

Guide de l'administrateur de sauvegarde de l'interface utilisateur Web NetBackup

Version 8.1.2

VERITAS™

Guide de l'administrateur de l'interface utilisateur Web NetBackup

Dernière mise à jour : 2018-10-20

Version du document : NetBackup 8.1.2

Mentions légales

Copyright © 2018 Veritas Technologies LLC. Tous droits réservés.

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

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

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

Le produit décrit dans ce document est distribué dans le cadre de licences limitant son utilisation, sa copie, sa distribution et sa décompilation ou son ingénierie inverse. Vous ne pouvez reproduire aucune partie de ce document sous quelque forme ou par quelque moyen que ce soit sans avoir reçu au préalable l'autorisation écrite de Veritas Technologies LLC et de ses ayants droit éventuels.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET L'ENTREPRISE N'ASSUME AUCUNE RESPONSABILITÉ QUANT À UNE GARANTIE OU CONDITION D'AUCUNE SORTE, EXPRESSE OU IMPLICITE, Y COMPRIS TOUTES GARANTIES OU CONDITIONS IMPLICITES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER OU DE RESPECT DES DROITS DE PROPRIÉTÉ INTELLECTUELLE, DANS LA MESURE OÙ CETTE CLAUSE D'EXCLUSION DE RESPONSABILITÉ RESPECTE LA LOI EN VIGUEUR. VERITAS TECHNOLOGIES LLC NE PEUT ETRE TENUE RESPONSABLE DES DOMMAGES INDIRECTS OU ACCESSOIRES LIES A LA FOURNITURE, AUX PERFORMANCES OU A L'UTILISATION DE CETTE DOCUMENTATION. LES INFORMATIONS CONTENUES DANS CETTE DOCUMENTATION SONT SUJETTES A MODIFICATION SANS PREAVIS.

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

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

<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 :

Dans le monde entier (sauf le 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 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/>

Services and Operations Readiness Tools (SORT) de Veritas

SORT (Services and Operations Readiness Tools) de Veritas est un site web qui fournit de l'information et des outils pour automatiser et simplifier certaines tâches administratives qui prennent du temps. 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, voyez la fiche de données :

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

Table des matières

Chapitre 1	Présentation de l'interface utilisateur Web NetBackup	7
	À propos de l'interface utilisateur Web NetBackup	7
	Terminologie	10
	Connexion à un serveur maître NetBackup à partir de l'interface utilisateur Web	12
	Tableau de bord NetBackup	13
Chapitre 2	Gestion des plans de protection	14
	Création d'un plan de protection	14
	Modifier ou supprimer un plan de protection	17
	Abonnement d'un bien ou d'un groupe de biens à un plan de protection	18
	Désabonner un bien d'un plan de protection	18
	À propos des politiques classiques NetBackup	19
	Tâches de l'administrateur de sauvegarde pour les plans de protection VMware	21
Chapitre 3	Gestion des travaux	22
	Surveillance des travaux	22
	Travaux : annulation, interruption, redémarrage, reprise, suppression	23
	Filtrage des travaux dans la liste des travaux	23
Chapitre 4	Configuration des notifications par courrier électronique pour les alertes	25
	À propos des alertes NetBackup	25
	Comment configurer des notifications par courrier électronique pour les alertes	26
	Conditions requises	27
	À propos des codes d'état pris en charge pour les alertes	27
	Configuration des notifications de messagerie	28

Chapitre 5	Rapports d'utilisation et licence de capacité	30
	Connaître la taille des données de sauvegarde sur les serveurs maîtres	30
	Établissez une relation de confiance entre les serveurs maîtres pour activer les rapports d'utilisation pour les serveurs maîtres distants sans connexion Internet	32
	Ajout de serveurs à une liste de serveurs pour autoriser les rapports d'utilisation pour les serveurs maîtres sans connexion Internet	34

Présentation de l'interface utilisateur Web NetBackup

Ce chapitre traite des sujets suivants :

- [À propos de l'interface utilisateur Web NetBackup](#)
- [Terminologie](#)
- [Connexion à un serveur maître NetBackup à partir de l'interface utilisateur Web](#)
- [Tableau de bord NetBackup](#)

À propos de l'interface utilisateur Web NetBackup

NetBackup 8.1.2 est doté d'une nouvelle interface utilisateur Web qui propose les fonctions suivantes :

- L'accès au serveur maître à partir d'un navigateur Web, y compris Chrome et Firefox.
Pour plus de détails sur les navigateurs pris en charge pour l'interface utilisateur Web, consultez la [liste de compatibilité logicielle NetBackup](#).
- Un tableau de bord qui donne un aperçu rapide des informations qui sont importantes pour vous.
- Un contrôle des accès en fonction des rôles (RBAC) qui permet à l'administrateur de configurer l'accès utilisateur à NetBackup et de déléguer les tâches liées à la sécurité, à la gestion des sauvegardes ou à la protection des charges de travail.
- Les administrateurs de sécurité NetBackup peuvent gérer la sécurité NetBackup, les certificats et RBAC.

- Les administrateurs de sauvegarde fournissent des services de protection pour remplir leurs objectifs de niveau de service (SLO). La protection des biens est assurée grâce aux plans de protection, à la gestion des travaux et à la visibilité de l'état de protection des biens.
- Les administrateurs de charge de travail peuvent abonner des biens à des plans de protection conformes aux objectifs de niveau de service, surveiller l'état de protection et effectuer une récupération en libre-service des machines virtuelles. Dans NetBackup 8.1.2, les administrateurs de charge de travail peuvent gérer et configurer les charges de travail cloud et VMware.
- Les rapports d'utilisation contrôlent la taille des données de sauvegarde sur vos serveurs maîtres. Vous pouvez aussi vous connecter facilement au compteur intelligent de Veritas pour afficher et gérer les licences NetBackup.

Contrôle d'accès dans l'interface utilisateur Web NetBackup

NetBackup utilise le contrôle d'accès en fonction des rôles pour accorder l'accès à l'interface utilisateur Web. Ce contrôle d'accès définit les tâches qu'un utilisateur peut effectuer et les biens qu'il peut afficher et gérer. Le contrôle d'accès est assuré à l'aide de règles d'accès.

