 358.
- Supprimer des jetons d'autorisation
  Se reporter à "Suppression de jetons d'autorisation" à la page 360.
- Afficher les détails de jeton d'autorisation
  Se reporter à "Affichage des détails de jeton d'autorisation" à la page 361.
- Nettoyer les jetons d'autorisation non valides ou expirés
  Se reporter à "Jetons d'autorisation expirés et nettoyage" à la page 361.

Création de jetons d'autorisation

Selon le paramètre de sécurité de déploiement de certificat, les hôtes NetBackup peuvent nécessiter un jeton d'autorisation pour obtenir un certificat basé sur l'ID d'hôte à partir de l'autorité de certification (serveur maître).

Se reporter à "Création d'un jeton de renouvellement" à la page 354.

- Si le paramètre de sécurité est **Très élevé**, toutes les demandes de certificat requièrent un jeton. Effectuez la procédure décrite dans cette rubrique.
- Si le paramètre de sécurité est **Elevé**, les certificats sont automatiquement déployés sur les hôtes qui sont connus du serveur maître. Si l'hôte n'est pas connu du serveur maître, le certificat doit être déployé à l'aide d'un jeton d'autorisation. Dans ce cas, effectuez la procédure décrite dans cette rubrique.
  Pour comprendre ce que signifie être connu du serveur maître, consultez la rubrique suivante :
  Se reporter à "À propos des niveaux de sécurité de déploiement de certificats NetBackup" à la page 334.
- Si le paramètre de sécurité est **Moyen**, cette procédure peut être moins utile car les certificats sont automatiquement déployés sur tous les hôtes qui en

demandent un. Cependant, le serveur maître doit être en mesure de vérifier l'IP et le nom d'hôte de l'hôte qui demande un certificat.

Remarque : Un jeton est requis pour demander un certificat au nom d'un hôte qui n'a aucune connectivité avec le serveur maître.

Se reporter à "Déploiement de certificats sur un client qui n'a aucune connectivité avec le serveur maître" à la page 349.

Remarque : N'utilisez pas cette procédure pour créer un jeton d'autorisation pour un hôte NetBackup dont le certificat actuel n'est pas dans un état valide car il est perdu, corrompu ou a expiré. Dans ce cas, un jeton de renouvellement doit être utilisé.

Se reporter à "Renouvellement des certificats basés sur l'ID d'hôte" à la page 353.

L'administrateur NetBackup du serveur maître peut utiliser la **console d'administration NetBackup** ou la ligne de commande pour créer le jeton.

Pour créer un jeton à l'aide de la console d'administration NetBackup

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** > **Gestion de certificat** > **Gestion de jeton**.
2. Dans le menu **Actions**, sélectionnez **Nouveau jeton**.

   La boîte de dialogue **Créer un jeton** s'affiche.
3. Entrez un nom unique et explicite pour le jeton. Le champ ne peut pas rester vide.

   Par exemple, pour créer un jeton pour demander des certificats pour plusieurs hôtes qui appartiennent à master_server_1, nommez le jeton Token1_MS1. Une bonne pratique consiste à écrire une description utile dans le champ **Raison** pour le jeton.
4. Entrez un chiffre pour l'option **Utilisations maximales autorisées** pour le nombre de fois que le jeton peut être utilisé. La valeur par défaut est 1, ce qui indique qu'un hôte peut utiliser le jeton une seule fois.

   Pour utiliser le même jeton pour plusieurs hôtes, entrez une valeur comprise entre 1 et 99999. Par exemple, pour utiliser le jeton pour 8 hôtes, entrez 8. Le neuvième hôte qui tente d'utiliser le jeton ne réussit pas.
5. Utilisez l'option **Valide pour** pour indiquer combien de temps le jeton peut être utilisé avant qu'il soit invalide et ne puisse pas être utilisé. Après la date **Valide pour**, le serveur maître doit générer un autre jeton.

   Sélectionnez une période entre 1 et 999 heures ou jours.

6. Facultatif : entrez la raison de la création du jeton. La raison s'affiche dans les journaux d'audit, ainsi que les autres entrées dans la boîte de dialogue.
7. Sélectionnez **Créer**.
8. Le nouveau jeton apparaît dans une boîte de dialogue. Sélectionnez **Copier** pour enregistrer la valeur du jeton dans le presse-papiers.
9. Transmettez la valeur du jeton à l'administrateur de l'hôte de serveur non-maître. La manière dont le jeton est transmis dépend de divers facteurs de sécurité dans l'environnement. Le jeton peut être transmis par courrier électronique, par fichier ou verbalement.
10. L'administrateur de l'hôte non maître utilise le jeton pour obtenir un certificat basé sur l'ID d'hôte à partir de l'autorité de certification. Consultez la procédure suivante pour obtenir des instructions :

    Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.

Pour créer un jeton à l'aide de la commande nbcertcmd

- Sur l'hôte, exécutez la commande suivante :

  ```
  nbcertcmd -createToken -name token_name
  ```

  Par exemple :

  ```
  nbcertcmd -createToken -name testtoken

  Token FCBVYUTDUIELUDOE created successfully.
  ```

  Des paramètres supplémentaires peuvent être utilisés pour indiquer le nombre d'utilisations maximum, la durée de validité et la raison de la création.

  Pour plus d'informations sur la commande `nbcertcmd`, consultez le *Guide de référence des commandes NetBackup*.

Suppression de jetons d'autorisation

Utilisez la **console d'administration NetBackup**ou la ligne de commande pour supprimer des jetons d'autorisation spécifiques. Un jeton peut être supprimé même s'il n'a pas expiré et si le nombre d'**Utilisations maximales autorisées** n'a pas encore été épuisé.

Pour créer un jeton à l'aide de la console d'administration NetBackup

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité > Gestion de certificat > Gestion de jeton**.
2. Dans le volet droit, sélectionnez le jeton à supprimer.

3 Sélectionnez **Modifier > Supprimer**.

4 Cliquez sur **Oui** dans la boîte de dialogue pour supprimer le jeton.

Pour supprimer un jeton à l'aide de la ligne de commande

- Exécuter la commande `nbcertcmd -deleteToken` (avec des paramètres supplémentaires).

  Pour plus d'informations sur la commande `nbcertcmd`, consultez le Guide de référence des commandes NetBackup.

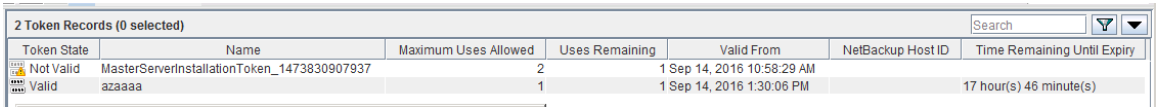
Affichage des détails de jeton d'autorisation

Les détails pour chaque jeton d'autorisation peuvent être affichés dans **console d'administration NetBackup** ou depuis la ligne de commande.

Pour afficher les détails de jeton à l'aide de la console d'administration NetBackup

1 Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** > **Gestion de certificat** > **Gestion de jeton**.

2 Les détails de jeton sont affichés dans le volet droit.



Pour afficher les détails de jeton à l'aide de la commande nbcertcmd

- Sur le serveur maître, exécutez la commande `nbcertcmd -listToken` pour afficher les détails de jetons (avec des paramètres supplémentaires).

  Les détails du jeton sont affichés.

Jetons d'autorisation expirés et nettoyage

Un jeton d'autorisation expire dans les situations suivantes (selon ce qui se produit en premier) :

- Lorsque la combinaison date-heure actuelle est ultérieure à l'attribut du jeton **Valide pour**.
- Lorsque le jeton est utilisé pour les demandes **Utilisations maximales autorisées**.

Un jeton d'autorisation expiré reste dans la base de données de jetons, mais ne peut pas être utilisé pour autoriser des demandes de déploiement de certificat.

Les jetons expirés peuvent être supprimés un par un ou être tous effacés simultanément à l'aide de l'opération **Nettoyage**. L'opération **Nettoyage** supprime tous les jetons expirés de la base de données de jetons.

Pour nettoyer des jetons d'autorisation expirés à l'aide de la console d'administration NetBackup

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** > **Gestion de certificat** > **Gestion de jeton**.
2. Dans le menu **Actions**, sélectionnez **Nettoyage**.
3. Cliquez sur **Oui** dans la boîte de dialogue de confirmation pour effacer tous les jetons expirés et les supprimer de la base de données de jetons.

Pour nettoyer les jetons à l'aide de la ligne de commande

- Utilisez la commande `nbcertcmd -cleanupToken` pour supprimer tous les jetons expirés.

Se reporter à "Suppression de jetons d'autorisation" à la page 360.

À propos de la liste de révocations des certificats basés sur l'ID d'hôte

La liste de révocations des certificats NetBackup (CRL) est une liste de certificats de sécurité numériques basés sur l'ID d'hôte qui ont été révoqués avant leur date d'expiration. Les hôtes qui possèdent des certificats révoqués ne doivent plus être approuvés.

La liste de révocations de certificats NetBackup est conforme au profil de la liste de révocations de certificats que l'Internet Engineering Task Force publie dans RFC 5280 à l'adresse suivante : https://www.ietf.org. L'autorité de certification NetBackup signe la liste de révocations de certificats. Le serveur maître NetBackup est l'autorité de certification. La liste CRL est publique et ne requiert pas de transmission sécurisée. Le terminal client CRL est ouvert, libre d'accès pour tout le monde.

Chaque hôte NetBackup doit avoir un certificat de sécurité et une liste de révocations valides de manière à pouvoir communiquer avec les autres hôtes NetBackup.

Fréquence à laquelle NetBackup génère une nouvelle liste de révocations de certificats

Le serveur maître NetBackup génère une nouvelle liste CRL comme suit :

- Au démarrage.
- Dans les soixante minutes depuis la dernière génération de la liste CRL.

- NetBackup vérifie toutes les 5 minutes s'il y a un nouveau certificat révoqué. Lorsqu'un certificat est révoqué, la mise à jour du serveur Web par NetBackup peut prendre jusqu'à 5 minutes.

La liste CRL expire au bout de 7 jours.

Fréquence à laquelle un hôte NetBackup obtient une liste CRL

Un hôte NetBackup obtient une liste de révocations de certificats lorsque NetBackup est installé sur l'hôte. Un hôte NetBackup obtient également une liste de révocations de certificats actualisée pendant une mise à niveau du logiciel NetBackup.

Après l'installation ou la mise à niveau, chaque hôte demande une nouvelle liste CRL à une certaine fréquence après le démarrage de l'hôte. (NetBackup utilise une méthode pull pour actualiser les listes CRL de l'hôte.) Le niveau de sécurité de déploiement du certificat du serveur maître NetBackup détermine la fréquence, comme indiqué dans le tableau suivant.

Tableau 15-8 Fréquence d'actualisation de liste CRL

Niveau de sécurité	Fréquence d'actualisation de liste CRL
Très élevée	Par heure
Haut	4 (heures)
Moyen	8 (heures)

Se reporter à "À propos des niveaux de sécurité de déploiement de certificats NetBackup" à la page 334.

Vous pouvez obtenir une nouvelle liste de révocations de certificats avant la période d'actualisation programmée.

Se reporter à "Actualisation de la liste de révocation de certificats sur le serveur maître" à la page 364.

Se reporter à "Actualisation de la liste de révocation de certificats sur un hôte NetBackup" à la page 364.

Pour plus d'informations

Se reporter à "Présentation des certificats de sécurité dans NetBackup" à la page 294.

Se reporter à "À propos des certificats basés sur l'ID d'hôte" à la page 328.

Se reporter à "Révocation de certificats basés sur l'ID d'hôte" à la page 365.

Actualisation de la liste de révocation de certificats sur le serveur maître

Utilisez la procédure suivante pour actualiser la liste de révocation de certificats sur le serveur maître. La procédure obtient la liste de révocation de certificats en cours auprès de l'autorité de certification NetBackup et la copie sur le serveur maître. Si un hôte dans l'environnement a été révoqué récemment, vous devez attendre jusqu'à 5 minutes avant que la liste de révocation de certificats indique que l'hôte a été révoqué.

Se reporter à "À propos de la liste de révocations des certificats basés sur l'ID d'hôte" à la page 362.

Actualisation de la liste de révocation de certificats sur le serveur maître

1. Connectez-vous au serveur maître en tant qu'administrateur.

   Pour un serveur maître en cluster, connectez-vous au nœud actif.

2. Pour un serveur maître en cluster, exécutez la commande suivante :

   ```
   nbcertcmd -getCRL -cluster [-server master_server_name]
   ```

   Pour obtenir la liste de révocation des certifications à partir d'un domaine NetBackup autre que le domaine par défaut, spécifiez l'option et l'argument `-server master_server_name`.

3. Exécutez la commande suivante :

   ```
   nbcertcmd -getCRL [-server master_server_name]
   ```

Actualisation de la liste de révocation de certificats sur un hôte NetBackup

Utilisez la procédure suivante pour actualiser la liste de révocation de certificats sur un hôte NetBackup. La procédure obtient la liste de révocation de certificats en cours auprès de l'autorité de certification NetBackup et la copie sur l'hôte local. Si un hôte dans l'environnement a été révoqué récemment, vous devez attendre jusqu'à 5 minutes avant que la liste de révocation de certificats indique que l'hôte a été révoqué.

Se reporter à "À propos de la liste de révocations des certificats basés sur l'ID d'hôte" à la page 362.

Pour actualiser la liste de révocation de certificats sur un hôte NetBackup

1. Connectez-vous en tant qu'administrateur de l'hôte NetBackup qui nécessite une nouvelle liste de révocation de certificats.
2. Exécutez la commande suivante :

   ```
   nbcertcmd -getCRL [-server master_server_name]
   ```

   Pour obtenir une liste CRL d'un domaine NetBackup autre que le domaine par défaut, spécifiez l'option et l'argument `-servermaster_server_name`.

Révocation de certificats basés sur l'ID d'hôte

Lorsque vous révoquez un certificat de sécurité numérique NetBackup, NetBackup révoque tous les autres certificats pour cet hôte. NetBackup ne fait plus confiance à l'hôte et ne peut plus communiquer avec les autres hôtes NetBackup.

Si vous révoquez un certificat à l'aide de la **console d'administration NetBackup**, vous devez sélectionner l'une des raisons suivantes :

Affiliation modifiée	L'hôte change l'affiliation pour un autre domaine NetBackup.
Autorité de certification compromise	L'autorité de certification est compromise.
Cessation de l'opération	L'hôte cesse d'être un hôte NetBackup. Par exemple, vous mettez hors service un serveur de médias ou un client NetBackup.
Clé compromise	La clé de certificat est compromise.
Remplacé	Un nouveau certificat remplace le certificat à révoquer.
Non spécifié	Autres raisons non spécifiées. Vous pouvez suspendre temporairement des privilèges pendant que vous enquêtez sur un événement de sécurité.

Si vous révoquez un certificat et déterminez par la suite que vous pouvez faire confiance à l'hôte, provisionnez un nouveau certificat sur cet hôte. Pour ce faire, utilisez un jeton de redistribution.

Se reporter à "Renouvellement des certificats basés sur l'ID d'hôte" à la page 353.

Remarque : Ne révoquez pas de certificat du serveur maître. Dans le cas contraire, les opérations NetBackup pourraient s'arrêter.

Après avoir révoqué le certificat d'un hôte, pensez à effectuer les actions suivantes dans NetBackup :

- Supprimez l'hôte des politiques de sauvegarde.
- Pour un serveur de médias NetBackup, désactivez-le.

Pensez également à toutes les actions qui ne sont pas liées à NetBackup afin de vous assurer qu'aucune personne mal intentionnée ne peut utiliser le certificat et la clé.

Se reporter à "À propos de la liste de révocations des certificats basés sur l'ID d'hôte" à la page 362.

Suppression de l'approbation entre un hôte et un serveur maître

Un hôte NetBackup peut approuver plusieurs autorités de certification (serveurs maîtres) à tout moment. Pour des raisons diverses, il peut être nécessaire pour un hôte NetBackup de supprimer la relation de confiance à partir d'un serveur maître précédemment approuvé.

Par exemple, si un client NetBackup est déplacé d'un serveur maître à un autre, il est recommandé de supprimer la relation de confiance à partir d'un serveur maître. Les bonnes pratiques de sécurité suggèrent l'approbation des entités plus petites requises pour fonctionner correctement. Si un hôte NetBackup ne doit plus communiquer avec les hôtes à partir d'un domaine NetBackup spécifique, supprimez le certificat de l'autorité de certification pour ce serveur maître de la banque de confiance de l'hôte.

Remarque : La suppression d'un certificat de l'autorité de certification ne supprime pas les certificats basés sur le nom d'hôte ou l'ID d'hôte que l'hôte peut avoir obtenu à partir de l'autorité de certification de l'hôte. Le `nbcertcmd -listCertDetails` continue d'afficher le certificat basé sur l'ID d'hôte.

Quand le certificat de l'autorité de certification est supprimé d'un hôte, le certificat basé sur l'ID d'hôte émis par une autorité de certification n'est pas automatiquement renouvelé parce que l'hôte n'approuve plus l'autorité de certification. Le certificat basé sur l'ID d'hôte par la suite expire.

Suppression de l'approbation entre un hôte et un serveur maître

1. L'administrateur de l'hôte de serveur non maître exécute la commande suivante sur l'hôte pour déterminer la signature de certificat de l'autorité de certification du serveur maître :

   ```
   nbcertcmd -listCACertDetails
   ```

   Dans cet exemple de sortie, l'hôte a des certificats de deux serveurs maîtres :

   ```
   nbcertcmd -listCACertDetails
        Subject Name : /CN=nbatd/OU=root@master1.abc.com/O=vx
          Start Date : Aug 23 14:16:44 2016 GMT
         Expiry Date : Aug 18 15:31:44 2036 GMT
    SHA1 Fingerprint : 7B:0C:00:32:96:20:36:52:92:E8:62:F3:56:
   74:8B:E3:2E:4F:22:4C

        Subject Name : /CN=nbatd/OU=root@master2.xyz.com/O=vx
          Start Date : Aug 25 12:09:55 2016 GMT
         Expiry Date : Aug 20 13:24:55 2036 GMT
    SHA1 Fingerprint : 7A:C7:6E:68:71:6B:82:FD:7E:80:FC:47:F6:
   8D:B2:E1:40:69:9C:8C
   ```

2. L'administrateur veut supprimer la relation de confiance pour le deuxième serveur maître et exécute la commande suivante sur l'hôte :

   ```
   nbcertcmd -removeCACertificate –fingerprint 7A:C7:6E:68:71:
   6B:82:FD:7E:80:FC:47:F6:8D:B2:E1:40:69:9C:8C
   ```

   Incluez la signature entier, y compris les deux points.

   Avertissement : Cette commande supprime le certificat de l'autorité de certification de la banque d'approbation. La banque d'approbation est appelée par les services NetBackup et le service NetBackup Web Management Console (`nbwebsvc`).

   ---

3. La **console d'administration NetBackup** sur le serveur maître affiche l'état du certificat comme étant **Actif**. Cependant, ce certificat ne se renouvelle pas automatiquement et peut expirer. L'administrateur NetBackup doit révoquer le certificat de l'hôte si l'hôte ne fait plus partie du domaine NetBackup.

Révoquer un certificat basé sur l'ID d'hôte

Les administrateurs de NetBackup peuvent prendre en compte la révocation d'un certificat basé sur l'ID d'hôte sous différentes conditions. Par exemple, si

l'administrateur détecte que la sécurité du client a été compromise, si un client est mis hors service, ou si NetBackup est désinstallé de l'hôte. Un certificat révoqué ne peut pas être utilisé pour communiquer avec les services web de serveur maître.

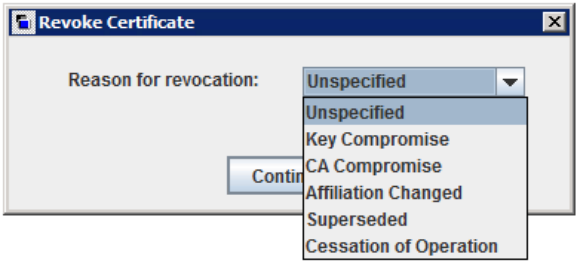
Se reporter à "Révocation de certificats basés sur l'ID d'hôte" à la page 365.

Les bonnes pratiques de sécurité suggèrent que l'administrateur révoque explicitement les certificats pour tout hôte qui n'est plus actif, que le certificat soit toujours déployé sur l'hôte, ou qu'il en ait été supprimé.

Remarque : Ne révoquez pas de certificat du serveur maître. Dans le cas contraire, les opérations NetBackup pourraient s'arrêter.

Pour révoquer un certificat basé sur l'ID d'hôte à l'aide de la console d'administration NetBackup

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** > **Gestion de certificat**.
2. Sélectionnez le certificat à révoquer.
3. Dans le menu **Actions**, sélectionnez **Révoquer le certificat**.
4. Sélectionnez une raison dans le menu déroulant et cliquez sur **Continuer**.



   Le certificat est révoqué.

5. Lorsque le certificat d'un hôte a été révoqué, effectuez les actions suivantes dans NetBackup :
   - Supprimez l'hôte des politiques de sauvegarde.
   - Pour un serveur de médias NetBackup, désactivez-le.

Pour révoquer un certificat basé sur l'ID d'hôte à l'aide de la ligne de commande

1. L'administrateur du serveur maître doit être connecté au service de gestion Web de NetBackup pour exécuter cette tâche. Pour vous connecter, utilisez la commande suivante :

   ```
   bpnbat -login -logintype WEB
   ```

   Se reporter à "Conditions requises de connexion web pour les options de commande nbcertcmd" à la page 329.

2. Exécutez une des commandes suivantes afin de révoquer le certificat en utilisant le nom d'hôte ou l'ID d'hôte.

   Révocation à l'aide du nom d'hôte :

   ```
   nbcertcmd -revokeCertificate -host host_name
   ```

   Remarque : Vous devez fournir le nom principal de l'hôte pour lequel vous souhaitez révoquer le certificat. Si vous ne spécifiez aucun des mappages d'ID d'hôte vers le nom d'hôte qui sont ajoutés pour l'hôte, le certificat ne peut pas être révoqué.

   Révocation à l'aide de l'ID d'hôte :

   ```
   nbcertcmd -revokeCertificate -hostID host_id
   ```

   Des paramètres supplémentaires peuvent être utilisés pour indiquer un code de raison de révocation et le serveur maître.

3. Lorsque le certificat d'un hôte a été révoqué, effectuez les actions suivantes dans NetBackup :

   - Supprimez l'hôte des politiques de sauvegarde.
   - Pour un serveur de médias NetBackup, désactivez-le.

Remarque : Révoquer un certificat ne supprime pas le certificat du magasin local de l'hôte non maître.

Détermination de l’état du certificat d’un hôte NetBackup

Si le certificat signé par une autorité de certification NetBackup est utilisé

Vous pouvez déterminer l’état d’un certificat NetBackup : actif ou révoqué. Cette opération peut permettre de résoudre les problèmes de connexion et de communication. Il existe trois méthodes pour déterminer l’état d’un certificat :

Vérification du certificat d’un hôte à partir de l’hôte lui-même	Cette méthode repose sur la commande NetBackup `nbcertcmd`. Se reporter à "Pour vérifier l’état du certificat de l’hôte à partir de l’hôte" à la page 371.
Vérification du certificat d’un hôte à partir d’un serveur NetBackup	Cette méthode repose sur la commande NetBackup `bptestbpcd`. Se reporter à "Pour vérifier depuis un serveur NetBackup si le certificat d’un autre hôte est révoqué" à la page 372.
Vérification du certificat d’un hôte à partir de la **console d’administration NetBackup**	Se reporter à "Pour vérifier le certificat d’un hôte à l’aide de la console d’administration NetBackup" à la page 372.

Se reporter à "À propos de la liste de révocations des certificats basés sur l’ID d’hôte" à la page 362.

Pour vérifier l'état du certificat de l'hôte à partir de l'hôte

1. (Facultatif) Sur l'hôte NetBackup, exécutez la commande suivante en tant qu'administrateur pour obtenir la liste de révocation des certifications à jour :

   UNIX : `/usr/openv/netbackup/bin/nbcertcmd -getCRL [-server master_server_name]`

   Windows : `install_path\NetBackup\bin\nbcertcmd -getCRL [-server master_server_name]`

   Pour obtenir une liste CRL d'un domaine NetBackup autre que le domaine par défaut, spécifiez l'option et l'argument `-servermaster_server_name`.

2. Sur l'hôte NetBackup, exécutez la commande suivante en tant qu'administrateur :

   UNIX : `/usr/openv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster] [-server master_server_name]`

   Windows : `install_path\NetBackup\bin\nbcertcmd -hostSelfCheck [-cluster] [-server master_server_name]`

   Si nécessaire, utilisez l'une des deux options suivantes ou les deux options :

`-cluster`	Utilisez cette option sur le nœud actif d'un cluster de serveurs maîtres NetBackup pour vérifier le certificat de l'hôte virtuel.
`-server`	Utilisez cette option avec l'argument *nom_serveur_maître* pour vérifier un certificat à partir d'un serveur maître autre que le serveur maître par défaut.

3. Examinez la sortie de la commande. La sortie indique que le certificat est ou n'est pas révoqué.

Pour vérifier depuis un serveur NetBackup si le certificat d'un autre hôte est révoqué

1. En tant qu'administrateur sur le serveur maître NetBackup ou un serveur de médias NetBackup, exécutez la commande suivante :

   UNIX : `/usr/openv/netbackup/bin/admincmd/bptestbpcd -host hostname -verbose`

   Windows : `install_path\NetBackup\bin\bptestbpcd -host hostname -verbose`

   Pour `-host hostname`, spécifiez l'hôte dont vous voulez vérifier le certificat.

2. Examinez la sortie de la commande. Si le certificat sur l'hôte spécifié est révoqué, le résultat de la commande contient la chaîne `The Peer Certificate is revoked`. Si la sortie de la commande ne comporte pas cette chaîne, le certificat est valide.

Pour vérifier le certificat d'un hôte à l'aide de la console d'administration NetBackup

1. Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité** > **Gestion des certificats**.
2. Examinez la colonne **État du certificat** pour l'hôte qui vous intéresse.

Si le certificat signé par une autorité de certification externe est utilisé

Vous pouvez déterminer l'état d'un certificat d'hôte signé par une autorité de certification externe : actif ou révoqué. Cette opération peut permettre de résoudre les problèmes de connexion et de communication.

Il existe deux méthodes pour déterminer l'état d'un certificat :

Vérification du certificat d'un hôte à partir de l'hôte lui-même	Se reporter à "Pour vérifier le certificat d'un hôte à partir de l'hôte lui-même" à la page 373.
Vérification du certificat d'un hôte à partir d'un serveur NetBackup	Se reporter à "Pour vérifier depuis un serveur NetBackup si le certificat d'un autre hôte est révoqué" à la page 373.

Pour vérifier le certificat d'un hôte à partir de l'hôte lui-même

1. Actualisez les CRL dans le cache des listes de révocation de certificats de NetBackup.
2. Sur l'hôte NetBackup, exécutez la commande suivante en tant qu'administrateur :

   UNIX : `/usr/openv/netbackup/bin/nbcertcmd -hostSelfCheck [-cluster]`

   Windows : `install_path\NetBackup\bin\nbcertcmd -hostSelfCheck [-cluster]`

   Utilisez l'option `-cluster` sur le nœud actif d'un serveur maître en cluster pour vérifier le certificat du nom virtuel.
3. Examinez la sortie de la commande. La sortie indique si le certificat est révoqué ou non.

Pour vérifier depuis un serveur NetBackup si le certificat d'un autre hôte est révoqué

1. En tant qu'administrateur sur le serveur maître NetBackup ou un serveur de médias NetBackup, exécutez la commande suivante :

   UNIX : `/usr/openv/netbackup/bin/admincmd/bptestbpcd -host hostname -verbose`

   Windows : `install_path\NetBackup\bin\bptestbpcd -host hostname -verbose`

   Pour `-host hostname`, spécifiez l'hôte dont vous voulez vérifier le certificat.
2. Examinez la sortie de la commande. Si le certificat sur l'hôte spécifié est révoqué, la sortie de la commande contient la chaîne suivante : Le certificat de pair a été révoqué. Si la sortie de la commande ne comporte pas cette chaîne, le certificat est valide.

Obtenir la liste des hôtes NetBackup ayant des certificats révoqués

Utilisez la procédure suivante pour obtenir la liste des hôtes NetBackup qui ont un certificat révoqué.

Se reporter à "À propos de la liste de révocations des certificats basés sur l'ID d'hôte" à la page 362.

Pour obtenir la liste des hôtes NetBackup ayant des certificats révoqués

1. Dans une fenêtre de commande, connectez-vous au **service NetBackup Web Management** sur le serveur maître (le compte de connexion doit disposer de droits d'administrateur NetBackup) en procédant comme suit :

   UNIX : `/usr/openv/netbackup/bin/bpnbat -login -loginType WEB`

   Windows : *`install_path`*`\NetBackup\bin\bpnbat -login -loginType WEB`

2. Exécutez la commande suivante pour extraire de la liste CRL une liste de certificats qui n'ont pas expiré, puis filtrer les résultats avec le mot « `Revoked` » :

   UNIX : `/usr/openv/netbackup/bin/nbcertcmd -listAllDomainCertificates | grep Revoked`

   Windows : *`install_path`*`\NetBackup\bin\nbcertcmd -listAllDomainCertificates | findstr Revoked`

Suppression de certificats basés sur l'ID d'hôte

Utilisez cette rubrique pour supprimer manuellement le certificat basé sur l'ID d'hôte d'un hôte NetBackup. Il est possible que vous deviez supprimer des certificats dans certains cas, par exemple : un hôte NetBackup qui est déplacé d'un domaine NetBackup vers un autre domaine NetBackup. Dans ce scénario, le certificat basé sur l'ID d'hôte actuel doit être supprimé et l'hôte doit avoir un certificat émis par la nouvelle autorité de certification (AC), le nouveau serveur maître.

Attention : La suppression manuelle des certificats basés sur l'ID d'hôte peut avoir un impact négatif sur la fonctionnalité NetBackup.

Remarque : Les certificats basés sur l'ID d'hôte sont automatiquement supprimés lors de la suppression du logiciel NetBackup.

Pour supprimer un certificat basé sur l'ID d'hôte à partir d'un hôte NetBackup

1. Exécutez la commande suivante sur l'hôte NetBackup pour afficher les détails de tous les certificats basés sur l'ID d'hôte associés.

   UNIX : `/usr/openv/netbackup/bin/nbcertcmd -listCertDetails`

   Windows : *`install_path`*`\NetBackup\bin\nbcertcmd -listCertDetails`

2. Pour supprimer un certificat, exécutez la commande suivante sur l'hôte :

   UNIX : `/usr/openv/netbackup/bin/nbcertcmd -deleteCertificate -hostid` *`host_ID`*

   Windows : *`install_path`*`\NetBackup\bin\nbcertcmd -deleteCertificate -hostid` *`host_ID`*

Pour supprimer un certificat basé sur l'ID d'hôte à partir d'un nœud actif dans une installation en cluster

1. Exécutez la commande suivante sur le nœud actif pour afficher les détails de tous les certificats basés sur l'ID d'hôte associés.

   UNIX : `/usr/openv/netbackup/bin/nbcertcmd -listCertDetails -cluster`

   Windows : *`install_path`*`\NetBackup\bin\nbcertcmd -listCertDetails -cluster`

2. Pour supprimer un certificat, exécutez la commande suivante sur le nœud actif du cluster :

   `nbcertcmd -deleteCertificate -hostid` *`host_ID`* `-cluster`

   UNIX : `/usr/openv/netbackup/bin/nbcertcmd -hostid` *`host_ID`* `-cluster]`

   Windows : *`install_path`*`\NetBackup\bin\nbcertcmd -hostid` *`host_ID`* `-cluster`

Déploiement de certificat basé sur l'ID d'hôte dans une configuration en cluster

Cette section fournit des informations sur le déploiement des certificats basés sur le nom d'hôte et l'ID d'hôte dans une installation NetBackup en cluster.

Pour plus d'informations sur les clusters NetBackup, consultez le *Guide de l'administrateur de serveur maître en cluster NetBackup*.

À propos du déploiement de certificats basés sur l'ID d'hôte sur un cluster NetBackup

Dans une installation de serveur maître NetBackup en cluster, les certificats basés sur l'ID d'hôte sont déployés comme suit :

- Un certificat pour chaque nœud de cluster : un certificat réside sur le disque local de chaque nœud.
- Un certificat pour le nom virtuel : un certificat réside sur le disque partagé du cluster.

Prenons l'exemple suivant :

Si une installation de cluster se compose de 4 nœuds, 5 certificats basés sur l'ID d'hôte sont déployés. Un certificat est déployé sur chacun des 4 nœuds et un autre sur le disque partagé, qui est utilisé pour le nom virtuel du serveur maître.

Remarque : Seuls les serveurs maîtres peuvent être mis en cluster dans NetBackup.

À propos du déploiement de certificats basés sur le nom d'hôte sur un cluster NetBackup

Dans une installation de serveur maître NetBackup en cluster, les certificats basés sur le nom d'hôte sont déployés comme suit :

- Un certificat pour chaque nœud de cluster : un certificat réside sur le disque local de chaque nœud.
- Un certificat pour le nom virtuel sur chaque nœud : un certificat réside sur le disque local de chaque nœud.

Se reporter à "Déploiement de certificats basés sur le nom d'hôte" à la page 326.

Déploiement d'un certificat basé sur un ID d'hôte sur un hôte NetBackup en cluster

Passez en revue les scénarios suivants pour le déploiement de certificat sur des nœuds de cluster :

- Dans le cas d'une nouvelle installation NetBackup le certificat est déployé automatiquement sur les nœuds actifs. Vous devez déployer manuellement les certificats sur tous les nœuds inactifs.
- En cas de reprise après incident, les certificats des nœuds actifs et inactifs ne sont pas restaurés. Après avoir installé NetBackup en mode de reprise après incident à la suite d'un incident, vous devez déployer manuellement les certificats sur tous les nœuds.

Se reporter à "Génération d'un certificat sur un serveur maître en cluster après une installation de reprise après incident" à la page 383.

Remarque : Dans le cas d'une mise à niveau, les nœuds actifs ou inactifs peuvent déjà avoir un certificat. Vous pouvez vérifier qu'un nœud de cluster possède un certificat.

Se reporter à "Affichage des informations de certificat pour une configuration NetBackup en cluster" à la page 381.

Se reporter à "Déploiement de certificat basé sur un ID d'hôte sur le nœud de serveur maître actif" à la page 377.

Se reporter à "Déploiement de certificat basé sur l'ID d'hôte sur les nœuds du serveur maître inactif" à la page 377.

Déploiement de certificat basé sur un ID d'hôte sur le nœud de serveur maître actif

Pendant l'installation de NetBackup, des certificats basés sur un ID d'hôte sont déployés sur le nœud de serveur maître actif et le nom virtuel. Le certificat pour le nœud actif est déployé sur un disque local. Le certificat pour le nom virtuel est déployé sur le disque partagé.

Déploiement de certificat basé sur l'ID d'hôte sur les nœuds du serveur maître inactif

Les certificats des nœuds inactifs ne sont pas déployés pendant l'installation. Vous devez déployer manuellement les certificats sur tous les nœuds inactifs après l'installation.

Se reporter à "Déploiement de certificats basés sur un hôte sur des nœuds de cluster" à la page 377.

Déploiement de certificats basés sur un hôte sur des nœuds de cluster

Vous devez déployer manuellement les certificats sur tous les nœuds inactifs.

Dans certains scénarios, vous devez déployer manuellement les certificats basés sur un ID d'hôte sur les nœuds actifs.

Pour déployer manuellement un certificat basé sur un ID d'hôte sur un nœud de cluster de serveur maître

- Exécutez les commandes suivantes sur le nœud du cluster du serveur maître :

- `nbcertcmd -getCACertificate`
- `nbcertcmd -getCertificate [-file` *`authorization_token_file`*`]`

Se reporter à "À propos de la gestion des jetons pour les certificats basés sur l'ID d'hôte" à la page 358.

Révocation d'un certificat basé sur un ID d'hôte pour une configuration NetBackup en cluster

Les administrateurs de NetBackup peuvent prendre en compte la révocation d'un certificat basé sur l'ID d'hôte sous différentes conditions. Par exemple, si l'administrateur détecte que la sécurité du client a été compromise, si un client est mis hors service, ou si NetBackup est désinstallé de l'hôte. Un hôte avec un certificat révoqué ne peut pas communiquer avec d'autres hôtes. Chaque hôte NetBackup doit avoir un certificat de sécurité valide et une liste de révocation de certificats pour que la communication aboutisse.

Se reporter à "À propos de la liste de révocations des certificats basés sur l'ID d'hôte" à la page 362.

L'administrateur de NetBackup peut révoquer des certificats pour un nœud de cluster ou le nom virtuel à partir de n'importe quel hôte dans un domaine NetBackup.

Assurez-vous de révoquer le certificat approprié.

Lorsque le certificat est révoqué, vous devez déployer un nouveau certificat basé sur un ID d'hôte. Créez un jeton de renouvellement sur le nœud en cluster et déployez un nouveau certificat en utilisant le jeton de renouvellement.

Se reporter à "Création d'un jeton de renouvellement pour un programme d'installation de NetBackup en cluster" à la page 380.

Se reporter à "Déploiement d'un certificat basé sur un ID d'hôte dans une configuration NetBackup en cluster à l'aide d'un jeton de renouvellement" à la page 379.

Pour révoquer un certificat à partir d'un nœud de cluster

1. Connectez-vous au Service NetBackup Web Management :

   ```
   bpnbat -login -logintype WEB
   ```

   Se reporter à "Conditions requises de connexion web pour les options de commande nbcertcmd" à la page 329.

2. Exécutez la commande suivante pour révoquer un certificat pour un nœud de cluster :

   ```
   nbcertcmd -revokeCertificate -host host_name
   ```

   Se reporter à "Révoquer un certificat basé sur l'ID d'hôte" à la page 367.

Pour révoquer un certificat pour le nom virtuel

1. Connectez-vous au Service NetBackup Web Management :

   ```
   bpnbat -login -logintype WEB
   ```

2. Exécutez la commande suivante pour révoquer un certificat basé sur l'ID d'hôte pour le nom virtuel :

   ```
   nbcertcmd -revokeCertificate -host virtual_name
   ```

   Se reporter à "Révoquer un certificat basé sur l'ID d'hôte" à la page 367.

Déploiement d'un certificat basé sur un ID d'hôte dans une configuration NetBackup en cluster à l'aide d'un jeton de renouvellement

Après la révocation d'un certificat basé sur l'ID d'hôte, vous pouvez déployer de nouveaux certificats sur une installation NetBackup en cluster à l'aide de jetons de renouvellement.

Se reporter à "Création d'un jeton de renouvellement pour un programme d'installation de NetBackup en cluster" à la page 380.

Pour déployer un nouveau certificat basé sur l'ID d'hôte sur un nœud de cluster

- Exécutez la commande suivante pour déployer un nouveau certificat sur le nœud de cluster en utilisant le jeton de renouvellement :

  ```
  nbcertcmd -getCertificate -file reissue_token_file -force
  ```

Pour déployer un nouveau certificat basé sur l'ID d'hôte pour le nom virtuel

- Exécutez la commande suivante pour déployer un nouveau certificat pour le nom virtuel en utilisant le jeton de renouvellement :

  ```
  nbcertcmd -getCertificate -file reissue_token_file_virtual -force
  -cluster
  ```

Création d'un jeton de renouvellement pour un programme d'installation de NetBackup en cluster

Vous devez renouveler un certificat sur un hôte dans certains cas, par exemple, lorsqu'un certificat est révoqué pour un hôte et que vous devez émettre nouveau certificat sur l'hôte.

Se reporter à "Déploiement d'un certificat basé sur un ID d'hôte dans une configuration NetBackup en cluster à l'aide d'un jeton de renouvellement" à la page 379.

Vous devez utiliser un jeton de renouvellement pour émettre un nouveau certificat pour l'hôte.

Se reporter à "À propos de la gestion des jetons pour les certificats basés sur l'ID d'hôte" à la page 358.

Pour créer un jeton de renouvellement pour un nœud de cluster

1. Connectez-vous au service de gestion Web NetBackup avec la commande suivante :

   ```
   bpnbat -login -logintype WEB
   ```

   Se reporter à "Conditions requises de connexion web pour les options de commande nbcertcmd" à la page 329.

2. Exécutez la commande suivante pour créer un jeton de renouvellement pour le nœud de cluster requis :

   ```
   nbcertcmd -createToken -name token_name -reissue -host host_name
   ```

   Se reporter à "Création d'un jeton de renouvellement" à la page 354.

Pour créer un jeton de renouvellement pour le nom virtuel

1. Connectez-vous au service de gestion Web NetBackup avec la commande suivante :

   ```
   bpnbat -login -logintype WEB
   ```

   Se reporter à "Conditions requises de connexion web pour les options de commande nbcertcmd" à la page 329.

2. Exécutez la commande suivante pour créer un jeton de renouvellement pour le nom virtuel.

   ```
   nbcertcmd -createToken -name token_name_virtual -reissue -host
   virtual_name
   ```

   Se reporter à "Création d'un jeton de renouvellement" à la page 354.

Renouvellement d'un certificat basé sur un ID d'hôte dans une configuration NetBackup en cluster

Des certificats basés sur l'ID d'hôte pour les nœuds de cluster et le nom virtuel sont automatiquement renouvelés. Les certificats sont automatiquement renouvelés 180 jours avant la date d'expiration.

Vous pouvez également renouveler les certificats manuellement, si nécessaire.

Se reporter à "À propos de l'expiration et du renouvellement des certificats basés sur l'ID d'hôte" à la page 350.

Pour renouveler manuellement le certificat pour un nœud de cluster

- Exécutez la commande suivante à partir d'un nœud de cluster pour renouveler le certificat pour le nœud :

  ```
  nbcertcmd -renewCertificate
  ```

Pour renouveler manuellement le certificat pour le nom virtuel

- Exécutez la commande suivante sur le nœud actif pour renouveler manuellement le certificat pour le nom virtuel :

  ```
  nbcertcmd -renewCertificate -cluster
  ```

Affichage des informations de certificat pour une configuration NetBackup en cluster

Exécutez les commandes suivantes pour afficher les détails du certificat d'un nœud de cluster ou le nom virtuel.

Pour afficher les détails du certificat d'un nœud de cluster

- Sur un nœud de cluster, exécutez la commande suivante :

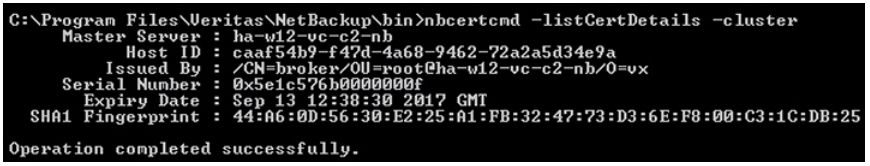
  ```
  nbcertcmd -listCertDetails
  ```

  Se reporter à "Affichage des détails de certificat basé sur l'ID d'hôte" à la page 332.

Pour afficher les détails du certificat pour le nom virtuel

- Exécutez la commande suivante sur le nœud actif pour afficher les détails du certificat pour le nom virtuel :

  ```
  nbcertcmd -listCertDetails -cluster
  ```



Se reporter à "Affichage des détails de certificat basé sur l'ID d'hôte" à la page 332.

Suppression des certificats de l'autorité de certification à partir de l'installation d'un NetBackup en cluster

Exécutez les commandes suivantes pour supprimer les certificats de l'autorité de certification (autorité de certification) à partir d'une configuration en cluster.

Attention : La suppression du certificat de l'autorité de certification à partir d'un nœud de serveur maître peut avoir un impact sur la fonctionnalité NetBackup.

Pour supprimer les certificats de l'autorité de certification à partir d'un nœud de cluster

1. Exécutez la commande suivante sur un nœud de cluster pour afficher les signatures des certificats de l'autorité de certification :

   ```
   nbcertcmd -listCACertDetails
   ```

2. Exécutez la commande suivante pour supprimer le certificat de l'autorité de certification en fournissant la signature appropriée :

   ```
   nbcertcmd -removeCACertificate -fingerprint fingerprint
   ```

Pour supprimer les certificats de l'autorité de certification pour le nom virtuel

1. Exécutez la commande suivante sur le nœud actif pour afficher les signatures des certificats de l'autorité de certification pour le nom virtuel :

   ```
   nbcertcmd -listCACertDetails -cluster
   ```

2. Exécutez la commande suivante sur le nœud actif pour supprimer le certificat de l'autorité de certification pour le nom virtuel en fournissant la signature appropriée `nbcertcmd -removeCACertificate -fingerprint` *`fingerprint_virtual`* `-cluster`

Génération d'un certificat sur un serveur maître en cluster après une installation de reprise après incident

Après avoir terminé la reprise après incident d'un serveur maître en cluster, vous devez générer un certificat sur le nœud actif, ainsi que sur tous les nœuds inactifs. Cette procédure est requise pour que les sauvegardes et les restaurations du cluster réussissent.

Génération du certificat local sur chaque nœud du cluster après une reprise après incident installation

1. Ajoutez tous les nœuds inactifs sur le cluster.

   Si tous les nœuds du cluster ne font pas partie du cluster actuellement, commencez par les ajouter au cluster. Consultez les instructions sur le cluster de votre système d'exploitation pour obtenir de l'aide concernant cette étape.

   Plus d'informations sur les technologies de cluster prises en charge sont disponibles. Consultez le *Guide de l'administrateur d'un serveur maître en cluster NetBackup*.

2. Exécutez la commande `nbcertcmd` pour stocker le certificat d'autorité de certification.

   UNIX : `/usr/openv/netbackup/bin/nbcertcmd -getCACertificate`

   Windows : *`install_path`*`\Veritas\NetBackup\bin\nbcertcmd -getCACertificate`

3. Utilisez la commande `bpnbat` comme indiqué pour autoriser les modifications nécessaires. Lorsque vous y êtes invité par le courtier d'authentification, entrez le nom du serveur virtuel (et non le nom du nœud local).

   ```
   bpnbat -login -loginType WEB
   ```

4 Utilisez la commande `nbcertcmd` pour créer un jeton de renouvellement. Le *nom d'hôte* est le nom du nœud local. Lorsque la commande s'exécute, la valeur de la chaîne de jeton s'affiche. Un jeton de renouvellement unique est nécessaire pour chaque nœud de cluster.

```
nbcertcmd -createtoken -name token_name -reissue -host hostname
```

5 Utilisez le jeton de renouvellement avec la commande `nbcertcmd` pour stocker le certificat de l'hôte. Cette commande vous invite à entrer la valeur de la chaîne de jeton. Entrez la chaîne de jeton obtenue à l'aide de la commande `nbcertcmd -createToken`.

```
nbcertcmd -getCertificate -token
```

Des informations supplémentaires sont disponibles. Consultez la section sur le déploiement des certificats sur les nœuds de serveur maître dans le *Guide de sécurité et de chiffrement Veritas NetBackup*.

Se reporter à "Packages de reprise après incident" à la page 325.

Communication entre un client NetBackup situé dans une zone démilitarisée et un serveur maître, via un tunnel HTTP

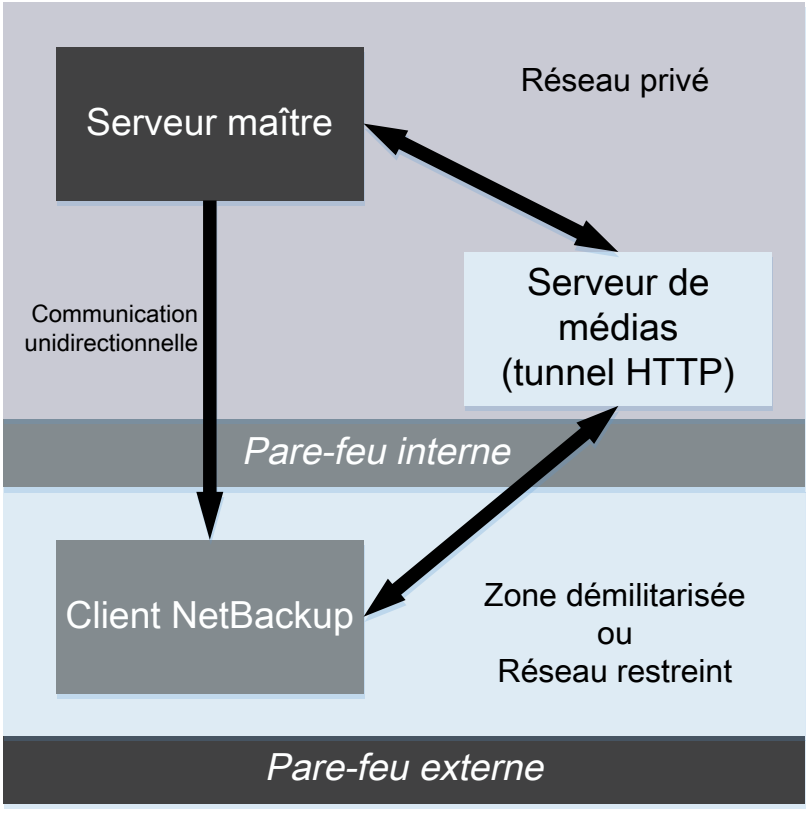
Dans une configuration de déploiement NetBackup, les ordinateurs client peuvent se trouver dans une zone démilitarisée (DMZ) où la communication s'effectue uniquement par le biais de ports web spécifiques.

Tous les clients NetBackup doivent être en mesure de communiquer avec le service de gestion Web sur le serveur maître pour déployer les certificats de sécurité et autoriser des pairs afin de sécuriser les connexions. Par exemple, le client NetBackup envoie des demandes au serveur maître pour le déploiement de certificats, ce qui est essentiel pour la communication sécurisée de NetBackup. Dans une configuration de zone démilitarisée, le client n'est peut-être pas en mesure d'envoyer des demandes de service web directement au serveur maître. Dans ce scénario, un client NetBackup envoie une demande de connexion et une demande de service web au tunnel HTTP sur le serveur de médias par la méthode de proxy HTTP CONNECT. Le tunnel HTTP accepte la demande de connexion et transmet la demande de service web au serveur maître.

La fonction de tunneling HTTP permet aux clients NetBackup dans une zone démilitarisée d'envoyer des demandes de service web au serveur maître. Le serveur de médias NetBackup constitue un tunnel HTTP qui transmet la demande de service web du client NetBackup au serveur maître. La suite de la communication de service web utilise la couche SSL (Secure Socket Layer).

Remarque : Le numéro de port 1556 sur le serveur de médias doit être accessible par le client NetBackup pour l'envoi des demandes de service web.

Figure 15-2 Communication de client NetBackup et de serveur maître dans une configuration de zone démilitarisée



Dans un environnement de domaine unique ou multiple, quand le client NetBackup dans une zone démilitarisée essaie d'envoyer une demande de connexion du service web au serveur maître, il suit un ordre précis :

Tableau 15-9 Ordre d'envoi d'une demande de connexion

Ordre	Description
1. Le client NetBackup essaie d'envoyer la demande de connexion directement au serveur maître.	Dans une zone démilitarisée, la demande de connexion du service web peut échouer.

Ordre	Description
2. Si la connexion directe échoue, le client vérifie ensuite qu'un serveur de médias est spécifié pour utiliser le tunneling HTTP pour envoyer la demande de connexion du service web au serveur maître.	
3. Si aucun serveur de médias n'est spécifié, le client consulte une liste de serveurs de médias disponible dans la configuration NetBackup et utilise ces serveurs pour envoyer des demandes de connexion du service web.	Le client NetBackup met à jour un fichier de cache interne (`websvctunnels.cache`) qui contient une liste de serveurs de médias automatiquement mis à jour basée sur les connexions précédentes établies avec succès. Le fichier de cache est disponible dans le même emplacement que le fichier `bp.conf` pour Windows et UNIX.

Informations supplémentaires

- Les options supplémentaires suivantes sont disponibles pour la configuration de la fonction HTTP Tunnel :
  - WEB_SERVER_TUNNEL_USE - vous pouvez utiliser cette option sur les clients NetBackup pour configurer le comportement de communication par défaut à l'aide de HTTP Tunnel.
  - WEB_SERVER_TUNNEL_ENABLE - par défaut, la fonction HTTP Tunnel est activée sur le serveur de médias. Vous pouvez utiliser cette option sur les serveurs de médias pour désactiver la fonction HTTP Tunnel.

  Pour plus d'informations, consultez le *Guide de l'administrateur NetBackup, volume I*.
- Si votre configuration de client NetBackup ne contient pas d'information sur les serveurs de médias dans le domaine, exécutez la commande `nbsetconfig` sur le serveur maître. Le registre d'un client Windows ou le fichier `bp.conf` d'un client UNIX comprend le serveur maître et les serveurs de médias que le client sélectionne pour envoyer des demandes de connexion et de service web.
- Si vous utilisez la commande `nbcertcmd -getCertificate` sur le client NetBackup dans une zone démilitarisée, et si vous voyez apparaître l'un des messages d'erreur suivants :
  - ÉTAT DE SORTIE 5955 : le nom d'hôte est inconnu du serveur maître.
  - ÉTAT DE SORTIE 5954 : le nom d'hôte n'a pas pu être résolu sur l'adresse IP de l'hôte ayant formulé la demande.

Utiliser un jeton de déployer le certificat de sécurité parce que le serveur maître ne parvient pas à associer l'adresse IP du tunnel HTTP à l'identité de l'hôte qui demande le certificat.

- Le rapport d'audit NetBackup répertorie le serveur de médias comme étant l'utilisateur si un tunnel HTTP est utilisé pour envoyer une demande de certificat au serveur maître.

Ajout manuel d'un hôte NetBackup

Il est déconseillé d'ajouter manuellement un hôte dans la base de données d'hôtes, sauf pour des scénarios spécifiques. Par exemple, vous pouvez ajouter manuellement un hôte lorsque vous récupérez un client Bare Metal Restore (BMR) dans un autre domaine NetBackup à l'aide de Auto Image Replication (AIR).

Pour plus d'informations sur Bare Metal Restore, consultez le *Guide de l'administrateur de NetBackup Bare Metal Restore*.

Remarque : Avant d'ajouter un hôte, vous devez vous assurer que l'entrée d'hôte que vous voulez ajouter n'existe pas déjà dans la base de données hôte.

Vous pouvez ajouter un hôte à l'aide de l'interface de ligne de commande uniquement.

Pour ajouter un hôte à la base de données hôte à l'aide de l'interface de ligne de commande

1. Exécutez la commande suivante pour authentifier votre connexion aux services web sur le serveur maître :

   ```
   bpnbat -login -loginType WEB
   ```

2. Exécutez la commande suivante pour ajouter un hôte :

   ```
   nbhostmgmt -addhost -host host name -server master server
   ```

Migration de l'autorité de certification NetBackup

Dans certains cas, vous devrez peut-être migrer votre hiérarchie d'autorité de certification NetBackup existante vers une nouvelle hiérarchie. NetBackup prend en charge la migration de l'autorité de certification NetBackup existante. Ce chapitre fournit des informations sur le processus de migration de l'autorité de certification NetBackup.

Les certificats de sécurité NetBackup permettant d'authentifier des hôtes NetBackup sont conformes à la norme pour les infrastructures à clés publiques X.509. Un

serveur maître NetBackup agit en tant qu'autorité de certification (AC) et émet des certificats numériques pour les hôtes. NetBackup utilise le daemon d'authentification NetBackup (NBATD) comme fournisseur d'infrastructure à clés publiques. NBATD et son implémentation client génèrent la clé privée RSA utilisée pour l'authentification.

NetBackup prend désormais en charge les autorités de certification avec les puissances de clé suivantes : 2 048 bits, 3 072 bits, 4 096 bits, 8 192 bits et 16 384 bits.

Remarque : Après l'installation ou la mise à niveau du serveur principal NetBackup, une nouvelle autorité de certification racine avec une puissance de clé de 2 048 bits est déployée par défaut. Lors de la mise à niveau, vous devez migrer l'autorité de certification existante vers une nouvelle autorité de certification.

Tableau 15-10 Procédures de migration de l'autorité de certification NetBackup pour divers cas d'utilisation

Cas d'utilisation	Description
Si vous avez besoin d'une autorité de certification NetBackup avec une puissance de clé autre que celle par défaut (2 048 bits)	Se reporter à "Définition de la puissance de clé requise avant l'installation ou la mise à niveau à l'aide de la variable d'environnement NB_KEYSIZE" à la page 389. Se reporter à "Migration manuelle de l'autorité de certification NetBackup après l'installation ou la mise à niveau" à la page 392.
Si vous souhaitez migrer l'autorité de certification NetBackup existante après la mise à niveau de l'ensemble du domaine NetBackup vers la version 8.3	Se reporter à "Migration de l'autorité de certification NetBackup lorsque l'ensemble du domaine NetBackup est mis à niveau" à la page 390.

Le processus de migration de l'autorité de certification NetBackup comprend les phases suivantes :

1. Lancement de la migration de l'autorité de certification NetBackup

Remarque : Si NetBackup Access Control (NBAC) est activé sur le serveur maître NetBackup, OpsCenter doit rétablir la relation de confiance avec le serveur maître après la migration de l'autorité de certification. Exécutez la commande suivante :

```
vssat setuptrust --broker nb_master_server_name:1556:nbatd
--securitylevel high
```

Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

La commande `vssat` se trouve à l'emplacement suivant :

Windows	*INSTALL_PATH*\NetBackup\sec\at\bin\vssat
UNIX	/usr/openv/netbackup/sec/at/bin

2. Activation de la nouvelle autorité de certification NetBackup
3. Fin de la migration de l'autorité de certification NetBackup
4. Mise hors service de l'ancienne autorité de certification NetBackup

Remarque : La désactivation de l'ancienne autorité de certification NetBackup est une tâche de nettoyage facultative.

Pour plus d'informations, consultez la vidéo sur la *migration de l'autorité de certification NetBackup*.

Définition de la puissance de clé requise avant l'installation ou la mise à niveau à l'aide de la variable d'environnement NB_KEYSIZE

Après l'installation ou la mise à niveau de NetBackup, une nouvelle autorité de certification racine avec une puissance de clé de 2 048 bits est déployée par défaut. Si vous souhaitez une plus grande puissance de clé, vous pouvez définir une variable d'environnement sur une valeur supérieure à 2 048 bits avant l'installation ou la mise à niveau.

