



# **SnapManager for Oracle utilise protection Manager pour protéger la sauvegarde des bases de données**

SnapManager Oracle

NetApp  
October 04, 2023

# Sommaire

- SnapManager for Oracle utilise protection Manager pour protéger la sauvegarde des bases de données . . . . 1
  - Détails de la base de données cible . . . . . 1
  - Configuration et topologie du stockage primaire et secondaire . . . . . 1
  - Programme de sauvegarde et stratégie de conservation . . . . . 5
  - Récapitulatif des workflows de sauvegarde des bases de données locales et secondaires . . . . . 6
  - Configuration et exécution de la sauvegarde protégées . . . . . 7
  - Restauration des bases de données à partir de la sauvegarde . . . . . 16

# SnapManager for Oracle utilise protection Manager pour protéger la sauvegarde des bases de données

Lorsqu'elles sont installées respectivement sur un hôte UNIX et sur le serveur, SnapManager for Oracle et protection Manager permettent à l'administrateur de bases de données SnapManager de configurer et d'exécuter des sauvegardes de bases de données Oracle basées sur des règles sur un système de stockage secondaire, et pour restaurer, si nécessaire, les données sauvegardées du stockage secondaire vers le stockage primaire.

Dans l'exemple suivant, un administrateur de bases de données qui utilise SnapManager crée un profil pour une sauvegarde locale sur le stockage primaire et un autre profil pour une sauvegarde protégée sur le stockage secondaire. Ensuite, l'administrateur de base de données travaille avec son administrateur de stockage réseau, qui utilise la console protection Manager, pour configurer une sauvegarde basée sur des règles de cette base de données du stockage primaire au stockage secondaire.

## Détails de la base de données cible

Cet exemple de protection intégrée des bases de données décrit la protection d'une base de données de paie. Les données suivantes sont utilisées dans l'exemple.

L'administrateur de base de données (DBA) de TechCo, une société de 3000 personnes dont le siège social est à Atlanta, doit créer une sauvegarde cohérente de la base de données de paie de production, PAYDB. La stratégie de protection pour la sauvegarde sur le stockage primaire et secondaire exige que l'administrateur de base de données et l'administrateur du stockage travaillent ensemble pour sauvegarder la base de données Oracle, aussi bien localement sur un système de stockage primaire, qu'à distance, sur un système de stockage secondaire sur un site distant.

### • Informations de profil

Lors de la création d'un profil dans SnapManager, vous avez besoin des données suivantes :

- Nom de la base de données : PAYDB
- Nom d'hôte : payroll.techco.com
- ID de base de données : payrolldb
- Nom du profil : Paypay\_prod
- Mode de connexion : authentification de la base de données
- Schéma de nommage des instantanés : smo\_hostname\_dbsid\_smoprofile\_scope\_mode\_smid (qui se traduit par « smo\_payroll.xyz.com\_payrolldb\_payroll\_prod\_f\_h\_x" )

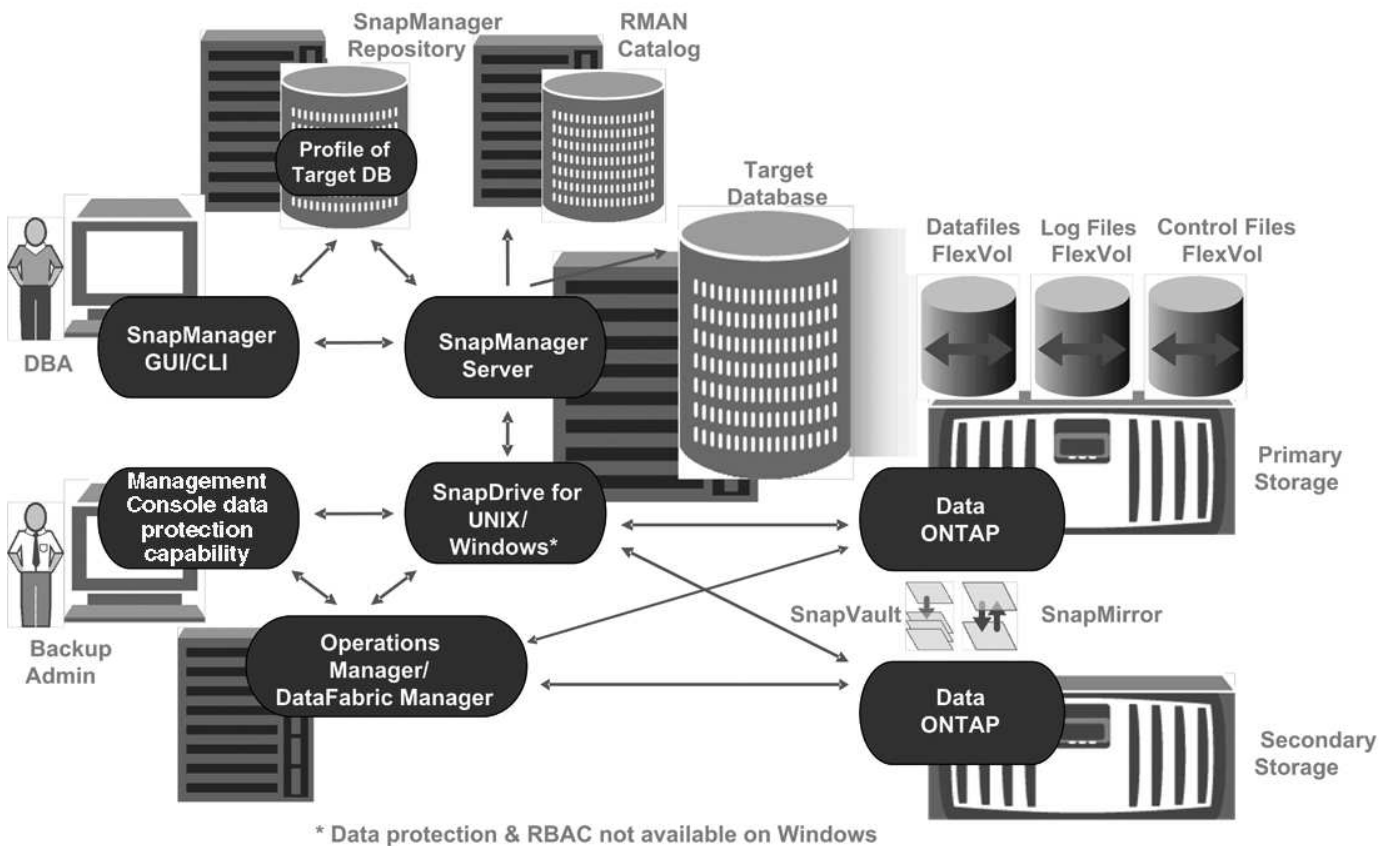
## Configuration et topologie du stockage primaire et secondaire