- Les règles d'accès associent un utilisateur ou un groupe d'utilisateurs à un rôle et à un groupe d'objets. Le rôle définit les autorisations dont dispose un utilisateur. Un groupe d'objets définit les biens et les objets NetBackup auxquels un utilisateur peut accéder. Vous pouvez créer plusieurs règles d'accès pour un utilisateur ou un groupe unique, permettant une personnalisation complète et flexible de l'accès utilisateur.
- NetBackup comporte trois rôles par défaut. Vous pouvez choisir celui qui répond le mieux aux besoins d'un utilisateur ou créer un rôle personnalisé tenant compte des exigences propres à cet utilisateur.
- Les groupes d'objets permettent de définir des groupes de serveurs d'application ou de biens, mais aussi d'indiquer les plans de protection que les utilisateurs peuvent afficher ou gérer. Par exemple, vous pouvez accorder des droits d'accès aux administrateurs VMware en créant un groupe d'objets contenant des serveurs d'application VMware spécifiques. Vous pouvez aussi ajouter au groupe d'objets les plans de protection spécifiques que l'administrateur VMware peut choisir afin de protéger les biens VMware.
- RBAC est disponible uniquement pour l'interface utilisateur Web et les API. Les autres méthodes de contrôle d'accès pour NetBackup ne sont pas prises en charge pour les API ni par l'interface utilisateur Web, à l'exception de l'audit amélioré (EA). Les utilisateurs qui sont configurés avec l'audit amélioré ont des autorisations complètes pour les API et l'interface utilisateur Web. Vous ne

ne pouvez pas utiliser l'interface utilisateur Web si le contrôle d'accès à NetBackup (NBAC) est activé.

Surveiller les travaux et les événements NetBackup

L'interface utilisateur Web NetBackup permet aux administrateurs de sécurité et de sauvegarde de surveiller plus facilement les événements et les opérations NetBackup afin de repérer les problèmes qui requièrent votre attention.

- Le tableau de bord permet à l'administrateur de sécurité NetBackup de consulter l'état des certificats de sécurité et des événements d'audit.
- Il permet aussi à l'administrateur de sauvegarde de consulter l'état des travaux NetBackup. Les notifications par courrier électronique peuvent également être configurées de sorte à ce que ces administrateurs reçoivent des notifications en cas d'échecs de travaux. NetBackup prend en charge tout système d'émission de tickets pouvant recevoir des courriers électronique entrants.

Plans de protection : un emplacement pour configurer les planifications, le stockage et les options de stockage

Les plans de protection offrent les avantages suivants :

- Outre la planification des sauvegardes, un plan de protection peut inclure une planification pour la réplication et la conservation à long terme.
- Vous pouvez facilement choisir entre un stockage sur site ou par snapshot.
- Lorsque vous sélectionnez le stockage disponible, toutes les fonctions supplémentaires disponibles pour ce stockage s'affichent. Par exemple, l'accélérateur ou l'accès instantané NetBackup pour le stockage de sauvegarde. Pour le stockage à long terme, le fournisseur cloud, CloudCatalyst, le chiffrement ou la compression.
- L'assistant Plan de protection vous aide à sélectionner le stockage pour les sauvegardes, la réplication ou le stockage à long terme en fonction du stockage pris en charge qui a été configuré.
- L'administrateur de sauvegarde crée et gère les plans de protection. Par conséquent, il est responsable du stockage et de la planification des sauvegardes.
- L'administrateur de charge de travail choisit principalement les plans de protection à utiliser pour protéger les biens ou les groupes de biens. Cependant, l'administrateur de sauvegarde peut également protéger les biens en les abonnant à des plans de protection si nécessaire.

Récupération en libre-service

L'interface utilisateur Web de NetBackup facilite la récupération des machines virtuelles. Vous pouvez également utiliser la fonction d'accès instantanée pour monter un snapshot d'une machine virtuelle pour un accès immédiat à ses fichiers : vous pouvez télécharger le fichier sur l'hôte local ou restaurer le fichier vers sa machine virtuelle d'origine.

Terminologie

Le tableau suivant décrit les concepts et les termes introduits dans la nouvelle interface utilisateur Web.

Tableau 1-1 Concepts et terminologie de l'interface utilisateur Web

Terme	Définition
Règle d'accès	Pour RBAC, définit un utilisateur ou un groupe d'utilisateurs, le rôle ou les autorisations, et le groupe d'objets auxquels l'utilisateur ou le groupe d'utilisateurs peut accéder. Un utilisateur ou un groupe peut avoir plusieurs règles d'accès.
Administrateur	Utilisateur disposant de l'ensemble des autorisations et des droits d'accès dans NetBackup et dans toutes les interfaces, y compris l'interface utilisateur Web NetBackup. L'utilisateur racine, l'administrateur et l'utilisateur de l'audit amélioré ont tous un accès complet à NetBackup. Dans les guides <i>de l'interface utilisateur Web NetBackup</i> , le terme <i>administrateur NetBackup</i> se rapporte également à un utilisateur qui dispose des autorisations complètes pour NetBackup, généralement un utilisateur de la console d'administration NetBackup. Voir également le terme <i>Rôle</i> .
Groupe de biens	Voir le terme <i>Groupe intelligent</i> .
Bien	Données devant être protégées, telles que les clients physiques, les machines virtuelles et les applications de base de données.
Politique classique	Dans l'interface utilisateur Web NetBackup, indique qu'une politique héritée protège le bien. Les politiques héritées sont créées avec la console d'administration NetBackup.

Terme	Définition
Groupe intelligent	<p>Permet à NetBackup de sélectionner automatiquement des biens à protéger en fonction de critères (requêtes) que vous spécifiez. Les modifications apportées dans l'environnement de production sont automatiquement appliquées dans le groupe intelligent. Ces groupes sont également appelés groupes de biens.</p> <p>Pour VMware, ces groupes se trouvent sous l'onglet Groupes de machines virtuelles intelligents.</p>
Accès instantané	<p>Une machine virtuelle avec accès instantané créée à partir d'une image de sauvegarde NetBackup est disponible presque instantanément, réalisant ainsi un objectif de temps de récupération proche de zéro. NetBackup monte le snapshot de la machine virtuelle directement sur le périphérique de stockage de la sauvegarde pour autoriser le cluster ou l'hôte ESXi à traiter le snapshot comme une machine virtuelle normale.</p>
Groupe d'objets	<p>Pour RBAC, collection de biens, de plans de protection, de serveurs et d'autres biens auxquels l'utilisateur a accès.</p>
Plan de protection	<p>Un plan de protection définit le moment d'exécution des sauvegardes, le temps pendant lequel elles sont conservées ainsi que le type de stockage à utiliser. Une fois qu'un plan de protection est configuré, vous pouvez y abonner des biens.</p>
RBAC	<p>Contrôle d'accès en fonction des rôles. Les administrateurs peuvent déléguer ou limiter l'accès à l'interface utilisateur Web NetBackup via les règles d'accès qui sont configurées dans RBAC.</p> <p>Remarque : Les règles que vous configurez dans RBAC ne contrôlent pas l'accès aux interfaces de ligne de commande ou à la console d'administration NetBackup. L'interface utilisateur Web n'est pas prise en charge avec le contrôle d'accès à NetBackup (NBAC) et ne peut pas être utilisée si NBAC est activé.</p>
Rôle	<p>Pour RBAC, définit les autorisations qu'un utilisateur peut avoir. NetBackup a trois rôles définis par le système qui permettent aux utilisateurs de gérer la sécurité, les plans de protection et les sauvegardes, ou de gérer les biens de la charge de travail.</p>
Stockage	<p>Stockage sur lequel les données sont sauvegardées, répliquées ou dupliquées (pour la conservation à long terme). Le stockage de snapshot est utilisé pour les charges de travail sur le cloud.</p>