Pour disposer d'une autorité de certification NetBackup avec une puissance de clé supérieure à 2 048 bits

1. Définissez la variable d'environnement `NB_KEYSIZE` sur le serveur maître avant de lancer l'installation ou la mise à niveau de NetBackup.

   Par exemple : `NB_KEYSIZE = 4096`

   La variable d'environnement `NB_KEYSIZE` peut avoir les valeurs suivantes : 2 048, 3 072, 4 096, 8 192 ou 16 384.

   Remarque : Si le mode FIPS est activé sur le serveur principal, vous pouvez uniquement spécifier la valeur 2 048 ou 3 072 bits pour la variable d'environnement `NB_KEYSIZE`.

   Attention : Vous devez soigneusement choisir la taille de clé pour votre environnement. Une taille de clé volumineuse peut réduire les performances. Une taille de clé de 2 048 bits offre une sécurité suffisante dans la plupart des cas d'utilisation.

2. Installez ou mettez à niveau NetBackup sur les hôtes.

   Dans le cas d'une mise à niveau, continuez la migration de l'autorité de certification.

   Se reporter à "Migration de l'autorité de certification NetBackup lorsque l'ensemble du domaine NetBackup est mis à niveau" à la page 390.

Migration de l'autorité de certification NetBackup lorsque l'ensemble du domaine NetBackup est mis à niveau

Avec la mise à niveau vers NetBackup 8.3, par défaut, une nouvelle autorité de certification racine avec une puissance de clé de 2 048 bits est déployée et le processus de migration de l'autorité de certification est lancé automatiquement. Vous pouvez également définir la variable d'environnement `NB_KEYSIZE` sur une valeur supérieure à 2 048 bits avant l'installation ou la mise à niveau.

Se reporter à "Définition de la puissance de clé requise avant l'installation ou la mise à niveau à l'aide de la variable d'environnement NB_KEYSIZE" à la page 389.

Remarque : Si vous disposez de serveurs de médias dotés d'une version de NetBackup antérieure à la version 8.2 et configurés comme serveurs de stockage en cloud, le processus de migration de l'autorité de certification n'est pas lancé. Assurez-vous que tous les hôtes NetBackup sont mis à niveau vers la version 8.3 ou une version ultérieure pour que la communication avec l'hôte puisse être établie correctement.

Lorsque tous les hôtes de votre domaine NetBackup sont mis à niveau vers NetBackup 8.3 ou une version ultérieure, utilisez la procédure suivante pour terminer le processus de migration de l'autorité de certification :

Pour migrer l'autorité de certification NetBackup lorsque tous les hôtes sont mis à niveau vers NetBackup 8.3

1. Exécutez la commande suivante pour vous assurer que tous les hôtes disposent des nouveaux certificats de l'autorité de certification dans leurs magasins d'approbation.

   ```
   nbseccmd -nbcaMigrate -hostsPendingTrustPropagation
   ```

2. Assurez-vous que la commande renvoie zéro (`0`) hôtes comme sortie.

   Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

3. **Avertissement :** Si un ou plusieurs hôtes NetBackup disposent de la version 8.2 ou d'une version antérieure, les sauvegardes de ces hôtes échoueront après l'activation. Par conséquent, vous devez vous assurer que tous les hôtes NetBackup du domaine sont mis à niveau vers la version 8.3 avant d'activer la nouvelle autorité de certification.

   Exécutez la commande suivante pour activer la nouvelle autorité de certification qui peut désormais commencer à émettre des certificats NetBackup :

   ```
   nbseccmd -nbcaMigrate -activateNewCA
   ```

4. Exécutez la commande suivante pour vous assurer que tous les hôtes disposent de certificats renouvelés par la nouvelle autorité de certification :

   ```
   nbseccmd -nbcaMigrate -hostsPendingRenewal
   ```

   Assurez-vous que la commande renvoie zéro (`0`) hôtes comme sortie.

5. Redémarrez le service NetBackup Messaging Broker (`nbmqbroker`) sur cet hôte.

6 Exécutez la commande suivante pour terminer le processus de migration de l'autorité de certification :

```
nbseccmd -nbcaMigrate -completeMigration
```

7 Après avoir terminé le processus de migration de l'autorité de certification NetBackup et vérifié que les hôtes utilisent des certificats émis par la nouvelle autorité de certification, vous pouvez mettre hors service l'ancienne autorité de certification NetBackup en toute sécurité.

Cette tâche de nettoyage est facultative.

Se reporter à "Mise hors service de l'autorité de certification NetBackup inactive " à la page 395.

Migration manuelle de l'autorité de certification NetBackup après l'installation ou la mise à niveau

Après l'installation ou la mise à niveau de NetBackup, une nouvelle autorité de certification racine avec une puissance de clé de 2 048 bits est déployée par défaut. Cependant, si vous souhaitez utiliser une autorité de certification avec une autre taille de clé ou passer à une nouvelle autorité de certification après l'installation ou la mise à niveau, vous devez lancer manuellement le processus de migration de l'autorité de certification.

Se reporter à "Définition de la puissance de clé requise avant l'installation ou la mise à niveau à l'aide de la variable d'environnement NB_KEYSIZE" à la page 389.

Pour migrer l'autorité de certification NetBackup après l'installation ou la mise à niveau

1 Exécutez la commande suivante pour lancer le processus de migration de l'autorité de certification :

```
nbseccmd -nbcaMigrate -initiateMigration -keysize key_value
```

Une nouvelle autorité de certification NetBackup est déployée avec cette commande.

Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

2 Exécutez la commande suivante pour renouveler des certificats sur l'hôte.

```
nbcertcmd -reissueCertificates
```

3 Arrêtez le service NetBackup Web Management Console (`nbwmc`) avant de renouveler le certificat sur le serveur Web NetBackup.

4. Exécutez la commande suivante pour renouveler le certificat sur le serveur Web NetBackup :

   ```
   configureCerts -renew_webserver_keys
   ```

5. Démarrez le service `nbwmc`.

6. Exécutez la commande suivante pour vous assurer que tous les hôtes disposent des nouveaux certificats de l'autorité de certification dans leurs magasins d'approbation.

   ```
   nbseccmd -nbcaMigrate -hostsPendingTrustPropagation
   ```

7. Assurez-vous que la commande renvoie zéro (`0`) hôtes comme sortie.

8. **Avertissement :** Si un ou plusieurs hôtes NetBackup disposent de la version 8.2 ou d'une version antérieure, les sauvegardes de ces hôtes échoueront après l'activation. Par conséquent, vous devez vous assurer que tous les hôtes NetBackup du domaine sont mis à niveau vers la version 8.3 avant d'activer la nouvelle autorité de certification.

   Exécutez la commande suivante pour activer la nouvelle autorité de certification qui peut désormais commencer à émettre des certificats NetBackup :

   ```
   nbseccmd -nbcaMigrate -activateNewCA
   ```

9. Exécutez la commande suivante pour renouveler des certificats d'hôte à l'aide de la nouvelle autorité de certification.

   ```
   nbcertcmd -renewCertificate
   ```

10. Exécutez la commande suivante pour vous assurer que tous les hôtes disposent de certificats renouvelés par la nouvelle autorité de certification :

    ```
    nbseccmd -nbcaMigrate -hostsPendingRenewal
    ```

    Assurez-vous que la commande renvoie zéro (`0`) hôtes comme sortie.

11. Redémarrez le service NetBackup Messaging Broker (`nbmqbroker`) sur cet hôte.

12 Exécutez la commande suivante pour terminer le processus de migration de l'autorité de certification :

```
nbseccmd -nbcaMigrate -completeMigration
```

13 Après avoir terminé le processus de migration de l'autorité de certification NetBackup et vérifié que les hôtes utilisent des certificats émis par la nouvelle autorité de certification, vous pouvez mettre hors service l'ancienne autorité de certification NetBackup en toute sécurité.

Cette tâche de nettoyage est facultative.

Se reporter à "Mise hors service de l'autorité de certification NetBackup inactive " à la page 395.

Établissement de la communication avec les clients ne disposant pas de certificats d'autorité de certification après la migration de l'autorité de certification

Dans certains cas, par exemple lors d'un problème de réseau, les clients NetBackup peuvent être inaccessibles lors de la migration de l'autorité de certification NetBackup. Ces clients ne peuvent pas obtenir de nouveaux certificats d'autorité de certification et la communication avec ces clients peut échouer.

Pour communiquer avec des clients NetBackup inaccessibles lors de la migration de l'autorité de certification

1 Exécutez la commande suivante sur le client pour obtenir un certificat :

```
nbcertcmd -getcacertificate -server master_server_name
```

2 Exécutez la commande suivante sur le client pour renouveler les certificats :

```
nbcertcmd -renewcertificate -server master_server_name
```

Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

Affichage d'une liste des autorités de certification NetBackup dans le domaine

Vous pouvez afficher une liste des autorités de certification NetBackup disponibles dans votre domaine NetBackup.

Pour afficher la liste des autorités de certification NetBackup dans le domaine

- Exécutez la commande suivante :

```
nbseccmd -nbcaList
```

Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

Si vous souhaitez afficher des autorités de certification présentant un état spécifique (par exemple, ABANDONED, ACTIVE ou DECOMMISSIONED), exécutez la commande suivante :

```
nbseccmd -nbcaList -state CA_state]
```

Affichage du résumé de migration de l'autorité de certification

Vous pouvez afficher le résumé de migration de l'autorité de certification NetBackup à différentes étapes. Les informations figurant dans le résumé de migration de l'autorité de certification incluent l'état actuel de la migration de l'autorité de certification et la signature de l'autorité de certification NetBackup émettrice de certificats actuelle.

Pour afficher le résumé de migration de l'autorité de certification

- Exécutez la commande suivante :

  ```
  nbseccmd -nbcaMigrate -summary
  ```

  Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

Mise hors service de l'autorité de certification NetBackup inactive

Après avoir terminé le processus de migration de l'autorité de certification NetBackup et vérifié que les hôtes utilisent des certificats émis par la nouvelle autorité de certification, vous pouvez mettre hors service l'ancienne autorité de certification NetBackup en toute sécurité.

Pour mettre hors service l'ancienne autorité de certification NetBackup

1. Exécutez la commande suivante :

   ```
   nbseccmd -nbcaMigrate -decommissionCA -fingerprint
   certificate_fingerprint
   ```

   Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

2. Cette étape est obligatoire si votre domaine NetBackup est activé pour NetBackup Access Control (NBAC) ou l'audit amélioré (EA) :

   Redémarrez les services NetBackup sur le serveur maître.

Chapitre 16

Configuration du chiffrement des données en transit (DTE)

Ce chapitre traite des sujets suivants :

À propos du canal de données

La communication de données comprend les données sauvegardées à l'aide de NetBackup. Les politiques de sécurité exigent que les administrateurs de sauvegarde

s'assurent que le canal sur lequel les clients NetBackup envoient des métadonnées et des données aux serveurs NetBackup est sécurisé. Dans NetBackup 10.0 et les versions ultérieures, les données et métadonnées sont chiffrées sur le réseau. Cette fonction est appelée « chiffrement du canal de données » ou « chiffrement des données en transit » (DTE).

Les canaux suivants sont classés en tant que canaux de données :

- Flux TAR (client vers serveur de médias) : canal sur lequel le flux TAR/flux de données circule entre le client et le serveur de médias. Lors d'une opération de sauvegarde, le serveur de médias reçoit les données du client et les envoie au stockage (par exemple, via un plug-in OST). Le sens est inversé lors d'une restauration.
- Flux TAR (serveur de médias vers serveur de médias) : canal utilisé lors de la duplication.
- Informations de catalogue (client vers serveur de médias) : canal sur lequel les informations du catalogue et les commandes de contrôle circulent entre le client et le serveur de médias. Le volume de données transmises sur ce canal est proportionnel au nombre de fichiers et de répertoires sauvegardés. Le serveur de médias envoie au serveur principal les informations du catalogue transmises par le client.
- Informations du catalogue (serveur de médias vers serveur principal) : canal sur lequel les informations du catalogue circulent du serveur de médias vers le serveur principal.

Remarque : Après l'installation ou la mise à niveau vers NetBackup 10.0, le chiffrement des données en transit est désactivé par défaut. Cependant, vous pouvez configurer le chiffrement des données en transit à différents niveaux : niveau global (serveur principal) et niveau client.

Prise en charge du chiffrement des données en transit

Le chiffrement des données en transit est pris en charge pour les opérations de données et de métadonnées NetBackup suivantes :

- Flux de données d'un client vers un serveur de médias
- Flux de données d'un serveur de médias vers un client
- Transfert de métadonnées d'un serveur de médias vers le serveur principal

- Flux de données d'un serveur de médias à l'autre lors de la duplication et de la sauvegarde synthétique

Le chiffrement des données en transit n'est pas pris en charge pour les opérations ou communications NetBackup suivantes :

- La communication entre un plug-in OST et le fournisseur de stockage sous-jacent n'est pas prise en charge. Elle comprend les éléments suivants :
  - Communication entre NetBackup et le stockage en cloud
  - Communication entre NetBackup et les fournisseurs OST tiers tels que DataDomain, NetApp, etc.
- Le chiffrement des données en transit n'est pas pris en charge pour les workflows MSDP suivants :
  - Duplication optimisée
  - Réplication AIR

  Pour ces deux opérations, vous devez explicitement configurer l'option suivante sur les deux serveurs de stockage :

  `OPTDUP_ENCRYPTION=1`

  La configuration DTE dans NetBackup ne contrôle pas le canal de données entre deux serveurs de stockage.
- La communication entre NetBackup et des applications de charge de travail telles que VMware, Hyper-V, Microsoft Exchange, Sharepoint, Nutanix et OpsCenter n'est pas prise en charge.
  Lors du transfert des données depuis une application de charge de travail vers NetBackup, les processus NetBackup transfèrent les données de manière sécurisée sur le canal TLS.
- Communication NDMP
- Communication du client SAN
- Communication avec le processus NBFSD
  Le processus utilise le protocole NFS ou CIFS standard.

Workflow de configuration du chiffrement des données en transit

Cette rubrique décrit la marche à suivre pour procéder au chiffrement des données en transit (DTE) dans votre environnement NetBackup. La configuration DTE comprend les 2 options principales suivantes :

- Mode DTE global

- Mode DTE client

Tableau 16-1 Workflow de configuration DTE

Numéro d'étape	Étape	Rubrique de référence
Étape 1	Examinez les paramètres de configuration de l'option de mode DTE global, et configurez-les selon vos besoins.	Se reporter à "Configuration du paramètre global de chiffrement des données en transit" à la page 400.
Étape 2	Examinez les paramètres de configuration de l'option de mode DTE client, et configurez-les selon vos besoins.	Se reporter à "Configuration du mode DTE sur un client" à la page 401.
Étape 3	Passez en revue la manière dont le chiffrement des données est défini en fonction de l'opération NetBackup que vous souhaitez exécuter et des paramètres de configuration DTE.	Se reporter à "Fonctionnement des paramètres de configuration DTE dans différentes opérations NetBackup" à la page 410. **Remarque :** Si vous prévoyez de modifier des paramètres de configuration DTE existants, examinez cette rubrique pour comprendre leur impact sur les opérations NetBackup.

Mis à part les paramètres principaux de configuration DTE, les paramètres suivants sont utilisés dans certains scénarios :

- Mode DTE du serveur de médias
  Se reporter à "Configuration du mode DTE sur le serveur de médias" à la page 405.
- Mode DTE d'image de sauvegarde
  Se reporter à "Modification du mode DTE d'une image de sauvegarde" à la page 406.
  Se reporter à "DTE_IGNORE_IMAGE_MODE pour les serveurs NetBackup" à la page 407.

Configuration du paramètre global de chiffrement des données en transit

Pour configurer le chiffrement des données en transit (DTE) dans votre environnement NetBackup, vous devez tout d'abord définir les paramètres globaux de configuration DTE (ou mode DTE global), puis le mode DTE client.

Le chiffrement des données en transit pour différentes opérations NetBackup est défini en fonction du mode DTE global, du mode DTE client et du mode DTE d'image.

Les valeurs prises en charge pour le mode DTE global sont les suivantes :

- `Preferred Off` (par défaut) : spécifie que le chiffrement des données en transit est désactivé dans le domaine NetBackup. Ce paramètre peut être écrasé par le paramètre du client NetBackup.
- `Preferred On` : spécifie que le chiffrement des données en transit est activé uniquement pour les clients NetBackup 9.1 et versions ultérieures.
  Ce paramètre peut être écrasé par le paramètre du client NetBackup.
- `Enforced` : spécifie que le chiffrement des données en transit s'applique si le paramètre du client NetBackup est défini sur "Automatique" ou "Activé". Lorsque cette option est sélectionnée, les travaux échouent pour les clients NetBackup pour lesquels le chiffrement des données en transit est défini sur "Désactivé" et pour les hôtes exécutant une version antérieure à la version 9.1.

Remarque : Par défaut, le mode DTE pour les clients 9.1 est défini sur `Off`, et sur `Automatic` pour les clients 10.0 et versions ultérieures.

Se reporter à "DTE_CLIENT_MODE pour les clients" à la page 401.

API RESTful à utiliser pour la configuration DTE globale :

- GET - /security/properties
- POST - /security/properties

Pour définir ou afficher le mode DTE global à l'aide de l'interface utilisateur Web NetBackup

1. Connectez-vous à l'interface utilisateur Web NetBackup.
2. En haut à droite, sélectionnez **Sécurité > Sécurité globale**.
3. Dans l'onglet **Communication sécurisée**, sélectionnez l'un des paramètres DTE globaux suivants :
   - `Preferred Off`

- `Preferred On`
- `Enforced`

Pour définir et afficher le mode DTE global à l'aide de l'interface de ligne de commande

1. Exécutez la commande suivante pour définir le mode DTE global :

   ```
   nbseccmd -setsecurityconfig -dteglobalmode 0|1|2
   ```

   Où la valeur `0` représente `Preferred Off`, `1` représente `Preferred On` et `2` représente `Enforced`.

2. Exécutez la commande suivante pour afficher la valeur définie pour le mode DTE global :

   ```
   nbseccmd -getsecurityconfig -dteglobalmode
   ```

Configuration du mode DTE sur un client

L'option de configuration `DTE_CLIENT_MODE` spécifie le mode de chiffrement des données en transit (DTE) défini sur le client NetBackup.

Se reporter à "DTE_CLIENT_MODE pour les clients" à la page 401.

Vous pouvez mettre à jour et afficher le mode DTE client à l'aide des commandes suivantes :

`bpsetconfig`/`nbsetconfig` et `bpgetconfig`/`nbgetconfig`

DTE_CLIENT_MODE pour les clients

L'option `DTE_CLIENT_MODE` spécifie le mode de chiffrement des données en transit (DTE) défini sur le client NetBackup.

Tableau 16-2 Informations de DTE_CLIENT_MODE

Utilisation	Description
Où l'utiliser	Sur les clients NetBackup.

Utilisation	Description
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations sur ces commandes, consultez le Guide de référence des commandes NetBackup. Utilisez le format suivant : `DTE_CLIENT_MODE = AUTOMATIC | ON | OFF` Le mode DTE est défini par défaut sur `OFF` pour les clients 9.1 et sur `AUTOMATIC` pour les clients 10.0 et versions ultérieures. ■ Si l'option `DTE_CLIENT_MODE` est définie sur `AUTOMATIC`, le client suit le mode DTE défini au niveau global : `Enforced`, `Preferred On` ou `Preferred Off`. ■ Si l'option est définie sur `ON`, le chiffrement des données en transit est activé pour le client. ■ Si l'option est définie sur `OFF`, le chiffrement des données en transit est désactivé pour le client. Ce paramètre peut être utilisé pour exclure un client du chiffrement si le mode DTE global est défini sur `Preferred On`. **Remarque :** Si le mode DTE global est défini sur `Enforced`, les travaux échouent pour les clients NetBackup pour lesquels l'option `DTE_CLIENT_MODE` est désactivée et pour les hôtes dont la version est antérieure à la 9.1.
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

Affichage du mode DTE d'un travail NetBackup

Le rôle principal du mode DTE global et du mode DTE client est de déterminer si les données en transit sont chiffrées pour une opération NetBackup. Si les données sont chiffrées lors de l'exécution d'un travail NetBackup, l'attribut "Mode DTE" du travail est défini sur `On`.

Si les données ne sont pas chiffrées lors de l'exécution d'un travail NetBackup, l'attribut "Mode DTE" du travail est défini sur `Off`.

API RESTful pour afficher le mode DTE d'un travail :

- GET - /admin/jobs

- GET - /admin/jobs/{jobId}

Pour afficher le mode DTE d'un travail à l'aide de l'interface utilisateur Web NetBackup

1. Connectez-vous à l'interface utilisateur Web NetBackup.
2. Sur la gauche, sélectionnez **Moniteur d'activité > Travaux**.

   La colonne `Data-in-transit encryption` affiche le mode DTE défini pour le travail.

Pour afficher le mode DTE d'un travail à l'aide de l'interface de ligne de commande

- Exécutez la commande suivante :

  ```
  bpdbjobs -dtemode Off|On
  ```

  La commande répertorie les travaux en fonction du mode DTE défini.

Affichage des attributs DTE d'une image NetBackup et d'une copie d'image

Le rôle principal du mode DTE global et du mode DTE client est de déterminer si les données en transit sont chiffrées pour une opération de sauvegarde. Si les données sont chiffrées lors d'une opération de sauvegarde, l'attribut de mode DTE de l'image NetBackup associée est défini sur `On`.

Si le mode DTE d'image est basé sur le mode DTE global et le mode DTE client, les données ne peuvent pas être chiffrées, et l'attribut de mode DTE de l'image est défini sur `Off`.

Se reporter à "Modification du mode DTE d'une image de sauvegarde" à la page 406.

Une copie d'image comporte deux attributs DTE :

Mode DTE de copie	Spécifie si les données sont transférées sur un canal sécurisé lors de la copie de l'image actuelle.

Mode DTE hiérarchique de copie	Spécifie si les données sont transférées sur un canal sécurisé lors de la copie de l'image actuelle et de ses copies parentes dans la hiérarchie. Si les données sont transférées sur un canal non sécurisé lors de la création de l'une des copies parentes dans la hiérarchie, le mode DTE hiérarchique de la copie actuelle est défini sur `Off`. Si le mode DTE hiérarchique de la copie est défini sur `Off`, la copie est considérée comme non sécurisée. Cela signifie que n'importe quelle copie parente peut être compromise et que la copie d'une copie compromise n'est pas sécurisée, même si la copie actuelle est générée de façon sécurisée.

Remarque : Le mode DTE d'image apparaît toujours `Off` si le serveur de médias exécute une version antérieure à la version 9.1. Les options Mode DTE de copie et Mode DTE hiérarchique de copie sont toujours définies sur `Off` si le serveur de médias exécute une version antérieure à la version 10.0.

API RESTful à utiliser pour afficher les attributs d'image :

- GET - /catalog/images
- GET - /catalog/images/{backupId}

Pour afficher les attributs DTE d'une image et de sa copie à l'aide de l'interface utilisateur Web NetBackup

1. Connectez-vous à l'interface utilisateur Web NetBackup.
2. Sur la gauche, sélectionnez **Catalogue**.

   Lorsque vous recherchez des images de sauvegarde, la liste d'images s'affiche au bas de l'écran. Les attributs DTE de l'image et de sa copie (Mode DTE d'image, Mode DTE de copie et Mode DTE hiérarchique de copie) sont également affichés.

Pour afficher les attributs DTE d'une image et de sa copie à l'aide de l'interface de ligne de commande

- Exécutez les commandes suivantes : `bpimagelist`, `bpclimagelist` et `bpimmedia`.

  Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

Pour afficher les attributs DTE d'une image à l'aide de la console d'administration NetBackup

- Dans la **console d'administration NetBackup**, consultez les rapports suivants pour vérifier le mode DTE (colonne Chiffrement des données en transit) de l'image :
  - **Gestion de NetBackup > Rapports > Images sur média**
  - **Gestion de NetBackup > Rapports > Rapports sur les bandes > Images sur bande**
  - **Gestion de NetBackup > Rapports > Rapports sur les disques > Images sur disque**

Configuration du mode DTE sur le serveur de médias

Le paramètre du serveur de médias peut uniquement être utilisé pour désactiver le chiffrement des données en transit (DTE) pour les opérations NetBackup.

Dans une configuration NetBackup dans laquelle le serveur de médias est anormalement lent en raison de l'ancienneté du matériel, vous pouvez désactiver le mode DTE du serveur de médias afin d'éviter tout problème de performances. Il est toutefois recommandé de mettre à niveau le matériel ancien du serveur de médias. Ce paramètre est disponible pour les serveurs de médias exécutant NetBackup 10.0 ou une version ultérieure.

API RESTful à utiliser pour la configuration DTE globale :

- GET - /config/media-servers/{hostName}
- PATCH - /config/media-servers/{hostName}

Pour définir ou afficher le mode DTE du serveur de médias

1. Assurez-vous de disposer d'un rôle RBAC avec les autorisations suivantes sur la ressource de serveur de médias :
   - Afficher
   - Mettre à jour
   - Gérer l'accès

Se reporter à " Rôles RBAC par défaut " à la page 155.

2. Exécutez la commande suivante pour définir le mode DTE du serveur de médias :

```
nbseccmd -setsecurityconfig -dtemediamode off|on -mediaserver
media_server_name
```

3. Exécutez la commande suivante pour afficher le mode DTE du serveur de médias :

```
nbseccmd -getsecurityconfig -dtemediamode -mediaserver
media_server_name
```

Remarque : Pour les serveurs de médias 9.1, vous pouvez uniquement afficher le mode DTE défini comme `On`, mais vous ne pouvez pas le définir.

Modification du mode DTE d'une image de sauvegarde

La fonction de chiffrement des données en transit (DTE) de NetBackup introduit un attribut d'image supplémentaire (le mode DTE) lorsqu'une image de sauvegarde est créée.

Le rôle principal du mode DTE global et du mode DTE client est de déterminer si les données en transit sont chiffrées pour une opération NetBackup. Si les données sont chiffrées lors d'une sauvegarde, l'attribut de mode DTE de l'image NetBackup associée est défini sur `On`.

Si le mode DTE d'image est basé sur le mode DTE global et le mode DTE client, les données ne peuvent pas être chiffrées lors de la sauvegarde, et l'attribut de mode DTE de l'image est défini sur `Off`.

Le mode DTE de l'image doit être appliqué et conservé pour toutes les opérations ultérieures sur cette image (par exemple, les opérations de restauration ou des opérations secondaires telles que la duplication, la réplication, l'importation, etc.). Si le mode DTE d'image est défini sur Activé, les données seront toujours chiffrées lors d'opérations ultérieures pour les hôtes prenant en charge le chiffrement des données en transit.

Si l'hôte ne prend pas en charge le chiffrement de données en transit, le travail échouera. Si le mode DTE d'image est défini sur Désactivé, l'application du chiffrement des donnés en transit lors d'opérations ultérieures dépendra des

modes DTE global et client définis lors des opérations. Il s'agit du comportement par défaut.

Dans certains cas, vous pouvez modifier le mode DTE d'image défini lors de la création de l'image de sauvegarde.

Pour modifier le mode DTE d'image

- Exécutez la commande suivante :

  ```
  bpimage -update -image_dtemode Off|On
  ```

  Vous pouvez également modifier le mode DTE d'image en accédant au nœud **Catalogue** de l'interface utilisateur Web NetBackup.

Se reporter à "DTE_IGNORE_IMAGE_MODE pour les serveurs NetBackup" à la page 407.

Se reporter à "Affichage des attributs DTE d'une image NetBackup et d'une copie d'image" à la page 403.

DTE_IGNORE_IMAGE_MODE pour les serveurs NetBackup

Utilisez l'option `DTE_IGNORE_IMAGE_MODE` si vous ne souhaitez pas que les données soient chiffrées même si le mode de chiffrement des données en transit (DTE) de l'image de sauvegarde est activé.

L'option `DTE_IGNORE_IMAGE_MODE` s'applique à toutes les images de sauvegarde.

Tableau 16-3 Informations sur DTE_IGNORE_IMAGE_MODE

Utilisation	Description
Où l'utiliser	Sur les serveurs NetBackup.

Utilisation	Description
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations sur ces commandes, consultez le Guide de référence des commandes NetBackup. Utilisez le format suivant : `DTE_IGNORE_IMAGE_MODE = NEVER | ALWAYS | WHERE_UNSUPPORTED` La valeur par défaut de l'option `DTE_IGNORE_IMAGE_MODE` est `NEVER`. ■ `NEVER` - Utilisez cette option pour spécifier que le chiffrement des données en transit s'applique en fonction du mode DTE de l'image. ■ `ALWAYS` - Utilisez cette option pour spécifier que le mode DTE de l'image est toujours ignoré lors du chiffrement des données en transit, que l'hôte NetBackup prenne en charge le chiffrement ou non. Le chiffrement des données en transit dépend du mode DTE global et du mode DTE du client. ■ `WHERE_UNSUPPORTED` - Utilisez cette option si votre environnement comporte des hôtes NetBackup antérieurs à la version 9.1 et si vous ne souhaitez pas que les travaux échouent pour ces hôtes lorsque le mode DTE est activé pour l'image. Avec cette configuration, le chiffrement des données en transit dépend des paramètres de mode DTE global et du client. Le mode DTE de l'image est ignoré.
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

Sélection des périphériques de médias (MDS) et allocation des ressources

Les ressources sont allouées en fonction du mode DTE global, du mode DTE client, du mode DTE du serveur de médias et du mode DTE d'image. Pour les unités de stockage dynamiques, comme MSDP ou les groupes d'unités de stockage, un serveur de médias dont le mode DTE est défini sur `On` est préféré s'il s'agit d'une condition requise pour le travail.

Si le travail requiert un serveur de médias dont le mode DTE est défini sur `On`, mais qu'aucun serveur de médias de ce type n'est disponible, NetBackup revient aux allocations de ressources initialement définies.

Dans ce cas, il est possible que le travail se poursuive, puis échoue en cours d'exécution (dans `nbjm` ou `bprd`, ou dans d'autres daemons et interfaces de ligne de commande) si NetBackup détecte que le chiffrement des données en transit est requis par le serveur de médias.

Le processus suivant présente les modalités de sélection des périphériques de médias et de validation du chiffrement des données en transit :

1. Dans le cas d'une opération de sauvegarde, passez directement à l'étape 2. Pour toutes les autres opérations (restauration, duplication, réplication, importation, vérification, etc.), le mode DTE d'image source est pris en compte :
   - Si le mode DTE d'une image est défini sur `ON`, le mode DTE du serveur de médias est défini sur `ON`, indépendamment de toute autre configuration DTE.
   - Si le mode DTE d'une image est défini sur Désactivé, les modes DTE global, client et du serveur de médias sont vérifiés.
2. Si le paramètre DTE global est défini sur `ENFORCED`, un serveur de médias compatible DTE est préféré.
3. Si le paramètre DTE global est défini sur `PREFERRED ON` ou `PREFERRED OFF`, un mode DTE client est pris en considération.
   - Si le mode DTE client est défini sur `ON`, un serveur de médias compatible DTE est préféré.
   - Si le mode DTE client est défini sur `OFF`, n'importe quel serveur de médias disponible peut être sélectionné.
   - Si le mode DTE client est défini sur `Automatic`, la décision est prise en fonction du paramètre DTE global. Cela signifie que si le paramètre DTE global est défini sur `PREFERRED OFF`, n'importe quel serveur de médias disponible est sélectionné (sinon, un serveur de médias compatible DTE est sélectionné).

De nombreux paramètres jouent un rôle important dans l'allocation des ressources. Les conditions spéciales suivantes s'appliquent :

- Un nom de client vide correspond à une opération secondaire (duplication, réplication, importation, vérification, etc.). Le mode DTE d'image ou le mode DTE global sont appliqués.
- Si le nom du client est spécifié, mais ne figure pas dans la base de données de l'hôte parce que le client exécute une version antérieure à la version 8.0, le client ne prend pas en charge le chiffrement des données en transit. Par conséquent, n'importe quel serveur de médias peut être sélectionné.
- Une fois les paramètres DTE global et client vérifiés, la version du serveur de médias et le paramètre DTE de ce dernier sont vérifiés.

    - Les serveurs de médias exécutant NetBackup 9.1 ou une version ultérieure sont par défaut compatibles DTE.
- Paramètre `DTE_IGNORE_IMAGE_MODE` (pour toute opération secondaire basée sur une image)
    - Si le mode DTE d'image est défini sur `ON`, et si l'option `DTE_IGNORE_IMAGE_MODE` est appliquée, les paramètres global, client et du serveur de médias sont utilisés pour la sélection du serveur de médias.

Fonctionnement des paramètres de configuration DTE dans différentes opérations NetBackup

Cette rubrique explique comment vous pouvez modifier les paramètres de configuration DTE afin de chiffrer les données en transit pour différentes opérations NetBackup.

Passez en revue les rubriques de référence suivantes avant de modifier les paramètres de configuration DTE.

Les tableaux suivants expliquent comment le paramètre DTE (chiffrement ou non) est défini pour un workflow NetBackup donné sous différentes configurations NetBackup avec les paramètres de configuration DTE.

Sauvegarde

Dans le workflow de sauvegarde, les données sont transférées entre un serveur de médias et un client au cours d'un travail de sauvegarde.

Figure 16-1 Workflow de sauvegarde

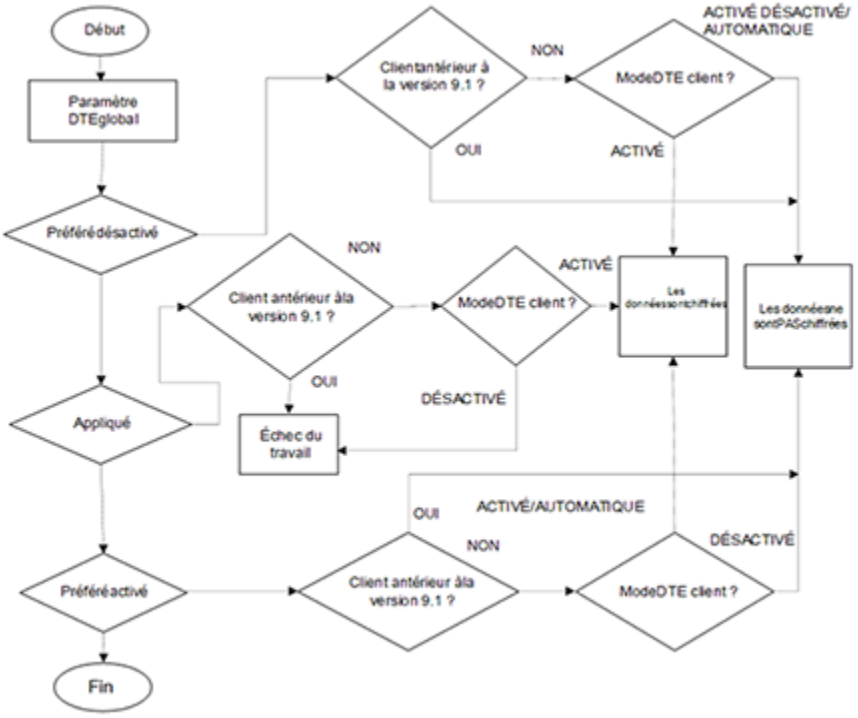


Tableau 16-4 Le mode DTE du serveur de médias est défini sur Activé (paramètre par défaut)

Mode DTE global	Mode DTE du client NetBackup 9.1 ou version ultérieure			Hôte NetBackup (serveur de médias ou client) exécutant une version antérieure à la version 9.1
	Activé	Désactivé	Automatique	
Préféré désactivé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées
Appliqué	Les données sont chiffrées	L'opération échoue	Les données sont chiffrées	L'opération échoue

Tableau 16-5 Le mode DTE du serveur de médias est défini sur Désactivé (paramètre par défaut)

Mode DTE global	Mode DTE du client NetBackup 9.1 ou version ultérieure			Hôte NetBackup (serveur de médias ou client) exécutant une version antérieure à la version 9.1
	Activé	Désactivé	Automatique	
Préféré désactivé	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	L'opération échoue	L'opération échoue	L'opération échoue	L'opération échoue

Restauration

Deux scénarios DTE sont possibles dans le workflow de restauration :

- Le mode DTE d'image est défini sur Désactivé
- Le mode DTE d'image est défini sur Activé

Quel que soit le scénario, un ou plusieurs serveurs de médias peuvent être impliqués (si plusieurs images sont sélectionnées) lors de la restauration des données sur un client pour un seul travail NetBackup.

Le mode DTE d'image est défini sur Désactivé

Tableau 16-6 Le mode DTE du serveur de médias est défini sur Activé (par défaut)

Mode DTE global	Mode DTE du client NetBackup 9.1 ou version ultérieure			Hôte NetBackup (serveur de médias ou client) exécutant une version antérieure à la version 9.1
	Activé	Désactivé	Automatique	
Préféré désactivé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées

Mode DTE global	Mode DTE du client NetBackup 9.1 ou version ultérieure			Hôte NetBackup (serveur de médias ou client) exécutant une version antérieure à la version 9.1
	Activé	Désactivé	Automatique	
Appliqué	Les données sont chiffrées	L'opération échoue	Les données sont chiffrées	L'opération échoue

Tableau 16-7 Le mode DTE du serveur de médias est défini sur Désactivé

Mode DTE global	Mode DTE du client NetBackup 9.1 ou version ultérieure			Hôte NetBackup (serveur de médias ou client) exécutant une version antérieure à la version 9.1
	Activé	Désactivé	Automatique	
Préféré désactivé	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	L'opération échoue	L'opération échoue	L'opération échoue	L'opération échoue

Tableau 16-8 Serveurs de médias mixtes (9.1 et 10.0 ou version ultérieure) – Media1 : mode DTE activé, Media2 : mode DTE désactivé

Mode DTE global	Mode DTE du client NetBackup 9.1 ou version ultérieure			Hôte NetBackup (serveur de médias ou client) exécutant une version antérieure à la version 9.1
	Activé	Désactivé	Automatique	
Préféré désactivé	Media1 – Les données sont chiffrées Media2 – L'opération échoue État du travail – Réussite partielle Mode DTE du travail – Activé	Media1 – Les données ne sont pas chiffrées Media2 – Les données ne sont pas chiffrées	Media1 – Les données ne sont pas chiffrées Media2 – Les données ne sont pas chiffrées	Media1 – Les données ne sont pas chiffrées Media2 – Les données ne sont pas chiffrées
Préféré activé	Media1 – Les données sont chiffrées Media2 – L'opération échoue État du travail – Réussite partielle Mode DTE du travail – Activé	Media1 – Les données ne sont pas chiffrées Media2 – Les données ne sont pas chiffrées	Media1 – Les données sont chiffrées Media2 – Les données ne sont pas chiffrées Mode DTE du travail – Désactivé	Media1 – Les données ne sont pas chiffrées Media2 – Les données ne sont pas chiffrées
Appliqué	Media1 – Les données sont chiffrées Media2 – L'opération échoue État du travail – Réussite partielle Mode DTE du travail – Activé	Media1 – L'opération échoue Media2 – L'opération échoue État du travail – Échec	Media1 – Les données sont chiffrées Media2 – L'opération échoue État du travail – Réussite partielle Mode DTE du travail – Activé	Media1 – L'opération échoue Media2 – L'opération échoue État du travail – L'opération échoue

Le mode DTE d'image est défini sur Activé

Si le mode DTE d'image est défini sur Activé, par défaut, le chiffrement des données en transit est activé par défaut pour la restauration pour les hôtes 9.1 et versions ultérieures, et le travail échoue si un hôte non pris compatible DTE est impliqué dans le workflow. Cependant, vous pouvez toujours effectuer une restauration en ignorant le mode DTE d'image.

Utilisez l'option de configuration `DTE_IGNORE_IMAGE_MODE` à définir sur le serveur principal. Valeurs possibles : `NEVER` (par défaut), `ALWAYS` et `WHERE_UNSUPPORTED`.

Tableau 16-9 Lorsque le mode DTE d'image et le mode DTE du serveur de médias sont définis sur Activé

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	**WHERE_UNSUPPORTED**	**ALWAYS**
Préféré désactivé	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Activé	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Désactivé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Automatique	Les données sont chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées
	Hôte NetBackup antérieur à la version 9.1 (serveur de médias ou client)	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Activé	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Désactivé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Automatique	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Hôte NetBackup antérieur à la version 9.1 (serveur de médias ou client)	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	**WHERE_UNSUPPORTED**	**ALWAYS**
Appliqué	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Activé	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Désactivé	L'opération échoue	L'opération échoue	L'opération échoue
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Automatique	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Hôte NetBackup antérieur à la version 9.1 (serveur de médias ou client)	L'opération échoue	L'opération échoue	L'opération échoue

Tableau 16-10 Lorsque le mode DTE d'image est défini sur Activé et le paramètre DTE du serveur de médias 10.0 et versions ultérieures est défini sur Désactivé

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Activé	L'opération échoue	L'opération échoue	L'opération échoue
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Désactivé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Automatique	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
	Hôte NetBackup antérieur à la version 9.1 (serveur de médias ou client)	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Activé	L'opération échoue	L'opération échoue	L'opération échoue
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Désactivé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Automatique	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
	Hôte NetBackup antérieur à la version 9.1 (serveur de médias ou client)	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Appliqué	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Activé	L'opération échoue	L'opération échoue	L'opération échoue
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Désactivé	L'opération échoue	L'opération échoue	L'opération échoue
	Client NetBackup 9.1 ou version ultérieure avec mode DTE défini sur Automatique	L'opération échoue	L'opération échoue	L'opération échoue
	Hôte NetBackup antérieur à la version 9.1 (serveur de médias ou client)	L'opération échoue	L'opération échoue	L'opération échoue

Remarque : Si le paramètre `DTE_IGNORE_IMAGE_MODE` est défini sur `ALWAYS`, le paramètre DTE est défini comme indiqué dans le tableau Tableau 16-7.

Sauvegarde et restauration MSDP

La fonction de chiffrement des données en transit (DTE) est désormais intégrée au serveur de stockage MSDP pour les workflows de sauvegarde et de restauration.

Pour la sauvegarde sur un pool de disques MSDP, le chiffrement du chemin d'accès des données depuis le client vers le serveur de médias est contrôlé par les paramètres DTE NetBackup (modes DTE global et client).

Si plusieurs serveurs d'équilibrage de charge sont connectés au serveur de stockage MSDP, le serveur de stockage et les serveurs de médias d'équilibrage de charge doivent exécuter la version 10.0 ou une version ultérieure pour chiffrer correctement les données en transit. Si certains de ces serveurs exécutent une version antérieure à la version 10.0, les données peuvent circuler sous forme de texte brut et le travail aboutira toujours, même si le chiffrement des données en transit n'a pas été appliqué.

Dans un environnement mixte où le serveur de stockage ou l'un des serveurs de médias d'équilibrage de charge exécute une version antérieure à la version 10.0, la configuration suivante sera requise pour appliquer le chiffrement de bout en bout :

- Le chiffrement des données en transit doit être activé côté NetBackup conformément aux configurations DTE (paramètres globaux/client/du serveur de médias).
- Le chiffrement doit être activé côté MSDP à l'aide de l'indicateur ENCRYPTION dans le fichier pd.conf.
  Consultez le *Guide de déduplication NetBackup* pour plus de détails sur l'activation du chiffrement à l'aide de MSDP.

Remarque : Si le chiffrement des données en transit est activé dans NetBackup, mais que l'indicateur `ENCRYPTION` dans `pd.conf` n'est pas activé, le chemin d'accès des données depuis le serveur de médias d'équilibrage de charge vers le serveur de stockage n'est pas chiffré. Le mode DTE du travail et le mode DTE d'image peuvent toutefois être activés.

Si le chiffrement des données en transit est activé dans NetBackup et que l'indicateur `ENCRYPTION` dans `pd.conf` est également activé, le chiffrement MSDP a la priorité sur le chiffrement des données en transit NetBackup. Les données au repos sont alors chiffrées, mais pas les données en transit.

Sauvegarde de politique Universal-Share

Pour le type de politique Universal-Share, la sélection de client peut être le nom du serveur de stockage sur lequel le partage universel réside ou le nom d'hôte sur lequel le partage universel est monté. Ainsi, le client pour ce type de politique peut être un hôte sur lequel le logiciel client NetBackup n'est pas installé.

En raison de cette limitation, NetBackup ne peut pas vérifier le mode DTE client. Il vérifie le mode DTE global et le mode DTE du serveur de médias pour la sauvegarde de politique Universal-Share et fonctionne conformément au tableau suivant :

Tableau 16-11 DTE pour la sauvegarde de politique Universal-Share

Mode DTE global	Mode DTE du serveur de médias 9.1 ou version ultérieure		Serveur de médias exécutant une version antérieure à la version 9.1
	Activé	Désactivé	
Préféré désactivé	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	Les données sont chiffrées	L'opération échoue	L'opération échoue

Sauvegarde et récupération de catalogue

Le serveur de médias doit exécuter la même version de NetBackup que le serveur principal pour le workflow de sauvegarde et de récupération de catalogue.

Passez en revue les points suivants :

- Le mode DTE pour les travaux de sauvegarde de catalogue est semblable au workflow de système de fichiers et la manière dont le chiffrement des données en transit est défini est semblable au workflow de sauvegarde décrit ci-dessus.
- Mode DTE des travaux de sauvegarde de catalogue :
  - Aucun mode DTE n'est défini pour le travail de sauvegarde de catalogue parent.
  - Aucun mode DTE n'est défini pour le travail enfant intermédiaire de base de données.
  - Le mode DTE de deux autres travaux enfants est défini en fonction des paramètres DTE configurés.
- Mode DTE des travaux de récupération de catalogue :
  - Le mode DTE des deux premiers travaux est défini comme indiqué dans les tableaux suivants, en fonction du mode DTE d'image.
  - Les deux premiers travaux remplacent le paramètre DTE global et les valeurs du fichier bp.conf du serveur principal. Le mode DTE du troisième travail est ainsi défini selon le paramètre DTE global et les valeurs du fichier bp.conf du serveur principal récupérés.

Le mode DTE d'image est défini sur Désactivé

Tableau 16-12 Lorsque le mode DTE d'image est défini sur Désactivé et le paramètre DTE du serveur de médias est défini sur Activé

Mode DTE global	Serveur principal NetBackup 9.1 et versions ultérieures avec mode DTE		
	Activé	**Désactivé**	**Automatique**
Préféré désactivé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données sont chiffrées
Appliqué	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées

Remarque : Lorsque le paramètre DTE global est défini sur `ENFORCED` et `DTE_CLIENT_MODE` est défini sur Désactivé, le paramètre DTE est utilisé pour éviter l'échec d'une récupération de catalogue.

Tableau 16-13 Lorsque le mode DTE d'image et le mode DTE du serveur de médias sont définis sur Désactivé

Mode DTE global	Serveur principal NetBackup 9.1 et versions ultérieures avec mode DTE		
	Activé	**Désactivé**	**Automatique**
Préféré désactivé	Les données sont chiffrées*	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Les données sont chiffrées*	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	Les données sont chiffrées*	Les données sont chiffrées*	Les données sont chiffrées*

* signifie que le paramètre DTE est utilisé pour éviter l'échec d'une récupération de catalogue. Le paramètre DTE du serveur de médias est ignoré (ce paramètre est défini sur Désactivé, à moins que le mode DTE client soit défini sur Automatique).

Le mode DTE d'image est défini sur Activé

Tableau 16-14 Lorsque le mode DTE d'image et le paramètre DTE du serveur de médias sont définis sur Activé

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	Serveur principal avec DTE_CLIENT_MODE défini sur Activé	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Serveur principal avec DTE_CLIENT_MODE défini sur Désactivé	Les données sont chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées
	Serveur principal avec DTE_CLIENT_MODE défini sur Automatique	Les données sont chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées
Préféré activé	Serveur principal avec DTE_CLIENT_MODE défini sur Activé	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Serveur principal avec DTE_CLIENT_MODE défini sur Désactivé	Les données sont chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées
	Serveur principal avec DTE_CLIENT_MODE défini sur Automatique	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
Appliqué	Serveur principal avec DTE_CLIENT_MODE défini sur Activé	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Serveur principal avec DTE_CLIENT_MODE défini sur Désactivé	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Serveur principal avec DTE_CLIENT_MODE défini sur Automatique	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées

Remarque : Si le paramètre `DTE_IGNORE_IMAGE_MODE` est défini sur `ALWAYS`, le paramètre DTE est défini comme indiqué dans le tableau Tableau 16-12.

Tableau 16-15 Lorsque le mode DTE d'image est défini sur Activé et le paramètre DTE du serveur de médias est défini sur Désactivé

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	Serveur principal avec DTE_CLIENT_MODE défini sur Activé	Les données sont chiffrées*	Les données sont chiffrées*	Les données sont chiffrées*
	Serveur principal avec DTE_CLIENT_MODE défini sur Désactivé	Les données sont chiffrées*	Les données sont chiffrées*	Les données ne sont pas chiffrées
	Serveur principal avec DTE_CLIENT_MODE défini sur Automatique	Les données sont chiffrées*	Les données sont chiffrées*	Les données ne sont pas chiffrées
Préféré activé	Serveur principal avec DTE_CLIENT_MODE défini sur Activé	Les données sont chiffrées*	Les données sont chiffrées*	Les données sont chiffrées*
	Serveur principal avec DTE_CLIENT_MODE défini sur Désactivé	Les données sont chiffrées*	Les données sont chiffrées*	Les données ne sont pas chiffrées
	Serveur principal avec DTE_CLIENT_MODE défini sur Automatique	Les données sont chiffrées*	Les données sont chiffrées*	Les données ne sont pas chiffrées
Appliqué	Serveur principal avec DTE_CLIENT_MODE défini sur Activé	Les données sont chiffrées*	Les données sont chiffrées*	Les données sont chiffrées*
	Serveur principal avec DTE_CLIENT_MODE défini sur Désactivé	Les données sont chiffrées*	Les données sont chiffrées*	Les données sont chiffrées
	Serveur principal avec DTE_CLIENT_MODE défini sur Automatique	Les données sont chiffrées*	Les données sont chiffrées*	Les données sont chiffrées*

* signifie que le paramètre DTE est utilisé pour éviter l'échec d'une récupération de catalogue. Le paramètre DTE du serveur de médias est ignoré (ce paramètre est défini sur Désactivé, à moins que le mode DTE client soit défini sur Automatique).

Duplication

Dans le workflow de duplication, une copie de sauvegarde est copiée d'une unité de stockage vers une autre, de sorte qu'aucun client n'intervienne. Les hôtes qui interviennent sont le serveur de médias source et le serveur de médias cible du même domaine.

Tableau 16-16 Le mode DTE d'image est défini sur Désactivé

Mode DTE global	Les deux serveurs de médias sont de version 9.1 ou ultérieure, avec le mode DTE		L'un des serveurs de médias exécute une version antérieure à la version 9.1
	Activé	Désactivé	
Préféré désactivé	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	Les données sont chiffrées	L'opération échoue	L'opération échoue

Tableau 16-17 Lorsque le mode DTE d'image et le paramètre DTE du serveur de médias sont définis sur Activé

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	Les deux serveurs de médias exécutent NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées
	Tout serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré activé	Les deux serveurs de médias exécutent NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Tout serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	Les deux serveurs de médias exécutent NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Tout serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	L'opération échoue	L'opération échoue	L'opération échoue

Remarque : Si le paramètre `DTE_IGNORE_IMAGE_MODE` est défini sur `ALWAYS`, le paramètre DTE est défini comme indiqué dans le tableau Tableau 16-16.

Tableau 16-18 Lorsque le mode DTE d'image est défini sur Activé et le paramètre DTE du serveur de médias 10.0 ou version ultérieure est défini sur Désactivé

Mode DTE global	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
	NEVER	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
Préféré activé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
Appliqué	L'opération échoue	L'opération échoue	L'opération échoue

Sauvegarde synthétique

Une sauvegarde synthétique peut être une sauvegarde synthétique complète ou cumulative. Les images utilisées pour créer l'image synthétique sont appelées « images de composant ». Par exemple, les images de composant d'une sauvegarde synthétique complète correspondent à la précédente image complète et aux images incrémentielles ultérieures. Le processus de sauvegarde NetBackup général accède au client pour créer une sauvegarde. Une sauvegarde synthétique est une image de sauvegarde créée sans le client. À la place, un processus de sauvegarde synthétique crée une image complète ou une image incrémentielle cumulative en utilisant uniquement les images de sauvegarde précédemment créées, appelées « images de composant ». Dans le workflow de sauvegarde synthétique, les images sont récupérées à partir de différentes unités de stockage sources, puis sont synthétisées et copiées sur une unité de stockage cible.

Les hôtes qui interviennent sont les serveurs de médias sources et le serveur de médias cible du même domaine.

Tableau 16-19 Le mode DTE est défini sur Désactivé dans l'image

Mode DTE global	Tous les serveurs de médias NetBackup 9.1 et versions ultérieures avec mode DTE		Tout serveur de médias exécutant une version de NetBackup antérieure à la version 9.1
	Activé	Désactivé	
Préféré désactivé	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	Les données sont chiffrées	L'opération échoue	L'opération échoue

Tableau 16-20 Lorsque le mode DTE de n'importe quelle image et le paramètre DTE du serveur de médias sont définis sur Activé

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	Tous les serveurs de médias exécutant NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées
	Tout serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Tous les serveurs de médias exécutant NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Tout serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	Tous les serveurs de médias exécutant NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Tout serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	L'opération échoue	L'opération échoue	L'opération échoue

Remarque : Si le paramètre `DTE_IGNORE_IMAGE_MODE` est défini sur `ALWAYS`, le paramètre DTE est défini comme indiqué dans le tableau Tableau 16-19.

Tableau 16-21 Lorsque le mode DTE d'image est défini sur Activé et le paramètre DTE du serveur de médias 10.0 ou version ultérieure est défini sur Désactivé

Mode DTE global	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
	NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
Préféré activé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
Appliqué	L'opération échoue	L'opération échoue	L'opération échoue

Remarque : Si le paramètre `DTE_IGNORE_IMAGE_MODE` est défini sur `ALWAYS`, le paramètre DTE est défini comme indiqué dans le tableau Tableau 16-19.

Remarque :

Vérification

Dans le workflow de vérification, l'en-tête de l'image de sauvegarde est lu et son intégrité est vérifiée avec le catalogue. Ainsi, aucun client n'intervient. Les hôtes qui interviennent sont le serveur de médias et le serveur principal du même domaine.

Tableau 16-22 Le mode DTE d'image est défini sur Désactivé

Mode DTE global	Serveur de médias NetBackup 9.1 et versions ultérieures avec mode DTE		Serveur de médias exécutant une version de NetBackup antérieure à la version 9.1
	Activé	Désactivé	
Préféré désactivé	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	Les données sont chiffrées	L'opération échoue	L'opération échoue

Tableau 16-23 Lorsque le mode DTE d'image et le paramètre DTE du serveur de médias sont définis sur Activé

Mode DTE global	Mode DTE du client NetBackup 9.1 ou version ultérieure	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	Serveur de médias 9.1 ou version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées
	Serveur de médias exécutant une version antérieure à la version 9.1	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Serveur de médias 9.1 ou version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Serveur de médias exécutant une version antérieure à la version 9.1	L'opération échoue	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	Serveur de médias 9.1 ou version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Serveur de médias exécutant une version antérieure à la version 9.1	L'opération échoue	L'opération échoue	L'opération échoue

Tableau 16-24 Lorsque le mode DTE d'image est défini sur Activé et le paramètre DTE du serveur de médias 10.0 ou version ultérieure est défini sur Désactivé

Mode DTE global	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
	NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
Préféré activé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
Appliqué	L'opération échoue	L'opération échoue	L'opération échoue

Importation

Dans le workflow d'importation, l'image de sauvegarde est lue à partir de l'unité de stockage et le catalogue NetBackup est créé. Ainsi, aucun client n'intervient. Les hôtes qui interviennent sont le serveur de médias et le serveur principal du même domaine.

Le tableau suivant s'applique à tous les workflows d'importation tels que l'importation de phase 1, l'importation de phase 2 et l'importation de politique de cycle de vie du stockage (SLP).

Tableau 16-25 Le mode DTE est défini sur Désactivé dans l'image

Mode DTE global	Serveur de médias 9.1 ou version ultérieure, avec mode DTE		Serveur de médias exécutant une version antérieure à la version 9.1
	Activé	Désactivé	
Préféré désactivé	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	Les données sont chiffrées	L'opération échoue	L'opération échoue

Tableau 16-26 Lorsque le mode DTE d'image et le paramètre DTE du serveur de médias sont définis sur Activé

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	Serveur de médias exécutant NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées
	Serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	**WHERE_UNSUPPORTED**	**ALWAYS**
Préféré activé	Serveur de médias exécutant NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Appliqué	Serveur de médias exécutant NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	L'opération échoue	L'opération échoue	L'opération échoue

Remarque : Pour l'importation de phase 1, vous devez définir `DTE_IGNORE_IMAGE_MODE` sur le serveur de médias pour ignorer le mode DTE de l'image pour les serveurs de médias 9.1 et versions ultérieures.

Pour le scénario d'importation de phase 1, les serveurs de médias exécutant une version de NetBackup antérieure à la version 9.1 ne tiennent pas compte du mode DTE de l'image. Si l'image a été créée avec le mode DTE défini sur Activé pour l'importation de phase 1, le travail n'échoue pas pour les serveurs de médias dont la version est antérieure à la version 9.1 et le mode DTE d'image est défini sur Désactivé dans le catalogue.

Remarque : Si le paramètre `DTE_IGNORE_IMAGE_MODE` est défini sur `ALWAYS`, le paramètre DTE est défini comme indiqué dans le tableau Tableau 16-25.

