



La réplication

ONTAP 9

NetApp
April 24, 2024

Sommaire

- La réplication 1
 - Copies Snapshot 1
 - Reprise sur incident et transfert de données SnapMirror..... 2
 - Sauvegardes SnapMirror dans le cloud sur le stockage objet..... 4
 - Archivage SnapVault 5
 - Sauvegarde dans le cloud et prise en charge des sauvegardes classiques 6
 - Disponibilité sans interruption avec MetroCluster 7

La réplication

Copies Snapshot

Les technologies de réplication ONTAP exigeaient les reprises après incident et les archivages. Avec l'avènement des services cloud, la réplication ONTAP a été adaptée au transfert des données entre les terminaux dans l'environnement NetApp Data Fabric. Ces utilisations reposent sur la technologie Snapshot de ONTAP.

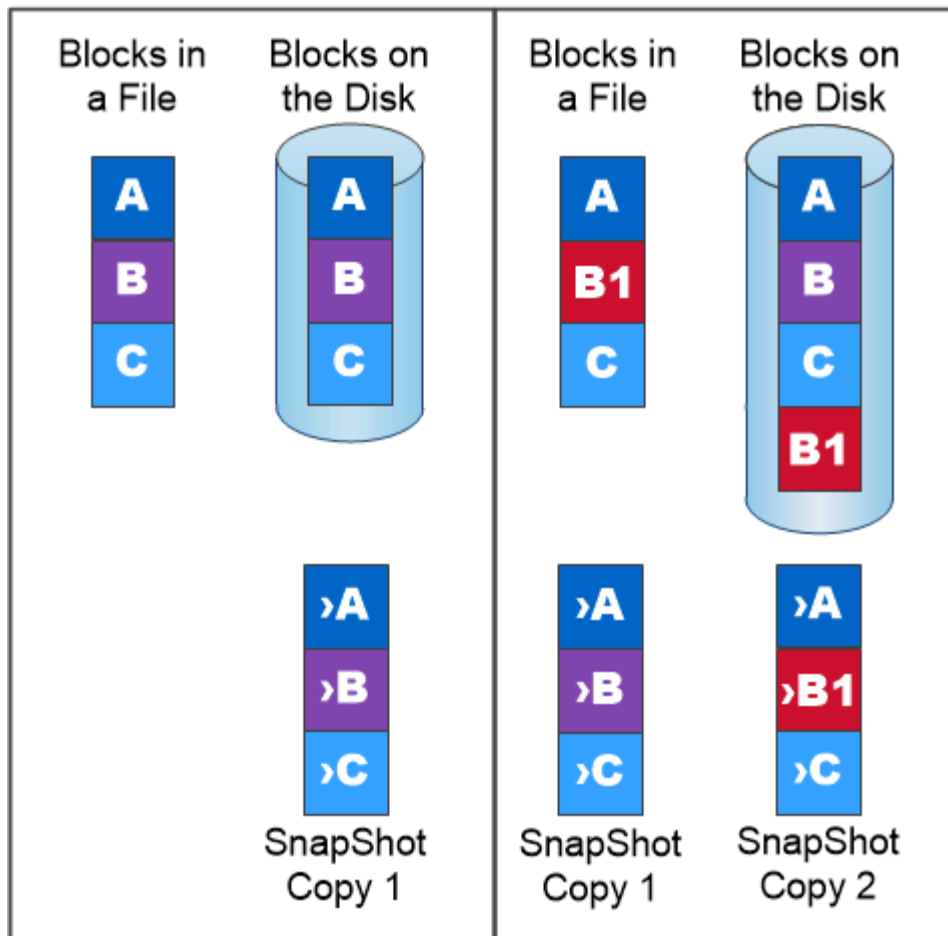
Une *copie snapshot* est une image ponctuelle en lecture seule d'un volume. Après la création d'une copie Snapshot, le système de fichiers actif et la copie Snapshot pointent vers les mêmes blocs de disque. Ainsi, la copie Snapshot n'utilise pas d'espace disque supplémentaire. Au fil du temps, l'image consomme un espace de stockage minimal et implique un impact négligeable sur les performances, car elle n'enregistre que les modifications apportées aux fichiers depuis la dernière copie Snapshot.

Les copies Snapshot doivent leur efficacité à la technologie de virtualisation du stockage principale d'ONTAP, sa *WAFL (Write Anywhere File Layout)*. comme une base de données, WAFL utilise des métadonnées pour pointer les blocs de données réels du disque. Contrairement à une base de données, WAFL ne remplace pas les blocs existants. Il écrit les données mises à jour sur un nouveau bloc et modifie les métadonnées.