Dans cet exemple, la société TechCo exécute sa base de données de paie sur un serveur de base de données qui est également un hôte SnapManager pour Oracle et

stocke ses données de paie et ses fichiers de configuration sur des systèmes de stockage primaires au siège de l'entreprise. Il est donc impératif de protéger la base de données en conservant des sauvegardes quotidiennes et hebdomadaires sur le système de stockage local ainsi que des sauvegardes sur les systèmes de stockage secondaires situés à cinquante kilomètres.

L'illustration suivante présente SnapManager pour Oracle et les composants de protection des données de la console de gestion NetApp requis pour prendre en charge la protection des sauvegardes locales et secondaires.

## Architecture



Pour gérer la base de données de paie et soutenir sa protection de sauvegarde locale et secondaire comme illustré dans le graphique précédent, le déploiement suivant est utilisé.

### • Hôte SnapManager

L'hôte SnapManager, payroll.techco.com, est situé au siège de l'entreprise et fonctionne sur un serveur UNIX, qui exécute également le programme de base de données qui génère et gère la base de données des salaires.

#### ◦ Connexions

Pour prendre en charge la sauvegarde locale et la protection de sauvegarde secondaire, l'hôte SnapManager dispose de connexions réseau aux composants suivants :

- SnapManager pour client Oracle

- Un référentiel SnapManager, qui exécute le programme de base de données, SnapDrive pour UNIX et SnapManager
- Systèmes de stockage primaire
- Systèmes de stockage secondaires
- Serveur DataFabric Manager

◦ **Produits installés**

L'hôte SnapManager est installé avec les produits suivants pour cet exemple :

- Serveur SnapManager
- SnapDrive pour UNIX
- Utilitaires hôtes

• **Systèmes de stockage primaire TechCo**

La base de données de paie, y compris les fichiers de données, les fichiers journaux et les fichiers de contrôle associés, réside dans les systèmes de stockage primaires. Ces sociétés sont situées au siège de la société TechCo, ainsi qu'à l'hôte SnapManager et au réseau connectant le stockage principal et l'hôte SnapManager. Les dernières transactions et mises à jour de la base de données de paie sont écrites sur les systèmes de stockage primaires. Les copies Snapshot, qui offrent une protection de sauvegarde locale de la base de données des paies, résident également sur les systèmes de stockage primaires.

◦ **Connexions**

Pour prendre en charge la protection secondaire de la sauvegarde, les systèmes de stockage primaires disposent de connexions réseau vers les composants suivants :

- Hôte SnapManager exécutant le programme de base de données, SnapDrive pour UNIX et SnapManager
- Systèmes de stockage secondaires
- Serveur DataFabric Manager

◦ **Produits installés**

Les licences suivantes doivent être activées sur ces systèmes pour cet exemple :

- Data ONTAP 7.3.1 ou version ultérieure
- SourceData ONTAP primaire
- FlexVol (requis pour NFS)
- SnapRestore
- Protocole NFS

• **Systèmes de stockage secondaire TechCo**

Les systèmes de stockage secondaires, situés sur un site de stockage secondaire connecté au réseau à cinquante kilomètres, sont utilisés pour stocker des sauvegardes secondaires de la base de données de paie.

◦ **Connexions**

Pour prendre en charge la protection secondaire de la sauvegarde, les systèmes de stockage

secondaires disposent de connexions réseau aux composants suivants :

- Systèmes de stockage primaire
- Serveur DataFabric Manager

◦ **Produits installés**

Les licences suivantes doivent être activées sur les systèmes de stockage secondaires dans cet exemple :

- Data ONTAP
- SourceData ONTAP secondaire
- SnapRestore
- FlexVol (requis pour NFS)
- Protocole NFS

• **Serveur DataFabric Manager**

Le serveur DataFabric Manager, techco\_dfm, est situé au siège de l'entreprise dans un emplacement accessible à l'administrateur du stockage. Le serveur DataFabric Manager, entre autres fonctions, coordonne les tâches de sauvegarde entre le stockage primaire et secondaire.

◦ **Connexions**

Pour prendre en charge la protection de sauvegarde secondaire, le serveur DataFabric Manager maintient des connexions réseau vers les composants suivants :

- Console de gestion NetApp
- Systèmes de stockage primaire
- Systèmes de stockage secondaires

◦ **Produits installés**

Pour cet exemple, le serveur DataFabric Manager dispose d'une licence pour les produits de serveur suivants :

- DataFabric Manager

• **Référentiel SnapManager**

Le référentiel SnapManager, situé sur un serveur dédié, stocke les données sur les opérations réalisées par SnapManager, par exemple l'heure des sauvegardes, des espaces de stockage et des fichiers de données sauvegardés, les systèmes de stockage utilisés, les clones et les copies Snapshot créées. Lorsqu'un administrateur de base de données tente une restauration complète ou partielle, SnapManager interroge le référentiel afin d'identifier les sauvegardes créées par SnapManager pour Oracle à des fins de restauration.