Tableau 16-27 Lorsque le mode DTE d'image est défini sur Activé et le paramètre DTE du serveur de médias 10.0 ou version ultérieure est défini sur Désactivé

Mode DTE global	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
	NEVER (par défaut)	**WHERE_UNSUPPORTED**	**ALWAYS**
Préféré désactivé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
Préféré activé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
Appliqué	L'opération échoue	L'opération échoue	L'opération échoue

Remarque : Si le paramètre `DTE_IGNORE_IMAGE_MODE` est défini sur `ALWAYS`, le paramètre DTE est défini comme indiqué dans le tableau Tableau 16-25.

Importation d'une SLP MSDP dans le domaine cible

Dans ce cas, l'image est déjà répliquée dans le pool de disques cible et l'objectif consiste à créer un catalogue à partir de cette image via une politique d'importation de SLP. Puisque cette opération est effectuée dans le domaine cible et qu'aucune opération interdomaine n'est effectuée, le paramètre DTE global cible est pris en compte.

Si le mode DTE de l'image répliquée est défini sur Activé, l'opération d'importation est effectuée avec le mode DTE défini sur Activé indépendamment des autres configurations DTE.

Si le mode DTE de l'image répliquée est défini sur Désactivé, le mode DTE est défini en fonction du paramètre DTE global du domaine cible et l'importation est effectuée en fonction du mode DTE défini.

Passez en revue les limitations MSDP suivantes, qui doivent être prises en compte pour ce workflow :

- Si plusieurs serveurs d'équilibrage de charge sont connectés au serveur de stockage MSDP, le serveur de stockage et les serveurs de médias d'équilibrage de charge doivent exécuter NetBackup 10.0 pour chiffrer correctement les données en transit. Si certains de ces serveurs (le serveur de stockage ou les serveurs de médias d'équilibrage de charge) ne sont pas compatibles DTE (version antérieure à la version 10.0), les données peuvent circuler sous forme de texte brut et le travail aboutira toujours, même si le chiffrement des données en transit n'est pas appliqué.

- Dans un environnement mixte où le serveur de stockage ou l'un des serveurs de médias d'équilibrage de charge exécute une version antérieure à la version 10.0, la configuration suivante est requise pour appliquer le chiffrement de bout en bout :
  - Le chiffrement des données en transit doit être activé côté NetBackup conformément aux paramètres de configuration DTE (mode DTE global/client/du serveur de médias).
  - Le chiffrement doit être activé côté MSDP à l'aide de l'indicateur `ENCRYPTION` dans le fichier pd.conf.

Pour plus de détails sur l'activation du chiffrement à l'aide de MSDP, consultez le Guide de déduplication NetBackup.

Remarque : Si vous activez le chiffrement des données en transit dans NetBackup, mais que l'indicateur ENCRYPTION n'est pas activé dans le fichier pd.conf, le chemin d'accès des données depuis le serveur de médias d'équilibrage de charge vers le serveur de stockage n'est pas chiffré. Le mode DTE du travail et le mode DTE d'image peuvent toutefois être activés.

Si le chiffrement des données en transit est activé côté NetBackup et que le chiffrement est activé côté MSDP (indicateur `ENCRYPTION` dans le fichier pd.conf), le chiffrement MSDP a la priorité sur le chiffrement des données en transit NetBackup. Les données au repos sont alors chiffrées, mais pas les données en transit.

Réplication

Si le serveur de stockage MSDP est utilisé pour la réplication, les considérations suivantes doivent être prises en compte :

- La fonction de chiffrement des données en transit (DTE) n'est pas intégrée au stockage MSDP pour les workflows de réplication et est contrôlée par l'indicateur `OPTDUP_ENCRYPTION` dans le fichier pd.conf.
- Le mode DTE du travail dépend du mode DTE d'image ou du paramètre DTE global du domaine source.
- Les valeurs correctes doivent être définies pour les paramètres de configuration DTE et l'indicateur `OPTDUP_ENCRYPTION` doit être défini pour les domaines source et cible.

Consultez le *Guide de déduplication NetBackup* pour plus de détails sur l'activation du chiffrement à l'aide de MSDP.

Tableau 16-28 Le mode DTE d'image est défini sur Désactivé

Mode DTE global	Serveur de médias 9.1 ou version ultérieure, avec mode DTE		Serveur de médias exécutant une version antérieure à la version 9.1
	Activé	Désactivé	
Préféré désactivé	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées	Les données ne sont pas chiffrées
Préféré activé	Les données sont chiffrées	Les données ne sont pas chiffrées	Les données sont chiffrées
Appliqué	Les données sont chiffrées	L'opération échoue	Les données sont chiffrées

Tableau 16-29 Lorsque le mode DTE d'image et le paramètre DTE du serveur de médias sont définis sur Activé

Mode DTE global	Hôte	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
		NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	Serveur de médias exécutant NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées
	Serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	Les données sont chiffrées	Les données sont chiffrées	Les données ne sont pas chiffrées
Préféré activé	Serveur de médias exécutant NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
Appliqué	Serveur de médias exécutant NetBackup 9.1 ou une version ultérieure	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées
	Serveur de médias exécutant une version de NetBackup antérieure à la version 9.1	Les données sont chiffrées	Les données sont chiffrées	Les données sont chiffrées

Remarque : Si le paramètre `DTE_IGNORE_IMAGE_MODE` est défini sur `ALWAYS`, le paramètre DTE est défini comme indiqué dans le tableau Tableau 16-28.

Tableau 16-30 Lorsque le mode DTE d'image est défini sur Activé et le paramètre DTE du serveur de médias 10.0 ou version ultérieure est défini sur Désactivé

Mode DTE global	Valeur de l'option de configuration DTE_IGNORE_IMAGE_MODE		
	NEVER (par défaut)	WHERE_UNSUPPORTED	ALWAYS
Préféré désactivé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
Préféré activé	L'opération échoue	L'opération échoue	Les données ne sont pas chiffrées
Appliqué	L'opération échoue	L'opération échoue	L'opération échoue

Remarque : Si le paramètre `DTE_IGNORE_IMAGE_MODE` est défini sur `ALWAYS`, le paramètre DTE est défini comme indiqué dans le tableau Tableau 16-28.

Chapitre 17

Autorité de certification externe et certificats externes

Ce chapitre traite des sujets suivants :

A propos de la prise en charge d'une autorité de certification externe dans NetBackup

Vous pouvez maintenant utiliser des certificats X.509 émis par votre autorité de certification approuvée.

NetBackup prend en charge les certificats basés sur un fichier et le magasin de certificats Windows en tant que sources pour les certificats externes pour les hôtes NetBackup. ainsi que les formats de certificats PEM, DER et P7B.

Remarque : NetBackup ne prend pas en charge le magasin de certificats Windows comme source pour le certifcat de serveur web NetBackup.

À propos de la terminologie utilisée pour les certificats dans NetBackup

Les termes suivants qui sont propres aux certificats de sécurité sont utilisés dans NetBackup :

- Une autorité de certification (CA) autre que l'autorité de certification NetBackup est appelée autorité de certification externe.

- Les certificats émis par une autorité de certification autre que l'autorité de certification NetBackup sont appelés certificats signés par une autorité de certification externe ou certificats externes.
- Les certificats émis par l'autorité de certification NetBackup sont appelés certificats signés par l'autorité de certification NetBackup ou certificats NetBackup.
- Un certificat NetBackup utilisé pour les communications sécurisées sur un canal de contrôle est également appelé certificat basé sur l'ID d'hôte.

Remarques importantes sur les certificats de l'hôte

- Un certificat basé sur un ID d'hôte est déployé sur le serveur maître pendant l'installation NetBackup. Vous devez configurer manuellement un certificat externe sur le serveur maître après l'installation.
  Se reporter à "Configuration du serveur maître pour utiliser un certificat signé par une autorité de certification externe" à la page 467.
- Vous pouvez configurer un certificat externe sur un hôte NetBackup (serveur de médias ou client) pendant l'installation ou après l'installation.
  Se reporter à "Configuration d'un hôte NetBackup (serveur de médias, client ou nœud de cluster) de sorte à utiliser un certificat signé par une autorité de certification externe après l'installation" à la page 470.
- Des certificats basés sur un ID d'hôte sont requis sur tous les hôtes NetBackup 8.1 et version ultérieure pour permettre des communications sécurisées mutuellement authentifiées. À partir de la version 8.2, les certificats NetBackup basés sur un ID d'hôte signés par l'autorité de certification peuvent être remplacés par des certificats signés par une autorité de certification externe.
  En plus du certificat basé sur un ID d'hôte, il est parfois nécessaire de déployer un certificat basé sur un nom d'hôte sur certains hôtes dans des domaines où le service NetBackup Access Control (NBAC) ou l'audit amélioré est activé. Les certificats basés sur le nom d'hôte sont émis par l'autorité de certification NetBackup.
  Se reporter à "Présentation des certificats de sécurité dans NetBackup" à la page 294.

Conditions requises pour la configuration du certificat externe

- Sur une plate-forme Windows, si des certificats externes sont utilisés pour la communication avec l'hôte, l'utilisateur `NT AUTHORITY\SYSTEM` doit être en mesure d'accéder aux certificats résidant sur `ECA_CERT_PATH`. L'option de configuration `ECA_CERT_PATH` est accessible depuis le Registre Windows.

- Sur la plate-forme Windows, les chemins d'accès UNC (Universal Naming Convention) (ou chemins d'accès réseau) ne sont pas pris en charge pour les paramètres d'autorité de certification externe suivants : chaîne de certification, clé privée du certificat, magasin d'approbation, fichier de phrase secrète pour la clé privée du certificat et cache CRL.
- La condition suivante s'applique au certificat de serveur Web NetBackup : Si le nom SAN (Subject Alternative Name) n'est pas vide, le certificat doit contenir tous les noms d'hôte connus du serveur maître (répertoriés dans les entrées de l'option de configuration `SERVER` des autres hôtes dans le domaine) dans le champ SAN du certificat.
- Conditions requises pour le nom d'objet du certificat :
  - Le nom d'objet ne doit pas être vide.
  - Le nom commun du nom d'objet ne doit pas être vide.
  - Le nom d'objet doit être unique pour chaque hôte.
  - Le nom d'objet doit contenir moins de 255 caractères.
- Seuls les caractères ASCII 7 sont pris en charge pour l'objet du certificat et le Subject Alternative Name (SAN).
- Conditions requises pour l'utilisation de la clé :

  Si le certificat est doté d'une extension d'utilisation de clé X509v3, il doit inclure les objectifs d'utilisation de clé suivants :
  - Pour le certificat de serveur Web, au moins une signature numérique ou un chiffrement de clé doit être présent.
  - Pour un certificat d'hôte NetBackup, l'objectif d'utilisation de la signature numérique doit être présent. Le chiffrement de clé peut être présent ou non.
  - Pour un certificat utilisé à la fois pour le serveur web et l'hôte NetBackup : l'objectif de signature numérique doit être présent. Le chiffrement de clé peut être présent ou non.
  - Le certificat peut avoir d'autres objectifs d'utilisation de clé répertoriés en plus de ceux spécifiés ici. Ces objectifs supplémentaires sont ignorés.
  - L'extension d'utilisation de clé X509v3 peut être critique ou non critique.
  - Un certificat sans extension d'utilisation de clé X509v3 est également utilisable avec NetBackup.

  Si le certificat est doté d'une extension d'utilisation de clé étendue X509v3, il doit inclure les objectifs d'utilisation de clé suivants :
  - Pour le certificat de serveur Web : authentification du serveur Web TLS.

- Pour un certificat d'hôte NetBackup : authentification du serveur Web TLS, authentification du client Web TLS.
- Pour un certificat utilisé à la fois pour le serveur web et l'hôte NetBackup : authentification du serveur web TLS et authentification du client web TLS
- Le certificat peut avoir d'autres objectifs d'utilisation de clé répertoriés en plus de ceux spécifiés ici. Ces objectifs supplémentaires sont ignorés.
- L'extension d'utilisation de clé étendue X509v3 peut être critique ou non.
- Un certificat sans extension d'utilisation de clé étendue X509v3 est également utilisable avec NetBackup.
- Si le certificat ne répond pas à ces critères, contactez votre fournisseur de certificats pour obtenir un nouveau certificat.

Options de ligne de commande utilisées pour la configuration de certificat externe

Utilisez les options de ligne de commande suivantes qui sont propres à la configuration de certificat externe :

`nbcertcmd`	■ `-cleanupCRLCache` ■ `-createECACertEntry` ■ `-deleteECACertEntry` ■ `-ecaHealthCheck` ■ `-enrollCertificate` ■ `-getExternalCertDetails` ■ `-listEnrollmentStatus` ■ `-removeEnrollment` ■ `-updateCRLCache`
`configureWebServerCerts`	■ `-addExternalCert` ■ `-removeExternalCert` ■ `-validateExternalCert`

Les options de ligne de commande suivantes sont utilisées à la fois pour les configurations de certificats externes et de certificats NetBackup :

`nbcertcmd`	■ `-listCertDetails` : cette option de commande s'applique par défaut aux certificats signés par l'autorité de certification NetBackup. Utilisée avec l'option `-ECA`, elle est applicable aux certificats signés par une autorité de certification externe. ■ `-listCACertDetails` : cette option de commande s'applique par défaut aux certificats signés par l'autorité de certification NetBackup. Utilisée avec l'option `-ECA`, elle est applicable aux certificats signés par une autorité de certification externe.

Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

Workflow d'utilisation de certificats externes pour la communication avec l'hôte NetBackup

Pour configurer l'utilisation de certificats signés par une autorité de certification externe dans NetBackup afin d'assurer une communication sécurisée, vous devez effectuer les étapes suivantes dans l'ordre indiqué :

Tableau 17-1 Workflow d'utilisation de certificats externes pour la communication avec l'hôte NetBackup

Étape	Description
Étape 1	Assurez-vous de remplir les conditions suivantes : ■ Les certificats externes pour le serveur Web, le serveur maître et tous les hôtes sont placés dans les emplacements appropriés. ■ En cas de certificats basés sur fichier, les fichiers de clé privée pour les certificats externes sont placés dans les emplacements appropriés. Se reporter à "ECA_PRIVATE_KEY_PATH pour les serveurs et les clients NetBackup" à la page 449. Si les clés privées sont chiffrées, les fichiers de phrase de passe doivent être placés dans les emplacements appropriés. Se reporter à "ECA_KEY_PASSPHRASEFILE pour les serveurs et les clients NetBackup" à la page 450. ■ Les listes CRL sont placées dans les emplacements requis sur les hôtes selon leurs options de configuration de liste CRL et elles sont accessibles. Se reporter à "À propos des listes de révocation des certifications pour l'autorité de certification externe" à la page 460.
Étape 2	Installez le logiciel NetBackup sur le serveur maître (ou mettez le serveur maître à niveau).

Étape	Description
Étape 3	Activez le domaine NetBackup pour qu'il utilise des certificats externes en configurant le serveur Web NetBackup. Se reporter à "Configuration d'un certificat externe pour le serveur Web NetBackup" à la page 465.
Étape 4	Configurez un certificat externe pour l'hôte de serveur maître NetBackup. Se reporter à "Configuration du serveur maître pour utiliser un certificat signé par une autorité de certification externe" à la page 467.
Étape 5	Installez le logiciel NetBackup sur le serveur de médias et les clients (ou mettez à niveau le serveur de médias et les clients). Si le serveur maître est configuré pour utiliser des certificats externes, le programme d'installation vous invite à fournir les informations du certificat externe pour l'hôte.
Étape 6	**Remarque :** Cette étape est nécessaire pour les hôtes (serveur de médias et clients) qui disposent du logiciel NetBackup à jour, mais qui ne sont pas configurés pour utiliser des certificats externes. Il se peut qu'aucun certificat externe ne soit configuré sur les hôtes NetBackup pour les raisons suivantes : ■ Vous n'avez pas fourni les informations du certificat externe pendant l'installation ou la mise à niveau de l'hôte. ■ Le serveur maître NetBackup n'a pas été configuré pour utiliser des certificats externes pendant l'installation ou la mise à niveau de l'hôte. Configurez manuellement un certificat externe pour un hôte NetBackup (serveur de médias ou client) après l'installation. Se reporter à "Configuration d'un hôte NetBackup (serveur de médias, client ou nœud de cluster) de sorte à utiliser un certificat signé par une autorité de certification externe après l'installation" à la page 470.

Options de configuration pour les certificats signés par une autorité de certification externe

Pour configurer un serveur de médias, un client ou un serveur maître NetBackup afin qu'il utilise un certificat signé par une autorité de certification externe pour la communication avec l'hôte, vous devez définir certaines options de configuration dans le fichier de configuration NetBackup (le fichier `bp.conf` sur la plate-forme UNIX ou le Registre Windows).

À propos des options de configuration obligatoires et facultatives

- Concernant la configuration de certificat externe, les options de configuration suivantes sont obligatoires pour les certificats basés sur fichier :
  - ECA_CERT_PATH
  - ECA_TRUST_STORE_PATH
  - ECA_PRIVATE_KEY_PATH
    Si la clé privée du certificat externe est chiffrée, l'option ECA_KEY_PASSPHRASEFILE est également obligatoire :
- Pour le magasin de certificats Windows, les options de configuration suivantes sont obligatoires :
  - ECA_CERT_PATH
- Les options suivantes sont facultatives :
  - ECA_CRL_CHECK
    Si l'option est définie sur DISABLE (ou 0) l'option ECA_CRL_PATH est ignorée et l'état de révocation du certificat de l'hôte homologue n'est pas vérifié.
    Si l'option est définie sur une valeur autre que DISABLE et 0, l'état de révocation du certificat de l'hôte homologue est vérifié par rapport à ECA_CRL_PATH.
  - ECA_DR_BKUP_WIN_CERT_STORE
    Pour le magasin de certificats Windows, spécifiez cette option si vous voulez sauvegarder les certificats externes pendant la sauvegarde de catalogue.
  - ECA_CRL_PATH_SYNC_HOURS
    Cette option est utilisée quand l'option ECA_CRL_CHECK est activée et l'option ECA_CRL_PATH définie.
  - ECA_CRL_REFRESH_HOURS
    Cette option est utilisée quand l'option ECA_CRL_CHECK est activée, mais que l'option ECA_CRL_PATH n'est pas définie (lorsque le CDP est utilisé en tant que source de liste CRL).

  Se reporter à "À propos des listes de révocation des certifications pour l'autorité de certification externe" à la page 460.

ECA_CERT_PATH pour les serveurs et clients NetBackup

L’option ECA_CERT_PATH spécifie le chemin d’accès du certificat signé par une autorité de certification externe de l’hôte. Cette option est obligatoire.

NetBackup prend en charge les sources de certificats suivantes pour les certificats d'hôte :

- Magasin de certificats Windows

  Remarque : Le magasin de certificats Windows n'est pas pris en charge pour les serveurs principaux en cluster.

- Certificats basés sur fichier

Ordre des certificats dans le fichier de certificat

Un fichier de certificat doit présenter une chaîne de certificats dont les certificats sont organisés dans l'ordre approprié. La chaîne débute par le certificat de serveur (également appelé certificat feuille), éventuellement suivi de certificats intermédiaires. La chaîne doit contenir tous les certificats intermédiaires jusqu'au certificat de l'autorité de certification racine, mais ne doit pas contenir le certificat de l'autorité de certification racine. La chaîne est créée de sorte que chaque certificat de la chaîne signe le certificat précédent dans la chaîne.

Le fichier de certificat doit être dans l'un des formats suivants :

- Fichier PKCS #7 ou P7B codé au format DER ou PEM contenant des certificats dans l'ordre spécifié
- Fichier avec les certificats PEM concaténés dans l'ordre spécifié

Tableau 17-2 Informations sur ECA_CERT_PATH

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup.

Utilisation	Description

Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option.
	
	Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes .
	
	Pour les certificats basés sur fichier, Respectez le format suivant :
	
	`ECA_CERT_PATH = Path to the external certificate of the host`
	
	Par exemple : `c:\server.pem`
	
	Si vous utilisez cette option sur une instance d'application Flex Appliance, le chemin d'accès doit être `/mnt/nbdata/hostcert/`.
	
	Pour le magasin de certificats Windows, utilisez le format suivant :
	
	`ECA_CERT_PATH = Certificate store name\Issuer name\Subject name`
	
	Vous pouvez spécifier plusieurs requêtes de sélection de certificats au format CSV (valeurs séparées par des virgules).
	
	`ECA_CERT_PATH = Store name1\Issuer name1\Subject name1,Store name2\Issuer name2\Subject name2`
	
	Se reporter à "Spécification d'un magasin de certificats Windows pour ECA_CERT_PATH" à la page 445.

Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

Spécification d'un magasin de certificats Windows pour ECA_CERT_PATH

NetBackup sélectionne un certificat dans n'importe quel magasin de certificats de l'ordinateur local sur un hôte Windows.

En cas de magasin de certificats Windows, `ECA_CERT_PATH` est une liste de clauses séparées par une virgule.

Chaque clause est au format *nom du magasin\émetteur\objet*. Chaque élément de clause contient une requête.

`$hostname` est un mot-clé qui est remplacé par le nom de domaine complet de l'hôte. Utilisez les guillemets doubles quand un symbole `\` est présent dans le chemin d'accès réel. Par exemple, `MY\Veritas\"NetBackup\$hostname"`.

`$shorthostname` est un mot-clé qui est remplacé par le nom court de l'hôte. Utilisez les guillemets doubles quand un symbole `\` est présent dans le chemin d'accès réel. Par exemple, `MY\Veritas\"NetBackup\$shorthostname"`.

Le nom du magasin doit correspondre exactement au nom du magasin où se trouve le certificat. Par exemple : « MY »

L'émetteur est facultatif. S'il est indiqué, NetBackup choisit les certificats pour lesquels le nom unique de l'émetteur contient la sous-chaîne fournie.

L'objet est obligatoire. NetBackup choisit le certificat pour lequel le nom unique de l'objet contient la sous-chaîne fournie.

Vous devez effectuer les actions suivantes :

- Ajouter le certificat racine aux autorités de certification racine approuvées ou aux autorités de certification racine tierces dans le magasin de certificats Windows.
- Si vous disposez d'autorités de certification intermédiaires, ajoutez leurs certificats aux autorités de certification intermédiaires dans le magasin de certificats Windows.

Exemples d'emplacements de certificat avec la CLAUSE WHERE :

- `My\Veritas\$hostname, My\ExampleCompany\$hostname`
  Où (le magasin de certificats est MY, le nom unique de l'émetteur contient `Veritas`, le nom unique de l'objet contient `$hostname`) OU (le nom du magasin de certificats est `MY`, le nom unique de l'émetteur contient `ExampleCompany`, le nom unique de l'objet contient `$hostname`)
- `MY\Veritas\"NetBackup\$hostname"`
  Où le nom du magasin de certificats est `MY`, le nom unique de l'émetteur contient `Veritas`, le nom unique de l'objet contient `NetBackup\$hostname`
- `MY\\$hostname`
  Où le nom du magasin de certificats est `MY`, le nom unique de l'émetteur contient une valeur quelconque, le nom unique de l'objet contient `$hostname`
- `MY\\$shorthostname`
  Où le nom du magasin de certificats est `MY`, le nom unique de l'émetteur contient une valeur quelconque, le nom unique de l'objet contient `$shorthostname`
- `MY\Veritas\NetBackup $hostname`

Où le nom du magasin de certificats est `MY`, le nom unique de l'émetteur contient `Veritas`, le nom unique de l'objet contient `NetBackup $hostname`

Si vous insérez un espace entre les mots, il est considéré comme un caractère valide.

Exemples d'emplacements de certificat avec des données non valides :

- `MY\\`

  Le nom unique de l'objet doit contenir une valeur.

- `My\$hostname`

  Le nom unique de l'objet doit contenir une valeur.

- `\\$hostname`

  Le nom du magasin de certificats doit inclure la valeur exacte du magasin dans lequel réside le certificat.

- `MY\CN=Veritas\CN=$hostname`

  Le nom unique de l'objet et le nom unique de l'émetteur ne peuvent pas contenir =, ni de balises spécifiques comme CN=.

ECA_TRUST_STORE_PATH pour les serveurs et les clients NetBackup

L'option `ECA_TRUST_STORE_PATH` spécifie le chemin d'accès du fichier de lot de certificats qui contient tous les certificats d'autorité de certification racine approuvés.

Ce fichier de certificats doit contenir un ou plusieurs certificats au format PEM.

Ne spécifiez pas l'option `ECA_TRUST_STORE_PATH` si vous utilisez le magasin de certificats Windows.

Le magasin d'approbation prend en charge les certificats aux formats suivants :

- Fichier PKCS #7 ou P7B comprenant des certificats des autorités de certification racine approuvées intégrés. Ce fichier peut être codé au format PEM ou DER.
- Fichier contenant les certificats des autorités de certification racine approuvées, codés au format PEM et concaténés ensemble.

Cette option est obligatoire pour les certificats basés sur un fichier.

Le certificat d'autorité de certification racine dans la distribution Cloudera peut être obtenu auprès de l'administrateur Cloudera. Sa configuration TLS peut être manuelle ou automatique pour le cluster Hadoop. Dans les deux cas, NetBackup requiert un certificat d'autorité de certification racine délivré par l'administrateur.

Le certificat d'autorité de certification racine du cluster Hadoop peut valider les certificats pour tous les nœuds et permettre à NetBackup d'exécuter le processus de sauvegarde et de restauration dans le cas d'un cluster sécurisé (SSL). Ce certificat d'autorité de certification racine est un lot de certificats émis pour tous les nœuds en question.

Le certificat d'autorité de certification racine doit être configuré sous `ECA_TRUST_STORE_PATH` dans le cas d'environnements d'autorité de certification auto-signée, tierce ou locale/intermédiaire. Par exemple, dans les environnements Cloudera présentant une configuration TLS automatique, le fichier d'autorité de certification racine `cm-auto-global_cacerts.pem` se trouve à l'emplacement suivant : `/var/lib/cloudera-scm-agent/agent-cert`. Consultez la documentation Cloudera pour plus de détails.

Tableau 17-3 Informations sur ECA_TRUST_STORE_PATH

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup. Si la validation de certificat est requise pour les serveurs VMware, RHV ou Nutanix AHV, cette option doit être définie sur le serveur principal NetBackup et les hôtes d'accès correspondants, indépendamment de l'autorité de certification qu'utilise NetBackup pour communiquer avec l'hôte (autorité de certification NetBackup ou externe). Si la validation de certificat est requise pour les serveurs VMware ou RHV, cette option doit être définie sur le serveur principal NetBackup et les hôtes d'accès correspondants, indépendamment de l'autorité de certification qu'utilise NetBackup pour communiquer avec l'hôte (autorité de certification NetBackup ou externe).
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Respectez le format suivant : `ECA_TRUST_STORE_PATH = Path to the external CA certificate` Par exemple : `c:\rootCA.pem` Si vous utilisez cette option sur une instance d'application Flex Appliance, le chemin d'accès doit être `/mnt/nbdata/hostcert/`.

Utilisation	Description
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

ECA_PRIVATE_KEY_PATH pour les serveurs et les clients NetBackup

L'option `ECA_PRIVATE_KEY_PATH` spécifie le chemin d'accès au fichier de la clé privée pour le certificat signé par l'autorité de certification externe de l'hôte.

Cette option est obligatoire pour les certificats basés sur un fichier.

Si la clé privée du certificat est chiffrée, vous devez spécifier l'option `ECA_KEY_PASSPHRASEFILE`.

Se reporter à "ECA_KEY_PASSPHRASEFILE pour les serveurs et les clients NetBackup" à la page 450.

NetBackup prend en charge les clés privées aux formats PKCS #1 et PKCS #8 chiffrées ou en texte brut. Elles peuvent être codées au format PEM ou DER. Dans le cas d'un chiffrement PKCS #1, la clé doit être codée au format PEM.

Pour les clés privées chiffrées, NetBackup prend en charge les algorithmes de chiffrement suivants :

- DES, 3DES et AES si la clé privée est au format PKCS #1
- DES, 3DES, AES, RC2 et RC4 si la clé privée est au format PKCS #8

Remarque : Vous ne devez pas spécifier l'option `ECA_PRIVATE_KEY_PATH` si le magasin de certificats Windows n'est spécifié pour l'option `ECA_CERT_PATH`.

Se reporter à "ECA_CERT_PATH pour les serveurs et clients NetBackup" à la page 443.

Tableau 17-4 Informations sur ECA_PRIVATE_KEY_PATH

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup.

Utilisation	Description
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Respectez le format suivant : `ECA_PRIVATE_KEY_PATH = Path to the private key of the external certificate` Par exemple : `c:\key.pem` Si vous utilisez cette option sur une instance d'application Flex Appliance, le chemin d'accès doit être `/mnt/nbdata/hostcert/`.
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

ECA_KEY_PASSPHRASEFILE pour les serveurs et les clients NetBackup

L'option `ECA_KEY_PASSPHRASEFILE` spécifie le chemin d'accès au fichier texte contenant la phrase de passe de la clé privée du certificat externe.

Spécifiez l'option `ECA_KEY_PASSPHRASEFILE` uniquement si la clé privée du certificat est chiffrée.

Se reporter à "ECA_PRIVATE_KEY_PATH pour les serveurs et les clients NetBackup" à la page 449.

Remarque : Ne spécifiez pas l'option `ECA_KEY_PASSPHRASEFILE` si vous utilisez le magasin de certificats Windows.

Se reporter à "ECA_CERT_PATH pour les serveurs et clients NetBackup" à la page 443.

Remarque : N'utilisez pas ECA_KEY_PASSPHRASEFILE sur les serveurs MSDP utilisés pour les niveaux cloud directs MSDP, car ils ne sont pas pris en charge avec les niveaux cloud directs MSDP.

Tableau 17-5 Informations sur ECA_KEY_PASSPHRASEFILE

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup.
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations sur ces commandes, consultez le Guide de référence des commandes NetBackup. Respectez le format suivant : `ECA_KEY_PASSPHRASEFILE = Path to the passphrase file`
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

ECA_CRL_CHECK pour les serveurs et les clients NetBackup

L'option `ECA_CRL_CHECK` permet de spécifier le niveau de contrôle de la révocation pour les certificats externes de l'hôte. Elle permet également de désactiver le contrôle de la révocation des certificats externes. En fonction du contrôle, l'état de révocation du certificat est validé à l'aide de la liste CRL pendant la communication avec l'hôte.

Vous pouvez utiliser les listes CRL à partir du répertoire qui est spécifié pour l'option de configuration `ECA_CRL_PATH` dans le fichier (`bp.conf` sur UNIX ou dans le Registre Windows) ou le point de distribution (CDP) des listes CRL.

Se reporter à "ECA_CRL_PATH pour les serveurs et les clients NetBackup" à la page 452.

Tableau 17-6 Informations sur ECA_CRL_CHECK

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup.

Utilisation	Description
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Respectez le format suivant : `ECA_CRL_CHECK = CRL check` Vous pouvez spécifier l'une des opérations suivantes : ■ DISABLE (ou 0) : le contrôle de révocation est désactivé. L'état de révocation du certificat n'est pas validé à l'aide de la liste de révocation de certificats pendant la communication avec l'hôte. ■ LEAF (ou 1) : l'état de révocation du certificat feuille est validé à l'aide de la liste CRL. Il s'agit de la valeur par défaut. ■ CHAIN (ou 2) : l'état de révocation de tous les certificats de la chaîne de certificat est validé à l'aide de la liste CRL.
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

ECA_CRL_PATH pour les serveurs et les clients NetBackup

L'option `ECA_CRL_PATH` spécifie le chemin d'accès au répertoire où se trouvent les listes de révocation des certifications (CRL) de l'autorité de certification externe.

Ces listes CRL sont copiées dans le cache CRL NetBackup. L'état de révocation du certificat externe est validé à l'aide des listes CRL du cache CRL.

Les listes CRL dans le cache CRL sont régulièrement mises à jour avec les listes du répertoire spécifié pour `ECA_CRL_PATH` en fonction de l'option `ECA_CRL_PATH_SYNC_HOURS`.

Se reporter à "ECA_CRL_PATH_SYNC_HOURS pour les serveurs et les clients NetBackup" à la page 454.

Si l'option `ECA_CRL_CHECK` ou `HADOOP_CRL_CHECK` n'est pas définie sur `DISABLE` (ou 0) et si l'option `ECA_CRL_PATH` n'est pas spécifiée, NetBackup télécharge les listes CRL à partir des URL spécifiées dans le point de distribution des listes CRL (CDP) et les utilise pour vérifier l'état de révocation du certificat de l'hôte homologue.

Se reporter à "ECA_CRL_CHECK pour les serveurs et les clients NetBackup" à la page 451.

Remarque : Pour valider l'état de révocation d'un certificat de serveur de virtualisation, l'option `VIRTUALIZATION_CRL_CHECK` est utilisée.

Pour valider l'état de révocation d'un certificat de serveur Hadoop, l'option `HADOOP_CRL_CHECK` est utilisée.

Tableau 17-7 Informations sur ECA_CRL_PATH

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup. Si la validation de certificat est requise pour les serveurs VMware, RHV, Nutanix AHV ou Hadoop, cette option doit être définie sur le serveur principal NetBackup et les hôtes d'accès ou de sauvegarde correspondants, indépendamment de l'autorité de certification qu'utilise NetBackup pour communiquer avec l'hôte (autorité de certification NetBackup ou externe). Si la validation de certificat est requise pour les serveurs VMware, RHV ou Hadoop, cette option doit être définie sur le serveur principal NetBackup et les hôtes d'accès ou de sauvegarde correspondants, indépendamment de l'autorité de certification qu'utilise NetBackup pour communiquer avec l'hôte (autorité de certification NetBackup ou externe).
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Utilisez le format suivant pour spécifier le chemin d'accès au répertoire de la liste de révocation des certifications : `ECA_CRL_PATH = Path to the CRL directory` Si vous utilisez cette option sur une instance d'application Flex Appliance, le chemin d'accès doit être `/mnt/nbdata/hostcert/`.
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

ECA_CRL_PATH_SYNC_HOURS pour les serveurs et les clients NetBackup

L'option `ECA_CRL_PATH_SYNC_HOURS` spécifie l'intervalle de temps en heures nécessaire pour mettre à jour les listes de révocation de certificats (CRL) dans le cache de CRL NetBackup, avec les listes CRL figurant dans le répertoire spécifié pour l'option de configuration `ECA_CRL_PATH`.

Se reporter à "ECA_CRL_PATH pour les serveurs et les clients NetBackup" à la page 452.

L'option `ECA_CRL_PATH_SYNC_HOURS` n'est pas applicable si le point de distribution est utilisé pour les listes CRL.

Par défaut, les listes CRL dans le cache sont mises à jour toutes les heures.

Pendant la communication avec l'hôte, l'état de révocation du certificat externe est validé par rapport aux listes de révocation des certifications du cache CRL.

Tableau 17-8 Informations sur ECA_CRL_PATH_SYNC_HOURS

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup.
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Utilisez le format suivant : `ECA_CRL_PATH_SYNC_HOURS = Number of hours` Nombre minimal d'heures que vous pouvez spécifier : 1 heure Nombre maximal d'heures que vous pouvez spécifier : 720 heures La valeur par défaut est une heure.
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

ECA_CRL_REFRESH_HOURS pour les serveurs et les clients NetBackup

L'option `ECA_CRL_REFRESH_HOURS` spécifie la durée (en heures) du téléchargement des listes CRL à partir des URL spécifiées dans les points de distribution (CDP) des listes CRL du certificat de l'hôte homologue.

L'option `ECA_CRL_REFRESH_HOURS` s'applique lorsque vous utilisez les points de distribution des listes CRL.

Se reporter à "ECA_CRL_PATH pour les serveurs et les clients NetBackup" à la page 452.

À la fin de l'intervalle de temps spécifié, les listes CRL de l'autorité de certification sont téléchargées à partir des URL disponibles dans les CDP.

Par défaut, les listes de révocation des certifications sont téléchargées à partir des CDP toutes les 24 heures.

Tableau 17-9 Informations ECA_CRL_REFRESH_HOURS

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup.
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Utilisez le format suivant : `ECA_CRL_REFRESH_HOURS = Number of hours` Nombre minimal d'heures que vous pouvez spécifier : 0 heure, ce qui signifie que les listes CRL des CDP ne sont pas téléchargées régulièrement. Nombre maximal d'heures que vous pouvez spécifier : 4 380 heures La valeur par défaut de cette option est 24 heures. **Remarque :** Les listes CRL sont également téléchargées à partir des CDP pendant la communication avec l'hôte si elles ont expiré ou ne sont plus disponibles dans le cache CRL, quel que soit l'intervalle de temps défini pour l'option `ECA_CRL_REFRESH_HOURS`.
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

ECA_DISABLE_AUTO_ENROLLMENT pour serveurs et clients NetBackup

Lorsque NetBackup est configuré pour utiliser les certificats signés par une autorité de certification externe, ces certificats sont automatiquement inscrits sur le serveur

principal pendant la communication avec l'hôte. Pour désactiver l'inscription automatique de ces certificats, définissez la valeur `ECA_DISABLE_AUTO_ENROLLMENT` sur « 1 ».

Lorsque l'inscription automatique est désactivée, vous pouvez inscrire les certificats externes manuellement à l'aide de la commande `nbcertcmd -enrollCertificate`.

Un certificat doit être inscrit auprès du serveur principal avant de pouvoir être utilisé pour la communication avec l'hôte.

L'inscription automatique est activée par défaut.

Tableau 17-10 Informations sur l'option ECA_DISABLE_AUTO_ENROLLMENT

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup.
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Respectez le format suivant : `ECA_DISABLE_AUTO_ENROLLMENT = 1`
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

ECA_DR_BKUP_WIN_CERT_STORE pour les serveurs et les clients NetBackup

L'option `ECA_DR_BKUP_WIN_CERT_STORE` indique s'il faut réaliser une sauvegarde des informations du magasin de certificats Windows pendant la sauvegarde du catalogue.

Par défaut, les informations du magasin de certificats Windows sont sauvegardées pendant la sauvegarde du catalogue.

Remarque : Si les informations du magasin de certificats Windows ne sont pas exportables, elles ne peuvent pas être sauvegardées pendant la sauvegarde du catalogue.

Tableau 17-11 Informations sur ECA_DR_BKUP_WIN_CERT_STORE

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup.
Utilisation	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Si vous ne voulez pas que l'opération de sauvegarde de catalogue effectue une sauvegarde des informations de magasin de certificats Windows, utilisez le format suivant : `ECA_DR_BKUP_WIN_CERT_STORE = NO`
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

Option MANAGE_WIN_CERT_STORE_PRIVATE_KEY pour les serveurs maîtres NetBackup

L'option `MANAGE_WIN_CERT_STORE_PRIVATE_KEY` permet de désactiver la gestion automatique des autorisations de la clé privée du certificat du magasin de certificats Windows.

Cette option s'applique au magasin de certificats Windows et uniquement lorsque les services NetBackup sont en cours d'exécution dans le contexte d'un compte de service local.

Lorsque les services NetBackup s'exécutent dans le contexte d'un compte de service local, les services doivent être autorisés à lire la clé privée du certificat dans le magasin de certificats Windows.

Lorsque l'option `MANAGE_WIN_CERT_STORE_PRIVATE_KEY` est définie sur `Automatic`, le service NetBackup en cours d'exécution dans le contexte d'un compte d'utilisateur privilégié accorde l'accès à tous les autres services NetBackup pour lire la clé privée lorsque cela est nécessaire.

Se reporter à "Limitations de la prise en charge du magasin de certificats Windows lorsque les services NetBackup s'exécutent avec un compte de service local" à la page 458.

Par défaut, les autorisations de la clé privée sont gérées automatiquement. Lorsque l'option `MANAGE_WIN_CERT_STORE_PRIVATE_KEY` est définie sur `Disabled`, les autorisations de la clé privée doivent être gérées manuellement.

Remarque : Il est déconseillé de définir l'option `MANAGE_WIN_CERT_STORE_PRIVATE_KEY` sur `Disabled`.

Pour mettre à jour manuellement les autorisations lorsque cette option est définie sur `Disabled`, exécutez la commande suivante :

```
nbcertcmd -setWinCertPrivKeyPermissions -reason audit reason -force
```

Consultez le Guide de référence des commandes NetBackup pour plus d'informations sur les options de ligne de commande.

Tableau 17-12 Informations relatives à l'option MANAGE_WIN_CERT_STORE_PRIVATE_KEY

Utilisation	Description
Où l'utiliser	Sur le serveur maître NetBackup.
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations sur ces commandes, consultez le Guide de référence des commandes NetBackup. Respectez le format suivant : `MANAGE_WIN_CERT_STORE_PRIVATE_KEY = Automatic`
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

Limitations de la prise en charge du magasin de certificats Windows lorsque les services NetBackup s'exécutent avec un compte de service local

Lorsque les services NetBackup s'exécutent avec un compte de service local, ils doivent être autorisés à lire la clé privée. NetBackup met à jour les autorisations de la clé privée lors de l'inscription de certificats afin que les services NetBackup aient accès en lecture à la clé privée.

Pour la définition des autorisations, le fournisseur de services de chiffrement (CSP) ou de stockage de clés (KSP) du certificat utilisé doit prendre en charge les descripteurs de sécurité.

Pour déterminer si le fournisseur prend en charge les descripteurs de sécurité, exécutez la commande suivante :

```
nbcertcmd -ecaHealthCheck -serviceUser LocalService
```

Consultez le Guide de référence des commandes NetBackup pour plus d'informations sur les options de ligne de commande.

Si le fournisseur ne prend pas en charge les descripteurs de sécurité, vous devez utiliser un fournisseur qui les prend en charge ou exécuter les services NetBackup avec un compte administrateur.

Pour changer de fournisseur, vous devez redéployer votre certificat. Vous ne pouvez pas changer de fournisseur une fois le certificat déployé. Fournisseurs prenant en charge les descripteurs de sécurité : fournisseur de stockage de clés des logiciels Microsoft, Microsoft Enhanced Cryptographic Provider v1.0, Microsoft Enhanced RSA and AES Cryptographic Provider, Microsoft Strong Cryptographic Provider, etc.

Si vous disposez d'un fichier PFX, vous pouvez le ré-importer pour changer de fournisseur.

1. Supprimez le certificat et la clé privée du magasin de certificats Windows.
2. Importez le fichier `pfx` à l'aide de la commande `certutil` :

   ```
   C:\Windows\System32\certutil.exe -importPfx -csp provider
   namepfxfile
   ```

Pour un certificat ADCS, vous pouvez changer de fournisseur à partir du modèle de certificat, puis redéployer le certificat.

Vous pouvez également sélectionner un fournisseur tout en demandant un nouveau certificat selon la configuration.

Pour exécuter les services NetBackup avec un compte administrateur, exécutez la commande suivante :

```
nbserviceusercmd.exe -changeUser
```

Consultez le Guide de référence des commandes NetBackup pour plus d'informations sur les options de ligne de commande.

À propos des listes de révocation des certifications pour l'autorité de certification externe

La liste de révocation des certifications pour une autorité de certification externe contient une liste des certificats numériques que l'autorité de certification a révoquée avant la date d'expiration planifiée et ne doit plus être approuvée.

NetBackup prend en charge les formats PEM et DER pour les listes de révocation des certifications pour l'autorité de certification externe.

Les listes de révocation des certifications pour l'ensemble des émetteurs ou des autorités de certification externes sont stockées dans le cache CRL NetBackup qui réside sur chaque hôte.

Pendant une communication sécurisée, chaque hôte NetBackup vérifie l'état de révocation du certificat externe de l'hôte homologue avec la liste CRL qui est disponible dans le cache de liste CRL NetBackup, selon l'option de configuration `ECA_CRL_CHECK`.

Se reporter à "ECA_CRL_CHECK pour les serveurs et les clients NetBackup" à la page 451.

Le cache de CRL de NetBackup est mis à jour avec les listes de révocation des certifications requises en utilisant l'une des sources de liste suivantes :

Option de configuration `ECA_CRL_PATH`	Une option de configuration NetBackup (provenant du fichier `bp.conf` sur le UNIX ou le Registre Windows) qui spécifie le chemin d'accès du répertoire des listes de révocation des certifications. Se reporter à "ECA_CRL_PATH_SYNC_HOURS pour les serveurs et les clients NetBackup" à la page 454. Se reporter à "Comment sont utilisées les listes de révocation des certificats de ECA_CRL_PATH" à la page 461.
Point de distribution de CRL (CDP)	Si vous n'avez pas spécifié l'option `ECA_CRL_PATH`, NetBackup télécharge les listes CRL à partir des URL qui sont indiquées dans le CDP des certificats de l'hôte homologue et les met dans le cache CRL NetBackup. Se reporter à "Comment les listes de révocation des certificats des URL du CDP sont utilisées" à la page 462. NetBackup prend en charge le téléchargement des listes de révocation des certifications à partir d'URL HTTP et HTTPS qui sont spécifiées dans le CDP.

Le cache de CRL NetBackup contient uniquement la dernière copie d'une liste de révocation des certifications pour chaque autorité de certification (y compris les autorités de certification racine et intermédiaire).

Le service `bpclntcmd -crl_download` met à jour le cache de CRL pendant la communication avec l'hôte dans les scénarios suivants, quel que soit l'intervalle de temps défini pour l'option `ECA_CRL_PATH_SYNC_HOURS` ou `ECA_CRL_REFRESH_HOURS` :

- Si les listes de révocation des certifications du cache de CRL ont expiré
- Si des listes de contrôle des révocations sont disponibles dans la source (`ECA_CRL_PATH` ou CDP), mais sont manquantes dans le cache de CRL

Remarque : Lorsque le service `bpclntcmd -crl_download` a mis à jour les listes CRL dans le cache de liste CRL, il ne télécharge pas ces listes pour la même autorité de certification pendant les 15 minutes suivantes, même si un scénario de téléchargement valide s'applique. Si vous voulez mettre à jour les listes pendant ces 15 minutes, arrêtez le service `bpclntcmd -crl_download`.

Comment sont utilisées les listes de révocation des certificats de ECA_CRL_PATH

Utilisez cette section si vous souhaitez utiliser `ECA_CRL_PATH` en tant que source de liste de révocation des certificats pour le cache de CRL de NetBackup.

Pour utiliser des listes de révocation des certificats provenant de ECA_CRL_PATH

1. Assurez-vous que les listes de révocation des certifications pour les autorités de certification externes sont stockées dans un répertoire et que le chemin d'accès au répertoire est accessible par l'hôte.

   Si vous disposez d'une instance d'application Flex Appliance, les fichiers doivent être enregistrés dans le répertoire suivant sur l'instance : `/mnt/nbdata/hostcert/crl`

   Vous pouvez spécifier les détails de liste CRL qui sont requis pour la configuration de l'autorité de certification externe pendant l'installation de NetBackup ou sa mise à niveau sur l'hôte.

   Sélectionnez l'une des options de liste CRL suivantes pendant l'installation ou la mise à niveau :

   - **Utiliser la liste de révocation de certificats définie dans le certificat** : aucune information supplémentaire requise.

- **Utiliser la CRL dans le chemin suivant** : vous êtes invité à indiquer un chemin d'accès à la liste CRL.
  Si vous choisissez d'utiliser l'option **Ne pas utiliser une liste de révocation de certificats**, le certificat de l'hôte homologue n'est pas vérifié par rapport à la liste CRL pendant la communication avec l'hôte.

Pour plus d'informations, consultez le Guide d'installation de NetBackup.

2. Spécifiez le chemin d'accès du répertoire de la liste de révocation des certificats pour l'option de configuration `ECA_CRL_PATH`.
3. Assurez-vous que l'option de configuration `ECA_CRL_CHECK` est définie sur une valeur différente de `DISABLE`.

   Pendant la communication avec l'hôte, l'état de révocation du certificat externe est vérifié avec la liste de révocation des certificats dans le cache de CRL de NetBackup qui contient les listes de révocation d'`ECA_CRL_PATH` .

   Par défaut, les listes de révocation des certificats provenant du cache sont mises à jour toutes les heures. Pour modifier l'intervalle de temps, définissez l'option `ECA_CRL_PATH_SYNC_HOURS` sur une valeur différente.

   Pour mettre à jour manuellement le cache de CRL avec les listes de révocation des certificats d'`ECA_CRL_PATH`, exécutez la commande `nbcertcmd -updateCRLCache`.

   Pour supprimer manuellement les listes de révocation des certificats à partir du cache de CRL, exécutez la commande `nbcertcmd -cleanupCRLCache`.

Comment les listes de révocation des certificats des URL du CDP sont utilisées

Utilisez cette section si vous souhaitez utiliser le point de distribution de la liste de révocation des certifications (CDP) en tant que source de liste de révocation des certificats (CRL) pour le cache de CRL de NetBackup.

Pour utiliser des listes de révocation des certification du CDP

1. Assurez-vous que l'option de configuration `ECA_CRL_PATH` n'est pas spécifiée.
2. Assurez-vous que l'hôte peut accéder aux URL qui sont spécifiées dans le CDP de l'hôte homologue.
3. Assurez-vous que l'option de configuration `ECA_CRL_CHECK` est définie sur une valeur différente de `DISABLE`.

   Pendant la communication avec l'hôte, l'état de révocation du certificat externe est vérifié avec la liste de révocation des certificats dans le cache de CRL de NetBackup contenant les listes de révocation des certificats des URL du CDP.

   Par défaut, les listes de révocation des certificats sont téléchargées à partir du CDP toutes les 24 heures et mises à jour dans le cache de CRL. Pour modifier l'intervalle de temps, définissez l'option de configuration `ECA_CRL_REFRESH_HOURS` sur une valeur différente.

   Pour supprimer manuellement les listes de révocation des certificats à partir du cache de CRL, exécutez la commande `nbcertcmd -cleanupCRLCache`.

À propos de l'inscription de certificats

Dans le cas de l'autorité de certification NetBackup, les certificats sont automatiquement inscrits sur le serveur maître pendant leur déploiement.

Si l'autorité de certification est externe, les certificats sont automatiquement inscrits sur le serveur maître lors de la communication de l'hôte si l'option `ECA_DISABLE_AUTO_ENROLLMENT` est activée. Vous pouvez inscrire le certificat manuellement à l'aide de la commande `nbcertcmd -enrollCertificate`.

Les certificats inscrits sont utilisés pour la communication avec l'hôte.

Se reporter à "Suppression de l'inscription de certificats" à la page 475.

À propos de l'inscription automatique d'un certificat externe

Un certificat externe d'un hôte est inscrit automatiquement auprès d'un serveur maître lorsque la communication est établie pour la première fois. Vous pouvez désactiver le processus automatique d'inscription de certificats et réaliser cette opération manuellement en utilisant la commande `nbcertcmd -enrollCertificate`.

Se reporter à "ECA_DISABLE_AUTO_ENROLLMENT pour serveurs et clients NetBackup" à la page 455.

Si l'inscription automatique est activée et que des certificats externes sont configurés pour la communication entre deux hôtes, NetBackup tente d'inscrire les certificats externes.

Les certificats externes sont inscrits sur le serveur maître associé. Ils seront alors utilisés pour les communications entre les hôtes associés à ce serveur maître.

Les certificats externes ne sont pas automatiquement inscrits dans les scénarios suivants :

- Communication avec les clients NAT
  Pour plus d'informations sur la prise en charge du client NAT dans NetBackup, consultez le Guide de l'administrateur NetBackup, volume I.
- Communication entre les serveurs de médias dans le cadre de la réplication d'image pour la déduplication du serveur de médias (MSDP)
- Communication avec la **console d'administration NetBackup**

A propos de l'affichage de l'état d'inscription des serveurs maîtres

Pour configurer un hôte NetBackup afin qu'il utilise un certificat externe, vous devez définir les options de configuration requises, puis inscrire un certificat pour l'hôte. Le certificat inscrit est utilisé pour la communication entre l'hôte et le domaine de serveur maître présent dans l'option `SERVER`.

Se reporter à "Configuration du serveur maître pour utiliser un certificat signé par une autorité de certification externe" à la page 467.

Se reporter à "Configuration d'un hôte NetBackup (serveur de médias, client ou nœud de cluster) de sorte à utiliser un certificat signé par une autorité de certification externe après l'installation" à la page 470.

Vous pouvez afficher l'état d'inscription en exécutant la commande `nbcertcmd -listEnrollmentStatus`. La commande répertorie uniquement les enregistrements où le nom de l'objet correspond au certificat configuré pour l'option `ECA_CERT_PATH`.

Les états d'inscription suivants sont affichés :

- Non inscrit : le certificat externe n'est pas inscrit sur ce domaine de serveur maître. Le serveur maître est présent dans la liste des serveurs maîtres de l'option `SERVER`.
- A mettre à jour : le certificat externe doit être inscrit à nouveau sur ce domaine de serveur maître.
- Inscrit : le certificat externe est inscrit sur le serveur maître.

Se reporter à "Inscription d'un certificat externe pour un hôte distant" à la page 472.

Configuration d'un certificat externe pour le serveur Web NetBackup

Remarque : Avant d'inscrire le certificat pour le serveur maître, vous devez terminer les étapes prérequises comme indiqué dans la rubrique suivante.

Se reporter à "Workflow d'utilisation de certificats externes pour la communication avec l'hôte NetBackup" à la page 441.

Par défaut, NetBackup utilise les certificats de sécurité que l'autorité de certification NetBackup a émis. Si vous disposez d'un certificat émis par une autorité de certification externe, vous pouvez configurer le serveur Web NetBackup afin qu'il l'utilise pour la communication sécurisée.

Remarque : Le magasin de certificats Windows n'est pas pris en charge en tant que source de certificats pour le serveur Web NetBackup.

Pour configurer un certificat externe pour le serveur Web

1. Vérifiez que vous disposez d'un certificat valide, de la clé privée du certificat et du lot de l'autorité de certification approuvée.
2. Exécutez la commande suivante :

   ```
   configureWebServerCerts -addExternalCert -nbHost -certPath
   certificate path -privateKeyPath private key path -trustStorePath
   CA bundle path [-passphrasePath passphrase file path]
   ```

   La commande `configureWebServerCerts` ne prend pas en charge l'utilisation des chemins d'accès au magasin de certificats Windows.

   Consultez le Guide de référence des commandes NetBackup pour plus d'informations sur les options de ligne de commande.

   - Dans une configuration en cluster, exécutez la commande suivante sur le nœud actif pour éviter un basculement :

     ```
     install_path/netbackup/bin/bpclusterutil -freeze
     ```

3. Redémarrez le service NetBackup Web Management Console Service pour indiquer les modifications.

   Sous UNIX, exécutez les commandes suivantes :

- *install_path*/netbackup/bin/nbwmc -terminate
- *install_path*/netbackup/bin/nbwmc start

Sous Windows, utilisez l'application **Services** du **Panneau de configuration Windows**.

Emplacement des commandes :

Windows	*install_path*\NetBackup\wmc\bin\install\
UNIX	*install_path*/wmc/bin/install

- Dans une configuration en cluster, libérez le cluster en utilisant la commande suivante sur le nœud actif :
  install_path/netbackup/bin/bpclusterutil -unfreeze

4 Vérifiez que vous pouvez accéder à l'interface utilisateur Web NetBackup à l'aide d'un navigateur, sans qu'aucun message d'avertissement de certificat ne s'affiche.

Mise à jour ou renouvellement de certificat externe pour le serveur Web

Vous pouvez mettre à jour ou renouveler le certificat externe que vous avez configuré pour le serveur Web.

Pour mettre à jour ou renouveler un certificat externe pour le serveur Web

1 Vérifiez que vous disposez du certificat externe le plus récent, de la clé privée correspondante et du fichier de lot de l'autorité de certification.

2 Exécutez la commande suivante (dans une configuration en cluster, exécutez la commande sur le nœud actif) :

```
configureWebServerCerts -addExternalCert -nbHost -certPath
certificate path -privateKeyPath private key path -trustStorePath
CA bundle path
```

Suppression du certificat externe configuré pour le serveur Web

Vous pouvez supprimer le certificat externe qui est configuré pour le serveur Web. Ensuite, NetBackup utilise le certificat signé par l'autorité de certification NetBackup pour la communication sécurisée.

Pour supprimer le certificat externe configuré pour le serveur Web

1. Exécutez la commande suivante (dans une configuration de serveur maître en cluster, exécutez cette commande sur le nœud actif) :

   ```
   configureWebServerCerts -removeExternalCert -nbHost
   ```

   - Dans une configuration de serveur maître en cluster, exécutez la commande suivante sur le nœud actif pour figer le cluster afin d'éviter un basculement :

     install_path/netbackup/bin/bpclusterutil -freeze

2. Redémarrez le service NetBackup Web Management Console Service.

   - Dans une configuration de serveur maître en cluster, exécutez la commande suivante sur le nœud actif pour libérer le cluster :

     install_path/netbackup/bin/bpclusterutil -unfreeze

Configuration du serveur maître pour utiliser un certificat signé par une autorité de certification externe

Un certificat basé sur un ID d'hôte NetBackup est déployé sur le serveur maître pendant l'installation ou la mise à niveau. Vous pouvez configurer le serveur maître pour utiliser un certificat signé par une autorité de certification externe après l'installation. Cela inclut :

- Définition des options de configuration de certificat externe
  Se reporter à "Options de configuration pour les certificats signés par une autorité de certification externe" à la page 442.
- Inscription du certificat externe pour l'hôte de serveur maître
  Le certificat inscrit est utilisé pour la communication entre l'hôte et le domaine de serveur maître répertorié dans l'option de configuration SERVER sur l'hôte.

Se reporter à "Affichage des certificats signés par une autorité de certification externe dans l'interface utilisateur Web NetBackup" à la page 474.

Se reporter à "Configuration d'un certificat externe pour un serveur maître en cluster" à la page 484.

Remarques importantes

- Vérifiez que le domaine NetBackup est activé pour utiliser les certificats signés par une autorité de certification externe en configurant le serveur Web NetBackup.

Se reporter à "Configuration d'un certificat externe pour le serveur Web NetBackup" à la page 465.