Terme	Définition
Abonner (à un plan de protection)	Action d'associer un bien ou un groupe de biens à un plan de protection. Le bien est protégé en fonction de la planification et des paramètres de stockage définis dans le plan. Dans l'interface utilisateur Web, l'action d' <i>abonnement</i> est également appelée <i>configuration de la protection</i> . <i>Désabonner</i> signifie supprimer un bien d'un plan.
Charge de travail	Type de bien. Par exemple, VMware ou cloud.
Workflow	Processus de bout en bout qui peut être exécuté à l'aide de l'interface utilisateur Web NetBackup. Par exemple, vous pouvez protéger et récupérer des biens VMware et cloud dans NetBackup 8.1.2.

Connexion à un serveur maître NetBackup à partir de l'interface utilisateur Web

Les utilisateurs peuvent se connecter à un serveur maître NetBackup à partir d'un navigateur Web via l'interface utilisateur Web NetBackup. Pour plus de détails sur les navigateurs pris en charge pour l'interface utilisateur Web, consultez la [liste de compatibilité logicielle NetBackup](#).

Les utilisateurs doivent posséder des droits d'administrateur ou racine ou posséder un rôle configuré pour eux dans le Contrôle des accès basé sur le rôle (RBAC) NetBackup.

Pour se connecter à un serveur maître NetBackup à l'aide de l'interface utilisateur Web NetBackup

- 1 Ouvrez un navigateur Web et accédez à l'URL suivante.

`https://masterserver/webui/login`

masterserver est le nom d'hôte ou adresse IP du serveur maître NetBackup auquel vous voulez vous connecter.

- 2 Entrez vos informations d'authentification et cliquez sur **Se connecter**.

Exemple :

Pour ce type d'utilisateur	Utilisez ce format	Exemple
Utilisateur local	<i>username</i>	racine
Utilisateur de domaine	<i>DOMAIN\username</i>	WINDOWS\Administrator

Tableau de bord NetBackup

Le tableau de bord NetBackup donne un aperçu rapide des détails liés à votre rôle dans votre société.

Tableau 1-2 Tableau de bord NetBackup pour l'administrateur de sauvegarde

Widget de tableau de bord	Description
Travaux	Fournit une liste d'informations sur les travaux, y compris le nombre de travaux actifs et en file d'attente, et l'état des travaux lancés et terminés.
Rapport d'utilisation	<p>Répertorie la taille des données de sauvegarde pour les serveurs maîtres NetBackup dans votre organisation. Ce rapport est utile pour le suivi des licences basées sur la capacité. Utilisez les listes déroulantes dans la partie supérieure droite pour sélectionner la période et la vue que vous souhaitez afficher. Cliquez sur le nom d'un serveur pour en consulter les détails spécifiques.</p> <p>Vous pouvez également accéder à des détails supplémentaires sur la manière de configurer NetBackup de sorte à afficher les informations sur le serveur maître dans ce widget.</p> <p>Se reporter à "Connaître la taille des données de sauvegarde sur les serveurs maîtres" à la page 30.</p>

Gestion des plans de protection

Ce chapitre traite des sujets suivants :

- [Création d'un plan de protection](#)
- [Modifier ou supprimer un plan de protection](#)
- [Abonnement d'un bien ou d'un groupe de biens à un plan de protection](#)
- [Désabonner un bien d'un plan de protection](#)
- [À propos des politiques classiques NetBackup](#)
- [Tâches de l'administrateur de sauvegarde pour les plans de protection VMware](#)

Création d'un plan de protection

Un plan de protection définit le moment d'exécution des sauvegardes, le temps pendant lequel elles sont conservées ainsi que le type de stockage à utiliser. Une fois que vous avez configuré un plan de protection, vous pouvez abonner des biens à ce plan.

Avant de créer un plan de protection, vous devez configurer toutes les options de stockage. Vous pouvez configurer ces options de stockage dans la console d'administration NetBackup. Consultez la procédure suivante (étape 8) pour connaître les types d'options de stockage configurables.

Pour créer un plan de protection

- 1 Sur la gauche, cliquez sur **Plans de protection**, puis sur **Créer**.
- 2 Entrez un **nom** et une **description** pour le plan, puis cliquez sur **Suivant**.

- 3** Dans **Planifier les sauvegardes**, sélectionnez la fréquence à laquelle vous voulez que cette planification s'exécute et la durée de conservation de la sauvegarde.

Cliquez sur **Enregistrer** pour terminer cette planification. Si vous voulez ajouter une autre planification de sauvegarde, cliquez sur **Enregistrer et en ajouter une autre**.
- 4** (Facultatif) Pour répliquer la sauvegarde, activez l'option **Répliquer**.

Pour utiliser l'option **Répliquer**, le stockage de sauvegarde doit être une source dans un environnement AIR ciblé. La **cible de réplication** est configurée à l'étape 8.

Pour plus d'informations sur la réplication, consultez *À propos de NetBackup Auto Image Replication (AIR)* dans le [Guide de l'administrateur NetBackup, volume I](#).
- 5** Vous pouvez régler la **fenêtre de démarrage de sauvegarde** afin de définir à quel moment les sauvegardes démarrent.