◦ **Connexions**

Pour prendre en charge la protection secondaire de la sauvegarde, les systèmes de stockage secondaires disposent de connexions réseau aux composants suivants :

- Hôte SnapManager
- SnapManager pour client Oracle

- **Console de gestion NetApp**

La console de gestion NetApp est la console d'interface graphique utilisée par l'administrateur du stockage pour configurer les planifications, les règles, les jeux de données et les affectations de pools de ressources afin de permettre la sauvegarde sur les systèmes de stockage secondaires, accessibles à l'administrateur du stockage.

- **Connexions**

Pour prendre en charge la protection de sauvegarde secondaire, NetApp Management Console dispose de connexions réseau vers les composants suivants :

- Systèmes de stockage primaire
- Systèmes de stockage secondaires
- Serveur DataFabric Manager

- **SnapManager pour client Oracle**

Le client SnapManager pour Oracle est l'interface graphique et la console de ligne de commande utilisée par l'administrateur de base de données de paie pour configurer et exécuter des sauvegardes et des sauvegardes locales sur le stockage secondaire.

- **Connexions**

Pour prendre en charge la sauvegarde locale et la protection de sauvegarde secondaire, le client SnapManager pour Oracle dispose de connexions réseau aux composants suivants :

- Hôte SnapManager
- Référentiel SnapManager, exécutant le programme de base de données, SnapDrive pour UNIX et SnapManager
- Hôte de base de données (s'il est distinct de l'hôte exécutant SnapManager)
- Serveur DataFabric Manager

- **Produits installés**

Pour prendre en charge la sauvegarde locale et la protection de sauvegarde secondaire, le logiciel client SnapManager pour Oracle doit être installé sur ce composant.

## **Programme de sauvegarde et stratégie de conservation**

L'administrateur de base de données souhaite s'assurer que les sauvegardes sont disponibles en cas de perte de données, en cas d'incident et pour des raisons réglementaires. Cela nécessite une stratégie de conservation soigneusement pensée pour les diverses bases de données.

Pour la base de données de paie de production, l'administrateur de base de données respecte la stratégie de rétention TechCo suivante :

Fréquence des sauvegardes	Durée de conservation	Durée de sauvegarde	Type de stockage
Une fois par jour	10 jours	7 h	Principal (local)
Une fois par jour	10 jours	7 h	Secondaire (archivage)
Une fois par semaine	52 semaines	Samedi 1 h	Secondaire (archivage)

- **Avantages de sauvegarde locale**

La sauvegarde locale quotidienne assure la protection des bases de données, qui est instantanée. Elle utilise une bande passante réseau nulle, utilise un espace de stockage supplémentaire minimal et offre une restauration instantanée. Elle offre également des fonctionnalités de sauvegarde et de restauration très granulaires.

Les dernières sauvegardes hebdomadaires de la base de données de paie étant conservées pendant au moins 52 semaines sur un site de stockage secondaire, il n'est donc plus nécessaire de conserver les sauvegardes quotidiennes pendant plus de 10 jours.

- **Avantages de sauvegarde protégés**

Des sauvegardes quotidiennes et hebdomadaires sur un système de stockage secondaire sur un site distant garantissent que si les données du site de stockage primaire sont endommagées, la base de données cible est toujours protégée et peut être restaurée à partir d'un système de stockage secondaire.

Les sauvegardes quotidiennes sur le stockage secondaire sont effectuées pour protéger le système de stockage primaire contre l'endommagement. Comme les dernières sauvegardes hebdomadaires de la base de données de paie sont conservées pendant au moins 52 semaines, il n'est pas nécessaire de conserver les sauvegardes quotidiennes plus de 10 jours.

## Récapitulatif des workflows de sauvegarde des bases de données locales et secondaires

Dans cet exemple, l'administrateur de bases de données (via SnapManager) et l'administrateur du stockage (via la fonctionnalité de protection des données de la console de gestion NetApp) coordonnent les actions afin de configurer la sauvegarde locale et la sauvegarde secondaire (également appelée sauvegarde protégée) de la base de données cible.

La séquence des actions réalisées est résumée comme suit :

- **Configuration de pool de ressources secondaire**

L'administrateur du stockage utilise la fonctionnalité de protection des données de la console de gestion NetApp pour configurer un pool de ressources des systèmes de stockage sur le site secondaire et qui peut servir à stocker la sauvegarde de la base de données des salaires.

- **Planification de sauvegarde secondaire**

L'administrateur du stockage utilise la fonctionnalité de protection des données de la console de gestion



NetApp pour configurer les planifications de sauvegardes secondaires.

- **Configuration de la stratégie de protection**

L'administrateur du stockage utilise la fonctionnalité de protection des données de NetApp Management Console pour configurer une stratégie de protection de sauvegarde secondaire pour la base de données cible. La règle de protection inclut les calendriers, les spécifie le type de protection de base pour implémenter la protection de sauvegarde (sauvegarde, mise en miroir ou une combinaison des deux). Elle définit également les règles de conservation pour les nœuds de stockage primaire, secondaire et parfois tertiaire.

- **Affectation de la stratégie de configuration et de protection des profils de base de données**

L'administrateur de base de données utilise SnapManager pour créer ou modifier un profil de la base de données cible prenant en charge la sauvegarde secondaire. Lors de la configuration du profil, l'administrateur de base de données :

- Permet la protection des sauvegardes sur un système de stockage secondaire.
- Attribue à ce profil la nouvelle règle de protection, créée dans et récupérée à partir de la fonctionnalité de protection des données NetApp Management Console.

L'assignation de la règle de protection comprend automatiquement la base de données cible dans un jeu de données partiellement provisionné, mais qui ne respecte pas la capacité de protection des données de NetApp Management Console. Lorsqu'il est entièrement provisionné, la configuration des jeux de données permet de sauvegarder la base de données cible sur un stockage secondaire.

Le nom du jeu de données utilise la syntaxe suivante : `smo_hostname_database_ename`, qui signifie « `smo_payroll.techco.com_paydb` ».

- **Provisionnement de stockage secondaire et tertiaire**

L'administrateur du stockage utilise la fonctionnalité de protection des données de NetApp Management Console pour attribuer des pools de ressources afin de provisionner les nœuds de stockage secondaires ou tertiaires (si la règle de protection spécifie les nœuds de stockage tertiaires).