- Les certificats externes pour le serveur Web NetBackup et le serveur maître doivent être émis par la même autorité de certification racine.
  Si les deux autorités de certification ne concordent pas, la communication entre la **Console d'administration NetBackup** et le service NetBackup Web Management Console (service `nbwmc`) échoue.
- Assurez-vous que les listes de révocation de certificats de l'autorité de certification externe sont stockées à l'emplacement requis.
  Si un point de distribution de la liste de révocation de certificats (CDP) est utilisé, assurez-vous que les URL qui sont spécifiées dans le CDP sont accessibles.
  Se reporter à "À propos des listes de révocation des certifications pour l'autorité de certification externe" à la page 460.
- Lorsque le serveur principal NetBackup est configuré pour utiliser l'utilisateur du service (utilisateur sans privilège sous UNIX et service local sous Windows) pour démarrer la plupart des daemons ou des services, vérifiez que les chemins d'accès ECA suivants sont accessibles à l'utilisateur du service :
  - ECA_CERT_PATH
  - ECA_PRIVATE_KEY_PATH
  - ECA_TRUST_STORE_PATH
  - ECA_KEY_PASSPHRASEFILE (facultatif)
  - ECA_CRL_PATH (facultatif)

  Se reporter à "À propos d'un compte utilisateur du service NetBackup" à la page 609.
  Pour accorder l'accès à l'utilisateur du service, procédez comme suit :
  Sous UNIX, utilisez la commande `chmod` ou `chown`.
  Sous Windows, exécutez la commande suivante :
  install_path\NetBackup\bin\goodies\nbserviceusercmd.exe -addAcl *ECA path* -reason *reason*

Pour configurer le serveur maître afin d'utiliser un certificat externe

1. Mettez à jour le fichier de configuration NetBackup (fichier `bp.conf` dans le Registre UNIX ou Windows) sur le serveur maître avec les paramètres propres au certificat externe.

   Se reporter à "Options de configuration pour les certificats signés par une autorité de certification externe" à la page 442.

Pour le magasin de certificats Windows	Utilisez la commande `nbsetconfig` pour configurer les paramètres suivants : ■ ECA_CERT_PATH ■ ECA_CRL_CHECK (facultatif) ■ ECA_CRL_PATH (facultatif) ■ ECA_CRL_PATH_SYNC_HOURS (facultatif) ■ ECA_CRL_REFRESH_HOURS (facultatif) ■ ECA_DR_BKUP_WIN_CERT_STORE (facultatif)
Pour les certificats basés sur un fichier	Utilisez la commande `nbsetconfig` pour configurer les paramètres suivants : ■ ECA_CERT_PATH ■ ECA_PRIVATE_KEY_PATH ■ ECA_TRUST_STORE_PATH ■ ECA_KEY_PASSPHRASEFILE (facultatif) ■ ECA_CRL_CHECK (facultatif) ■ ECA_CRL_PATH (facultatif) ■ ECA_CRL_PATH_SYNC_HOURS (facultatif) ■ ECA_CRL_REFRESH_HOURS (facultatif) **Remarque :** Si vous disposez d'une instance d'application Flex Appliance, les fichiers de certificat doivent être enregistrés dans les répertoires suivants sur l'instance : ECA_CERT_PATH, ECA_PRIVATE_KEY et ECA_TRUST_STORE_PATH : `/mnt/nbdata/hostcert/` ECA_CRL_PATH : `/mnt/nbdata/hostcert/crl`

2 Exécutez la commande suivante sur le serveur maître pour inscrire un certificat externe sur le domaine de serveur maître défini dans l'option `SERVER` :

```
nbcertcmd -enrollCertificate
```

Pour plus d'informations sur la commande, consultez le Guide de référence des commandes de NetBackup.

Configuration d'un hôte NetBackup (serveur de médias, client ou nœud de cluster) de sorte à utiliser un certificat signé par une autorité de certification externe après l'installation

Un hôte NetBackup (serveur de médias ou client) est configuré pour utiliser un certificat externe pendant l'installation ou la mise à niveau. Vous avez la possibilité d'effectuer la configuration après l'installation.

Utilisez cette section pour configurer un hôte afin qu'il utilise un certificat externe.

Vous pouvez utiliser cette section afin de configurer un certificat externe pour un nœud de cluster.

Se reporter à "À propos de la configuration de certificat externe pour un serveur maître en cluster" à la page 479.

La configuration inclut les étapes suivantes :

- Définition des options de configuration de certificat externe
  Se reporter à "Options de configuration pour les certificats signés par une autorité de certification externe" à la page 442.
- Assurez-vous que l'inscription automatique est activée (l'option `ECA_DISABLE_AUTO_ENROLLMENT` est définie sur `TRUE`) ou inscrivez le certificat externe manuellement pour l'hôte
  Se reporter à "Inscription d'un certificat externe pour un hôte distant" à la page 472.
  Le certificat inscrit est utilisé pour la communication entre l'hôte et le domaine de serveur maître répertorié dans l'option de configuration `SERVER` sur l'hôte.

Le certificat inscrit est utilisé pour la communication avec l'hôte.

Se reporter à "Affichage des certificats signés par une autorité de certification externe dans l'interface utilisateur Web NetBackup" à la page 474.

Remarques importantes

- Vérifiez que le domaine NetBackup est activé pour utiliser les certificats signés par une autorité de certification externe en configurant le serveur Web NetBackup.
  Se reporter à "Configuration d'un certificat externe pour le serveur Web NetBackup" à la page 465.
- Il est recommandé d'inscrire un certificat externe pour l'hôte de serveur maître avant d'en inscrire un pour les autres hôtes.

Se reporter à "Configuration du serveur maître pour utiliser un certificat signé par une autorité de certification externe" à la page 467.

- Assurez-vous que les listes de révocation de certificats de l'autorité de certification externe sont stockées à l'emplacement requis.
  Si un point de distribution de la liste de révocation de certificats (CDP) est utilisé, assurez-vous que les URL qui sont spécifiées dans le CDP sont accessibles.
  Se reporter à "À propos des listes de révocation des certifications pour l'autorité de certification externe" à la page 460.

Pour configurer un hôte (serveur de médias ou client) afin d'utiliser un certificat externe

1 Mettez à jour le fichier de configuration (`bp.conf` ou Registre Windows) avec les paramètres propres au certificat externe requis sur l'hôte :

  Se reporter à "Options de configuration pour les certificats signés par une autorité de certification externe" à la page 442.

Pour le magasin de certificats Windows	Utilisez la commande `nbsetconfig` pour configurer les paramètres suivants : ■ ECA_CERT_PATH ■ ECA_CRL_CHECK (facultatif) ■ ECA_CRL_PATH (facultatif) ■ ECA_CRL_PATH_SYNC_HOURS (facultatif) ■ ECA_CRL_REFRESH_HOURS (facultatif) ■ ECA_DR_BKUP_WIN_CERT_STORE (facultatif)

Pour les certificats basés sur un fichier	Utilisez la commande `nbsetconfig` pour configurer les paramètres suivants : ■ ECA_CERT_PATH ■ ECA_PRIVATE_KEY_PATH ■ ECA_TRUST_STORE_PATH ■ ECA_KEY_PASSPHRASEFILE (facultatif) ■ ECA_CRL_CHECK_LEVEL (facultatif) ■ ECA_CRL_PATH (facultatif) ■ ECA_CRL_PATH_SYNC_HOURS (facultatif) ■ ECA_CRL_REFRESH_HOURS (facultatif) **Remarque :** Si vous disposez d'une instance d'application Flex Appliance, les fichiers de certificat doivent être enregistrés dans les répertoires suivants sur l'instance : ECA_CERT_PATH, ECA_PRIVATE_KEY et ECA_TRUST_STORE_PATH : `/mnt/nbdata/hostcert/` ECA_CRL_PATH : `/mnt/nbdata/hostcert/crl`

2 Assurez-vous que l'option de configuration `ECA_DISABLE_AUTO_ENROLLMENT` est définie sur `TRUE` à l'aide de la commande `nbgetconfig`. pour activer l'inscription automatique.

Si l'option est désactivée et que vous voulez inscrire manuellement le certificat, exécutez la commande suivante sur l'hôte pour inscrire un certificat externe sur le domaine de serveur maître défini via l'option de configuration `SERVER` sur l'hôte :

```
nbcertcmd -enrollCertificate
```

Se reporter à "A propos de l'affichage de l'état d'inscription des serveurs maîtres" à la page 464.

Pour plus d'informations sur la commande, consultez le *Guide de référence des commandes NetBackup*.

Inscription d'un certificat externe pour un hôte distant

Utilisez cette section pour inscrire un certificat externe pour un hôte NetBackup à distance. Ainsi, l'administrateur de sécurité est en mesure d'inscrire un certificat externe pour plusieurs hôtes distants depuis le même hôte.

Pour inscrire un certificat externe pour un hôte distant (ou pour exécuter une opération de synchronisation d'inscription) sur un hôte distant, assurez-vous que le serveur à partir duquel vous voulez inscrire le certificat figure dans l'option de configuration `SERVER` sur l'hôte distant.

Pour inscrire un certificat pour un hôte distant

- Sur l'hôte local, exécutez la commande suivante :

  ```
  nbcertcmd -enrollCertificate -remoteHost remote_host_name -server
  master_server_name
  ```

Inscrit un certificat externe pour l'hôte distant spécifié sur le serveur maître que vous fournissez avec l'option `-server`. Ce serveur maître doit être disponible dans l'option de configuration `SERVER` de l'hôte distant.

Se reporter à "Options de configuration pour les certificats signés par une autorité de certification externe" à la page 442.

Pour plus d'informations sur les commandes, consultez le *Guide de référence des commandes NetBackup*.

Affichage des autorités de certification prises en charge par votre domaine NetBackup

L'option de **configuration des certificats du serveur maître** dans la **console d'administration NetBackup** et l'**interface utilisateur Web NetBackup** affiche les autorités de certification (autorité de certification NetBackup, autorité de certification externe ou les deux) prises en charge par votre domaine NetBackup.

- Dans la **console d'administration NetBackup**, développez **Gestion de la sécurité > Paramètres de sécurité globaux** et cliquez sur l'onglet **Communication sécurisée** pour afficher les autorités de certification prises en charge.
- Dans l'**interface utilisateur Web NetBackup**, cliquez sur l'option **Paramètres de sécurité globaux** pour afficher les autorités de certification prises en charge.

Affichage des certificats signés par une autorité de certification externe dans l'interface utilisateur Web NetBackup

Vous pouvez afficher une liste des certificats externes qui sont fournis aux hôtes dans votre domaine en utilisant l'écran **Interface utilisateur Web NetBackup > Sécurité > Certificats**.

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

Renouvellement d'un certificat externe basé sur fichier

Utilisez cette section pour renouveler un certificat externe basé sur fichier sans redémarrer les services NetBackup

Lorsque vous remplacez les fichiers du certificat, de la clé privée et de la phrase de passe un par un alors que tous les services sont en cours de fonctionnement, la communication peut échouer en raison d'une erreur de correspondance entre le certificat et la clé privée. Pour éviter toute défaillance de communication, créez des copies des fichiers que NetBackup peut utiliser s'il existe une incompatibilité entre les fichiers.

Pour renouveler un certificat externe basé sur fichier

1. Effectuez une copie du fichier de certificat et renommez-le avec l'extension `.old`.

   Par exemple, si le nom du fichier de certificat est `cert.pem`, renommez-le `cert.pem.old`.

2. Faites une copie du fichier de clé privée et renommez-le avec l'extension `.old`.

3. Réalisez l'étape suivante si la clé privée du certificat est chiffrée.

   Effectuez une copie du fichier de phrase de passe et renommez-le avec l'extension `.old`.

4. Remplacez les fichiers de certificat, de clé privée et de phrase de passe d'origine par les fichiers renouvelés.

5. Assurez-vous que la communication avec l'hôte fonctionne avec le certificat renouvelé, puis supprimez les anciens fichiers de certificat.

Suppression de l'inscription de certificats

Vous pouvez supprimer l'inscription du certificat externe sur un serveur maître si vous ne voulez pas utiliser le certificat pour les communications de l'hôte.

Pour supprimer l'inscription de certificats

- Exécutez la commande suivante :

```
nbcertcmd -removeEnrollment -server master_server_name
```

Désactivation de l'autorité de certification NetBackup dans un domaine NetBackup

Utilisez cette section pour désactiver la prise en charge de l'autorité de certification NetBackup existante de votre domaine lorsque tous les hôtes dans votre domaine sont configurés pour utiliser des certificats externes pour la communication avec l'hôte.

Remarque : Si votre environnement contient des clients NAT et que le service NetBackup Messaging Broker (`nbmqbroker`) est activé, vous devrez peut-être redémarrer le service après avoir désactivé l'autorité de certification NetBackup afin d'utiliser uniquement les certificats externes.

Pour plus d'informations sur la prise en charge de NAT dans NetBackup, consultez le Guide de l'administrateur NetBackup, volume I.

Si les hôtes peuvent communiquer de manière sécurisée, mais ne peuvent pas être configurés pour utiliser des certificats externes (NetBackup 8.1, 8.1.1 ou 8.1.2), ne désactivez pas la configuration de l'autorité de certification NetBackup pour éviter une défaillance de la communication.

Pour désactiver la prise en charge de l'autorité de certification NetBackup dans votre domaine

1. Assurez-vous que tous les hôtes dans votre domaine sont configurés pour utiliser des certificats externes.

   Se reporter à "Configuration d'un certificat externe pour le serveur Web NetBackup" à la page 465.

   Se reporter à "Configuration du serveur maître pour utiliser un certificat signé par une autorité de certification externe" à la page 467.

   Se reporter à "Configuration d'un hôte NetBackup (serveur de médias, client ou nœud de cluster) de sorte à utiliser un certificat signé par une autorité de certification externe après l'installation" à la page 470.

2. Une fois l'ensemble des hôtes du domaine configurés pour utiliser des certificats externes, annulez la prise en charge de l'autorité de certification NetBackup de chaque hôte (serveurs de médias et clients) dans le domaine.

   Exécutez les commandes suivantes sur chaque hôte dans l'ordre indiqué :

   - `nbcertcmd -removeCACertificate -fingerPrint NetBackup CA certificate fingerprint`
   - `nbcertcmd -deleteCertificate -hostid` *`host ID of the host`*

3. Annulez la prise en charge de l'autorité de certification de l'autorité de certification NetBackup sur le serveur maître.

   Exécutez les commandes suivantes sur le serveur maître dans l'ordre indiqué :

   - `nbcertcmd -removeCACertificate -fingerPrint NetBackup CA certificate fingerprint`
   - `nbcertcmd -deleteCertificate -hostid` *`host ID of the master server`*

4. Révoquez tous les certificats basés sur l'ID d'hôte dans le domaine. Il s'agit d'une étape facultative.

   Se reporter à "Révoquer un certificat basé sur l'ID d'hôte" à la page 367.

5 Supprimez la prise en charge de l'autorité de certification NetBackup du serveur Web. Assurez-vous que vous n'avez pas besoin de certificats NetBackup pour la communication avec l'hôte.

Exécutez la commande suivante sur le serveur web :

```
configureWebServerCerts -removeNBCert
```

Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

6 Redémarrez NetBackup Web Management Console (`nbwmc`).

Activation de l'autorité de certification NetBackup dans un domaine NetBackup

Utilisez cette section pour permettre à un domaine NetBackup d'utiliser des certificats signés par l'autorité de certification NetBackup (ou des certificats basés sur l'ID d'hôte) pour la communication avec l'hôte.

Pour permettre à un domaine NetBackup de prendre en charge la configuration de l'autorité de certification NetBackup

1 Configurez le serveur Web NetBackup pour qu'il utilise des certificats NetBackup (basés sur l'ID d'hôte).

- Exécutez la commande suivante :

  ```
  configureWebServerCerts -addNBCert
  ```

  Se reporter à "Configuration d'un certificat externe pour le serveur Web NetBackup" à la page 465.

- Redémarrez NetBackup Web Management Console (`nbwmc`).

2 Déployez un certificat NetBackup basé sur l'ID d'hôte sur le serveur maître :

Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.

3 Déployez un certificat NetBackup basé sur l'ID d'hôte sur chaque hôte.

Se reporter à "Déploiement des certificats basés sur l'ID de l'hôte" à la page 338.

Désactivation d'une autorité de certification externe dans un domaine NetBackup

Utilisez cette section pour désactiver une autorité de certification externe dans un domaine NetBackup.

Pour désactiver une autorité de certification externe

1. Assurez-vous que chaque hôte dans le domaine est configuré pour utiliser des certificats basés sur l'ID d'hôte NetBackup.
2. Supprimez toutes les options de configuration de certificat externe dans le fichier de configuration (`bp.conf` sur le Registre Windows ou UNIX) présent sur l'hôte.

   Par exemple, `ECA_CERT_PATH`.

   Se reporter à "Options de configuration pour les certificats signés par une autorité de certification externe pour un nom virtuel" à la page 481.
3. Annulez la prise en charge de l'autorité de certification externe sur le serveur maître.
   - Supprimez toutes les options de configuration de certificat externe dans le fichier de configuration (`bp.conf` sur le Registre Windows ou UNIX) présent sur le serveur maître.

     Par exemple, `ECA_CERT_PATH`.

     Se reporter à "Options de configuration pour les certificats signés par une autorité de certification externe pour un nom virtuel" à la page 481.
4. Supprimez toutes les entrées de certificat externe de la base de données NetBackup.

   Exécutez la commande suivante :

   ```
   nbcertcmd -deleteECACertEntry -subject subject name of the certificate
   ```
5. Annulez la prise en charge de l'autorité de certification externe sur le serveur web.

   ```
   configureWebServerCerts -removeExternalCert
   ```

   Pour plus d'informations sur les commandes, consultez le Guide de référence des commandes NetBackup.

Modification du nom d'objet d'un certificat externe inscrit

Utilisez cette section pour modifier le nom d'objet d'un certificat externe déjà inscrit d'hôte.

Pour modifier le nom d'objet d'un certificat externe inscrit

1. Modifiez le nom d'objet du certificat.
2. Si l'hôte fait partie de plusieurs domaines de serveur maître, vous devez effectuer cette étape pour tous ces serveurs.

   Effectuez l'une des opérations suivantes :

   - Exécutez la commande suivante pour inscrire manuellement le certificat :
     `Install_Path/bin/nbcertcmd -enrollCertificate`
   - Exécutez la commande suivante pour supprimer l'inscription existante :
     `Install_Path/bin/nbcertcmd -removeEnrollment`

À propos de la configuration de certificat externe pour un serveur maître en cluster

Vous pouvez désormais utiliser des certificats X.509 émis par votre autorité de certification approuvée, pour un serveur maître en cluster.

Vous devez d'abord activer votre domaine NetBackup de sorte à utiliser les certificats signés par une autorité de certification externe en configurant le serveur Web NetBackup.

Vous pouvez ensuite configurer le serveur maître en cluster NetBackup pour qu'il utilise des certificats signés par une autorité de certification externe afin d'assurer une communication sécurisée avec l'hôte.

Se reporter à "Workflow permettant l'utilisation des certificats externes pour un serveur maître en cluster" à la page 480.

Remarques importantes

Consultez les remarques suivantes avant de configurer l'utilisation de certificats externes dans NetBackup :

- Le certificat NetBackup ou le certificat basé sur l'ID d'hôte est déployé sur le serveur maître pendant l'installation de NetBackup. Vous devez configurer manuellement un certificat externe sur le serveur maître en cluster après l'installation.
- Dans une configuration de serveur maître en cluster, vous devez configurer un certificat externe pour chaque nœud de cluster, qui se trouve sur le disque local de chaque nœud. En outre, vous devez configurer un certificat pour le nom virtuel, qui se trouve sur le disque partagé du cluster.
- Les options de configuration NetBackup (par exemple, `CLUSTER_ECA_CERT_PATH`) qui sont requises pour l'inscription de certificats externes pour le nom virtuel

sont enregistrées dans le fichier `nbcl.conf`. Ce fichier se trouve sur le disque partagé et les options de configuration de certificat externe pour chaque nœud de cluster sont enregistrées dans le fichier `bp.conf` ou le Registre Windows.

- Le magasin de certificats Windows n'est pas pris en charge en tant que source de certificats externes pour le nom virtuel. Il peut être utilisé en tant que source pour les certificats des nœuds de cluster.
- Il n'existe aucune option de configuration de liste CRL distincte pour le nom virtuel. En fonction de l'option de configuration `ECA_CRL_CHECK` sur le nœud, les listes CRL (`ECA_CRL_PATH` ou CDP) des nœuds de cluster sont utilisées pour vérifier l'état de révocation du certificat de l'hôte homologue pendant la communication. Par conséquent, les options de configuration de liste CRL doivent être définies avant d'utiliser un certificat externe pour le nom virtuel du serveur maître.
  Se reporter à "À propos des listes de révocation des certifications pour l'autorité de certification externe" à la page 460.

Workflow permettant l'utilisation des certificats externes pour un serveur maître en cluster

Pour configurer l'utilisation de certificats signés par une autorité de certification externe dans NetBackup afin d'assurer une communication sécurisée, vous devez effectuer les étapes suivantes dans l'ordre indiqué :

Tableau 17-13 Workflow d'utilisation de certificats externes dans une configuration en cluster

Étape	Processus
1	Vérifiez que : ■ Le certificat pour le nom virtuel est placé dans l'emplacement approprié sur le disque partagé. ■ Les certificats externes pour les nœuds de cluster sont placés dans les emplacements appropriés sur les nœuds. ■ Les listes CRL sont placées dans les emplacements requis sur les nœuds selon leurs options de configuration de liste CRL et elles sont accessibles. Se reporter à "À propos des listes de révocation des certifications pour l'autorité de certification externe" à la page 460.
2	Installez le logiciel NetBackup ou mettez à niveau le logiciel existant sur chaque nœud de cluster.

Étape	Processus
3	Activez le domaine NetBackup pour qu'il utilise des certificats externes en configurant le serveur Web NetBackup. Se reporter à "Configuration d'un certificat externe pour le serveur Web NetBackup" à la page 465.
4	Configurez un certificat externe pour le nom virtuel et pour chaque nœud de cluster. Se reporter à "Configuration d'un certificat externe pour un serveur maître en cluster" à la page 484.

Options de configuration pour les certificats signés par une autorité de certification externe pour un nom virtuel

Pour configurer un serveur maître NetBackup en cluster afin qu'il utilise un certificat signé par une autorité de certification externe pour la communication avec l'hôte, vous devez définir certaines options de configuration dans le fichier `nbcl.conf`.

Option CLUSTER_ECA_CERT_PATH pour le serveur principal en cluster

L'option `CLUSTER_ECA_CERT_PATH` est spécifique au serveur principal en cluster. Elle spécifie le chemin d'accès du certificat signé par l'autorité de certification externe du nom virtuel.

Tableau 17-14 Informations sur CLUSTER_ECA_CERT_PATH

Utilisation	Description
Où l'utiliser	Sur un serveur principal en cluster.
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Respectez le format suivant : `CLUSTER_ECA_CERT_PATH = Path to the certificate of the virtual identity`
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

Option CLUSTER_ECA_TRUST_STORE_PATH pour un serveur principal en cluster

L'option `CLUSTER_ECA_TRUST_STORE_PATH` est spécifique au serveur principal en cluster. Elle spécifie le chemin d'accès au fichier de lot de certificats qui contient tous les certificats d'autorité de certification racine approuvés au format PEM.

Tableau 17-15 Informations sur CLUSTER_ECA_TRUST_STORE_PATH

Utilisation	Description
Où l'utiliser	Sur un serveur principal en cluster.
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Respectez le format suivant : `CLUSTER_ECA_TRUST_STORE_PATH = Path to the external CA certificate`
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

Option CLUSTER_ECA_PRIVATE_KEY_PATH pour un serveur principal en cluster

L'option `CLUSTER_ECA_PRIVATE_KEY_PATH` est spécifique au serveur principal en cluster. Elle spécifie le chemin d'accès à la clé privée pour le certificat signé par l'autorité de certification externe du nom virtuel.

Si la clé privée du certificat de nom virtuel est chiffrée, vous devez définir l'option `CLUSTER_ECA_KEY_PASSPHRASEFILE`.

Se reporter à "Option CLUSTER_ECA_KEY_PASSPHRASEFILE pour un serveur principal en cluster" à la page 483.

Tableau 17-16 Informations sur CLUSTER_ECA_PRIVATE_KEY_PATH

Utilisation	Description
Où l'utiliser	Sur un serveur principal en cluster.

Utilisation	Description
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Respectez le format suivant : `CLUSTER_ECA_PRIVATE_KEY_PATH = Path to the private key of the external certificate`
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

Option CLUSTER_ECA_KEY_PASSPHRASEFILE pour un serveur principal en cluster

L'option `CLUSTER_ECA_KEY_PASSPHRASEFILE` est spécifique au serveur principal en cluster. Elle spécifie le chemin d'accès au fichier texte contenant la phrase de passe de la clé privée du certificat du nom virtuel.

`CLUSTER_ECA_KEY_PASSPHRASEFILE` est facultative. Vous devez définir cette option si la clé privée du certificat du nom virtuel est chiffrée.

Se reporter à "Option CLUSTER_ECA_PRIVATE_KEY_PATH pour un serveur principal en cluster" à la page 482.

Tableau 17-17 Informations sur CLUSTER_ECA_KEY_PASSPHRASEFILE

Utilisation	Description
Où l'utiliser	Sur un serveur principal en cluster.
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le NetBackupGuide de référence des commandes . Respectez le format suivant : `CLUSTER_ECA_KEY_PASSPHRASE_FILE = Path to the passphrase file`
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

Configuration d'un certificat externe pour un serveur maître en cluster

Utilisez cette section afin de configurer un certificat signé par une autorité de certification externe pour un serveur maître en cluster. Le certificat inscrit est utilisé pour la communication avec l'hôte.

Conditions requises

- Vérifiez que le domaine NetBackup est activé pour utiliser les certificats signés par une autorité de certification externe en configurant le serveur Web NetBackup.

  Se reporter à "Configuration d'un certificat externe pour le serveur Web NetBackup" à la page 465.

- Vérifiez que les certificats externes pour le serveur Web NetBackup et le nom virtuel sont émis par la même autorité de certification.

  Si les deux autorités de certification ne concordent pas, la communication entre la **console d'administration NetBackup** et le service NetBackup Web Management Console (service `nbwmc`) échoue.

Pour inscrire un certificat externe pour un serveur maître en cluster

1. Mettez à jour le fichier de configuration NetBackup qui est présent sur le disque partagé (`nbcl.conf`) avec les options de configuration de certificat externe.

   Se reporter à "Options de configuration pour les certificats signés par une autorité de certification externe pour un nom virtuel" à la page 481.

   Utilisez la commande `nbsetconfig` pour configurer les options suivantes :

   - `CLUSTER_ECA_CERT_PATH`
   - `CLUSTER_ECA_TRUST_STORE_PATH`
   - `CLUSTER_ECA_PRIVATE_KEY_PATH`
   - `CLUSTER_ECA_KEY_PASSPHRASEFILE` (facultatif)

   Vous devez configurer les options de configuration de liste CRL pour chaque nœud.

Se reporter à "À propos des listes de révocation des certifications pour l'autorité de certification externe" à la page 460.

2 Exécutez la commande suivante sur le serveur maître :

```
nbcertcmd -enrollCertificate -cluster
```

Le certificat inscrit est utilisé pour la communication entre le nœud actif et le domaine de serveur maître répertorié dans l'option de configuration `SERVER` sur l'hôte.

Pour plus d'informations sur la commande, consultez le *Guide de référence des commandes NetBackup*.

3 Configurez un certificat externe sur chaque nœud de cluster.

Se reporter à "Configuration d'un hôte NetBackup (serveur de médias, client ou nœud de cluster) de sorte à utiliser un certificat signé par une autorité de certification externe après l'installation" à la page 470.

Chapitre 18

Régénération de clés et de certificats

Ce chapitre traite des sujets suivants :

Régénération des clés et des certificats

Certaines clés et certains certificats peuvent être recréés simplement en redémarrant les services NetBackup. Si vous rencontrez des erreurs liées aux clés ou aux

certificats, en tant que pratique d'excellence, redémarrez les services NetBackup et vérifiez si les clés ou les certificats sont recréés. Si la clé ou le certificat n'est pas créé, suivez les procédures présentées dans les sections suivantes.

Régénération des clés et des certificats du courtier d'authentification NetBackup

Suivez les étapes pour régénérer les éléments suivants pour les courtiers d'authentification NetBackup :

- Clés publiques et privées sur le serveur maître et le serveur de médias.
- Certificats sur le serveur de médias et les clients.

Pour régénérer des clés et des certificats du courtier d'authentification NetBackup

1. Redémarrez le service d'authentification NetBackup. Assurez-vous que le service est en cours d'exécution.
2. Exécutez la commande suivante :

   ```
   bpnbaz -ConfigureAuth
   ```

   À l'invite, répondez **o**.

   Pour obtenir des informations sur la commande, consultez le *Guide de référence des commandes de NetBackup*.
3. Redémarrez tous les services NetBackup. Avant de redémarrer les services, assurez-vous qu'aucun travail n'est en cours d'exécution.

   Pour plus d'informations sur le redémarrage des services, consultez le *Guide de l'administrateur de NetBackup, volume I*.

Régénération des clés et des certificats d'identité d'hôte

Pour régénérer les clés publiques d'identité hôte, les clés privées et les certificats sur le serveur maître, le serveur de médias et les clients :

- Modifiez la paire de clés pour un hôte.
  Modification des résultats d'une paire de clés dans un nouveau certificat basé sur l'ID d'hôte et un nouveau certificat basé sur le nom d'hôte.
  Se reporter à "Modification de la paire de clés pour un hôte" à la page 356.

Régénération des clés et des certificats de service web

Suivez les étapes pour régénérer une clé et un certificat publique/public de service web sur le serveur maître.

Pour régénérer des clés et des certificats de service web

1. Générez le certificat de sécurité. Exécutez la commande suivante :
   - Windows

     ```
     set WEBSVC_PASSWORD=<Mot de l'utilisateur>
     nbcertconfig -t -user <Nom utilisateur>
     ```

   - UNIX

     ```
     export WEBSVC_PASSWORD=<Mot de passe de l'utilisateur>
     nbcertconfig -t -user <Nom utilisateur>
     ```

2. Configurez le service d'authentification NetBackup pour l'utilisateur de service web et le service web. Exécutez la commande suivante :

   ```
   nbcertconfig -u -user <Nom utilisateur>
   nbcertconfig -m -user <Nom utilisateur>
   ```

3. Redémarrez le service d'authentification NetBackup.

Régénération des clés et des certificats nbcertservice

Suivez les étapes pour régénérer des clés et des certificats nbcertservice sur le serveur maître.

Pour régénérer des clés et des certificats nbcertservice

1. Supprimez l'ancien dossier avec le nom d'utilisateur.
2. Générez le certificat de sécurité. Exécutez la commande suivante :
   - Windows

     ```
     set WEBSVC_PASSWORD=<Mot de l'utilisateur>
     nbcertconfig -u -user <Nom utilisateur>
     ```

   - UNIX

     ```
     export WEBSVC_PASSWORD=<Mot de passe de l'utilisateur>
     nbcertconfig -u -user <Nom utilisateur>
     ```

Régénération des clés et des certificats tomcat

Suivez les étapes pour générer la clé publique tomcat, la clé privée et les certificats sur le serveur maître.

Remarque : La clé jkskey est une clé pour déchiffrer le keystore utilisé par tomcat et est sauvegardée en tant qu'élément de la sauvegarde de catalogue. Il est inutile de la régénérer.

Pour régénérer des clés et des certificats tomcat

1. Générez le certificat de sécurité. Exécutez la commande suivante :
   - Windows

     ```
     set WEBSVC_PASSWORD=<Password of User>
     nbcertconfig -t -user <User Name>
     ```
   - UNIX

     ```
     export WEBSVC_PASSWORD=<Password of User>
     nbcertconfig -t -user <User Name>
     ```
2. Régénérer d'autres fichiers dans le dossier `tomcatcreds`, outre le `magasin de clés` et le fichier d'`informations d'authentification`. Exécutez la commande suivante :
   - Windows

     ```
     c:\Program
     Files\Veritas\NetBackup\wmc\bin\install>configurecerts.bat
     ```
   - UNIX

     ```
     /usr/openv/wmc/bin/install/configurecerts
     ```

Régénération des clés JWT

Pour régénérer des clés JWT publiques et privées sur le serveur maître :

- Fermez la console d'administration NetBackup et redémarrez tous les services NetBackup.
  Pour plus d'informations sur le redémarrage des services, consultez le *Guide de l'administrateur NetBackup, volume I*.

Régénération de certificats de passerelle NetBackup

Pour régénérer des certificats nbgateway sur le serveur maître :

- Redémarrez la totalité du service NetBackup.
  Pour plus d'informations sur le redémarrage des services, consultez le *Guide de l'administrateur NetBackup, volume I*.

Régénération de certificats de magasin d'approbation Web

Pour générer des certificats de magasin d'approbation Web sur les serveurs maître et de médias, exécutez la commande suivante :

```
nbcertcmd -getCACertificate
```

À l'invite, répondez **o**.

Pour plus d'informations sur la commande nbcertcmd, consultez le *Guide de référence des commandes NetBackup*.

Régénération des certificats de plug-in vCenter VMware

Suivez les étapes pour régénérer des certificats de plug-in vCenter sur le serveur maître.

Pour régénérer les certificats de plug-in vCenter VMware

1. Listez les certificats existants et identifiez l'entrée existante pour les certificats non valides. Exécutez la commande suivante :
   - Windows
     ```
     C:\Program
     Files\Veritas\NetBackup\wmc\bin\install\manageClientCerts.bat
     -list
     ```
   - UNIX
     ```
     /usr/openv/wmc/bin/install/manageClientCerts -list
     ```
2. Supprimez le certificat non valide. Exécutez la commande suivante :
   - Windows

```
C:\Program
Files\Veritas\NetBackup\wmc\bin\install\manageClientCerts.bat
-delete
```

- UNIX

  ```
  /usr/openv/wmc/bin/install/manageClientCerts -delete
  ```

3. Générez un nouveau certificat. Exécutez la commande suivante :

   - Windows

     ```
     C:\Program
     Files\Veritas\NetBackup\wmc\bin\install\manageClientCerts.bat
     -create <master_server_name>
     ```

   - UNIX

     ```
     /usr/openv/wmc/bin/install/manageClientCerts -create
     <master_server_name>
     ```

4. Enregistrez le nouveau certificat créé avec le plug-in vCenter.

   Pour plus d'informations, consultez le *Guide du plug-in NetBackup pour VMware vCenter*.

Régénération des certificats de session de la console d'administration NetBackup

Pour régénérer des certificats de session sur le serveur maître :

- Fermez la console d'administration NetBackup et redémarrez tous les services NetBackup.

  Pour plus d'informations sur le redémarrage des services, consultez le *Guide de l'administrateur NetBackup, volume I*.

Régénération des clés et des certificats OpsCenter

Suivez les étapes pour régénérer des clés et des certificats OpsCenter :

Pour régénérer des clés et des certificats OpsCenter

1. Reconfigurez l'authentification. Exécutez les commandes suivantes sur le serveur OpsCenter :

   ```
   OpsCenter_Install_path\server\bin\stopAt

   OpsCenter_Install_path\server\bin\configureAt

   OpsCenter_Install_path\server\bin\startAt
   ```

2. Redémarrez les services OpsCenter. Exécutez les commandes suivantes sur le serveur OpsCenter :

   ```
   OpsCenter_Install_path\server\bin>opsadmin.bat stop

   OpsCenter_Install_path\server\bin>opsadmin.bat start
   ```

Pour plus d'informations sur les commandes OpsCenter, consultez le *NetBackupGuide de l'administrateur OpsCenter*.

Régénération du fichier de clé de chiffrement NetBackup

Pour régénérer le fichier de clé de chiffrement NetBackup, exécutez la commande suivante :

```
bpkeyutil -clients client_name1,client_name2,...,client_namen
```

À l'invite, entrez la phrase de passe que vous aviez initialement enregistrée.

Pour plus d'informations sur les fichiers de clés, voir Se reporter à "Création des fichiers de clés de chiffrement sur les clients" à la page 507.

Pour effectuer cette tâche à l'aide de la commande `bpkeyutil`, consultez le *Guide de référence des commandes NetBackup*.

Section 3

Chiffrement des données au repos

Chapitre 19

Sécurité du chiffrement des données au repos

Ce chapitre traite des sujets suivants :

Terminologie de chiffrement de données au repos

Le tableau suivant décrit la terminologie de chiffrement de données au repos.

Tableau 19-1 Terminologie de chiffrement de données au repos

Terme	Description
Advanced Encryption Standard (AES)	Indique l'algorithme de chiffrement synchrone qui a remplacé le DES.
Chiffrement asynchrone	Comprend les algorithmes de chiffrement qui utilisent une clé publique et une clé privée.

Terme	Description
Norme de chiffrement des données (DES)	Indique la norme de chiffrement des données synchrone acceptée des années 1970 jusqu'en 1998.
Vecteur d'initialisation	Indique une valeur de lancement qui est utilisée pour préparer un algorithme de chiffrement. La préparation permet de brouiller toutes les éventuelles structures reconnaissables en utilisant la même clé pour chiffrer un certain nombre de fichiers de données. Ces fichiers commencent par la même structure.
Chiffrement de clé publique	Utilise le chiffrement asynchrone.
Chiffrement synchrone	Comprend les algorithmes de chiffrement qui utilisent la même clé pour le chiffrement et le déchiffrement. Pour une taille de clé identique, les algorithmes synchrones sont plus rapides et plus sécurisés que leurs homologues asynchrones.

Considérations de chiffrement des données au repos

Le tableau suivant décrit les limitations du chiffrement de données au repos.

Tableau 19-2 Limitations du chiffrement de données au repos

Limitation	Description
Effet du chiffrement des données sur les performances de l'ordinateur	Les algorithmes de chiffrement sont comme des algorithmes de compression de données car ils utilisent une grande quantité d'UC. La compression de données sans ajout de matériel informatique (dédié ou partagé), peut affecter l'ordinateur et les performances de NetBackup.
La compression de données doit être exécutée avant le chiffrement des données	Les algorithmes de compression de données recherchent des modèles de configuration de données pour compresser les données. Les algorithmes de chiffrement brouillent les données et suppriment toutes les configurations. Par conséquent, si la compression de données est souhaitée, elle doit être effectuée avant l'étape de chiffrement des données.
Choix d'un algorithme de chiffrement	Il existe de nombreux algorithmes de chiffrement et tailles de clé associées. Quel choix proposer à un utilisateur pour le chiffrement des données ? AES (Advanced Encryption Standard) est devenue la norme de chiffrement des données et prend en charge les clés de chiffrement 128, 192 ou 256 bits.
Taille de clé suggérée	En général plus la clé est grande, plus elle est sécurisée et plus longtemps les données seront sécurisées. AES est l'un des meilleurs choix parce qu'il est considéré comme sûr avec chacune des trois tailles de clé (128, 192, 256 bits) prises en charge.

Limitation	Description
Certification de FIPS pour ma solution de chiffrement	Alors que la certification FIPS peut être requise pour son utilisation par le gouvernement des USA, ce ne devrait pas être le seul critère utilisé pour évaluer une solution de chiffrement. D'autres éléments devraient faire partie de tout processus de prise de décision comme suit : ■ Les certificats FIPS s'appliquent seulement à la version nommée d'un produit. C'est uniquement lorsque le produit est utilisé conformément à la "Politique de sécurité de FIPS", le document qui est soumis quand le produit a été validé. Les futures versions de produit et des utilisations non standard seraient soumis à une mise en cause de la validation. ■ La sécurité des algorithmes comme AES ne réside pas dans l'opacité de leur fonctionnement. Au contraire, la sécurité réside dans la difficulté à déduire une clé de chiffrement inconnue. Des années d'examen minutieux et de l'examen par les pairs d'ES, ont généré des mises en application matures. En fait, des tests existent pour AES, les clés et les ensembles de données spécifiques y sont entrés et vérifiés par rapport au résultat attendu. ■ Le chiffrement des données est similaire au degré de sécurité dans l'automobile. La plupart des problèmes sont liés à des clés perdues/mal placées, non pas à des verrous défectueux. ■ Puisque les abus peuvent souvent engendrer des problèmes, l'utilisation d'un produit de chiffrement devrait être envisagée. Les considérations d'utilisation incluent ce qui suit : ■ Intégration du chiffrement avec le produit ■ Intégration du chiffrement dans les processus d'affaires. ■ Niveau de granularité de clé de chiffrement approprié ■ Possibilité de récupération

Limitation	Description
Niveau de granularité de clé de chiffrement approprié	Cette granularité de clé de chiffrement appropriée peut expliquer avec l'exemple de la sécurité à la maison. Il est pratique d'avoir une seule clé pour la maison. Vous pouvez entrer dans votre garage, ouvrir la porte d'entrée ou la porte du jardin en utilisant la même clé. Cette sécurité est bonne jusqu'à ce que la clé soit compromise (par exemple, si la clé est dérobée). Vous êtes alors obligé de remplacer tous les verrous associés a cette clé. Un exemple extrême est de disposer d'une clé pour chaque tiroir ou placard de la maison. La perte d'une clé n'imposerait alors le remplacement que d'un seul verrou. La solution appropriée se situe probablement quelque part entre ces deux extrêmes. Vous devez évaluer votre niveau de tolérance vis à vis d'une clé compromise ou perdue d'un point de vue commercial. Une clé perdue implique que toutes les données qui sont chiffrées avec cette clé sont détruites. Une clé compromise implique que toutes les données qui sont chiffrées avec cette clé doivent être déchiffrées et être chiffrées à nouveau pour redevenir sécurisées.

Types de destination pour le chiffrement des données au repos

Les types de destination suivants sont disponibles pour le chiffrement des données au repos :

- Chiffrement côté client
  Se reporter à "A propos du chiffrement de client NetBackup" à la page 499.
- Chiffrement MSDP
  Consultez la rubrique « À propos du chiffrement MSDP » dans le Guide de déduplication NetBackup.
- Chiffrement de lecteur de bande : le nom du pool de volumes doit comporter le préfixe `ENCR_` pour que NetBackup autorise le chiffrement pour les bandes.
- Chiffrement cloud
  Consultez la rubrique « À propos du chiffrement des données pour le stockage en cloud » dans le Guide de l'administrateur NetBackup Cloud.
- AdvancedDisk : le nom du pool de disques doit comporter le préfixe `ENCR_` pour que NetBackup autorise le chiffrement pour AdvancedDisk.

Questions importantes sur la sécurité du chiffrement

Avant d'envisager la sécurité de chiffrement, les questions suivantes doivent être étudiées.

Les réponses dépendent de vos besoins particuliers de chiffrement comme suit :

- Comment puis-je choisir le meilleur chiffrement ?
- Pourquoi utiliser la sécurité de chiffrement ?
- De quelle protection ai-je besoin contre les attaques internes éventuelles ?
- De quelle protection ai-je besoin contre les attaques externes éventuelles ?
- Quelles sont les zones de NetBackup que la sécurité de chiffrement protège ?
- Ai-je besoin de créer des schémas de l'architecture de NetBackup affichant la sécurité de chiffrement au travail ?
- Dans quels cas ai-je besoin d'utiliser le déploiement pour la sécurité du chiffrement ?

Comparaison des options de chiffrement

Les options NetBackup suivantes existent pour le chiffrement des données au repos :

- Chiffrement du client NetBackup avec chiffrement standard
- Chiffrement du client NetBackup avec chiffrement hérité
- Appliances et périphériques matériels de chiffrement tiers

Le tableau suivant présente les options de chiffrement disponibles avec leurs avantages et inconvénients potentiels.

Tableau 19-3 Comparaison des options de chiffrement

Option de chiffrement	Avantages potentiels	Inconvénients potentiels
Chiffrement du client, chiffrement standard Se reporter à "Configuration du chiffrement standard sur des clients" à la page 504.	■ La clé de chiffrement se trouve sur l'ordinateur client et est contrôlée par l'administrateur de NetBackup ■ Peut être déployé sans affecter les serveurs maîtres et de médias NetBackup ■ Peut être déployé sur une base client	■ La clé de chiffrement sur le client ne s'adapte pas parfaitement aux environnements où chaque client doit disposer d'une seule clé de chiffrement et d'une clé de chiffrement individuelle. ■ Le chiffrement et la compression ayant lieu sur le client peuvent affecter la performance client

Option de chiffrement	Avantages potentiels	Inconvénients potentiels
Chiffrement du client, chiffrement hérité Se reporter à "Configuration du chiffrement hérité sur les clients" à la page 512.	Mêmes avantages que le chiffrement du client avec chiffrement standard.	Mêmes inconvénients que le chiffrement du client avec chiffrement standard.
Appliances et périphériques matériels de chiffrement tiers	■ Peu ou pas d'incidence sur les performances due au matériel ajouté. ■ Généralement certifié NIST FIPS 140.	■ Les laboratoires d'essais de compatibilité de NetBackup testent certaines de ces solutions. Ces tests ne constituent ni une approbation, ni un rejet ni une solution particulière. Ils permettent de s'assurer que la fonctionnalité de base a été vérifiée dans le cadre d'une utilisation avec une version spécifique de NetBackup. ■ Aucune intégration avec la configuration, le fonctionnement ou le diagnostic de NetBackup. ■ Le scénario de reprise après incident est fourni par l'appliance ou le périphérique.

A propos du chiffrement de client NetBackup

L'option de chiffrement de client NetBackup est plus adaptée dans les cas suivants :

- Clients qui peuvent traiter la charge d'UC pour la compression/ le chiffrement
- Clients qui veulent conserver la maîtrise des clés de chiffrement des données
- Situations où l'intégration la plus étroite de NetBackup et du chiffrement est souhaitable
- Situations où le chiffrement est nécessaire client par client

Conditions d'installation requises pour la sécurité par chiffrement

Les sauvegardes chiffrées requièrent le logiciel de chiffrement de NetBackup, qui est inclus dans les installations de clients et de serveurs NetBackup. Pour pouvoir utiliser le chiffrement, vous devez disposer d'une licence valide. Consultez le Guide de l'administrateur NetBackup, volume I pour plus de détails sur la gestion des licences NetBackup.

Guide de l'administrateur NetBackup, Volume I

Pour une liste des plates-formes sur lequel vous pouvez configurer le chiffrement de NetBackup, consultez les notes de mise à jour de NetBackup.

Exécution d'une sauvegarde de chiffrement

Vous pouvez exécuter une sauvegarde de chiffrement comme suit :

- Choix du chiffrement pour une sauvegarde
  Se reporter à "Choix du chiffrement pour une sauvegarde" à la page 500.
- Processus standard de sauvegarde de chiffrement
  Se reporter à "Processus standard de sauvegarde de chiffrement" à la page 501.
- Processus hérité de sauvegarde de chiffrement
  Se reporter à "Processus hérité de sauvegarde de chiffrement" à la page 502.

Choix du chiffrement pour une sauvegarde

Quand une sauvegarde démarre, le serveur détermine à partir d'un attribut de politique si la sauvegarde doit être chiffrée. Le serveur se connecte ensuite au bpcd sur le client pour lancer la sauvegarde et transmet l'attribut de politique de **chiffrement** vers la requête de sauvegarde.

Le client compare l'attribut de politique de **chiffrement** à CRYPT_OPTION dans la configuration sur le client comme suit :

- Si l'attribut de politique est défini sur oui et CRYPT_OPTION sur REQUIRED ou ALLOWED, le client effectue une sauvegarde chiffrée.
- Si l'attribut de politique est défini sur oui et CRYPT_OPTION sur DENIED, le client n'effectue aucune sauvegarde.
- Si l'attribut de politique est défini sur aucun et CRYPT_OPTION sur ALLOWED ou DENIED, le client effectue une sauvegarde non chiffrée.
- Si l'attribut de politique est défini sur aucun et CRYPT_OPTION sur REQUIRED, le client n'effectue pas la sauvegarde.

Le tableau suivant affiche le type de sauvegarde qui est effectuée pour chaque condition :

Tableau 19-4 Type de sauvegarde effectué

CRYPT_OPTION	Attribut de politique de chiffrement avec CRYPT_OPTION	Attribut de politique de chiffrement sans CRYPT_OPTION
REQUIRED	Chiffré	Aucun

CRYPT_OPTION	Attribut de politique de chiffrement avec CRYPT_OPTION	Attribut de politique de chiffrement sans CRYPT_OPTION
ALLOWED	Chiffré	Non chiffré
DENIED	Aucun	Non chiffré

Se reporter à "Processus standard de sauvegarde de chiffrement" à la page 501.

Se reporter à "Processus de restauration du chiffrement standard NetBackup" à la page 503.

Se reporter à "Processus hérité de sauvegarde de chiffrement" à la page 502.

Se reporter à "Processus de restauration du chiffrement hérité de NetBackup" à la page 503.

Processus standard de sauvegarde de chiffrement

Les conditions préalables de chiffrement d'une sauvegarde standard sont les suivantes :

- **Remarque :** Dans NetBackup 7.5 et les versions ultérieures, le logiciel de chiffrement est automatiquement installé avec le serveur NetBackup UNIX et les installations du client.

  Un fichier de clés doit exister. Le fichier de clés est créé lorsque vous exécutez la commande `bpkeyutil` à partir du serveur ou du client.

- L'attribut de **chiffrement** doit être sélectionné dans la politique NetBackup qui inclut le client.

Si les conditions préalables sont satisfaites, la sauvegarde se déroule comme suit :

- Le client prend la dernière clé dans le fichier de clé.

  Pour chaque fichier qui est sauvegardé :

  - Le client crée un en-tête de chiffrement `tar`. L'en-tête `tar` contient une somme de contrôle de la clé et du chiffre que NetBackup a utilisés pour le chiffrement.
  - Pour enregistrer les données du fichier qui ont été chiffrées avec la clé, le client utilise le chiffre défini par l'entrée de configuration de CRYPT_CIPHER. (Le chiffre par défaut est AES-128-CFB.)

  Remarque : Seules les données de fichier sont chiffrées. Les noms de fichiers et les attributs ne sont pas chiffrés.

- L'image de sauvegarde sur le serveur inclut un indicateur qui signale si la sauvegarde a été chiffrée.

Processus hérité de sauvegarde de chiffrement

Les conditions préalables de chiffrement d'une sauvegarde héritée sont les suivantes :

- Le logiciel de chiffrement doit inclure la bibliothèque DES appropriée, comme suit :
  - Pour le chiffrement DES 40 bits, `libvdes40.`suffix; le suffixe est `so`, `sl`, ou `dll`, selon la plate-forme cliente.
  - Pour le chiffrement du 56 bits DES, `libvdes56.`suffix; le suffixe est `so`, `sl`, ou `dll`, selon la plate-forme cliente.

    Remarque : Le logiciel de chiffrement est automatiquement installé avec les installations serveur et client NetBackup UNIX.

- Un fichier de clé spécifié avec l'option de configuration CRYPT_KEYFILE doit exister. Lorsque vous spécifiez une phrase secrète NetBackup à l'aide de la commande de serveur `bpinst` ou de la commande client `bpkeyfile`, vous créez un fichier de clé.
- Vous devez sélectionner l'attribut de **chiffrement** sur la politique NetBackup qui inclut le client.

Si les conditions préalables sont réunies et que la sauvegarde doit être chiffrée, les événements suivants se produisent :

- Le client récupère les dernières données de son fichier de clé et les fusionne avec l'heure actuelle (l'heure de sauvegarde) pour générer une clé DES. Pour le DES 40 bits, 16 bits de la clé sont toujours définis sur zéro.

  Pour chaque fichier sauvegardé, les événements suivants se produisent :
  - Le client crée un en-tête `tar` de chiffrement. L'en-tête `tar` contient une somme de contrôle du DES que NetBackup a utilisé pour le chiffrement.
  - Le client écrit les données de fichier qui ont été chiffrées avec la clé DES. Notez que seules les données de fichier sont chiffrées. Les noms et les attributs de fichier ne sont pas chiffrés.
- Le serveur indique les noms de fichier, les attributs et les données du client et les enregistre sur une image de sauvegarde sur le serveur. Le serveur N'EXECUTE PAS le chiffrement ou le déchiffrement des données. L'image de

sauvegarde sur le serveur inclut l'heure de sauvegarde et un indicateur qui signale si la sauvegarde a été chiffrée.

Processus de restauration du chiffrement standard NetBackup

Les prérequis à la restauration d'une sauvegarde chiffrée standard sont les suivants :

- Le logiciel de chiffrement doit être chargé sur le client.

  Remarque : Le logiciel de chiffrement est automatiquement installé avec les installations serveur et client NetBackup UNIX.

- Un fichier de clé doit exister. Le fichier de clé est créé lorsque vous exécutez la commande `bpkeyutil` à partir du serveur ou du client.

Quand la restauration se produit, le serveur détermine à partir de l'image de sauvegarde si la sauvegarde a été chiffrée. Le serveur se connecte ensuite à `bpcd` sur le client pour lancer la restauration. Le serveur envoie au client un indicateur de chiffrement sur la demande de restauration.

Quand une sauvegarde a correctement lieu, la restauration se produit comme suit :

- Le serveur envoie des noms de fichier, des attributs et des données de fichiers chiffrés au client à restaurer.
- Si le client lit un en-tête de chiffrement `tar`, le client compare la somme de contrôle dans l'en-tête aux sommes de contrôle des clés dans le fichier de clé. Si la somme de contrôle des clés correspond à la somme de contrôle de l'en-tête, NetBackup utilise cette clé pour déchiffrer les données de fichier. Il utilise le chiffre défini dans l'en-tête.
- Le fichier est déchiffré et restauré si une clé et un chiffre sont disponibles. Si la clé ou le chiffre ne sont pas disponibles, le fichier n'est pas restauré et un message d'erreur est généré.

Processus de restauration du chiffrement hérité de NetBackup

Les conditions préalables de restauration d'une sauvegarde chiffrée héritée sont les suivantes :

- Le logiciel de chiffrement hérité doit être chargé sur le client.

  Remarque : Le logiciel de chiffrement est automatiquement installé avec les installations serveur et client NetBackup UNIX.

- Le logiciel de chiffrement doit inclure la bibliothèque DES 40 bits. Le nom de la bibliothèque DES 40 bits est `libvdes40.`suffix; le suffixe est `so`, `sl`, ou `dll` selon la plate-forme cliente.
- Si l'option de CRYPT_STRENGTH est définie à DES_56, le logiciel de chiffrement doit également inclure la bibliothèque DES 56 bits. Le nom de la bibliothèque DES 56 bits est `libvdes56.`suffix; le suffixe est `so`, `sl`, ou `dll` selon la plate-forme cliente.
- Un fichier de clé spécifié avec l'option de configuration CRYPT_KEYFILE doit exister. Lorsque vous spécifiez une phrase secrète NetBackup à l'aide de la commande de serveur `bpinst` ou de la commande client `bpkeyfile`, vous créez un fichier de clé.

Le serveur détermine à partir de l'image de sauvegarde si la sauvegarde a été chiffrée. Le serveur se connecte ensuite à `bpcd` sur le client pour lancer la restauration. Le serveur envoie un indicateur de chiffrement et un temps de sauvegarde de l'image de sauvegarde sur la demande de restauration au client.

Si les conditions préalables sont réunies, ce qui suit se produit :

- Le serveur envoie des noms de fichier, des attributs et des données de fichiers chiffrés au client à restaurer.
- Le client prend ses données de fichier de clé et les fusionne avec le temps de sauvegarde afin de générer une ou plusieurs clés DES 40 bits. Si la bibliothèque DES 56 bits est disponible, le client génère également une ou plusieurs clés DES 56 bits.
- Si le client lit un en-tête de `tar` de chiffrement, le client compare la somme de contrôle dans l'en-tête aux sommes de contrôle de ses clés DES. Si la somme de contrôle d'une clé DES correspond à la somme de contrôle dans l'en-tête, NetBackup utilise cette clé DES pour déchiffrer les données de fichier.

Le fichier est déchiffré et restauré si une clé DES est disponible. Si la clé DES n'est pas disponible, le fichier n'est pas restauré et un message d'erreur est généré.

Configuration du chiffrement standard sur des clients

Cette rubrique décrit comment configurer le chiffrement NetBackup standard.

Les options de configuration suivantes sont situées dans le fichier `bp.conf` sur les clients d'UNIX et dans le registre pour les clients Windows.

Les options de configuration sont les suivantes :

- CRYPT_OPTION

- CRYPT_KIND
- CRYPT_CIPHER

Vous pouvez également utiliser la **console d'administration NetBackup** pour configurer les options à partir du serveur. Elles sont situées dans l'onglet **Chiffrement** de la boîte de dialogue **Propriétés du client**.

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

Gestion des options standard de chiffrement

Le tableau suivant décrit les trois options de configuration liées au chiffrement pour le chiffrement standard qui peut exister sur un client NetBackup.

Assurez-vous que les options sont définies aux valeurs appropriées pour votre client.

Tableau 19-5 Trois options de configuration liées au chiffrement

Option	Valeur	Description
`CRYPT_OPTION = option`		Définit les options de chiffrement sur les clients NetBackup. Les valeurs possibles de l'*option* sont les suivantes :
	`denied|DENIED`	Indique que le client n'autorise pas les sauvegardes chiffrées. Si le serveur demande une sauvegarde chiffrée, cette demande est considérée comme une erreur.
	`allowed|ALLOWED`	(la valeur par défaut) Indique que le client permet les sauvegardes chiffrées ou non chiffrées.
	`required|REQUIRED`	Indique que le client autorise uniquement les sauvegardes chiffrées. Si le serveur demande une sauvegarde non chiffrée, cette demande est considérée comme une erreur.
`CRYPT_KIND = kind`		Définit le type de chiffrement sur les clients NetBackup. L'option *type* peut être définie sur l'une des valeurs d'options ci-après.
	`NONE`	Ni le chiffrement standard, ni le chiffrement hérité n'est configuré sur le client.
	`STANDARD`	Indique que vous voulez utiliser le chiffrement 128 bits basé sur chiffre ou le chiffrement de 256 bits. Cette option est la valeur par défaut si le chiffrement standard est configuré sur le client.

Option	Valeur	Description
	`LEGACY`	Indique que vous voulez utiliser le chiffrement basé sur hérité, avec le DES 40 bits ou 56 bits.
`CRYPT_CIPHER = cipher`		Définit le type de chiffre à utiliser. Il peut être défini sur l'une des valeurs d'option suivantes.
	AES-128-CFB	Advanced Encryption Standard de 128 bits. C'est la valeur par défaut.
	BF-CFB	Blowfish de 128 bits
	DES-EDE-CFB	Deux clés DES triple
	AES-256-CFB	Advanced Encryption Standard de 256 bits.