Les copies Snapshot sont efficaces car, au lieu de copier des blocs de données, ONTAP référence les métadonnées lors de la création d'une copie Snapshot. Ainsi, vous éliminez à la fois le temps de recherche que d'autres systèmes impliquent pour localiser les blocs à copier et le coût lié à la copie.

Vous pouvez utiliser une copie Snapshot pour restaurer des fichiers ou des LUN individuels, ou pour restaurer l'ensemble du contenu d'un volume. ONTAP compare les informations du pointeur de la copie Snapshot aux données d'un disque pour reconstruire l'objet manquant ou endommagé, sans temps d'indisponibilité ni coûts de performance significatifs.

Une règle *Snapshot* définit la façon dont le système crée des copies Snapshot de volumes. La règle indique quand créer les copies Snapshot, le nombre de copies à conserver, comment les nommer et comment les étiqueter pour la réplication. Par exemple, un système peut créer une copie Snapshot tous les jours à 12 h 10, conserver les deux copies les plus récentes, les nommer « diotidienne » (ajoutée avec un horodatage) et les étiqueter « dootidienne » pour la réplication.



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

Reprise sur incident et transfert de données SnapMirror

SnapMirror est une technologie de reprise après incident conçue pour le basculement du stockage primaire vers le stockage secondaire sur un site distant. Comme son nom l'indique, SnapMirror crée une réplique ou *mirror* de vos données de travail dans un stockage secondaire à partir duquel vous pouvez continuer à transmettre des données en cas de catastrophe sur le site primaire.

Les données sont mises en miroir au niveau du volume. La relation entre le volume source du stockage primaire et le volume de destination du stockage secondaire est appelée « relation *protection des données* ». les clusters dans lesquels résident les volumes et les SVM qui fournissent des données à partir de ces volumes doivent être *peered*. Une relation de pairs permet l'échange de clusters et de SVM sécurité des données.



Vous pouvez également créer une relation de protection des données entre les SVM. Dans ce type de relation, toute ou partie de la configuration du SVM, depuis les exportations NFS et les partages SMB vers le RBAC, est répliquée, ainsi que les données au sein des volumes dont est propriétaire le SVM.

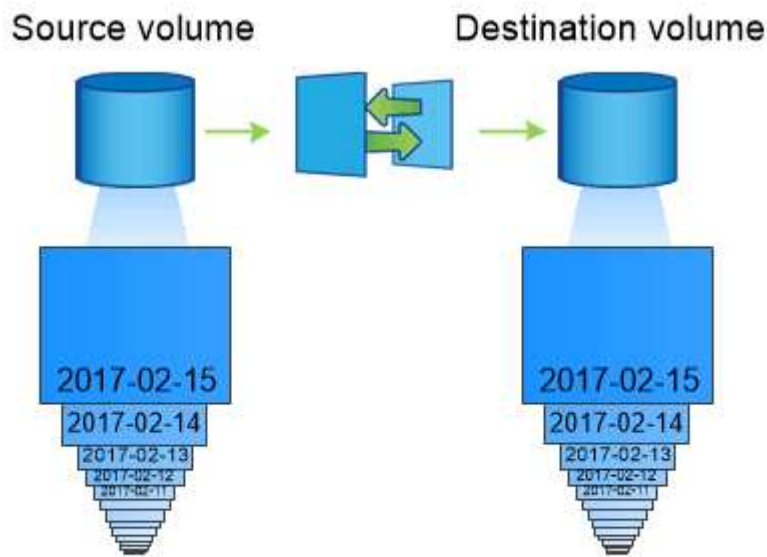
À partir de ONTAP 9.10.1, vous pouvez créer des relations de protection des données entre les compartiments S3 à l'aide de SnapMirror S3. Les compartiments de destination peuvent être sur les systèmes ONTAP locaux ou distants, ou sur les systèmes non ONTAP tels qu'StorageGRID et AWS.

La première fois que vous appelez SnapMirror, il effectue un *transfert de base* du volume source vers le volume de destination. Le transfert de base implique généralement les étapes suivantes :

- Créer une copie Snapshot du volume source.
- Transférez la copie Snapshot et tous les blocs de données qu'elle référence vers le volume de destination.
- Transférez les copies Snapshot restantes et moins récentes sur le volume source vers le volume de destination pour toute utilisation en cas de corruption du miroir « actif ».