- **Sauvegarde sur stockage local**

L'administrateur de bases de données ouvre le profil avec la protection activée dans SnapManager et crée une sauvegarde complète sur le stockage local. La nouvelle sauvegarde apparaît dans SnapManager selon la planification de la protection, mais elle n'est pas encore protégée.

- **Confirmation de sauvegarde secondaire**

La sauvegarde étant basée sur un profil de protection activé, la sauvegarde est transférée vers un environnement secondaire selon le planning de la règle de protection. L'administrateur de base de données utilise SnapManager pour confirmer le transfert de la sauvegarde vers le stockage secondaire. Une fois la sauvegarde copiée sur le stockage secondaire, SnapManager modifie l'état de protection des sauvegardes de « non protégé » à « protégé ».

## Configuration et exécution de la sauvegarde protégées

Vous devez configurer SnapManager et protection Manager pour prendre en charge la sauvegarde de base de données sur le stockage secondaire. L'administrateur de la base

de données et l'administrateur du stockage doivent coordonner leurs actions.

## Utilisation de SnapManager pour Oracle pour créer le profil de base de données pour une sauvegarde locale

Les administrateurs de base de données utilisent SnapManager pour créer un profil de base de données qui sera utilisé pour lancer une sauvegarde sur du stockage local sur un système de stockage primaire. La création de profils et les processus de sauvegarde sont entièrement exécutés dans SnapManager, mais ils n'impliquent pas protection Manager.

Un profil contient les informations relatives à la base de données gérée, notamment ses informations d'identification, ses paramètres de sauvegarde et ses paramètres de protection pour les sauvegardes. En créant un profil, vous n'avez pas besoin de spécifier les détails de la base de données chaque fois que vous effectuez une opération sur cette base de données, mais il vous suffit de fournir le nom du profil. Un profil ne peut référencer qu'une seule base de données. Cette même base de données peut être référencée par plusieurs profils.

1. Accédez au client SnapManager pour Oracle.
2. Dans l'arborescence des référentiels SnapManager, cliquez avec le bouton droit de la souris sur l'hôte que vous souhaitez associer à ce profil et sélectionnez **Créer un profil**.
3. Dans la page informations sur la configuration du profil, entrez les informations suivantes et cliquez sur **Suivant**.
  - Nom du profil : Paypay\_prod
  - Mot de passe du profil: Payroll123
  - Commentaire : base de données paie de production
4. Dans la page informations sur la configuration de la base de données, entrez les informations suivantes et cliquez sur **Suivant**.
  - Nom de la base de données : PAYDB
  - SID de base de données : payrolldb
  - Hôte de base de données : acceptez la valeur par défaut

Comme vous créez un profil à partir d'un hôte dans l'arborescence du référentiel, SnapManager affiche le nom de l'hôte.

5. Dans la deuxième page informations sur la configuration de la base de données, acceptez les informations suivantes de la base de données et cliquez sur **Suivant** :
  - Compte hôte, représentant le compte utilisateur Oracle : oracle
  - Groupe hôte, représentant le groupe Oracle : dba
6. Dans la page Database Connection information (informations de connexion à la base de données), sélectionnez **Use database Authentication** (utiliser l'authentification de la base de données) pour permettre aux utilisateurs de s'authentifier à l'aide des informations

Dans cet exemple, entrez les informations suivantes et cliquez sur **Suivant**.

- SYSDBA Privileged User Name, représentant l'administrateur de la base de données système disposant de privilèges d'administration : sys

- Mot de passe (mot de passe SYSDBA) : oracle
- Port de connexion à l'hôte de base de données : 1521

7. Dans la page informations sur la configuration RMAN, sélectionnez **n'utilisez pas RMAN** et cliquez sur **Suivant**.

Oracle Recovery Manager (RMAN) est un outil Oracle qui vous aide à sauvegarder et à restaurer vos bases de données Oracle à l'aide d'une détection au niveau des blocs.

8. Dans la page informations d'attribution de nom d'instantané, spécifiez une convention d'attribution de nom pour les snapshots associés à ce profil en sélectionnant des variables. La seule variable requise est la variable **smid**, qui crée un identifiant de snapshot unique.

Pour cet exemple, procédez comme suit :

- Dans la liste jeton variable, sélectionnez la variable **{usertext}** et cliquez sur **Ajouter**.
- Entrez "payroll.techco.com\_" comme nom d'hôte et cliquez sur **OK**.
- Cliquez sur **Left** jusqu'à ce que le nom d'hôte apparaisse juste après "smo" dans la zone format.
- Cliquez sur **Suivant**.

La convention de nommage des snapshots de smo\_hostname\_smopprofile\_dbsid\_scope\_mode\_smid devient "smo\_payroll.techco.com\_payroll\_prod2\_payrolldb\_f\_a\_x" (où le "f" indique une sauvegarde complète, le "a" indique le mode automatique et le "x" représente le SMID unique).

9. Sur la page effectuer une opération, vérifiez les informations et cliquez sur **Créer**.

10. Cliquez sur **Operation Details** pour afficher des informations sur l'opération de création de profil et les informations d'éligibilité à la restauration basée sur le volume.

## Utilisation de protection Manager pour configurer un pool de ressources secondaire

Pour prendre en charge la sauvegarde de la base de données sur le stockage secondaire, l'administrateur du stockage utilise protection Manager pour organiser les systèmes de stockage secondaires activés avec la licence SnapVault secondaire dans un pool de ressources pour les sauvegardes.

Idéalement, les systèmes de stockage d'un pool de ressources sont interchangeables en termes d'acceptabilité en tant que destination de sauvegarde. Par exemple, lors du développement de la stratégie de protection de la base de données de paie, vous, en tant qu'administrateur du stockage, avez identifié des systèmes de stockage secondaires ayant des niveaux de performance et de qualité de service similaires à ceux qui appartiennent au même pool de ressources.

Vous avez déjà créé des agrégats d'espace inutilisé sur les systèmes de stockage que vous envisagez d'attribuer à des pools de ressources. Cela permet de s'assurer que l'espace disponible est suffisant pour contenir les sauvegardes.