Gestion du fichier de clé de chiffrement de NetBackup

Cette rubrique décrit comment gérer le fichier de clés de chiffrement NetBackup.

Remarque : Le fichier de clés doit être le même sur tous les nœuds d'un cluster.

Utilisez la commande `bpkeyutil`pour installer le fichier de clé de chiffrement et la phrase de passe au format chiffre sur le client de NetBackup Encryption.

- Pour un client Windows, le chemin d'accès de commande est comme suit

  install_path\NetBackup\bin\bpkeyutil

- Pour un client UNIX, le chemin d'accès de commande est comme suit

  /usr/openv/netbackup/bin/bpkeyutil

Vous êtes invités à ajouter une phrase de passe pour ce client.

NetBackup utilise la phrase de passe spécifiée pour créer le fichier de clé comme suit :

- NetBackup utilise une combinaison des deux algorithmes suivants pour créer une clé de phrase de passe pouvant atteindre jusqu'à 256 bits.
  - Algorithme de hachage sécurisé ou SHA1
  - Algorithme de résumé de message ou MD5
- NetBackup utilise la clé privée NetBackup et l'algorithme AES de 128 bits pour chiffrer la clé.

- La clé est enregistrée dans le fichier de clés se trouvant sur le client.
- A l'exécution, NetBackup utilise la clé et un vecteur d'initialisation aléatoire pour chiffrer les données client. Le vecteur d'initialisation est stocké dans l'en-tête de l'image de sauvegarde.

Les phrases de passe précédentes restent disponibles dans le fichier de clés pour permettre des restaurations des sauvegardes qui ont été chiffrées à l'aide de ces expressions.

Attention : Vous devez vous souvenir les phrases de passe, y compris des anciennes phrases de passe. Si l'un des fichiers de clés d'un client est endommagé ou perdu, vous avez besoin de toutes les phrases de passe précédentes pour recréer le fichier de clés. Sans ce fichier de clés, vous ne pouvez pas restaurer les fichiers qui ont été chiffrés avec les phrases de passe.

Seul l'administrateur de l'ordinateur client doit avoir accès au fichier de clés.

Pour un client UNIX, vous devez vérifier ce qui suit :

- Le propriétaire est de type racine.
- Les bits de mode sont 600.
- Le fichier ne se trouve pas sur un système de fichiers pouvant être monté en NFS.

Configuration de chiffrement standard à partir du serveur

Vous pouvez configurer depuis le serveur la plupart des clients NetBackup pour le chiffrement à l'aide de la commande `bpkeyutil`.

Conditions préalables requises :

- Le logiciel client NetBackup doit être en cours d'exécution sur les plates-formes qui prennent en charge le chiffrement de NetBackup (consultez le document Notes de mise à jour de NetBackup).
- Les clients NetBackup doivent exécuter la version requise NetBackup.

Création des fichiers de clés de chiffrement sur les clients

Utilisez les directives suivantes pour créer des fichiers de clés de chiffrement sur les clients :

- Si le serveur est dans un cluster et est également un client de chiffrement, tous les nœuds dans le cluster doivent avoir le même fichier de clés.

- La commande `bpkeyutil` définit le fichier de clés de chiffrement et la phrase secrète basés sur un chiffrement sur chaque client NetBackup Encryption.
  - Pour un serveur Windows, le chemin d'accès complet à la commande est comme suit :

    install_path\NetBackup\bin\bpkeyutil

  - Pour un serveur UNIX, le chemin d'accès complet à la commande est comme suit :

    /usr/openv/netbackup/bin/bpkeyutil

Création de fichiers de clés

Pour chaque client de chiffrement, exécutez la commande suivante :

```
bpkeyutil -clients client_name
```

Vous êtes invité à ajouter une nouvelle phrase de passe au fichier de clés de ce client.

Pour configurer plusieurs clients afin qu'ils utilisent la même phrase de passe, spécifiez une liste de noms de client séparés par une virgule, comme suit :

```
bpkeyutil -clients client_name1,client_name2,...,client_namen
```

Pour créer le fichier de clés, NetBackup utilise la phrase de passe que vous spécifiez.

NetBackup utilise la phrase de passe spécifiée pour créer le fichier de clé comme suit :

- NetBackup utilise une combinaison des deux algorithmes suivants pour créer une clé de phrase de passe pouvant atteindre jusqu'à 256 bits.
  - Algorithme de hachage sécurisé ou SHA1
  - Algorithme de résumé de message ou MD5
- NetBackup utilise la clé privée NetBackup et l'algorithme AES de 128 bits pour chiffrer la clé.
- La clé est enregistrée dans le fichier de clés se trouvant sur le client.
- A l'exécution, NetBackup utilise la clé et un vecteur d'initialisation aléatoire pour chiffrer les données client. Le vecteur d'initialisation est stocké dans l'en-tête de l'image de sauvegarde.

Les phrases de passe précédentes demeurent disponibles dans le fichier pour des restaurations des sauvegardes qui ont été chiffrées avec ces phrases.

Attention : Vous devez vous assurer que les phrases de passe, qu'elles soient déjà utilisées ou non, sont sécurisées et peuvent être récupérées. Si l'un des fichiers de clés d'un client est endommagé ou perdu, vous avez besoin de toutes les phrases de passe précédentes pour recréer le fichier de clés. Sans ce fichier de clé, vous ne pouvez pas restaurer les fichiers qui ont été chiffrés avec les phrases de passe.

Seul l'administrateur de l'ordinateur client doit avoir accès au fichier de clés. Pour un client UNIX, vous devez vérifier ce qui suit :

- Le propriétaire est de type racine.
- Les bits de mode sont 600.
- Le fichier ne se trouve pas sur un système de fichiers pouvant être monté en NFS.

Pratiques d'excellence pour la restauration de fichiers de clés

Même lorsqu'une sauvegarde chiffrée n'a pas de fichier de clés disponible, vous pouvez restaurer les fichiers.

Conservation de manuel pour protéger les phrases de passe des fichiers de clés

La conservation manuelle est la méthode la plus sécurisée pour protéger vos phrases de passe de fichier de clés.

Quand vous ajoutez une phrase à l'aide de la commande `bpkeyutil` complétez la conservation manuelle comme suit :

- Ecrivez la phrase sur le papier.
- Scellez le papier sous enveloppe
- Mettez l'enveloppe dans un coffre-fort.

Si vous devez ultérieurement restaurer des sauvegardes chiffrées et vous avez perdu le fichier de clés, procédez comme suit :

- Réinstallez NetBackup.
- Utilisez `bpkeyutil` pour créer un nouveau fichier de clés à l'aide des phrases de passe du coffre-fort.

Sauvegarde automatique du fichier de clés

La méthode de sauvegarde automatique est moins sécurisée, mais elle garantit l'existence d'une copie de sauvegarde de votre fichier de clés.

Cette méthode nécessite la création d'une politique non chiffrée pour sauvegarder le fichier de clés. Si le fichier de clés est perdu, vous pouvez le restaurer à partir de la sauvegarde non chiffrée.

Le problème de cette méthode est que le fichier de clés d'un client peut être restauré sur un autre client.

Si vous voulez inclure le fichier de clés à la sauvegarde sur un client, ajoutez le nom du chemin d'accès du fichier de clés à la liste d'inclusion du client.

Les restaurations redirigées exigent des modifications spécifiques de la configuration pour permettre la restauration.

Restaurer un fichier de sauvegarde chiffré sur un autre client

Les restaurations redirigées sont décrites dans la procédure qui suit.

Pour restaurer une sauvegarde chiffrée vers un autre client

1. Le serveur doit permettre des restaurations redirigées et vous (l'utilisateur) devez être autorisé à effectuer de telles restaurations.

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

2. Vous devez obtenir la phrase de passe utilisée sur l'autre client lorsque vous avez effectué la sauvegarde chiffrée. Sans cette phrase de passe, vous ne pouvez pas restaurer les fichiers.

   Remarque : si la phrase secrète est la même sur les deux clients, passez à l'étape 5.

3. Pour conserver votre propre fichier de clé (actuel), déplacez ou le renommez le.

4. Utilisez la commande `bpkeyutil` pour créer un fichier de clé correspondant à celui de l'autre client. Lorsque le processus `bpkeyutil` vous demande la phrase secrète, spécifiez la phrase secrète de l'autre client.
5. Restaurez les fichiers sur l'autre client.

   Après que vous avez restauré les fichiers chiffrés du client, renommez ou supprimez le fichier de clé que vous avez créé dans l'étape 4.

   Vous rétablissez ensuite le fichier de clé initial sur son emplacement ou vous lui réaffectez son nom d'origine. Si vous ne rétablissez pas l'emplacement et le nom d'origine de votre fichier de clé, vous pouvez ne pas être à même de restaurer vos propres sauvegardes chiffrées.

Configuration du chiffrement standard directement sur les clients

Vous pouvez également configurer le chiffrement de NetBackup directement sur des clients comme expliqué dans les rubriques suivantes :

- Définition de l'attribut standard de chiffrement dans les politiques
  Se reporter à "Définition de l'attribut standard de chiffrement dans les politiques" à la page 511.
- Modifier les paramètres de chiffrement client à partir du serveur
  Se reporter à "Modification des paramètres de chiffrement client à partir du serveur NetBackup" à la page 512.

Définition de l'attribut standard de chiffrement dans les politiques

Vous devez définir l'attribut de **chiffrement** sur votre politique NetBackup comme suit :

- Si l'attribut est défini, le serveur NetBackup demande aux clients NetBackup de cette politique d'effectuer des sauvegardes chiffrées.
- Si l'attribut n'est pas défini, le serveur NetBackup ne demande pas aux clients NetBackup de cette politique d'effectuer des sauvegardes chiffrées.

Vous pouvez utiliser l'onglet **Attributs** de la politique dans la **console d'administration NetBackup** pour définir ou effacer l'attribut de **chiffrement** d'une politique.

Pour plus d'informations sur la façon de configurer des politiques, consultez le Guide de l'administrateur NetBackup, volume I.

Modification des paramètres de chiffrement client à partir du serveur NetBackup

Vous pouvez modifier les paramètres de chiffrement pour un client NetBackup à partir de la boîte de dialogue **Propriétés du client** sur le serveur NetBackup.

Pour modifier les paramètres de chiffrement client du serveur NetBackup

1. Ouvrez la **console d'administration NetBackup** sur le serveur.
2. Développez **Propriétés de l'hôte > Clients**.
3. Dans la liste des **clients**, cliquez deux fois sur le nom du client à modifier. La fenêtre de **Propriétés du client** s'affiche.
4. Développez **Propriétés > Chiffrement** pour afficher les paramètres de chiffrement pour ce client.

   Consultez la rubrique suivante pour plus d'informations au sujet des options de configuration qui correspondent aux paramètres dans le volet **Chiffrement** :

   Se reporter à "Gestion des options standard de chiffrement" à la page 505.

   Pour obtenir des explications supplémentaires des paramètres, cliquez sur le bouton **Aide** dans la fenêtre ou consultez le Guide de l'administrateur NetBackup, volume I.

Configuration du chiffrement hérité sur les clients

Cette rubrique traite de la configuration du chiffrement NetBackup hérité.

Les options de configuration sont situées dans le fichier `bp.conf` sur les clients UNIX et dans le registre pour les clients Windows.

Les options sont les suivantes :

- CRYPT_OPTION
- CRYPT_STRENGTH
- CRYPT_LIBPATH
- CRYPT_KEYFILE

Vous pouvez également utiliser la **console d'administration NetBackup** pour configurer les options à partir du serveur. Elles sont situées dans l'onglet **Chiffrement** de la boîte de dialogue **Propriétés du client**.

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

Vous pouvez définir les options CRYPT_OPTION et CRYPT_STRENGTH dans la commande `bpinst -LEGACY_CRYPT`. Les paramètres d'option équivalents sont respectivement -crypt_option, -crypt_strength.

A propos de la configuration du chiffrement hérité à partir du client

Le tableau suivant contient les options de configuration liées au chiffrement hérité sur un client NetBackup. Assurez-vous que ces options sont définies selon les valeurs appropriées pour votre client. Elles sont définies si vous exécutez la commande `bpinst -LEGACY_CRYPT` du serveur sur le nom du client.

Tableau 19-6 Options de chiffrement héritées

Option	Valeur	Description
`CRYPT_OPTION =` *`option`*		Définit les options de chiffrement sur les clients NetBackup. Les valeurs possibles de l'*option* sont les suivantes :
	`denied|DENIED`	Indique que le client n'autorise pas les sauvegardes chiffrées. Si le serveur demande une sauvegarde chiffrée, cette demande est considérée comme une erreur.
	`allowed|ALLOWED`	(Valeur par défaut) Indique que le client autorise les sauvegardes chiffrées ou non chiffrées.
	`required|REQUIRED`	Indique que le client exige des sauvegardes chiffrées. Si le serveur demande une sauvegarde non chiffrée, cette demande est considérée comme une erreur.
`CRYPT_KIND =` *`kind`*		Définit le type de chiffrement sur les clients NetBackup. Les valeurs possibles de l'option *kind* sont les suivantes :
	`NONE`	Ni le chiffrement standard, ni le chiffrement hérité n'est configuré sur le client.
	`LEGACY`	Spécifie le type de chiffrement hérité, 40 bits DES ou 56 bits DES. Cette option est la valeur par défaut si le type de chiffrement hérité est configuré sur le client alors que le type de chiffrement standard n'est pas configuré.
	`STANDARD`	Spécifie le type de code du chiffrement, qui peut être de 128 bits ou de 256 bits.

Option	Valeur	Description
`CRYPT_STRENGTH = strength`		Définit les options de chiffrement sur les clients NetBackup. Les valeurs possibles de *strength* sont les suivantes :
	`des_40|DES_40`	(Valeur par défaut) Spécifie le chiffrement DES 40 bits.
	`des_56|DES_56`	Spécifie le chiffrement DES 56 bits.
`CRYPT_LIBPATH = directory_path`		Définit le répertoire qui contient les bibliothèques de chiffrement sur les clients NetBackup. NetBackup est installé dans le répertoire *install_path*, par défaut `C:\VERITAS`.
	`/usr/openv/lib/`	Valeur par défaut sur les systèmes UNIX.
	install_path`\NetBackup\bin\`	Valeur par défaut sur les systèmes UNIX.
`CRYPT_KEYFILE = file_path`		Définit le fichier contenant les clés de chiffrement sur les clients NetBackup.
	`/usr/openv/var/keyfile`	Valeur par défaut sur les systèmes UNIX.
	install_path`\NetBackup\var\keyfile.dat`	Valeur par défaut sur les systèmes Windows.

Gestion des fichiers de clé de chiffrement hérités

Cette rubrique décrit la gestion des fichiers de clés de chiffrement hérités.

Remarque : Le fichier de clé doit être le même sur tous les nœuds d'un cluster.

Chaque client NetBackup qui effectue des sauvegardes chiffrées et des restaurations a besoin d'un fichier de clé. Le fichier de clé contient les données que le client utilise pour générer des clés DES pour chiffrer des sauvegardes.

Vous pouvez utiliser la commande `bpkeyfile` sur le client pour gérer le fichier de clé. Consultez la description de la commande `bpkeyfile` dans le Guide de référence des commandes NetBackup pour obtenir une description détaillée.

La première chose que vous devez faire est de créer un fichier de clés s'il n'existe pas déjà. Le fichier de clés existe si vous définissez une phrase de passe à partir de la commande `bpinst -LEGACY_CRYPT` depuis le serveur à ce nom de client.

Le nom de fichier devrait être identique au nom de fichier que vous avez spécifié avec l'option de configuration CRYPT_KEYFILE comme suit :

- Pour des clients Windows, le nom de fichier de clé par défaut est comme suit

  install_path\NetBackup\var\keyfile.dat

- Pour des clients UNIX, le nom de fichier de clé par défaut est comme suit

  /usr/openv/var/keyfile

NetBackup utilise une phrase de passe de fichier de clé pour générer une clé DES et utilise la clé DES pour chiffrer un fichier de clé.

Généralement, vous utilisez la phrase secrète du fichier de clé qui est codé en dur dans les applications NetBackup. Pour assurer une sécurité supplémentaire, vous pouvez toutefois utiliser votre propre phrase secrète du fichier de clé.

Se reporter à "Degré de sécurité de fichier de clé hérité supplémentaire pour clients UNIX" à la page 522.

Remarque : Si vous ne voulez pas utiliser votre propre phrase de passe de fichier de clé, n'entrez pas une nouvelle phrase de passe de fichier de clé. Au lieu de cela, utilisez la phrase de passe standard de fichier de clé et entrez une nouvelle phrase de passe de NetBackup.

Vous devez décider quelle phrase de passe de NetBackup à utiliser. La phrase de passe de NetBackup est utilisée pour générer les données qui sont placées dans le fichier de clé. Ces données sont utilisées pour générer des clés DES pour chiffrer des sauvegardes.

Pour créer le fichier de clé par défaut sur le client UNIX qui est chiffré avec la phrase de passe standard de fichier de clé, entrez une commande telle que la suivante :

```
bpkeyfile /usr/openv/var/keyfile
Enter new keyfile pass phrase: (standard keyfile pass phrase)
Re-enter new keyfile pass phrase: (standard keyfile pass phrase)
Enter new NetBackup pass phrase: ************************
Re-enter new NetBackup pass phrase: ************************
```

Vous pouvez entrer de nouvelles phrases de passe NetBackup assez souvent. Des informations sur les anciennes phrases de passe sont conservées dans le fichier de clé. Cette méthode vous permet de restaurer n'importe quelle donnée qui a été chiffrée avec des clés DES générées à partir d'anciennes phrases de passe. Vous pouvez utiliser l'option -change_netbackup_pass_phrase (ou -cnpp) sur la commande `bpkeyfile` afin d'entrer une nouvelle phrase de passe NetBackup.

Si vous voulez entrer une nouvelle phrase secrète NetBackup sur un client Windows, entrez une commande similaire à l'exemple suivant :

```
bpkeyfile.exe -cnpp install_path\NetBackup\var\keyfile.dat
Enter old keyfile pass phrase: (standard keyfile pass phrase)
Enter new NetBackup pass phrase: **********
Re-enter new NetBackup pass phrase: **********
```

Attention : Vous devez vous assurer que les phrases de passe, qu'elles soient déjà utilisées ou non, sont sécurisées et peuvent être récupérées. Si l'un des fichiers de clés d'un client est endommagé ou perdu, vous avez besoin de toutes les phrases de passe précédentes pour recréer le fichier de clés. Sans ce fichier de clé, vous ne pouvez pas restaurer les fichiers qui ont été chiffrés avec les phrases de passe.

Seul l'administrateur de l'ordinateur client doit avoir accès au fichier de clé.

Pour un client UNIX, vous devez vérifier ce qui suit :

- Le propriétaire est de type racine.
- Les bits de mode sont 600.
- Le fichier ne se trouve pas sur un système de fichiers pouvant être monté en NFS.

Vous devez considérer de sauvegarder ou non votre fichier de clé. Pour les sauvegardes chiffrées, une telle sauvegarde a peu de valeur, parce que le fichier de clé ne peut être restauré que si le fichier de clé est déjà sur le client. Au lieu de cela, vous pouvez installer une politique NetBackup qui fait les sauvegardes non chiffrées des fichiers de clés des clients. Cette politique est utile si vous avez besoin d'une restauration de secours du fichier de clé. Cependant, cette méthode signifie également que le fichier de clé d'un client peut être restauré sur un client différent.

Si vous voulez empêcher la sauvegarde du fichier de clé d'être, ajoutez le nom du chemin d'accès du fichier de clé à la liste du client.

Configuration du chiffrement hérité du serveur

Vous pouvez configurer depuis le serveur la plupart des clients NetBackup pour le chiffrement à l'aide de la commande `bpinst`.

Les conditions requises pour cette méthode incluent ce qui suit :

- Le logiciel du client NetBackup doit être en cours d'exécution sur une plate-forme qui prend en charge le chiffrement NetBackup.
  Consultez les *Notes de mise à jour NetBackup* pour des détails sur les plates-formes prises en charge.

- Les clients NetBackup doivent exécuter la version requise NetBackup.
- Si un serveur en cluster est un client pour NetBackup Encryption, assurez-vous que tous les nœuds dans le cluster ont le même fichier de clé.

La commande `bpinst` est chargée dans le répertoire bin de NetBackup sur le serveur comme suit :

- Pour un serveur Windows, le répertoire bin est le suivant

  install_path\NetBackup\bin

- Pour un serveur UNIX, le répertoire bin est le suivant

  /usr/openv/netbackup/bin

Consultez la description de la commande `bpinst` dans le Guide de référence des commandes NetBackup pour plus d'informations sur les options disponibles avec la commande `bpinst`.

Pour des exemples sur l'utilisation de `bpinst` :

Se reporter à "Transmission de la configuration de chiffrement hérité aux clients" à la page 517.

Se reporter à "Transfert des phrases de passe de chiffrement hérité vers des clients" à la page 518.

Normalement, vous spécifiez des noms de client dans la commande `bpinst`. Cependant, si vous incluez l'option -policy_names, vous spécifiez des noms de politique à la place. L'option affecte tous les clients dans les politiques spécifiées.

Transmission de la configuration de chiffrement hérité aux clients

Vous pouvez utiliser les options -crypt_option et -crypt_strength sur la commande `bpinst` pour définir la configuration de chiffrement sur des clients NetBackup comme suit :

- L'option -crypt_option spécifie si le client doit refuser les sauvegardes chiffrées (refusées), autoriser les sauvegardes chiffrées (autorisées) ou requérir les sauvegardes chiffrées (requises).
- L'option -crypt_strength spécifie la longueur de clé DES (40 ou 56) que le client devrait utiliser pour les sauvegardes chiffrées.

Pour installer le logiciel client de chiffrement et requérir des sauvegardes chiffrées avec une clé DES 56 bits, utilisez la commande suivante du serveur :

```
bpinst -LEGACY_CRYPT -crypt_option required -crypt_strength des_56 \
-policy_names policy1 policy2
```

L'exemple utilise un caractère de continuation UNIX (\) parce qu'il est long. Pour autoriser des sauvegardes chiffrées ou non chiffrées avec une clé DES 40 bits, utilisez la commande suivante :

```
bpinst -LEGACY_CRYPT -crypt_option allowed -crypt_strength des_40 \
client1 client2
```

Dans les environnements en cluster vous pouvez procédez comme suit :

- Transférez la configuration vers client uniquement à partir du noeud actif.
- Spécifiez les noms d'hôte des nœuds (et non pas les noms virtuels) de la liste de clients.

Remarque : Le paramètre `USE_VXSS` du serveur maître dans le fichier `bp.conf` doit être défini sur `AUTOMATIC`. Utilisez ce paramètre lors de l'envoi d'un maître NBAC vers un hôte sur lequel NetBackup n'a pas été installé. Utilisez également ce paramètre quand NBAC n'a pas activé le paramètre `USE_VXSS` du serveur maître dans `bp.conf`.

Transfert des phrases de passe de chiffrement hérité vers des clients

Pour envoyer une phrase de passe à un client NetBackup, vous pouvez utiliser les options de `bpinst` -passphrase_prompt ou -passphrase_stdin. Le client NetBackup utilise la phrase de passe pour créer ou mettre à jour des données dans son fichier de clés.

Le fichier de clés contient les données que le client utilise pour générer des clés DES afin de chiffrer des sauvegardes comme suit :

- Si vous utilisez l'option -passphrase_prompt, vous êtes invité sur votre terminal à une phrase de passe de 0 à 62 caractères. Les caractères sont masqués à mesure que vous saisissez la phrase de passe. Vous êtes de nouveau invité à retaper la phrase de passe pour la confirmer.
- Si vous utilisez l'option -passphrase_stdin, vous devez entrer la phrase de passe de 0 à 62 caractères deux fois par l'entrée standard. Généralement, l'option -passphrase_prompt est plus sécurisée que l'option -passphrase_stdin, mais -passphrase_stdin est plus pratique si vous utilisez `bpinst` dans un script d'environnement d'exécution.

Pour entrer une phrase de passe pour le client client1 d'un serveur NetBackup par l'entrée standard, vous devez entrer les commandes comme suit :

```
bpinst -LEGACY_CRYPT -passphrase_stdin client1 <<EOF
This pass phase is not very secure
This pass phase is not very secure
EOF
```

Pour entrer une phrase de passe pour le client client2 d'un serveur NetBackup, vous devez entrer les commandes comme suit :

```
bpinst -LEGACY_CRYPT -passphrase_prompt client2
Enter new NetBackup pass phrase: ********************
Re-enter new NetBackup pass phrase: ********************
```

Vous pouvez entrer de nouvelles phrases de passe assez souvent. Le client NetBackup conserver des informations sur les anciennes phrases de passe dans son fichier de clés. Il peut restaurer les données qui ont été chiffrées avec des clés DES générées à partir d'anciennes phrases de passe.

Attention : Vous devez vous assurer que les phrases de passe, qu'elles soient déjà utilisées ou non, sont sécurisées et peuvent être récupérées. Si l'un des fichiers de clés d'un client est endommagé ou perdu, vous avez besoin de toutes les phrases de passe précédentes pour recréer le fichier de clés. Sans ce fichier de clé, vous ne pouvez pas restaurer les fichiers qui ont été chiffrés avec les phrases de passe.

Vous devez décider si vous voulez utiliser la même phrase de passe pour plusieurs clients. Utiliser la même phrase de passe est pratique parce que vous pouvez utiliser une commande unique `bpinst` pour spécifier une phrase de passe pour chaque client. Vous pouvez également effectuer des restaurations redirigées entre les clients lorsqu'ils utilisent la même phrase de passe.

Remarque : Si vous voulez empêcher des restaurations redirigées, vous devriez spécifier des phrases de passe différentes en entrant une commande distincte `bpinst` pour chaque client.

Pour des environnements en cluster, vous pouvez procédez comme suit :

- Transférez la configuration vers client uniquement à partir du noeud actif.
- Spécifiez les noms d'hôte des nœuds (et non pas les noms virtuels) de la liste de clients.

Remarque : Le paramètre `USE_VXSS` du serveur maître dans le fichier `bp.conf` doit être défini sur `AUTOMATIC`. Utilisez ce paramètre lors de l'envoi d'un maître NBAC vers un hôte sur lequel NetBackup n'a pas été installé. Utilisez également ce paramètre quand NBAC n'a pas activé le paramètre `USE_VXSS` du serveur maître dans `bp.conf`.

Restauration d'une sauvegarde chiffrée héritée créée sur un autre client

Si un serveur permet des restaurations redirigées, vous (l'utilisateur) devez être autorisé à effectuer de telles restaurations.

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

Pour restaurer une sauvegarde chiffrée qui a été créée sur un autre client :

1. Vous devez obtenir la phrase de passe utilisée sur l'autre client lorsque vous avez effectué la sauvegarde chiffrée. Sans cette phrase de passe, vous ne pouvez pas restaurer les fichiers.

   Remarque : si la phrase secrète est la même sur les deux clients, passez à l'étape 4.

2. Pour conserver votre propre fichier de clé (actuel), déplacez ou le renommez le.

3 Utilisez la commande `bpkeyfile` pour créer un fichier de clé correspondant à celui de l'autre client. Lorsque le processus `bpkeyutil` vous demande la phrase secrète, spécifiez la phrase secrète de l'autre client.

```
bpkeyfile -change_key_file_pass_phrase key_file_path
```

key_file_path est le chemin d'accès pour un nouveau fichier de clés sur votre client. Ce fichier de clés correspond à celui de l'autre client.

Une fois que vous avez entré la commande, `bpkeyfile` vous invite à entrer la phrase secrète du client (obtenue à l'étape 1).

Pour plus d'informations à propos de `bpkeyfile`, consultez le Guide de référence des commandes NetBackup.

4 Restaurez les fichiers sur l'autre client.

Après que vous avez restauré les fichiers chiffrés du client, renommez ou supprimez le fichier de clé que vous avez créé dans l'étape 3.

Vous rétablissez ensuite le fichier de clé initial sur son emplacement ou vous lui réaffectez son nom d'origine. Si vous ne rétablissez pas l'emplacement et le nom d'origine de votre fichier de clé, vous pouvez ne pas être à même de restaurer vos propres sauvegardes chiffrées.

Définition d'un attribut de chiffrement hérité dans des politiques

Vous devez définir l'attribut de **chiffrement** de votre politique NetBackup comme suit :

- Si l'attribut est défini, le serveur NetBackup demande aux clients NetBackup de cette politique d'effectuer des sauvegardes chiffrées.
- Si l'attribut n'est pas défini, le serveur NetBackup ne demande pas aux clients NetBackup de cette politique d'effectuer des sauvegardes chiffrées.

Vous pouvez utiliser l'onglet **Attributs** de la politique dans la **console d'administration NetBackup** pour définir ou effacer l'attribut de **chiffrement** d'une politique.

Pour plus d'informations sur la façon de configurer des politiques, consultez le Guide de l'administrateur NetBackup, volume I.

Vous pouvez également utiliser la commande `bpinst` pour définir ou effacer l'attribut **Chiffrement** pour les politiques NetBackup. Cette méthode est pratique si vous voulez définir ou effacer l'attribut pour plusieurs politiques.

Par exemple, pour définir l'attribut de **chiffrement** pour policy1 et policy2 à partir d'un serveur NetBackup, entrez une commande comme suit :

```
bpinst -LEGACY_CRYPT -policy_encrypt 1 -policy_names policy1 policy2
```

Le paramètre 1 définit l'attribut de chiffrement (0 l'effacerait).

Modifier les paramètres client de chiffrement hérités du serveur

Vous pouvez modifier les paramètres de chiffrement pour un client NetBackup à partir de la boîte de dialogue **Propriétés du client** sur le serveur NetBackup.

Pour modifier les paramètres de chiffrement client du serveur NetBackup

1. Dans la **console d'administration NetBackup** située sur le serveur, développez le **Propriétés de l'hôte > Clients**.
2. Dans la liste des **clients**, cliquez deux fois sur le nom du client à modifier. La boîte de dialogue **Propriétés du client** s'affiche.
3. Dans le volet **Propriétés,** cliquez sur **Chiffrement** pour afficher les paramètres de chiffrement de ce client.

   Pour obtenir des explications supplémentaires sur les paramètres, cliquez sur le bouton Aide dans la boîte de dialogue ou consultez leGuide de l'administrateur NetBackup, volume I.

Degré de sécurité de fichier de clé hérité supplémentaire pour clients UNIX

Cette rubrique s'applique uniquement aux clients NetBackup UNIX. La sécurité supplémentaire n'est pas disponible pour les clients Windows.

Remarque : Il est déconseillé d'utiliser la fonction de sécurité supplémentaire de fichier de clé dans un cluster.

Le fichier de clé d'un client de chiffrement est chiffré en utilisant une clé DES qui est générée à partir d'une phrase de passe de fichier de clé. Par défaut, le fichier de clé est chiffré en utilisant une clé DES qui est générée à partir de la phrase de passe standard qui est codée en dur dans NetBackup.

L'utilisation de la phrase de passe standard de fichier de clé vous permet d'effectuer les sauvegardes et les restaurations chiffrées automatisées de la même façon que vous effectuez les sauvegardes et les restaurations non chiffrées.

Cette méthode représente cependant des problèmes potentiels si une personne non autorisée accède au fichier de clé de votre client. Cette personne peut être en mesure de déterminer quelles clés de chiffrement vous utilisez pour les sauvegardes ou d'utiliser le fichier de clé pour restaurer les sauvegardes chiffrées de votre client.

Pour cette raison, vous devez vous assurer que seul l'administrateur du client a accès au fichier de clé.

Pour assurer une protection supplémentaire, vous pouvez utiliser votre propre phrase de passe de fichier de clé pour générer la clé DES afin de chiffrer le fichier de clé. Une personne non autorisée peut encore accéder à ce fichier de clé, mais la restauration est plus difficile.

Si vous utilisez votre propre phrase de passe de fichier de clé, la sauvegarde et la restauration ne sont plus automatisées comme avant. Voici une description de ce qui se produit sur un client NetBackup d'UNIX si vous avez utilisé votre propre phrase de passe de fichier de clé.

Pour démarrer une sauvegarde ou une restauration sur un client, le serveur NetBackup se connecte au daemon `bpcd` sur le client et fait une demande.

Pour effectuer une sauvegarde ou une restauration chiffrée, `bpcd` a besoin de déchiffrer et de lire le fichier de clé.

Si la phrase secrète standard de fichier de clé est utilisée, `bpcd` peut déchiffrer automatiquement le fichier de clé.

Si vous utilisez votre propre phrase secrète de fichier de clé, `bpcd` ne peut plus déchiffrer automatiquement le fichier de clé et le daemon `bpcd` par défaut ne peut pas être utilisé. Vous devez lancer `bpcd` avec un paramètre spécial. Se reporter à "Exécuter la commande bpcd -keyfile" à la page 523.

Remarque : Dans un environnement en cluster, si vous modifiez le fichier de clé sur un nœud, vous devez apporter la même modification dans le fichier de clé sur tous les nœuds.

Exécuter la commande bpcd -keyfile

Cette rubrique décrit l'exécution de la commande `bpcd` en tant que programme autonome.

Pour exécuter `bpcd` comme programme autonome :

1. Utilisez l'option -change_key_file_pass_phrase (ou -ckfpp) sur la commande `bpkeyfile` pour modifier la phrase de passe du fichier de clés, comme dans l'exemple suivant :

   ```
   bpkeyfile -ckfpp /usr/openv/var/keyfile
   Enter old keyfile pass phrase: (standard keyfile pass phrase)
   Enter new keyfile pass phrase: (standard keyfile pass phrase)
   ******
   Re-enter new keyfile pass phrase: (standard keyfile pass
   phrase) ******
   ```

   Si vous saisissez un retour de chariot à l'invite, NetBackup utilise la phrase de passe standard du fichier de clés.

2. Arrêtez le `bpcd` existant en émettant la commande `bpcd -terminate`.

3. Lancez la commande `bpcd` avec l'option -keyfile. Entrez la nouvelle phrase de passe du fichier de clés une fois invité.

   ```
   bpcd -keyfile
   Please enter keyfile pass phrase: ******
   ```

   `bpcd` s'exécute maintenant en arrière-plan et attend des demandes du serveur NetBackup.

   Vous pouvez modifier la phrase de passe du fichier de clés à tout moment avec la commande `bpkeyfile` et l'option -ckfpp. La nouvelle phrase de passe du fichier de clés n'entre en vigueur que la prochaine fois que vous démarrez `bpcd`

   Vous pouvez également modifier la phrase de passe de NetBackup utilisée pour générer les clés DES afin de chiffrer des sauvegardes. Modifiez cette phrase à tout moment avec la commande `bpkeyfile` et l'option -cnpp. Notez, cependant, que la nouvelle phrase de passe de NetBackup n'entre en vigueur que lorsque vous détruisiez le processus `bpcd` actuel et redémarrez `bpcd`

Interrompez bpcd sur les clients UNIX

Pour arrêter `bpcd` sur des clients UNIX, utilisez la commande `bpcd -terminate`.

Chapitre 20

Service Gestion des clés NetBackup

Ce chapitre traite des sujets suivants :

À propos de KMS conforme à la norme FIPS

NetBackup KMS peut désormais être exécuté en mode FIPS, dans lequel les clés de chiffrement que vous créez sont toujours approuvées FIPS. La configuration du mode FIPS est activée par défaut.

Se reporter à "À propos des normes FIPS (Federal Information Processing Standards)" à la page 527.

Quand vous créez une clé, une valeur salt est toujours générée avec la nouvelle clé. La fourniture de la valeur salt est obligatoire quand vous voulez récupérer une clé.

Considérez l'exemple suivant : `hrs09to12hrs` est une clé créée à l'aide d'une version antérieure de NetBackup :

```
Key Group Name : ENCR_Monday

Supported Cipher : AES_256

Number of Keys : 8

Has Active Key : Yes

Creation Time : Wed Feb 25 22:46:32 2015

Last Modification Time: Wed Feb 25 22:46:32 2015

Description : -

Key Tag :
5e16a6ea988fc8ec7cc9bdbc230811b65583cdc0437748db4521278f9c1bbdf9

Key Name : hrs09to12hrs

Current State : ACTIVE

Creation Time : Wed Feb 25 22:50:01 2015

Last Modification Time: Wed Feb 25 23:14:18 2015

Description : active
```

La clé `hrs09to12hrs` est transférée du groupe de clés `ENCR_Monday` vers un nouveau groupe de clés `ENCR_77`.

```
C:\Program Files\Veritas\NetBackup\bin\admincmd>nbkmsutil -modifykey
-keyname hrs09to12hrs -kgname ENCR_Monday -move_to_kgname ENCR_77

Key details are updated successfully
```

Répertoriez maintenant toutes les clés du groupe de clés `ENCR_77`. Notez que la nouvelle clé `Fips77` est approuvée FIPS, mais pas la clé `hrs09to12hrs`, qui a été créée à l'aide d'une version plus ancienne de NetBackup.

```
C:\Program Files\Veritas\NetBackup\bin\admincmd>nbkmsutil -listkeys
-kgname NCR_77

Key Group Name : ENCR_77 Supported

Cipher : AES_256

Number of Keys : 2

Has Active Key : Yes

Creation Time : Thu Feb 26 04:44:12 2015

Last Modification Time: Thu Feb 26 04:44:12 2015

Description : -
```

```
Key Tag :
5e16a6ea988fc8ec7cc9bdbc230811b65583cdc0437748db4521278f9c1bbdf9

Key Name : hrs09to12hrs

Current State : ACTIVE

Creation Time : Wed Feb 25 22:50:01 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : No

Key Tag :
4590e304aa53da036a961cd198de97f24be43b212b2a1091f896e2ce3f4269a6

Key Name : Fips77

Current State : INACTIVE

Creation Time : Thu Feb 26 04:44:58 2015

Last Modification Time: Thu Feb 26 04:48:17 2015

Description : active

FIPS Approved Key : Yes

Salt : 53025d5710ab36ac1099194fb97bad318da596e27fdfe1f2

Number of Keys: 2
```

La nouvelle clé `Fips77` est approuvée FIPS et a également une valeur salt.

KMS conforme à la norme FIPS est pris en charge sur les plates-formes suivantes :

- MS Windows Server 2012
- Linux.2.6.16 x86-64 Suse-10
- Linux.2.6.18 x86-64 RHEL-5

À propos des normes FIPS (Federal Information Processing Standards)

Les normes FIPS (Federal Information Processing Standards) définissent les conditions de sécurité et d'interopérabilité des systèmes informatiques établies par les gouvernements américain et canadien. La norme FIPS 140-2 définit les exigences de sécurité applicables aux modules cryptographiques. Elle décrit les fonctions de sécurité approuvées pour le chiffrement de clé, l'authentification de message et le hachage symétriques et asymétriques.

Pour plus d'informations sur la norme FIPS 140-2 et son programme de validation, consultez le site Web du programme de validation des modules cryptographiques du National Institute of Standards and Technology (NIST) et du Communications Security Establishment Canada (CSEC) à l'adresse http://csrc.nist.gov/groups/STM/cmvp.

Le module de chiffrement NetBackup est désormais conforme à la norme FIPS. NetBackup KMS utilise le Module de chiffrement NetBackup et peut désormais être exécuté en mode FIPS.

Se reporter à "À propos de KMS conforme à la norme FIPS" à la page 525.

Installation du KMS

La procédure suivante décrit comment installer le KMS.

Remarque : Pour plus d'informations sur la configuration du KMS dans un environnement de stockage en cloud, consultez le Guide de l'administrateur cloud NetBackup.

Le service de KMS est appelé `nbkms`

Le service ne s'exécute que lorsque le fichier de données a été configuré, réduisant ainsi l'effet sur des environnements n'utilisant pas le KMS.

Pour installer KMS

1. Exécutez la commande `nbkms -createemptydb`.
2. Entrez une phrase secrète pour la clé HMK. Vous pouvez également appuyer sur **Entrée** pour créer une clé générée aléatoirement.
3. Entrez un ID pour le HMK. Cet ID peut être un élément descriptif que vous voulez utiliser pour identifier le HMK.
4. Entrez une phrase secrète pour la clé de protection de clé (KPK).
5. Entrez un ID pour le KPK. Cet ID peut être un élément descriptif que vous voulez utiliser pour identifier le KPK.

   Le service de KMS démarre après avoir entré l'ID et appuyé sur Entrée.
6. Démarrez le service en exécutant la commande suivante :

   `nbkms`

   Sous Unix : /usr/openv/netbackup/bin/nbkms

   Sous Windows : *NetBackup_install_path*\NetBackup\bin\nbkms.exe

7 Utilisez la commande `grep` comme suit pour vérifier que le service a démarré :

```
ps -ef | grep nbkms
```

8 Exécutez la commande suivante pour enregistrer le service `nbkms` auprès des services Web de NetBackup :

```
nbkmscmd -discovernbkms
```

9 Créez le groupe de clés. Le nom de groupe de clés doit être une correspondance identique au nom de pool de volumes. Tous les noms de groupe de clés doivent avoir un préfixe `ENCR_`.

Remarque : Lors de l'utilisation de la gestion des clés avec le stockage en cloud et PureDisk, le préfixe `ENCR_` n'est pas requis pour le nom du groupe de clés.

Pour créer un groupe de clés (stockage hors cloud), utilisez la syntaxe de commande suivante. `nbkmsutil -createkg -kgname ENCR_`*`volumepoolname`*

Le préfixe `ENCR_` est essentiel. Quand BPTM reçoit une demande de pool de volumes incluant le préfixe `ENCR_`, il fournit ce nom de pool de volumes au KMS. Le KMS l'identifie en tant que correspondance exacte du pool de volumes et choisit l'enregistrement actif de clé pour des sauvegardes hors de ce groupe.

Pour créer un groupe de clés de stockage en cloud utilisez la syntaxe de commande suivante.

```
nbkmsutil -createkg -kgname storage_server_name:volume_name
```

10 Créez un enregistrement de clé à l'aide de l'option `-createkey`.

```
nbkmsutil -createkey -kgname ENCR_volumepool -keyname keyname
-activate -desc "message"
```

Le nom de clé et le message sont facultatifs ; ils peuvent vous aider à identifier cette clé quand vous affichez la clé.

L'option `-activate` ignore l'état prelive et crée cette clé comme active.

11 Fournissez la phrase secrète à nouveau lorsque le script vous y invite.

Dans l'exemple suivant, le groupe de clés est appelé `ENCR_pool1` et le nom de clé est `Q1_2008_key`. La description explique que cette clé existe pour les mois de janvier, février et mars.

```
nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q1_2008_key
-activate -desc "key for Jan, Feb, & Mar"
```

12 Vous pouvez créer un autre enregistrement de clé à l'aide de la même commande. Un nom de clé différent et une description vous permettent de distinguer les enregistrements de clés : `nbkmsutil -createkey -kgname ENCR_pool1 -keyname Q2_2008_key -activate -desc "key for Apr, May, & Jun"`

Remarque : Si vous créez plus d'un enregistrement de clé à l'aide de la commande `nbkmsutil -kgname` *`name`* `-activate`, seule la dernière clé demeure active.

---

13 Pour répertorier toutes les clés qui appartiennent à un nom de groupe de clés, utilisez la commande suivante :

`nbkmsutil -listkeys -kgname` *keyname*

Remarque : Vous avez besoin de la phrase secrète, de la valeur salt (le cas échéant), du nom du groupe de clés et de l'étiquette de la clé pour récupérer cette clé si elle est perdue. Vous devez stocker toutes ces informations à un emplacement sécurisé. La valeur salt, le nom du groupe de clés et l'étiquette de la clé peuvent être affichés dans la sortie de la commande `nbkmsutil -listkeys`.

La commande et la sortie suivantes utilisent les exemples dans cette procédure.

```
# nbkmsutil -listkeys -kgname ENCR_pool1
Key Group Name         : ENCR_pool1
Supported Cipher       : AES_256
Number of Keys         : 2
Has Active Key         : Yes
Creation Time          : Thu Aug  8 16:23:06 2013
Last Modification Time: Thu Aug  8 16:23:06 2013
Description            : -
 Key Tag    : 825784185f87145c368c54e919908905a45f79927cb733337a53e9b174bbe046
 Key Name               : Q2_2013_key
 Current State          : ACTIVE
 Creation Time          : Thu Aug  8 16:25:19 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description            : key for Apr, May, & Jun
 FIPS Approved Key      : No

 Key Tag    : f63af53ead99920e98f3e0f4a586afccf32e79e75240e65499d1cd0cbd7c7fdd
 Key Name               : Q1_2013_key
 Current State          : INACTIVE
 Creation Time          : Thu Aug  8 16:25:03 2013
 Last Modification Time: Thu Aug  8 16:25:19 2013
 Description            : key for Jan, Feb, & March
 FIPS Approved Key      : No
Number of Keys: 2
```

Se reporter à "Installation de KMS avec mise en cluster HA" à la page 532.

Se reporter à "Utiliser le KMS avec NBAC" à la page 531.

Utiliser le KMS avec NBAC

Les modifications suivantes ont été apportées à NBAC pour prendre en charge l'introduction du KMS :

- Ajout du nouvel objet d'autorisation `KMS`
- Ajout du nouveau groupe d'utilisateur NetBackup `NBU_KMS Admin`

Les autorisations qu'un utilisateur a sur l'objet KMS détermine les tâches associées à KMS que vous êtes autorisé à effectuer.

Tableau 20-1 affiche les autorisations par défaut du KMS pour chacun des groupes d'utilisateurs NetBackup.

Tableau 20-1 Autorisations par défaut de KMS pour des groupes d'utilisateur NetBackup

Définir	Activité	NBU_User	NBU_Operator	NBU_Admin	NBU_Security Admin	Vault_Operator	Administrateur NBU_ SAN	Administrateur NBU_ KMS
Parcourir	Parcourir	---	---	X	---	---	---	X
Lecture	Lecture	---	---	X	---	---	---	X
Configurer	Nouveau	---	---	---	---	---	---	X
Configurer	Supprimer	---	---	---	---	---	---	X
Configurer	Modifier	---	---	---	---	---	---	X

Outre les autorisations de KMS listées ci-dessus, le groupe d'administrateur NBU_KMS possède également les autorisations suivantes sur d'autres objets d'autorisation :

- BUAndRest a les autorisations Parcourir, Lecture, Sauvegarde, Restauration, Liste
- HostProperties a les autorisations Parcourir, Lecture
- Licence a les autorisations Parcourir, Lecture

Installation de KMS avec mise en cluster HA

Dans un environnement typique de NetBackup, il est possible que tous les packages facultatifs ne soient pas installés, sous licence ou configurés. Dans de tels scénarios, aucun service qui concernent ces produits facultatifs ne peut être en permanence actif. Ces services sont par conséquent non contrôlés par défaut et ne font pas basculer NetBackup s'ils échouent. Si à un moment ultérieur un produit facultatif est installé, sous licence et configuré, ses services peuvent alors être manuellement configurés et NetBackup peut basculer Dans cette section, nous présentons les étapes manuelles pour installer le KMS afin de contrôler le cluster.

Activer la surveillance du service de KMS

Vous pouvez activer la surveillance du service KMS et le basculement de NetBackup lorsque le service échoue.

Pour activer le contrôle du service KMS et du basculement NetBackup lorsqu'il échoue

1. Ouvrez une invite de commande sur le nœud actif du cluster.
2. Modifiez le répertoire comme suit :

   Sous Windows : `<NetBackup_install_path>\NetBackup\bin`

   Sous UNIX : `/usr/openv/netbackup/bin`
3. Exécutez la commande suivante.

   Sous Windows : `bpclusterutil -enableSvc "NetBackup Key Management Service"`

   Sous UNIX : `bpclusterutil -enableSvc nbkms`

Désactivation de la surveillance du service KMS

Vous pouvez désactiver le contrôle du service de KMS.

Pour désactiver le contrôle du service de KMS

1. Ouvrez une invite de commande sur le nœud actif du cluster.
2. Modifiez le répertoire comme suit :

   Sous Windows : `<NetBackup_install_path>\NetBackup\bin`

   Sous UNIX : `/usr/openv/netbackup/bin`
3. Exécutez la commande suivante :

   Sous Windows : `bpclusterutil -disableSvc "NetBackup Key Management Service"`

   Sous UNIX : `bpclusterutil -disableSvc nbkms`

Configuration de KMS

La configuration du KMS s'effectue en créant la base de données de clés, les groupes de clés et les enregistrements de clés. NetBackup est ensuite configuré pour fonctionner avec le KMS.

Pour configurer et démarrer le KMS

1. Créez la base de données de clés, la clé principale de l'hôte (HMK) et la clé de protection de clé (KPK).
2. Créez un groupe de clés qui correspond au pool de volumes.
3. Créez un enregistrement actif de clé.

Création de la base de données de clés

Utilisez la procédure suivante pour créer une base de données de clés vide. Une base de données de clés est créée en invoquant le nom de service avec l'option `-createemptydb`. Ce processus vérifie et garantie qu'une base de données de clés existante n'existe pas déjà et poursuit ensuite la création. Deux clés de protection doivent être créées lorsque le KMS est initialisé. Il s'agit de la clé machine d'hôte (HMK) et la clé de protection de clé (KPK).

Comme avec toutes les activités de création de clé de KMS, l'utilisateur se voit proposer les options suivantes pour créer ces clés :

- Les clés sont générées par des phrases secrètes
- Phrases secrètes générées aléatoirement

Vous êtes invité à fournir un ID logique à associer à chaque clé. A la fin de cette opération, la base de données de clés et les clés de protection sont établies.

Sur un système de Windows, elles peuvent être trouvées dans les fichiers suivants :

```
NetBackup_install_path\kms\db\KMS_DATA.dat
NetBackup_install_path\kms\key\KMS_HMKF.dat
NetBackup_install_path\kms\key\KMS_HKPKF.dat
```

Sur un système UNIX, elles peuvent être trouvées dans les fichiers suivants :

```
/usr/openv/kms/db/KMS_DATA
/usr/openv/kms/key/KMS_HMKF
/usr/openv/kms/key/KMS_HKPKF
```

Pour créer la base de données de clés

1. Exécutez la commande suivante :

   ```
   nbkms -createemptydb.
   ```

2. Entrez une phrase secrète pour la clé HMK (Host Master Key) ou appuyez sur Entrée pour utiliser une clé générée aléatoirement. Saisissez à nouveau la phrase secrète à l'invite suivante.

3. Entrez l'ID HMK. Cet ID est associé au HMK ; vous pouvez l'utiliser pour trouver cette clé particulière à l'avenir.
4. Entrez une phrase secrète pour la clé de protection de clé ou appuyez sur Entrée pour utiliser une clé générée aléatoirement. Saisissez à nouveau la phrase secrète à l'invite suivante.
5. Entrez l'ID du KPK. Cet ID peut être un élément descriptif que vous voulez utiliser pour identifier le KPK.

Groupes de clés et enregistrements de clé

Un groupe de clés est un ensemble logique d'enregistrements de clés où un seul enregistrement se trouve en état actif.

Une définition de groupe de clés comprend les éléments suivants :

- Nom
  Donné à un groupe de clés. Doit être unique dans le keystore. Le renommage du groupe de clés est pris en charge si le nouveau nom est unique dans le keystore.
- Etiquette
  Identifiant de groupe de clés unique (non mutable).
- Chiffre
  Chiffre pris en charge Toutes les clés appartenant à ce groupe de clés sont créées avec ce chiffre à l'esprit (non mutable).
- Description
  N'importe quelle description (mutable).
- Heure de création
  Heure de création de ce groupe de clés (non mutable).
- Dernier heure de modification
  Date de dernière modification d'un des attributs mutables (ou immuable).

Création de groupes de clés

La première étape pour configurer le chiffrement consiste à créer un groupe de clés.

Dans l'exemple suivant, le groupe de clés `ENCR_mygroup` est créé :

```
nbkmsutil -createkg -kgname ENCR_mygroup
```

Remarque : En cas de stockage AdvancedDisk ou de stockage sur bande, il est important que le nom du groupe que vous créez (c.-à-d., `mygroup`) soit préfixé de `ENCR_`.

Création d'enregistrements de clé

L'étape suivante consiste à créer un enregistrement actif de clé. L'enregistrement de clé peut être créé dans l'état prelive et être transféré vers l'état actif. Ou il peut être directement créé dans l'état actif.

Un enregistrement de clé comprend les informations essentielles suivantes :

- Nom
  Nom donné à une clé, devrait être unique dans un KG. Le renommage du groupe de clés est pris en charge si le nouveau nom est unique dans le keystore.
- Etiquette de clé
  Identifiant de clé unique (non mutable).
- Etiquette de groupe de clés
  Identifiant KG unique auquel cette clé appartient (non mutable).
- Etat
  Etat actuel de la clé (mutable).
- Clé de chiffrement
  Clé utilisée pour chiffrer ou déchiffrer la sauvegarde ou pour restaurer des données (non mutables).
- Description
  N'importe quelle description (mutable).
- Heure de création
  Heure de création de clé (non mutable).
- Dernier heure de modification
  Date de dernière modification d'un des attributs mutables (ou immuable).

Les états suivants d'enregistrement de clé sont disponibles :

- Prelive indique que l'enregistrement a été créé, mais n'a pas été utilisé
- Actif indique que l'enregistrement et la clé sont utilisés pour le chiffrement et le déchiffrement
- Inactif indique que l'enregistrement et la clé ne peuvent pas être utilisés pour le chiffrement. Ils peuvent toutefois être utilisés pour le déchiffrement
- Désapprouvé indique que l'enregistrement ne peut pas être utilisé pour le chiffrement ou le déchiffrement

- Terminé indique que l'enregistrement peut être supprimé

Présentation des états d'enregistrement de clé

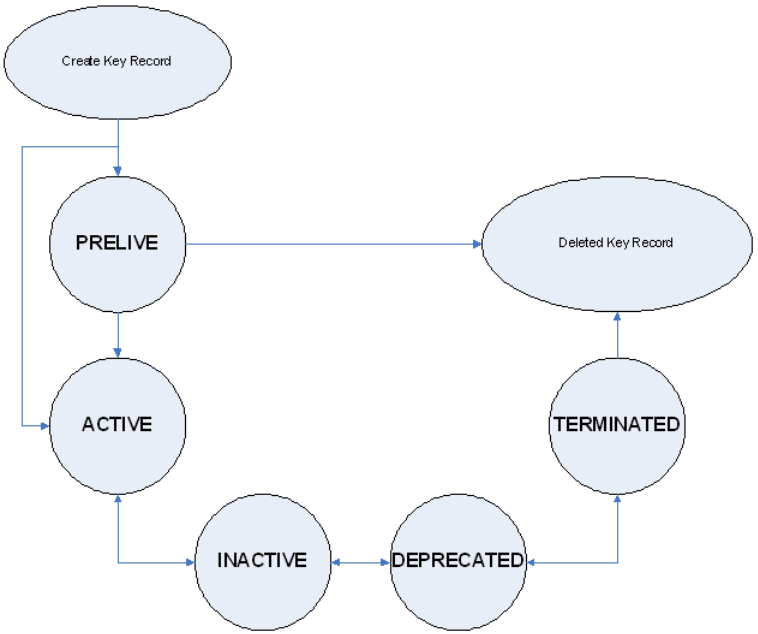
Les états d'enregistrement de clé sont prelive, actif, inactif, obsolète et terminé. Les états d'enregistrement de clé adhèrent à un cycle de vie d'enregistrement de clé. Une fois qu'une clé est entrée dans l'état actif (c'est-à-dire configurée pour le chiffrement), la clé doit progresser dans l'odre appropriée à travers le cycle de vie. La commande appropriée inclut le passage d'un état à son état adjacent. Une clé ne peut pas contourner les états.

Entre l'état actif et l'état terminé, l'enregistrement peut déplacer un état à la fois dans une direction ou l'autre. En dehors de cette plage d'état, les transitions sont unidirectionnelles. Les enregistrements de clés supprimés ne peuvent pas être récupérés (à moins qu'ils aient été créés en utilisant une phrase de passe) et les clés actives ne peuvent pas être redéplacées à l'état prelive.

Remarque : Des clés peuvent être créées dans l'état prelive ou actif. Les enregistrements actifs de clés sont disponibles pour des opérations de sauvegarde et de restauration. Une clé inactive est uniquement disponible pour des opérations de restauration. Les clés désapprouvées ne sont pas disponibles pour être utilisées. Si votre enregistrement de clé est dans l'état désapprouvé et vous tentez d'effectuer une sauvegarde ou une restauration avec cet enregistrement de clé, il peut échouer. Un enregistrement de clé dans l'état terminé peut être supprimé du système.

Le schéma suivant indique le déroulement du processus de création de clés dans un état prelive ou actif.

Figure 20-1 Etats possibles pour la création de clés



Considérations d'états d'enregistrement de clé

Les considérations suivantes peuvent être suivies pour des états d'enregistrement de clé.

- Les transitions d'état d'enregistrement de clé sont bien définies et vous devez parcourir tout le chemin d'accès des états pour supprimer un enregistrement de clé.
- Définir un enregistrement de clé sur « actif » définit l'état de l'enregistrement de clé actif sur « inactif » pour ce groupe. Il ne peut y avoir qu'un seul enregistrement actif dans un groupe.
- L'état désapprouvé est utile pour enregistrer une clé et restreindre son utilisation. Si, en tant qu'administrateur, vous pensez qu'une clé a été compromise, vous pouvez manuellement suspendre son utilisation par toute personne l'utilisant sans supprimer la clé du système. Vous pouvez définir l'enregistrement de clé sur l'état désapprouvé et toute personne tentant d'effectuer une sauvegarde ou une restauration avec cette clé désapprouvée obtiendra une erreur.
- La suppression d'enregistrement de clé implique deux étapes permettant de réduire la possibilité de supprimer accidentellement une clé. Vous devez d'abord définir les clés désapprouvées sur terminé et vous pouvez ensuite supprimer

l'enregistrement de clé. Seuls les enregistrements terminés de clé peuvent être supprimés (autre que les clés se trouvant dans l'état prelive).

- Vous pouvez utiliser l'état prelive pour créer un enregistrement de clé avant de l'utiliser.

État d'enregistrement de clé prelive

Un enregistrement de clé créé dans l'état prelive peut être activé ou supprimé.