Une fois le transfert de base terminé, SnapMirror transfère uniquement les nouvelles copies Snapshot vers le miroir. Les mises à jour sont asynchrones, en fonction du planning que vous configurez. La conservation met en miroir la règle Snapshot sur la source. Vous pouvez activer le volume de destination en cas d'incident au niveau du site primaire et réactiver le volume source une fois le service restauré.

Étant donné que SnapMirror transfère uniquement les copies Snapshot après la création de la copie de base, la réplication est rapide et sans interruption. Comme l'indique le cas de basculement, les contrôleurs du système secondaire doivent être équivalents ou presque équivalents aux contrôleurs du système primaire pour assurer un service efficace des données à partir du stockage en miroir.



A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

utilisation de SnapMirror pour le transfert de données

Vous pouvez également utiliser SnapMirror pour répliquer les données entre les terminaux de NetApp Data Fabric. Lorsque vous créez la règle SnapMirror, vous avez le choix entre une réplication ponctuelle ou une réplication récurrente.

Sauvegardes SnapMirror dans le cloud sur le stockage objet

SnapMirror est une technologie de sauvegarde et de restauration conçue pour les utilisateurs ONTAP qui souhaitent migrer leurs workflows de protection des données vers le cloud. Les entreprises qui se détournent de leurs architectures de sauvegarde sur bande existantes peuvent utiliser le stockage objet comme référentiel alternatif pour la conservation et l'archivage des données à long terme. SnapMirror Cloud permet la réplication du stockage ONTAP vers objet dans le cadre d'une stratégie de sauvegarde incrémentielle à l'infini.

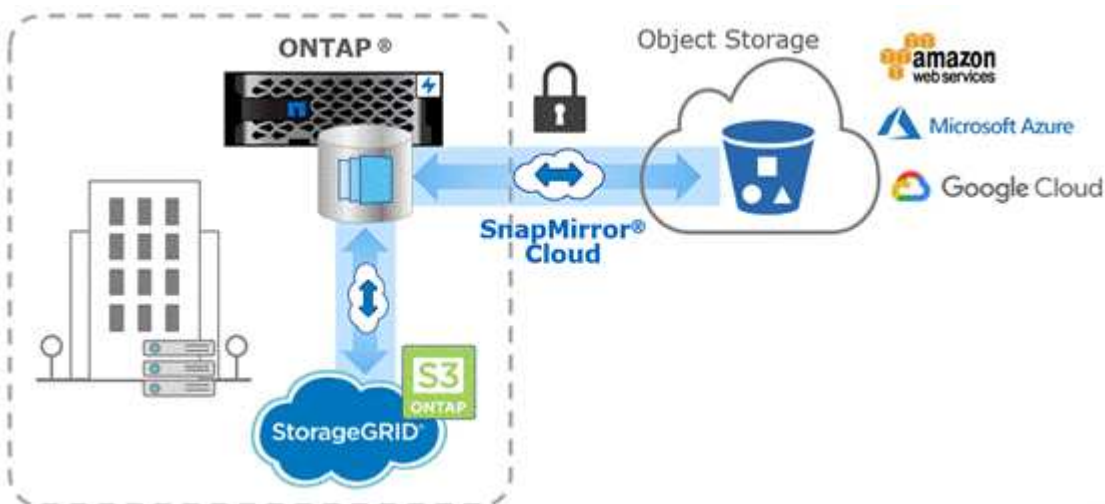
SnapMirror Cloud a été introduit dans ONTAP 9.8 en tant qu'extension de la gamme de technologies de réplication SnapMirror. Même si SnapMirror est fréquemment utilisé pour les sauvegardes ONTAP à ONTAP, SnapMirror Cloud utilise le même moteur de réplication pour transférer les copies Snapshot pour ONTAP vers des sauvegardes de stockage objet conformes S3.

Conçu pour les sauvegardes, SnapMirror Cloud prend en charge à la fois les workflows de conservation et d'archivage à long terme. Tout comme SnapMirror, la sauvegarde SnapMirror Cloud initiale effectue un transfert de base d'un volume. Pour les sauvegardes ultérieures, SnapMirror Cloud génère une copie Snapshot du volume source et transfère la copie Snapshot avec uniquement les blocs de données modifiés vers une cible de stockage objet.

Les relations SnapMirror Cloud peuvent être configurées entre les systèmes ONTAP et certaines cibles de stockage objet sur site et dans le cloud public, notamment Amazon S3, Google Cloud Storage et Microsoft Azure Blob Storage. Des cibles supplémentaires de stockage objet sur site incluent StorageGRID et ONTAP S3.