Les sauvegardes peuvent démarrer à tout moment pendant la journée, mais la planification affiche les fenêtres par défaut lors de l'installation. Les fenêtres par défaut du système s'étendent entre 08:00 et 20:00 du lundi au vendredi, et sont ouvertes le samedi et le dimanche. Vous pouvez conserver ces fenêtres par défaut ou les modifier pour n'importe quel jour de la semaine. Par ailleurs, les fenêtres de sauvegarde sont appliquées à toutes les planifications.
- 6** (Facultatif) Pour conserver une copie en stockage à long terme, activez l'option **Conserver une copie à long terme**.

NetBackup duplique immédiatement une copie vers le stockage à long terme après la fin de la sauvegarde.

L'option **Conserver une copie à long terme** ne peut être sélectionnée que pour une planification.
- 7** Cliquez sur **Suivant**.

8 Configurez les options de stockage pour ce plan de protection.

Lors de la création d'un plan de protection, sélectionnez uniquement le stockage auquel un serveur de médias NetBackup 8.1.2 ou version plus récente peut accéder.

Option de stockage	Conditions requises	Description
Stockage de snapshot uniquement	CloudPoint est requis pour cette option.	Configurez CloudPoint dans la console d'administration NetBackup à l'aide de la fonction de serveur de gestion de snapshots. Si vous utilisez l'option de stockage de snapshot uniquement, aucune autre option de stockage ne peut être sélectionnée. Passez à l'étape 9.
Stockage de sauvegarde	OpenStorage est requis pour cette option. Les bandes, les groupes d'unités de stockage et Replication Director ne sont pas pris en charge.	<p>Cliquez sur Modifier pour sélectionner la cible de stockage. Après avoir sélectionné la cible de stockage, cliquez sur Utiliser le stockage sélectionné.</p> <p>La fonction d' accélérateur de NetBackup permet d'exécuter les plans de protection plus rapidement que les sauvegardes traditionnelles, en créant un flux de données compact qui utilise moins de largeur de bande réseau. Si le serveur de stockage sur le serveur maître NetBackup prend en charge l'accélérateur NetBackup, cette fonction est incluse dans le plan de protection. Pour plus de détails sur l'accélérateur NetBackup, contactez l'administrateur NetBackup, consultez le Guide de l'administrateur NetBackup, Volume I ou consultez le Guide de l'administrateur NetBackup pour VMware.</p> <p>La fonction d' accès instantané permet à des points de récupération de machines virtuelles du plan de prendre en charge la création de machines virtuelles avec accès instantané.</p>
Cible de réplication	Le stockage de sauvegarde doit être une source dans un environnement AIR ciblé.	Cliquez sur Modifier pour sélectionner le serveur maître cible de réplication. Sélectionnez un serveur maître, puis une politique de cycle de vie du stockage. Cliquez sur Utiliser la cible de réplication sélectionnée pour revenir à l'écran des options de stockage.
Stockage avec conservation à long terme	OpenStorage est requis pour cette option. Les bandes, les groupes d'unités de stockage et Replication Director ne sont pas pris en charge.	Cliquez sur Modifier pour sélectionner le fournisseur de stockage en cloud. Après avoir sélectionné le fournisseur cloud cible, cliquez sur Utiliser le stockage sélectionné .

- 9 Cliquez sur **Suivant**.
- 10 Examinez les détails du plan et cliquez sur **Enregistrer**.

Modifier ou supprimer un plan de protection

Modifier un plan de protection

Vous pouvez apporter des modifications à différents éléments d'un plan de protection. Le **nom**, la **description** et les **options de stockage** peuvent être modifiés.

Pour modifier un plan de protection

- 1 Sur la gauche, cliquez sur **Plans de protection**.
- 2 Cliquez sur le plan de protection que vous voulez modifier.
- 3 Cliquez sur **Modifier** dans la partie supérieure droite de l'écran.
- 4 (Facultatif) Modifiez le **nom** ou la **description** du plan de protection.
- 5 (Facultatif) Cliquez sur **Modifier** pour modifier le **stockage de sauvegarde**, la **cible de réplication** ou le **stockage à long terme**.

Se reporter à "[Création d'un plan de protection](#)" à la page 14.

Supprimer un plan de protection

Avant de supprimer un plan de protection, vous devez en ajouter les biens à un autre plan de protection. Le déplacement des biens vers un autre plan de protection garantit que les données sont protégées sur ces biens protégés par ce plan. Pour supprimer un plan de protection, tous les biens doivent en avoir été supprimés.

Pour supprimer un plan de protection

- 1 Notez le plan de protection (nouveau ou existant) auquel vous voulez ajouter les biens.
Se reporter à "[Création d'un plan de protection](#)" à la page 14.
- 2 Localisez les biens actuellement protégés par le plan que vous voulez supprimer.
- 3 Abonnez ces biens au plan de protection dont vous avez pris note.
Se reporter à "[Abonnement d'un bien ou d'un groupe de biens à un plan de protection](#)" à la page 18.
- 4 Désabonnez les biens du plan de protection que vous voulez supprimer.
- 5 Sur la gauche, cliquez sur **Plans de protection**.

- 6 Sélectionnez le plan de protection que vous voulez supprimer.
- 7 Cliquez sur **Supprimer** dans la partie supérieure droite de l'écran.

Abonnement d'un bien ou d'un groupe de biens à un plan de protection

Vous pouvez abonner un seul bien ou un groupe de biens à un plan de protection. Un bien ou un groupe de biens peut être abonné à plusieurs plans de protection. Pour pouvoir abonner des biens à un plan de protection, vous devez créer un plan de protection.

Remarque : Pour abonner un groupe de biens à un plan de protection, l'**autorisation Gérer les serveurs d'application et les groupes de biens** doit être sélectionnée pour le rôle RBAC.

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

Pour abonner un bien ou un groupe de biens à un plan de protection

- 1 Sur la gauche, cliquez sur le type de charge de travail (par exemple : **VMware**).
- 2 Sélectionnez un type de bien (par exemple : **Machines virtuelles, Groupes de machines virtuelles intelligents**).
- 3 Cochez la case en regard du nom du bien.
- 4 Dans le coin supérieur droit, cliquez sur **Configurer la protection**.
- 5 Sélectionnez un plan de protection dans la liste.
- 6 Examinez les détails du plan de protection.
- 7 Cliquez sur **Protéger**.

Se reporter à "[Création d'un plan de protection](#)" à la page 14.

Désabonner un bien d'un plan de protection

Vous pouvez désabonner des biens individuels ou des groupes de biens d'un plan de protection.