L'état prelive peut être utilisé de la façon suivante :

- L'administrateur de KMS veut tester la création d'un enregistrement de clé sans affecter le système. Si l'enregistrement est correctement créé, il peut alors être activé. S'il n'est pas correctement créé, il peut être supprimé.
- L'administrateur de KMS veut créer un enregistrement de clé, mais seulement l'activer à un moment donné dans le futur. Les raisons de ce problème peuvent inclure le retard de configuration de l'enregistrement sur actif jusqu'à ce que le keystore de KMS ait été sauvegardé (ou le mot de passe ait été enregistré). Ou le retard de configuration de l'enregistrement sur actif jusqu'à une certaine heure dans le futur.

  Les enregistrements de clés dans l'état prelive peuvent être activés ou supprimés du système.

État d'enregistrement de clé actif

Des enregistrements actifs de clés peuvent être utilisés pour chiffrer et déchiffrer des données. S'il y a lieu, l'enregistrement actif de clé peut être rendu inactif. L'état actif est l'un des trois états de gestion des données les plus importants. L'état inactif et l'état désapprouvé sont les deux autres états importants de gestion des données.

Des enregistrements de clés peuvent être directement créés dans l'état actif en contournant l'état prelive. Des enregistrements de clés dans l'état actif peuvent rester actifs ou être rendus inactifs. Les enregistrements actifs ne peuvent pas retourner à l'état prelive.

État d'enregistrement de clé inactif

Des enregistrements inactifs de clés peuvent être utilisés pour déchiffrer des données. S'il y a lieu, l'enregistrement inactif de clé peut être de nouveau être activé ou être déplacé à l'état désapprouvé. L'état inactif est l'un des trois états de gestion des données les plus importants. L'état actif et l'état obsolète sont les deux autres états importants de gestion des données.

Les enregistrements de clés dans l'état inactif peuvent rester inactifs, être activés ou rendus obsolètes.

État d'enregistrement de clé obsolète

Des enregistrements désapprouvés de clés ne peuvent pas être utilisés pour chiffrer ou déchiffrer des données. S'il y a lieu, l'enregistrement de clé dans l'état désapprouvé ont pu être rendu inactif ou terminé. L'état désapprouvé est l'un des trois états de gestion des données les plus importants. L'état actif et l'état inactif sont les deux autres états importants de gestion des données.

L'état désapprouvé peut être utilisé des manières suivantes :

- L'utilisation d'une clé doit être suivie ou réglementée. La tentative d'utilisation d'une clé désapprouvée peut échouer, jusqu'à ce que son état soit modifié sur l'état approprié.
- Une clé ne devrait plus être nécessaire, mais pour plus de sécurité, elle n'est pas définie sur l'état terminé.
  Des enregistrements de clés dans l'état désapprouvé peuvent rester désapprouvés, être rendus inactifs ou être terminés.

État d'enregistrement de clé terminé

L'état terminé ajoute une seconde étape ou une étape de sécurité pour supprimer un enregistrement de clé dans l'état désapprouvé. Un enregistrement terminé de clé peut être déplacé à l'état désapprouvé et être finalement rendu de nouveau actif si nécessaire. Un enregistrement terminé de clé peut également être supprimé du KMS.

Attention : Avant de supprimer une clé, assurez-vous qu'aucune image valide existante n'a été chiffrée avec cette clé

Les enregistrements de clés dans l'état terminé peuvent rester terminés, devenir désapprouvés ou être physiquement supprimés.

Sauvegarde des fichiers de base de données KMS

Sauvegarder la base de données KMS implique de sauvegarder les fichiers KMS.

L'utilitaire de KMS a une option qui permet de suspendre les fichiers de base de données ou d'empêcher temporairement quiconque de modifier les fichiers de données. Il est important d'exécuter l'option de suspension si vous prévoyez de copier les fichiers `KMS_DATA`, `KMS_HMKF` et `KMS_KPKF` dans un autre emplacement pour les sauvegarder.

Pendant la suspension, NetBackup supprime l'accès en écriture pour ces fichiers ; seul l'accès en lecture est autorisé.

Quand vous exécutez `nbkmsutil -quiescedb`, il renvoie une suspension réussie et le nombre d'appels en cours. Le nombre d'appels en cours n'est qu'un nombre. Un nombre est placé sur le fichier pour le nombre de demandes en attente sur ce fichier.

Après la suspension, vous pouvez sauvegarder les fichiers en les copiant sur un autre emplacement de répertoire.

Après avoir copié les fichiers, vous pouvez réactiver les fichiers de base de données KMS à l'aide de `nbkmsutil -unquiescedb`.

Lorsque le nombre d'appels de suspension en cours atteint zéro, le KMS exécute des commandes qui pourraient modifier les fichiers `KMS_DATA`, `KMS_HMKF` et `KMS_KPKF`. L'accès en écriture est de nouveau accessible pour ces fichiers.

Récupération de KMS en restaurant tous les fichiers de données

Si vous avez effectué des copies de sauvegarde des fichiers `KMS_DATA`, `KMS_HMKF` et `KMS_KPKF`, il suffit de restaurer ces trois fichiers. Démarrez alors le service `nbkms` et le système KMS sera de nouveau en service.

Récupération de KMS en restaurant seulement le fichier de données de KMS

Vous pouvez restaurer la copie sauvegardée du fichier de données KMS `kms/db/KMS_DATA` en régénérant les fichiers `KMS_HMKF` et `KMS_KPKF` avec des mots de passe. Ainsi, si vous avez écrit les phrases secrètes pour la clé machine d'hôte (HMK) et la clé de protection de clé, vous pouvez exécuter une commande afin de régénérer ces fichiers. Le système vous invite à entrer la phrase secrète et si la phrase secrète correspond à la phrase secrète initialement entrée, vous pourrez réinitialiser les fichiers.

Récupération de KMS en restaurant uniquement le fichier de données KMS

1. Exécutez la commande de `nbkms -resetkpk`.
2. Exécutez la commande `nbkms -resethmk`.
3. Démarrez le service `nbkms`.

Récupération de KMS en régénérant la clé de chiffrement des données

Vous pouvez régénérer la base de données KMS en régénérant les clés de chiffrement des données. Le but est de créer une nouvelle base de données KMS vide et de la remplir avec tous les enregistrements de clés.

Remarque : Une clé générée aléatoirement ne peut pas être récupérée si elle est perdue.

Récupération de KMS en régénérant la clé de chiffrement des données

1. Créez une base de données KMS vide en exécutant la commande suivante

   ```
   nbkms -createemptydb
   ```

   Vous ne devez pas utiliser les mêmes clé machine d'hôte et clé de protection de clé. Vous pouvez choisir de nouvelles clés.

2. Exécutez la commande `nbkmsutil -recoverkey` et spécifiez le groupe de clés, le nom de clé et l'étiquette.

   ```
   nbkmsutil -recoverkey -kgname ENCR_pool1 -keyname Q1_2008_key
     -tag
   d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
   ```

   Si vous n'avez pas gardé de copie électronique de la sortie de la commande `nbkmsutil -listkey` lorsque vous avez créé la clé, vous devez entrer les 64 caractères manuellement.

3. Entrez la phrase secrète (et la valeur salt si la clé a été initialement générée avec NetBackup 7.7 ou une version ultérieure) dans l'invite. Elle doit correspondre exactement à la phrase secrète saisie auparavant.

   La valeur salt (le cas échéant) doit correspondre à la valeur salt associée à la clé que vous souhaitez récupérer.

   Remarque : Si l'étiquette que vous entrez existe déjà dans la base de données de KMS, alors vous ne pouvez pas recréer la clé.

4. Si la clé récupérée est la clé que vous voulez utiliser pour des sauvegardes, exécutez la commande suivante pour activer la clé :

   ```
   nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key
    -state active
   ```

   L'option `-recoverkey`place l'enregistrement de clé dans l'état inactif et elle est introduite dans la base de données KMS dans l'état inactif.

5. Si c'est un enregistrement de clé qui doit être désapprouvé, exécutez la commande suivante :

   ```
   nbkmsutil -modifykey -kgname ENCR_pool1 -keyname Q1_2008_key
   -state deprecated
   ```

Problèmes de sauvegarde des fichiers de données KMS

Des problèmes de sauvegarde des fichiers de données KMS peuvent se produire avec les bandes normales de NetBackup ou avec la sauvegarde de catalogue.

Attention : Les fichiers de données KMS ne sont pas inclus dans les sauvegardes de catalogue de NetBackup.

Si les KPK, les HMK et les fichiers de clés étaient inclus dans une sauvegarde de catalogue et la bande de sauvegarde de catalogue est perdue, le keystore est compromis car la bande contient tout les éléments requis pour accéder aux clés.

Des problèmes significatifs peuvent exister si les bandes de données et de sauvegarde de catalogue sont toutes deux perdues sur le même camion de transport, par exemple. Si les deux bandes sont perdues ensemble, la situation n'est pas mieux que n'avoir jamais chiffré la bande dès le départ.

Le chiffrement du catalogue n'est pas une bonne solution non plus. Si le KPK, le HMK et le fichier de clés étaient inclus dans une sauvegarde de catalogue et la sauvegarde de catalogue elle-même est chiffrée, c'est comme si vous aviez laissé les clés dans la voiture verrouillée. C'est pour éviter ce problème que le KMS a été établi en tant que service distinct pour NetBackup et que les fichiers KMS sont dans un répertoire distinct des répertoires NetBackup. Il existe cependant des solutions pour sauvegarder les fichiers de données KMS.

Solutions pour sauvegarder les fichiers de données KMS

La meilleure solution pour sauvegarder des fichiers de données KMS consiste à effectuer l'opération en dehors du processus normal de NetBackup ou de compter sur les clés de chiffrement générées par phrase de passe pour reconstruire manuellement le KMS. Toutes les clés peuvent être générées par des phrases de passe. Ainsi si vous avez enregistré toutes les phrases de passe, vous pouvez recréer le KMS manuellement à partir des informations que vous avez notées. La sauvegarde de KMS peut être effectuée en plaçant les informations de KMS sur un CD, un DVD ou un lecteur USB distinct.

Création d'un enregistrement de clé

La procédure suivante explique comment créer un enregistrement de clé à l'aide d'une phrase secrète, en contournant l'état prelive et en créant une clé active.

Remarque : Si vous tentez d'ajouter une clé à un groupe qui possède déjà une clé active, la clé existante est automatiquement placée dans l'état inactif.

Création d'un enregistrement de clé et d'une clé active

1. Pour créer un enregistrement de clé, entrez la commande suivante :

```
nbkmsutil -createkey -usepphrase -kgname ENCR_mygroup -keyname
my_latest_key -activate -desc "key for Jan, Feb, March data"
```

2. Entrez une phrase secrète.

Liste des clés d'un groupe de clés

Utilisez la procédure suivante pour lister toutes ou une sélection de clés que vous avez créées dans un groupe de clés particulier.

Pour lister les clés dans un groupe de clés

- Pour lister les clés dans un groupe de clés, entrez la commande suivante :

```
nbkmsutil -listkeys -kgname ENCR_mygroup
```

`nbkmsutil` sort la liste dans le format détaillé par défaut. Voici une sortie de liste non détaillée.

```
KGR ENCR_mygroup AES_256 1 Yes 134220503860000000

134220503860000000 -
KR my_latest_key Active 134220507320000000 134220507320000000
key for Jan, Feb, March data
Number of keys: 1
```

Les options suivantes aident à répertorier toutes les clés d'un groupe de clés ou une clé spécifique d'un groupe de clés :

```
nbkmsutil -listkeys -all | -kgname <key_group_name> [ -keyname
<key_name> | -activekey ]

[ -noverbose | -export ]
```

L'option `-all` dresse la liste de toutes les clés de tous les groupes de clés. Les clés sont répertoriées dans un format détaillé.

L'option `-kgname` dresse la liste des clés du groupe de clés spécifié.

L'option `-keyname` dresse la liste d'une clé spécifique dans le groupe de clés spécifié. Elle doit cependant être utilisée avec l'option -kgname.

L'option `-activekey` dresse la liste d'une clé active dans le groupe de clés spécifié. Elle doit cependant être utilisée avec l'option `-kgname`.

Remarque : Les options `-activekey` et `-keyname` s'excluent mutuellement.

L'option `-noverbose` dresse la liste des détails des clés et des groupes de clés dans un formulaire formaté (non-accessible en lecture). Le paramètre par défaut est une liste détaillée.

L'option `-export` génère une sortie requise par le fichier key_file. (Le `key_file` est utilisé dans le fichier `nbkmsutil -export -path <key_container_path > -key_file`. Vous pouvez utiliser la sortie pour un autre -key_file.

Exécutez la commande suivante pour répertorier toutes les clés d'un groupe de clés :

```
nbkmsutil -listkeys -kgname <key_group_name>
```

Exécutez la commande suivante pour répertorier les clés spécifiques d'un groupe de clés :

```
nbkmsutil -listkeys -kgname <key_group_name> -keyname <key_name>
```

Exécutez la commande suivante pour répertorier toutes les clés de tous les groupes :

```
nbkmsutil -listkeys -all
```

Exécutez la commande suivante pour répertorier toutes les clés d'un groupe de clés :

```
nbkmsutil -listkeys -kgname <key_group_name>
```

Exécutez la commande suivante pour répertorier les clés actives d'un groupe de clés :

```
nbkmsutil -listkeys -kgname <key_group_name> -activekey
```

Configuration de NetBackup pour fonctionner avec le KMS

La configuration de NetBackup pour fonctionner avec le KMS implique les rubriques suivantes :

- NetBackup obtient des enregistrements de clés de KMS
  Se reporter à "NetBackup et enregistrements de clé de KMS" à la page 546.
- Configuration de NetBackup pour utiliser le chiffrement
  Se reporter à "Exemple de configuration de NetBackup pour utiliser le chiffrement de bande" à la page 546.

NetBackup et enregistrements de clé de KMS

La première étape pour configurer NetBackup afin qu'il fonctionne avec le KMS consiste à installer un lecteur de bande prenant en charge NetBackup et capable de chiffrer, ainsi que le média de bande requis.

La deuxième étape est de configurer NetBackup normalement, sauf que les médias capables de chiffrement doivent être placés dans un pool de volumes avec le même nom que le groupe de clés que vous avez créé lors de la configuration de KMS.

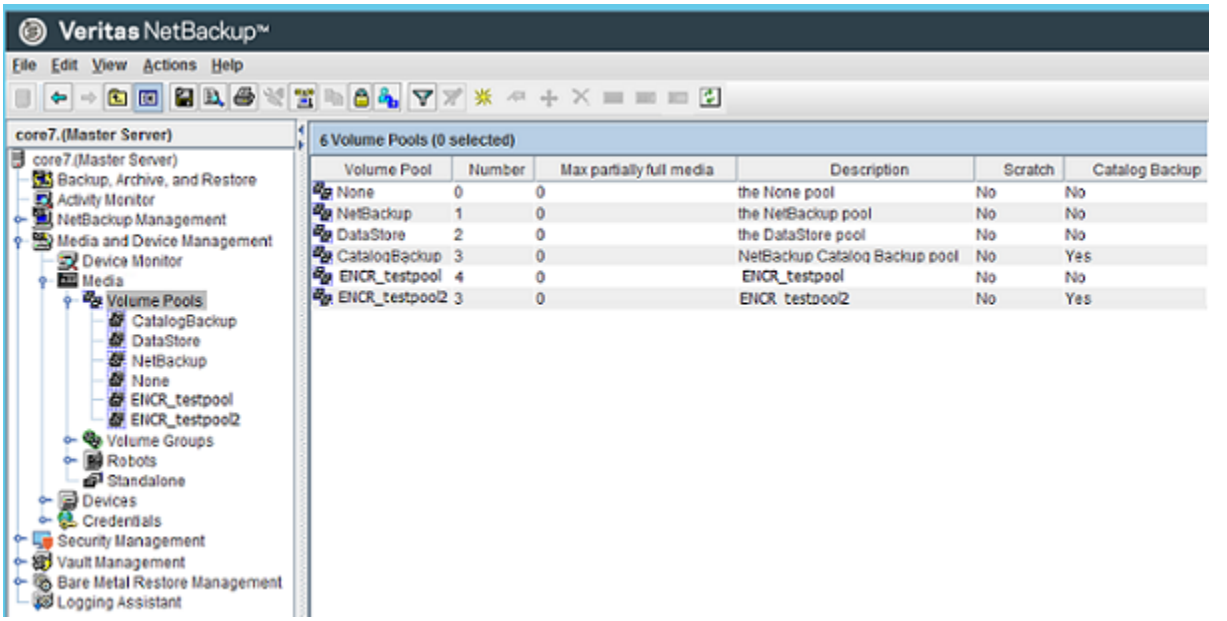
Remarque : Pour AdvancedDisk et le stockage sur bande, la fonction de gestion des clés nécessite que le nom du groupe de clés et celui du pool de volumes de NetBackup correspondent et qu'ils soient préfixés de `ENCR_`. Pour le stockage en cloud et PureDisk, le nom du groupe de clés doit être *storage_server_name*:*volume_name*. Cette méthode de prise en charge du chiffrement est disponible sans devoir apporter de grands changements à l'infrastructure de gestion-système de NetBackup.

Exemple de configuration de NetBackup pour utiliser le chiffrement de bande

L'exemple suivant configure deux pools de volumes NetBackup créés pour le chiffrement (avec le préfixe `ENCR_`).

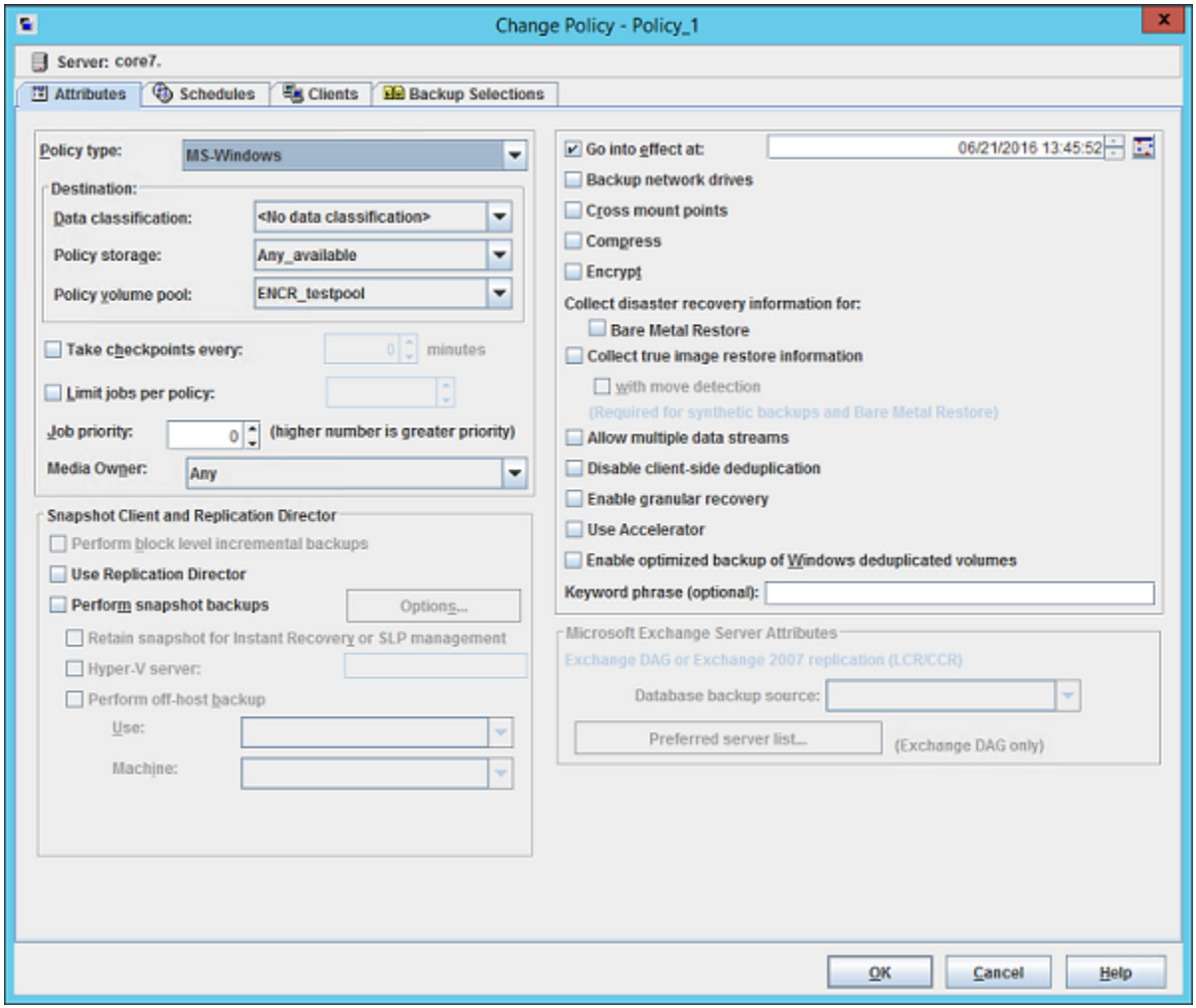
Le schéma suivant affiche la **console d'administration NetBackup** avec deux pools de volumes ayant la bonne convention de nommage pour utiliser le KMS.

Figure 20-2 Console d'administration NetBackup avec deux pools de volumes configurés pour utiliser le KMS



décrit une politique NetBackup configurée pour utiliser le pool de volumes , qui possède le même nom que le groupe de clés que vous avez configuré auparavant.

Figure 20-3 Boîte de dialogue Modifier une politique de NetBackup avec le pool de volumes de KMS



Quand une image de NetBackup a été chiffrée, l'indicateur de clé est enregistré et associé à l'image. Vous pouvez consulter ces informations via les rapports de la **console d'administration NetBackup** ou dans la sortie des commandes `bpimmedia` et `bpimagelist`.

Configuration du KMS NetBackup à l'aide de l'application Web KMS

Si vous configurez le KMS NetBackup (NBKMS), NetBackup ne l'utilise pas pour des opérations de gestion des clés. Pour activer le serveur KMS, exécutez la commande suivante :

```
nbkmscmd -configureKMS -type NBKMS
```

Utilisation de KMS pour le chiffrement

Vous pouvez utiliser le KMS pour exécuter une sauvegarde de bande chiffrée, vérifier une sauvegarde de bande chiffrée et gérer des clés. Les rubriques suivantes fournissent des exemples pour chacun de ces scénarios :

- Exemple d'exécution d'une sauvegarde sur bande chiffrée
  Se reporter à "Exemple d'exécution d'une sauvegarde sur bande chiffrée" à la page 550.
- Exemple de vérification d'une sauvegarde de chiffrement
  Se reporter à "Exemple de vérification d'une sauvegarde de chiffrement" à la page 551.
- Importation d'images chiffrées par KMS
  Se reporter à "Importation d'images chiffrées par KMS" à la page 549.

Importation d'images chiffrées par KMS

L'importation des images chiffrées par KMS est une opération en deux phases. Dans la première phase, les en-têtes de médias et chaque en-tête de sauvegarde de fragment sont lus. Ces données ne sont jamais chiffrées. Cependant, les en-têtes de sauvegarde indiquent si les données du fichier de fragments sont chiffrées à l'aide de KMS ou non. En résumé, la phase un ne requiert pas de clé.

La phase deux recompile le fichier de catalogue `.f` qui nécessite la lecture des données chiffrées. L'étiquette de clé `key-tag` (`KAD` en termes `SCSI`) est stockée sur la bande par le matériel. Le processus `NBU`/`BPTM` lit l'étiquette de clé `key-tag` du lecteur et l'envoie au KMS pour rechercher la clé. Si le service trouve la clé, les processus de la phase deux continuent à lire les données chiffrées. Si le service ne trouve aucune clé, les données ne sont pas accessibles en lecture tant que le service KMS n'a pas recréé la clé. C'est là que la phrase de passe est importante.

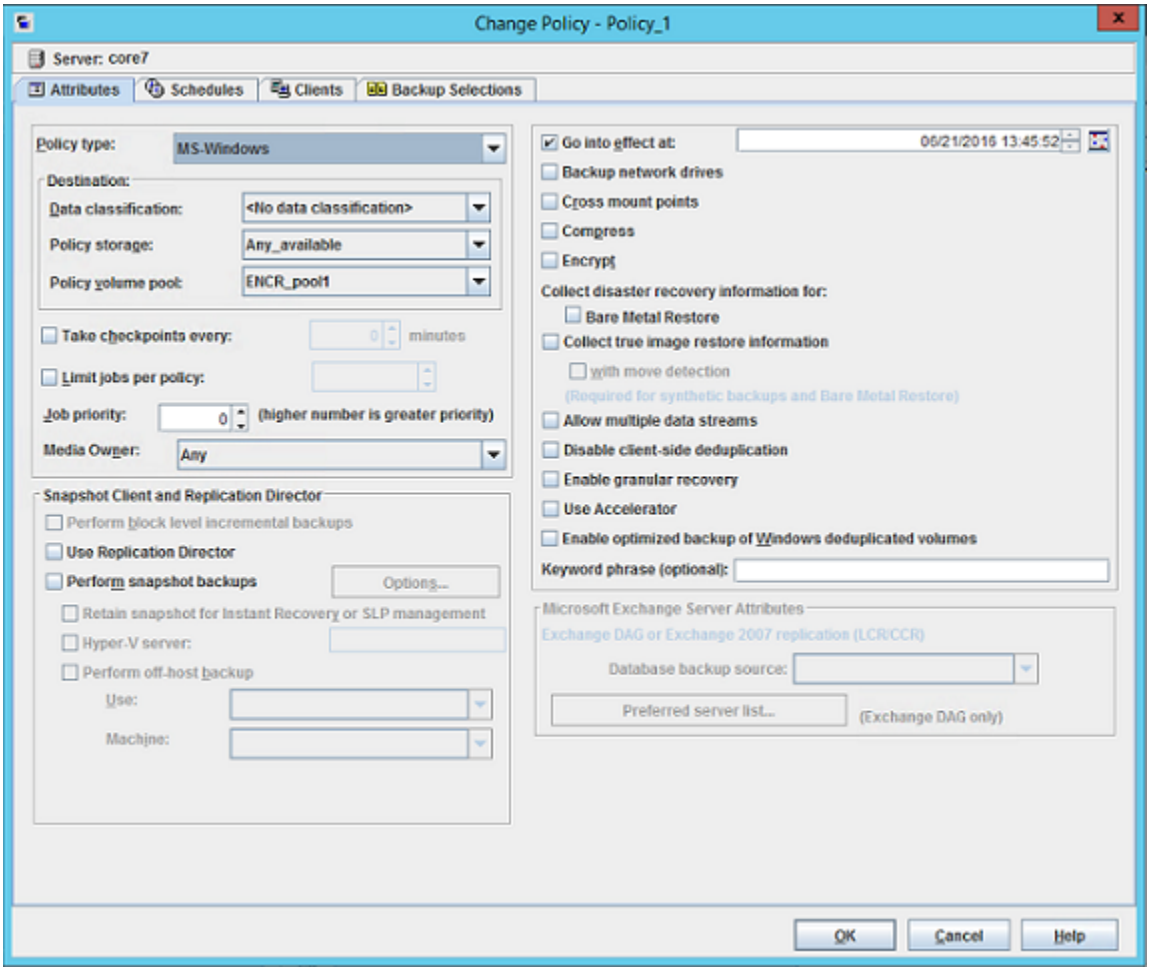
Si vous ne les avez pas détruites, le service KMS contient toutes les clés déjà utilisées et vous pouvez importer n'importe quelle bande chiffrée. Transférez le keystore sur votre site DR pour ne pas avoir à le recréer.

Exemple d'exécution d'une sauvegarde sur bande chiffrée

Pour exécuter une sauvegarde de bande chiffrée, vous devez disposer d'une politique configurée pour puiser à partir d'un pool de volumes ayant le même nom que votre groupe de clé.

décrit une politique NetBackup que vous avez configurée pour utiliser le pool de volumes .

Figure 20-4 Boîte de dialogue Modifier une politique de NetBackup avec le pool de volumes ENCR_pool1 de KMS



Exemple de vérification d'une sauvegarde de chiffrement

Quand NetBackup exécute une sauvegarde de bande chiffrée et vous affichez les Images sur média, vous consultez l'étiquette de clé de chiffrement qui est enregistrée avec l'enregistrement. Cette étiquette de clé indique que ce qui a été écrit sur la bande a été chiffré. L'étiquette de clé de chiffrement identifie de manière unique la clé utilisée pour chiffrer les données. Vous pouvez exécuter un rapport et lire la colonne de la politique pour déterminer si tous les éléments d'une bande particulière ont été chiffrés.

Éléments constitutifs d'une base de données KMS

La base de données KMS se compose de trois fichiers :

- Le fichier de keystore (`KMS_DATA`) contient tous les enregistrements de groupe de clés et de clés avec quelques métadonnées.
- Le fichier de KPK (`KMS_KPKF`) contient le KPK utilisé pour chiffrer les parties de cryptogramme des enregistrements de clés qui sont stockés dans le fichier de keystore.
- Le fichier de HMK (`KMS_HMKF`) contient le HMK utilisé pour chiffrer tout le contenu du fichier de keystore. L'en-tête de fichier de keystore est une exception. Il contient certaines métadonnées comme l'ID de KPK et l'ID de HMK qui n'est pas chiffré).

Création d'une base de données vide de KMS

Une base de données KMS vide peut être créée en exécutant la commande `nbkms -createemptydb`.

Cette commande vous invite à saisir les informations suivantes :

- Phrase secrète de la clé principale de l'hôte (HMK) (laissez vide pour une clé principale de l'hôte quelconque)
- ID HMK
- Phrase secrète KPK (laissez vide pour un KPK quelconque)
- ID KPK

Les procédures de sauvegarde et de récupération d'urgence de bases de données KMS varient pour les KPK et HMK générés aléatoirement ou par phrase secrète, comme indiqué ci-dessous.

Pour effectuer une récupération lorsque les HMK et les KPK ont été générés aléatoirement

1. Restaurez le fichier de keystore d'une sauvegarde.
2. Exécutez la commande `nbkms -info` pour trouver l'ID de KPK et l'ID de HMK du KPK et du HMK requis pour déchiffrer ce fichier de keystore. La sortie devrait également vous informer que les HMK et les KPK pour ce fichier de keystore ont été générés aléatoirement.
3. Restaurez le fichier de HMK correspondant à l'ID de HMK d'une sauvegarde sécurisée.
4. Restaurez le fichier de KPK correspondant à l'ID de KPK d'une sauvegarde sécurisée.

Importance de l'ID de KPK et de l'ID de HMK

Pour déchiffrer le contenu d'un fichier de keystore, il est essentiel d'identifier les KPK et HMK appropriés pour cette tâche. L'ID de KPK et l'ID de HMK vous permettent d'effectuer cette identification. Puisque ces ID sont stockés non chiffrés dans l'en-tête de fichier de keystore, ils peuvent être déterminés même si vous avez seulement accès au fichier de keystore. Il est important de choisir des ID uniques et de se souvenir de l'association des ID aux phrases secrète et aux fichiers pour pouvoir exécuter une reprise après incident.

Mise à jour périodique du HMK et du KPK

Le HMK et le KPK peuvent être mis à jour périodiquement à l'aide des options `modifyhmk` et `modifykpk` de l'interface de ligne de commande KMS. Ces opérations vous invitent à saisir une nouvelle phrase secrète et un nouvel ID, puis à mettre à jour le KPK/HMK. Vous pouvez choisir une KPK/HKM aléatoire ou basée sur une phrase secrète à chacune de ces invocations.

Remarque : C'est une pratique d'excellence d'utiliser l'option `-usepphrase` lorsque vous modifiez la HMK et la KPK afin qu'on vous demande d'utiliser une phrase secrète connue pour une récupération ultérieure. Avec l'option -nopphrase, KMS génère une phrase secrète aléatoire qui est inconnue et élimine la possibilité de récupération ultérieure, si nécessaire.

Sauvegarde des clés de keystore et d'administrateur de KMS

Les fichiers de données importants du KMS peuvent être sauvegardés en effectuant des copies de la base de données de clés KMS_DATA, de la clé HMK KMS_HMKF et de la clé de protection de clé KMS_HKPKF.

Sous Windows, ces fichiers sont à l'emplacement suivant :

NetBackup_install_path\kms\kms\db\KMS_DATA.dat
NetBackup_install_path\Veritas\kms\key\KMS_HMKF.dat
NetBackup_install_path\Veritas\kms\key\KMS_KPKF.dat

Sous UNIX, ces fichiers sont à cet emplacement :

/usr/openv/kms/db/KMS_DATA
/usr/openv/kms/key/KMS_HMKF
/usr/openv/kms/key/KMS_KPKF

Commandes de l'interface de ligne de commande (CLI)

Les rubriques suivantes décrivent l'interface de ligne de commande (CLI) :

- Aide pour l'utilisation de l'interface de ligne de commande
  Se reporter à "Aide pour l'utilisation de l'interface de ligne de commande" à la page 554.
- Créer un groupe de clés
  Se reporter à "Créer un nouveau groupe de clés" à la page 555.
- Créer une clé
  Se reporter à "Créer une clé" à la page 555.
- Modifier les attributs du groupe de clés
  Se reporter à "Modifier les attributs du groupe de clés" à la page 556.
- Modifier les attributs de clé
  Se reporter à "Modifier les attributs de clé" à la page 556.
- Obtenir les informations des groupes de clés
  Se reporter à "Obtenir les informations des groupes de clés" à la page 557.
- Obtenir les informations des clés
  Se reporter à "Obtenir les informations des clés" à la page 558.
- Suppression d'un groupe de clés
  Se reporter à "Suppression d'un groupe de clés" à la page 558.

- Supprimer une clé
  Se reporter à "Supprimer une clé" à la page 559.
- Récupérer une clé
  Se reporter à "Récupérer une clé" à la page 559.
- Modifier la clé machine d'hôte (HMK)
  Se reporter à "Modifier la clé machine d'hôte (HMK)" à la page 564.
- Obtention de l'ID de clé machine d'hôte (HMK)
  Se reporter à "Obtention de l'ID de clé machine d'hôte (HMK)" à la page 564.
- Modifier la clé de protection de clé (KPK)
  Se reporter à "Modifier la clé de protection de clé (KPK)" à la page 565.
- Obtention de l'ID de clé de protection de clé (KPK)
  Se reporter à "Obtention de l'ID de clé de protection de clé (KPK)" à la page 564.
- Obtention des statistiques du fichier keystore
  Se reporter à "Obtention des statistiques du fichier keystore" à la page 565.
- Suspension de la base de données KMS
  Se reporter à "Suspension de la base de données KMS" à la page 565.
- Annulation de la suspension de la base de données KMS
  Se reporter à "Annulation de la suspension de la base de données KMS" à la page 566.

Aide pour l'utilisation de l'interface de ligne de commande

Pour obtenir de l'aide sur l'utilisation de l'interface de ligne de commande, utilisez la commande du service Gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

Utilisez `nbkmsutil -help -option` pour obtenir de l'aide sur une option spécifique.

```
# nbkmsutil -help
nbkmsutil [ -createkg ] [ -createkey ]
[ -modifykg ] [ -modifykey ]
[ -listkgs ] [ -listkeys ]
[ -deletekg ] [ -deletekey ]
[ -modifyhmk ] [ -modifykpk ]
[ -gethmkid ] [ -getkpkid ]
[ -quiescedb ] [ -unquiescedb ]
[ -recoverkey]
[ -export ]
[ -import ]
[ -recoverkey ]
```

```
[ -ksstats ]
[ -help ]
```

Créer un nouveau groupe de clés

Pour créer un nouveau groupe de clés, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

```
# nbkmsutil -help -createkg
nbkmsutil -createkg -kgname <key_group_name>
[ -cipher <type> ]
[ -desc <description> ]
```

Remarque : Le chiffre par défaut est AES_256.

`-kgname`	Spécifie le nom du nouveau groupe de clés (il doit être unique dans le keystore).
`-cipher`	Spécifie le type de chiffrement pris en charge par ce groupe de clés.

Créer une clé

Pour créer une nouvelle clé, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

```
# nbkmsutil -help -createkey
nbkmsutil -createkey [ -nopphrase ]
-keyname <key_name>
-kgname <key_group_name>
[ -activate ]
[ -desc <description> ]
```

Remarque : L'état de clé par défaut est prelive.

`-nopphrase`	Crée la clé sans utilise de phrase de passe. Si cette option n'est pas spécifiée, l'utilisateur est invité à saisir une phrase de passe.
`-keyname`	Spécifie le nom de la nouvelle clé (il devrait être unique dans un groupe de clés auquel elle appartient).
`-kgname`	Spécifie le nom d'un groupe de clés existant auquel la nouvelle clé doit être ajoutée.

`-activate` Configure l'état de clé sur actif (l'état de clé par défaut est prelive).

Remarque : Une valeur salt est générée lorsque vous créez une clé avec une phrase secrète. Si vous tentez de récupérer une clé, le système vous demande d'entrer une valeur salt en plus de la phrase de passe et de l'étiquette de clé.

Modifier les attributs du groupe de clés

Pour modifier les attributs d'un groupe de clés, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

```
# nbkmsutil -help -modifykg
nbkmsutil -modifykg -kgname <key_group_name>
[ -name <new_name_for_the_key_group> ]
[ -desc <new_description> ]
```

`-kgname` Spécifie le nom du groupe de clés à modifier.

`-name` Spécifie le nouveau nom du groupe de clés (il doit être unique dans le keystore).

Modifier les attributs de clé

Pour modifier les attributs de clés, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

```
# nbkmsutil -help -modifykey
nbkmsutil -modifykey -keyname <key_name>
-kgname <key_group_name>
[ -state <new_state> | -activate ]
[ -name <new_name_for_the_key> ]
[ -desc <new_description> ]
[ -move_to_kgname <key_group_name> ]
```

Remarque : Les options `-state` et `-activate` s'excluent mutuellement.

`-keyname` Spécifie le nom de la clé à modifier.

`-kgname` Spécifie le nom du groupe de clés auquel cette clé appartient.

`-name`	Spécifie le nouveau nom de la clé (il doit être unique dans le groupe de clés).
`-state`	Spécifie le nouvel état de la clé (voir la commande valide de transition d'état de clé)
`-activate`	Définit l'état de la clé sur actif.
`-desc`	Ajoute la nouvelle description à la clé.
`-move_to_kgname`	Spécifie le nom du groupe de clés vers lequel déplacer la clé.

Obtenir les informations des groupes de clés

Pour obtenir les détails de groupes de clés, utilisez la commande de service Gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

```
nbkmsutil -help -listkgs
nbkmsutil -listkgs [ -kgname <key_group_name> |
-cipher <type> |
-emptykgs |
-noactive ]
[ -noverbose ]
```

Remarque : Par défaut, tous les groupes de clés sont répertoriés. Si aucune option n'est spécifiée, les informations de tous les groupes de clés sont retournées.

`-kgname`	Spécifie le nom d'un groupe de clés.
`-cipher`	Fournit les informations de tous les groupes de clés qui prennent en charge le type spécifique de chiffre.
`-emptykgs`	Fournit les informations de tous les groupes de clés ne contenant aucune clé.
`-noactive`	Fournit les informations de tous les groupes de clés ne contenant aucune clé active.
`-noverbose`	Imprime les informations selon un certain format de formulaire (non accessible en lecture). La valeur par défaut est détaillée. La sortie est affichée sous forme explicite.

Obtenir les informations des clés

Pour obtenir les détails des clés, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

```
#nbkmsutil -help -listkeys
nbkmsutil -listkeys -all | -kgname <key_group_name>
[ -keyname <key_name> | -activekey ]
[ -noverbose | -export ]
```

`-kgname`	Spécifie le nom du groupe de clés. Les informations de toutes les clés appartenant à un groupe de clés sont retournées.
`-keyname`	Fournit les informations d'une clé spécifique qui appartient à un groupe spécifique de clés.
`-activekey`	Fournit les informations de la clé active d'un groupe spécifique de clés.
`-noverbose`	Imprime les informations selon un certain format de formulaire (non accessible en lecture). La valeur par défaut est détaillée. Le résultat s'affiche sous une forme lisible.
`-export`	Génère un résultat requis par le fichier key_file. Le fichier key_file est utilisé dans le fichier `nbkmsutil -export -path <key_container_path > -key_file`. Le résultat peut être utilisé pour un autre fichier key_file.

Suppression d'un groupe de clés

Pour supprimer un groupe de clés, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

Remarque : Seuls les groupes de clé vides peuvent être supprimés.

```
# nbkmsutil -help -deletekg
nbkmsutil -deletekg -kgname <key_group_name> -force
```

`-kgname`	Spécifie le nom du groupe de clés à supprimer. Seuls les groupes de clé vides peuvent être supprimés.
`-force`	Toutes les clés du groupe de clés sont supprimées.

Seuls les groupes de clés vides peuvent être supprimés avec l'option `-deletekg`. Vous pouvez cependant forcer la suppression du groupe de clés même si celui-ci

n'est pas vide. Exécutez la commande suivante pour forcer la suppression d'un groupe de clés :

```
# nbkmsutil -deletekg -kgname <key_group_name> -force
```

Supprimer une clé

Pour supprimer une clé, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

```
# nbkmsutil -help -deletekey
nbkmsutil -deletekey -keyname <key_name>
-kgname <key_group_name>
```

Remarque : Des clés dans l'état prelive ou terminé peuvent être supprimées.

`-keyname`	Spécifie le nom de la clé à supprimer (pour la supprimer, la clé doit être dans l'état prelive ou terminé).
`-kgname`	Spécifie le nom du groupe de clés auquel cette clé appartient.

Récupérer une clé

Pour récupérer une clé, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

```
# nbkmsutil -help -recoverkey
nbkmsutil -recoverkey -keyname <key_name>
-kgname <key_group_name>
-tag <key_tag>
[ -desc <description> ]
```

Remarque : L'état de clé sera défini sur inactif.

La restauration pourrait échouer si une clé utilisée dans le chiffrement des données de sauvegarde est perdue (et aucune copie n'est disponible). Ces clés peuvent être récupérées (recréées) lorsque les attributs de la clé d'origine (étiquette, phrase secrète et salt) sont connus.

`-keyname`	Spécifie le nom de la clé à récupérer (recréer).
`-kgname`	Spécifie le nom du groupe de clés auquel cette clé doit appartenir.

`-tag`	Spécifie l'étiquette qui identifie la clé d'origine (nous devons utiliser la même étiquette).

Remarque : L'utilisateur est invité à entrer la phrase de passe correcte pour obtenir la bonne clé (le système ne vérifie pas la validité des phrases de passe entrées).

Remarque : Chaque fois que vous récupérez une clé, le système vous demande une valeur salt. Dans cette version de KMS, une valeur salt est générée pour les clés dérivées de phrases de passe. Pour récupérer les clés générées avec une version plus ancienne de KMS, laissez vide le champ de valeur salt.

A propos de l'exportation et de l'importation de clés à partir de la base de données KMS

L'exportation et l'importation de clés permettent à l'utilisateur de synchroniser rapidement plusieurs domaines NetBackup pour utiliser le même ensemble de clés, ou de déplacer rapidement un ensemble de clés d'un domaine à un autre. Cette fonction est particulièrement utile pour une restauration sur un domaine NetBackup différent suite à une reprise après incident.

Exportation des clés

La commande `-export` permet d'exporter des clés et des groupes de clés au niveau des domaines. La liste suivante contient des informations importantes sur exportation des clés et groupes de clés :

- Les clés sont toujours exportées avec leur groupe de clés.
- Les clés et les groupes de clés sont exportés dans un conteneur (fichier) de clés chiffré sur l'hôte sur lequel l'utilitaire Service de gestion de clés KMS (`nbkmsutil`) est exécuté.

  Le conteneur de clés est protégé par une phrase secrète.

  Remarque : La même phrase secrète doit être fournie quand vous voulez importer les clés et les groupes de clés.

- Pour spécifier le contenu d'exportation, vous pouvez sélectionner des groupes de clés spécifiques ou exporter les clés que vous sélectionnez.

Utilisez la commande `-export` comme indiqué :

```
nbkmsutil -export -path <secure_key_container>
```

```
[ -key_groups <key_group_name_1 ...> | -key_file <key_file_name> ]
```

Par défaut, le keystore entier est exporté.

La commande `-path` se rapporte à un chemin d'accès entièrement qualifié où le conteneur sécurisé de clés est stocké.

La commande `-key_groups` permet de répertorier les noms de groupes de clés séparés par des espaces.

La commande `-key_file` est le chemin d'accès au fichier qui répertorie les clés à exporter dans un format spécifique.

La commande `<key_group_name>/<key_name>` permet à l'utilisateur d'exporter une sélection de clés. Vous pouvez utiliser "*" pour exporter toutes les clés d'un groupe particulier, comme illustré :

```
<key_group_name>/*
```

Vous pouvez exécuter la commande `nbkmsutil -listkeys -export` pour générer une sortie dans un format requis par cette option. Référez-vous à `nbkmsutil -listkeys -export` pour plus de détails.

Pour plus de détails au sujet des listes de clés :

Se reporter à "Liste des clés d'un groupe de clés" à la page 544.

Remarque : Les commandes `-key_groups` et `-key_file` s'excluent mutuellement.

Exécutez la commande suivante pour exporter le keystore entier :

```
nbkmsutil -export -path <secure_key_container>
```

Exécutez la commande suivante pour exporter des groupes de clés sélectionnés :

```
nbkmsutil -export -path
<secure_key_container> -key_groups
<key_group_name_1 key_group_name_2 ...>
```

Exécutez la commande suivante pour exporter une sélection de clés :

```
nbkmsutil -export -path
<secure_key_container> -key_file
<key_file_name>
```

Résolution des erreurs d'exportation courantes

Ensemble d'erreurs qui se produisent quand vous exportez les clés et groupes de clés. Cette section vous offre la solution à ces erreurs.

- L'exportation peut échouer quand le conteneur de clés que vous spécifiez existe déjà sur l'hôte.
  Spécifiez un autre fichier de conteneur de clés et réexécutez l'opération d'exportation.
- L'exportation échoue également quand vous mentionnez des clés ou des noms de groupes de clés incorrects.
  Vous devez corriger les clés ou les noms de groupes de clés et les exporter de nouveau.

Importer des clés

La commande `-import` aide à importer des clés et des groupes de clés à travers des domaines. La liste suivante contient des informations importantes sur l'importation des clés et des groupes de clés :

- Lors de l'importation des clés et des groupes de clés, vous devez avoir le fichier de conteneur de clés qui est créé pendant l'opération d'exportation. Vous avez besoin également de la même phrase secrète qui est utilisée pendant l'exportation.
- L'importation des clés est une opération atomique. Elle annule toutes les mises à jour si une erreur se produit lors de l'opération.
- L'importation partielle n'est pas prise en charge.
- Un aperçu de la sortie d'importation est disponible. Exécutez la commande `-preview` pour afficher les résultats de l'importation.
- L'opération d'importation peut avoir deux modes, un qui inclut la commande `-preserve_kgname` et un autre qui exclut la commande `-preserve_kgname`.
  Par défaut, les groupes de clés sont importés avec le format de nom suivant :
  `< Original_Kgname_<timestamp> >`
  Vous pouvez choisir de conserver le nom du groupe de clés en spécifiant explicitement l'option `<-preserve_kgname>`.
- Les clés en double telles que les clés avec la même étiquette de clé ou la même clé ne sont pas importées.
- L'importation ne prend pas en charge la fusion de groupes de clés.

Vous pouvez cependant fusionner les clés, importer le groupe de clés sans utiliser la commande `<-preserve_kgname>`. Exécutez la commande `nbkmsutil -modifykey -keyname <key_name> -kgname <key_group_name>` afin de déplacer la clé du groupe actuel vers le groupe requis.

Pour plus d'informations sur le déplacement des clés, voir :

Se reporter à "Modifier les attributs de clé" à la page 556.

Si les mêmes clés ou les clés qui ont les mêmes indicateurs de clé existent dans un groupe de clés, elles sont ignorées pendant l'importation. Exécutez les commandes suivantes afin d'importer les clés et les groupes de clés :

```
# nbkmsutil -import -path <secure_key_container>

[-preserve_kgname]

[ -desc <description> ]

[ -preview ]
```

La commande `-preserve_kgname` conserve les noms de groupe de clés pendant l'importation.

La commande `-desc <description>` est une description qui est associée aux groupes de clés pendant l'importation.

La commande `-preview` affiche un aperçu des résultats de l'importation.

Exécutez l'opération d'importation avec la commande `-preserve_kgname` comme suit :

```
nbkmsutil -import -path

<secure_key_container>

[-preserve_kgname]
```

Quand vous exécutez la commande `-import` avec la commande `-preserve_kgname`, l'opération d'importation essaye d'importer les noms de groupes de clés d'origine depuis le conteneur de clés. Si un groupe de clés avec le même nom existe, l'opération d'importation échoue.

Exécutez l'opération d'importation sans la commande `-preserve_kgname` comme suit :

```
nbkmsutil -import -path

<secure_key_container>
```

Quand vous exécutez la commande `-import` sans `-preserve_kgname`, elle importe les groupes de clés, mais les groupes de clés sont renommés à l'aide d'un suffixe, par exemple un horodatage. Chaque groupe de clés renommé conserve un nom unique.

Résolution des erreurs d'importation courantes

Ensemble d'erreurs qui se produisent quand vous importez les clés et groupes de clés. Cette section vous offre la solution à ces erreurs.

- Pendant une importation, quand vous importez des groupes de clés avec l'option `[-preserve_kgname ]` et si ce groupe existe déjà dans KMS, l'opération entière échoue.
  Vous devez supprimer ou renommer les groupes de clés existants ou exclure l'option [`[-preserve_kgname ]`] et réexécuter l'opération d'importation.
- KMS NetBackup a une limite de 100 groupes de clés. Chaque groupe a une limite de 30 clés. L'opération échoue si plus de 100 groupes de clés sont importés.
  Vous devez supprimer les groupes de clés indésirables existants et réexécuter l'opération d'importation.

Modifier la clé machine d'hôte (HMK)

Pour modifier la clé machine d'hôte, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

La HMK est utilisée pour chiffrer le keystore. Pour modifier le HMK actuel, l'utilisateur devrait fournir une graine ou une phrase de passe facultative. Un ID (ID de HMK) pouvant nous rappeler la phrase de passe spécifiée peut également être fourni. La phrase de passe et l'ID de HMK sont lus en mode interactif.

```
# nbkmsutil -help -modifyhmk
nbkmsutil -modifyhmk [ -nopphrase ]
```

Obtention de l'ID de clé machine d'hôte (HMK)

Pour obtenir l'ID de HMK, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus. L'ID de HMK est alors retourné.

```
# nbkmsutil -help -gethmkid
nbkmsutil -gethmkid
```

Obtention de l'ID de clé de protection de clé (KPK)

Pour obtenir l'ID de KPK, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus. La commande renvoie l'ID de KPK actuel.

```
# nbkmsutil -help -getkpkid
nbkmsutil -getkpkid
```

Modifier la clé de protection de clé (KPK)

Pour modifier la clé de protection de clé, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

La KPK est utilisée pour chiffrer les clés de KMS. Actuellement, la KPK est par keystore. Pour modifier la clé KPK actuelle, l'utilisateur doit fournir une valeur de départ ou une phrase de passe facultative. Fournissez également un ID (ID du KPK) qui peut nous rappeler la phrase de passe spécifiée. La phrase de passe et l'ID du KPK sont lus en mode interactif.

```
# nbkmsutil -help -modifykpk
nbkmsutil -modifykpk [ -nopphrase ]
```

Obtention des statistiques du fichier keystore

Pour obtenir les statistiques de keystore, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

Cette commande renvoie les statistiques suivantes de keystore :

- Nombre total de groupes de clés
- Nombre total de clés
- Appels de suspension en attente

```
# nbkmsutil -help -ksstats
nbkmsutil -ksstats [ -noverbose ]
```

Suspension de la base de données KMS

Pour suspendre la base de données KMS, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

Cette commande envoie la demande de suspension au KMS. Si la commande réussit, le nombre actuel de suspensions en attente qui est retourné comme tâches de sauvegarde multiples pourrait suspendre la base de données de KMS.

```
# nbkmsutil -help -quiescedb
nbkmsutil -quiescedb
```

Annulation de la suspension de la base de données KMS

Pour annuler la suspension de la base de données KMS, utilisez la commande de service de gestion des clés (KMS) NetBackup (commande `nbkmsutil`) avec les arguments inclus.

Cette commande envoie une demande de réactivation au KMS. Si la commande aboutit, le nombre de suspensions actuel en attente est retourné. Un compte égale à zéro (0) signifie que la base de données KMS est entièrement réactivée.

```
# nbkmsutil -help -unquiescedb
nbkmsutil -unquiescedb
```

Options de création de clé

L'utilisation de la fonction de KMS de NetBackup devrait inclure la création d'une sauvegarde des répertoires `kms/db` et `kms/key`. Les clés de protection et la base de données de clés existent dans deux sous-répertoires distincts pour faciliter leur segmentation lors de la création d'une copie de sauvegarde.

Remarque : En raison de leur petite taille, du fait qu'ils changent rarement et qu'ils ne doivent pas être inclus sur aucune bande de NetBackup chiffrée, les fichiers devrait être manuellement copiés sur des médias de sauvegarde.

Remarque : L'approche recommandée pour créer des clés avec cette version de KMS est de toujours créer des clés à partir de phrases de passe. Ceci est valable pour les deux clés de protection (clé machine d'hôte et clé de protection de clé) et les clés de chiffrement des données associées aux enregistrements de clé. Il est recommandé d'enregistrer les phrases de passe utilisés pour créer les clés et de les stocker à des fins de récupération.

Bien que cette utilisation permettant au système de KMS de générer aléatoirement les clés de chiffrement soit une meilleure solution, elle ne peut pas effectuer de récupération de la perte ou de la corruption de toutes les copies de clés de protection et de keystore, et par conséquent n'est pas recommandée.

Dépannage du KMS

Utilisez la procédure suivante pour démarrer le dépannage du KMS.

Démarrer le dépannage du KMS

1. Déterminez le code d'erreur et la description.
2. Déterminez si le KMS est en cours d'exécution et vérifiez que les fichiers de données de KMS suivants existent :

   ```
   kms/db/KMS_DATA
   kms/key/KMS_HMKF
   kms/key/KMS_KPKF
   ```

   Si les fichiers n'existent pas, alors le KMS n'a pas été configuré ou la configuration a été supprimée. Découvrez ce qui est arrivé aux fichiers s'ils n'existent pas. Si le KMS n'a pas été configuré, le service `nbkms` n'est pas en cours d'exécution. Si le service KMS n'est pas en cours d'exécution ou n'est pas configuré, cela n'affecte pas l'opération de NetBackup. Si vous avez précédemment utilisé le préfixe `ENCR_`pour un nom de pool de volumes, ce nom doit être modifié car `ENCR_` a maintenant une signification spéciale pour NetBackup.
3. Obtenez les informations de configuration de KMS :

   Obtenez une liste de groupe de clés en exécutant la commande `nbkmsutil -listkgs`. Obtenez une liste de toutes les clés pour un groupe de clés en exécutant la commande `nbkmsutil -listkeys -kgname` *`key_group_name`*.
4. Obtenez les informations des journaux opérationnels tels que des journaux de KMS par des journaux d'identificateur d'objet 286 VxUL et BPTM.
5. Evaluez les informations des journaux. Les erreurs de KMS sont remises au BPTM.
6. Evaluez les erreurs de KMS enregistrées dans le journal de KMS.

Solution pour des sauvegardes n'effectuant pas de chiffrement

Si des sauvegardes de bande ne sont pas chiffrées, considérez les solutions suivantes :

- Vérifiez qu'une sauvegarde n'est pas chiffrée en vérifiant que le champ de l'étiquette de clé de chiffrement n'est pas défini dans l'enregistrement d'image.
- Vérifiez que les noms du groupe de clés et du pool de volumes correspondent.
- Vérifiez qu'il existe un enregistrement de clé dans le groupe de clés avec un état actif.

Vérifiez les autres options ne configurant pas le KMS :

- Vérifiez que tout les éléments associés à la gestion traditionnelle de médias sont correctement configurés.
- Vérifiez que la politique NetBackup extraie une bande du bon pool de volumes.
- Vérifiez que le lecteur de bande capable de chiffrement ait à sa disposition un média capable de chiffrement. Par exemple, le média LTO4 est-il installé sur le lecteur de bande LTO4 ?

Solution pour les restaurations n'effectuant pas de déchiffrement

Si les restaurations de bandes chiffrées ne déchiffrent pas, considérez les solutions suivantes :

- Vérifiez que l'image de sauvegarde initiale a été chiffrée pour commencer en affichant le champ d'étiquette de clé de chiffrement dans l'enregistrement d'image.
- Vérifiez que l'enregistrement de clé avec le même champ d'étiquette de clé de chiffrement se trouve dans un état d'enregistrement qui prend en charge les restaurations. Ces états sont actif et inactif.
- Si l'enregistrement de clé n'est pas dans le bon état, replacez la clé dans l'état inactif.

D'autres options ne configurant pas le KMS d'Autre à prendre en considération :

- Vérifiez que le lecteur et le média prennent en charge le chiffrement.
- Le média chiffré en cours de lecture est-il dans un lecteur de bande capable de chiffrer ?

Exemple de dépannage - sauvegarde avec aucun enregistrement de clé active

L'exemple suivant affiche ce qui se produit lorsque vous tentez une sauvegarde quand il n'existe aucun enregistrement de clé active.

Figure 20-5 affiche une liste d'enregistrements de clés. Trois d'entre eux ont le groupe de clés `ENCR_mygroup` et le même nom de pool de volumes. Un groupe de clés nommé `Q2_2008_key` était actif. A la fin de la séquence de commande, l'état du groupe de clés `Q2_2008_key` est défini sur inactif.