- Accédez à la console de gestion NetApp de protection Manager.
- Dans la barre de menus, cliquez sur **Data > Resource pools**.

La fenêtre pools de ressources s'affiche.

- Cliquez sur **Ajouter**.

L'assistant Ajouter un pool de ressources démarre.

4. Suivez les étapes de l'assistant pour créer le pool de ressources **paydb\_backup\_Resource**.

Utilisez les paramètres suivants :

- Nom : utilisez **paydb-backup\_Resource**
- Seuils d'espace (utilisez les valeurs par défaut) :
  - Seuils d'utilisation de l'espace : activés
  - Seuil presque atteint (pour le pool de ressources) : 80 %
  - Seuil complet (pour le pool de ressources) : 90 %

## Utilisation de protection Manager pour configurer les planifications de sauvegarde secondaires

Pour prendre en charge la sauvegarde de la base de données sur du stockage secondaire, l'administrateur du stockage utilise protection Manager afin de configurer un programme de sauvegarde.

Avant de configurer la planification de sauvegardes secondaires, l'administrateur du stockage confère au partenaire DBA les informations suivantes :

- Planification que l'administrateur de base de données souhaite suivre pour les sauvegardes secondaires

Dans ce cas, les sauvegardes une fois par jour sont effectuées à 7 h Les sauvegardes hebdomadaires sont également exécutées le samedi à 1 h

- a. Accédez à la console de gestion NetApp de protection Manager.
- b. Dans la barre de menus, cliquez sur **stratégies > protection > horaires**.

L'onglet programmes de la fenêtre stratégies de protection s'affiche.

- c. Sélectionnez l'horaire quotidien **chaque jour à 8:00 PM** dans la liste des horaires.
- d. Cliquez sur **Copier**.

Un nouvel horaire quotidien, **copie du quotidien à 8:00 PM**, est affiché dans la liste. Elle est déjà sélectionnée.

- e. Cliquez sur **Modifier**.

La feuille de propriétés Modifier horaire quotidien s'ouvre sur l'onglet horaire.

- f. Modifiez le nom de l'horaire sur **Payroll Daily à 7 PM**, mettez à jour la description, puis cliquez sur **Apply**.

Vos modifications sont enregistrées.

- g. Cliquez sur l'onglet **événements quotidiens**.

L'heure de sauvegarde quotidienne actuelle de la planification est de 8:00 s'affiche.

h. Cliquez sur **Ajouter** et saisissez **7:00 PM** dans le nouveau champ heure, puis cliquez sur **appliquer**.

L'heure de sauvegarde quotidienne actuelle de l'agenda est maintenant de 7:00

i. Cliquez sur **OK** pour enregistrer vos modifications et quitter la feuille de propriétés.

Votre nouvel horaire quotidien, **paie quotidienne à 7 h**, est affiché dans la liste des horaires.

j. Sélectionnez l'horaire hebdomadaire **dimanche à 8:00 PM plus tous les jours** dans la liste des horaires.

k. Cliquez sur **Copier**.

Un nouvel horaire hebdomadaire, **copie du dimanche à 8:00 PM plus quotidien**, est affiché dans la liste. Elle est déjà sélectionnée.

l. Cliquez sur **Modifier**.

La feuille de propriétés Modifier horaire hebdomadaire s'ouvre sur l'onglet planification.

m. Modifiez le nom de l'horaire à **Payroll Saturday à 1 h plus quotidiennement à 7 h** et mettez à jour la description.

n. Dans la liste déroulante **horaire quotidien**, sélectionnez l'horaire quotidien que vous venez de créer, **paie quotidienne à 7 h**.

La sélection de **Payroll Daily à 7 PM** signifie que ce calendrier définit le moment où les opérations quotidiennes se produisent lorsque le **Payroll Saturday à 1 h plus quotidien à 7 h** calendrier est appliqué à une police.

o. Cliquez sur **OK** pour enregistrer vos modifications et quitter la feuille de propriétés.

Votre nouvel horaire hebdomadaire, **paie le samedi à 1 h plus tous les jours à 7 h**, est affiché dans la liste des horaires.

## Utilisation de protection Manager pour configurer une stratégie de protection de sauvegarde secondaire

Après avoir configuré le planning de sauvegarde, l'administrateur du stockage configure une stratégie de stockage de sauvegarde protégée dans laquelle ce planning doit être inclus.

Avant de configurer la règle de protection, l'administrateur du stockage confère au partenaire DBA les informations suivantes :

- Durée de conservation à spécifier pour le stockage secondaire
- Type de protection de stockage secondaire requis

La stratégie de protection créée peut être répertoriée dans SnapManager pour Oracle par le partenaire de l'administrateur de bases de données, et attribuée à un profil de base de données pour les données à protéger.

1. Accédez à la console de gestion NetApp de protection Manager.
2. Dans la barre de menus, cliquez sur **stratégies > protection > Présentation**.

L'onglet Présentation de la fenêtre stratégies de protection s'affiche.

3. Cliquez sur **Ajouter une stratégie** pour lancer l'assistant Ajouter une stratégie de protection.

4. Exécutez l'assistant en procédant comme suit :

a. Spécifiez un nom de stratégie descriptif.

Dans cet exemple, entrez **données de paie TechCo : sauvegarde** et une description, puis cliquez sur **Suivant**.

b. Sélectionnez une stratégie de base.

Pour cet exemple, sélectionnez **Sauvegarder** et cliquez sur **Suivant**.

c. Dans la feuille de propriétés de la stratégie de noeud de données principal, acceptez les paramètres par défaut et cliquez sur **Suivant**.



Dans cet exemple, la planification de sauvegarde locale configurée dans SnapManager est appliquée. Tout programme de sauvegarde local spécifié à l'aide de cette méthode est ignoré.

d. Dans la feuille de propriétés connexion données primaires à sauvegarde, sélectionnez un programme de sauvegarde.