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

Pour désabonner un bien d'un plan de protection

- 1 Sur la gauche, cliquez sur le type de charge de travail (par exemple : **VMware**).
- 2 Sélectionnez un type de bien unique (par exemple : **Machines virtuelles**).
- 3 Cliquez sur le nom du bien.
Si vous cochez la case, vous devez cliquer sur le nom du bien ou sur **Afficher les détails** dans la barre d'outils.
- 4 Dans le plan de protection duquel vous voulez désabonner le bien, cliquez sur **Désabonner du plan de protection**.

Pour désabonner un groupe de biens d'un plan de protection

- 1 Sur la gauche, cliquez sur le type de charge de travail (par exemple : **VMware**).
- 2 Sélectionnez un type de groupe de biens (par exemple : **Groupes de machines virtuelles intelligents**).
- 3 Cliquez sur le nom du groupe de biens.
- 4 Cliquez sur le cadenas situé en bas.
- 5 Cliquez sur **Désabonner** dans le champ **Protégé par**.
- 6 Cliquez sur **Oui** pour confirmer la suppression.

Se reporter à ["Création d'un plan de protection"](#) à la page 14.

Se reporter à ["Modifier ou supprimer un plan de protection"](#) à la page 17.

À propos des politiques classiques NetBackup

Vous pouvez protéger un bien en utilisant une politique classique NetBackup, un plan de protection ou les deux en même temps. Cette rubrique répond aux questions courantes au sujet des politiques classiques NetBackup dans l'interface utilisateur Web NetBackup.

Tableau 2-1 Questions fréquemment posées sur les politiques classiques

Question	Réponse
<p>Dans la colonne Protégé par de l'interface utilisateur Web, que signifie Politique classique uniquement ?</p>	<p>Le bien n'est pas actuellement abonné à un plan de protection. Cependant, il a été abonné à un plan de protection ou couvert par une politique classique à un moment donné et son état est Dernière sauvegarde. Le bien peut ou non être protégé par une politique classique active (contactez l'administrateur NetBackup pour en savoir plus).</p>
<p>Où puis-je trouver les détails d'une politique classique ?</p>	<p>Les détails d'une politique classique ne sont pas visibles dans l'interface utilisateur Web. Pour gérer une politique classique, un administrateur NetBackup peut utiliser la console d'administration NetBackup ou les interfaces de ligne de commande NetBackup. En outre, l'administrateur NetBackup ou l'administrateur de sauvegarde peut gérer et créer des politiques en utilisant les API NetBackup.</p>
<p>Quand dois-je abonner un bien à un plan de protection au lieu de protéger le bien avec une politique classique ?</p>	<p>Seul un administrateur NetBackup peut créer une politique classique. Si vous ne disposez pas des autorisations requises pour abonner les biens aux plans de protection, demandez à l'administrateur de sauvegarde de configurer le plan de protection. L'administrateur de sauvegarde peut choisir de protéger le bien par un plan de protection (interface utilisateur Web) ou par une politique classique (console d'administration).</p>
<p>Puis-je utiliser à la fois un plan de protection et une politique classique pour protéger un bien ?</p>	<p>Oui. L'interface utilisateur Web affiche les détails du plan de protection, mais pas les détails de la politique classique. Vous pouvez contacter l'administrateur NetBackup pour obtenir les détails de la politique classique.</p>
<p>Que dois-je faire quand un bien est désabonné d'un plan de protection et que l'interface utilisateur Web affiche Politique classique uniquement pour ce bien ?</p>	<p>Vous pouvez demander à l'administrateur NetBackup si une politique classique protège le bien.</p>

Tâches de l'administrateur de sauvegarde pour les plans de protection VMware

Les tâches VMware suivantes nécessitent des autorisations d'administrateur de sauvegarde :

- *Ajouter des serveurs VMware et leurs informations d'authentification*
- *Création d'un groupe de machines virtuelles intelligent*
- *Suppression d'un groupe de machines virtuelles intelligent*

Consultez le [Guide de l'administrateur VMware de l'interface utilisateur Web NetBackup](#) pour obtenir des instructions sur ces tâches.

Gestion des travaux

Ce chapitre traite des sujets suivants :

- [Surveillance des travaux](#)
- [Travaux : annulation, interruption, redémarrage, reprise, suppression](#)
- [Filtrage des travaux dans la liste des travaux](#)

Surveillance des travaux

Utilisez le nœud **Travaux** pour surveiller les travaux dans votre environnement NetBackup et afficher les détails d'un travail spécifique.

Pour surveiller un travail

- 1 Cliquez sur **Travaux** et sélectionnez le nom du travail ou cochez la case correspondant au travail à afficher. Vous pouvez sélectionner la case à cocher pour qu'un travail effectue une action particulière, telle que le redémarrage du travail. Dans **Etat**, cliquez sur le code d'état pour afficher le message associé au code.
 - Sélectionnez l'onglet **Vue d'ensemble** pour afficher les informations concernant un travail.
 - L'onglet **Détails** affiche **Liste de fichiers** et **Etat**. La **liste de fichiers** contient les fichiers qui sont inclus dans l'image de sauvegarde. Sélectionnez l'onglet **Détails** pour afficher les détails consignés sur un travail. Vous pouvez filtrer les journaux par type d'erreur. Dans **Etat**, cliquez sur le numéro du code d'état pour afficher les informations au sujet de ce code d'état dans la base de connaissances Veritas.

Consultez le [Guide de référence des codes d'état NetBackup](#).

- 2 Dans cet onglet, vous pouvez effectuer des tâches supplémentaires.

Se reporter à "[Travaux : annulation, interruption, redémarrage, reprise, suppression](#)" à la page 23.

Travaux : annulation, interruption, redémarrage, reprise, suppression

Pour gérer les travaux

- 1 Cliquez sur **Travaux**.
- 2 Sélectionnez un ou plusieurs travaux.
- 3 Le menu supérieur indique les actions que vous êtes en mesure d'effectuer pour les travaux sélectionnés.

Annuler	Vous pouvez annuler les travaux qui ne sont pas encore terminés. Les états possibles pour ces travaux sont les suivants : en file d'attente, replacé dans la file d'attente, actif, inachevé ou interrompu. Lorsqu'un travail parent est annulé, tous ses travaux enfant le sont aussi.
Interrompre	Vous pouvez interrompre les travaux de sauvegarde et de restauration qui contiennent des points de contrôle.
Redémarrer	Vous pouvez redémarrer les travaux qui sont terminés, qui ont échoué ou qui ont été annulés ou interrompus. Un nouvel ID de travail est créé pour le nouveau travail.
Reprendre	Vous pouvez reprendre les travaux qui ont été interrompus ou qui sont inachevés.
Supprimer	Vous pouvez supprimer les travaux qui sont terminés. Lorsqu'un travail parent est supprimé, tous ses travaux enfant le sont aussi.