La réplication SnapMirror Cloud est une fonctionnalité ONTAP sous licence. Elle requiert une application approuvée pour orchestrer les workflows de protection des données. Plusieurs options d'orchestration sont disponibles pour la gestion des sauvegardes SnapMirror Cloud :

- Plusieurs partenaires de sauvegarde tiers qui prennent en charge la réplication SnapMirror Cloud. Les fournisseurs participants sont disponibles sur le ["Blog NetApp"](#).
- Sauvegarde et restauration BlueXP pour une solution NetApp native pour les environnements ONTAP
- API pour développer des logiciels personnalisés pour les workflows de protection des données ou exploiter les outils d'automatisation



Archivage SnapVault

La licence SnapMirror permet la prise en charge des relations SnapVault pour la sauvegarde et des relations SnapMirror pour la reprise sur incident. À partir de ONTAP 9.3, les licences SnapVault sont obsolètes et les licences SnapMirror peuvent être utilisées pour configurer les relations Vault, mirror et mirror-and-vault. La réplication SnapMirror est utilisée pour la réplication ONTAP vers ONTAP des copies Snapshot, et prend en charge à la fois des opérations de sauvegarde et de reprise d'activité.

SnapVault est une technologie d'archivage conçue pour la réplication de copie Snapshot disque à disque à des fins de conformité aux normes et autres pour la gouvernance. Contrairement à une relation SnapMirror, dans laquelle la destination contient généralement uniquement les copies Snapshot actuellement dans le volume source, la destination SnapVault conserve en général les copies Snapshot instantanées créées sur une période bien plus longue.

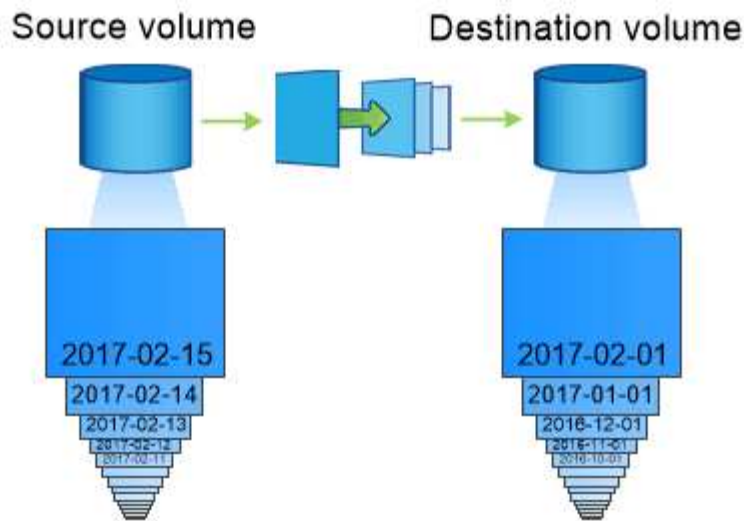
Vous pouvez conserver tous les mois des copies Snapshot de vos données sur une période de 20 ans, par exemple, pour vous conformer aux réglementations gouvernementales relatives à la comptabilité de votre entreprise. Etant donné qu'il n'est pas nécessaire de transmettre des données à partir du stockage Vault, vous pouvez utiliser des disques plus lents et moins coûteux sur le système de destination.

Tout comme SnapMirror, SnapVault effectue un transfert de base dès la première fois que vous l'appellez. Il effectue une copie Snapshot du volume source, puis transfère la copie et les blocs de données qu'il renvoie vers le volume de destination. Contrairement à SnapMirror, SnapVault n'inclut pas d'anciennes copies Snapshot dans la configuration de base.

Les mises à jour sont asynchrones, en fonction du planning que vous configurez. Les règles que vous définissez dans la règle pour la relation identifient les nouvelles copies Snapshot à inclure dans les mises à jour et le nombre de copies à conserver. Les libellés définis dans la politique (« mensuel », par exemple) doivent correspondre à un ou plusieurs libellés définis dans la politique Snapshot de la source. Dans le cas contraire, la réplication échoue.



SnapMirror et SnapVault partagent la même infrastructure de commandes. Vous spécifiez la méthode à utiliser lors de la création d'une stratégie. Les deux méthodes exigent des clusters de peering et des SVM.



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

Sauvegarde dans le cloud et prise en charge des sauvegardes classiques

Outre les relations de protection des données SnapMirror et SnapVault, qui étaient disque à disque uniquement pour ONTAP 9.7 et les versions antérieures, plusieurs solutions de sauvegarde offrent une alternative moins onéreuse pour la conservation à long terme des données.