Figure 20-5 Liste des enregistrements de clés

```
fel (root) [385]: nbkmsutil -listkeys -kgname ENCR_mygroup
Key Group Name        : ENCR_mygroup
Supported Cipher      : AES_256
Number of Keys        : 3
Has Active Key        : Yes
Creation Time         : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description           : -
  Key Tag    : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name              : Q2_2008_key
  Current State         : Active
  Creation Time         : Sat Mar 15 11:02:46 2008
  Last Modification Time: Sat Mar 15 11:02:46 2008
  Description           : key for Apr, May, & Jun
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name              : Q1_2008_key
  Current State         : Inactive
  Creation Time         : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description           : Key for Jan, Feb, & March
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name              : test
  Current State         : Inactive
  Creation Time         : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description           : -
Number of Keys: 3
fel (root) [383]: nbkmsutil -modifykey -keyname Q2_2008_key -kgname ENCR_mygroup -state
Inactive
Key details are updated successfully
```

Figure 20-6 affiche la liste des enregistrements de clés qui sont produits de nouveau et vous pouvez voir que l'état de `Q2_2008_key` est maintenant répertorié comme inactif.

Figure 20-6 Liste des enregistrements de clés avec le groupe de clés actives modifié

```
fel (root) [384]: nbkmsutil -listkeys -kgname ENCR_mygroup
Key Group Name         : ENCR_mygroup
Supported Cipher       : AES_256
Number of Keys         : 3
Has Active Key         : No
Creation Time          : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description            : -
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name               : Q1_2008_key
  Current State          : Inactive
  Creation Time          : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description            : Key for Jan, Feb, & March
  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name               : test
  Current State          : Inactive
  Creation Time          : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description            : -
  Key Tag    : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name               : Q2_2008_key
  Current State          : Inactive
  Creation Time          : Sat Mar 15 11:02:46 2008
  Last Modification Time: Mon Mar 17 13:53:33 2008
  Description            : key for Apr, May, & Jun

Number of Keys: 3
```

Sans clé active, qu'arrive-t-il à la sauvegarde ?

Figure 20-7 affiche la sortie du journal de BPTM. Elle consigne le message du code d'erreur 1227 dans le journal de BPTM.

Figure 20-7 Sortie de la commande `bptm`

```
14:29:16.381 [19978] <2> manage_drive_attributes: MediaPool [ENCR_mygroup], MediaLabel [MEDIA=JRO111;]
14:29:16.384 [19978] <2> manage_drive_attributes: encryption status: nexus scope 0, key scope 0
14:29:16.384 [19978] <2> manage_drive_attributes: encryp mode 0x0, decryp mode 0x0, algorithm index 0, key instance
0
14:29:16.384 [19978] <2> KMSCLIB::kmsGetKeyAndKad: Entering function....(KMSClib.cpp:583)
14:29:16.384 [19978] <2> KMSCLIB::GetQueryableFacetInstance: Entering function....(KMSClib.cpp:207)
14:29:16.384 [19978] <2> KMSCLIB::InitOrb: Entering function....(KMSClib.cpp:158)
14:29:16.385 [19978] <2> Orb::init: Created anon service name: NB_19978_1536015948517350(Orb.cpp:600)
14:29:16.385 [19978] <2> Orb::init: endpointvalue is : pbxiop://1556:NB_19978_1536015948517350(Orb.cpp:618)
14:29:16.385 [19978] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-
ORBDottedDecimalAddresses 0" -ORBSvcConfDirective "static PBXIOP_Factory ''" -ORBSvcConfDirective "static
EndpointSelectorFactory ''" -ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory PBXIOP_Factory'" -
ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory IIOP_Factory'" -ORBSvcConfDirective "static
PBXIOP_Evaluator_Factory '-orb kmslib'" -ORBSvcConfDirective "static Resource_Factory '-ORBConnectionCacheMax 1024
'" -ORBEndpoint pbxiop://1556:NB_19978_1536015948517350 -ORBSvcConf /dev/null -ORBSvcConfDirective "static
Server_Strategy_Factory '-ORBMaxRecvGIOPPayloadSize 268435456'"(Orb.cpp:725)
14:29:16.406 [19978] <2> vnet_cached_gethostbyname: vnet_hosts.c.307: found host in cache: felix.min.veritas.com
14:29:16.406 [19978] <2> vnet_cached_gethostbyaddr_rnl: vnet_hosts.c.506: found IP in cache: 127.0.0.1
14:29:16.460 [19978] <2> db_error_add_to_file: dberrorq.c:midnite = 1205730000
14:29:16.461 [19978] <16> get_encryption_key: NBKMS failed with error status: Key group does not have an active key
(1227)
14:29:16.462 [19978] <2> send_MDS_msg: MEDIADB 1 42 JRO111 4000007 *NULL* 6 1205781805 1205782033 1206991633 0 64 2
2 1 4 0 8193 1024 0 8 0
```

La boîte de dialogue Détails du travail affiche l'état détaillé. Vous pouvez consulter un message indiquant ce qui a échoué et l'état détaillé. Avec les informations du diagnostic précédent, vous pouvez déterminer le problème particulier ou identifier à quoi un problème donné est associé.

Exemple de dépannage - restauration avec un état d'enregistrement de clé inexact

L'exemple suivant indique une restauration avec un enregistrement de clé dans un état inexact.

Figure 20-8 indique qu'un enregistrement requis est défini sur désapprouvé. Ce qui suit indique la liste. La même commande est utilisée pour passer de l'état inactif à désapprouvé.

Figure 20-8 Liste des enregistrements de clés avec le groupe de clés désapprouvées

```
fel (root) [426]: !385
nbkmsutil -listkeys -kgname ENCR_mygroup

Key Group Name        : ENCR_mygroup
Supported Cipher      : AES_256
Number of Keys        : 3
Has Active Key        : No
Creation Time         : Sat Mar 15 10:45:55 2008
Last Modification Time: Sat Mar 15 10:45:55 2008
Description           : -

  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe90
  Key Name              : Q1_2008_key
  Current State         : Inactive
  Creation Time         : Sat Mar 15 10:46:51 2008
  Last Modification Time: Sat Mar 15 10:46:51 2008
  Description           : Key for Jan, Feb, & March

  Key Tag    : d5a2a3df1a32eb61aff9e269ec777b5b9092839c6a75fa17bc2565f725aafe91
  Key Name              : test
  Current State         : Inactive
  Creation Time         : Sat Mar 15 13:12:25 2008
  Last Modification Time: Sat Mar 15 13:12:25 2008
  Description           : -

  Key Tag    : cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d
  Key Name              : Q2_2008_key
  Current State         : Deprecated
  Creation Time         : Sat Mar 15 11:02:46 2008
  Last Modification Time: Mon Mar 17 14:52:59 2008
  Description           : key for Apr, May, & Jun

Number of Keys: 3
```

Figure 20-9 affiche le journal de `bptm` avec l'erreur 1242 retournée.

Figure 20-9 Sortie de journal de `bptm` avec l'erreur 1242

```
14:53:48.782 [21109] <2> io_read_back_header: drive index 0, reading backup header
14:53:48.791 [21109] <2> io_position_for_read: successfully positioned JRO111 to file number 3
14:53:48.796 [21109] <2> io_position_for_read: next block encryption status: LON 0x0000000000000009, algorithm
index 1, encryption status 0x6
14:53:48.796 [21109] <2> io_position_for_read: Kad type 0x0, kad length 32 Kad
[cf7ac430d8795a9b39e703821371ed10be6ec80eab72d89aef6f8a791fc2460d]
14:53:48.796 [21109] <2> KMSCLIB::kmsGetKeyAndKadByKeyTag: Entering function....(KMSClib.cpp:655)
14:53:48.796 [21109] <2> KMSCLIB::GetQueryableFacetInstance: Entering function....(KMSClib.cpp:207)
14:53:48.796 [21109] <2> KMSCLIB::InitOrb: Entering function....(KMSClib.cpp:158)
14:53:48.797 [21109] <2> Orb::init: Created anon service name: NB_21109_1537488329610200(Orb.cpp:600)
14:53:48.798 [21109] <2> Orb::init: endpointvalue is : pbxiop://1556:NB_21109_1537488329610200(Orb.cpp:618)
14:53:48.798 [21109] <2> Orb::init: initializing ORB kmslib with: kmslib -ORBSvcConfDirective "-
ORBDottedDecimalAddresses 0" -ORBSvcConfDirective "static PBXIOP_Factory ''" -ORBSvcConfDirective "static
EndpointSelectorFactory ''" -ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory PBXIOP_Factory'" -
ORBSvcConfDirective "static Resource_Factory '-ORBProtocolFactory IIOP_Factory'" -ORBSvcConfDirective "static
PBXIOP_Evaluator_Factory '-orb kmslib'" -ORBSvcConfDirective "static Resource_Factory '-ORBConnectionCacheMax 1024
'" -ORBEndpoint pbxiop://1556:NB_21109_1537488329610200 -ORBSvcConf /dev/null -ORBSvcConfDirective "static
Server_Strategy_Factory '-ORBMaxRecvGIOPPayloadSize 268435456'"(Orb.cpp:725)
14:53:48.818 [21109] <2> vnet_cached_gethostbyname: vnet_hosts.c.307: found host in cache: felix.min.veritas.com
14:53:48.818 [21109] <2> vnet_cached_gethostbyaddr_rnl: vnet_hosts.c.506: found IP in cache: 127.0.0.1
14:53:48.842 [21109] <2> db_error_add_to_file: dberrorq.c:midnite = 1205730000
14:53:48.844 [21109] <16> get_encryption_key: NBKMS failed with error status: Operation not allowed for key record
in this state (1242)
```

Chapitre 21

Service Gestion des clés externe

Ce chapitre traite des sujets suivants :

À propos du KMS externe

La prise en charge du KMS externe offre une alternative au service de gestion des clés NetBackup (KMS) pour les clés de chiffrement de données au repos.

Les images de sauvegarde stockées sur des configurations de stockage telles que le stockage sur bande, en cloud, MSDP et AdvancedDisk peuvent être chiffrées à l'aide des clés gérées par le serveur KMS externe.

NetBackup prend en charge la communication avec le KMS externe via le protocole d'interopérabilité de gestion de clés (KMIP).

Consultez la NetBackupListe de compatibilité pour les versions de KMIP prises en charge par NetBackup.

NetBackup prend en charge l'authentification avec le serveur KMS externe à l'aide des certificats de sécurité. Lors de chaque opération, NetBackup présente le certificat au KMS externe et demande à effectuer l'opération requise. Le KMS externe valide le certificat et exécute cette opération si l'utilisateur dispose des autorisations requises.

Pour plus d'informations, consultez la vidéo sur la *prise en charge du KMS externe dans NetBackup*.

Configuration des certificats et autorisations

Avant de configurer un certificat à utiliser avec NetBackup, vous devez effectuer certaines configurations sur le serveur KMS externe pour vous assurer que NetBackup dispose des autorisations requises pour effectuer des opérations spécifiques aux clés. Les étapes de configuration peuvent varier selon les solutions de KMS externe.

Assurez-vous de remplir les conditions suivantes :

- Une entité (utilisateur) est créée dans le KMS externe qui représente le serveur maître NetBackup.
- L'hôte du serveur maître dispose d'un certificat approuvé par le serveur KMS externe.
- Le nom commun du certificat est associé à l'entité qui représente le serveur maître.

Workflow pour configurer le KMS externe

Pour l'intégration du KMS externe, la configuration centralisée sur le serveur maître NetBackup est utilisée. Le serveur maître doit établir une connexion sortante vers

le port KMIP du serveur KMS externe. Configurez le canal de communication avec le KMS externe sur le serveur maître à l'aide des informations d'authentification. Le serveur maître envoie alors toutes les demandes aux serveurs KMS externes pour le compte d'autres serveurs tels que les serveurs de médias.

Tableau 21-1 Workflow pour configurer un KMS

Numéro d'étape	Étape	Rubrique de référence
Étape 1	Validation des informations d'authentification du KMS	Se reporter à "Validation des informations d'authentification du KMS" à la page 575.
Étape 2	Configuration des informations d'authentification du KMS	Se reporter à "Configuration des informations d'authentification du KMS" à la page 578.
Étape 3	Configuration du KMS	Se reporter à "Configuration du KMS" à la page 579.
Étape 4	Création des clés	Se reporter à "Création de clés dans un KMS externe" à la page 582.
Étape 5	Configuration du stockage	Pour plus d'informations, consultez le Guide de l'administrateur NetBackup, volume I.
Étape 6	Configuration de la politique	Pour plus d'informations, consultez le Guide de l'administrateur NetBackup, volume I.

Validation des informations d'authentification du KMS

Si des informations d'authentification incorrectes sont configurées dans NetBackup, la communication avec le serveur KMS externe peut échouer. Pour éviter cela, vous pouvez effectuer certaines validations avant qu'une information d'authentification puisse être configurée pour être utilisée par le KMS. Si une validation échoue, l'information d'authentification ne peut pas être configurée.

Les validations suivantes sont effectuées lors de la configuration d'une nouvelle information d'authentification ou de la mise à jour d'une information d'authentification existante. Il n'est pas recommandé de configurer des informations d'authentification si l'une des validations échoue :

- Le chemin d'accès au certificat est valide.
- Le chemin d'accès au magasin d'approbation est valide.
- Le chemin d'accès à la clé privée est valide.

- Les certificats de la chaîne de certificats sont lisibles.
- Les certificats du magasin d'approbation sont lisibles.
- La clé privée est lisible.
- Le champ Nom commun n'est pas vide.
- Le certificat n'a pas expiré.
- Le certificat est en cours de validité.
- La clé privée correspond au certificat.
- Les certificats sont dans l'ordre approprié.
- Les validations suivantes de la liste de révocation des certifications (CRL) sont effectuées si `ECA_CRL_PATH` est configuré et si le niveau de vérification de la liste CRL est différent de DISABLE :
  - Le répertoire de la liste CRL comprend des fichiers de liste CRL.
  - Le niveau de vérification de la liste CRL est valide.
  - Le chemin d'accès à la liste CRL est valide.
  - Les listes CRL disponibles sont lisibles.

Pour valider les informations d'authentification du KMS et vérifier la compatibilité avec le KMS

1. Exécutez la commande suivante :

   ```
   nbkmiputil -kmsServer kms_server_name -port port
   -certPathcert_path -privateKeyPath private_key_path
   -trustStorePathtrust_store_path -validate
   ```

   La commande `nbkmiputil` valide la fonctionnalité KMS, y compris la connexion au serveur KMS.

   Elle teste également des opérations telles que le répertoriage et la récupération de clés, ainsi que la définition et la récupération d'attributs. Pour définir des attributs, vous devez disposer d'une autorisation d'écriture pour le serveur KMS. La commande `nbkmiputil` valide également la signature de l'autorité de certification sur le certificat de serveur qui est échangé par le biais du protocole TLS. `nbkmiputil` utilise le protocole TLS 1.2 et un protocole ultérieur pour la communication sécurisée avec le serveur KMS externe.

2. (Cette étape est facultative.) Si le fournisseur du KMS n'est pas répertorié en tant que fournisseur de KMS pris en charge dans la liste de compatibilité matérielle NetBackup, et si vous souhaitez vérifier la compatibilité du fournisseur avec NetBackup, utilisez la commande suivante :

   L'exécution de cette commande nécessite que vous disposiez des privilèges d'écriture pour le serveur KMS externe. La commande crée huit clés symétriques sur le serveur KMS externe et exécute diverses opérations KMIP pour vérifier la compatibilité. Une fois la compatibilité vérifiée, vous devez explicitement supprimer les clés qui sont créées.

3. Vérifiez que le serveur maître NetBackup est compatible avec le fournisseur du KMS et qu'il peut communiquer avec ce dernier à l'aide du protocole KMIP. Exécutez la commande suivante :

   ```
   nbkmiputil -kmsServer kms_server_name -port port
   -certPathcert_path -privateKeyPath private_key_path
   -truststorepathtrust_store_path -ekmsCheckCompat
   ```

   Il est recommandé d'exécuter l'option `-ekmsCheckCompat` pour vérifier si vous pouvez configurer le service KMS dans votre environnement.

   Cette option crée huit clés de test sur le serveur KMS spécifié, que vous pourrez supprimer manuellement par la suite.

4. Si une validation échoue, contactez le Support technique de Veritas.

Configuration des informations d'authentification du KMS

Pour configurer le KMS externe dans NetBackup, vous devez d'abord configurer les informations d'authentification utilisées par NetBackup pour authentifier le serveur KMS externe. Lors de cette étape, vous devez spécifier le chemin d'accès aux artefacts de l'infrastructure à clés publiques (PKI) requis pour l'authentification basée sur les certificats. Les informations suivantes sont requises :

- Chemin d'accès au fichier du certificat
- Chemin d'accès au fichier de magasin de clés
- Chemin d'accès au fichier du magasin d'approbation
- Chemin d'accès à la phrase secrète ou au fichier de la phrase secrète

---

Remarque : Après la mise à jour de la configuration ou des clés du KMS externe, l'utilisation de la clé appropriée dans le workflow de sauvegarde ou de restauration par NetBackup peut prendre un certain temps. En effet, NetBackup met en cache la clé pendant 10 minutes (pour le KMS externe). Pour utiliser immédiatement une clé, il est possible d'effacer le cache en exécutant la commande suivante sur le serveur de médias correspondant :

```
bpclntcmd -clear_host_cache
```

Pour configurer les informations d'authentification du KMS

- Exécutez la commande suivante :

  ```
  nbkmscmd -configureCredential -credName credential_name -certPath
  certificate_file_path -privateKeyPath private_key_file_path
  -trustStorePath CA_certificate_file_path [-passphrasePath
  private_key_passphrase_file_path] [-crlCheckLevel LEAF | CHAIN |
  DISABLE] [-server master_server_name] [-description description]
  ```

Répertoriage des informations d'authentification du KMS

Pour répertorier toutes les informations d'authentification

- Exécutez la commande suivante :

  ```
  nbkmscmd -listCredential
  ```

Pour répertorier des informations d'authentification spécifiques

- Exécutez la commande suivante :

```
nbkmscmd -listCredential -credName credential_name
```

Mise à jour des informations d'authentification du KMS

Pour mettre à jour les informations d'authentification

- Exécutez la commande suivante :

  ```
  nbkmscmd -updateCredential -credName credential_name -certPath
  certificate_file_path -privatekeyPath private_key_file_path
  -trustStorePath CA_certificate_file_path -crlCheckLevel DISABLE
  ```

Suppression des informations d'authentification du KMS

Pour supprimer les informations d'authentification

- Exécutez la commande suivante :

  ```
  nbkmscmd -deleteCredential -credName credential_name
  ```

Configuration du KMS

Pour configurer le KMS NetBackup (NBKMS)

- Exécutez la commande suivante :

  ```
  nbkmscmd -configureKMS -name configuration_name -type NBKMS -hmkId
  host_master_key_ID_to_identify_HMK_passphrase -kpkId
  key_protection_key_ID_to_identify_KPK_passphrase
  [-useRandomPassphrase 0 | 1] [-enabledForBackup 0 | 1] [-priority
  priority_of_KMS_server] [-server master_server_name] [-description
  description]
  ```

Pour configurer le KMS externe :

- Exécutez la commande suivante :

  ```
  nbkmscmd -configureKMS -name configuration_name -type KMIP -port
  port_to_connect_to_external_KMS_server -kmsServerName
  network_name_of_external_KMS_server -credId credential_ID |
  -credName credential_name [-enabledForBackup 0 | 1] [-priority
  priority_of_KMS_server] [-server master_server_name] [-description
  description]
  ```

Répertoriage des configurations du KMS

Pour répertorier les détails de configuration de tous les serveurs KMS

- Exécutez la commande suivante :

  ```
  nbkmscmd -listKMSConfig
  ```

Pour répertorier les détails de configuration d'un serveur KMS spécifique

- Exécutez la commande suivante :

  ```
  nbkmscmd -listKMSConfig -name configuration_name
  ```

Mise à jour de la configuration du KMS

Mise à jour de la priorité d'un KMS

Pour mettre à jour la priorité du KMS, exécutez la commande suivante : `nbkmscmd -updateKMSConfig -name configuration_name -priority priority`

Désactivation d'une configuration du KMS pour la sauvegarde

Pour désactiver les clés du KMS spécifié à utiliser pour la sauvegarde, exécutez la commande suivante : `nbkmscmd -updateKMSConfig -name configuration_name -enabledForBackup 0`

Remarque : Après toute mise à jour de la configuration ou des clés du KMS externe, l'utilisation de la clé appropriée dans le workflow de sauvegarde ou de restauration par NetBackup peut prendre un certain temps. En effet, NetBackup met en cache la clé pendant 10 minutes (pour le KMS externe). Pour utiliser immédiatement une clé, il est possible d'effacer le cache en exécutant la commande suivante sur le serveur de médias correspondant :

```
bpclntcmd -clear_host_cache
```

Suppression de la configuration du KMS

Pour supprimer la configuration du KMS, exécutez la commande suivante : `nbkmscmd -deleteKMSConfig -name configuration_name`

Configuration des clés dans un KMS externe pour une utilisation par NetBackup

NetBackup peut utiliser les clés déjà créées dans un KMS externe, ou vous pouvez créer des clés dans un KMS externe à l'aide de NetBackup, pour lequel le serveur maître NetBackup doit être autorisé à créer des clés.

NetBackup peut découvrir les clés créées dans un KMS externe pour une utilisation par NetBackup. Spécifiez les attributs personnalisés `x-application` et `x-keygroup` lors de la génération des clés ou associez ces attributs aux clés existantes afin que NetBackup puisse déterminer les clés à utiliser. NetBackup utilise n'importe quelle clé possédant ces attributs pour le chiffrement.

Le nom du groupe de clés pour le pool de volumes de bande doit être préfixé de `ENCR_`.

Prenez l'exemple suivant : vous avez configuré un pool de volumes de bande avec le nom `ENCR_P1`. Le nom du pool de volumes indique que les images de sauvegarde dans ce pool de volumes sont chiffrées.

`x-keygroup` est sensible à la casse et doit correspondre exactement au nom du pool de volumes.

Pour configurer des clés

1. Créez une clé dans un KMS externe avec l'attribut personnalisé `x-keygroup` et en définissant sa valeur sur `ENCR_P1`.
2. Définissez l'attribut personnalisé `x-application` en définissant sa valeur sur `NetBackup` pour indiquer que cette clé appartient à NetBackup.
3. Pour les clés déjà créées et devant être utilisées pour le chiffrement de ce pool de volumes, vous pouvez créer les attributs personnalisés.
4. Pour définir ces attributs, vous pouvez utiliser l'interface utilisateur spécifiée par le fournisseur de KMS correspondant.

   Si l'interface utilisateur du fournisseur du KMS ne prend pas en charge l'ajout et la définition d'attributs personnalisés, vous pouvez utiliser la commande `nbkmiputil` pour définir les attributs pour les clés.

   ```
   nbkmiputil -kmsServer kms_server_name -port 5696 -certPath
   cert_path -privateKeyPath private_key_path -trustStorePath
   caCertificatePath -setAttribute -attributeName attributeName
   -attributeValue attributeVal
   ```

   Pour plus d'informations sur la commande, consultez le Guide de référence des commandes NetBackup.

Création de clés dans un KMS externe

Vous pouvez utiliser NetBackup pour créer des clés dans un KMS externe. NetBackup doit disposer des autorisations requises pour créer des clés dans le KMS externe.

Pour créer des clés dans un KMS externe

- Exécutez la commande suivante :

  `nbkmscmd -createkey -name` *`configuration_name`* `-keyGroupName` *`keygroup_name`* `-keyName` *`key_name`* `-comment` *`comments`*

  La commande `createKey` crée une clé active. Pour le KMS externe, plusieurs clés peuvent être actives dans un groupe de clés. NetBackup utilise la clé active la plus récente. La commande définit également tous les attributs requis pour la clé.

  Remarque : Après toute mise à jour de la configuration ou des clés du KMS externe, l'utilisation de la clé appropriée dans le workflow de sauvegarde ou de restauration par NetBackup peut prendre un certain temps. En effet, NetBackup met en cache la clé pendant 10 minutes (pour le KMS externe). Pour utiliser immédiatement la clé, exécutez la commande suivante sur le serveur de médias correspondant pour effacer le cache :

  `bpclntcmd -clear_host_cache.`

Répertoriage des clés

Utilisez la procédure donnée pour répertorier les ID de clés du KMS spécifié.

Pour répertorier les ID de clés

- `nbkmscmd -listKeys -name` *`configuration_name`*

Détermination d'un nom de groupe de clés lors de la configuration du stockage

NetBackup utilise les clés préconfigurées d'un KMS externe lors de la configuration du stockage.

Assurez-vous que les clés sont créées dans un serveur KMS externe avec l'attribut `x-keygroup` et attribuées à un nom de groupe de clés.

Pour chaque configuration de stockage, NetBackup détermine le nom du groupe de clés comme suit :

MSDP	Spécifier le nom du groupe de clés
Cloud	Le nom du groupe de clés est *Name_of_storage_server*:*Name_of_disk_volume*
Bandes	Le nom du pool de volumes est utilisé comme nom de groupe de clés Pour le stockage sur bande, le nom du pool de volumes doit être préfixé de `ENCR`.
AdvancedDisk	Pour UNIX : *Name_of_storage_server*:*Name_of_disk_volume* Pour Windows : *Name_of_storage_server*

Utilisation de plusieurs serveurs KMS

NetBackup prend en charge plusieurs serveurs KMS. Vous pouvez utiliser plusieurs serveurs KMS et migrer d'un serveur KMS vers un autre. Vous pouvez également utiliser un serveur KMS distinct pour chaque configuration de stockage telle que le stockage sur bande, le stockage en cloud et le stockage MSDP.

Se reporter à "Migration d'un serveur KMS vers un autre serveur KMS" à la page 584.

Se reporter à "Utilisation d'un serveur KMS distinct pour chaque configuration de stockage" à la page 585.

Pour utiliser plusieurs serveurs KMS de manière efficace, vous devez définir les attributs de configuration du KMS suivants :

enableForBackup	Spécifie si les clés provenant de ce KMS doivent être utilisées ou non pour la sauvegarde. La valeur par défaut est 1. Indiquez « 0 » si les clés de ce KMS ne doivent pas être utilisées pour la sauvegarde. Cet attribut ne s'applique pas aux restaurations. Si une image de sauvegarde a été chiffrée à l'aide de la clé de ce KMS, NetBackup utilise ce serveur KMS lors la restauration et récupère les clés pour restaurer les données. Ces serveurs KMS peuvent toujours être utilisés pour restaurer une image. Ainsi, si vous souhaitez supprimer la configuration du KMS, assurez-vous qu'aucune image n'est chiffrée à l'aide des clés de ce serveur KMS. Si la clé est perdue, les données ne peuvent pas être restaurées à partir de cette image et seront perdues. Lors de la migration du serveur KMS, au moins une configuration KMS doit avoir cette propriété définie sur 1. Sinon, toutes les sauvegardes échoueront.

priority

Spécifie le serveur KMS à utiliser lorsque NetBackup recherche des clés lors du chiffrement ou du déchiffrement. Par défaut, la priorité du serveur KMS est définie sur 0. Le serveur KMS dont la valeur est la plus élevée devient prioritaire lors du chiffrement ou du déchiffrement.

Lors de la sauvegarde ou de la restauration, NetBackup utilise le classement des serveurs KMS en fonction de leur priorité pour récupérer des clés. Ainsi, le KMS dont la priorité est la plus élevée est utilisé en premier pour récupérer des clés. Si plusieurs serveurs KMS ont la même priorité, l'un d'entre eux est utilisé.

Lors de la configuration d'un KMS (à l'aide de l'interface de ligne de commande ou de l'API) dans NetBackup, vous pouvez choisir une valeur pour ces attributs. Les options permettant de définir ces attributs sont disponibles dans les options `configureKMS` et `updateKMSConfig` de l'interface de ligne de commande `nbkmscmd`.

Se reporter à "Configuration du KMS" à la page 579.

Se reporter à "Mise à jour de la configuration du KMS" à la page 580.

Migration d'un serveur KMS vers un autre serveur KMS

Si vous disposez d'un serveur KMS configuré dans votre environnement (par exemple, un KMS/KMS1 NetBackup) et que vous souhaitez migrer vers un autre serveur KMS (par exemple, un KMS/KMS2 externe), utilisez la procédure suivante :

Pour migrer d'un serveur KMS (KMS1) vers un autre serveur KMS (KMS2)

1. Créez les clés requises dans le KMS2 pour vous assurer que tous les pools de stockage du domaine dont le chiffrement est activé disposent de clés dans le KMS2.
2. Exécutez la commande suivante pour ajouter la configuration du KMS2 dans NetBackup :

```
nbkmscmd -configureKMS -name KMS2 -type KMIP -port
port_to_connect_to_external_KMS_server -kmsServerName
network_name_of_external_KMS_server -credId credential_ID
-credNamecredential_name  -enabledForBackup 1 -priority
priority_of_KMS_server -server master_server_name -description
description
```

3 Exécutez la commande suivante pour mettre à jour l'indicateur `enabledForBackup` pour le KMS1 :

```
nbkmscmd -updatekmsconfig -name KMS1 -enabledForBackup 0
```

Désormais, aucune des sauvegardes ne sera chiffrée à l'aide des clés du KMS1. Si une clé est requise et introuvable dans le KMS2, NetBackup ne reviendra pas au KMS1.

4 Assurez-vous qu'aucune des images de sauvegarde existantes n'est chiffrée à l'aide du KMS1.

5 Supprimez la configuration du KMS1 de la configuration NetBackup.

Si vous disposez d'images chiffrées à l'aide du serveur KMS supprimé (KMS1), vous ne pourrez pas restaurer les données de ces images. Reconfigurez le serveur KMS (KMS1) et assurez-vous que les clés correspondantes sont disponibles dans ce serveur KMS avant de restaurer les données.

Utilisation d'un serveur KMS distinct pour chaque configuration de stockage

Vous pouvez utiliser des serveurs KMS distincts pour différentes configurations de stockage. Par exemple, vous pouvez utiliser un serveur KMS pour le stockage sur bande et un autre pour le stockage en cloud. Vous pouvez également utiliser des serveurs KMS distincts pour différents volumes de bande ou différents serveurs de stockage MSDP.

NetBackup recherche les clés des groupes de clés. Chaque groupe de clés est associé à un stockage. Par exemple, chaque volume de bande compatible avec le chiffrement dispose d'un groupe de clés correspondant.

Pour utiliser des serveurs KMS distincts pour le stockage sur bande et le stockage en cloud

1 Ajoutez la première configuration KMS dans NetBackup, par exemple, KMS1. La valeur par défaut de l'attribut `enableForBackup` pour KMS1 est 1.

2 Ajoutez la deuxième configuration KMS dans NetBackup, par exemple, KMS2. La valeur par défaut de l'attribut `enableForBackup` pour KMS2 est 1.

Se reporter à "Configuration du KMS" à la page 579.

3 Créez tous les groupes de clés et toutes les clés nécessaires pour le stockage sur bande dans KMS1. Assurez-vous qu'aucun des groupes de clés ne correspond au stockage en cloud.

4 Créez tous les groupes de clés et toutes les clés nécessaires pour le stockage en cloud dans KMS2. Assurez-vous qu'aucun des groupes de clés ne correspond au stockage sur bande.

   Se reporter à "Configuration des clés dans un KMS externe pour une utilisation par NetBackup" à la page 581.

   Se reporter à "Création de clés dans un KMS externe" à la page 582.

5 Pour vérifier la configuration, exécutez les sauvegardes en utilisant le stockage sur bande et le stockage en cloud.

   Les serveurs de stockage de type bande et cloud compatibles avec le chiffrement utilisent des serveurs KMS différents. Lors de la sauvegarde, NetBackup récupère le classement des KMS et recherche le groupe de clés dans le premier serveur KMS, puis dans l'autre.

   Ainsi, si KMS1 a une priorité plus élevée que KMS2, la clé requise est d'abord recherchée dans KMS1. Même pour les sauvegardes sur le stockage en cloud, la demande de clé est d'abord transmise à KMS1, puis à KMS2. Par conséquent, assurez-vous que KMS1 ne contient aucun groupe de clés correspondant au stockage en cloud.

   Lors des restaurations également, les clés sont recherchées dans les serveurs KMS disponibles en fonction de leur priorité.

Utilisation du KMS externe lors de la sauvegarde et de la restauration

Sauvegarde

Workflow du KMS lors de la sauvegarde

1 Lorsque vous exécutez une sauvegarde, le serveur de médias envoie la demande de clé en fonction du nom du groupe de clés ou du nom du pool de disques au service Web KMS.

2 Les clés d'un serveur KMS externe sont créées avec un attribut `x-keygroup`.

   Les noms des groupes de clés pour les pools de volumes de bande doivent être préfixés de `ENCR_`.

3 Le service Web KMS se connecte au serveur KMS externe et vérifie si une clé active avec l'attribut personnalisé `x-keyGroup` est présente. Si la clé est présente, elle est récupérée et renvoyée au serveur de médias.

4 Si le KMS externe n'est pas configuré ou si aucune clé de ce type n'est disponible dans le KMS externe, le service Web revient à `nbkms` pour la recherche de clé.

Restauration

Workflow du KMS lors de la restauration

1 Lors de la restauration, le serveur de médias envoie l'ID de clé ou KAD (données associées à la clé) au service Web KMS pour récupérer la clé.

2 Le service Web KMS se connecte à tous les serveurs KMS et récupère toutes les clés possibles qui correspondent au KAD.

3 Le serveur de médias utilise toutes les clés pour trouver la clé correspondante et utilise cette clé pour déchiffrer l'image.

4 Si le KMS est configuré et utilisé pour la sauvegarde et la restauration, vous pouvez consulter les détails de la configuration du KMS dans les détails du travail en cas de stockage sur bande, de stockage AdvancedDisk et de stockage en cloud.

Remarque : Les détails de la configuration KMS n'apparaissent pas dans les détails du travail en cas de stockage MSDP.

Rotation des clés

Le KMS externe vous permet de disposer d'une ou plusieurs clés actives dans un groupe de clés. NetBackup récupère toujours la clé la plus récente parmi les clés actives pour le chiffrement des données. Si vous souhaitez modifier la clé pour le chiffrement (rotation des clés), créez une nouvelle clé active sous un groupe de clés spécifique. La clé la plus récente est utilisée pour la demande de chiffrement suivante pour ce groupe de clés.

Remarque : Après toute mise à jour dans la configuration ou les clés du KMS externe, l'utilisation de la clé appropriée dans le workflow de sauvegarde ou de restauration par NetBackup peut prendre un certain temps. En effet, NetBackup met en cache la clé pendant 10 minutes (pour le KMS externe).

Pour utiliser immédiatement une clé, il est possible d'effacer le cache en exécutant la commande suivante sur le serveur de médias correspondant :

```
bpclntcmd -clear_host_cache
```

Reprise après incident lorsque la sauvegarde de catalogue est chiffrée à l'aide d'un serveur KMS externe

Dans le cadre d'une sauvegarde de catalogue, une notification par courrier électronique contenant les informations de package de reprise après incident est envoyée. Si l'image de sauvegarde du catalogue est chiffrée, le courrier électronique contient également des informations du KMS. Vous devez configurer les serveurs KMS répertoriés dans le courrier électronique avant de restaurer le catalogue.

Pour restaurer un catalogue lorsque la sauvegarde du catalogue est chiffrée à l'aide d'un serveur KMS externe

1. Installez NetBackup à l'aide du package de reprise après incident approprié.
2. Le courrier électronique de reprise après incident contient des informations spécifiques au KMS se présentant comme suit :

   ```
   The master server ms1.example.veritas.com is configured to use
   the following Key Management Servers.

   KMS Server Name = kms1.example.veritas.com, KMS Server Type =
   KMIP

   KMS Server Name = kms2.example.veritas.com, KMS Server Type =
   KMIP

   KMS Server Name = ms1.example.veritas.com, KMS Server Type = NBKMS
   ```

   Configurez les serveurs KMS répertoriés dans le courrier électronique.
3. Exécutez la restauration du catalogue.

   Consultez le Guide de dépannage NetBackup.

Alerte d'expiration des informations d'authentification du KMS

NetBackup utilise les certificats stockés dans le service du gestionnaire des informations d'authentification pour se connecter au serveur KMS. Si le certificat a expiré, les travaux échouent. Pour éviter cela, vous pouvez configurer les notifications afin d'être informé lorsque le certificat des informations authentification est sur le point d'expirer.

Pour configurer les notifications, consultez le Guide de l'administrateur NetBackup, volume I.

Chapitre 22

Conformité FIPS dans NetBackup

Ce chapitre traite des sujets suivants :

À propos de la norme FIPS

Les normes FIPS (Federal Information Processing Standards) définissent les exigences de sécurité et d'interopérabilité des ordinateurs établies par les gouvernements américain et canadien. La norme FIPS 140-2 définit les exigences de sécurité applicables aux modules cryptographiques. Elle décrit les fonctions de sécurité approuvées pour le chiffrement de clés, l'authentification de messages et le hachage symétriques et asymétriques. Pour plus d'informations sur la norme FIPS 140-2 et son programme de validation, consultez le site Web du programme de validation des modules cryptographiques du National Institute of Standards and Technology (NIST) et du Communications Security Establishment Canada (CSEC) à l'adresse suivante :

http://csrc.nist.gov/groups/STM/cmvp

À propos de la prise en charge de la norme FIPS dans NetBackup

Par défaut, le mode FIPS est désactivé dans NetBackup.

Les charges de travail suivantes sont prises en charge en mode compatible FIPS :

- Oracle, MS-SQL, SAP HANA, DB2, VMware, Hyper-V, RHV, Nutanix, DynamicNAS, MongoDB, Hadoop, HBase, MySQL, PostgreSQL, SQLite, MariaDB, SharePoint

La prise en charge suivante au niveau du système d'exploitation est disponible en mode FIPS :

- Une fois le mode FIPS activé sur RHEL 8, le système d'exploitation requiert que chaque package RPM inclue un résumé SHA-256. Les packages RPM n'incluant pas ce résumé ne pourront pas être installés. Les packages RPM créés à l'aide de la chaîne d'outils native présente sur les plates-formes RHEL 6 et RHEL 7 n'incluent aucun résumé SHA-256 et leur installation sur RHEL 8 risque donc d'échouer lorsque le mode FIPS est activé. Ce problème concerne la version 9.1 de NetBackup et les installations antérieures, car les packages de ces versions sont créés à l'aide de la chaîne d'outils native du système d'exploitation sur RHEL 7 ou versions antérieures.
  À partir de NetBackup 10.0, les packages sont créés à l'aide d'une chaîne d'outils qui ajoute le résumé SHA-256. Ces packages peuvent être installés sur RHEL 8 avec le mode FIPS activé.

Les composants, configurations ou opérations ci-après ne sont pas pris en charge en mode FIPS :

- Chiffrement côté client

  Remarque : Pour effectuer une sauvegarde avec chiffrement côté client, vous devez désactiver le mode FIPS sur l'hôte client.

- Sauvegardes NDMP
  Base de données Sybase utilisée par NetBackup
- Installation et mises à niveau de NetBackup
- Opérations `nbcheck` et `nbtelemetry`
- Reprise après incident

- Scripts (Perl, batch, shell, python) exécutés dans NetBackup
- OpsCenter
- Fichiers binaires ou utilitaires : `restore_spec_utility`, `rbac_user_migration`, `nbcloudrestore`, `nbcallhomeproxyconfig`, `nbdeployutil`, `vwcp_manage`, `nbfcv`, `nbbsdtar`, `bpkeyutil`, `nbrepo`
- Domaine NetBackup avec NBAC activé
  Si NBAC est configuré dans le domaine NetBackup, il est recommandé de ne pas activer le mode FIPS.
- Les processus MQBROKER ne prennent pas en charge la configuration FIPS de NetBackup sous Windows.
- La version MIT Kerberos utilisée par Hadoop et HBase ne fonctionne pas avec les versions d'OpenSSL compatibles avec FIPS. Pour effectuer une sauvegarde avec l'authentification Kerberos, vous devez désactiver le mode FIPS sur l'hôte de sauvegarde.
- NetBackup CloudPoint ne prend pas en charge l'hôte CloudPoint configuré en mode FIPS.
- SharePoint utilise en interne des algorithmes de chiffrement non conformes aux normes FIPS. La politique FIPS de Windows bloque les algorithmes de hachage MD5 utilisés par SharePoint. Par conséquent, la politique FIPS du système d'exploitation doit être désactivée pour que les restaurations SharePoint réussissent.
  Notez que FIPS pour NetBackup est pris en charge pour la protection de SharePoint.
  Consultez les articles suivants pour plus de détails :
  FIPS et SharePoint Server
  SharePoint 2016 et FIPS

Conditions préalables

Vérifiez les conditions préalables spécifiées avant de configurer FIPS dans votre environnement NetBackup.

- Vérifiez les points suivants avant d'activer le mode FIPS dans le domaine NetBackup et sur les clients NetBackup.
  - Le serveur principal et les serveurs de médias exécutent NetBackup 10.0 ou une version ultérieure.
  - Les clients NetBackup exécutent la version 8.1 ou une version ultérieure.
  - Vous avez consulté les informations de prise en charge de la norme FIPS.

Se reporter à "À propos de la prise en charge de la norme FIPS dans NetBackup" à la page 591.

Remarque : Si le mode FIPS est activé et si les sauvegardes sont dirigées vers le pool de déduplication du serveur de médias (MSDP), la consommation de l'UC de votre système peut augmenter.

- Pour une communication SSL optimale entre les processus NetBackup lorsque le mode FIPS est activé, vérifiez les points suivants :
  - La clé privée de l'autorité de certification NetBackup est au format de chiffrement PKCS 8, conforme à la norme FIPS.
  - La clé privée est générée à l'aide d'un algorithme conforme à la norme FIPS, tel que RSA.
  - La puissance de clé de l'autorité de certification NetBackup est définie sur 2 048 ou 3 072 bits.
    Si la puissance de clé privée ne correspond pas à la valeur prise en charge, migrez l'autorité de certification.
    Se reporter à "Migration de l'autorité de certification NetBackup" à la page 387.
    Si vous avez configuré l'autorité de certification externe, contactez l'administrateur de sécurité concerné.
    Se reporter à "A propos de la prise en charge d'une autorité de certification externe dans NetBackup" à la page 437.
  - Le processus de migration de l'autorité de certification NetBackup est terminé.

Avertissement : Si les conditions préalables ne sont pas respectées, certaines des fonctions de NetBackup peuvent ne pas fonctionner.

Spécification du caractère aléatoire de l'entropie dans NetBackup

En informatique, l'entropie désigne le caractère aléatoire utilisé par un système d'exploitation ou une application pour chiffrer des données ou pour d'autres usages nécessitant des données aléatoires.

Cette condition s'applique uniquement aux plates-formes Linux et aux programmes ou processus Java.

Vous devez spécifier le caractère aléatoire à utiliser avec des arguments JVM. Si aucun caractère aléatoire n'est spécifié, `dev/random` est utilisé par défaut.

L'argument JVM suivant est spécifié pour le programme Java :
`-DjavaDjava.security.egd=file:/dev/./random`

Activez l'option de configuration `use_urandom` pour utiliser `dev/urandom` et redémarrer les services ou relancer la console d'administration NetBackup.

Se reporter à "USE_URANDOM pour les serveurs et les clients NetBackup" à la page 603.

Configuration du mode FIPS dans votre domaine NetBackup

Cette section décrit la procédure d'activation du mode FIPS dans un domaine NetBackup. Avant de poursuivre, vérifiez que votre environnement remplit les conditions préalables ci-dessous.

Se reporter à "Conditions préalables" à la page 592.

Se reporter à "À propos de la prise en charge de la norme FIPS dans NetBackup" à la page 591.

Les paramètres suivants sont requis pour la configuration du mode FIPS :

- Activez le mode FIPS pour chaque hôte du domaine NetBackup.
- Activez le mode FIPS pour le courtier d'authentification NetBackup en mettant à jour le fichier de configuration `VRTSatlocal.conf` sur le serveur principal.
  Se reporter à "Activation du mode FIPS pour le courtier d'authentification NetBackup" à la page 596.
- Activez le mode FIPS pour la **console d'administration NetBackup**.
  Se reporter à "Activation du mode FIPS pour la console d'administration NetBackup" à la page 597.

Remarque : Appliquez cette procédure de configuration sur chaque hôte NetBackup.

Activation du mode FIPS sur un hôte NetBackup

Cette section explique comment activer le mode FIPS sur un serveur principal, un serveur de médias ou un client dans un domaine NetBackup. Vous devez effectuer les configurations suivantes sur chaque hôte pour activer le mode FIPS.

Pour activer le mode FIPS sur un hôte NetBackup

1. Activez l'indicateur `NB_FIPS_MODE` dans le fichier de configuration NetBackup.

   Se reporter à "Option NB_FIPS_MODE pour les serveurs et les clients NetBackup" à la page 603.

2. Redémarrez les services NetBackup.

Pour vérifier si un daemon ou une commande spécifique s'exécute en mode FIPS, consultez les journaux correspondants. Les lignes de journal sont disponibles seulement pour les daemons et les commandes utilisant un chiffrement.

Exemple 1 : pour vérifier si la commande `nbcertcmd` s'exécute en mode FIPS

1. Exécutez la commande suivante :

   ```
   nbcertcmd -ping
   ```

   Emplacement de la commande :

   Windows : *`install_path`*`\NetBackup\bin\nbcertcmd`

   UNIX : `/usr/openv/netbackup/bin/nbcertcmd`

2. Consultez les journaux `nbcertcmd`.

   Emplacement du répertoire des journaux :

   Windows : *`install_path`*`\NetBackup\logs\nbcert`

   UNIX : `/usr/openv/netbackup/logs/nbcert`

   Les lignes de journal suivantes doivent être présentes :

```
<2> nbcertcmd: ./nbcertcmd -ping ProcessContext: ProcessName:[nbcertcmd],
FipsMode:[ENABLED], Username:[root], IsServiceAdmin:[0], UserID:[0], GroupID:[0]
```

Exemple 2 : pour vérifier si la NetBackup Web Management Console s'exécute en mode FIPS

- Par défaut, le mode FIPS est désactivé lorsque le service **NetBackup Web Management Console** (`nbwmc`) est en cours d'exécution. Le mode FIPS est activé pour le service `nbwmc` une fois celui-ci activé pour l'hôte NetBackup.

  Consultez le fichier journal `catalina` sur l'hôte du serveur principal NetBackup pour vérifier que le service `nbwmc` s'exécute en mode FIPS.

  Emplacement du fichier journal :

  Windows :
  `install_path``\NetBackup\wmc\webserver\logs\catalina-`*`date`*`.log`

  UNIX : `/usr/openv/wmc/webserver/logs/catalina-`*`date`*`.log`

  Les lignes de journal suivantes doivent être présentes :

  ```
  The nbwmc service is running in FIPS approved mode
  ```

Activation du mode FIPS pour le courtier d'authentification NetBackup

Le service du courtier d'authentification NetBackup (`nbatd`) s'exécute uniquement sur le serveur principal NetBackup. Il n'est donc pas nécessaire d'activer le mode FIPS sur le serveur principal pour le service `nbatd`.

Le mode FIPS est désactivé par défaut.

Pour activer le mode FIPS pour le service `nbatd`

1. Ouvrez le répertoire suivant sur le serveur principal :

   Sous UNIX : `/usr/openv/netbackup/sec/at/bin/`

   Sous Windows : *`install_path`*`\NetBackup\sec\at\bin\`

2. Exécutez la commande suivante :

   Sous UNIX : `run vssregctl -s -f /usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf -b "Security\Authentication\Client" -k FipsMode -t int -v 1`

   Sous Windows : `run vssregctl -s -f "`*`install_path`*`\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf" -b "Security\Authentication\Client" -k FipsMode -t int -v 1`

   Par exemple :

   Si le *chemin_installation* est `"C:\Program Files\VERITAS"`, exécutez la commande suivante sous Windows :

   ```
   vssregctl -s -f "C:\Program Files\VERITAS\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf" -b "Security\Authentication\Client" -k FipsMode -t int -v 1 3
   ```

   Consultez les journaux `nbatd`.

   Emplacement des journaux `nbatd` :

   Sous UNIX :

   ```
   /usr/openv/logs/nbatd
   ```

   Sous Windows :

   ```
   install_path\NetBackup\logs\nbatd
   ```

   Les lignes de journal suivantes doivent être présentes :

   ```
   *** Trying to start Broker In FIPS mode ***

   *** Broker In FIPS mode already ***
   ```

3. Redémarrez les services NetBackup.

Activation du mode FIPS pour la console d'administration NetBackup

Par défaut, le mode FIPS est désactivé pour la **console d'administration NetBackup**.

Pour activer le mode FIPS pour la console d'administration NetBackup (sur un hôte local ou distant)

1. Ouvrez le fichier de configuration de la **console d'administration NetBackup**.

   Sur les ordinateurs Windows, le fichier contenant les options de configuration de la **console d'administration NetBackup** est le suivant :
   `install_path\java\setconf.bat`

   Sur les ordinateurs UNIX, le fichier contenant les options de configuration de la **console d'administration NetBackup** est le suivant :
   `/usr/openv/java/nbj.conf`

2. Dans le fichier de configuration, activez l'option `NB_FIPS_MODE`. Utilisez le format suivant :

   ```
   NB_FIPS_MODE = true
   ```

3. Enregistrez les modifications.

4. Redémarrez la **console d'administration NetBackup**.

Pour vérifier si la console d'administration NetBackup s'exécute en mode FIPS

- Consultez les journaux de la **console d'administration NetBackup**.

  Emplacement du journal :

  Sous Windows :
  `install_path\logs\user_ops\nbjlogs\jbp.root.jnbSA.`*`pid`*`.log`

  Sous UNIX :
  `/usr/openv/netbackup/logs/user_ops/nbjlogs/jbp.root.jnbSA.` *`pid`*`.log`

  Sur une console autonome, créez une structure de répertoires et consultez les journaux.

  Si le fichier journal contient les lignes de journal suivantes, cela signifie que la console s'exécute en mode FIPS :

  ```
  com.safelogic.cryptocomply.fips.approved_only: true
  ```

  Les lignes de journal suivantes doivent être présentes :

  ```
  JavaPresentationLayer- FIPS mode enforced. Reconfiguring SunJSSE.
  JavaPresentationLayer- Administration console is running in FIPS approved
  ```

Remarque : Cette configuration du mode FIPS n'affecte pas le mode FIPS du KMS NetBackup. Le KMS NetBackup continue de s'exécuter en mode FIPS par défaut.

Pour désactiver le mode FIPS pour NetBackup

Les configurations suivantes sont requises pour désactiver le mode FIPS dans votre domaine NetBackup :

- Désactivez le mode FIPS pour chaque hôte NetBackup.
  Se reporter à "Désactivation du mode FIPS pour un hôte NetBackup" à la page 599.
- Désactivez le mode FIPS pour le service du courtier d'authentification NetBackup (`nbatd`).
  Se reporter à "Désactivation du mode FIPS pour le courtier d'authentification NetBackup (`nbatd`) " à la page 600.
- Désactivez le mode FIPS pour la **console d'administration NetBackup**.
  Se reporter à "Désactivation du mode FIPS pour la console d'administration NetBackup" à la page 602.

Désactivation du mode FIPS pour un hôte NetBackup

Procédez comme suit sur chaque hôte NetBackup pour désactiver le mode FIPS.

Pour désactiver le mode FIPS pour un hôte

1. Désactivez l'indicateur `NB_FIPS_MODE` dans le fichier de configuration de NetBackup.

   Se reporter à "Option NB_FIPS_MODE pour les serveurs et les clients NetBackup" à la page 603.
2. Redémarrez les services NetBackup.

Pour vérifier si le mode FIPS est désactivé pour un daemon ou une commande spécifique, consultez les journaux correspondants. Les lignes de journal sont disponibles seulement pour les daemons et les commandes utilisant un chiffrement.

Exemple 1 : pour vérifier si le mode FIPS est désactivé pour la commande `nbcertcmd`

1. Accédez au répertoire suivant :

   UNIX : `/usr/openv/netbackup/bin`

   Windows : *`install_path`*`\NetBackup\bin`
2. Exécutez la commande suivante : `nbcertcmd -ping`

3. Accédez aux journaux `nbcertcmd` présents dans le répertoire suivant :

   UNIX : `/usr/openv/netbackup/logs/nbcert`

   Windows : *`install_path`*`\NetBackup\logs\nbcert`

4. Consultez les journaux. Le fichier journal doit contenir les lignes de journal suivantes :

```
ProcessContext: ProcessName:[nbcertcmd], FipsMode:[DISABLED], Username:[r
IsServiceAdmin:[0], UserID:[0], GroupID:[0]
```

Exemple 2 : pour vérifier si le mode FIPS est désactivé pour le service NetBackup Web Management Console (`nbwmc`)

1. La désactivation du mode FIPS pour les services NetBackup désactive également le mode FIPS pour les services `nbwmc` en cours d'exécution sur l'hôte du serveur principal.

   Ouvrez le fichier journal suivant sur l'hôte du serveur principal NetBackup :

   UNIX : `/usr/openv/wmc/webserver/logs/catalina-`*`date`*`.log`

   Windows :
   `install_path``\NetBackup\wmc\webserver\logs/catalina-`*`date`*`.log`

2. Vérifiez si le fichier journal contient la ligne de journal suivante :

```
The nbwmc service is running in non-FIPS mode
```

Désactivation du mode FIPS pour le courtier d'authentification NetBackup (`nbatd`)

Procédez comme suit pour désactiver le mode FIPS pour le `nbatd` qui s'exécute sur l'hôte du serveur principal NetBackup.

Pour désactiver le mode FIPS pour `nbatd`

1. Recherchez le répertoire suivant sur le serveur principal :

   Sous UNIX :

   ```
   /usr/openv/netbackup/sec/at/bin/
   ```

   Sous Windows :

   ```
   install_path\NetBackup\sec\at\bin\
   ```

2. Exécutez la commande suivante :

   Sous UNIX :

   ```
   run vssregctl -s -f
   /usr/openv/var/global/vxss/eab/data/root/.VRTSat/profile/VRTSatlocal.conf
   -b "Security\Authentication\Client" -k FipsMode -t int -v 0
   ```

   Sous Windows :

   ```
   run vssregctl -s -f
   "install_path\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf"
   -b "Security\Authentication\Client" -k FipsMode -t int -v 0
   ```

   Si le chemin d'installation est `"C:\Program Files\VERITAS"`, exécutez la commande suivante sous Windows :

   ```
   vssregctl -s -f "C:\Program
   Files\VERITAS\NetBackup\var\global\vxss\eab\data\systemprofile\VRTSatlocal.conf"
   -b "Security\Authentication\Client" -k FipsMode -t int -v 0
   ```

3. Redémarrez les services NetBackup.

Pour vérifier si le mode FIPS est désactivé pour le service `nbatd`

1. Accédez aux journaux `nbatd` à l'emplacement suivant :

   UNIX :

   ```
   /usr/openv/logs/nbatd/
   ```

   Windows :

   ```
   install_path\NetBackup\logs\nbatd\
   ```

2. Vérifiez si le fichier journal contient la ligne de journal suivante :

   ```
   Broker Not In FIPS mode
   ```

Désactivation du mode FIPS pour la console d'administration NetBackup

Procédez comme suit sur chaque hôte NetBackup pour désactiver le mode FIPS.

Pour désactiver le mode FIPS pour la console d'administration NetBackup (sur un hôte local ou distant)

1. Ouvrez le fichier de configuration de la **console d'administration NetBackup**.

   Sur les ordinateurs UNIX, le fichier contenant les options de configuration de la **console d'administration NetBackup** est le suivant :
   `/usr/openv/java/nbj.conf`

   Sur les ordinateurs Windows, le fichier contenant les options de configuration de la **console d'administration NetBackup** est le suivant :
   `install_path\java\setconf.bat`

2. Désactivez l'option `NB_FIPS_MODE` dans le fichier de configuration. Utilisez le format suivant :

   NB_FIPS_MODE = false

3. Enregistrez les modifications.

4. Redémarrez la **console d'administration NetBackup**.

Pour vérifier si le mode FIPS est désactivé pour la console d'administration NetBackup

- Consultez les journaux de la **console d'administration NetBackup**.

  Emplacement du journal :

  Sous UNIX :
  `/usr/openv/netbackup/logs/user_ops/nbjlogs/jbp.root.jnbSA.` *`pid`*`.log`

  Sous Windows :
  `install_path\logs\user_ops\nbjlogs\jbp.root.jnbSA.`*`pid`*`.log`

  Sur une console autonome, créez une structure de répertoires (par exemple, `C:\Program Files\Veritas\NetBackup\logs\user_ops\nbjlogs`) et consultez les journaux.

  Si le fichier journal contient les lignes de journal suivantes, cela signifie que le mode FIPS est désactivé pour la console :

  ```
  JavaPresentationLayer- Fips approved mode system property is - false
  JavaPresentationLayer- Administration console is running in non-FIPS mode
  ```

Option NB_FIPS_MODE pour les serveurs et les clients NetBackup

Utilisez l'option `NB_FIPS_MODE` pour activer le mode FIPS dans votre domaine NetBackup.

Tableau 22-1 Informations sur NB_FIPS_MODE

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup.

Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option.
	Pour plus d'informations au sujet de ces commandes, consultez le Guide de référence des commandes NetBackup.
	L'option `NB_FIPS_MODE` est désactivée par défaut.
	Pour l'activer, utilisez le format suivant :
	`NB_FIPS_MODE = ENABLE`
	Pour la désactiver, utilisez le format suivant :
	`NB_FIPS_MODE = DISABLE`

Équivalent dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

USE_URANDOM pour les serveurs et les clients NetBackup

Dans le domaine informatique, l'entropie désigne les éléments aléatoires sur lesquels s'appuie un système d'exploitation ou une application pour chiffrer des données ou pour d'autres usages nécessitant des données aléatoires.

Activez l'option `USE_URANDOM` pour spécifier `/dev/urandom` comme le périphérique de caractères fournissant une sortie aléatoire sécurisée par chiffrement dans votre environnement NetBackup.

Tableau 22-2 Informations sur USE_URANDOM

Utilisation	Description
Où l'utiliser	Sur les serveurs ou clients NetBackup.