Filtrage des travaux dans la liste des travaux

Appliquez un filtre pour afficher les travaux ayant un état spécifique. Par exemple, vous pouvez afficher tous les travaux actifs ou tous les travaux interrompus.

Pour filtrer la liste des travaux

- 1** Cliquez sur **Travaux**.
- 2** Au-dessus de la liste des travaux, cliquez sur l'option **Filtrer**.
- 3** Dans la fenêtre **Filtrer**, sélectionnez une option de filtrage afin de modifier de manière dynamique les travaux qui sont affichés. Les options de filtre sont les suivantes :
 - **Tout**
 - **Actif**
 - **Terminé**
 - **Échec**
 - **Inachevé**
 - **Partiellement réussi**
 - **En attente**
 - **Succès**
 - **Interrompu**
 - **En attente de nouvelle tentative**
- 4** Cliquez sur **Appliquer des filtres**.
- 5** Pour supprimer les filtres sélectionnés, cliquez sur **Tout effacer**.

Configuration des notifications par courrier électronique pour les alertes

Ce chapitre traite des sujets suivants :

- [À propos des alertes NetBackup](#)
- [Comment configurer des notifications par courrier électronique pour les alertes](#)
- [Conditions requises](#)
- [À propos des codes d'état pris en charge pour les alertes](#)
- [Configuration des notifications de messagerie](#)

À propos des alertes NetBackup

L'administrateur de sauvegarde peut configurer NetBackup de sorte à envoyer des notifications par courrier électronique en cas d'échecs de travaux. Ces notifications peuvent également être dirigées vers un système d'émission de tickets pris en charge.

Cette fonction évite aux administrateurs NetBackup de perdre du temps à surveiller NetBackup en cas d'échecs de travaux et de créer manuellement des tickets pour effectuer le suivi des problèmes. NetBackup prend en charge les systèmes d'émission de tickets qui utilisent le service de courrier électronique entrant pour

la création de ticket. Par exemple, ServiceNow, Remedy ou HP Service Manager (HPSM).

NetBackup génère des alertes en fonction de certains codes d'état.

Se reporter à ["À propos des codes d'état pris en charge pour les alertes"](#) à la page 27.

Les alertes qui sont similaires ou dont la cause est similaire sont marquées comme des doublons. Aucune notification par courrier électronique n'est envoyée pour les doublons pendant les 24 heures suivant la première alerte. Si l'envoi d'une notification par courrier électronique échoue, NetBackup réessaie de l'envoyer toutes les 2 heures (trois tentatives maximum).

NetBackup effectue l'audit d'un événement si des modifications sont apportées aux paramètres d'alerte, ou s'il ne peut pas générer une alerte ou envoyer une notification par courrier électronique.

Pour plus d'informations, consultez le [Guide de sécurité et de chiffrement NetBackup](#).

Comment configurer des notifications par courrier électronique pour les alertes

Dans certaines situation d'échec des travaux ou lorsque certains codes d'état NetBackup sont détectés, des alertes sont générées et envoyées à votre système d'émission de tickets via des notifications par courrier électronique.

Se reporter à ["À propos des alertes NetBackup"](#) à la page 25.

Se reporter à ["À propos des codes d'état pris en charge pour les alertes"](#) à la page 27.

Le tableau suivant fournit la liste des procédures à suivre pour générer des alertes et des tickets.

Tableau 4-1 Générer des alertes et des tickets NetBackup

Étape	Action	Rubrique de référence
1	Passez en revue les conditions requises.	Se reporter à "Conditions requises" à la page 27.
2	Découvrez les situations ou les codes d'état qui déclenchent l'envoi d'alertes au système d'émission de tickets, sous forme de notifications par courrier électronique.	Se reporter à "À propos des codes d'état pris en charge pour les alertes" à la page 27.

Étape	Action	Rubrique de référence
3	Configurez les notifications par courrier électronique afin que les alertes soient envoyées au système d'émission de tickets.	<p>Remarque : Vous pouvez exclure les codes d'état pour lesquels vous ne voulez pas envoyer de notifications par courrier électronique.</p> <p>Se reporter à "Configuration des notifications de messagerie" à la page 28.</p>
4	Consultez les alertes (ou les tickets) NetBackup dans le système d'émission de tickets.	Connectez-vous au système d'émission de tickets pour consulter les tickets générés par des alertes NetBackup.

Conditions requises

Vérifiez ce qui suit avant de générer des alertes et de les visualiser à l'aide du système d'émission de tickets.

- Le système d'émission de tickets est en cours d'exécution.
- Le serveur SMTP est en cours d'exécution.
- Une politique est configurée dans le système d'émission de tickets pour créer des tickets (ou des incidents) en fonction des messages électroniques entrants envoyés par NetBackup.

À propos des codes d'état pris en charge pour les alertes

NetBackup 8.1.2 prend en charge les alertes pour les échecs de travaux VMware et conserve ces alertes pendant 90 jours. NetBackup génère des alertes pour les codes d'état pris en charge pour les types de tâches suivants : sauvegarde, snapshot, réplication de snapshot, index depuis snapshot et sauvegarde depuis le snapshot. Pour obtenir la liste complète des codes d'état pour lesquels les alertes sont générées, consultez la section « Codes d'état des notifications d'alerte NetBackup » du [Guide de référence des codes d'état NetBackup](#).

[Tableau 4-2](#) indique certaines des situations ou certains des codes d'état pour lesquels les alertes sont générées. Ces alertes sont envoyées au système d'émission de tickets via les notifications par courrier électronique.

Tableau 4-2 Exemples de codes d'état pris en charge

Code d'état	Message d'erreur
10	échec d'affectation
196	la sauvegarde du client n'a pas été tentée car la fenêtre de sauvegarde a été fermée
213	Vous ne pouvez utiliser aucune unité de stockage dans l'immédiat
219	l'unité de stockage requise n'est pas disponible
2001	Aucun lecteur disponible
2074	Le volume de disque est arrêté
2505	Connexion impossible à la base de données
4200	Echec de l'opération : impossible d'acquérir un verrouillage de snapshot
5449	Le script n'est pas approuvé pour l'exécution
7625	Échec de la connexion au socket SSL

Configuration des notifications de messagerie

Vous pouvez configurer NetBackup pour envoyer des notifications par courrier électronique lorsqu'un événement lié à l'échec d'une tâche se produit.