Dans cet exemple, sélectionnez **Payroll Saturday à 1 AM plus Daily à 7 PM** comme programme de sauvegarde, puis cliquez sur **Next**.

Dans cet exemple, la planification que vous avez sélectionnée inclut à la fois les horaires hebdomadaires et quotidiens que vous avez configurés précédemment.

e. Dans la feuille de propriétés de la stratégie de sauvegarde, spécifiez le nom du nœud de sauvegarde et les temps de conservation pour les sauvegardes quotidiennes, hebdomadaires ou mensuelles.

Dans cet exemple, indiquez une durée de conservation quotidienne des sauvegardes de 10 jours et une durée de conservation hebdomadaire des sauvegardes de 52 semaines. Après avoir terminé chaque feuille de propriétés, cliquez sur **Suivant**.

Une fois toutes les feuilles de propriétés terminées, l'assistant Ajout de stratégie de protection affiche une feuille récapitulative pour la stratégie de protection que vous souhaitez créer.

5. Cliquez sur **Terminer** pour enregistrer vos modifications.

La politique de protection \* données de paie TechCo : sauvegarde\* figure parmi les autres politiques configurées pour protection Manager.

Le partenaire de l'administrateur de bases de données peut désormais utiliser SnapManager for Oracle pour répertorier et affecter cette stratégie lors de la création du profil de base de données pour les données à protéger.

## Utilisation de SnapManager pour Oracle pour créer le profil de base de données et affecter une stratégie de protection

Vous devez créer un profil dans SnapManager pour Oracle, activer la protection dans le profil et attribuer une règle de protection pour créer une sauvegarde protégée.

Un profil contient des informations sur la base de données gérée, notamment ses informations d'identification, ses paramètres de sauvegarde et ses paramètres de protection pour les sauvegardes. Après avoir créé un profil, vous n'avez pas besoin de spécifier les détails de la base de données chaque fois que vous effectuez une opération. Un profil ne peut référencer qu'une seule base de données, mais cette même base de données peut être référencée par plusieurs profils.

1. Accédez au client SnapManager pour Oracle.
2. Dans l'arborescence des référentiels, cliquez avec le bouton droit de la souris sur l'hôte et sélectionnez **Créer un profil**.
3. Sur la page informations sur la configuration du profil, entrez les détails du profil et cliquez sur **Suivant**.

Vous pouvez entrer les informations suivantes :

- Nom du profil : Paypaie\_prod2
  - Mot de passe du profil: Payroll123
  - Commentaire : base de données paie de production
4. Dans les pages informations sur la configuration de la base de données, entrez les détails de la base de données, puis cliquez sur **Suivant**.

Vous pouvez entrer les informations suivantes :

- Nom de la base de données : PAYDB
  - SID de base de données : payrolldb
  - Hôte de base de données : acceptez la valeur par défaut. Comme vous créez un profil à partir d'un hôte dans l'arborescence du référentiel, SnapManager affiche le nom de l'hôte.
  - Compte hôte, représentant le compte utilisateur Oracle : oracle
  - Groupe hôte, représentant le groupe Oracle : dba
5. Sur la page informations de connexion à la base de données, cliquez sur **utiliser l'authentification de base de données** pour permettre aux utilisateurs de s'authentifier à l'aide des informations de base de données.
  6. Entrez les détails de la connexion à la base de données et cliquez sur **Suivant**.

Vous pouvez entrer les informations suivantes :

- SYSDBA Privileged User Name, représentant l'administrateur de la base de données système disposant de privilèges d'administration : sys
  - Mot de passe (mot de passe SYSDBA) : oracle
  - Port de connexion à l'hôte de base de données : 1521
7. Sur la page informations sur la configuration RMAN, cliquez sur **n'utilisez pas RMAN** et cliquez sur **Suivant**.

Oracle Recovery Manager (RMAN) est un outil Oracle qui vous aide à sauvegarder et à restaurer vos bases de données Oracle à l'aide d'une détection au niveau des blocs.

8. Sur la page informations d'attribution de nom d'instantané, spécifiez une convention d'attribution de nom pour les snapshots associés à ce profil en sélectionnant des variables.

La variable smid crée un identifiant de snapshot unique.

Effectuez les opérations suivantes :

- a. Dans la liste jeton variable, sélectionnez texte utilisateur et cliquez sur **Ajouter**.
- b. Entrez payroll.techco.com\_ comme nom d'hôte et cliquez sur **OK**.
- c. Cliquez sur **Left** jusqu'à ce que le nom d'hôte apparaisse juste après smo dans la zone format.
- d. Cliquez sur **Suivant**.

La convention de nommage des snapshots de smo\_hostname\_smopprofile\_dbssid\_scope\_mode\_smid devient "smo\_payroll.techco.com\_payroll\_prod2\_payrolldb\_f\_a\_x" (où "f" indique une sauvegarde complète, "a" indique le mode automatique et "x" représente le SMID unique).

9. Sélectionnez **protection Manager protection Policy**.

**Protection Manager protection Policy** permet de sélectionner une règle de protection qui a été configurée à l'aide de NetApp Management Console.

10. Sélectionnez **TechCo données de paie : sauvegarde** comme règle de protection dans les règles de protection extraites de la console de gestion NetApp, et cliquez sur **Next**.
11. Sur la page effectuer une opération, vérifiez les informations et cliquez sur **Créer**.
12. Cliquez sur **Operation Details** pour afficher des informations sur l'opération de création de profil et les informations d'éligibilité à la restauration basée sur le volume.
  - L'attribution d'une règle de protection NetApp Management Console au profil de base de données crée automatiquement un jeu de données non conforme, visible par l'opérateur de la console de gestion NetApp, avec le nom de convention smo\_<hostname>\_<profilName>, ou dans cet exemple : smo\_payroll.tech.com\_PAYDB.
  - Si le profil n'est pas éligible pour la restauration de volume (également appelée « restauration rapide »), les événements suivants se produisent :
    - L'onglet **Résultats** indique que la création du profil a réussi et que des avertissements se sont produits pendant l'opération.
    - L'onglet **Operation Details** contient un journal D'AVERTISSEMENT, qui indique que le profil n'est pas éligible pour la restauration rapide et explique pourquoi.