De nombreuses applications tierces de protection des données proposent des sauvegardes classiques pour les données gérées par ONTAP. Veeam, Veritas et CommVault entre autres proposent une sauvegarde intégrée pour les systèmes ONTAP.

Depuis ONTAP 9.8, SnapMirror Cloud permet la réplication asynchrone des copies Snapshot à partir d'instances ONTAP vers les terminaux de stockage objet. La réplication SnapMirror Cloud requiert une application sous licence pour l'orchestration et la gestion des workflows de protection des données. Les relations SnapMirror avec le cloud sont prises en charge par les systèmes ONTAP afin de sélectionner des cibles de stockage objet sur site et dans le cloud public, notamment AWS S3, Google Cloud Storage Platform ou Microsoft Azure Blob Storage, qui améliorent l'efficacité avec les logiciels de sauvegarde des fournisseurs. Contactez votre conseiller NetApp pour obtenir une liste des fournisseurs d'applications certifiées et de stockage objet pris en charge.

Si la protection des données native du cloud vous intéresse, BlueXP peut être utilisé pour configurer les relations SnapMirror ou SnapVault entre les volumes sur site et les instances Cloud Volumes ONTAP dans le cloud public.

BlueXP fournit également des sauvegardes d'instances Cloud Volumes ONTAP à l'aide d'un modèle SaaS. Les utilisateurs peuvent sauvegarder leurs instances Cloud Volumes ONTAP dans le stockage objet de cloud public compatible S3 et S3 à l'aide de Cloud Backup disponible sur NetApp Cloud Central.

["Ressources de documentation Cloud Volumes ONTAP et BlueXP"](#)

Disponibilité sans interruption avec MetroCluster

Les configurations MetroCluster protègent les données grâce à la mise en œuvre de deux clusters en miroir séparés physiquement. Chaque cluster réplique de manière synchrone les données et la configuration SVM de l'autre. En cas d'incident sur un site, un administrateur peut activer la SVM en miroir et commencer à transférer les données depuis le site survivant.

- Les *configurations MetroCluster* reliées à la structure prennent en charge les clusters à l'échelle de la zone métropolitaine.
- *Stretch MetroCluster* configurations prennent en charge les clusters à l'échelle du campus.

Les grappes doivent être pételées dans les deux cas.

MetroCluster utilise la fonctionnalité ONTAP appelée *SyncMirror* pour mettre en miroir de manière synchrone les données d'agrégats pour chaque cluster dans des copies, ou *plex*, dans le stockage de l'autre cluster. En cas de basculement, le plex distant sur le cluster survivant est mis en ligne et le SVM secondaire commence à transmettre les données.



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

utilisation de SyncMirror dans des implémentations non MetroCluster

Vous pouvez, par ailleurs, utiliser SyncMirror dans une implémentation non MetroCluster pour vous protéger contre la perte de données si le nombre de disques défaillants est supérieur à la protection du type RAID ou en cas de perte de connectivité avec les disques du groupe RAID. La fonctionnalité est disponible uniquement pour les paires haute disponibilité.

Les données agrégées sont mises en miroir dans des plexes stockés sur différents tiroirs disques. Si l'un des tiroirs n'est plus disponible, le plex non affecté continue à transmettre des données pendant que vous corrigez la défaillance.

N'oubliez pas qu'un agrégat en miroir avec SyncMirror nécessite deux fois plus de stockage qu'un agrégat non mis en miroir. Chaque plex requiert autant de disques que le plex IT miroirs. Vous auriez besoin de 2,880 Go d'espace disque, par exemple pour mettre en miroir un agrégat de 1,440 Go, 1,440 Go par plex.

Avec SyncMirror, il est recommandé de conserver au moins 20 % d'espace libre pour les agrégats en miroir pour une disponibilité et des performances de stockage optimales. Bien que la recommandation soit de 10 % pour les agrégats non mis en miroir, le système de fichiers peut utiliser 10 % d'espace supplémentaire pour absorber les modifications incrémentielles. Les modifications incrémentielles augmentent l'utilisation de l'espace pour les agrégats en miroir grâce à l'architecture Snapshot d'ONTAP basée sur la copie en écriture. Le non-respect de ces bonnes pratiques peut avoir un impact négatif sur les performances de resynchronisation SyncMirror, qui a un impact indirect sur les workflows opérationnels, tels que la mise à niveau sans interruption pour les déploiements cloud non partagés et la reprise pour les déploiements MetroCluster.



SyncMirror est également disponible pour les implémentations de virtualisation FlexArray.

Informations sur le copyright

Copyright © 2024 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.