Pour configurer des notifications par courrier électronique

- 1 En haut à droite, cliquez sur **Paramètres > Paramètres de notification d'alerte**.
- 2 Cliquez sur **Notifications par courrier électronique**.
- 3 Activez l'option **Envoyer des notifications par courrier électronique**.
- 4 Entrez les informations de courrier électronique, notamment l'adresse du destinataire, l'adresse de l'expéditeur et le nom de l'expéditeur.
- 5 Entrez les informations du serveur SMTP, notamment son nom et son numéro de port.

Fournissez le nom d'utilisateur et le mot de passe SMTP si vous avez spécifié ces informations d'authentification plus tôt sur le serveur SMTP.
- 6 Cliquez sur **Enregistrer**.

Exclure des codes d'état spécifiques des notifications par courrier électronique

Vous pouvez exclure des codes d'état spécifiques afin qu'aucune notification ne soit envoyée pour ces erreurs.

Pour exclure des codes d'état spécifiques

- 1 En haut à droite, cliquez sur **Paramètres > Paramètres de notification d'alerte**.
- 2 Cliquez sur **Exclure des codes d'état**.
- 3 Entrez les codes d'état ou la plage de codes d'état (séparés par des virgules) pour lesquels vous ne voulez pas recevoir de notifications par courrier électronique.
- 4 Cliquez sur **Enregistrer**.

Exemple de notification par courrier électronique pour une alerte

Une notification par courrier électronique pour une alerte contient des informations sur le serveur maître, la tâche, la politique, la planification et l'erreur. Les courriers électroniques peuvent contenir d'autres informations selon le type de tâche. Par exemple : pour les échecs de tâche VMware, les informations telles que le serveur vCenter et l'hôte ESX sont présentes dans la notification par courrier électronique.

Exemple de notification par courrier électronique :

```

Serveur maître : master1.exemple.com
Nom du client : client1.exemple.com
ID du travail : 50
Heure de début du travail : 2018-05-17 14:43:52.0
Heure de fin du travail : 2018-05-17 15:01:27.0
Type de travail : BACKUP
ID tâche parent : 49
Nom de la politique : Win_policy
Type de politique : WINDOWS_NT
Nom de la planification : schedule1
Type de planification : FULL
Code d'état 2074
Message d'erreur : Volume de disque arrêté
    
```

Rapports d'utilisation et licence de capacité

Ce chapitre traite des sujets suivants :

- [Connaître la taille des données de sauvegarde sur les serveurs maîtres](#)
- [Établissez une relation de confiance entre les serveurs maîtres pour activer les rapports d'utilisation pour les serveurs maîtres distants sans connexion Internet](#)
- [Ajout de serveurs à une liste de serveurs pour autoriser les rapports d'utilisation pour les serveurs maîtres sans connexion Internet](#)

Connaître la taille des données de sauvegarde sur les serveurs maîtres

L'application de rapports d'utilisation indique la taille des données de sauvegarde pour les serveurs maîtres NetBackup de votre organisation. Ces rapports sont utiles pour la planification lorsque vous utilisez des licences basées sur la capacité. Par défaut, NetBackup recueille et signale les informations sur l'utilisation et les tendances une fois par semaine.

Les données des rapports sur l'utilisation sont recueillies par l'intermédiaire des exécutions planifiées de l'utilitaire `nbdeployutil`. Les exécutions planifiées de `nbdeployutil` sont activées par défaut.

Pour plus d'informations, consultez [Planification des rapports sur les licences de capacité](#).

Cette application inclut également un lien vers le **compteur intelligent de Veritas**. Ce portail permet aux clients NetBackup de gérer de façon proactive leur utilisation des licences à l'aide d'une visibilité presque en temps réel sur les tendances de consommation.

Tableau 5-1 Types de politique pris en charge pour les rapports d'utilisation

BigData	Informix	Oracle	VMware
MS-Exchange-Server	MS-SQL-Server	Standard	
Hyper-V	NDMP	Sybase	

Conditions requises

Lorsque les conditions suivantes sont remplies, NetBackup collecte automatiquement les données pour les rapports d'utilisation.

- Vous utilisez des licences basées sur la capacité. Les rapports d'utilisation ne s'appliquent pas à la méthode traditionnelle de gestion des licences.
- Seuls les rapports automatiques planifiés s'affichent dans l'interface utilisateur Web. Si vous générez manuellement les rapports de licences basées sur la capacité, les données ne s'affichent pas dans le rapport d'utilisation de l'interface utilisateur Web NetBackup.

Le fichier suivant doit exister :

UNIX : `/usr/opensv/var/global/incremental/Capacity_Trend.out`

Windows :

`chemin_installation\var\global\incremental\Capacity_Trend.out`

- Si vous voulez qu'un de vos serveurs maîtres recueille les données des rapports sur l'utilisation pour d'autres serveurs maîtres distants, une configuration supplémentaire est requise. Vous devez créer une relation de confiance entre les serveurs maîtres. Vous devez également ajouter le serveur maître local (où vous prévoyez d'exécuter `nbdeployutil`) à la liste des **serveurs** sur chaque serveur maître distant.

Se reporter à "[Ajout de serveurs à une liste de serveurs pour autoriser les rapports d'utilisation pour les serveurs maîtres sans connexion Internet](#)" à la page 34.

Se reporter à "[Établissez une relation de confiance entre les serveurs maîtres pour activer les rapports d'utilisation pour les serveurs maîtres distants sans connexion Internet](#)" à la page 32.

Informations supplémentaires

Consultez le [Guide de l'administrateur NetBackup, Volume II](#) pour obtenir plus de détails sur les licences basées sur la capacité, la planification et les options liées aux rapports de licences basées sur la capacité, ainsi que pour obtenir des informations sur le dépannage de `nbdeployutil`.

Établissez une relation de confiance entre les serveurs maîtres pour activer les rapports d'utilisation pour les serveurs maîtres distants sans connexion Internet

Une relation de confiance entre domaines est nécessaire pour les opérations de réplication. Procédez également à cette configuration pour activer les rapports d'utilisation dans l'interface utilisateur Web NetBackup si les serveurs distants n'ont pas de connexion Internet. Vous devez configurer la relation de confiance dans le domaine source et le domaine cible. Notez que vous ne pouvez pas extraire les propriétés d'hôte d'un serveur maître approuvé des listes **Propriétés de l'hôte > Clients**.