## Utilisation de protection Manager pour provisionner le nouveau jeu de données

Une fois le jeu de données smo\_paydb créé, l'administrateur du stockage utilise protection Manager pour affecter des ressources du système de stockage pour provisionner le nœud de sauvegarde du dataset.

Avant de provisionner le jeu de données nouvellement créé, l'administrateur de stockage confère au partenaire DBA le nom du jeu de données spécifié dans le profil.

Dans ce cas, le nom du jeu de données est smo\_payroll.tech.com\_PAYDB.

1. Accédez à la console de gestion NetApp de protection Manager.
2. Dans la barre de menus, cliquez sur **Data > Dataensembles > Overview**.

L'onglet Datasets de la fenêtre Datasets affiche la liste des ensembles de données qui incluent le jeu de données qui vient d'être créé via SnapManager.

3. Localisez et sélectionnez le jeu de données **smo\_payroll.tech.com\_PAYDB**.



Lorsque vous sélectionnez ce jeu de données, la zone graphique affiche le jeu de données smo\_paydb avec son nœud de sauvegarde non provisionné. Son statut de conformité est signalé comme non-conforme.

4. Avec le jeu de données smo\_paydb toujours en surbrillance, cliquez sur **Edit**.

La console de gestion NetApp de protection Manager affiche la fenêtre Modifier le dataset pour le jeu de données **smo\_payroll.tech.com\_PAYDB**. Le volet de navigation de la fenêtre affiche les options de configuration pour le nœud principal du dataset, la connexion de sauvegarde et le nœud de sauvegarde.

5. Dans le volet de navigation, recherchez les options du nœud de sauvegarde du jeu de données et sélectionnez **provisioning/pools de ressources**.

La fenêtre Modifier l'ensemble de données affiche un paramètre pour la stratégie d'approvisionnement par défaut et une liste de pools de ressources disponibles.

6. Pour cet exemple, sélectionnez le pool de ressources **paydb\_backup\_Resource** et cliquez sur **>**.

Le pool de ressources sélectionné est répertorié dans le champ « pools de ressources pour ce nœud ».

7. Cliquez sur **Terminer** pour enregistrer vos modifications.

Protection Manager provisionne automatiquement le nœud de sauvegarde secondaire avec les ressources du pool de ressources paydb\_backup\_Resource.

## Utilisation de SnapManager pour Oracle pour créer une sauvegarde protégée

Lors de la création d'une sauvegarde pour cet exemple, l'administrateur de bases de données sélectionne pour créer une sauvegarde complète, définit les options de sauvegarde et sélectionne la protection sur le stockage secondaire. Bien que la sauvegarde soit initialement effectuée sur un stockage local, car cette sauvegarde repose sur un profil protégé, la sauvegarde est ensuite transférée vers du stockage secondaire selon le planning de la règle de protection défini dans protection Manager.

1. Accédez au client SnapManager pour Oracle.
2. Dans l'arborescence du référentiel SnapManager, cliquez avec le bouton droit de la souris sur le profil contenant la base de données à sauvegarder, puis sélectionnez **Sauvegarder**.

L'assistant de sauvegarde SnapManager pour Oracle démarre.

3. Saisissez production\_pay comme étiquette.
4. Entrez la paie de production Jan 19 sauvegarde comme commentaire.
5. Sélectionnez **Auto** comme type de sauvegarde que vous souhaitez créer.

Cela permet à SnapManager de déterminer s'il faut effectuer une sauvegarde en ligne ou hors ligne.

6. Sélectionnez **Daily** ou **Weekly** comme fréquence de sauvegarde.
7. Pour confirmer que la sauvegarde est dans un format valide pour Oracle, cochez la case en regard de **Verify backup**.

Cette opération utilise Oracle DBVerify pour vérifier le format et la structure du bloc.

8. Pour forcer l'état de la base de données dans le mode approprié (par exemple, de l'ouverture au montage), sélectionnez **Autoriser le démarrage ou l'arrêt de la base de données, si nécessaire**, puis cliquez sur **Suivant**.
9. Dans la page base de données, tablespaces ou fichiers de données à sauvegarder, sélectionnez **sauvegarde complète** et cliquez sur **Suivant**.
10. Pour protéger la sauvegarde sur le stockage secondaire, cochez **protéger la sauvegarde** et cliquez sur **Suivant**.
11. Dans la page Exécuter l'opération, vérifiez les informations que vous avez fournies et cliquez sur **Sauvegarder**.
12. Dans la page de progression, affichez la progression et les résultats de la création de la sauvegarde.
13. Pour afficher les détails de l'opération, cliquez sur **Détails de l'opération**.

## Utilisation de SnapManager pour Oracle pour confirmer la protection de la sauvegarde

Avec SnapManager pour Oracle, vous pouvez afficher la liste des sauvegardes associées à un profil, déterminer si les sauvegardes sont activées pour la protection et afficher la classe de conservation (quotidienne ou hebdomadaire, dans cet exemple).

Au début, la nouvelle sauvegarde de cet exemple montre que la protection est planifiée, mais pas encore protégée (dans l'interface graphique de SnapManager et dans la sortie de la commande backup show). Après avoir assuré que la sauvegarde a été copiée sur le stockage secondaire, SnapManager modifie l'état de protection de la sauvegarde de « non protégé » à « protégé » dans l'interface utilisateur graphique et à l'aide de la commande backup list.

1. Accédez au client SnapManager pour Oracle.
2. Dans l'arborescence du référentiel SnapManager, développez le profil pour afficher ses sauvegardes.
3. Cliquez sur l'onglet **backups/clones**.
4. Dans le volet Rapports, sélectionnez **Détails de sauvegarde**.
5. Affichez la colonne protection et vérifiez que l'état est protégé.