Utilisation	Description
Comment l'utiliser	Exécutez les commandes `nbgetconfig` et `nbsetconfig` pour afficher, ajouter ou modifier l'option. Pour plus d'informations au sujet de ces commandes, consultez le Guide de référence des commandes NetBackup. La valeur par défaut de l'option `USE_URANDOM` est `0`. Lorsque `USE_URANDOM` est définie sur la valeur par défaut, le périphérique de caractères à utiliser est basé sur la valeur de l'option `NB_FIPS_MODE`. Si l'option `NB_FIPS_MODE` est activée, `dev/random` est utilisé. Si l'option `NB_FIPS_MODE` est désactivée, `dev/urandom` est utilisé. Se reporter à "Option NB_FIPS_MODE pour les serveurs et les clients NetBackup" à la page 603. Pour activer l'option `USE_URANDOM`, utilisez le format suivant : `USE_URANDOM = 1` Si `USE_URANDOM` est définie sur `2` (ou si elle est désactivée), le périphérique de caractères `dev/random` est utilisé pour fournir une sortie aléatoire sécurisée par chiffrement.
Équivalent dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la **console d'administration NetBackup**.

Chapitre 23

Compte de services Web NetBackup

Ce chapitre traite des sujets suivants :

Compte de services web NetBackup

À partir de NetBackup 8.0, le serveur maître NetBackup comprend un serveur web configuré pour la prise en charge des opérations de sauvegarde critiques. Le serveur web opère sous le contrôle des éléments de compte utilisateur avec des privilèges limités. Ces éléments de compte utilisateur doivent être disponibles sur chaque serveur maître (ou sur chaque nœud d'un serveur maître en cluster).

NetBackup requiert des informations de compte pour les services web en tant qu'élément de l'installation du serveur maître NetBackup.

Plus d'informations sont disponibles sur la configuration de ce compte avant l'installation et sur la manière de modifier le compte après l'installation.

Consultez le *Guide d'installation NetBackup* pour plus d'informations sur la création de l'utilisateur du serveur web et du groupe.

Se reporter à "Modification du compte utilisateur du service web" à la page 606.

Remarque : Pour des raisons de sécurité, n'autorisez pas les utilisateurs du serveur web ou les groupes à disposer des privilèges d'administrateur ou de superutilisateur.

Modification du compte utilisateur du service web

Pour prendre en charge la modification des comptes d'utilisateur de service web, utilisez le script d'utilitaire `wmcUtils`. Ce script d'utilitaire est valide uniquement si un utilisateur du service web et un groupe ont été créés. Avant de l'utiliser, vérifiez que l'utilisateur du service web et le groupe existent et que l'utilisateur fait partie du groupe. Considérez les éléments suivants lorsque vous modifiez le compte d'utilisateur du service web :

- Si votre environnement utilise les utilisateurs de domaine Windows, utilisez le format `DOMAIN\USER`.
- Si vous utilisez un environnement en cluster sur une plate-forme Windows, le compte d'utilisateur du service web NetBackup doit être un utilisateur `DOMAIN`. (Exemple : utilisateur AD)
- Si vous utilisez des environnements en cluster, l'utilisateur du service web NetBackup peut être un utilisateur local ou de domaine.
- Si vous utilisez un environnement en cluster sur des plates-formes Linux ou UNIX, l'utilisateur du service web NetBackup peut être un utilisateur local. En outre, le groupe peut être un groupe local. L'utilisateur du service web NetBackup doit avoir le même nom et le même UID sur tous les nœuds du cluster. En outre, le groupe doit avoir le même nom et le même GID sur tous les nœuds du cluster. Il est recommandé d'utiliser des utilisateurs de domaine (exemple : NIS) pour les environnements en cluster.

Remarque : N'utilisez pas l'utilisateur consigné pour exécuter le script d'utilitaire `wmcUtils`. Si vous êtes connecté à un environnement en tant que *my_domain\my_user*, vous ne pouvez pas utiliser ce compte pour exécuter le service `NetBackup Web Management Console`. NetBackup ne prend pas en charge ce scénario.

Pour modifier le compte d'utilisateur du service web sous Windows

1. Ouvrez une invite de commande.
2. Remplacez le répertoire par : *`chemin_installation`*`\wmc\bin\install`

3 Exécutez `wmcUtils.bat -changeUser` pour modifier l'utilisateur du service web.

Exemple : (`nbwebsvc1` est l'utilisateur du service web et `nbwebgrp1` est le groupe d'utilisateurs dont `nbwebsvc1` est membre)

```
wmcUtils.bat -changeUser nbwebsvc1 nbwebgrp1
```

Pour plus d'informations sur le script d'utilitaire `wmcUtils.bat`, utilisez l'option `wmcUtils.bat -help`.

4 (Conditionnel) Si vous utilisez un environnement en cluster, exécutez `wmcUtils.bat -changeUser` sur les nœuds actifs et inactifs.

5 Entrez le mot de passe de l'utilisateur du service web (exemple : `nbwebsvc1`) lorsque vous y êtes invité par le script.

Le service `NetBackup Web Management Console` redémarre lorsque le mot de passe entré est correct. Si vous entrez un mot de passe incorrect, un message d'erreur **Échec d'ouverture de session** s'affiche avant que le service `NetBackup Web Management Console` ne démarre.

6 Pour vérifier que l'utilisateur du service web est modifié, assurez-vous que *`install_path`*`\bin\nbcertcmd.exe -ping` fonctionne.

Remarque : La sortie du script d'utilitaire `wmcUtils.bat` est capturée dans `nbwmc_support.log`. Le journal se trouve ici : *`chemin_installation`*`\wmc\webserver\logs\nbwmc_support.log`

Pour modifier le compte d'utilisateur du service web sous Linux ou UNIX

1 Ouvrez un shell.

2 Changez le répertoire en : `/usr/openv/wmc/bin/install`

3 Exécutez `wmcUtils -changeUser` pour modifier l'utilisateur du service web.

Exemple : (`nbwebsvc1` est l'utilisateur du service web et `nbwebgrp1` est le groupe d'utilisateurs dont `nbwebsvc1` est membre)

```
usr/openv/wmc/bin/install/wmcUtils -changeUser nbwebsvc1 nbwebgrp1
```

Pour plus d'informations sur le script d'utilitaire `wmcUtils`, utilisez l'option `wmcUtils -help`.

4 (Conditionnel) Si vous utilisez un environnement en cluster, exécutez `wmcUtils.bat -changeUser` sur les nœuds actifs et inactifs.

5 Entrez le mot de passe de l'utilisateur du service web (exemple : `nbwebsvc1`) lorsque vous y êtes invité par le script.

Le service `NetBackup Web Management Console` redémarre lorsque le mot de passe entré est correct. Si vous entrez un mot de passe incorrect, un message d'erreur **Échec d'ouverture de session** s'affiche avant que le service `NetBackup Web Management Console` ne démarre.

6 Pour vérifier que l'utilisateur du service web est modifié, assurez-vous que `/usr/openv/netbackup/bin/nbcertcmd -ping` fonctionne.

Remarque : La sortie du script d'utilitaire `wmcUtils` est capturée dans `nbwmc_support.log`. Le journal se trouve ici : `/usr/openv/wmc/webserver/logs/nbwmc_support.log`

Chapitre 24

Exécution de services NetBackup avec un compte utilisateur sans privilège (utilisateur du service)

Ce chapitre traite des sujets suivants :

À propos d'un compte utilisateur du service NetBackup

À partir de NetBackup 9.1, il est possible d'exécuter la plupart des services du serveur principal à l'aide d'un utilisateur sans privilège, ce qui est vivement

recommandé. L'utilisateur sans privilège est appelé `service user` et est uniquement utilisé pour exécuter les services NetBackup.

Remarques importantes relatives à l'utilisation d'un compte utilisateur du service

Passez en revue les points suivants pour exécuter les services NetBackup avec le compte utilisateur du service.

- N'utilisez pas le compte utilisateur du service pour effectuer des opérations NetBackup. Le compte utilisateur du service est uniquement destiné à exécuter des services NetBackup.
- Il est recommandé de réserver le groupe principal de l'utilisateur du service à l'utilisateur du service.
- L'utilisation de l'utilisateur racine comme utilisateur du service est déconseillée.
- `nbwebsvc` ne doit pas être utilisé comme utilisateur du service.
- `nbwebgrp` doit être un groupe secondaire de l'utilisateur du service.
- Le nombre de processus exécutables avec l'utilisateur du service doit être identique au nombre de processus exécutés avec l'utilisateur racine.
  Utilisez `ulimit -u` pour rechercher le nombre maximal de processus utilisateur exécutables avec l'utilisateur du service.
- Le nombre de fichiers qui peuvent être ouverts avec l'utilisateur du service doit être identique au nombre de fichiers ouverts avec l'utilisateur racine.
  Utilisez la commande `ulimit -Hn` pour afficher le nombre maximal de fichiers qui peuvent être ouverts avec l'utilisateur du service.
- L'utilisation d'un compte utilisateur du service différent du compte utilisateur racine nécessite une conversion ponctuelle qui peut augmenter considérablement la durée de la mise à niveau en fonction de la taille de votre catalogue.
- Hormis le répertoire d'installation, tous les chemins externes doivent être accessibles par l'utilisateur du service.
  Se reporter à "Octroi d'autorisations d'accès aux chemins externes pour le compte utilisateur du service" à la page 612.
- Les chemins d'accès aux variables d'environnement doivent être accessibles par l'utilisateur du service.
- L'utilisateur de service doit avoir accès au répertoire temporaire du système d'exploitation, habituellement `/tmp` ou `/var/tmp`. Cela peut être indiqué par une macro P_tmpdir.
- Le compte utilisateur du service peut être un compte sans mot de passe.

- Si un utilisateur du service est configuré, les fichiers journaux hérités (`/user/openv/netbackup/logs` sous UNIX ou `C:\Program Files\Veritas\NetBackup\logs` sous Windows) présentent le préfixe comme `SERVICE_USER`.

  Par exemple : `SERVICE_USER.040921_00001.log`
- Le nom d'utilisateur du service doit contenir au maximum 32 caractères, uniquement anglais.

Configuration d'un compte utilisateur du service

Cet utilisateur du service doit être créé à l'avance et disposer du groupe secondaire `nbwebgrp`.

Configuration d'un compte utilisateur du service sous UNIX

Lors de l'installation ou de la mise à niveau du serveur principal sous UNIX, une nouvelle invite peut s'afficher pour spécifier un nouvel utilisateur (de préférence un utilisateur non racine) qui peut être utilisé en tant qu'utilisateur du service. Ce nouvel utilisateur sert désormais à exécuter la plupart des daemons sur le serveur principal.

Pour créer le compte d'utilisateur local sous UNIX, exécutez la commande suivante :

```
useradd -c 'NetBackup Services account'
-d/usr/openv/service_user_nameservice_user_name
```

Pour ajouter l'utilisateur du service au groupe secondaire `nbwebgrp`, exécutez la commande suivante :

```
usermod -a -G nbwebgrp service_user_name
```

Vérifiez les éléments suivants :

- Dans un environnement en cluster, vérifiez que les comptes locaux sont définis de façon cohérente sur tous les nœuds de cluster. Si vous utilisez un environnement en cluster sur des plates-formes Linux ou UNIX, l'utilisateur du service NetBackup peut être un utilisateur local. L'utilisateur du service NetBackup doit porter le même nom et le même UID sur tous les nœuds du cluster.
- Il est recommandé d'utiliser des utilisateurs de domaine (exemple : NIS) dans un environnement en cluster. Les comptes LDAP sont pris en charge et peuvent être utilisés sous UNIX.
- Le compte de service NetBackup doit utiliser un shell compatible avec POSIX.

Configuration d'un compte utilisateur du service sous Windows

Sous Windows, une nouvelle installation utilise le compte intégré Service local. Aucune modification n'a été apportée au processus de mise à niveau.

Modification d'un compte utilisateur du service après une installation ou une mise à niveau

Sous UNIX, vous pouvez remplacer le compte utilisateur du service par un compte utilisateur à l'aide de la commande `nbserviceusercmd`.

Sous Windows, vous pouvez définir le compte utilisateur du service sur Administrateur, Système local ou Service local à l'aide de la commande `nbserviceusercmd`.

Pour plus d'informations, consultez le Guide de référence des commandes NetBackup.

Octroi d'autorisations d'accès aux chemins externes pour le compte utilisateur du service

Les opérations NetBackup échouent si le compte utilisateur du service ne disposent pas des autorisations d'accès aux chemins d'accès de répertoire externes à NetBackup, ainsi qu'à leur contenu. Hormis le répertoire d'installation, tous les chemins externes doivent être accessibles par l'utilisateur du service, par exemple :

- Chemin d'accès à la reprise après incident (DR)
- Chemins d'accès externes aux certificats de l'autorité de certification
- Chemins d'accès externes utilisés comme paramètres pour les commandes suivantes :
  - `nbdb_admin`
  - `create_nbdb`
  - `nbdb_move`
  - `nbdb_backup`
  - `nbdb_restore`
  - `nbdb_unload`
  - `cat_export`

- `cat_import`

Pour octroyer des autorisations d'accès aux chemins externes pour le compte utilisateur du service :

1. Vérifiez que les chemins d'accès spécifiques aux opérations NetBackup ne sont pas partagés entre plusieurs utilisateurs sur l'hôte.
   - Sous UNIX, vérifiez que les chemins d'accès ne sont pas les suivants : Répertoire /tmp, /root ou d'origine d'un autre utilisateur non racine
   - Sous Windows, vérifiez que les chemins d'accès ne sont pas les répertoires d'un compte utilisateur différent et résidant dans `C:\users`.
2. Exécutez la commande suivante pour permettre au compte utilisateur du service d'accéder aux chemins d'accès externes et à leur contenu :
   - Sous UNIX : `chown -R service_user_namepath`
     Une fois la commande `chown` exécutée, vérifiez que l'utilisateur du service peut écrire sur le chemin d'accès spécifié à l'aide de la commande suivante : `su service_user_name -c "touch path/test.txt"`
   - Sous Windows : `netbackup_install_path\NetBackup\bin\goodies\nbserviceusercmd.exe -addacl path -reason reason`

Services NetBackup exécutés avec le compte d'utilisateur du service

À partir de NetBackup 9.1, les services NetBackup suivants s'exécutent avec le compte utilisateur du service :

Windows	UNIX
SQLANYs_VERITAS_NB	NB_dbsrv
NetBackup Request Daemon	bprd
NetBackup Database Manager	bpdbm
-	bpjobd
NetBackup Compatibility Service	bpcompatd
NetBackup Audit Manager	nbaudit
NetBackup Event Manager	nbevtmgr

Windows	UNIX
NetBackup Enterprise Media Manager	nbemm
NetBackup Resource Broker	nbrb
NetBackup Job Manager	nbjm
NetBackup Policy Execution Manager	nbpem
NetBackup Service Layer	nbsl
NetBackup Storage Lifecycle Manager	nbstserv
NetBackup Proxy Service	nbproxy
NetBackup Indexing Manager	nbim
NetBackup Agent Request Server	nbars
NetBackup Key Management Service	nbkms
NetBackup Vault Manager	nbvault
Anomaly Detection Management Service	nbanomalymgmt
vnetd-child-proxies ■ vnetd -proxy inbound_proxy -number 0 ■ vnetd -proxy outbound_proxy -number 0 ■ vnetd -proxy http_api_tunnel -number 0 ■ vnetd -proxy http_pbx_tunnel -number 0	vnetd-child-proxies ■ vnetd -proxy inbound_proxy -number 0 ■ vnetd -proxy outbound_proxy -number 0 ■ vnetd -proxy http_api_tunnel -number 0 ■ vnetd -proxy http_pbx_tunnel -number 0

Remarque : Si vous avez sélectionné le compte de service avec privilèges Administrateur (compte utilisateur utilisé par le service autonome `vnetd`), les proxies enfants `vnetd` seront exécutés avec le même compte Administrateur.

Chapitre 25

Immuabilité et ineffaçabilité des données dans NetBackup

Ce chapitre traite des sujets suivants :

À propos des données immuables et indélébiles

NetBackup protège vos données contre le chiffrement, la modification et la suppression à l'aide des propriétés WORM.

WORM est l'acronyme de Write Once Read Many.

Les propriétés WORM fournissent deux niveaux supplémentaires de sécurité pour les images de sauvegarde :

- Immuabilité : cette protection permet de s'assurer que l'image de sauvegarde est en lecture seule et ne peut pas être modifiée, endommagée ou chiffrée après la sauvegarde.
- Indélébilité : cette propriété empêche la suppression de l'image de sauvegarde avant son expiration. Ainsi, les données sont protégées contre toute suppression malveillante.

La configuration de ces propriétés WORM protège vos données contre certaines attaques de logiciels malveillants dans une certaine mesure, par exemple des ransomwares.

NetBackup permet d'enregistrer des sauvegardes sur des périphériques de stockage WORM afin que leurs données ne soient pas endommagées. Elle vous permet également de bénéficier d'options avancées proposées par vos fournisseurs de stockage pour protéger vos données de sauvegarde conformément aux lois en vigueur.

Une fois que les images de sauvegarde sont enregistrées à l'aide d'une unité de stockage compatible WORM, les données ne peuvent pas être supprimées avant l'heure de déverrouillage de WORM et ne peuvent plus être modifiées. La durée de déverrouillage WORM est définie lorsque l'image est créée ou que la période d'expiration d'image est prolongée.

La durée de verrouillage WORM (durée après laquelle elle devient effaçable) d'une sauvegarde correspond à son délai d'expiration. Le niveau de conservation dans la politique ou la politique de cycle de vie du stockage détermine le délai d'expiration.

La seule modification autorisée de l'image de sauvegarde est la prolongation de son délai d'expiration. Notez que le délai d'expiration de la sauvegarde peut être prolongé, mais pas raccourci. Pour prolonger le délai d'expiration, utilisez la commande `bpexpdate -extend_worm_locks`. Pour plus d'informations sur `bpexpdate`, consultez le Guide de référence des commandes NetBackup

Workflow de configuration des données immuables et indélébiles

Effectuez les étapes suivantes dans l'ordre indiqué pour protéger vos données en configurant l'immuabilité et l'indélébilité.

Tableau 25-1 Workflow de configuration des données immuables et indélébiles

Étape	Description
1	Configurez les paramètres WORM suivants sur le serveur de stockage. L'administrateur de stockage configure ces paramètres en dehors de NetBackup. ■ **Compatible WORM** : si l'unité de stockage et le pool de disques associé utilisent la propriété WORM lors de la création d'images de sauvegarde, celles-ci sont définies comme non modifiables et ineffaçables. ■ **Durée minimale de verrouillage** : spécifie la durée minimale autorisée pendant laquelle les données d'une image de sauvegarde sont indélébiles. L'administrateur de stockage définit cette durée sur l'unité de stockage logique (LSU) ou le volume de domaine (DV), que NetBackup découvre. ■ **Durée maximale de verrouillage** : spécifie la durée minimale autorisée pendant laquelle les données d'une image de sauvegarde sont indélébiles. L'administrateur de stockage définit cette durée sur l'unité de stockage logique (LSU) ou le volume de domaine, que NetBackup découvre. Consultez la documentation relative au plug-in du fournisseur OST.
2	Configurez un pool de disques à l'aide de volumes compatibles WORM. Pour plus d'informations, voir l'aide en ligne de NetBackup.
3	Configurez une unité de stockage avec l'option **Utiliser WORM** activée.
4	Configurez une politique de sauvegarde à l'aide de l'unité de stockage compatible WORM. Création d'une politique de sauvegarde

Remarque : En cas de modifications de stockage ou de mises à niveau logicielles d'un fournisseur OST tiers, vous devez mettre à jour manuellement les serveurs de stockage et les pools de disques. Consultez la section Achèvement de la mise à jour de votre système après une mise à niveau du Guide de mise à niveau de NetBackup.

Suppression d'une image immuable du stockage à l'aide de la commande `bpexpdate`

La suppression d'une image immuable survient uniquement lorsque le stockage utilisé permet la suppression du verrouillage. La suppression du verrouillage peut être effectuée à l'aide du mode Entreprise sur une appliance Flex ou un périphérique de stockage tiers prenant en charge la suppression du verrouillage. Lorsqu'une image immuable est supprimée, le stockage que vous utilisez est responsable de

la suppression du verrouillage et NetBackup est responsable de la suppression de l'image.

Lorsque vous utilisez une appliance Flex, vous devez utiliser la ligne de commande ou une session SSH pour supprimer le verrouillage sur l'image. Si vous utilisez un périphérique de stockage tiers, consultez la documentation du fournisseur pour obtenir des instructions sur la suppression d'images verrouillées.

Supprimer l'image immuable d'une appliance Flex

1. Vérifiez que l'appliance Flex est en mode Entreprise.
2. A partir de la ligne de commande NetBackup, utilisez la commande `bpimagelist` pour trouver l'ID de l'image.

   Cette procédure utilise l'exemple d'ID d'image suivant :

   ```
   Backup ID: server123.veritas.com_1234567890
   ```

3. Supprimez le verrouillage d'image sur le stockage à l'aide de l'option de ligne de commande ou de la session SSH. Vous devez utiliser l'utilisateur `msdadm` par défaut pour exécuter les options suivantes.

   Option de ligne de commande :

   - Ouvrez le répertoire `/usr/openv/pdde/pdcr/bin/`.
   - Utilisez la commande suivante pour interroger et modifier la base de données de catalogue pour l'ID de sauvegarde donné (exemple : `server123.veritas.com_1234567890`). L'option `-worm disable` désactive le verrouillage de conservation pour une image à l'aide de l'ID de sauvegarde.

     ```
     catdbutil -worm disable -backupid
     ```

   Option de session SSH :

   - Ouvrez une session SSH sur l'instance de serveur de stockage WORM.
   - Utilisez la commande `retention policy disable` pour interroger et modifier la base de données de catalogue pour la politique donnée. Les arguments `policydisable` désactivent le verrouillage de conservation pour une image à l'aide de l'ID de politique utilisé pour la conservation d'image dotée d'un verrouillage de conservation.

   Pour plus d'informations sur les options de commande dans cette étape, consultez le Guide de déduplication NetBackup.

4 Ajoutez l'ID de l'image à `bpexpdate` avec l'option `-try_expire_worm_copy`.

```
bpexpdate -d 0 backupid server123.veritas.com_1234567890
-try_expire_worm_copy -copy 1
```

5 Utilisez **o** ou **n** pour confirmer la suppression.

Si le verrouillage de stockage n'est pas supprimé, NetBackup renvoie une erreur indiquant qu'il existe une erreur de verrouillage WORM.

Se reporter à "Suppression d'une image immuable du catalogue à l'aide de la commande`bpexpdate`" à la page 619.

Se reporter à "À propos des données immuables et indélébiles" à la page 615.

Suppression d'une image immuable du catalogue à l'aide de la commande`bpexpdate`

Vous pouvez supprimer une image immuable du catalogue NetBackup et conserver cette image sur le stockage.

Supprimer une image immuable du catalogue

1 Ouvrez l'interface de ligne de commande (CLI)NetBackup.

2 Supprimez l'image du catalogue à l'aide de la commande `bpexpdate` avec les options `-try_expire_worm_copy` et `-nodelete`.

```
bpexpdate -d 0 -backupid server123.veritas.com_1234567890
 -copy 1 -try_expire_worm_copy -nodelete
```

L'utilisation conjointe des options `-try_expire-worm_copy` et `-nodelete` supprime l'image du catalogue uniquement et n'affecte pas le stockage.

3 Utilisez **o** ou **n** pour confirmer la suppression.

Suppression d'une image immuable du stockage à l'aide de la commande

Se reporter à "À propos des données immuables et indélébiles" à la page 615.

Chapitre 26

Détection d'anomalies de sauvegarde

Ce chapitre traite des sujets suivants :

À propos de la détection des anomalies de sauvegarde

NetBackup est désormais en mesure de détecter les anomalies dans les métadonnées de sauvegarde. Pour ce faire, il détecte les données de travail inhabituelles dans le flux de sauvegarde de données. Par exemple, il peut détecter un nombre ou une taille de fichier anormale.

Les métadonnées, attributs ou fonctions suivants du travail de sauvegarde sont vérifiés pendant la détection des anomalies de sauvegarde :

- Taille de l'image de sauvegarde
- Nombre de fichiers de sauvegarde
- Données transférées en Ko
- Taux de déduplication

- Date/heure d'achèvement du travail de sauvegarde

Tout écart inhabituel de ces attributs de travail de sauvegarde est considéré comme une anomalie et notifié à l'aide de l'interface utilisateur Web NetBackup.

Workflow de détection et de notification des anomalies de sauvegarde

Le workflow de détection et de notification des anomalies de sauvegarde est décrit ci-dessous :

Tableau 26-1 Workflow

Étape	Description
Étape 1	Installez ou mettez à niveau le logiciel NetBackup sur le serveur principal et le serveur de médias. Consultez le Guide d'installation et de mise à niveau de NetBackup.
Étape 2	Activez le serveur principal ou le serveur de médias pour détecter les anomalies de sauvegarde. Se reporter à "Détection d'anomalies de sauvegarde sur le serveur principal " à la page 622. Se reporter à " Détection d'anomalies de sauvegarde sur le serveur de médias " à la page 623.
Étape 3	Configurez les paramètres de détection d'anomalies à l'aide de l'interface utilisateur Web NetBackup. Se reporter à " Configuration des paramètres de détection d'anomalies" à la page 624.
Étape 4	Affichez les anomalies à l'aide de l'interface utilisateur Web NetBackup. Se reporter à "Affichage des anomalies" à la page 625.

Comment sont détectées les anomalies de sauvegarde

Considérez l'exemple suivant :

Dans une organisation, environ 1 Go de données est sauvegardé chaque jour pour un client et une politique de sauvegarde donnés avec le type de planification COMPLETE. Un jour, 10 Go de données sont sauvegardés. Cette instance est capturée en tant qu'anomalie de taille d'image et notifiée. L'anomalie est détectée, car la taille de l'image ce jour-là (10 Go) est bien plus importante que d'habitude (1 Go).

Cette déviation significative des métadonnées est qualifiée d'anomalie en fonction de son score d'anomalie.

Le score d'anomalie est calculé en fonction de l'écart entre les données relevées et un ensemble d'observations similaires effectuées dans le passé. Dans cet exemple, cet ensemble renvoie 1 Go comme taille moyenne des sauvegardes de données. Vous pouvez déterminer la gravité des anomalies en fonction de leur score.

Par exemple :

Score d'anomalie d'Anomalie_A = 7

Score d'anomalie d'Anomalie_B = 2

Conclusion : Anomalie_A est plus grave qu'Anomalie_B

NetBackup tient compte des paramètres de configuration (paramètres par défaut et avancés si disponibles) pendant la détection de l'anomalie.

Détection d'anomalies de sauvegarde sur le serveur principal

Cette rubrique décrit la procédure permettant au serveur principal de détecter les anomalies de sauvegarde.

Pour permettre au serveur principal de détecter les anomalies de sauvegarde

1. Installez le logiciel de serveur principal NetBackup sur votre système (ou mettez le logiciel de serveur principal à niveau).

   Après l'installation, les configurations suivantes sont automatiquement réalisées sur le serveur principal :

   - Le service `NetBackup Anomaly Detection Management` (`nbanomalymgmt`) est démarré sur le serveur principal par défaut avec deux autres services

de détection d'anomalies. Le processus de détection d'anomalies de sauvegarde est démarré en arrière-plan.

2 Configurez les paramètres de détection d'anomalies de sauvegarde à l'aide de l'interface utilisateur Web NetBackup. NetBackup tient compte de ces paramètres lors de la procédure de détection d'anomalies.

Se reporter à " Configuration des paramètres de détection d'anomalies" à la page 624.

Se reporter à "Comment sont détectées les anomalies de sauvegarde" à la page 621.

Lorsque des anomalies sont détectées, elles sont notifiées via l'interface utilisateur Web de NetBackup.

Se reporter à "Affichage des anomalies" à la page 625.

Détection d'anomalies de sauvegarde sur le serveur de médias

Cette rubrique décrit le workflow permettant au serveur de médias de détecter les anomalies de sauvegarde.

Pour permettre au serveur de médias de détecter les anomalies de sauvegarde

1 Installez le logiciel de serveur de médias NetBackup sur votre système (ou mettez le logiciel de serveur de médias à niveau).

2 Sur le serveur de médias, démarrez le service `nbanomalymgmt` manuellement. Utilisez le script suivant :

```
nbanomalymgmt -start
```

3 (Facultatif) Pour préserver les données précédemment collectées par le serveur principal, procédez comme suit :

- Assurez-vous que le service `nbanomalymgmt` sur le serveur principal est arrêté.
- Copiez le fichier `NB_Anomaly.db` du dossier `anomaly_detection` sur le serveur principal vers le dossier `anomaly_detection` du serveur de médias.

- Démarrez le service `nbanomalymgmt` sur le serveur de médias.

4 Configurez les paramètres de détection d'anomalies de sauvegarde dans l'interface utilisateur Web NetBackup. NetBackup tient compte de ces paramètres lors de la procédure de détection d'anomalies.

Se reporter à " Configuration des paramètres de détection d'anomalies" à la page 624.

Se reporter à "Comment sont détectées les anomalies de sauvegarde" à la page 621.

Lorsque des anomalies sont détectées, elles sont notifiées via l'interface utilisateur Web de NetBackup.

Se reporter à "Affichage des anomalies" à la page 625.

Configuration des paramètres de détection d'anomalies

Une fois que vous avez activé le paramètre de détection d'anomalies, la collecte des données d'anomalie, le service de détection et les événements sont activés. Il existe des paramètres de détection d'anomalies de base et avancés.

Se reporter à "À propos de la détection des anomalies de sauvegarde" à la page 620.

Pour configurer des paramètres de détection d'anomalies

1 Connectez-vous à l'interface utilisateur Web NetBackup.

2 Sur la gauche, sélectionnez **Détection et rapports > Détection d'anomalies**.

3 Dans la partie supérieure droite, cliquez sur **Paramètres des anomalies**.

4 Cliquez sur **Modifier** sur la droite pour configurer les paramètres de détection d'anomalies en sélectionnant l'une des options suivantes :

- **Tout désactiver**
- **Activer la collecte des données d'anomalie**
- **Activer la collecte des données d'anomalie et le service de détection**
- **Activer la collecte des données d'anomalie, le service de détection et les événements**

5 Cliquez sur **Enregistrer**.

6 Cliquez sur **Modifier** pour modifier les **paramètres de base** suivants :

- **Sensibilité de la détection d'anomalies**

- **Paramètres de conservation des données**
- **Paramètres de collecte de données**
- **Paramètres du serveur proxy d'anomalie**

7 Cliquez sur **Enregistrer**.

8 Cliquez sur **Paramètres avancés**.

9 Modifiez **Désactiver les paramètres d'anomalie pour les clients**.

10 Cliquez sur **Enregistrer**.

11 Modifiez **Désactiver le type de politique ou des fonctions spécifiques pour l'apprentissage automatique**.

12 Cliquez sur **Enregistrer**.

Affichage des anomalies

NetBackup est désormais en mesure de détecter les anomalies dans les métadonnées de sauvegarde. Pour ce faire, il détecte les données de travail inhabituelles dans le flux de sauvegarde de données. Par exemple, il peut détecter un nombre ou une taille de fichier anormale.

Se reporter à "À propos de la détection des anomalies de sauvegarde" à la page 620.

Remarque : Si le nombre d'anomalies est égal à `0`, aucune anomalie n'a été générée ou les services de détection d'anomalie ne sont pas en cours d'exécution.

Pour afficher les anomalies

1 Connectez-vous à l'interface utilisateur web NetBackup.

2 Sur la gauche, sélectionnez **Détection et rapports > Détection d'anomalies**.

Les colonnes suivantes s'affichent :

- ID du travail : ID du travail pour lequel l'anomalie est détectée
- Nom du client : nom du client NetBackup où l'anomalie est détectée
- Type de politique : type de politique du travail de sauvegarde associé
- Nombre : nombre d'anomalies détectées pour ce travail
- Score : gravité de l'anomalie. Plus l'anomalie est grave, plus le score est élevé.
- Gravité des anomalies : gravité des anomalies notifiées pour ce travail

- Résumé des anomalies : résumé des anomalies notifiées pour ce travail
- Reçu : date à laquelle l'anomalie est notifiée
- État de vérification : indique si le faux positif est signalé pour cette anomalie ou non
- Nom de politique : nom de politique du travail de sauvegarde associé
- Nom de planification : nom de planification du travail de sauvegarde associé
- Type de planification : type de planification du travail de sauvegarde associé

3 Développez une ligne pour consulter les détails de l'anomalie sélectionnée.

Pour chaque enregistrement d'anomalie, la valeur actuelle de cette fonction et sa plage réelle basée sur les données passées s'affichent.

Considérez l'exemple suivant :

Une anomalie de taille d'image affiche 100 Mo (contre 350 à 450 Mo habituellement). L'anomalie ainsi signalée laisse entendre que la taille de l'image est de seulement 100 Mo, alors qu'elle est habituellement comprise entre 350 et 450 Mo, sur la base de l'analyse des données passées. En raison de la différence significative entre la taille actuelle des images et la plage habituelle, NetBackup envoie une notification d'anomalie.

Configuration de la détection automatique d’anomalies

Le flux de détection d’anomalies peut déclencher une analyse antimalware pour identifier les anomalies graves. Vous devez utiliser le fichier de configuration pour configurer les paramètres requis.

Pour activer l'analyse automatique des images sur lesquelles une anomalie a été détectée

1. Créez le fichier de configuration suivant :

   `/usr/openv/var/global/anomaly_detection/anomaly_config.conf`

2. Ajoutez le contenu suivant au fichier de configuration `anomaly_config.conf` :

```
#Use this setting to start malware scan on anomaly detected image
automatically.

[AUTOMATED_MALWARE_SCAN_SETTINGS]

ENABLE_AUTOMATED_SCAN=1

# Enable all clients. In this case pool mentioned
SCAN_HOST_POOL_NAME will be used for clients not mentioned

# under batch

ENABLE_ALL_CLIENTS=1

SCAN_HOST_POOL_NAME=<scan_host_pool_name> # Default pool name

#Use specific pool for mentioned clients

NUM_CLIENTS_BATCH_SPECIFIED=2

ENABLE_SCAN_ON_SPECIFIC_CLIENT_1=client1,client2

SCAN_HOST_POOL_NAME_1=<scan_host_pool_for_batch_1>

ENABLE_SCAN_ON_SPECIFIC_CLIENT_2=client3,client4

SCAN_HOST_POOL_NAME_2=<scan_host_pool_for_batch_2>
```

3 Assurez-vous que tous les paramètres sont spécifiés sous `[AUTOMATED_MALWARE_SCAN_SETTINGS]`. Consultez les descriptions de paramètres suivantes :

`ENABLE_AUTOMATED_SCAN=1`

Lance l'analyse antimalware sur les images présentant un score élevé d'anomalies.

`ENABLE_ALL_CLIENTS=1`

Sélectionne tous les clients pour l'analyse. Si la valeur de ce paramètre est 0, seuls les clients spécifiés sous le paramètre suivant sont analysés :
`ENABLE_SCAN_ON_SPECIFIC_CLIENT_<Batch_Number>`

`NUM_CLIENTS_BATCH_SPECIFIED=<batches>`

Spécifie le nombre de lots pour un pool d'hôtes d'analyse différent.

Utilisez ce paramètre, par exemple, si vous souhaitez utiliser un pool d'hôtes d'analyse spécifique pour un ensemble de clients.

Chapitre 27

Détection de malwares

Ce chapitre traite des sujets suivants :

À propos de la détection de malwares

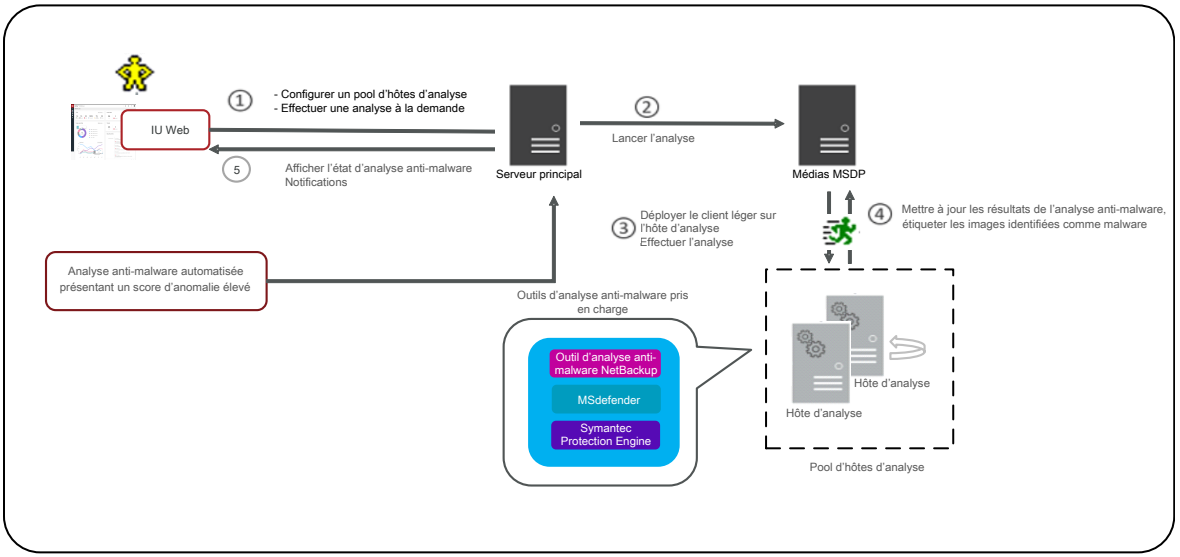
NetBackup détecte les malwares dans les images de sauvegarde prises en charge et trouve la dernière image connue saine (ne contenant aucun malware).

La détection de malwares offre les avantages suivants :

- Vous pouvez sélectionner une ou plusieurs images de sauvegarde des types de politiques pris en charge pour l'analyse à la demande. Vous pouvez utiliser une liste prédéfinie d'hôtes d'analyse.
- Si un malware est détecté pendant l'analyse, une notification est affichée dans l'interface utilisateur Web.

Le workflow de détection de malwares est le suivant :

Figure 27-1 Workflow de détection de malwares



- Le serveur principal vérifie que les images de sauvegarde concernées sont éligibles pour l'analyse. Le serveur principal vérifie qu'elles disposent d'une copie compatible avec la fonction d'accès instantané et que le type de politique est pris en charge.

  Remarque : Les images de sauvegarde dont la validation a échoué sont ignorées.

- Une fois les images de sauvegarde en file d'attente pour l'analyse à la demande, le serveur principal identifie le serveur de stockage et crée un montage avec accès instantané pour le type de partage configuré spécifié dans le pool d'hôtes d'analyse.

- Le serveur principal demande au serveur de médias disponible de lancer l'analyse antimalware sur l'hôte d'analyse.
- L'hôte d'analyse procède au montage avec accès instantané sur l'hôte d'analyse et lance l'analyse à l'aide de l'outil de détection de malwares configuré dans le pool d'hôtes d'analyse.
- Une fois l'analyse terminée, l'hôte d'analyse est démonté et les résultats sont envoyés au serveur de médias. Ensuite, le serveur de médias envoie les résultats au serveur principal.
- Le serveur principal met à jour les résultats de l'analyse et procède au démontage de l'accès instantané.
- Jusqu'à trois analyses peuvent être lancées simultanément sur l'hôte d'analyse.

Workflow de détection et de notification de malwares

Le workflow de détection et de notification de malwares est le suivant :

Tableau 27-1

Description de l'étape	Lien
Installation ou mise à niveau du logiciel NetBackup sur le serveur principal, le serveur de médias et le serveur de stockage MSDP vers la version 10.0 ou une version ultérieure.	Guide d'installation et de mise à niveau de NetBackup
L'accès instantané BYO doit être configuré sur le serveur de stockage MSDP.	Consultez la section Configuration du partage universel du Guide de déduplication Veritas NetBackup™

Description de l'étape	Lien
Configurez le type de partage requis, comme NFS ou SMB. Remarques : ■ Procédez comme suit sur le serveur de stockage MSDP : ■ Paramétrez les configurations NFS et SMB. L'hôte d'analyse doit également inclure un client NFS ou SMB. ■ Pour le partage SMB, assurez-vous de disposer des détails d'un domaine Active Directory et d'un identifiant valide. ■ Assurez-vous que l'utilisateur spécifié dans le type de partage dispose des autorisations de montage requises.	Consultez la section Configuration du partage universel du Guide de déduplication Veritas NetBackup™
Sur l'hôte d'analyse, configurez l'un des outils de détection de malwares suivants : ■ Symantec Protection Engine ■ MS Defender ■ Outil d'analyse antimalware NetBackup **Remarque :** Assurez-vous que l'utilisateur hôte dispose de l'autorisation requise pour lancer l'analyse avec l'outil de détection de malwares configuré et qu'il peut accéder au montage.	Se reporter à "Conditions préalables pour un hôte d'analyse" à la page 632.
Dans l'interface utilisateur Web NetBackup, configurez les paramètres de détection de malwares.	

Conditions préalables pour un hôte d'analyse

L'hôte d'analyse est un ordinateur hôte sur lequel l'outil de détection de malwares requis est configuré. Une fois l'outil intégré à NetBackup, NetBackup lance l'analyse sur l'hôte d'analyse.

Les conditions requises suivantes s'appliquent à l'hôte d'analyse :

- L'outil de détection de malwares doit être installé et configuré.
- Un partage de type client NFS ou SMB doit être configuré sur l'hôte d'analyse.

- L'hôte d'analyse doit être accessible à partir du serveur de stockage MSDP via SSH.

  Remarque : La connexion SSH du serveur de stockage à l'hôte d'analyse doit être établie.

- `OpenSSH` doit être configuré sur l'hôte d'analyse Windows.

  Remarque : Sous Windows 2016, activez OpenSSH. Sous Windows 2019, appliquez les derniers correctifs.

- Configuration minimale requise pour l'hôte d'analyse : processeur 8 cœurs et 32 Go de RAM.
- Les systèmes d'exploitation suivants sont pris en charge pour l'hôte de sauvegarde :
  - Windows Server 2016 et versions ultérieures
  - Linux RHEL versions 8.x et ultérieures
  - SUSE SLES 15 et versions ultérieures

Conditions préalables pour le pool d'hôtes d'analyse

Le pool d'hôtes d'analyse est un groupe d'hôtes d'analyse.

Les configurations de pools d'hôtes d'analyse doivent être effectuées à partir de l'interface utilisateur Web NetBackup une fois l'hôte d'analyse configuré.

- Tous les hôtes d'analyse que vous ajoutez au pool d'hôtes d'analyse doivent être dotés du même outil de détection de malwares que le pool d'hôtes d'analyse.
- Tous les hôtes d'analyse que vous ajoutez au pool doivent être dotés du même type de partage que le pool d'hôtes d'analyse.
- Pour ajouter un hôte d'analyse à un pool d'analyse, vous avez besoin des informations d'authentification de l'hôte d'analyse et de la clé RSA. Pour obtenir la clé RSA de l'hôte d'analyse, consultez la section Se reporter à "Gestion des informations d'authentification" à la page 642..

Outils de détection de malwares pris en charge et leurs configurations

Tableau 27-2 Outils de détection de malwares pris en charge et leurs configurations.

Nom de l'outil de détection de malwares	Plate-forme	Procédure de configuration

Outil d'analyse antimalware NetBackup	Windows	■ Téléchargez l'**outil d'analyse antimalware NetBackup** depuis le centre de téléchargement Veritas
		■ Extrayez les fichiers .zip téléchargés. Les fichiers extraits doivent présenter la structure suivante :
		`NBAntiMalwareClient`
		`Client_1.0`
		`Readme.txt`
		`NBAntiMalwareClient_1.0_AMD64`
		`savapi-sdk-win64.zip`
		`setup.bat`
		`cleanup.bat`
		■ Lisez le fichier `Readme.txt` pour connaître les processus d'installation et de désinstallation.
		Pour installer l'outil d'analyse antimalware NetBackup sur un ordinateur Windows :
		■ Accédez au dossier `NBAntiMalwareClient_1.0_AMD64` et exécutez le fichier `setup.bat`.
		■ Entrez l'emplacement d'installation de l'outil d'analyse antimalware NetBackup.
		Si vous souhaitez désinstaller l'outil d'analyse antimalware NetBackup d'un ordinateur Windows :
		■ Exécutez le fichier `cleanup.bat`.

Nom de l'outil de détection de malwares	Plate-forme	Procédure de configuration
	Linux	

Nom de l'outil de détection de malwares	Plate-forme	Procédure de configuration

		■ Téléchargez l'**outil d'analyse antimalware NetBackup** depuis le centre de téléchargement Veritas
		■ Extrayez le fichier .zip téléchargé. Les fichiers doivent présenter la structure suivante :
		`NBAntiMalwareClient Client_1.0_LinuxR_x86`
		`savapi-sdk-linux64.zip`
		`setup.sh`
		`cleanup.sh`
		`NBAntiMalwareClient_ 1.0_LinuxS_x86 -> NBAntiMalwareClien _1.0_LinuxR_x86`
		`savapi-sdk-linux64.zip`
		`setup.sh`
		`cleanup.sh`
		■ Lisez le fichier `Readme.txt` pour connaître les processus d'installation et de désinstallation.
		Pour installer l'outil d'analyse antimalware NetBackup sur un ordinateur Linux RHEL :
		■ Accédez au dossier `NBAntiMalwareClient_ 1.0_LinuxR_x86` et exécutez le fichier `setup.sh`.
		■ Entrez l'emplacement d'installation de l'outil d'analyse antimalware NetBackup.
		Pour installer l'outil d'analyse antimalware NetBackup sur un ordinateur Linux SUSE :
		■ Accédez au dossier `NBAntiMalwareClient_1.0_LinuxS_x86` et exécutez le fichier `setup.sh`.
		■ Entrez l'emplacement d'installation de l'outil d'analyse

Nom de l'outil de détection de malwares	Plate-forme	Procédure de configuration
		antimalware NetBackup. Si vous souhaitez désinstaller l'outil d'analyse antimalware NetBackup d'un ordinateur Linux : ■ Exécutez le fichier `cleanup.sh`.

Nom de l'outil de détection de malwares	Plate-forme	Procédure de configuration

Symantec Protection Engine	Windows	■ Définissez le chemin d'accès au fichier exécutable de ligne de commande dans la variable d'environnement PATH.
		Par exemple :
		`C:\Program Files \Symantec\Scan Engine\ CmdLineScanner \C`
		■ Exécutez la commande `ssecls -mode scan -scantype S C:\` sur cmd et vérifiez que le résultat est correct.
		Remarque : En cas d'erreur de licence, appliquez les licences mises à jour.
		■ Variable d'environnement du paramètre facultatif SCAN_FILE_BUCKET_SIZE
		Par exemple :
		`SCAN_FILE_BUCKET_SIZE = 40`
		`If SCAN_FILE_BUCKET_SIZE not set then default SCAN_FILE_BUCKET_ SIZE is 20.`

	Linux	

Nom de l'outil de détection de malwares	Plate-forme	Procédure de configuration

		■ Définissez le chemin d'accès au fichier exécutable pour LD_LIBRARY_PATH et PATH dans le fichier `bashrc`.
		Par exemple :
		`export LD_LIBRARY_PATH=/opt/SYMCScan/ssecls/C:/root/clientserver-2.10.97.234/bin`
		`export PATH="$PATH:/Symantec_Protection_Engine_NAS_8.2.0.35_Linux_IN/SPE_NAS/Command_Line_Scanner/C/64_Bit/RedHat"`
		■ Exécutez la commande `ssecls -mode scan -scantype F /` sur cmd et vérifiez que le résultat est correct.
		Remarque : En cas d'erreur de licence, appliquez les licences mises à jour.
		■ Variable d'environnement du paramètre facultatif SCAN_FILE_BUCKET_SIZE
		Par exemple :
		`SCAN_FILE_BUCKET_SIZE = 40`
		`If SCAN_FILE_BUCKET_SIZE not set then default SCAN_FILE_BUCKET_SIZE is 20.`

Nom de l'outil de détection de malwares	Plate-forme	Procédure de configuration

Antivirus Microsoft Defender	Windows	■ Définissez le chemin d'accès au fichier exécutable dans la variable d'environnement **PATH**.
		Par exemple :
		`C:\Program Files\ Windows Defender`
		■ Exécutez la commande dans l'invite de commande `MpCmdRun -Scan -ScanType 3 -DisableRemediation -File <filepath>' check if result is proper`
		Par exemple :
		`C:\Program Files\Windows Defender> MpCmdRun -Scan -ScanType 3 -DisableRemediation -File "C:\Program Files\Windows Defender" Scan starting... Scan finished. Scanning C:\Program Files \Windows Defender found no threats.`

Configuration d'un nouveau pool d'hôtes d'analyse

1. Sur la gauche, cliquez sur **Détection et rapports > Détection de malwares**.
2. Sur la page **Détection de malwares**, cliquez sur **Configurer un pool d'hôtes d'analyseur** pour accéder à la page de liste de pools d'hôtes.

   Pour plus d'informations sur la configuration, consultez le Guide de sécurité et de chiffrement NetBackup.
3. Sur la page **Pools d'hôtes d'analyseur de malware**, cliquez sur **Ajouter** pour ajouter un nouveau pool d'hôtes.

4 Sur la page **Ajouter des pools d'hôtes d'analyseur de malware**, renseignez les informations telles que **Nom du pool d'hôtes**, **Application malveillante** et **Type de partage**.

5 Cliquez sur **Enregistrer et ajouter des hôtes**.

Ajout d'un nouvel hôte à un pool d'hôtes d'analyse

Procédez comme suit pour ajouter un nouvel hôte d'analyse au pool d'hôtes d'analyse configuré.

Remarque : Pour configurer un nouvel hôte d'analyse, consultez la rubrique Se reporter à "Conditions préalables pour le pool d'hôtes d'analyse" à la page 633.

---

1 Sur la gauche, cliquez sur **Détection et rapports > Détection de malwares**.

2 Cliquez sur la page **Détection de malwares**, puis sur **Paramètres de détection de malwares** dans le coin supérieur droit.

3 Sur la page **Pools d'hôtes d'outil d'analyse antimalware**, sélectionnez le pool d'hôtes d'analyse de votre choix et cliquez sur **Gérer les hôtes** dans le menu Action.

4 Sur la page **Gérer les hôtes d'outil d'analyse antimalware**, cliquez sur **Ajouter**.

5 Sur la page **Ajouter un hôte d'outil d'analyse antimalware**, entrez le **nom de l'hôte**.

6 Cliquez sur **Enregistrer** ou sur **Enregistrer et gérer les informations d'authentification** pour mettre à jour les informations d'authentification. Se reporter à "Gestion des informations d'authentification" à la page 642.

Ajout d'un hôte d'analyse existant

Procédez comme suit pour ajouter un hôte d'analyse existant à un autre pool d'hôtes d'analyse du même type de partage.

Pour configurer un hôte d'analyse existant

1 Sur la gauche, cliquez sur **Détection et rapports > Détection de malwares**.

2 Cliquez sur la page **Détection de malwares**, puis sur **Paramètres de détection de malwares** dans le coin supérieur droit.

3. Sur la page **Pools d'hôtes d'outil d'analyse antimalware**, sélectionnez le pool d'hôtes d'analyse de votre choix et cliquez sur **Gérer les hôtes** dans le menu Action.
4. Sur la page **Gérer les hôtes d'outil d'analyse antimalware**, cliquez sur **Ajouter un hôte existant** pour sélectionner un hôte préexistant.

   Remarque : La liste inclut tous les hôtes d'analyse de tous les pools d'hôtes d'analyse.

5. Dans la fenêtre **Ajouter un hôte d'outil d'analyse antimalware existant**, sélectionnez le ou les hôtes d'analyse souhaités.
6. Cliquez sur **Ajouter**.

Gestion des informations d'authentification

Ajout de nouvelles informations d'authentification

1. Sur la page **Gérer les informations d'authentification**, sélectionnez **Ajouter de nouvelles informations d'authentification** et cliquez sur **Suivant**.
2. Sur la page **Gérer les informations d'authentification**, ajoutez les informations telles que le **nom des informations d'authentification**, la **balise** et la **description**.
3. Dans l'onglet **Informations d'authentification d'hôte**, ajoutez le **nom d'utilisateur de l'hôte**, le **mot de passe de l'hôte**, le **port SSH**, la **clé RSA**et le **type de partage**, .

   Remarque : Pour obtenir la clé RSA pour l'hôte d'analyse distant, utilisez `ssh-keyscan <remove_host_name> 2>/dev/null | grep ssh-rsa | awk '{print $3}' | base64 -d | sha256sum` sur le stockage MSDP Linux ou le serveur de médias.

4. Pour le partage de type **SMB**, entrez des informations supplémentaires telles que le **domaine Active Directory**, le **groupe Active Directory**, l'**utilisateur Active Directory** et le **mot de passe**.
5. Cliquez sur **Enregistrer**.

Sélection d'informations d'authentification existantes

1. Sur la page **Gérer les informations d'authentification**, sélectionnez **Sélectionner des informations d'authentification existantes** et cliquez sur **Suivant**.
2. Dans l'onglet **Sélectionner des informations d'authentification**, sélectionnez les informations d'authentification désirées et cliquez sur **Enregistrer**.

Suppression de l'hôte d'analyse

1. Sur la gauche, cliquez sur **Détection et rapports > Détection de malwares**.
2. Cliquez sur la page **Détection de malwares**, puis sur **Paramètres de détection de malwares** dans le coin supérieur droit.
3. Sur la page **Pools d'hôtes d'outil d'analyse antimalware**, sélectionnez le pool d'hôtes d'analyse de votre choix et cliquez sur **Gérer les hôtes** dans le menu Action.
4. Sélectionnez l'hôte de votre choix et cliquez sur **Supprimer**.

Désactivation de l'hôte d'analyse

1. Sur la gauche, cliquez sur **Détection et rapports > Détection de malwares**.
2. Cliquez sur la page **Détection de malwares**, puis sur **Paramètres de détection de malwares** dans le coin supérieur droit.
3. Sur la page **Pools d'hôtes d'outil d'analyse antimalware**, sélectionnez le pool d'hôtes d'analyse de votre choix et cliquez sur **Gérer les hôtes** dans le menu Action.
4. Sélectionnez l'hôte de votre choix et cliquez sur **Désactiver**.

Analyse antimalware

Vous pouvez lancer une analyse pour détecter les malwares.

1. Sur la gauche, cliquez sur **Détection et rapports > Détection de malwares**.
2. Sur la page **Détection de malwares**, cliquez sur **Analyser maintenant**.

3 Sur la page **Analyse de malware**, sélectionnez **Politique standard** ou **Politique Windows** le cas échéant.

Remarque : Les résultats de la recherche sont mis à jour en fonction de la politique sélectionnée.

4 Dans le tableau **Client**, sélectionnez un client à analyser.

5 Cliquez sur **Suivant**.

6 Dans la liste **Sélectionner la période des sauvegardes**, vérifiez la plage de dates et d'heures, et modifiez-la si nécessaire.

Remarque : Selon les critères de sélection, l'analyse est lancée sur 100 images au maximum.

7 Dans la section **Sélectionner un pool d'hôtes d'analyseur de malware**, **sélectionnez** le nom de pool d'hôtes approprié.

8 Dans **Sélectionner l'état des résultats de l'analyse de malware pour les images à analyser**, choisissez l'une des options suivantes :

- **Non analysé**
- **Non affecté**
- **Affecté**
- **Tout**

9 Cliquez sur **Analyser maintenant**.

Remarque : Le flux de détection vous permet de sélectionner une plage de dates et d'autres filtres. Après avoir appliqué tous les filtres, les 100 premières images sont analysées. Si le nombre d'images est supérieur à 100, l'utilisateur doit analyser les images restantes en appliquant les mêmes filtres.

Remarque : La fonction d'analyse antimalware sur l'hôte peut lancer l'analyse de trois images en même temps.

10 Une fois la détection lancée, accédez à **Détection de malwares**, puis à **Progression de la détection de malwares** pour afficher les champs suivants :

- **Non analysé**

- **Non affecté**
- **Affecté**
- **Echec**

Remarque : Passez la souris sur une info-bulle d'état indiquant un échec de l'analyse pour en afficher la raison.

Remarque : Les images de sauvegarde dont la validation a échoué sont ignorées. L'analyse antimalware est prise en charge pour les images de sauvegarde enregistrées sur le stockage MSDP avec la fonction d'accès instantané pour les types de politiques pris en charge uniquement.

Flux de récupération pour l'analyse de malware

Pour les images de sauvegarde, l'état d'analyse de malware s'affiche dans l'assistant de récupération. Si une image sélectionnée est affectée, NetBackup affiche un avertissement à l'utilisateur avant de démarrer la récupération. Pour en savoir plus sur la récupération, consultez les guides d'administrateur de l'interface utilisateur Web de charge de travail respectifs.

SI les données analysées sont infectées, utilisez la CLI `bpcleanrestore` pour restaurer les données nettoyées. Pour plus d'informations, consultez le *Guide de référence des commandes NetBackup*.

Configuration du délai d'expiration de l'analyse de malware pour le serveur NetBackup

`MALWARE_SCAN_OPERATION_TIMEOUT` permet de configurer la durée d'analyse autorisée avant l'expiration de l'opération.

L'analyse de l'image de sauvegarde peut prendre un certain temps en fonction de facteurs tels que la taille et le nombre de fichiers de la sauvegarde. Par défaut, l'analyse expire après deux jours. Pour le délai d'expiration, l'utilisateur peut définir une valeur comprise entre 1 heure et 30 jours.

Tableau 27-3 Informations sur l'option MALWARE_SCAN_OPERATION_TIMEOUT

Utilisation	Description
Où l'utiliser	Vous devez définir la clé de configuration sur le serveur de médias MSDP sur lequel `ScanManager`(nbcs) est démarré. Si vous disposez de plusieurs serveurs de médias MSDP, la clé de configuration doit être définie sur chacun d'eux.
Comment l'utiliser	Utilisez la commande `nbgetconfig` ou `nbsetconfig` pour afficher, ajouter ou modifier la valeur du délai d'expiration. Cette valeur doit être spécifiée en minutes comme suit. **MALWARE_SCAN_OPERATION_TIMEOUT = 120** Par défaut, le délai d'expiration de l'opération d'analyse est de 2 880 minutes (2 jours). La valeur admise est comprise entre 60 minutes (1 heure) et 43 200 minutes (30 jours).
Propriété équivalente dans la console d'administration	Aucun équivalent n'existe dans les propriétés d'hôte de la console d'administration NetBackup.