Remarque : Cette configuration n'est pas nécessaire pour les rapports d'utilisation si tous les serveurs maîtres disposent d'une connexion Internet.

Avant de commencer

Pour plus d'informations sur l'utilisation des commandes, consultez le [Guide de référence des commandes NetBackup](#). Pour plus de détails sur `authalias.conf`, consultez le [Guide de sécurité et de chiffrement NetBackup](#).

Effectuez les étapes suivantes sur les serveurs source et cible:

- Identifiez les versions de NetBackup qui sont installées sur les serveurs source et cible.
- Obtenez les jetons d'autorisation du serveur distant.
Utilisez la commande `bpnbat` pour vous connecter et la commande `nbcertcmd` pour obtenir les jetons d'autorisation.
- Obtenez les signatures pour le serveur distant.
Pour obtenir la signature SHA1 du certificat racine, utilisez la commande `nbcertcmd -displayCACertDetail`.
- Assurez-vous que vous disposez de l'une des autorisations suivantes :
 - Autorisations d'administrateur système avec les autorisations `root` pour UNIX, autorisations d'administrateur pour Windows ou d'utilisateur NetBackupCLI pour une appliance NetBackup 3.1.
 - Accès à la console d'administration NetBackup, avec les autorisations `<username>ADMIN = ALL` via `auth.conf`.
 - Autorisations d'utilisateur d'audit améliorées via `authalias.conf`.

Établissez une relation de confiance entre les serveurs maîtres pour activer les rapports d'utilisation pour les serveurs maîtres distants sans connexion Internet

- Si le serveur maître source ou le serveur maître cible se trouve sur la version 8.0 ou une version antérieure, assurez-vous que l'option **Activer la communication non sécurisée avec les hôtes NetBackup 8.0 et versions antérieures** est activée dans les paramètres de sécurité globaux.

Ajout d'un serveur maître approuvé lorsque les serveurs source et cible se trouvent sur la version NetBackup 8.1 ou une version ultérieure

- 1 Dans la **NetBackup Administration Console**, développez **Gestion NetBackup > Propriétés de l'hôte > Serveurs maîtres** (volet gauche).
- 2 Dans le volet droit, sélectionnez le serveur maître, puis accédez à **Actions > Propriétés**.
- 3 Dans le volet gauche de la boîte de dialogue de propriétés, sélectionnez **Serveurs**.
- 4 Dans l'onglet **Serveurs maîtres approuvés**, cliquez sur **Ajouter**.
- 5 Entrez le nom d'hôte complet du serveur maître distant puis cliquez sur **Valider une autorité de certification**.
- 6 Dans la boîte de dialogue **Valider une autorité de certification**, vérifiez si la signature de certificat d'autorité de certification du serveur distant est correcte.
Pour continuer, cliquez sur **Oui**.
Si les signatures ne correspondent pas, cliquez sur **Non**. Contactez l'administrateur du serveur distant pour fournir les signatures correctes.
- 7 Entrez les détails du serveur maître approuvé grâce à l'une des méthodes suivantes.
 - (Méthode recommandée) Sélectionnez **Spécifiez le jeton d'authentification du serveur maître approuvé** et entrez les détails du jeton du serveur maître distant.
 - Sélectionnez **Spécifiez les informations d'authentification du serveur maître approuvé** et entrez le nom d'utilisateur et le mot de passe. Notez que cette méthode peut présenter une faille de sécurité. Seul un jeton d'authentification peut fournir un accès restreint et permettre une communication sécurisée entre les hôtes.
Pour établir une relation de confiance avec une appliance maître NetBackup 3.1, utilisez les informations d'authentification NetbackupCLI.
- 8 Cliquez sur **OK**.
- 9 Effectuez la même procédure sur le serveur maître distant que vous avez ajouté à l'étape 5.

Ajout d'un serveur maître approuvé lorsque les serveur source et cible se trouvent sur NetBackup version 8.0 ou une version antérieure

- 1 Dans la **NetBackup Administration Console**, développez **Gestion NetBackup > Propriétés de l'hôte > Serveurs maîtres** (volet gauche).
- 2 Dans le volet droit, sélectionnez le serveur maître, puis accédez à **Actions > Propriétés**.
- 3 Dans le volet gauche de la boîte de dialogue de propriétés, sélectionnez **Serveurs**.
- 4 Dans l'onglet **Serveurs maîtres approuvés**, cliquez sur **Ajouter**.
- 5 Entrez le nom d'hôte complet du serveur maître distant puis cliquez sur **Valider une autorité de certification**.
- 6 Entrez le **nom d'utilisateur** et le **mot de passe** de l'hôte de serveur maître distant.
- 7 Cliquez sur **OK**.

Ajout de serveurs à une liste de serveurs pour autoriser les rapports d'utilisation pour les serveurs maîtres sans connexion Internet

Si vous voulez ajouter des informations de rapport sur l'utilisation pour un serveur maître, mais que ce serveur ne dispose pas d'une connexion Internet, vous devez ajouter le nom du serveur maître local à la liste de serveurs du serveur maître distant. Le serveur maître local est l'emplacement où vous prévoyez d'exécuter `nbdeployutil`.

Pour ajouter un serveur à une liste

- 1 Sur le serveur maître distant, ouvrez une session en tant qu'utilisateur racine ou qu'administrateur.
- 2 Dans le volet gauche de la **console d'administration NetBackup**, développez **Gestion NetBackup > Propriétés de l'hôte**.
- 3 Sélectionnez **Serveurs maîtres**.
- 4 Dans le volet droit, cliquez deux fois sur le serveur maître à modifier.
- 5 Dans la boîte de dialogue Propriétés (volet de gauche), cliquez sur **Serveurs**.
- 6 Sélectionnez l'onglet **Serveurs supplémentaires**.
- 7 Cliquez sur **Ajouter**.

Ajout de serveurs à une liste de serveurs pour autoriser les rapports d'utilisation pour les serveurs maîtres sans connexion Internet

- 8** Dans la boîte de dialogue **Ajouter une nouvelle entrée de serveur**, saisissez le nom du serveur maître à l'emplacement où vous prévoyez d'exécuter `nbdeployutil`.
- 9** Cliquez sur **Ajouter**. La boîte de dialogue reste ouverte pour vous permettre d'en saisir un autre.
- 10** Cliquez sur **Fermer**.