## Restauration des bases de données à partir de la sauvegarde

En cas de perte ou de destruction accidentelle du contenu actif de la base de données de paie, SnapManager et les fonctionnalités de protection des données de la console de gestion NetApp prennent en charge la restauration de ces données à partir d'une sauvegarde locale ou d'un stockage secondaire.

### Utilisation de SnapManager pour Oracle pour restaurer une sauvegarde locale sur le stockage primaire

Vous pouvez restaurer les sauvegardes locales qui existent sur le stockage primaire. L'ensemble du processus est effectué à l'aide de SnapManager pour Oracle.

Vous pouvez également afficher un aperçu des informations relatives à un processus de restauration de

sauvegarde. Pour afficher des informations sur l'éligibilité à la restauration d'une sauvegarde, vous pouvez le faire. SnapManager analyse les données sauvegardées afin de déterminer si le processus de restauration peut être terminé à l'aide de la restauration basée sur les volumes ou de la méthode de restauration basée sur les fichiers.

L'aperçu de restauration affiche les informations suivantes :

- Quel mécanisme de restauration (restauration rapide, restauration du système de fichiers côté stockage, restauration de fichiers côté stockage ou restauration de copie de fichiers côté hôte) sera utilisé pour restaurer chaque fichier.
- Pourquoi des mécanismes plus efficaces n'ont pas été utilisés pour restaurer chaque fichier.

Dans l'aperçu du plan de restauration, SnapManager ne restaure rien. L'aperçu affiche des informations pouvant contenir jusqu'à 20 fichiers.

Si vous souhaitez prévisualiser une restauration des fichiers de données mais que la base de données n'est pas montée, SnapManager monte la base de données. Si la base de données ne peut pas être montée, l'opération échoue et SnapManager retourne la base de données à son état d'origine.

1. Dans l'arborescence référentiel, cliquez avec le bouton droit de la souris sur la sauvegarde à restaurer et sélectionnez **Restaurer**.
2. Sur la page d'accueil de l'Assistant de restauration et de récupération, cliquez sur **Suivant**.
3. Sur la page Restore Configuration information (Restaurer les informations de configuration), sélectionnez **Complete Datafile/Tablespace Restore with Control Files**.
4. Cliquez sur **Autoriser l'arrêt de la base de données si nécessaire**.

SnapManager modifie l'état de la base de données si nécessaire. Par exemple, si la base de données est hors ligne et doit être en ligne, SnapManager la force en ligne.

5. Sur la page informations sur la configuration de la récupération, cliquez sur **tous les journaux**.

SnapManager restaure et restaure la base de données vers la dernière transaction et applique tous les journaux requis.

6. Sur la page Restore Source Location Configuration (Configuration de l'emplacement source de restauration), affichez les informations relatives à la sauvegarde sur le stockage primaire et cliquez sur **Next** (Suivant).

Si la sauvegarde n'existe que sur le stockage primaire, SnapManager restaure la sauvegarde à partir du stockage primaire.

7. Sur la page informations sur la configuration de la restauration de volume, sélectionnez **tentative de restauration de volume** pour essayer la méthode de restauration de volume.
8. Cliquez sur **Retour à la restauration basée sur les fichiers**.

Ceci permet à SnapManager d'utiliser la méthode de restauration basée sur les fichiers si la méthode de restauration de volume ne peut pas être utilisée.

9. Cliquez sur **Preview** pour voir les vérifications d'éligibilité pour une restauration rapide et les informations sur les vérifications obligatoires et superflus.
10. Sur la page Exécuter l'opération, vérifiez les informations que vous avez saisies, puis cliquez sur **Restaurer**.

11. Pour afficher les détails du processus, cliquez sur **Détails de l'opération**.

## Utilisation de SnapManager pour Oracle pour restaurer les sauvegardes à partir du stockage secondaire

Les administrateurs peuvent restaurer des sauvegardes protégées à partir d'un stockage secondaire et choisir le mode de copie des données vers le stockage primaire.

Avant de tenter de restaurer la sauvegarde, vérifiez les propriétés de la sauvegarde, puis assurez-vous que la sauvegarde est libérée sur le système de stockage primaire et protégée sur le stockage secondaire.

1. Dans l'arborescence du référentiel SnapManager pour Oracle, cliquez avec le bouton droit de la souris sur la sauvegarde à restaurer et sélectionnez **Restaurer**.
2. Dans la page d'accueil de l'Assistant de restauration et de récupération, cliquez sur **Suivant**.
3. Dans la page Restore Configuration information (Restaurer les informations de configuration), cliquez sur **Complete Datafile/tablespace Restore with Control Files**.
4. Cliquez sur **Autoriser l'arrêt de la base de données si nécessaire**, puis cliquez sur **Suivant**.

SnapManager modifie l'état de la base de données si nécessaire. Par exemple, si la base de données est hors ligne et doit être en ligne, SnapManager la force en ligne.

5. Sur la page informations sur la configuration de la récupération, cliquez sur **tous les journaux**. Cliquez ensuite sur **Suivant**.

SnapManager restaure et restaure la base de données vers la dernière transaction et applique tous les journaux requis.

6. Dans la page Restore Source Location Configuration (Configuration de l'emplacement source de restauration), sélectionnez l'ID de la source de sauvegarde protégée et cliquez sur **Next** (Suivant).
7. Dans la page informations sur la configuration de la restauration de volume, cliquez sur **tentative de restauration de volume** pour tenter la restauration de volume.
8. Cliquez sur **Retour à la restauration basée sur les fichiers**.

Ceci permet à SnapManager d'utiliser la méthode de restauration basée sur les fichiers si la méthode de restauration de volume ne peut pas être terminée.

9. Pour consulter les vérifications d'éligibilité pour la restauration rapide et les informations sur les vérifications obligatoires et les vérifications à découvert, cliquez sur **Preview**.
10. Sur la page Exécuter l'opération, vérifiez les informations que vous avez fournies et cliquez sur **Restaurer**.
11. Pour afficher les détails du processus, cliquez sur **Détails de l'opération**.

## Informations sur le copyright

Copyright © 2023 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

**LÉGENDE DE RESTRICTION DES DROITS :** L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.